Source:	**TSG SA WG2**
Title:	**CRs on 23.228 (IMS Phase 2)**
Agenda item:	**7.2.3**
Document for:	**APPROVAL**

The following CRs have been agreed by TSG SA WG2 and are requested to be approved by TSG SA plenary #26.

Note: the source of all these CRs is now SA2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

S2 doc #	Title	Spec	CR #	Rev	Cat	C_Ver	Rel	WI
S2-043364	Treatment of SIP forking request	23.228	446	3	F	6.7.0	Rel-6	IMS2
S2-043332	Floor control	23.228	447	1	F	6.7.0	Rel-6	IMS2
S2-043335	Clarification of which origination and termination procedures can be used to construct end to end session flows	23.228	448	1	F	6.7.0	Rel-6	IMS2
S2-043336	Put the non-IMS SIP network interworking scenarios in the correct clauses	23.228	449	1	F	6.7.0	Rel-6	IMS2
S2-043341	Clarify that IMS end-points shall be able to support sending or receiving DTMF tone indications	23.228	450	1	F	6.7.0	Rel-6	IMS2
S2-043338	"Clarification of which endpoints may be involved in Session Redirects and	23.228	451	1	F	6.7.0	Rel-6	IMS2
S2-043794	Addition of Application Server termination section	23.228	452	3	F	6.7.0	Rel-6	IMS2
S2-043842	Revision of session set-up from external SIP client	23.228	453	4	F	6.7.0	Rel-6	IMS2
S2-043791	Various editorial corrections	23.228	454	1	D	6.7.0	Rel-6	IMS2
S2-043472	Missing step in identity procedure	23.228	455		F	6.7.0	Rel-6	IMS2
S2-043473	Correction to PSTN Termination	23.228	456		F	6.7.0	Rel-6	IMS2
S2-043792	Removal of support for local services	23.228	458	1	F	6.7.0	Rel-6	IMS2
S2-043476	Removal of Editor's Note on ISC	23.228	459		F	6.7.0	Rel-6	IMS2
S2-043477	Changes to SIP URL terminology	23.228	460		F	6.7.0	Rel-6	IMS2
S2-043843	Reorganization and clarification of session flows	23.228	461	2	F	6.7.0	Rel-6	IMS2
S2-043795	Changes for commonality in regards to token generation	23.228	462	1	F	6.7.0	Rel-6	IMSCOOP
S2-043807	Tel-URI related reference updates	23.228	464	1	D	6.7.0	Rel-6	IMS2
S2-043571	Forward HSS name	23.228	465		F	5.12.0	Rel-5	IMS-CCR
S2-043572	Forward HSS name	23.228	466		A	6.7.0	Rel-6	IMS-CCR
S2-043808	Informing AS on Registration	23.228	467	1	F	6.7.0	Rel-6	IMS2

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.228 CR 447** ⌘**rev 1** ⌘ Current version: **6.7.0** ⌘

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: ⌘	Floor Control		

Source: ⌘	Siemens

Work item code:⌘	IMS2	***Date:*** ⌘	13/10/2004

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: ⌘	There is misalignment between TS 23.228 and TS 24.147. According to the stage 3 specification TS 24.147 (clause 8) the floor control protocol terminates at the MRFP rather than in the control plane.
Summary of change:⌘	Delete floor control as task of a conferencing AS; add floor control as MRFP functionality.
Consequences if not approved: ⌘	Misalignment between TS 23.228 and TS 24.147.

Clauses affected: ⌘	4.7

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	23.002, CR
		X	Test specifications		
		X	O&M Specifications		

Other comments: ⌘	

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

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

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

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

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

4.7   Multimedia Resource Function

The architecture concerning the Multimedia Resource Function is presented in Figure 4.5a below.
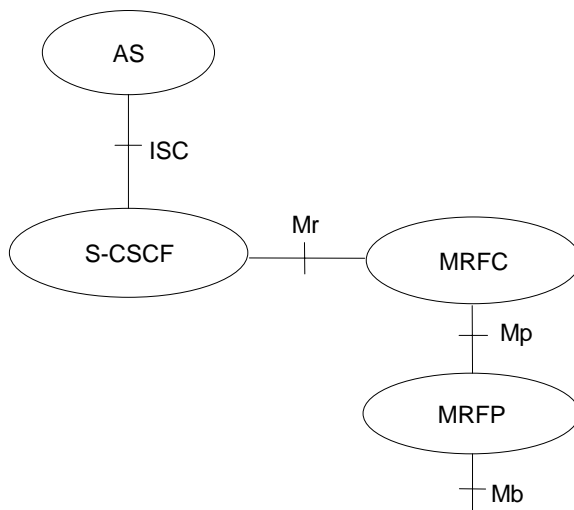

Figure 4.7: Architecture of MRF

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)

- ~~Provide a floor control mechanism, by which end users (e.g. participants, chairman) can influence floor and provide information to the MRFC on how incoming media streams should be mixed and distributed accordingly.~~

The protocol used for the Mr reference point is SIP (as defined by RFC 3261 [12], other relevant RFC's, and additional enhancements introduced to support 3GPP´s needs).

The Mp reference point allows an MRFC to control media stream resources provided by an MRFP.

The Mp reference point has the following properties:

- Full compliance with the H.248 standard.

- Open architecture where extensions (packages) definition work on the interface may be carried out.

The protocol for the Mp reference point is not specified in this release.

3GPP TSG-SA WG2 Meeting #42
Sophia Antipolis, France. October 11-15, 2004.

Tdoc ⌘ S2-043335

was *S2-043264*

CR-Form-v7.1

CHANGE REQUEST

⌘　　　**23.228** CR **448**　⌘**rev** **1** ⌘　Current version: **6.7.0** ⌘

*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: ⌘	Clarification of which origination and termination procedures can be used to construct end to end session flows
Source: ⌘	Lucent Technologies

Work item code: ⌘	IMS2	***Date:*** ⌘	14/10/2004

Category: ⌘	**F**	***Release:*** ⌘	Rel-6

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

Use one of the following releases:
   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: ⌘	Addition of new origination and termination procedures to 23.228 during Release 6 haven't been fully integrated into the text of sub-clause 5.4.10 and 5.5. This means that the full range of end to end sessions may not be understood from reading the specification.
Summary of change: ⌘	Origination and termination procedures that have already been added to 23.228 are now named in 5.4.10 and included in table 5.2. In addition, clause 5 is updated to ensure the definition of which origination and termination procedures use which S-CSCF to S-CSCF procedures are only defined in one place (in table 5.2).
Consequences if not approved: ⌘	Confusion is likely as to which end to end scenarios can be constructed from the origination, termination and S-CSCF to S-CSCF procedures.

Clauses affected: ⌘	5.4.10, 5.5.1, 5.5.2, 5.5.3, 5.5.4

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

| *Other comments:* | ⌘ | Note that this CR assumes the approval of CR 449 and CR452 to 23.228. |

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.

*** Changes to clause 5.4.10 ***

5.4.10 Overview of session flow procedures

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

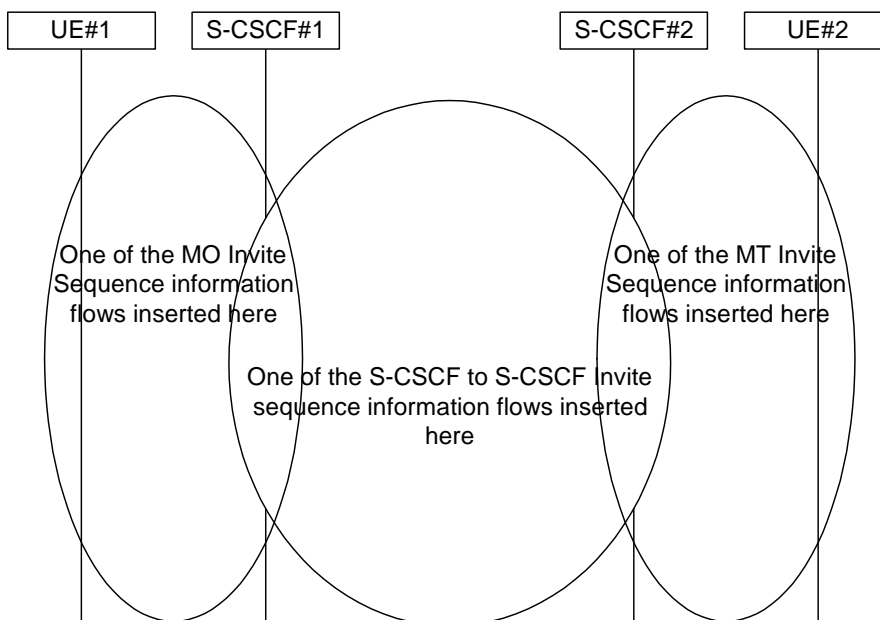For an IP Multi-Media Subsystem session, the session flow procedures are shown in the following diagram.

Figure 5.9: Overview of Session Flow Sections

The following procedures are defined:

For the origination sequence:

- (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

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

- (NI-O) Non-IMS network termination (external SIP client), see subclause 5.6.6

For the termination sequence:

- (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

- (AS-T#1) PSI Application Server termination, direct, see subclause 5.4.12.2

- (AS-T#2) PSI Application Server termination, indirect, see subclause 5.4.12.2

- (AS-T#3) PSI Application Server termination, direct, using DNS, see subclause 5.4.12.3

- (AS-T#4) PUI Application Server termination, indirect, see subclause 5.7.5

- (NI-T) Non-IMS network termination (external SIP client), see subclause 5.7.6

For Serving-CSCF/MGCF-to-Serving-CSCF/MGCF sequences (see subclause 5.5):

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

- (S-S#2) Session origination and termination are served by the same operator.

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

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

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 Non-IMS network 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. AS-T#1,2,3 Application Server terminations 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 Non-IMS network origination	~~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.

~~In addition, variants of MO#1, MO#2, MT#1 and MT#2 are supported for interworking with external SIP clients, which do not support the SIP extensions required for IMS end points. These variants are not used in combination with any other session procedure.~~

*** End of changes to clause 5.4.10 ***

*** Changes to clause 5.5 ***

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 subclause 5.4.10 to see which ~~Origination~~ origination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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-O PSTN origination. The ~~"~~"Originating Network~~"~~" of S-S#1 is the home network. The element labeled S-CSCF#1 is the MGCF of the PSTN-O procedure.

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

NI-O Non-IMS network origination. The external SIP client of figure 5.16f 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.
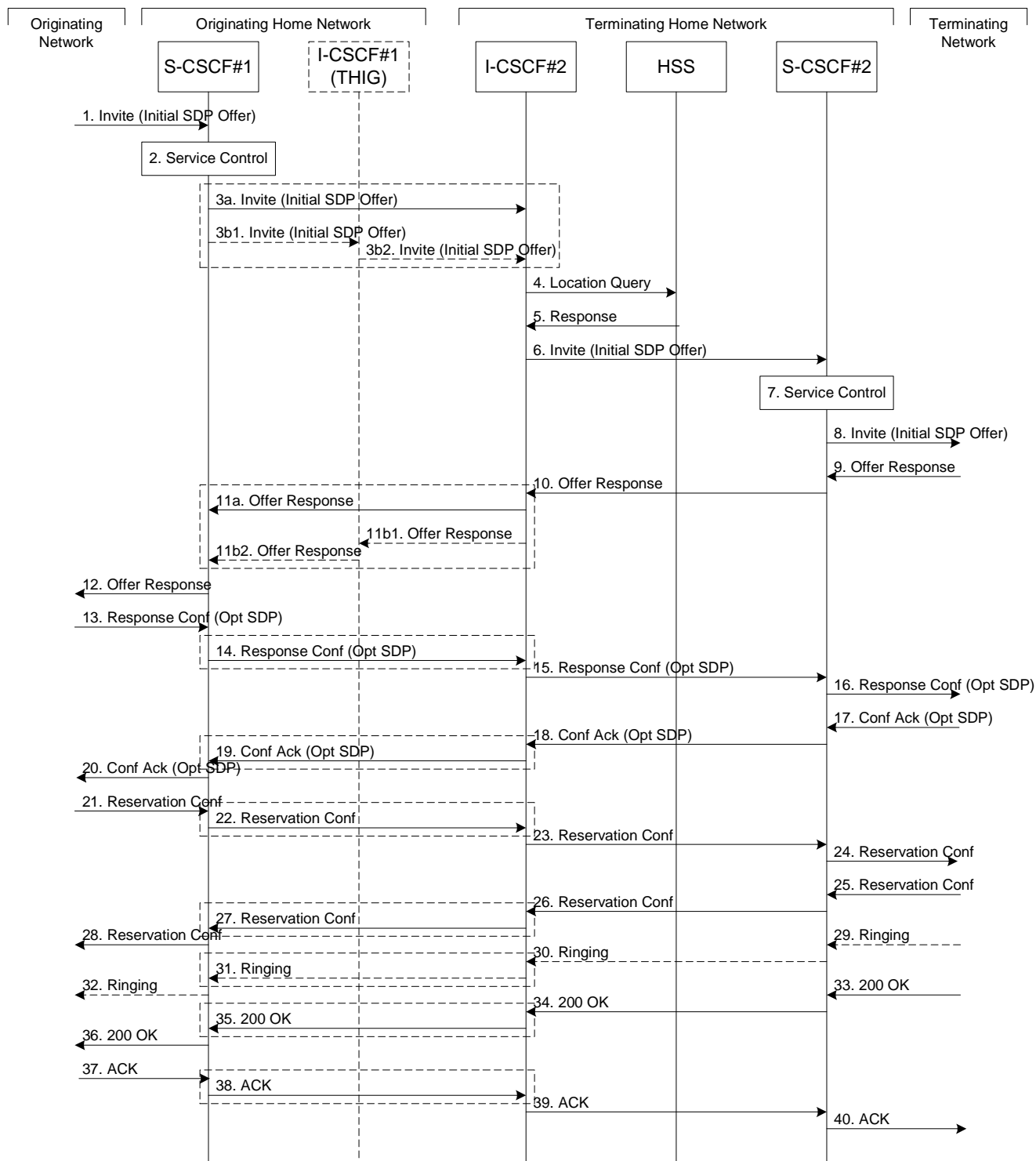
Refer to table 5.2 in subclause 5.4.10 to see which ~~Termination~~ termination sequences ~~that~~ share this common S-S procedure~~.~~ ~~are:~~ In addition the text below clarifies the role of the "Terminating Network".

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 (5.4.12a, 5.4.12b, 5.4.12c, 5.19c) replace all elements of the Terminating Home Network and Terminating Network of figure 5.10.

NI-T Non-IMS network terminations. The external SIPclient of figure 5.19d 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 subclause 5.4.10 to see which ~~Origination~~ origination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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-O	PSTN 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 5.16d.

NI-O	Non-IMS network origination. This sequence is not valid for S-S#2.

Refer to table 5.2 in subclause 5.4.10 to see which ~~Termination~~ termination sequences ~~that~~ share this common S-S procedure ~~are~~:. 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 (5.4.12a, 5.4.12b, 5.4.12c, 5.19c) replace all elements of the Terminating Home Network and Terminating Network of figure 5.11.

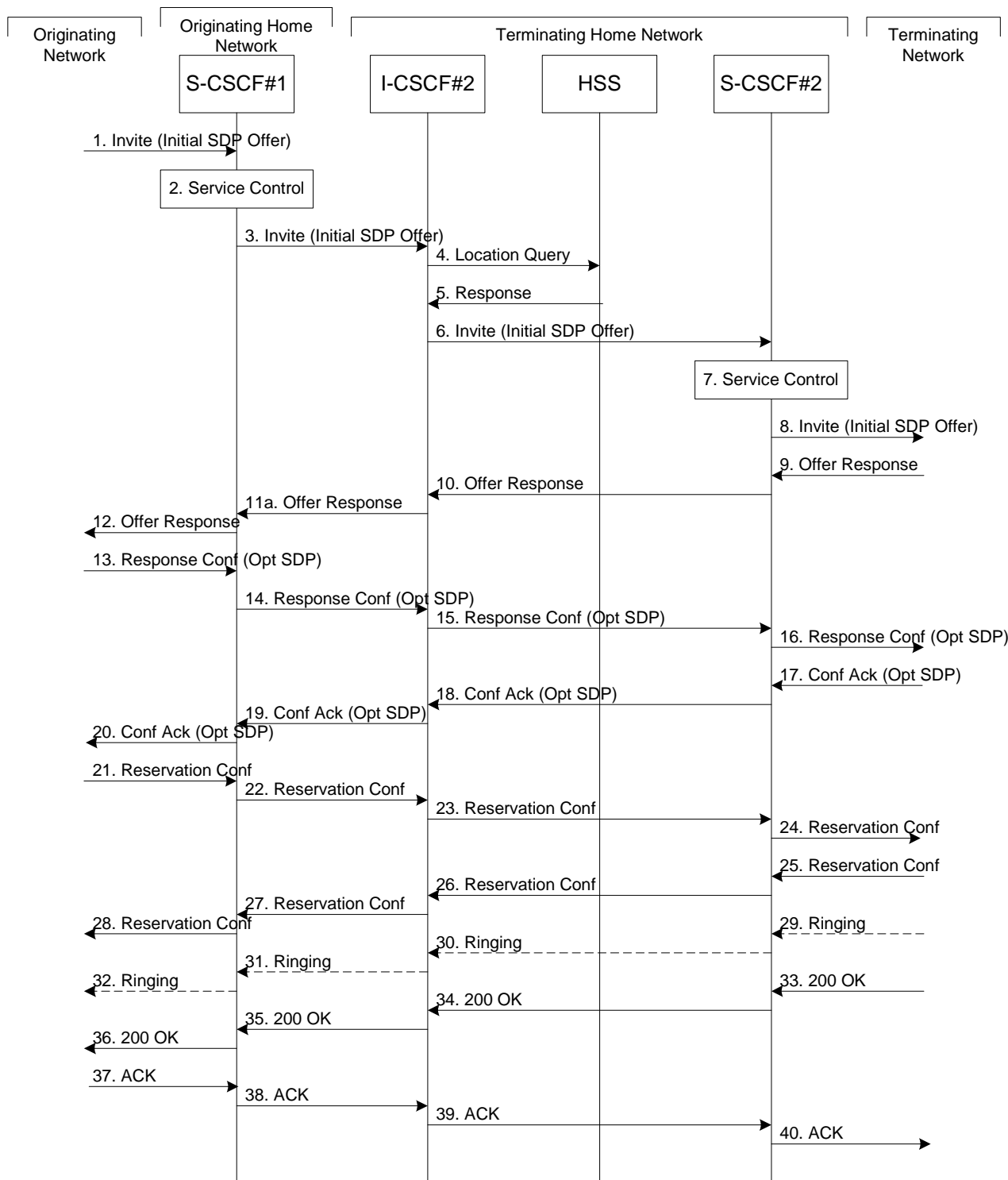NI-T	Non-IMS network termination. This sequence is not valid for S-S#2.

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 subclause 5.4.10 to see which oOrigination sequences that share this common S-S procedure are:. 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-OPSTN origination. The "Originating Network" of S-S#3 is the home network. The element labeled S-CSCF#1 is the MGCF of the PSTN-O procedure.

AS-0   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 5.16d.

NI-O   Non-IMS network origination. This sequence is not valid for S-S#3.

Refer to table 5.2 in subclause 5.4.10 to see which Termination termination sequences that share this common S-S procedure are:. In addition the text below clarifies the role of the "Terminating Network".

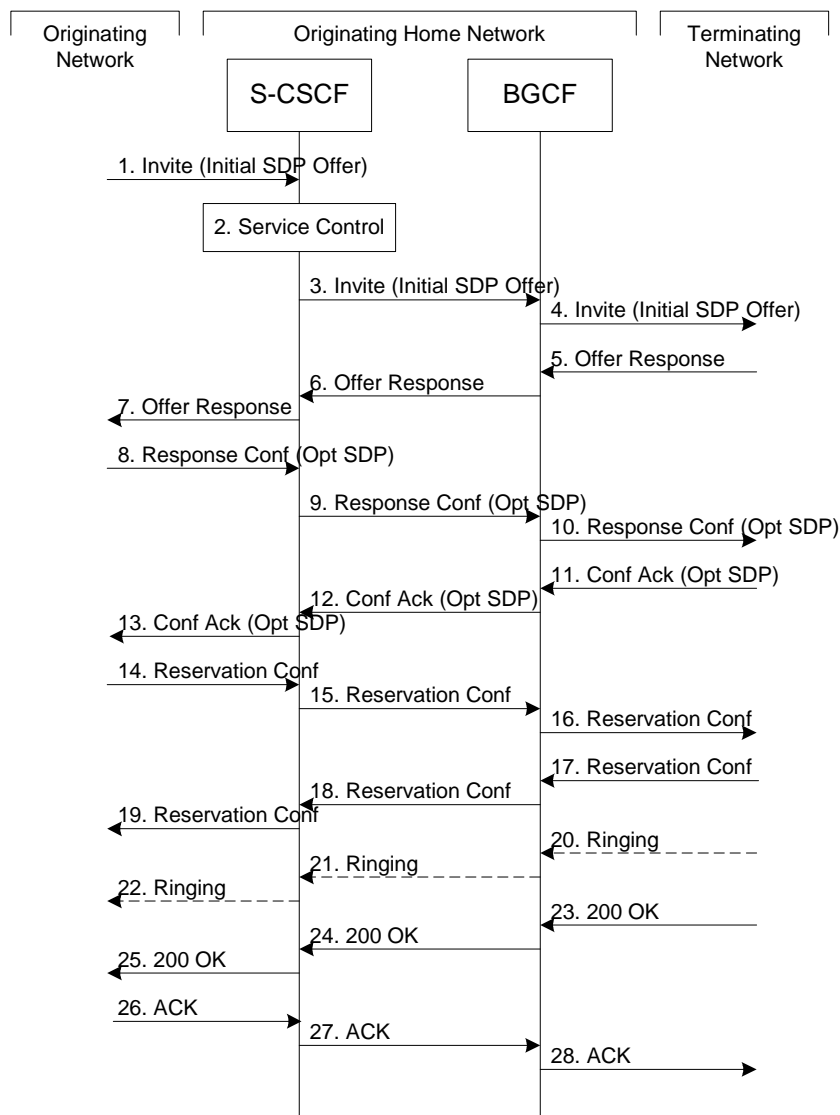PSTN-T PSTN termination. This occurs when the MGCF is selected to be in the same network as the S-CSCF.

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 subclause 5.4.10 to see which ~~Origination~~ origination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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-0   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 5.16d.

NI-O   Non-IMS network origination. The external SIP client of figure 5.16f 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 5.4.10 to see which ~~Termination~~ termination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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.
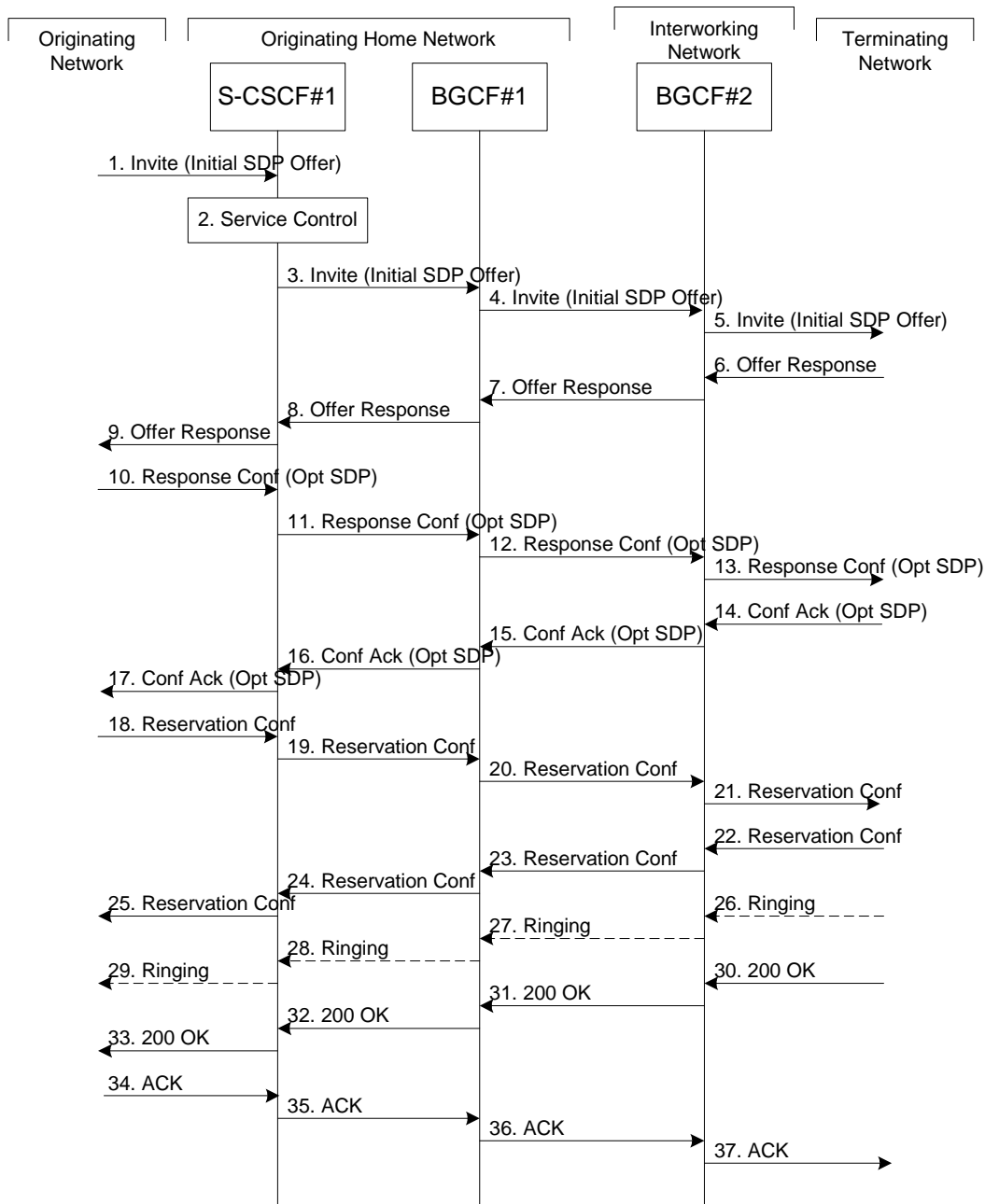
Figure 5.13: Serving to PSTN procedure - different operator

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 originating end answers the session.

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

*** End of changes to clause 5.5 ***

3GPP TSG-SA WG2 Meeting #42
Sophia Antipolis, France. October 11-15, 2004.

Tdoc ⌘ *S2-043336*

CR-Form-v7.1

CHANGE REQUEST

⌘   **23.228** CR **449**   ⌘**rev** **1** ⌘   Current version: **6.7.0** ⌘

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: ⌘	Put the non-IMS SIP network interworking scenarios in the correct sub-clauses	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	IMS2	***Date:*** ⌘ 14/10/2004
Category: ⌘ **F**		***Release:*** ⌘ Rel-6

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

Use one of the following releases:
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 sub-clauses describing the interworking of IMS with non-IMS SIP networks have been placed in the wrong sub-clauses in clause 5. Specifically, 5.6.4 describes a procedure where the non-IMS SIP network is terminating a session yet it has been placed in sub-clause 5.6, Origination procedures. Likewise 5.7.4 describes a procedures where the non-IMS SIP network originates a session but it has been placed in sub-clause 5.7, Termination procedures. The confusion seems to have arisen because the procedures have been interpreted from the IMS UE's point of view rather than from the non-IMS SIP network's point of view. See 5.6.3 for an example of the correct way to categorise a procedure involving IMS interworking to a non-IMS network.
Summary of change: ⌘	Existing sub-clauses 5.6.4 and 5.7.4 are voided and their contents placed in new sub-clauses 5.7.6 and 5.6.6 respectively. The original clause titles have been changed to clarify the meaning of the procedures and minor wording changes made to the first paragraph in each case. Figure numbers will need to be amended as necessary.
Consequences if not approved: ⌘	Document not up to the usual 3GPP SA2 high standards.
Clauses affected: ⌘	5.6.4, 5.6.6 (new), 5.7.4, 5.7.6 (new)

		Y	N		
Other specs affected:	⌘		**X**	Other core specifications ⌘	
			X	Test specifications	

	X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:

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

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

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

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

*** First Modified Text ***

5.6.4 Void~~Mobile Origination procedure towards an external SIP client~~

~~This clause describes the IMS originating 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. Below figures 5.16.a, 5.16.b and 5.16.c 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 clause 5.6.2. The same principles apply in roaming cases, i.e. analogous variants of MO#1 defined in clause 5.6.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.~~

Originating Home Network | Terminating External network

| UE | P-CSCF | S-CSCF | External SIP Client |

1. INVITE Require: Precondition
2. INVITE Require: Precondition
3. INVITE Require: Precondition

4. 420 (Bad Extension) Unsupported: precondition
5. 420 (Bad Extension) Unsupported: precondition
6. 420 (Bad Extension) Unsupported: precondition
7. ACK
8. ACK
9. ACK

3GPP UAC creates an INVITE that does not require precondition support. It sets the media components inactive, see following flows

~~Figure 5.16a. Originating session towards external SIP client, detection phase~~

~~The Originating 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.~~
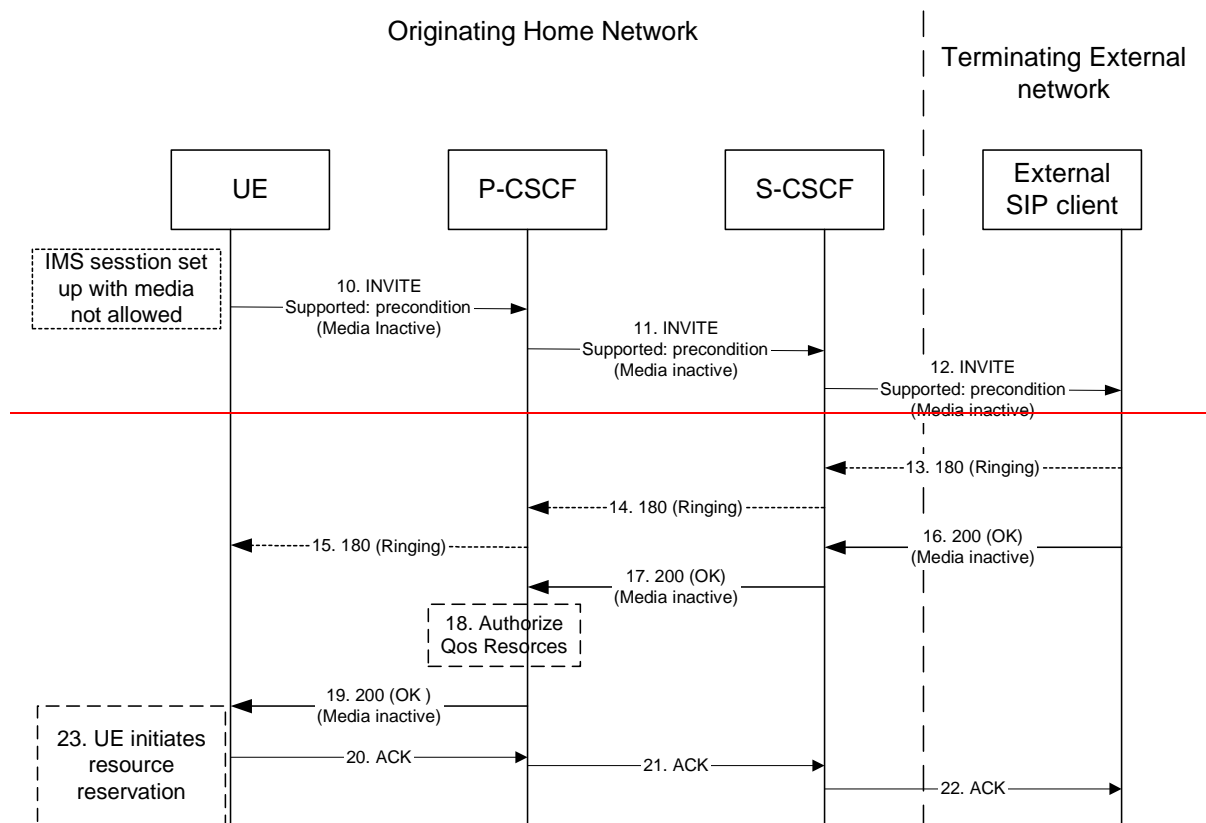
Figure 5.16b. Originating session towards external SIP client, re-initiate session set up not requiring precondition capabilities and with inactive media

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 5.16b & 5.16c.

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 5.16c. Continuation of originating 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 5.16c.

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.

*** End of First Modified Text ***

*** Second Modified Text ***

5.6.6   Origination from an external SIP client

This subclause 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 parameters have been negotiated and accepted. Figures 5.16e and 5.16f show 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 subclause 5.7.2. The same principles apply in roaming cases, i.e. analogous variants of MT#1 defined in subclause 5.7.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
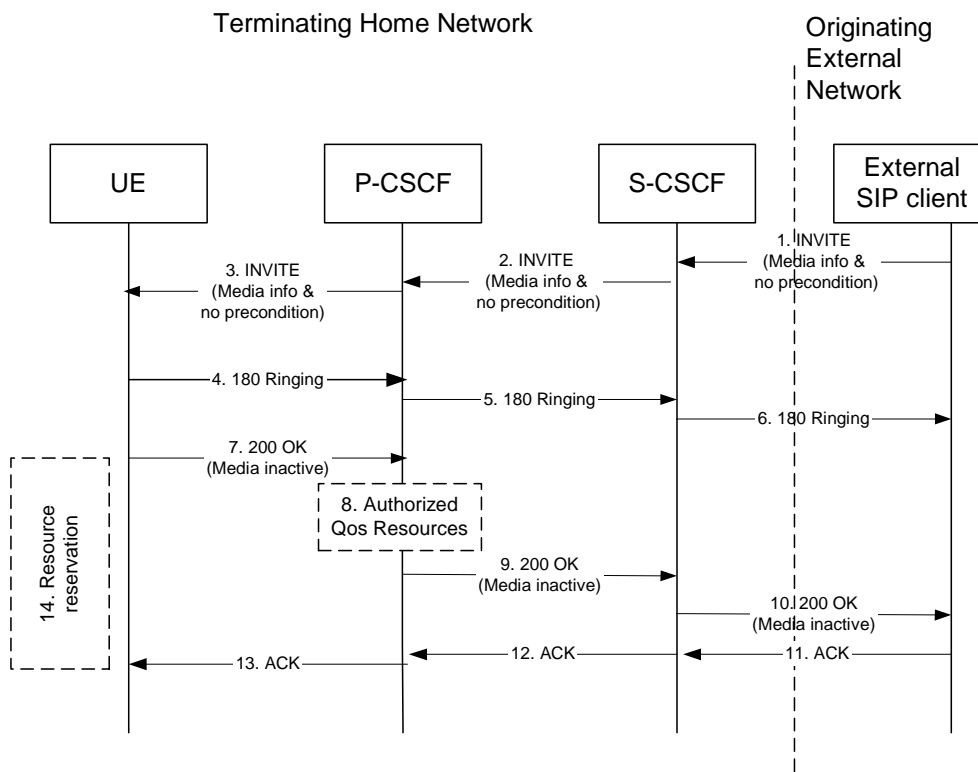
Figure 5.16e: Terminating session from external SIP client, detection & initial setup with media not allowed

1-3.   A session arrives at the UE in the IMS network with media information but without requiring precondition capability.

4-6.   Ringing information is sent end to end towards the originating party.

7-10.   The UE begins the resource reservation according to the session and media parameters. The P-CSCF/PDF may authorise the media parameters being negotiated and the originating party is notified of the session setup details with all media components set to inactive.

11-13. The originating party acknowledges the session.

14. When the UE has completed the resource reservation procedures, the UE continues with the session setup according to figure 5.16f. The UE sets the media components to active state.
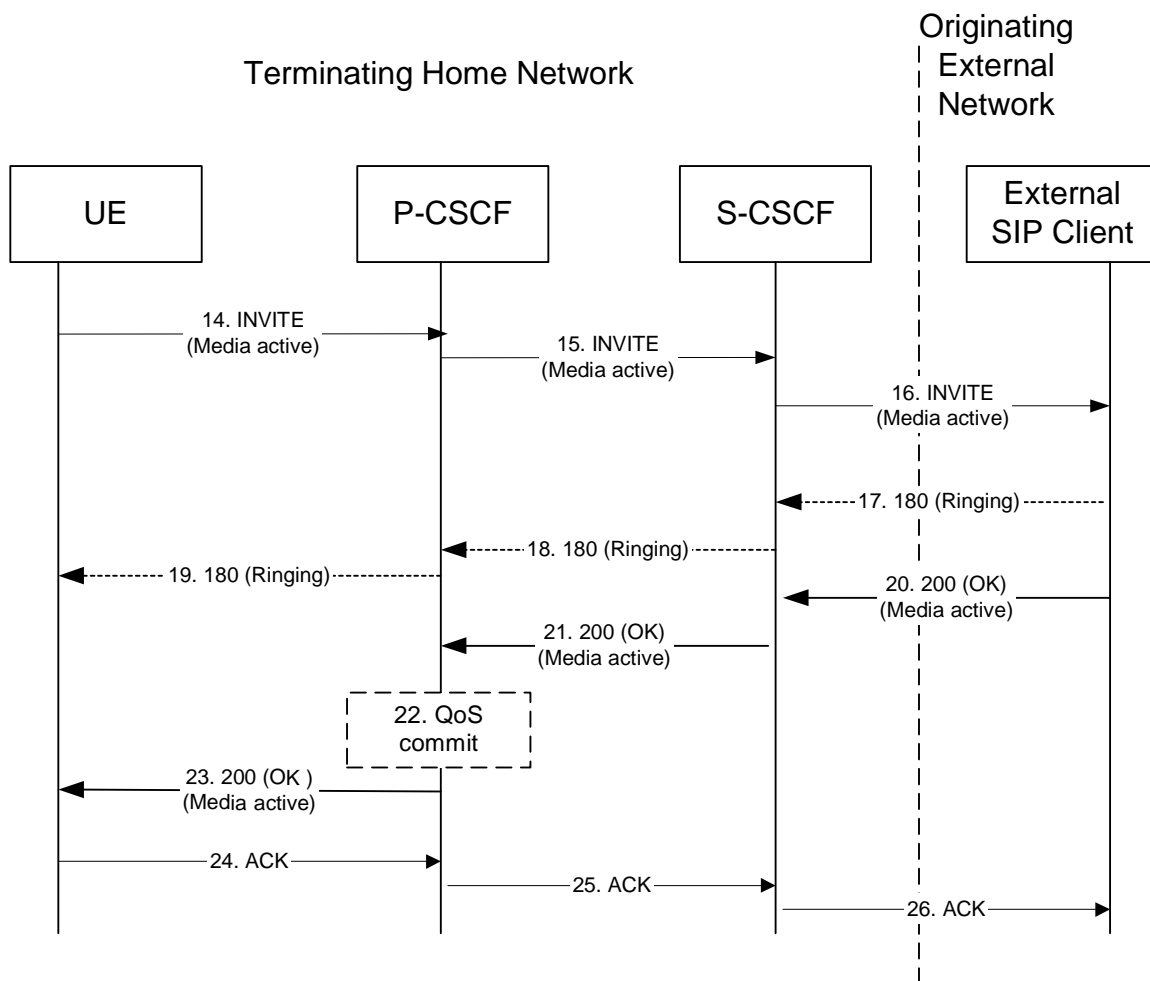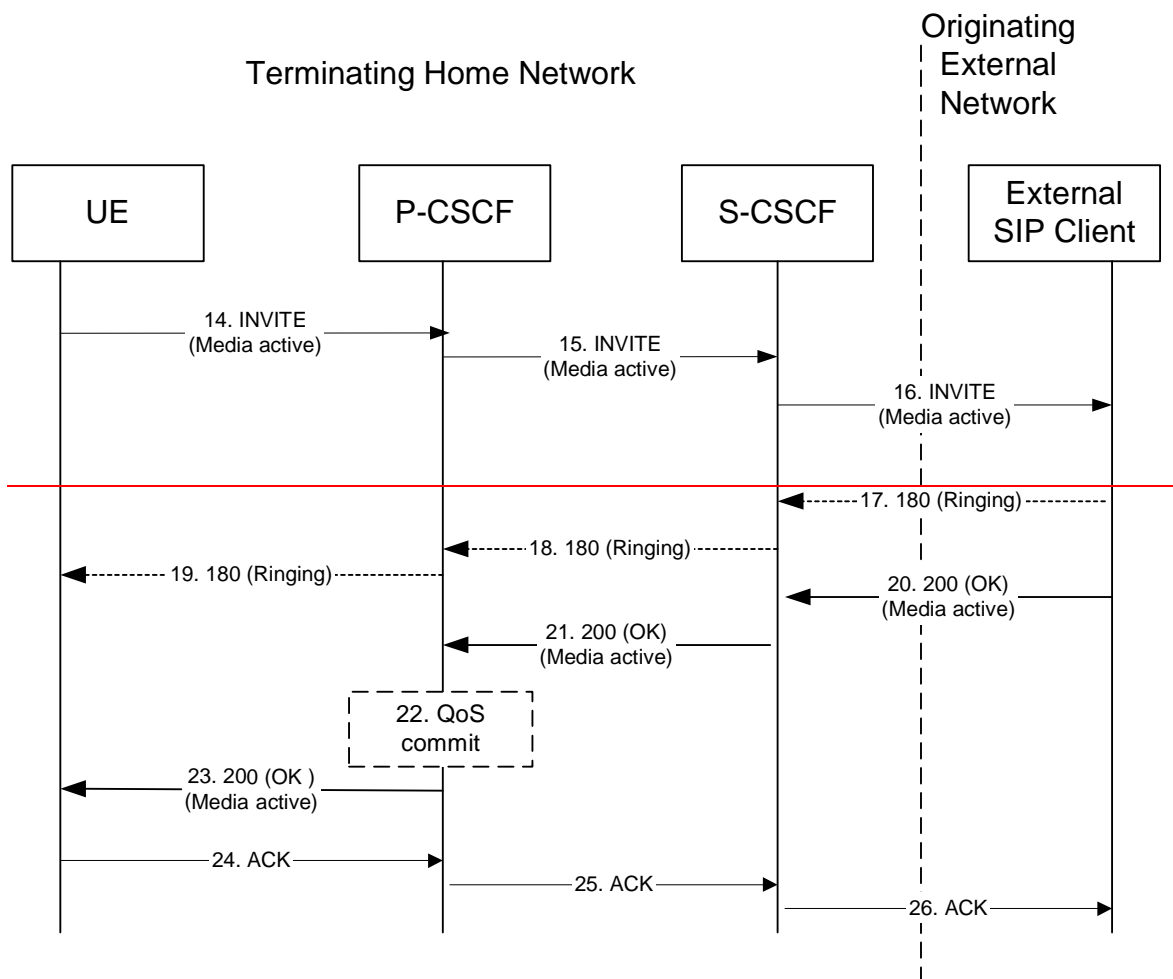
Figure 5.16f: Continuation of terminating session from external SIP client, session setup with active media

14-16. By sending a re-INVITE indicating the support for the precondition capability, the terminating UE initiates setting of media components to active.

17-19. Ringing Information may be sent from an external SIP entity (in this case the originating party) through the session path towards the terminating UE.

20-23. The originating SIP client accepts the re-INVITE with the active media streams. In step 22, The P-CSCF/PDF may commit/approve the resources authorised for the session.

Session is acknowledged end-to-end.

*** End of Second Modified Text ***

*** Third Modified Text ***

5.7.4 Void~~Mobile Termination from an external SIP client~~

~~This clause describes the terminating session setup procedures 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 parameters have been negotiated and accepted. Session flows 5.19a and 5.19b show 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 clause 5.7.2. The same principles apply in roaming cases, i.e. analogous variants of MT#1 defined in clause 5.7.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.

Figure 5.19a. Terminating session from external SIP client, detection & initial setup with media not allowed

1-3. A session arrives at the UE in the IMS network with media information but without requiring precondition capability.

4-6. Ringing information is sent end to end towards the originating party.

7-10. The UE begins the resource reservation according to the session and media parameters. The P-CSCF/PDF may authorise the media parameters being negotiated and the originating party is notified of the session setup details with all media components set to inactive.

11-13. The originating party acknowledges the session.

14. When the UE has completed the resource reservation procedures, the UE continues with the session setup according to flow 5.19b. The UE sets the media components to active state.

Figure 5.19b. Continuation of terminating session from external SIP client, session setup with active media

14-16. By sending a re-INVITE indicating the support for the precondition capability, the terminating UE initiates setting of media components to active.

17-19. Ringing Information may be sent from an external SIP entity (in this case the originating party) through the session path towards the terminating UE.

20-23. The originating SIP client accepts the re-INVITE with the active media streams. In step 22, The P-CSCF/PDF may commit/approve the resources authorised for the session.

24-26. Session is acknowledged end-to-end.

*** End of Third Modified Text ***

*** Fourth Modified Text ***

5.7.6 Termination at external SIP client

This subclause 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 5.19d, 5.19e and 5.19f 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 subclause 5.6.2. The same principles apply in roaming cases, i.e. analogous variants of MO#1 defined in subclause 5.6.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
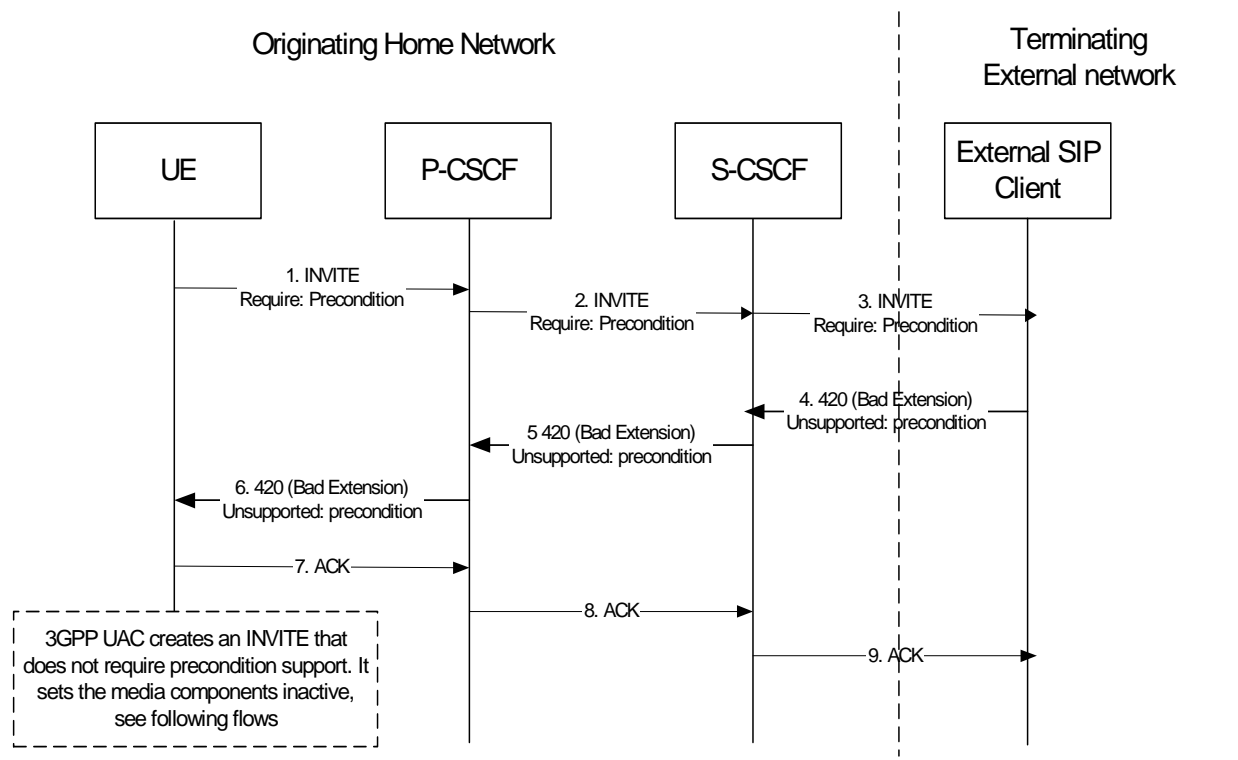
Figure 5.19d: Originating session towards external SIP client, detection phase

The Originating 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.
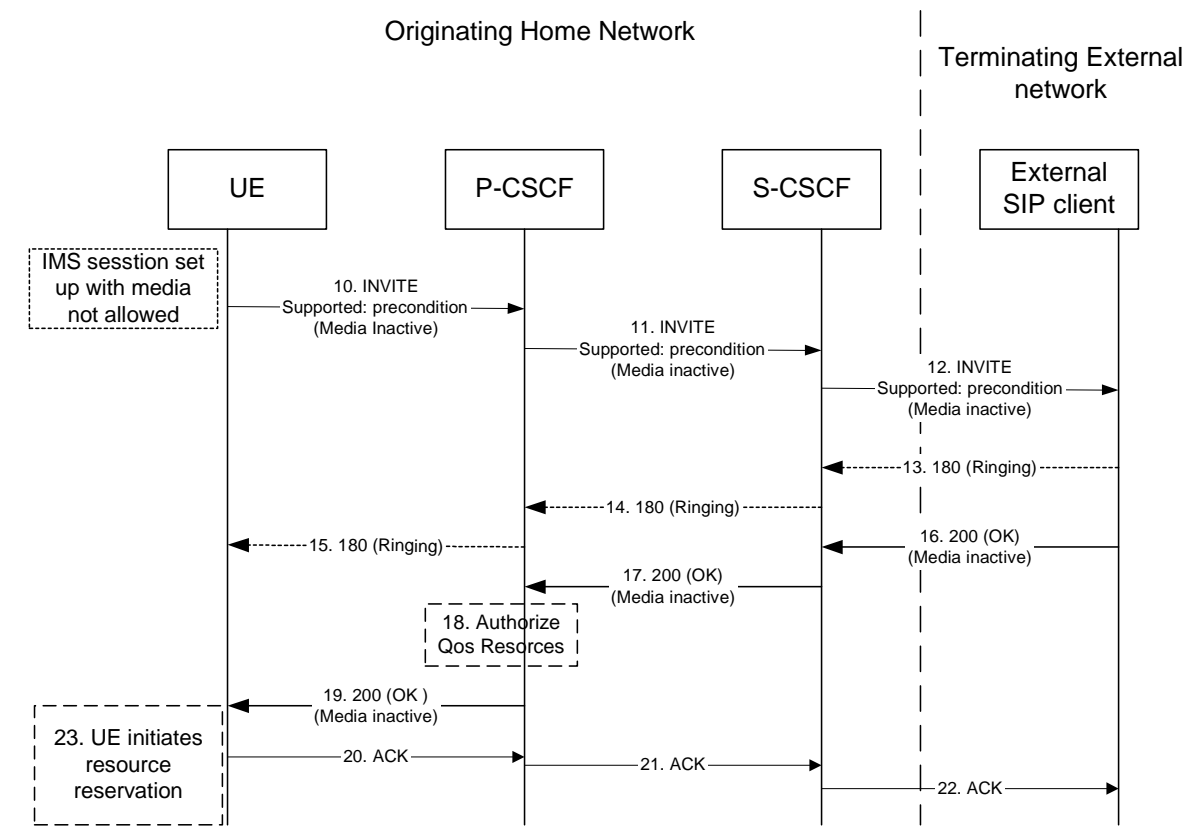
Figure 5.19e: Originating session towards external SIP client, re-initiate session set up not requiring precondition capabilities and with inactive media

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 figures 5.19e & 5.19f.

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.
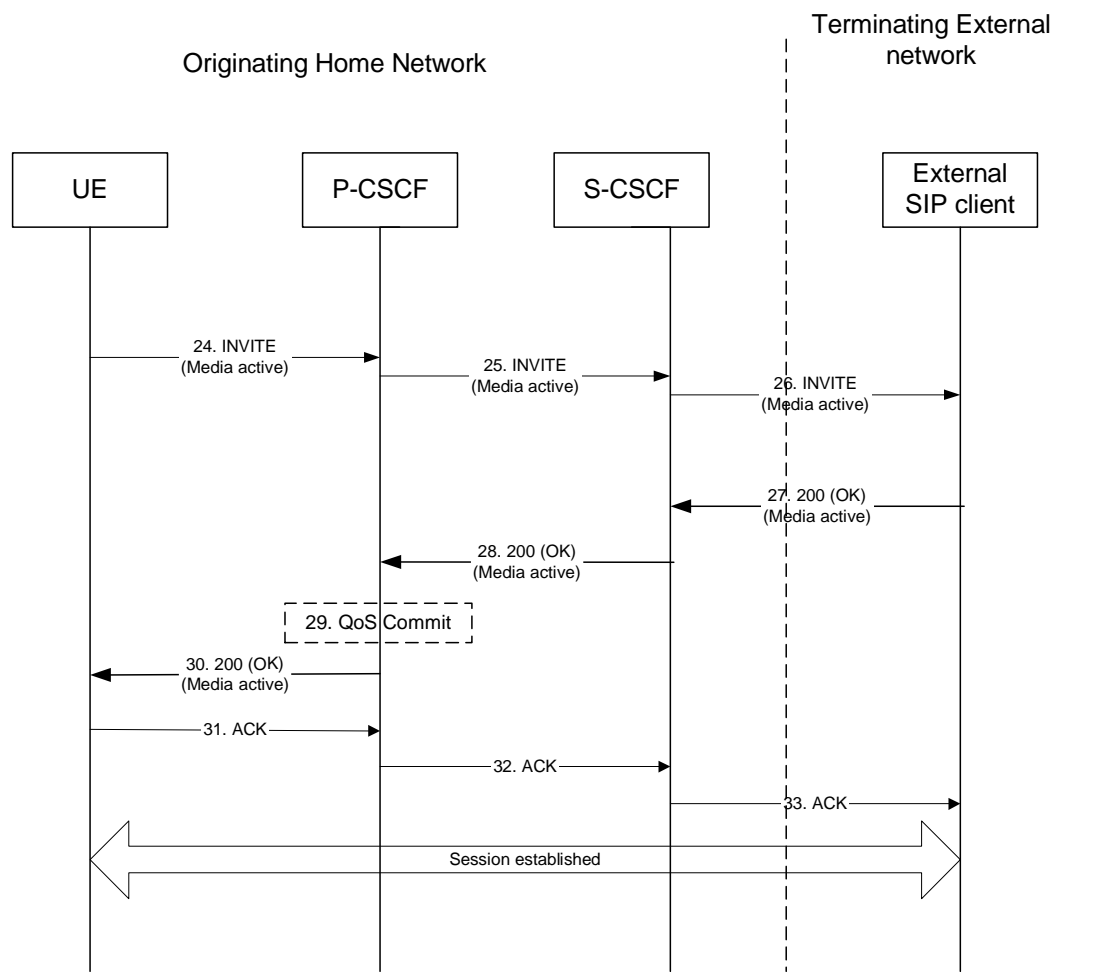
Figure 5.19g: Continuation of originating session towards external SIP client, session set up with active media

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 5.19g.

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.

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.
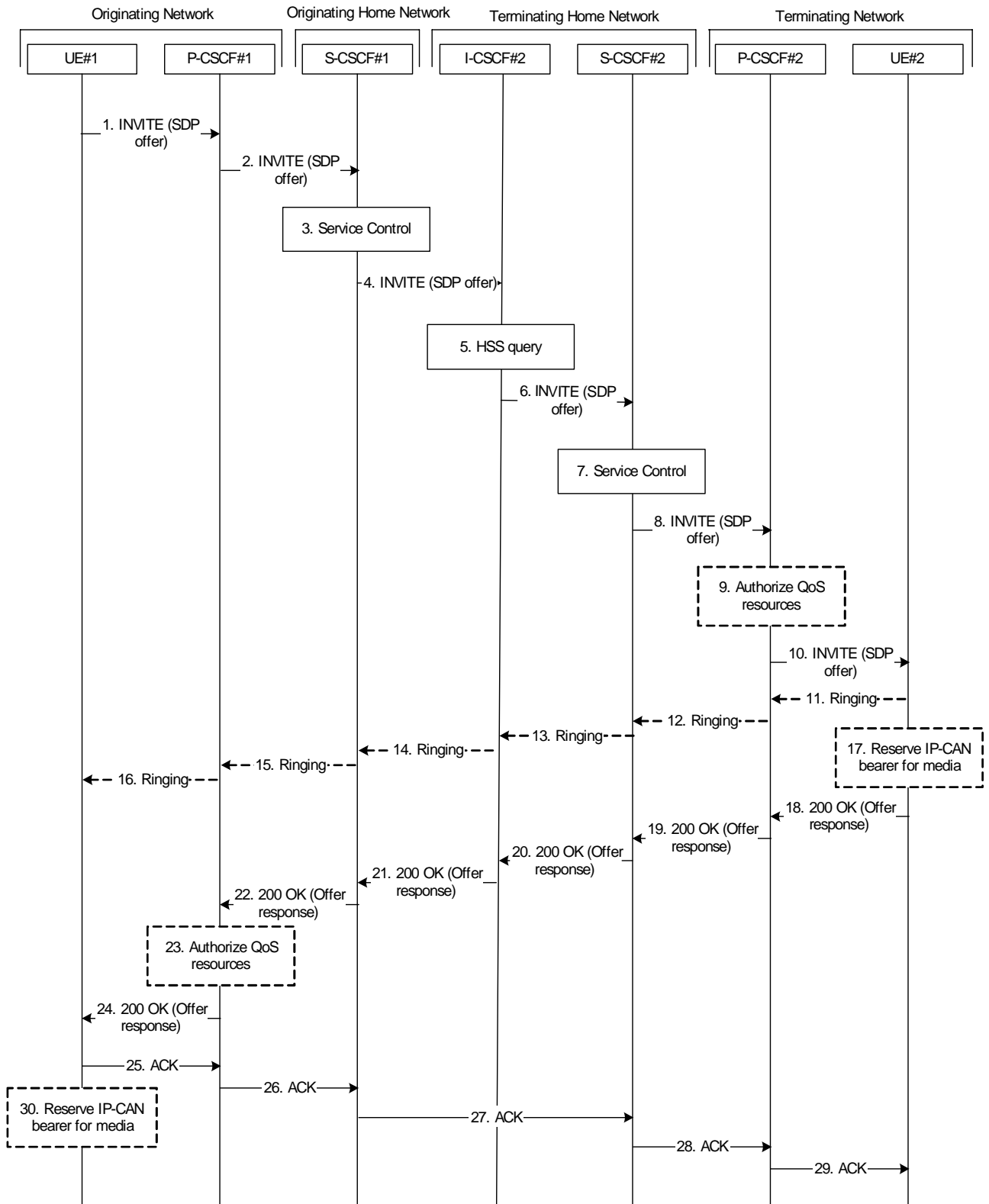

Figure 5.~~19c.~~19g: End-to-end session flow procedure without preconditions

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 by the PDF.

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 by the PDF.

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.

*** End of Fourth Modified Text ***

3GPP TSG-SA WG2 Meeting #42
Sophia Antipolis, France. October 11-15, 2004.

Tdoc ⌘ *S2-043338*

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **451** | ⌘**rev** | **1** | ⌘ | Current version: | **6.7.0** | ⌘ |

*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:	⌘	Correct redirection scenarios

Source:	⌘	Lucent Technologies

Work item code: ⌘	IMS2	**Date:** ⌘	14/10/2004

Category:	⌘	**F**		**Release:** ⌘	Rel-6

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

Use *one* of the following releases:
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 redirection and refer sections of TS 23.228 only describe a restricted set of endpoints that may invoke redirection or refer operations as well as a limited set of endpoints to which the sessions may be redirected or referred. This incorrectly limits the possible combination of scenarios.

Summary of change:⌘	Additional statements have been added to affected clauses to clarify the type of endpoint that may invoke the functions described.

Consequences if not approved:	⌘	Not including these modifications erroneously implies that the scenarios not explicitly mentioned are not allowed.

Clauses affected:	⌘	5.11.5.2a, 5.11.5.3, 5.11.5.6, and 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.

*** Changes to clause 5.11.5.2a ***

5.11.5.2a   Session Redirection to PSTN Termination (REDIRECT to originating UE#1)

The S-CSCF of the destination user (S-CSCF#2) may determine that the session is to be redirected to a PSTN Termination; e.g. CS-domain endpoint, or to the PSTN. For session redirection to PSTN termination where the S-CSCF of the called party (S-CSCF#2) wishes to use the SIP REDIRECT method, the S-CSCF#2 will pass the new destination information (the PSTN Termination information) to the originator ~~(UE#1)~~. The originator ~~(UE#1)~~ can then initiate a new session to the redirected to destination denoted by S-CSCF#2. The originator may be a UE as shown in the example flow in figure 5.37a, or it may be any other type of originating entity as defined in subclause 5.4.10. The endpoint to which the session is redirected may be the PSTN as shown in figure 5.37a, or it may be any other type of terminating entity as defined in subclause 5.4.10. The originator may alternately receive a redirect from a non-IMS network SIP client. Only the scenario in which a call from a UE is redirected by S-CSCF service logic to a PSTN endpoint is shown.

Handling of redirection to a PSTN Termination where the S-CSCF#2 REDIRECTS to the originating UE#1 is shown in the figure 5.37a:
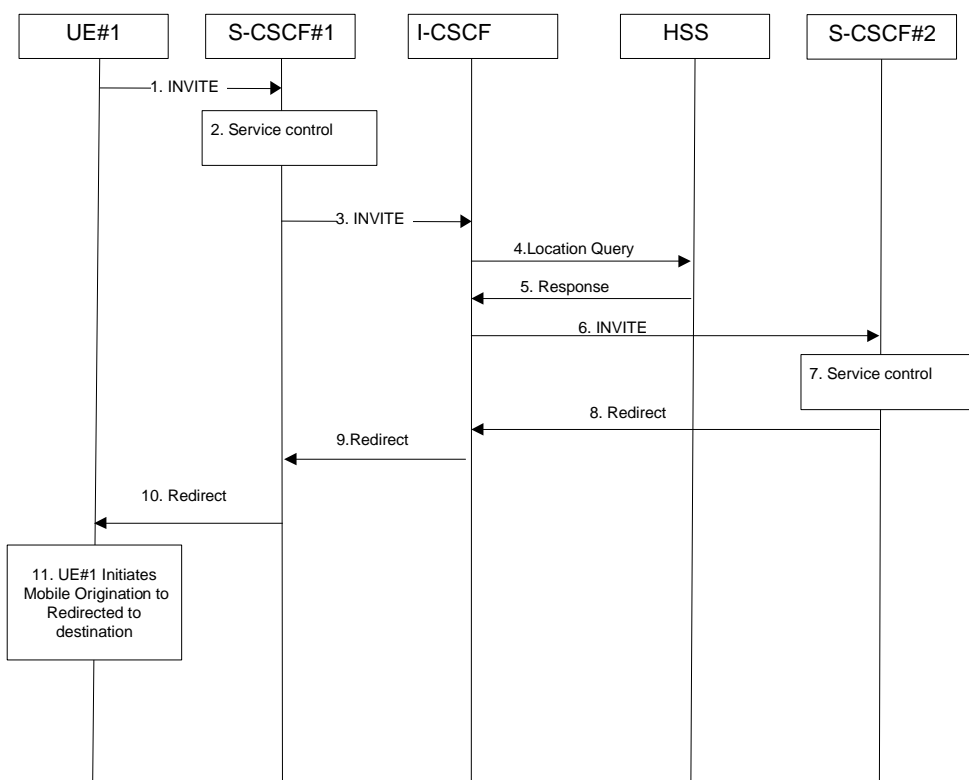

Figure 5.37a: Session redirection to PSTN Termination (REDIRECT to originating UE#1)

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE#1 to S-CSCF#1 by the procedures of the originating flow.

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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a PSTN termination. S-CSCF#2 determines that it wishes to use the SIP REDIRECT method to pass the redirection destination information (the 'redirected-to PSTN Termination' information) to the originator (UE#1).

8. S-CSCF#2 sends a SIP Redirect response to I-CSCF with the redirection destination.

9. I-CSCF sends a Redirect response to S-CSCF#1, containing the redirection destination.

10. S-CSCF#2 forwards the Redirect response to UE#1, containing the redirection destination

UE#1 initiates a session to the 'redirected-to PSTN Termination' according to the mobile origination procedures supported in the UE (e.g. CS, IMS).

*** End of changes to clause 5.11.5.2a ***

*** Changes to clause 5.11.5.3 ***

5.11.5.3 Session Redirection initiated by S-CSCF to general endpoint (REDIRECT to originating UE#1)

The S-CSCF in the scenario above may determine that the session is to be redirected to an endpoint outside the IP MultiMedia System and outside the CS-domain. Examples of these destinations include web pages, email addresses, etc. It recognizes this situation by the redirected URL being other than a sip: or tel: URL.

In cases when the destination subscriber is not currently registered in the IM CN subsystem, the I-CSCF may assign a temporary S-CSCF to invoke the service logic on behalf of the intended destination. This temporary S-CSCF takes the role of S-CSCF#2 in the following information flow. For session redirection to a general endpoint where the S-CSCF of the called party (S-CSCF#2) wishes to use the SIP REDIRECT method, the S-CSCF#2 will pass the new destination information to the originator. As a result the originator should initiate a new session to the redirected-to destination provided by S-CSCF#2. The originator may be a UE as shown in the example flow in figure 5.38, an Application Server or a non-IMS network SIP client. The originator may also receive a redirect from a non-IMS network SIP client. Only the scenario in which the originating UE receives a redirect based on S-CSCF service logic is shown.

Handling of redirection to a general URL is shown in the following information flow:
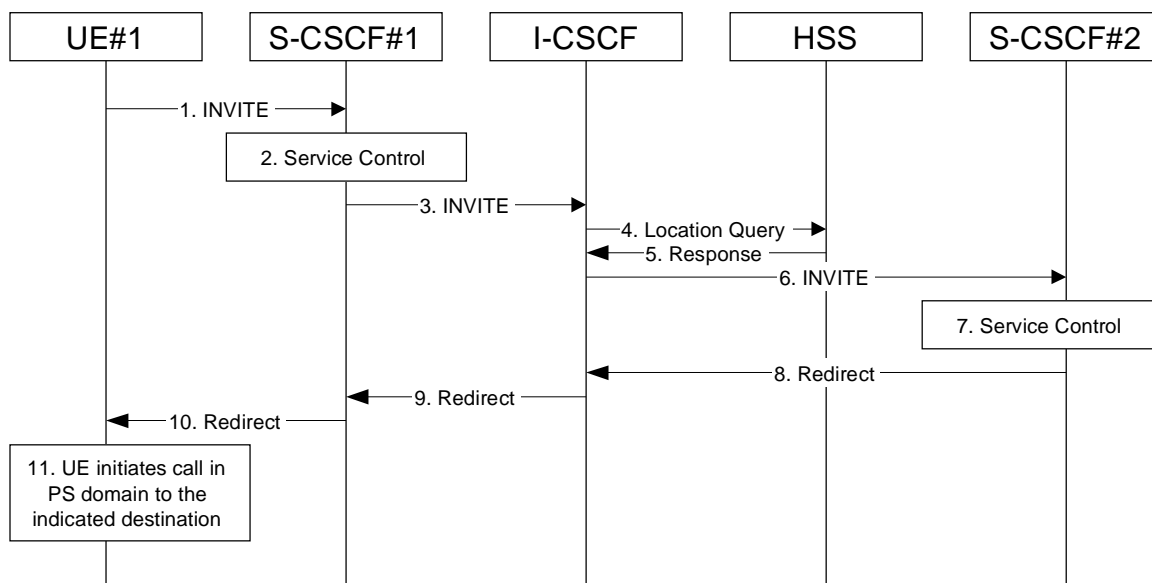

Figure 5.38: Session redirection initiated by S-CSCF to general endpoint

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.

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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a new destination URL outside the IMS and outside the CS domain, i.e. other than a sip: or tel: URL.

8. S-CSCF#2 sends a SIP Redirect response back to I-CSCF, with redirection destination being the general URL.

9. I-CSCF sends a Redirect response back to S-CSCF#1, containing the redirection destination.

10. S-CSCF#1 forwards the Redirect response back to UE#1.

11. UE#1 initiates the session to the indicated destination.

*** End of changes to clause 5.11.5.3 ***

*** Changes to clause 5.11.5.6 ***

5.11.5.6　　　　Session Redirection initiated by originating UE#1 after Bearer Establishment (REDIRECT to originating UE#1)

The UE of the destination user may request the session be redirected after a customer-specified ringing interval. The UE may also implement customer-specific feature processing, and base its decision to redirect this session on such things as identity of caller, current sessions in progress, other applications currently being accessed, etc. UE sends the SIP Redirect response to its P-CSCF, who forwards back along the signaling path to the originating endpoint, who initiates a session to the new destination.

The service implemented by this information flow is typically "Session Forward No Answer".

The originating end point may be a UE as shown in the example flow in figure 5.41 or it may be any other type of originating entity as defined in subclause 5.4.10. Redirect to another IMS endpoint (e.g. a sip: URL) is shown in the ~~following information flow~~figure.~~:~~　The redirecting endpoint may be a UE as shown or an Application Server or a non-IMS network SIP client. Further, the endpoint to which the session is redirected may be a UE as shown in figure 5.41, 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 redirected by a second UE to a third UE is shown.

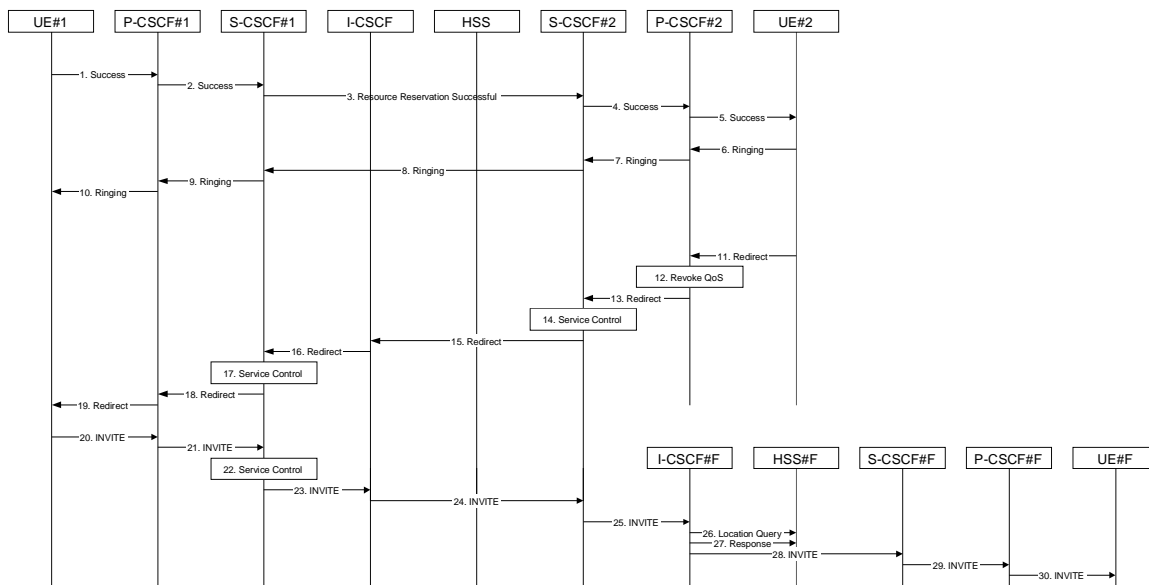The flow presented here assumes that service-based local policy is in use.

Figure 5.41: Session redirection after bearer establishment

Step-by-step processing is as follows:

1-10.　Normal handling of a basic session establishment, up through establishment of the bearer channel and alerting of the destination user or by a previous session redirection after bearer establishment procedure.

11. Based on a timeout or other indications, UE#2 decides the current session should be redirected to a new destination URL. This new destination URL may be a phone number, an email address, a web page, or anything else that can be expressed as a URL. The Redirect response is sent to P-CSCF#2.

12. P-CSCF#2 shall revoke any authorisation for QoS for the current session.

13. P-CSCF#2 forwards the Redirect response to S-CSCF#2.

14. S-CSCF#2 invokes whatever service logic is appropriate for this session redirection. If UE#2 does not subscribe to session redirection service, or did not supply a new destination URL, S-CSCF#2 may supply one or may terminate the session setup attempt with a failure response. The new destination URL may be a phone number, an email address, a web page, or anything else that can be expressed as a URL. S-CSCF#2 generates a private URL, addressed to itself, containing the new destination.

15. S-CSCF#2 sends a SIP Redirect response back to I-CSCF, containing the private URL addressed to S-CSCF#2.

16. I-CSCF sends a Redirect response back to S-CSCF#1, containing the redirection destination.

17. S-CSCF#1 checks the number of redirections that have occurred for this session setup attempt, and if excessive, aborts the session. S-CSCF#1 stores the new destination information, generates a private URL addressed to itself pointing to the stored information, and generates a modified Redirect response with the private URL.

18. S-CSCF#1 sends the modified Redirect response to P-CSCF#1

19. P-CSCF#1 shall revoke any authorisation for QoS for the current session and sends the Redirect response to UE#1.

20. UE#1 initiates a new INVITE request to the address provided in the Redirect response. The new INVITE request is sent to P-CSCF#1

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

22. S-CSCF#1 retrieves the destination information saved in step #17, and invokes whatever other service logic is appropriate for this new session setup attempt.

23. S-CSCF#1 determines the network operator of the new destination address. The INVITE message is sent to I-CSCF#2, the I-CSCF for S-CSCF#2.

24. I-CSCF forwards the INVITE to S-CSCF#2

25. S-CSCF#2 decodes the private URL, determines the network operator of the new destination, and sends the INVITE request to the I-CSCF for that network operator.

26. The remainder of this session completes as normal.

*** End of changes to clause 5.11.5.6 ***

*** Changes to clause 5.11.6.1 ***

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:
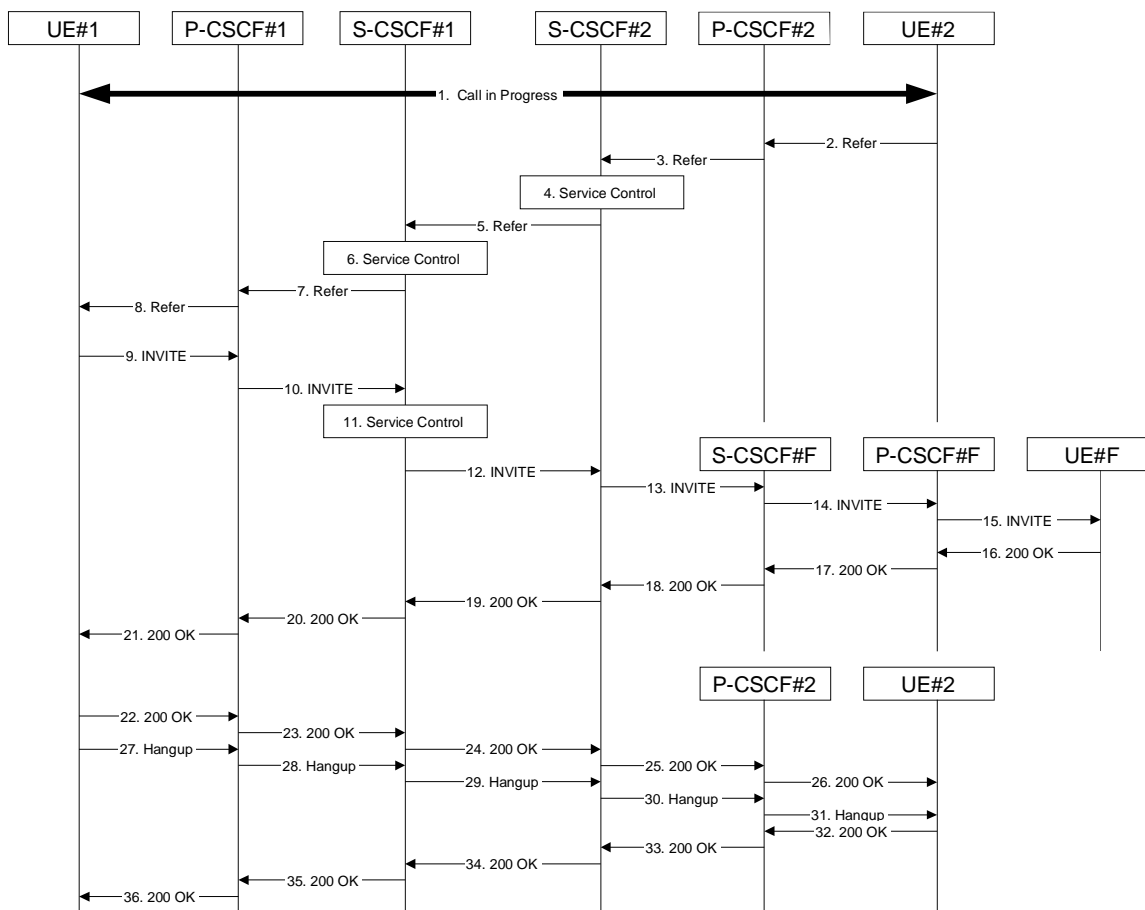

Figure 5.42: Refer operation

Step-by-step description of the information flow:

1. A multi-media session is assumed to already exist between UE#1 and UE#2, established either as a basic session or by one of the supplemental services described in this ~~section~~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 URL, 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 URL.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*** End of changes to clause 5.11.6.1 ***

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **450** | ⌘ **rev** | **1** | ⌘ | Current version: | **6.7.0** | ⌘ |

*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: ⌘	Clarify that IMS end-points shall be able to support sending or receiving DTMF tone indications	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	IMS2	***Date:*** ⌘ 13/10/2004
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: ⌘	The existing text in 5.4.1 implies that DTMF tone indications can only be sent in one direction, ie from the UE.
Summary of change: ⌘	Text is added to 5.4.1 that state that IMS end-points shall be able to support sending or receiving DTMF tone indications.
Consequences if not approved: ⌘	It will not be possible to maintain some PSTN services when interworking with non-IMS networks such as PSTN.

Clauses affected: ⌘	5.4.1

	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.

## 5.4.1	Bearer interworking concepts

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

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

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

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

CR-Form-v7.1

CHANGE REQUEST

⌘	**23.228** CR **446**	⌘**rev** **3** ⌘	Current version:	**6.7.0** ⌘

*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:	⌘	Treatment of SIP forking request		
Source:	⌘	Huawei, China mobile		
Work item code:⌘	IMS2		**Date:** ⌘	14/10/2004
Category:	⌘ **F**		**Release:** ⌘	Rel-6

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

Use one of the following releases:
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 last SA2 meetiong, the S2-042850 clarifies that when the UE or MGCF receives the first 200 OK(for INVITE), the UE or MGCF just acknowledges the 200 OK and does not cancel other early dialogues. If the subsequent final 200 OK is received, the UE or MGCF shall acknowledge the dialogue and immediately send a BYE to drop the dialog. Though RFC 3261 has defined that if the forwarded response was a final response, the proxy MUST generate a CANCEL request for all pending client transactions associated with this response context. But it is stated in section 16.7 in RFC 3261 that a stateful proxy will forward exactly one final response to a non-INVITE request, and either exactly one non-2xx response or one or more 2xx responses to an INVITE request. So this procedure only deletes the dialogues between the proxy and the terminating clients. The early dialogues between the originating client and the proxy still exist. And there is no means to delete these dialogues unless the session timer expires, which will not be a short time. So the UE or MGCF can also terminate the early dialogues upon the reception of a first final 200 OK (for INVITE).
Summary of change:⌘	Clarified that the UE or MGCF can also terminate early dialogues upon the reception of a first final 200 OK.
Consequences if not approved: ⌘	On receipt of the first final 200 OK, other dialogues between the originating client and the proxy will exist for a long time even though the corresponding early dialogues between the proxy and the terminating clients have been dropped.

Clauses affected:	⌘	4.2.7.3		

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

Other comments:	⌘	

4.2.7.3   Support for forked requests

UE and MGCF shall be ready to receive responses generated due to a forked request and behave according to the procedures specified in [12] and in this section.

The UE and MGCF may accept or reject early dialogues from different terminations as described in [12], for example if the UE is only capable of supporting a limited number of simultaneous dialogs.

Upon the reception of a first final 200 OK (for INVITE), the UE or MGCF shall acknowledge the 200 OK. In addition the UE or MGCF may require updating the allocated resources according to the resources needed. In case the UE or MGCF receives a subsequent 200 OK, the UE or MGCF shall acknowledge the dialogue and immediately send a BYE to drop the dialog.

> Note: Upon the reception of a first final 200 OK (for INVITE), the UE or MGCF may terminate the early dialogue, as specified in [12].

The UE and MGCF may include preferences according to "draft-ietf-sip-callerprefs-10" [42], in INVITE's, indicating that proxies should not fork the INVITE request. The S-CSCF and AS should follow the preferences, if included in the INVITE request. On the terminating side, UE and MGCF shall be able to receive, as specified in [12], several requests for the same dialog that were forked by a previous SIP entity.

Application Servers and MRFCs shall be capable to handle forked requests according to the procedures specified in [12].

CR-Form-v7

CHANGE REQUEST

⌘	**23.228** CR **455**	⌘**rev**	**-**	⌘	Current version:	**6.7.0**	⌘

*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: ⌘	Missing step in identity procedure	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	IMS2	***Date:*** ⌘ 15/11/2004
Category: ⌘ **F**		***Release:*** ⌘ Rel-6

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

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

Reason for change: ⌘	The procedure for providing the authenticated identity of the originating party is incorrectly missing one step.	
Summary of change: ⌘	Add the missing step.	
Consequences if not approved: ⌘	Procedure appears to be in error.	

Clauses affected: ⌘	5.11.4.1	

	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.

5.11.4   Procedures for providing or blocking identity

5.11.4.0   General

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

- The public user identity is used by any user for requesting communications to other users (see section 4.3.3.2).

- The display name is the user's name if available, an indication of privacy or unavailability otherwise. The display name is a text string which may identify the subscriber, the user or the terminal.

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

5.11.4.1   Procedures for providing the authenticated identity of the originating party

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

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

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

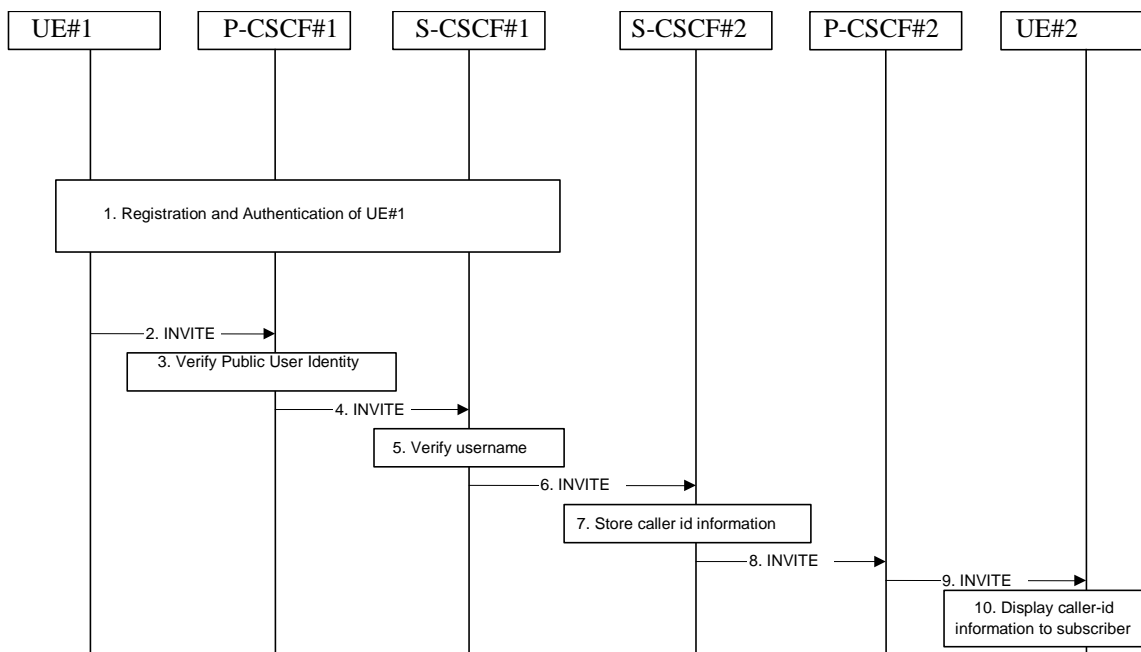**Figure 5.34: Providing the authenticated Identity of the originating party**

The detailed procedure is as follows:

1. Registration and authentication of UE#1 is performed.

2. UE#1 initiates a new multi-media session, by sending an INVITE request to P-CSCF#1. This INVITE request includes a public user identity, and may include a display name that may identify the specific person using the UE.

3. P-CSCF#1 checks the public user identity of the originating party, and replaces it (or rejects the request) if it is incorrect.

4. P-CSCF#1 forwards the INVITE request, with the verified public user identity , to S-CSCF#1.

5. S-CSCF#1 invokes whatever service logic is appropriate for this session set up attempt to check in particular that no identity restriction is active.

6. S-CSCF#1 forwards the INVITE request, with verified public user identity and display name of the originating party if present, to S-CSCF#2.

7. S-CSCF#2 stores the caller ID information.

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

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

10. UE#2 displays the public user identity and the display name information (i.e. user-name if available, indication of privacy or unavailability otherwise) to the terminating party.

CR-Form-v7

CHANGE REQUEST

| ⌘ | **23.228** CR **456** | ⌘**rev** | **-** | ⌘ | Current version: | **6.7.0** | ⌘ |

*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:** | ⌘ | Correction to PSTN Termination |

| **Source:** | ⌘ | Lucent Technologies |

| **Work item code:** ⌘ | IMS2 | **Date:** ⌘ | 15/11/2004 |

| **Category:** | ⌘ | **F** | **Release:** ⌘ | Rel-6 |

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

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

| **Reason for change:** | ⌘ | There is text in the PSTN termination procedure that indicates the procedure may be used with any of the S-S procedures. This conflicts with text in the overview section that indicates this procedure can only be used with S-S#3 and S-S#4. |

| **Summary of change:** ⌘ | Remove the incorrect text from the PSTN termination procedure. |

| **Consequences if not approved:** | ⌘ | Conflicting text remains in the document. |

| **Clauses affected:** | ⌘ | 5.7.3 |

		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.

5.7.3 (PSTN-T) PSTN termination

The MGCF in the IM CN subsystem is a SIP endpoint that initiates and receives requests on behalf of the PSTN and Media Gateway (MGW).Other nodes consider the signalling as if it came from a S-CSCF. The MGCF incorporates the network security functionality of the S-CSCF.

PSTN termination may be done in the same operator's network as the S-CSCF of the session originator. Therefore, the location of the MGCF/MGW are given only as "Terminating Network" rather than "Home Network" or "Visited Network."

Further, agreements between network operators may allow PSTN termination in a network other than the originator's visited network or home network. This may be done, for example, to avoid long distance or international tariffs.

~~This termination procedure can be used for any of the inter-serving procedures, in place of the S-CSCF.~~

Figure 5.19: PSTN termination procedure

The PSTN termination procedure is as follows:

1. MGCF receives an INVITE request, containing an initial SDP, through one of the origination procedures and via one of the inter-serving procedures.

2. MGCF initiates a H.248 interaction to pick an outgoing channel and determine media capabilities of the MGW.

3. MGCF determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. This response is sent via the S-S procedure.

4. The originating endpoint sends a Response Confirmation. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in Step 3 or a subset. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method.

5. MGCF initiates a H.248 interaction to modify the connection established in step #2 and instruct MGW to reserve the resources necessary for the media streams.

6. MGCF responds to the offered media towards the originating party.

7. GW reserved the resources necessary for the media streams.

8. When the originating endpoint has completed its resource reservation, it sends the successful Resource Reservation message to MGCF, via the S-S procedures.

9. MGCF sends an IAM message to the PSTN

10. MGCF sends response to the successful resource reservation towards originating end.

11. The PSTN establishes the path to the destination. It may optionally alert the destination user before completing the session. If so, it responds with an ACM message.

12. If the PSTN is alerting the destination user, MGCF indicates this to the originating party by a provisional response indicating Ringing. This message is sent via the S-S procedures.

13. When the destination party answers, the PSTN sends an ANM message to MGCF

14. MGCF initiates a H.248 interaction to make the connection in the MGW bi-directional.

15. MGCF sends a SIP 200-OK final response along the signalling path back to the session originator

16. The Originating party acknowledges the final response with a SIP ACK message

CR-Form-v7

CHANGE REQUEST

| ⌘ | **23.228** CR **459** | ⌘**rev** | **-** | ⌘ | Current version: | **6.7.0** | ⌘ |

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: ⌘	Removal of Editor's Note on ISC	
Source: ⌘	Lucent Technologies	
Work item code:⌘	IMS2	***Date:*** ⌘ 15/11/2004
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)

Reason for change: ⌘	Procedures for AS sessions have been adopted and thus the Editor's Note has been addressed and should be removed.
Summary of change:⌘	Removal of Editor's Note.
Consequences if not approved: ⌘	Note implies that the work is not complete.

Clauses affected: ⌘	4.2.4

	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.

4.2.4   IP multimedia Subsystem Service Control Interface (ISC)

The ISC interface is between the Serving CSCF and the service platform(s).

An Application Server (AS) offering value added IM services resides either in the user's home network or in a third party location. The third party could be a network or simply a stand-alone AS.

The Serving-CSCF to AS interface is used to provide services residing in an AS. Two cases were identified:

- Serving-CSCF to an AS in Home Network.

- Serving-CSCF to an AS in External Network (e.g., Third Party or Visited)

The SIP Application Server may host and execute services. The SIP Application Server can influence and impact the SIP session on behalf of the services and it uses the ISC interface to communicate with the S-CSCF.

The ISC interface shall be able support subscription to event notifications between the Application Server and S-CSCF to allow the Application Server to be notified of the implicit registered public user identities, registration state and UE capabilities and characteristics in terms of SIP User Agent capabilities and characteristics.

The S-CSCF shall decide whether an Application Server is required to receive information related to an incoming initial SIP request to ensure appropriate service handling. The decision at the S-CSCF is based on (filter) information received from the HSS. This filter information is stored and conveyed on a per application server basis for each user. The name(s)/address(es) information of the application server(s) are received from the HSS.

For an incoming SIP request, the S-CSCF shall perform any filtering for ISC interaction before performing other routing procedures towards the terminating user, e.g. forking, caller preferences etc.

The S-CSCF does not handle service interaction issues.

Once the IM SSF, OSA SCS or SIP Application Server has been informed of a SIP session request by the S-CSCF, the IM SSF, OSA SCS or SIP Application Server shall ensure that the S-CSCF is made aware of any resulting activity by sending messages to the S-CSCF.

From the perspective of the S-CSCF, The "SIP Application server", "OSA service capability server" and "IM-SSF" shall exhibit the same interface behaviour.

When the name/address of more than one "application server" is transferred from the HSS, the S-CSCF shall contact the "application servers" in the order supplied by the HSS. The response from the first "application server" shall be used as the input to the second "application server". Note that these multiple "application servers" may be any combination of the SIP Application server, OSA service capability server, or IM-SSF types.

The S-CSCF does not provide authentication and security functionality for secure direct third party access to the IM subsystem. The OSA framework provides a standardized way for third party secure access to the IM subsystem.

If a S-CSCF receives a SIP request on the ISC interface that was originated by an Application Server destined to a user served by that S-CSCF, then the S-CSCF shall treat the request as a terminating request to that user and provide the terminating request functionality as described above. Both registered and unregistered terminating requests shall be supported.

It shall be possible for an Application Server to generate SIP requests and dialogs on behalf of users. Such requests are forwarded to the S-CSCF serving the user, and the S-CSCF shall perform regular originating procedures for these requests.

> Editor's note: The detailed procedures for handling such requests (e.g. security, charging, routing, etc…) are FFS.

More specifically the following requirements apply to the IMS Service control interface:

1. The ISC interface shall be able to convey charging information as per 3GPP TS 32.200[25] and 3GPP TS 32.225[26].

2. The protocol on the ISC interface shall allow the S-CSCF to differentiate between SIP requests on Mw, Mm and Mg interfaces and SIP Requests on the ISC interface.

Figure 4.3: Void

Besides the Cx interface the S-CSCF supports only one standardised protocol for service control, which delegates service execution to an "Application Server". The protocol to be used on the ISC interface shall be SIP (as defined by RFC 3261 [12], other relevant RFC's, and additional enhancements introduced to support 3GPP´s needs on the Mw, Mm, Mg interfaces). On the ISC interface, extensions to SIP shall be avoided but are not expressly prohibited.

The notion of a "SIP leg" used throughout this specification is identical to the notion of a call leg which is the same as a SIP dialog defined by RFC 3261 [12]. The same SIP leg that is received by the S-CSCF on the Mw, Mm and Mg interfaces is sent on the ISC interface. The same SIP leg that is received by the S-CSCF on the ISC interface is sent on the Mw, Mm and Mg interfaces.

Concerning the relationship between the SIP legs of the ISC interface and the SIP legs of the Mw, Mm, and Mg interfaces the S-CSCF acts as a SIP proxy, as shown in Figures 4.a-4e below.

Figures 4.3a-4.3e below depict the possible high-level interactions envisioned between the S-CSCF and the Application Server.
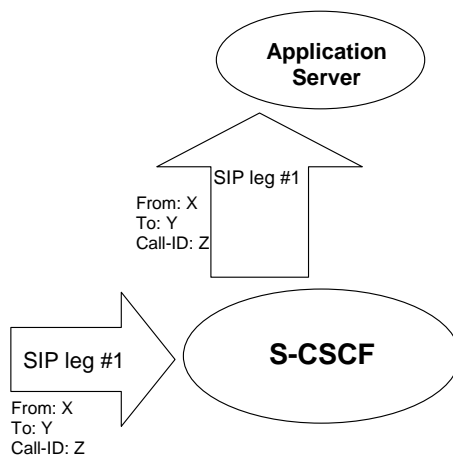

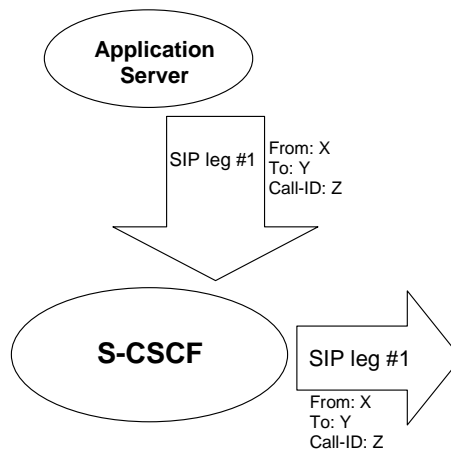**Figure 4.3a: Application Server acting as terminating UA, or redirect server**

Figure 4.3b: Application Server acting as originating UA
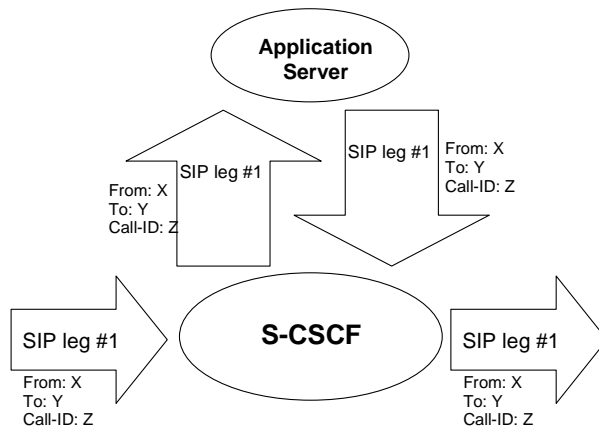
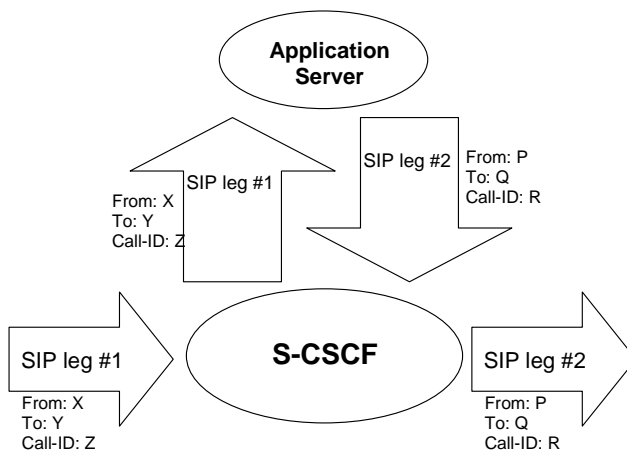**Figure 4.3c: Application Server acting as a SIP proxy**

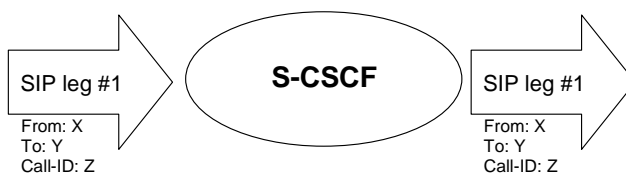**Figure 4.3d: Application Server performing 3rd party call control**

Figure 4.3e: A SIP leg is passed through the S-CSCF without Application Server involvement

CR-Form-v7

CHANGE REQUEST

| ⌘ | **23.228** CR **460** | ⌘ **rev** | **-** | ⌘ | Current version: | **6.7.0** | ⌘ |

*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: ⌘	Changes to SIP URL terminology	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	IMS2	***Date:*** ⌘ 15/11/2004
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)

Reason for change: ⌘	SIP identities are referred to by two different designations (SIP URL and SIP URI) which is misleading.
Summary of change: ⌘	Change SIP terminology to consistently use URI
Consequences if not approved: ⌘	Implementor's will wonder if Stage-2 meant to imply some difference based on the terminology used.

Clauses affected: ⌘	4.3.3.2, 4.3.3.3, 4.3.4, 4.3.5, 4.3.6, 4.6.3, 5.11.4.1, 5.11.5.1, 5.11.5.3, 5.11.5.4, 5.11.5.5, 5.11.5.6, 5.11.6.1, and E.3.1

	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.

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

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 ~~SIP URL~~SIP URI (as defined in RFC 3261 [12] and RFC2396 [13]) or the "tel:"-URL format [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 URL~~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 URL. This phone number can be in the form of E.164 format (prefixed with a '+' sign), or a local format using local dialling plan and prefix. The IMS will interpret the phone number with a leading '+' to be a fully defined international number.

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 useridentities; other identities that are not defined by the operator may also exist.
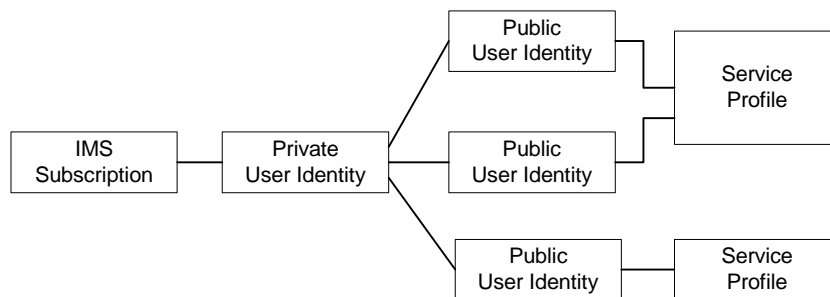
Figure 4.5: Relationship of the private user identity and public user identities

The IMS Service Profile is a collection of service and user related data as defined in 3GPP TS 29.228 [30]. The Service Profile is independent from the Implicit Registration Set, e.g. IMPUs with different Service Profiles may belong to the same Implicit Registration Set. Initial filter criteria in the service profile provide a simple service logic comprising of user / operator preferences that are of static nature i.e. they do not get changed on a frequent basis.

Application servers will provide more complex and dynamic service logic that can potentially make use of additional information not available directly via SIP messages (e.g. location, time, day etc.).

The IMS service profile is defined and maintained in the HSS and its scope is limited to IM CN Subsystem. 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 giventime. 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 URL~~SIP URI (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol, (e.g. Gm, Mw, Mm, and Mg). These ~~SIP URL~~SIP URIs would be used when identifying these nodes in header fields of SIP messages. However this does not require that these ~~URLs~~ 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 URL~~SIP URI "tel:" format [15] to a SIP routable ~~SIP URL~~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.

Public Service Identities shall take the form of ~~SIP URL~~SIP URI as defined in RFC 3261 [12] and RFC 2396 [13] or the "tel:"-URL format as defined in RFC 2806 [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.

The IM CN Subsystem shall provide capability of routing IMS messages using Public Service Identity.

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

4.6.3   Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:

Registration

-    May behave as a Registrar as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts registration requests and makes its information available through the location server (eg. HSS).

Session-related and session-unrelated flows

-    Session control for the registered endpoint's sessions. It shall reject IMS communication to/from public user identity(s) that are barred for IMS communications after completion of registration, as described in subclause 5.2.1.

-    May behave as a Proxy Server as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts requests and services them internally or forwards them on, possibly after translation.

-    May behave as a User Agent as defined in RFC 3261 [12] or subsequent versions, i.e. it may terminate and independently generate SIP transactions.

-    Interaction with Services Platforms for the support of Services

-    Provide endpoints with service event related information (e.g. notification of tones/announcement together with location of additional media resources, billing notification)

-    For an originating endpoint (i.e. the originating user/UE, or originating AS)

    -    Obtain from a database the Address of the I-CSCF for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URLSIP URI), when the destination user is a customer of a different network operator, and forward the SIP request or response to that I-CSCF.

    -    When the destination name of the destination user (e.g. dialled phone number or SIP URLSIP URI), and the originating user is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.

    -    Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.

    -    Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.

    -    In case the request is an originating request from an Application Server:

        -    Verify that the request coming from the AS is an originating request, and apply procedures accordingly (e.g. invoke interaction with Service Platforms for originating services, etc…);

        -    Process and proceed with the request even if the user on whose behalf the AS had generated the request is unregistered.

        -    Process and proceed with other requests to and from the user on whose behalf the AS had generated the request.

        -    Reflect in the charging information that an AS has initiated the session on behalf of a user.

-    For a destination endpoint (i.e. the terminating user/UE)

- Forward the SIP request or response to a P-CSCF for a MT procedure to a home user within the home network, or for a user roaming within a visited network where the home network operator has chosen not to have an I-CSCF in the path

- Forward the SIP request or response to an I-CSCF for a MT procedure for a roaming user within a visited network where the home network operator has chosen to have an I-CSCF in the path.

- Modify the SIP request for routing an incoming session to CS domain according to HSS and service control interactions, in case the user is to receive the incoming session via the CS domain.

- Forward the SIP request or response to a BGCF for call routing to the PSTN or the CS domain.

- If the SIP request contains preferences for characteristics of the destination endpoint, perform preference and capability matching as specified in "draft-ietf-sip-callerprefs-10" [41].

Charging and resource utilisation:

- Generation of CDRs

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

5.11.4.1　Procedures for providing the authenticated identity of the originating party

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

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

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

Figure 5.34: Providing the authenticated Identity of the originating party

The detailed procedure is as follows:

1. Registration and authentication of UE#1 is performed.

2. UE#1 initiates a new multi-media session, by sending an INVITE request to P-CSCF#1. This INVITE request includes a public user identity, and may include a display name that may identify the specific person using the UE.

3. P-CSCF#1 checks the public user identity of the originating party, and replaces it (or rejects the request) if it is incorrect.

4. P-CSCF#1 forwards the INVITE request, with the verified public user identity , to S-CSCF#1.

5. S-CSCF#1 invokes whatever service logic is appropriate for this session set up attempt to check in particular that no identity restriction is active.

6. S-CSCF#1 forwards the INVITE request, with verified public user identity and display name of the originating party if present, to S-CSCF#2.

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

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

10. UE#2 displays the public user identity and the display name information (i.e. user-name if available, indication of privacy or unavailability otherwise) to the terminating party.

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 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 before forwarding the INVITE request to UE#2.

5.11.5 Session Redirection Procedures

5.11.5.0 General

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

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

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

5.11.5.1 Session Redirection initiated by S-CSCF to IMS

One of the functional elements in a basic session flow that may initiate a redirection is the S-CSCF of the destination user. The user profile information obtained from the HSS by the 'Cx-pull' during registration may contain complex

logic and triggers causing session redirection. S-CSCF#2 sends the SIP INVITE request to the I-CSCF for the new destination (I-CSCF#F in the diagram), who forwards it to S-CSCF#F, who forwards it to the new destination.

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

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

This is shown in the following information flow:

Figure 5.36: Session redirection initiated by S-CSCF to IMS

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.

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 destination subscriber belongs. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a new destination ~~URL~~URI within the IP Multimedia Subsystem. Based on operator policy and the user profile, S-CSCF#2 may restrict the media streams allowed in the redirected session.

8. S-CSCF#2 sends a SIP INVITE request to an I-CSCF (I-CSCF#F) for the network operator to whom the forwarded destination subscribes. This INVITE request may optionally go through an I-CSCF(THIG) if S-CSCF#2 is in a different operator's network than I-CSCF#F.

9. I-CSCF#F queries the HSS (HSS#F) for current location information of the destination user.

10. HSS#F responds with the address of the current Serving CSCF (S-CSCF#F) for the terminating user.

11. I-CSCF forwards the INVITE request to S-CSCF#F, who will handle the session termination.

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

13. S-CSCF#F forwards the INVITE toward the destination UE, according to the procedures of the terminating flow.

14. The destination UE responds with the SDP message, and the session establishment proceeds normally.

## 5.11.5.2	Session Redirection to PSTN Termination (S-CSCF #2 forwards INVITE)

The S-CSCF of the destination user (S-CSCF#2) may determine that the session is to be redirected to a PSTN Termination; e.g. CS-domain endpoint, or to the PSTN. For session redirection to PSTN termination where the S-CSCF of the called party (S-CSCF#2) wishes to remain in the path of SIP signalling, the S-CSCF forwards the INVITE to a BGCF. Then the BGCF (in the local network or in another network) will forward the INVITE to a MGCF, which will forward towards the destination according to the termination flow.

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

Handling of redirection to a PSTN Termination where the S-CSCF#2 forwards the INVITE is shown in the figure 5.37:

Figure 5.37: Session redirection to PSTN Termination (S-CSCF #2 forwards INVITE)

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE #1 to S-CSCF#1 by the procedures of the originating flow.

2. S-CSCF#1 performs whatever service control 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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a PSTN termination. . S-CSCF#2 determines that it wishes to remain in the path of the SIP signalling.

8. S-CSCF#2 forwards the INVITE using the Serving to Serving procedures S-S#3 or S-S#4. The PSTN terminating flows are then followed.

9. The destination responds with the SDP message, and the session establishment proceeds normally.

5.11.5.2a Session Redirection to PSTN Termination (REDIRECT to originating UE#1)

The S-CSCF of the destination user (S-CSCF#2) may determine that the session is to be redirected to a PSTN Termination; e.g. CS-domain endpoint, or to the PSTN. For session redirection to PSTN termination where the S-CSCF of the called party (S-CSCF#2) wishes to use the SIP REDIRECT method, the S-CSCF#2 will pass the new destination information (the PSTN Termination information) to the originator (UE#1). The originator (UE#1) can then initiate a new session to the redirected to destination denoted by S-CSCF#2.

Handling of redirection to a PSTN Termination where the S-CSCF#2 REDIRECTS to the originating UE#1 is shown in the figure 5.37a:

Figure 5.37a: Session redirection to PSTN Termination (REDIRECT to originating UE#1)

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE#1 to S-CSCF#1 by the procedures of the originating flow.

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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a PSTN termination. S-CSCF#2 determines that it wishes to use the SIP REDIRECT method to pass the redirection destination information (the 'redirected-to PSTN Termination' information) to the originator (UE#1).

8. S-CSCF#2 sends a SIP Redirect response to I-CSCF with the redirection destination.

9. I-CSCF sends a Redirect response to S-CSCF#1, containing the redirection destination.

10. S-CSCF#2 forwards the Redirect response to UE#1, containing the redirection destination

UE#1 initiates a session to the 'redirected-to PSTN Termination' according to the mobile origination procedures supported in the UE (e.g. CS, IMS).

5.11.5.3 Session Redirection initiated by S-CSCF to general endpoint (REDIRECT to originating UE#1)

The S-CSCF in the scenario above may determine that the session is to be redirected to an endpoint outside the IP MultiMedia System and outside the CS-domain. Examples of these destinations include web pages, email addresses, etc. It recognizes this situation by the redirected ~~URL~~URI being other than a sip: URI or tel: URL.

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

Handling of redirection to a general ~~URL~~URI is shown in the following information flow:

Figure 5.38: Session redirection initiated by S-CSCF to general endpoint

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.

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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a new destination ~~URL~~URI outside the IMS and outside the CS domain, i.e. other than a sip: URI or tel: URL.

8. S-CSCF#2 sends a SIP Redirect response back to I-CSCF, with redirection destination being the general ~~URL~~URI.

9. I-CSCF sends a Redirect response back to S-CSCF#1, containing the redirection destination.

10. S-CSCF#1 forwards the Redirect response back to UE#1.

11. UE#1 initiates the session to the indicated destination.

5.11.5.4 Session Redirection initiated by P-CSCF

One of the functional elements in a basic session flow that may initiate a redirection is the P-CSCF of the destination user. In handling of an incoming session setup attempt, the P-CSCF normally sends the INVITE request to the destination UE, and retransmits it as necessary until obtaining an acknowledgement indicating reception by the UE.

In cases when the destination user is not currently reachable in the IM CN subsystem (due to such factors as roaming outside the service area or loss of battery, but the registration has not yet expired), the P-CSCF may initiate a redirection of the session. The P-CSCF informs the S-CSCF of this redirection, without specifying the new location; S-CSCF determines the new destination and performs according to sections 1, 2, or 3 above, based on the type of destination.
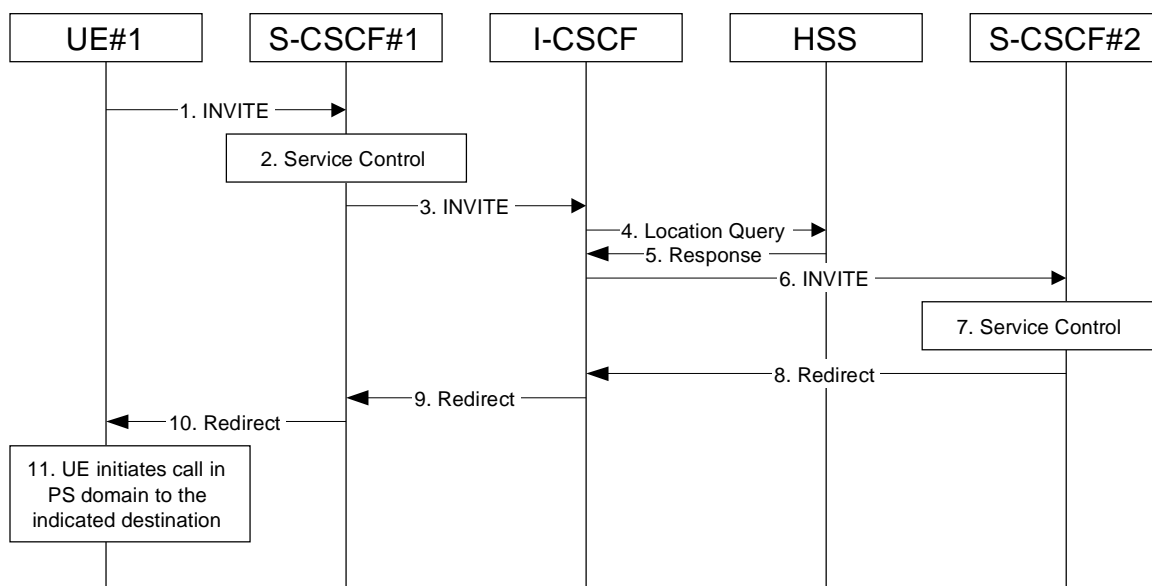
This is shown in the following information flow:

Figure 5.39: Session redirection initiated by P-CSCF

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.

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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

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

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

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

10. Timeout expires in P-CSCF waiting for a response from UE#2. P-CSCF therefore assumes UE#2 is unreachable.

11. P-CSCF#2 generates an Unavailable response, without including a new destination, and sends the message to S-CSCF#2.

12. S-CSCF#2 invokes whatever service logic is appropriate for this session redirection. If the user does not subscribe to session redirection service, or did not supply a forwarding destination, S-CSCF#2 may terminate the session setup attempt with a failure response. Otherwise, S-CSCF#2 supplies a new destination ~~URL~~URI, which may be a phone number, an email address, a web page, or anything else that can be expressed as a ~~URL~~URI. Processing continues according to subsections 1, 2, or 3 above, based on the type of destination ~~URL~~URI.

5.11.5.5   Session Redirection initiated by UE

The next functional element in a basic session flow that may initiate a redirection is the UE of the destination user. The UE may implement customer-specific feature processing, and base its decision to redirect this session on such things as identity of caller, current sessions in progress, other applications currently being accessed, etc. UE sends the SIP Redirect response to its P-CSCF, who forwards back along the signalling path to S-CSCF#1, who initiates a session to the new destination.

The service implemented by this information flow is typically "Session Forward Busy", "Session Forward Variable" or "Selective Session Forwarding".
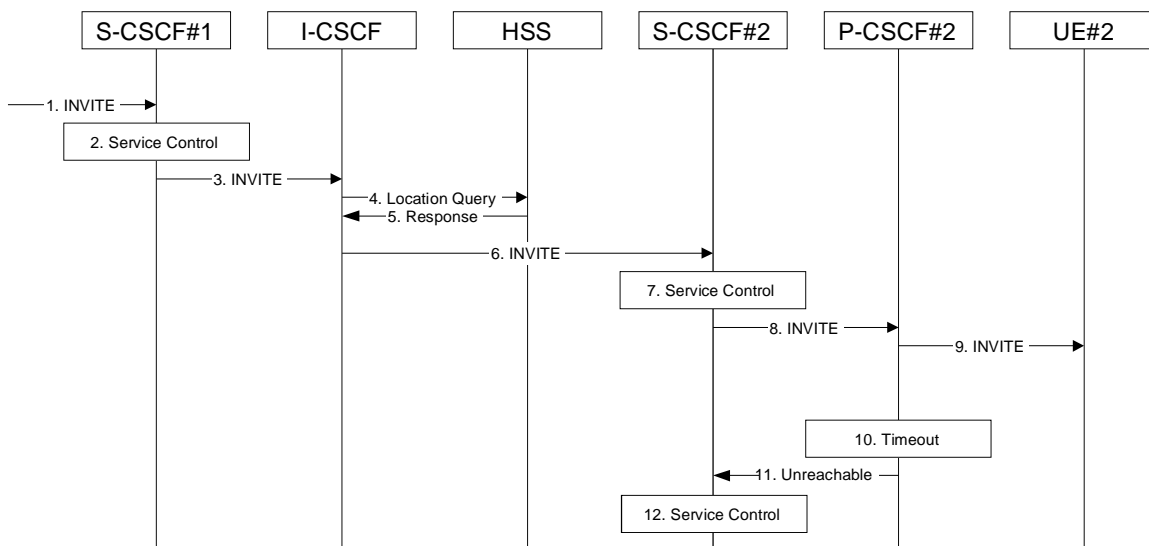
This is shown in the following information flow:
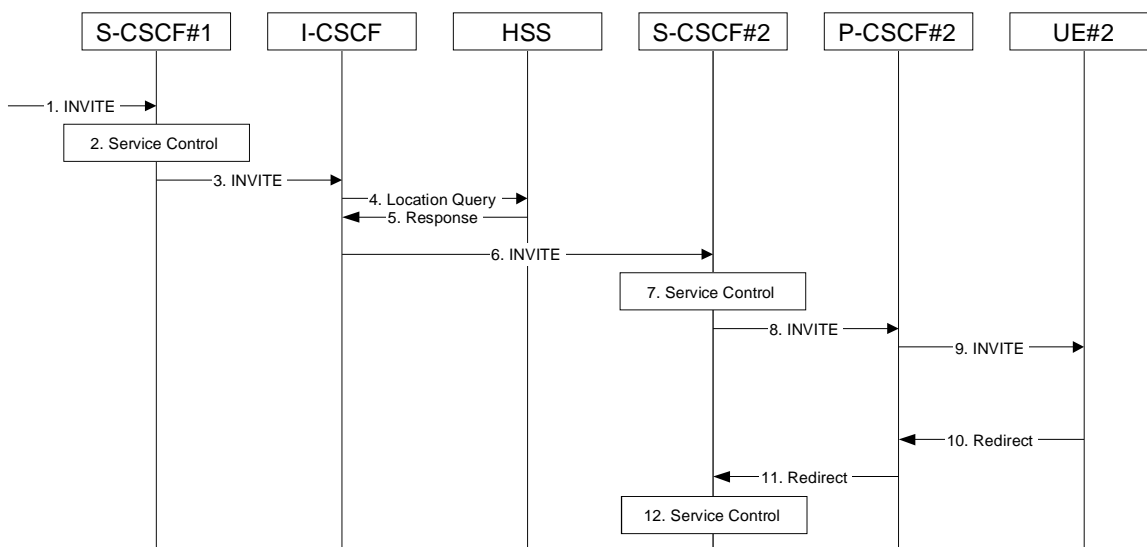
Figure 5.40: Session redirection initiated by UE

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.

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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

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

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

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

10. UE#2 determines that this session should be redirected, and optionally supplies the new destination ~~URL~~URI. This new destination ~~URL~~URI may be a phone number, an email address, a web page, or anything else that can be expressed as a ~~URL~~URI. The Redirect response is sent to P-CSCF#2

11. P-CSCF#2 forwards the Redirect response to S-CSCF#2.

12. S-CSCF#2 invokes whatever service logic is appropriate for this session redirection. If UE#2 does not subscribe to session redirection service, or did not supply a new destination ~~URL~~URI, S-CSCF#2 may supply one or may terminate the session setup attempt with a failure response. The new destination ~~URL~~URI may be a phone number, an email address, a web page, or anything else that can be expressed as a ~~URL~~URI. The procedures of subsection 1, 2, or 3 given above are followed, based on the type of ~~URL~~URI.

5.11.5.6   Session Redirection initiated by originating UE#1 after Bearer Establishment (REDIRECT to originating UE#1)

The UE of the destination user may request the session be redirected after a customer-specified ringing interval. The UE may also implement customer-specific feature processing, and base its decision to redirect this session on such things as identity of caller, current sessions in progress, other applications currently being accessed, etc. UE sends the SIP Redirect response to its P-CSCF, who forwards back along the signaling path to the originating endpoint, who initiates a session to the new destination.

The service implemented by this information flow is typically "Session Forward No Answer".

Redirect to another IMS endpoint (e.g. a sip: ~~URL~~URI) is shown in the following information flow:

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

Figure 5.41: Session redirection after bearer establishment

Step-by-step processing is as follows:

1-10.   Normal handling of a basic session establishment, up through establishment of the bearer channel and alerting of the destination user or by a previous session redirection after bearer establishment procedure.

11. Based on a timeout or other indications, UE#2 decides the current session should be redirected to a new destination ~~URL~~URI. This new destination ~~URL~~URI may be a phone number, an email address, a web page, or anything else that can be expressed as a ~~URL~~URI. The Redirect response is sent to P-CSCF#2.

12. P-CSCF#2 shall revoke any authorisation for QoS for the current session.

13. P-CSCF#2 forwards the Redirect response to S-CSCF#2.

14. S-CSCF#2 invokes whatever service logic is appropriate for this session redirection. If UE#2 does not subscribe to session redirection service, or did not supply a new destination ~~URL~~URI, S-CSCF#2 may supply one or may terminate the session setup attempt with a failure response. The new destination ~~URL~~URI may be a phone number, an email address, a web page, or anything else that can be expressed as a ~~URL~~URI. S-CSCF#2 generates a private ~~URL~~URI, addressed to itself, containing the new destination.

15. S-CSCF#2 sends a SIP Redirect response back to I-CSCF, containing the private ~~URL~~URI addressed to S-CSCF#2.

16. I-CSCF sends a Redirect response back to S-CSCF#1, containing the redirection destination.

17. S-CSCF#1 checks the number of redirections that have occurred for this session setup attempt, and if excessive, aborts the session. S-CSCF#1 stores the new destination information, generates a private ~~URL~~URI addressed to itself pointing to the stored information, and generates a modified Redirect response with the private ~~URL~~URI.

18. S-CSCF#1 sends the modified Redirect response to P-CSCF#1

19. P-CSCF#1 shall revoke any authorisation for QoS for the current session and sends the Redirect response to UE#1.

20. UE#1 initiates a new INVITE request to the address provided in the Redirect response. The new INVITE request is sent to P-CSCF#1

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

22. S-CSCF#1 retrieves the destination information saved in step #17, and invokes whatever other service logic is appropriate for this new session setup attempt.

23. S-CSCF#1 determines the network operator of the new destination address. The INVITE message is sent to I-CSCF#2, the I-CSCF for S-CSCF#2.

24. I-CSCF forwards the INVITE to S-CSCF#2

25. S-CSCF#2 decodes the private ~~URL~~URI, determines the network operator of the new destination, and sends the INVITE request to the I-CSCF for that network operator.

26. The remainder of this session completes as normal.

5.11.6 Session Transfer Procedures

5.11.6.0 General

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

5.11.6.1 Refer operation

The refer primitive is an information flow indicating a "Refer" operation, which includes a component element "Refer-To" and a component element "Referred-By". An information flow illustrating this is as follows:
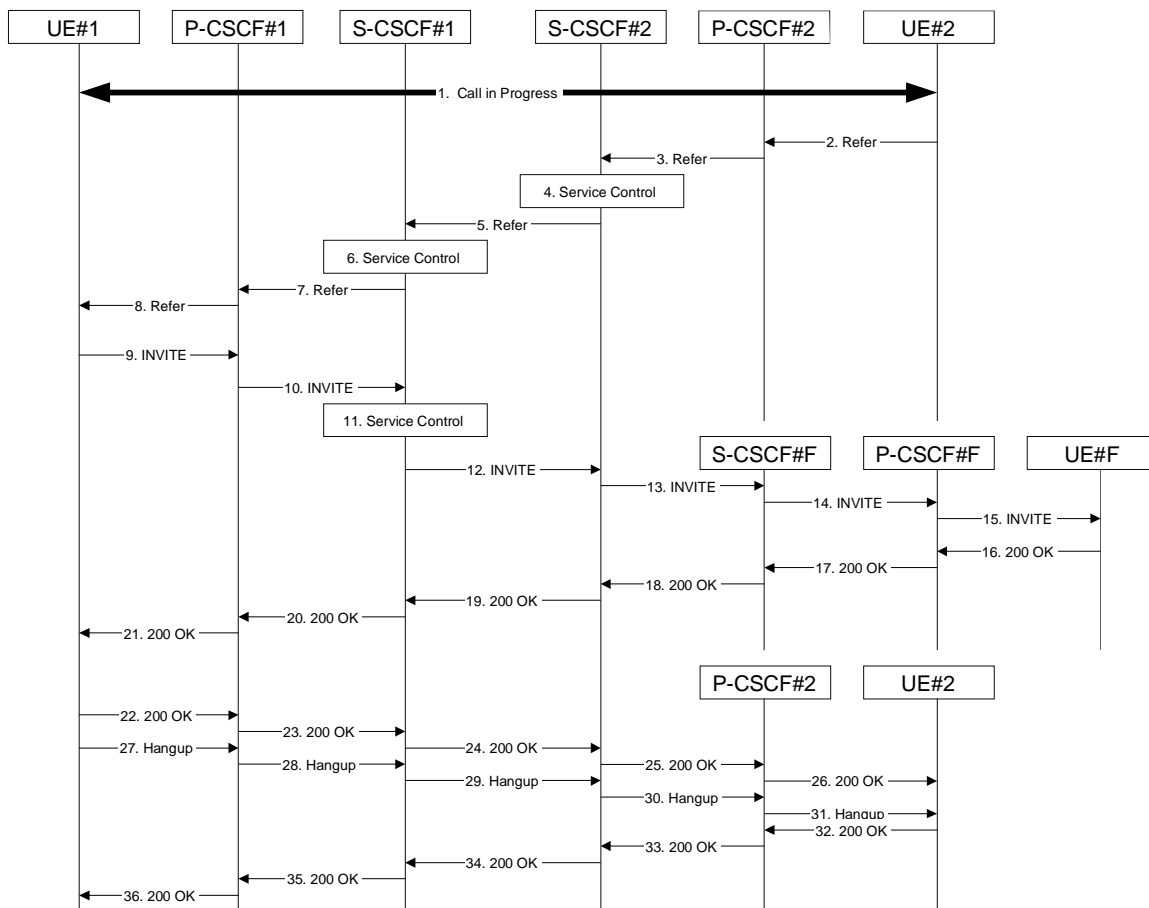
Figure 5.42: Refer operation

Step-by-step description of the information flow:

1. A multi-media session is assumed to already exist between UE#1 and UE#2, established either as a basic session or by one of the supplemental services described in this section.

2. UE#2 sends the Refer command to P-CSCF#2, containing "Refer-To" UE#F and "Referred-By" UE#2.

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

4. S-CSCF#2 invokes whatever service logic is appropriate for this request. If UE#2 does not subscribe to a transfer service, the request is rejected. S-CSCF#2 generates a private ~~URL~~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 ~~URL~~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 ~~URL~~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 ~~URL~~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 ~~URL~~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 ~~URL~~URI destination, and determines the final destination of the new session. It determines the network operator addressed by the destination ~~URL~~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#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.

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

# E.3	Address and identity management concepts

## E.3.1	Deriving IMS identifiers from the USIM

If the UICC does not contain an ISIM application, then the private user identity shall be derived from the USIM's IMSI, which allows for uniquely identifying the user within the 3GPP operator's network. The format of the private user identity derived from the IMSI is specified in 3GPP TS 23.003 [24].

If the UICC does not contain an ISIM application, then:

- A Temporary Public User identity shall be derived from the USIM's IMSI, and shall be used during initial SIP registration procedures.   The Temporary public user identity shall take the form of a ~~SIP URL~~SIP URI (as defined in RFC 3261 [12] and RFC 2396 [13]).   The format of the Temporary public user identity is specified in 3GPP TS 23.003 [24].

It is strongly recommended that the Temporary Public User Identity is set to barred for IMS non-registration procedures. The following applies if the Temporary Public User Identity is barred:

- A Temporary public user identity shall not be displayed to the user and shall not be used for public usage such as displaying on a business card.

- The Temporary Public User Identity shall only be used during the registration to obtain implicitly registered Public User Identities.

- The implicitly registered public user identities shall be used for session handling, in other SIP messages and at subsequent registration processes.

- After the initial registration, the UE shall only use the implicitly registered Public User Identity(s).

- A Temporary public user identity shall only be available to the CSCF and HSS nodes.

Note that in case of Temporary Public Identity is used, the user can not initiate any sessions until the implicitly registered public identities are available in the UE.

If the UICC does not have an ISIM application, then, the home domain name shall be derived from the Mobile Country Code and Mobile Network Code fields of the USIM's IMSI. The format of the home domain name is specified in 3GPP TS 23.003 [24].

In order to support pre-Rel 5 UICC accessing IMS services, a Temporary public user identity is generated using appropriate identity related to subscriber's subscription (e.g. in 3GPP it shall use IMSI)

When a Temporary Public Identity has been used to register an IMS user, the implicit registration will ensure that the UE, P-CSCF & S-CSCF have public user Identity(s) for all IMS procedures after the initial registration has been completed.

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

3GPP TSG-SA WG2 Meeting #43
Seoul, Korea.15th - 19th November 2004.

Tdoc ⌘ *S2-043571*

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **465** | ⌘**rev** | **-** | ⌘ | Current version: | **5.12.0** | ⌘ |

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: ⌘	Forward HSS name	
Source: ⌘	Siemens	
Work item code:⌘	IMS-CCR	**Date:** ⌘ 28/10/2004
Category: ⌘	**F**	**Release:** ⌘ Rel-5

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

Use one of the following releases:
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: ⌘	Subclause 5.8.1 of TS 23.228 describes an option, which is not supported by stage 3 specifications. There are no means defined to communicate an HSS address in the SIP registration flow from I-CSCF to S-CSCF.
Summary of change:⌘	Delete the option.
Consequences if not approved: ⌘	Inconsistency between stage 2 and stage 3.

Clauses affected: ⌘	5.8.1

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

Other comments: ⌘	

How to create CRs using this form:

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

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

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

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

5.8.1 User identity to HSS resolution

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

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

The subscription locator is accessed via the Dx interface. The Dx interface is the standard interface between the CSCF and the SLF.

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

The Dx interface provides:

- an operation to query the subscription locator from the I-CSCF or from the S-CSCF, respectively

- a response to provide the HSS name towards the I-CSCF or towards the S-CSCF, respectively.

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

The following two sections present the session flows on REGISTER and on INVITE messages.

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **466** | ⌘**rev** | **-** | ⌘ | Current version: | **6.7.0** | ⌘ |

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: ⌘	Forward HSS name		
Source: ⌘	Siemens		
Work item code:⌘	IMS-CCR	*Date:* ⌘	28/10/2004
Category: ⌘	**A**	*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: ⌘	Subclause 5.8.1 of TS 23.228 describes an option, which is not supported by stage 3 specifications. There are no means defined to communicate an HSS address in the SIP registration flow from I-CSCF to S-CSCF.
Summary of change:⌘	Delete the option.
Consequences if not approved: ⌘	Inconsistency between stage 2 and stage 3.

Clauses affected: ⌘	5.8.1	

	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.

5.8.1 User identity to HSS resolution

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

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

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

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

The Dx interface provides:

- an operation to query the subscription locator from the I-CSCF or from the S-CSCF, respectively

- a response to provide the HSS name towards the I-CSCF or towards the S-CSCF, respectively.

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

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

The Dh interface provides:

- an operation to query the subscription locator from the AS

- a response to provide the HSS name towards the AS.

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

Subclause 5.8.4 presents the message flow on the Dh interface.

CR-Form-v7

CHANGE REQUEST

| ⌘ | **23.228** CR **454** | ⌘**rev** **1** ⌘ | Current version: **6.7.0** ⌘ |

*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: ⌘	Various editorial corrections		
Source: ⌘	Lucent Technologies		
Work item code:⌘	IMS2	**Date:** ⌘	15/11/2004
Category: ⌘	**D**	**Release:** ⌘	Rel-6

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

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

Reason for change: ⌘	As text has been added for Release 6 many editorial errors have been added as well. This CR provides corrections for these errors.
Summary of change:⌘	Applied changes to correct incorrect use of punctuation, incorrect figure numbers, incorrect figure references, incorrect document references, incorrect formating or style use, and incorrect flow numbering.
Consequences if not approved: ⌘	The document is is difficult to use and subject to misinterpretation.
Clauses affected: ⌘	2, 4.2.4, 4.2.4a, 4.2.4b, 4.2.5, 4.2.7.2, 4.3.3.1, 4.3.3.2, 4.3.3.3, 4.3.3.4, 4.3.6, 4.4, 4.6.3, 5.1.2, 5.1.5.1, 5.2.1, 5.2.1a.0, 5.2.1a.1, 5.2.2.2, 5.2.2.3, 5.2.2.4, 5.3.1, 5.3.2.1, 5.4.3, 5.4.9.0, 5.4.12.1, 5.4.12.2, 5.4.12.3, 5.5.4, 5.6.0, 5.6.5, 5.7a, 5.8.1, 5.8.4, 5.10.2, 5.11.3.1, 5.11.3.3, 5.11.3.4, 5.11.4.0, 5.11.4.1, 5.11.4.2, 5.11.5.1, 5.11.5.2, 5.11.5.2a, 5.11.5.6, 5.12.2, 5.16.1.1.0, 5.16.1.1.1, 5.16.1.1.2, 5.16.2.1, and 5.16.2.2.1, and 5.16.2.2.3

		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.

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

1 Scope

This document defines the stage-2 service description for the IP Multimedia Core Network Subsystem (IMS), which includes the elements necessary to support IP Multimedia (IM) services. ITU-T Recommendation I.130 [4] describes a three-stage method for characterisation of telecommunication services, and ITU-T Recommendation Q.65 [3] defines stage 2 of the method.

This document does not cover the Access Network functionality except as they relate to provision of IM services, these aspects are covered in the normative Annex E. 3GPP TS 23.060 [23] describes GPRS. GSM 03.64 [5] contains an overall description of the GSM GPRS radio interface. 3GPP TS 25.301 [11] contains an overall description of the UMTS Terrestrial Radio Access Network.

This document identifies the mechanisms to enable support for IP multimedia applications. In order to align IP multimedia applications wherever possible with non-3GPP IP applications, the general approach is to adopt non-3GPP specific IP based solutions.

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 2806: "URLs for Telephone Calls".

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

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

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

[37]   3GPP TS 26.xxx141: "IMS messaging and Presence; Media formats and codecs".

[38]   draft-ietf-sip-callee-caps-01 (October 2003)IETF RFC 3840: "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

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

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

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

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

[42] draft-ietf-sip-callerprefs-10 (October 2003): IETF RFC 3841: "Caller Preferences for the Session Initiation Protocol (SIP)")".

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

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

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

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

4.2.4 IP multimedia Subsystem Service Control Interface (ISC)

The ISC interface is between the Serving CSCF and the service platform(s).

An Application Server (AS) offering value added IM services resides either in the user's home network or in a third party location. The third party could be a network or simply a stand-alone AS.

The Serving-CSCF to AS interface is used to provide services residing in an AS. Two cases were identified:

- Serving-CSCF to an AS in Home Network.

- Serving-CSCF to an AS in External Network (e.g., Third Party or Visited)

The SIP Application Server may host and execute services. The SIP Application Server can influence and impact the SIP session on behalf of the services and it uses the ISC interface to communicate with the S-CSCF.

The ISC interface shall be able support subscription to event notifications between the Application Server and S-CSCF to allow the Application Server to be notified of the implicit registered public user identitPublic User Identities, registration state and UE capabilities and characteristics in terms of SIP User Agent capabilities and characteristics.

The S-CSCF shall decide whether an Application Server is required to receive information related to an incoming initial SIP request to ensure appropriate service handling. The decision at the S-CSCF is based on (filter) information received from the HSS. This filter information is stored and conveyed on a per application serverApplication Server basis for each user. The name(s)/address(es) information of the application serverApplication Server(s) are received from the HSS.

For an incoming SIP request, the S-CSCF shall perform any filtering for ISC interaction before performing other routing procedures towards the terminating user, e.g. forking, caller preferences etc.

The S-CSCF does not handle service interaction issues.

Once the IM SSF, OSA SCS or SIP Application Server has been informed of a SIP session request by the S-CSCF, the IM SSF, OSA SCS or SIP Application Server shall ensure that the S-CSCF is made aware of any resulting activity by sending messages to the S-CSCF.

From the perspective of the S-CSCF, The "SIP Application server", "OSA service capability server" and "IM-SSF" shall exhibit the same interface behaviour.

When the name/address of more than one ~~"application server"~~Application Server is transferred from the HSS, the S-CSCF shall contact the ~~"application servers"~~Application Servers in the order supplied by the HSS. The response from the first ~~"application server"~~Application Server shall be used as the input to the second ~~"application server"~~Application Server. Note that these multiple ~~"application servers"~~Application Servers may be any combination of the SIP Application server, OSA service capability server, or IM-SSF types.

The S-CSCF does not provide authentication and security functionality for secure direct third party access to the IM subsystem. The OSA framework provides a standardized way for third party secure access to the IM subsystem.

If a S-CSCF receives a SIP request on the ISC interface that was originated by an Application Server destined to a user served by that S-CSCF, then the S-CSCF shall treat the request as a terminating request to that user and provide the terminating request functionality as described above. Both registered and unregistered terminating requests shall be supported.

It shall be possible for an Application Server to generate SIP requests and dialogs on behalf of users. Such requests are forwarded to the S-CSCF serving the user, and the S-CSCF shall perform regular originating procedures for these requests.

> Editor's note: The detailed procedures for handling such requests (e.g. security, charging, routing, etc…) are FFS.

More specifically the following requirements apply to the IMS Service control interface:

1. The ISC interface shall be able to convey charging information as per 3GPP TS 32.200[25] and 3GPP TS 32.225[26].

2. The protocol on the ISC interface shall allow the S-CSCF to differentiate between SIP requests on Mw, Mm and Mg interfaces and SIP Requests on the ISC interface.

Figure 4.3: Void

Besides the Cx interface the S-CSCF supports only one standardised protocol for service control, which delegates service execution to an ~~"Application Server"~~Application Server. The protocol to be used on the ISC interface shall be SIP (as defined by RFC 3261 [12], other relevant RFC's, and additional enhancements introduced to support 3GPP´s needs on the Mw, Mm, Mg interfaces). On the ISC interface, extensions to SIP shall be avoided but are not expressly prohibited.

The notion of a "SIP leg" used throughout this specification is identical to the notion of a call leg which is the same as a SIP dialog defined by RFC 3261 [12]. The same SIP leg that is received by the S-CSCF on the Mw, Mm and Mg interfaces is sent on the ISC interface. The same SIP leg that is received by the S-CSCF on the ISC interface is sent on the Mw, Mm and Mg interfaces.

Concerning the relationship between the SIP legs of the ISC interface and the SIP legs of the Mw, Mm, and Mg interfaces the S-CSCF acts as a SIP proxy, as shown in Figures ~~4.a 4e~~4.3a – 4.3e below.

Figures 4.3a-4.3e below depict the possible high-level interactions envisioned between the S-CSCF and the Application Server.
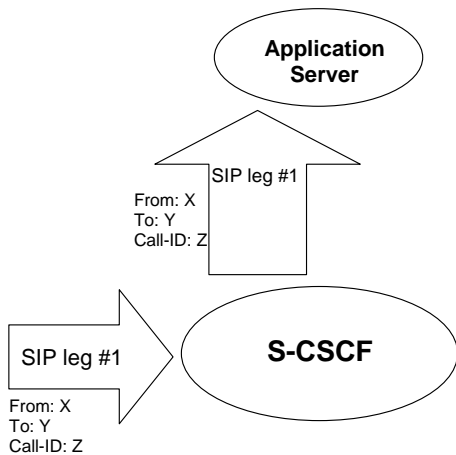
Figure 4.3a: Application Server acting as terminating UA, or redirect server
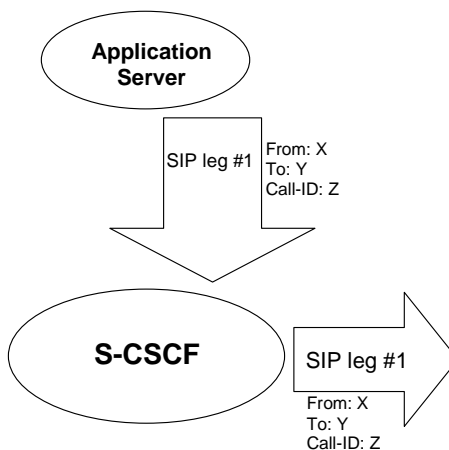
Figure 4.3b: Application Server acting as originating UA
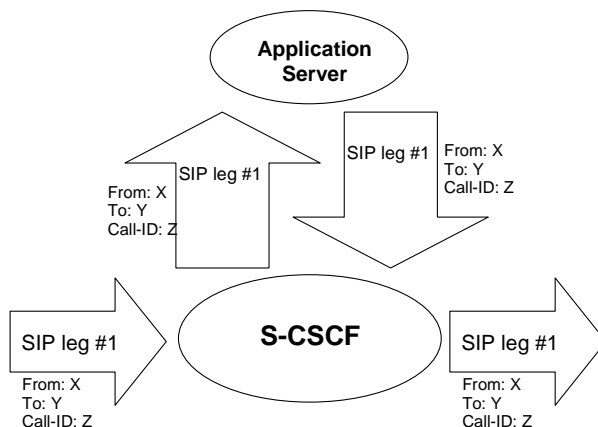
Figure 4.3c: Application Server acting as a SIP proxy
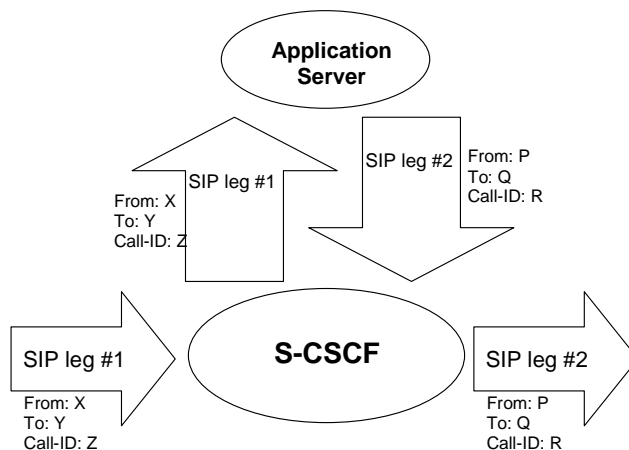
**Figure 4.3d:	Application Server performing 3rd party call control**
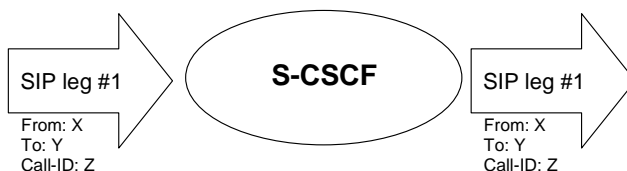
**Figure 4.3e:	A SIP leg is passed through the S-CSCF without Application Server involvement**

## 4.2.4a	HSS to service platform Interface

The ~~"application server"~~Application Server (SIP Application Server and/or the OSA service capability server and/or IM-SSF) may communicate to the HSS. The Sh and Si interfaces are used for this purpose.

For the Sh interface, the following shall apply:

1.	The Sh interface is an intra-operator interface.

2.	The Sh interface is between the HSS and the "SIP ~~application server~~Application Server" and between the HSS and the "OSA service capability server". The HSS is responsible for policing what information will be provided to each individual ~~application server~~Application Server.

3.	The Sh interface transports transparent data for e.g. service related data , user related information, …
	In this case, the term transparent implies that the exact representation of the information is not understood by the HSS or the protocol.

4.	The Sh interface also supports mechanisms for transfer of user related data stored in the HSS (e.g. user service related data, MSISDN, visited network capabilities, user location (cell global ID/SAI or the address of the serving network element, etc))

	Note:	before providing information relating to the location of the user to a SIP Application Server, detailed privacy checks frequently need to be performed in order to meet the requirements in TS22.071 [27]. The SIP Application Server can ensure that these privacy requirements are met by using the Le interface to the GMLC (see TS 23.271) instead of using the Sh interface.

5.	The Sh interface also supports mechanisms for transfer of standardised data, e.g. for group lists, which can be accessed by different ~~application server~~Application Servers. Those ~~application server~~Application Servers sharing the data shall understand the data format. This enables sharing of common information between ~~application server~~Application Servers, e.g. data managed via the Ut reference point.

The Si interface is between the HSS and the IM-SSF. It transports CAMEL subscription information including triggers for use by CAMEL based application services.

4.2.4b   S-CSCF Service Control Model
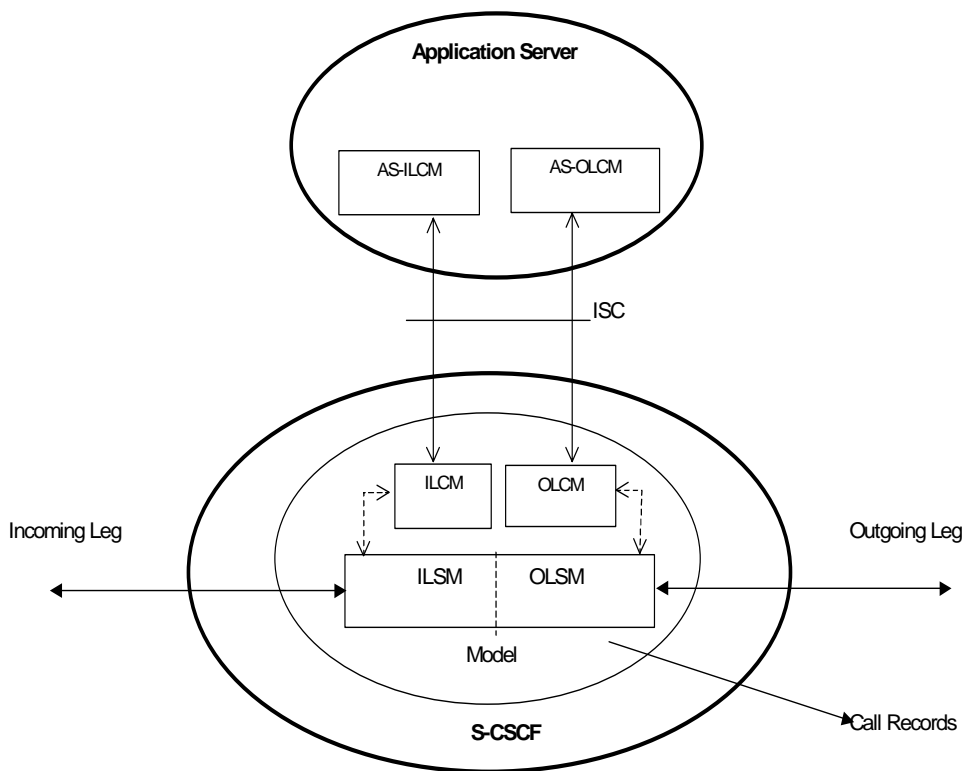
Figure 4.3f: Service Control Model with Incoming Leg Control and Outgoing Leg Control

Figure 1Figure 4.3f illustrates the relationship between the S-CSCF and AS. It includes a first-level of modelling inside the S-CSCF and inside the AS. To keep the model simple only one incoming leg and one outgoing leg are shown. In practice a session may consist of more than one incoming leg and/or more than one outgoing leg(s), when using User Agents. An AS may create one or more outgoing legs independent of incoming legs. An AS may create one or more outgoing legs even when there are no incoming legs.

While the above figures show session related flows, the service control model can be applied to other SIP transactions such as registration. Incoming or outgoing leg information e.g. state information, may be passed between the S-CSCF and AS implicitly or explicitly. Implicitly means that SIP information in transit carries information about the state of the session (e.g. an INVITE message received at the S-CSCF on an incoming leg may be sent to the AS with no changes or with some additional information). Explicitly means that SIP information is generated, e.g. to transfer state change information from an S-CSCF to an AS in circumstances where there is no ongoing SIP transaction that can be used. It is a matter for Stage 3 design to determine when to use implicit or explicit mechanisms and to determine what extensions to SIP are necessary.

The internal model of the S-CSCF (shown in Figure 1Figure 4.3f) may sometimes exhibit proxy server like behaviour either by passing the requests to the Application Server or by passing the requests out of the system. A Proxy server may maintain session state or not. The S-CSCF may sometimes exhibit User Agent like behaviour. Some Applications require state to be maintained in the S-CSCF. Their exact behaviour depends on the SIP messages being handled, on their context, and on S-CSCF capabilities needed to support the services. It is a matter for Stage 3 design to determine the more detailed modelling in the S-CSCF.

The internal model of the AS (shown in Figure 1Figure 4.3f) may exhibit User Agent like behaviour. The exact behaviour depends on the SIP messages being handled and on their context. Detailed Stage 3 modelling for the AS is not required.

The definitions used in the model are:

Combined ILSM OLSM – Incoming/outgoing Leg State Model: Models the behaviour of an S-CSCF for handling SIP messages on incoming and outgoing session legs. The Combined I/OLSM shall be able to store session state information. It may act on each leg independently, acting as a SIP Proxy, Redirect Server or User Agent dependant on the information received in the SIP request, the filter conditions specified or the state of the session.

It shall be possible to split the application handling on each leg and treat each endpoint differently.

ILCM - Incoming Leg Control Model: Models the behaviour of an S-CSCF for handling SIP information sent to and received from an AS for an incoming session leg. The ILCM shall store transaction state information.

OLCM - Outgoing Leg Control Model: Models the behaviour of an S-CSCF for handling SIP information received from and sent to an AS for an outgoing session leg. The OLCM shall store transaction state information.

AS-ILCM - Application Server Incoming Leg Control Model: Models AS behaviour for handling SIP information for an incoming leg. The AS-ILCM shall store Transaction State, and may optionally store Session State depending on the specific service being executed.

AS-OLCM - Application Server Outgoing Leg Control Model: Models AS behaviour for handling SIP information for an outgoing leg. The AS-OLCM shall store Transaction State, and may optionally store Session State depending on the specific service being executed.

4.2.5 The QoS requirements for an IM CN subsystem session

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

1. Independence between QoS signalling and Session Control

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

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

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

3. Void.

4. Restricted Resource Access at the IP BS Level

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

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

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

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

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

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

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

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

e. In establishing an IMS session, it shall be possible to use already allocated bearer resources, if these resources fulfill the needs of the session. However, note that QoS policy control mechanisms of the IP-CAN may not allow to use already allocated bearer resources.

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

7. The Efficiency of QoS Signalling and Resource Allocation

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

8. Dynamic QoS Negotiation and Resource Allocation

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

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

9. Prevention of Theft of Service

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

10. Prevention of Denial of Service

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

4.2.6 QoS Requirements for IM CN subsystem signalling

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

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

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

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

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

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

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

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

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

# 4.2.7	Support of SIP forking

## 4.2.7.1	SIP Forking

SIP forking is the ability of a SIP proxy server to fork SIP request messages to multiple destinations according to RFC 3261 [12].

## 4.2.7.2	Forking within and outside the IM CN Subsystem

The IM CN subsystem shall have the capability to fork requests to multiple destinations; this capability is subject to rules for forking proxies defined in RFC 3261 [12].

- The S-CSCF shall support the ability for a ~~public user identit~~Public User Identity to be registered from multiple contact addresses, as defined in RFC 3261 [12]. The S-CSCF shall support forking so that an incoming SIP request addressed to a Public User Identity is proxied to multiple registered contact addresses. This allows forking across multiple contact addresses of the same Public User Identity.

- When multiple contact addresses have been registered, then the S-CSCF shall exhibit the following behaviour with regards to forking the incoming SIP request:

  1. If the UE has indicated capability information upon IMS registration in terms of	SIP User Agent capabilities and characteristics described in ~~"draft-ietf-sip-callee-caps-01"~~RFC 3840 [38], then the S-CSCF shall use it to generate a target contact set using the matching mechanism described in ~~"draft-ietf-sip-callerprefs-10" [xx]~~RFC 3841 [42]. If the UE has not indicated any capabilities for the contact addresses upon registration, then the S-CSCF may still use the preference information, if indicated for the contact addresses upon registration, as described in the following bulletpoint below.

  2. If the UE has indicated preference information for contact addresses upon registration, then the S-CSCF shall use it to decide if parallel or sequential forking is used across the contact addresses that have matching callee capabilities, as described in RFC 3261 [12]. If the UE has not indicated any preference for the matching contact addresses upon registration, or if the preferences for the matching contact addresses have equal value, then it is up to the configuration of the S-CSCF if parallel or sequential forking is to be performed across the contact addresses that have matching callee capabilities.

- Application Servers in the IMS may act as a forking proxy in the sense of RFC 3261 [12].

  Note:	The AS may subscribe to the registration event package to retrieve the contact address(es) of the UE.

- S-CSCFs shall provide the necessary support for forking by Application Servers.

Additionally, other networks outside the IM CN Subsystem are able to perform SIP forking.

## 4.2.7.3	Support for forked requests

UE and MGCF shall be ready to receive responses generated due to a forked request and behave according to the procedures specified in [12] and in this section.

The UE and MGCF may accept or reject early dialogues from different terminations as described in [12], for example if the UE is only capable of supporting a limited number of simultaneous dialogs.

Upon the reception of a first final 200 OK (for INVITE), the UE or MGCF shall acknowledge the 200 OK. In addition the UE or MGCF may require updating the allocated resources according to the resources needed. In case the UE or MGCF receives a subsequent 200 OK, the UE or MGCF shall acknowledge the dialogue and immediately send a BYE to drop the dialog.

The UE and MGCF may include preferences according to "draft-ietf-sip-callerprefs-10" [42], in INVITE's, indicating that proxies should not fork the INVITE request. The S-CSCF and AS should follow the preferences, if included in the INVITE request. On the terminating side, UE and MGCF shall be able to receive, as specified in [12], several requests for the same dialog that were forked by a previous SIP entity.

Application Servers and MRFCs shall be capable to handle forked requests according to the procedures specified in [12].

4.3 Naming and addressing concepts

4.3.1 Address management

The mechanisms for addressing and routing for access to IM CN subsystem services and issues of general IP address management are discussed in TS 23.221 [7].

When a UE is assigned an IPv6 prefix, it can change the global IPv6 address it is currently using via the mechanism defined in RFC 3041 [16a], or similar means. When a UE is registered in the IM CN Subsystem with an IP address, any change to this IP address that is used to access the IM CN subsystem will result in dropping the active SIP dialogs, and shall trigger automatic registration. This automatic registration updates the UE's IP address and security association. To avoid disruption of ongoing IM CN subsystem services, the UE should not change the IP address that it uses to access the IM CN subsystem while engaged in active SIP dialogs (e.g. INVITE or SUBSCRIBE-NOTIFY dialogs).

4.3.2 Void

Figure 4.4: Void

4.3.3 Identification of users

4.3.3.0 General

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

4.3.3.1 Private user identities

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

- The Private User Identity is not used for routing of SIP messages.

- The Private User Identity shall be contained in all Registration requests, (including Re-registration and De-registration requests) passed from the UE to the home network.

- An ISIM application shall securely store one Private User Identity. It shall not be possible for the UE to modify the Private User Identity information stored on the ISIM application.

- The Private User Identity is a unique global identity defined by the Home Network Operator, which may be used within the home network to identify the user's subscription (e.g. IM service capability) from a network perspective. The Private User Identity identifies the subscription, not the user.

- The Private User Identity shall be permanently allocated to a user's subscription (it is not a dynamic identity), and is valid for the duration of the user's subscription with the home network.

- The Private User Identity is used to identify the user's information (for example authentication information) stored within the HSS (for use for example during Registration).

- The Private User Identity may be present in charging records based on operator policies.

- The Private User Identity is authenticated only during registration of the user, (including re-registration and de-registration).

- The HSS needs to store the Private User Identity.

- The S-CSCF needs to obtain and store the Private User Identity upon registration and unregistered termination.

4.3.3.2 Public user identities

Every IM CN subsystem user shall have one or more ~~public user identit~~Public User Identities [8]. The ~~public user identit~~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 identit~~Public User Identity/identities shall take the form of SIP URL (as defined in RFC 3261 [12] and RFC2396 [13]) or the "tel:"-URL format [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 identit~~Public User Identities shall not be used for routing within the IMS, and session requests based upon E.164 format ~~public user identit~~Public User Identities will require conversion into SIP URL 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 URL. This phone number can be in the form of E.164 format (prefixed with a '+' sign), or a local format using local dialling plan and prefix. The IMS will interpret the phone number with a leading '+' to be a fully defined international number.

4.3.3.4 Relationship of ~~private~~ Private and ~~public user identit~~Public User Identities

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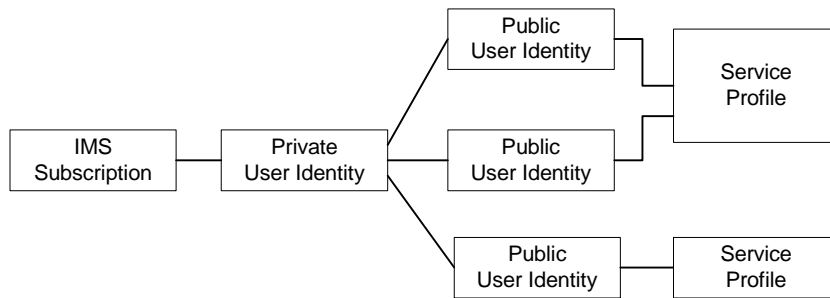
Figure 4.5: Relationship of the ~~private user identit~~Private User Identity and ~~public user identit~~Public User Identities

The IMS Service Profile is a collection of service and user related data as defined in 3GPP TS 29.228 [30]. The Service Profile is independent from the Implicit Registration Set, e.g. ~~IMPUs~~ 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 identit~~Public User Identity shall be registered at a single S-CSCF at one time. All ~~public user identit~~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 identit~~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 identit~~Public User Identity is associated with one and only one service profile. Each service profile is associated with one or more ~~public user identit~~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 identit~~Private User Identities within the same IMS subscription. Hence, a particular ~~public user identit~~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 identit~~Public User Identity with ~~private user identit~~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 identit~~Public User Identity sharing mechanism described above is not intended to support sharing of identities across large numbers of ~~private user identit~~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 identit~~Public User Identities within a subscription are shared and which are not.
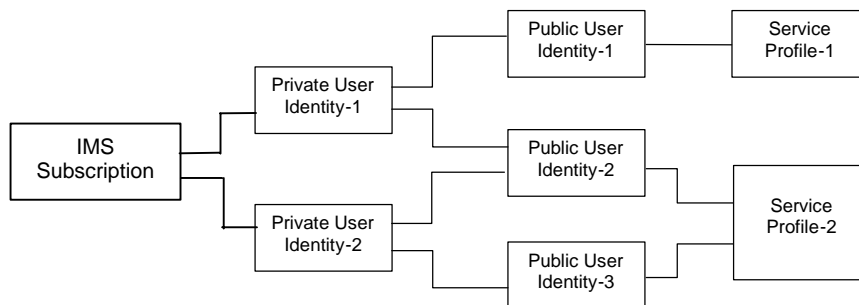
Figure 4.6 – The relation of a shared Public User Identity (Public-ID-2) and Private User Identities

All Service Profiles of a user shall be stored in the same HSS, even if the user has one or more shared ~~public user identit~~Public User Identities.

4.3.4 Identification of network nodes

The CSCF, BGCF and MGCF nodes shall be identifiable using a valid SIP URL (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol, (e.g. Gm, Mw, Mm, and Mg). These SIP URLs would be used when identifying these nodes in header fields of SIP messages. However this does not require that these URLs will be globally published in DNS.

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 URL "tel:" format [15] to a SIP routable SIP URL 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 server~~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.

Public Service Identities shall take the form of SIP URL as defined in RFC 3261 [12] and RFC 2396 [13] or the "tel:"-URL format as defined in RFC 2806 [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~~Application Server, which executes the service specific logic as identified by the Public Service Identity.

The IM CN Subsystem shall provide capability of routing IMS messages using Public Service Identity.

4.4 Signalling concepts

A Single session control between the UE and CSCF~~.~~:

- ~~~~For Multi-Media type services delivered via the PS Domain within this architecture, a single session control protocol shall be used between the user equipment UE and the CSCF (over the Gm reference point).

Protocols over the Gm reference point~~.~~:

- – The single protocol applied between the UE and CSCF (over the Gm reference point) within this architecture will be based on SIP (as defined by RFC 3261 [12], other relevant RFC's, and additional enhancements required to support 3GPP's needs).

A Single session control on the Mw, Mm, Mg, Mi, Mj, Mk:

- – A single session control protocol shall be used on the session control interfaces between:

    - MGCF and CSCF (Mg),

    - between CSCFs (Mw), and

    - between a CSCF and external IP networks (Mm),

    - Between between CSCF and BGCF (Mi),

    - Between between BGCF and MGCF (Mj), and

    - Between between BGCF and BGCF (Mk).

Protocols for the Mw, Mm, Mg, Mi, Mj, Mk:

- – The single session control protocol applied to these interfaces will be based on SIP (as defined by RFC 3261 [12], other relevant RFC's, and additional enhancements required to support 3GPP´s needs).

UNI vs. NNI session control:

- – The SIP based signalling interactions between CN elements may be different then than SIP based signalling between the UE and the CSCF.

Based on operator preference, network configuration hiding may be applied. If network configuration hiding is applied, then the I-CSCF(THIG) shall be used in order to fulfil the requirements as identified in TS 22.228 [8]. It is used to restrict the following information from being passed outside of an operator's network: exact number of S-CSCFs, capabilities of S-CSCFs, or capacity of the network. A more detailed motivation for such functionality is given in Annex C.

Restrict access from external networks:

- – The signalling solution shall allow the operator to restrict access from external networks (application level).

Access to HSS:

- – A network operator can control access to the HSS.

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

4.6.3   Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:

Registration

- May behave as a Registrar as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts registration requests and makes its information available through the location server (eg. HSS).

Session-related and session-unrelated flows

- Session control for the registered endpoint's sessions. It shall reject IMS communication to/from ~~public user identit~~Public User Identity(s) that are barred for IMS communications after completion of registration, as described in subclause 5.2.1.

- May behave as a Proxy Server as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts requests and services them internally or forwards them on, possibly after translation.

- May behave as a User Agent as defined in RFC 3261 [12] or subsequent versions, i.e. it may terminate and independently generate SIP transactions.

- Interaction with Services Platforms for the support of Services

- Provide endpoints with service event related information (e.g. notification of tones/announcement together with location of additional media resources, billing notification)

- For an originating endpoint (i.e. the originating user/UE, or originating AS)

  - Obtain from a database the Address of the I-CSCF for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URL), when the destination user is a customer of a different network operator, and forward the SIP request or response to that I-CSCF.

  - When the destination name of the destination user (e.g. dialled phone number or SIP URL), and the originating user is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.

  - Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.

  - Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.

  - In case the request is an originating request from an Application Server:

    - Verify that the request coming from the AS is an originating request, and apply procedures accordingly (e.g. invoke interaction with Service Platforms for originating services, etc…);

    - Process and proceed with the request even if the user on whose behalf the AS had generated the request is unregistered.

    - Process and proceed with other requests to and from the user on whose behalf the AS had generated the request.

    - Reflect in the charging information that an AS has initiated the session on behalf of a user.

- For a destination endpoint (i.e. the terminating user/UE)

  - Forward the SIP request or response to a P-CSCF for a MT procedure to a home user within the home network, or for a user roaming within a visited network where the home network operator has chosen not to have an I-CSCF in the path

  - Forward the SIP request or response to an I-CSCF for a MT procedure for a roaming user within a visited network where the home network operator has chosen to have an I-CSCF in the path.

  - Modify the SIP request for routing an incoming session to CS domain according to HSS and service control interactions, in case the user is to receive the incoming session via the CS domain.

  - Forward the SIP request or response to a BGCF for call routing to the PSTN or the CS domain.

  - If the SIP request contains preferences for characteristics of the destination endpoint, perform preference and capability matching as specified in "draft-ietf-sip-callerprefs-10" [41].

Charging and resource utilisation:

- Generation of CDRs

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

5.1.2   Procedures related to Serving-CSCF assignment

5.1.2.1   Assigning a Serving-CSCF for a user

When a UE attaches and makes itself available for access to IMS services by explicitly registering in the IMS, a S-CSCF shall be assigned to serve the UE.

The assignment of an S-CSCF is performed in the I-CSCF. The following information is needed in the selection of the S-CSCF:

1. Required capabilities for user services
    This information is provided by the HSS.

2. Operator preference on a per-user basis
    This information is provided by the HSS.

3. Capabilities of individual S-CSCFs in the home network
    This is internal information within the operator's network. This information may be used in the S-CSCF selection. This information is obtained by the I-CSCF by methods not standardised in this release.

4. Topological (i.e. P-CSCF) information of where the user is located
    This is internal information within the operator's network. This information may be used in the S-CSCF selection. The P-CSCF name is received in the registration request. The topological information of the P-CSCF is obtained by the I-CSCF by methods not standardised in this Release ~~5~~.

5. Topological information of where the S-CSCF is located
    This is internal information within the operator's network. This information may be used in the S-CSCF selection. This information is obtained by the I-CSCF by methods not standardised in this release.

6. Availability of S-CSCFs
    This is internal information within the operator's network. This information may be used in the S-CSCF selection. This information is obtained by the I-CSCF by methods not standardised in this release.

In order to support the S-CSCF selection described above and to allow the S-CSCF to perform its tasks, it is required that the following types of information be transferred between the CSCF and the HSS:

1   The Cx reference point shall support the transfer of CSCF-UE security parameters from HSS to CSCF.

-   This allows the CSCF and the UE to communicate in a trusted and secure way (there is no à priori trust relationship between a UE and a CSCF)

-   The security parameters can be for example pre-calculated challenge-response pairs, or keys for an authentication algorithm, etc.

2   The Cx reference point shall support the transfer of service parameters of the subscriber from HSS to CSCF.

-   This may include e.g. service parameters, ~~application server~~Application Server address, triggers, information on subscribed media etc. The information on subscribed media is provided in the form of a profile identifier; details of the allowed media parameters associated with the profile identifier are configured in the S-CSCF.

3   The Cx reference point shall support the transfer of CSCF capability information from HSS to CSCF.

- This may include e.g. supported service set, protocol version numbers etc.

4   The Cx reference point shall support the transfer of session signalling transport parameters from CSCF to HSS. The HSS stores the signalling transport parameters and they are used for routing mobile terminated sessions to the Serving-CSCF.

- The parameters may include e.g. IP-address and port number of CSCF, transport protocol etc.

The information mentioned in items 1 – 4 above shall be transferred before the CSCF is able to serve the mobile user. It shall also be possible to update this information while the CSCF is serving the user, for example if new services are activated for the user.

5.1.2.2   Cancelling the Serving-CSCF assignment

Cancellation of the assigned Serving CSCF is either:

- Initiated from the Serving CSCF itself, e.g. due to timeout of the registration

- Performed as a result of an explicit deactivation/de-registration from the IMS. This is triggered by the UE.

- Performed due to a request from the HSS over the Cx interface, e.g. due to changes in the subscription.

5.1.2.3   Re-assignment of a Serving-CSCF

Re-assignment of a S-CSCF shall be possible in the following cases:

- The S-CSCF that was previously assigned is unavailable during registration.

- In the initial registration, when the S-CSCF has been allocated for the unregistered user

5.1.3   Procedures related to Interrogating-CSCF

The architecture shall support multiple I-CSCFs for each operator. A DNS-based mechanism for selecting the I-CSCF shall be used to allow requests to be forwarded to an I-CSCF based, for example, on the location or identity of the forwarding node.

5.1.4   Procedures related to Proxy-CSCF

The routing of the SIP registration information flows shall not take into account previous registrations (i.e., registration state). The routing of the session information flows (e.g., INVITE) shall take into account the information received during the registration process.

5.1.5   Subscription Updating Procedures

5.1.5.0   General

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

5.1.5.1   Subscription updating information flow

This section provides the information flows for subscription data updating procedure.
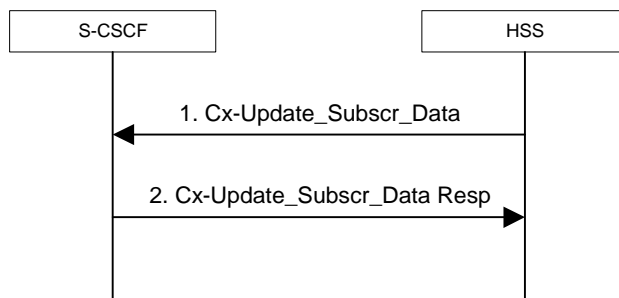
Figure 5.0b: Subscription data updating

1. The HSS sends the Cx-Update_Subscr_Data with the subscription data to the S-CSCF.

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

5.2 Application level registration procedures

5.2.0 General

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

5.2.1 Requirements considered for registration

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

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

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

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

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

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

6. The Serving-CSCF is able to retrieve a service profile of the user who has IMS subscription. The S-CSCF shall check the registration request against the filter information and if necessary inform the ~~application server~~Application Server about the registration of the user. It shall be possible for the filter information to allow either just the initial registration of the user or also subsequent re-registrations of the user to be communicated to the ~~application server~~Application Server. The Serving-CSCF knows how to reach the Proxy-CSCF currently serving the user who is registered.

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

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

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

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

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

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

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

13. The UE may indicate its capabilities and characteristics in terms of SIP User Agent capabilities and characteristics described in "draft-ietf-sip-callee-caps-01" [38] during IMS registration. The UE may also update its capabilities by initiating a re-registration when the capabilities are changed on the UE.

5.2.1a   Implicit Registration

5.2.1a.0   General

When an user has a set of ~~public user identit~~Public User Identities defined to be implicitly registered via single IMS registration of one of the ~~public user identit~~Public User Identity's in that set, it is considered to be an Implicit Registration. No single public identity shall be considered as a master to the other ~~public user identit~~Public User Identities. Figure 5.0~~b~~c shows a simple diagram of implicit registration and ~~public user identit~~Public User Identities. Figure 5.0~~c~~d shows a similar diagram when multiple ~~private user identit~~Private User Identities are involved. In order to support this function, it is required that:

- HSS has the set of ~~public user identit~~Public User Identities that are part of implicit registration.

- Cx reference point between S-CSCF and HSS shall support download of all ~~public user identit~~Public User Identities associated with the implicit registration, during registration of any of the single ~~public user identit~~Public User Identities within the set.

- All ~~public user identit~~Public User Identities of an Implicit Registration set must be associated to the same ~~private user identit~~Private User Identities. See figure 5.~~2.1.b~~0d for the detailed relationship between the public and private user entities within an Implicit Registration set.

- When one of the ~~public user identit~~Public User Identities within the set is registered, all Public user identities associated with the implicit registration set are registered at the same time.

- When one of the ~~public user identit~~Public User Identities within the set is de-registered, all ~~public user identit~~Public User Identities that have been implicitly registered are de-registered at the same time.

- Registration and de-registration always relates to a particular contact address and a particular ~~private user identit~~Private User Identity. A Public user identity that has been registered (including when implicitly registered) with different contact addresses remains registered in relation to those contact addresses that have not been de-registered.

- Public user identities belonging to an implicit registration set may point to different service profiles; or some of these ~~public user identit~~Public User Identities may point to the same service profile.

- When a ~~public user identit~~Public User Identity belongs to an implicit registration set, it cannot be registered or de-registered individually without the ~~public user identit~~Public User Identity being removed from the implicit registration list.

- All IMS related registration timers should apply to the set of implicitly registered ~~public user identit~~Public User Identities

- S-CSCF, P-CSCF and UE shall be notified of the set of ~~public user identit~~Public User Identities belonging to the implicitly registered function.   Session set up shall not be allowed for the implicitly registered ~~public user identit~~Public User Identities until the entities are updated, except for the explicitly registered ~~public user identit~~Public User Identity.

- The S-CSCF shall store during registration all the Service profiles corresponding to the ~~public user identit~~Public User Identities being registered.

- When a ~~public user identit~~Public User Identity is barred from IMS communications, only the HSS and S-CSCF shall have access to this ~~public user identit~~Public User Identity.

Figure 5.0~~b~~c: Relationship of ~~public user identit~~Public User Identities when implicitly registered

Figure 5.0~~c~~d – The relation of two shared Public User Identities (Public-ID-3 and 4) and Private User Identities

5.2.1a.1   Implicit Registration for UE without ISIM

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

- The Temporary public identity shall be used for initial registration process

- It shall be defined in HSS that if the user does not have implicit registration activated then the user shall not be allowed to register in the IMS using the Temporary ~~public user identit~~Public User Identity.

5.2.2 Registration flows

5.2.2.1 Requirements to consider for registration

The additional requirement for the registration information flow for this section is:

1. A Serving-CSCF is assigned at registration, this does not preclude additional Serving-CSCFs or change of CSCF at a later date. Procedures for use of additional CSCFs are not standardised in this release.

5.2.2.2 Assumptions

The following are considered as assumptions for the registration procedures as described in subclause 5.3.2.3:

1. IP-CAN bearer is already established for signalling and a mechanism exists for the first REGISTER message to be forwarded to the proxy.

2. The I-CSCF shall use a mechanism for determining the Serving-CSCF address based on the required capabilities. The I-CSCF obtains the name of the S-CSCF from its role as an S-CSCF selector (~~Figure 5 1~~Figure 5.1) for the determination and allocation of the Serving-CSCF during registration.

3. The decision for selecting the S-CSCF for the user in the network is made in the I-CSCF.

4. A role of the I-CSCF is the S-CSCF selection.

In the information flows described in subclauses 5.2.2.3 and 5.2.2.4, there is a mechanism to resolve a name and address. The text in the information flows indicates when the name-address resolution mechanism is utilised. These flows do not take into account security features such as user authentication. The description of the impact of IMS security features is done in [19] 33.203.

5.2.2.3 Registration information flow – User not registered

The application level registration can be initiated after the registration to the access is performed, and after IP connectivity for the signalling has been gained from the access network. For the purpose of the registration information flows, the user is considered to be always roaming. For user roaming in their home network, the home network shall perform the role of the visited network elements and the home network elements.
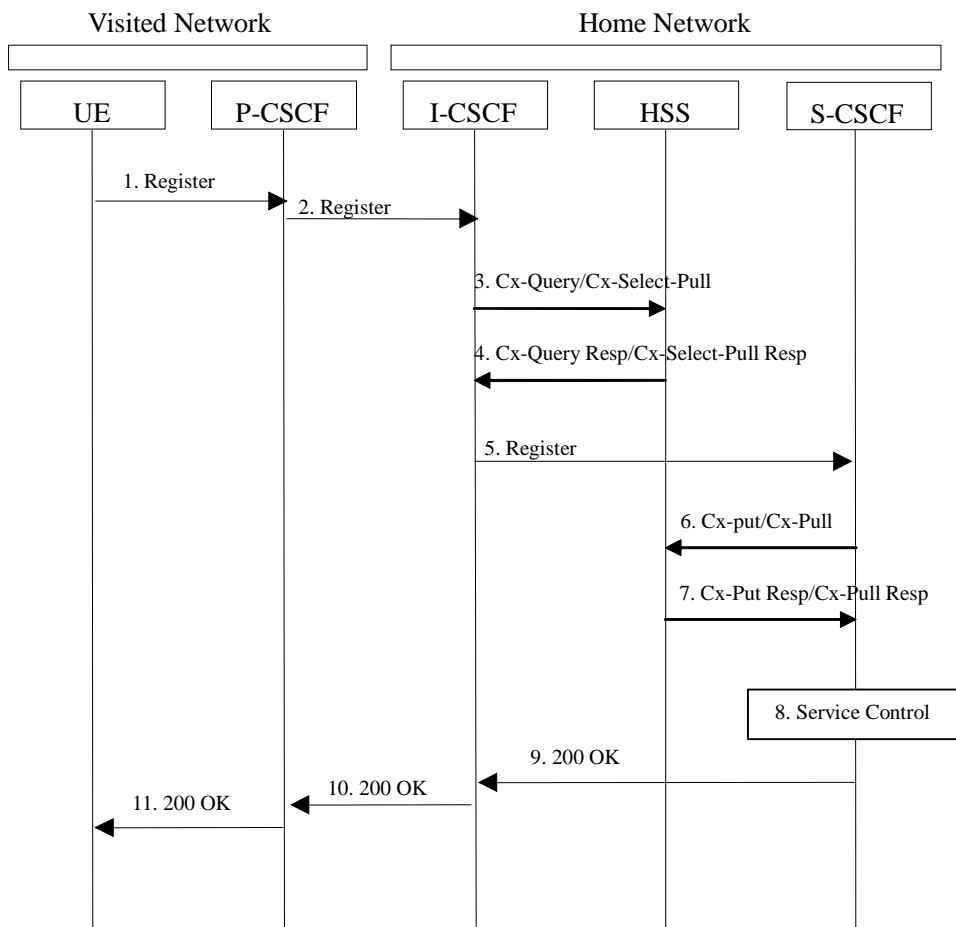
Figure 5.1: Registration – User not registered

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

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

3. The I-CSCF shall send the Cx-Query/Cx-Select-Pull information flow to the HSS (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, P-CSCF network identifier).

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

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

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

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

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

6. The S-CSCF shall send Cx-Put/Cx-Pull (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, S-CSCF name) to the HSS.

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

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

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

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

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

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

5.2.2.4 Re-Registration information flow – User currently registered

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

   Note: if the UE does not re-register, any active sessions may be deactivated.
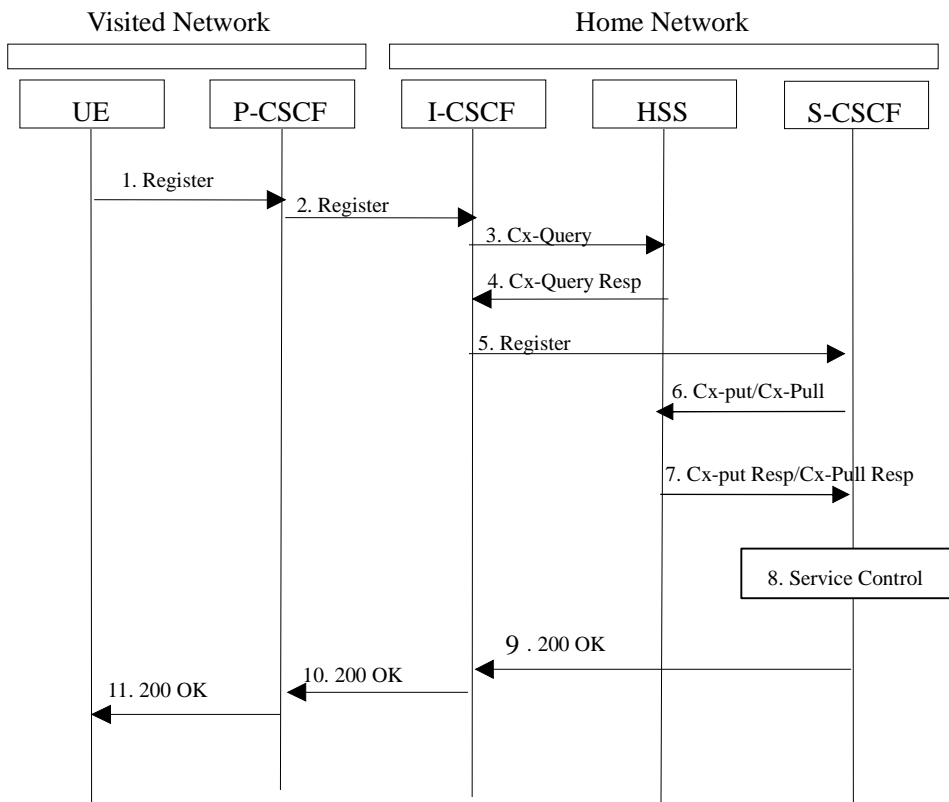
Figure 5.2: Re-registration - user currently registered

1. The UE initiates a re-registration. For periodic registration, the UE initiates a re-registration prior to expiry of the agreed registration timer. To re-register, the UE sends a new REGISTER request. The UE sends the REGISTER information flow to the proxy (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, home network domain name, UE IP address, capability information).

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

3. The I-CSCF shall send the Cx-Query information flow to the HSS (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity and P-CSCF network identifier).

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

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

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

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

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

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

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

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

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

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

5.2.2.5 Stored information.

Table 5.1 provides an indication of some of the information stored in the indicated nodes during and after the registration process. Note that Table 5.1 is not an exhaustive list of stored information, i.e. there can be additional information stored due to registration.

Table 5.1 Information Storage before, during and after the registration process

Node	Before Registration	During Registration	After Registration
UE - in local network	Credentials Home Domain Proxy Name/Address	Same as before registration	Credentials Home Domain Proxy Name/Address
Proxy-CSCF - in Home or Visited network	Routing Function	Initial Network Entry point UE Address Public and Private User IDs	Final Network Entry point UE Address Public and Private User IDs
Interrogating-CSCF - in Home network	HSS or SLF Address	Serving-CSCF address/name P-CSCF Network ID Home Network contact Information	No State Information
HSS	User Service Profile	P-CSCF Network ID	Serving-CSCF address/name\
Serving-CSCF (Home)	No state information	HSS Address/name User profile (limited – as per network scenario) Proxy address/name P-CSCF Network ID Public/Private User ID UE IP Address	May have session state Information Same as during registration

5.3 Application level de-registration procedures

5.3.1 Mobile initiated de-registration

When the UE wants to de-register from the IMS then the UE shall perform application level de-registration. De-registration is accomplished by a registration with an expiration time of zero seconds. De-registration follows the same path as defined in subclause 5.2.2.3 "Registration Information Flow – User not registered".
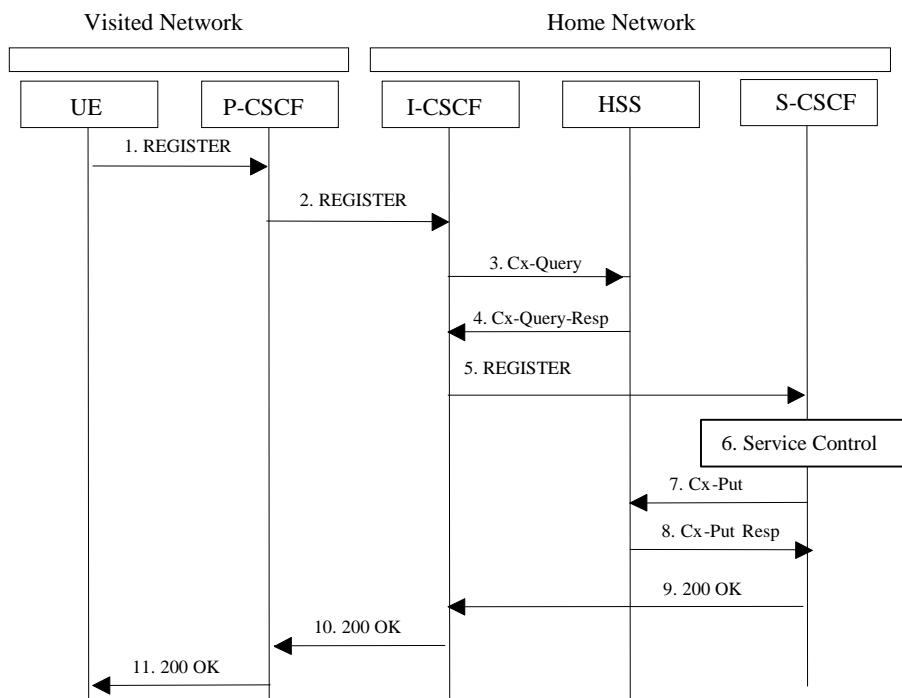

Figure 5.3: De-registration - user currently registered

1. The UE decides to initiate de-registration. To de-register, the UE sends a new REGISTER request with an expiration value of zero seconds. The UE sends the REGISTER information flow to the proxy (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, home network domain name, UE IP address).

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

3. The I-CSCF shall send the Cx-Query information flow to the HSS (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, P-CSCF network identifier).

4. The HSS shall determine that the ~~public user identit~~Public User Identity ~~user~~ is currently registered. The Cx-Query Resp (indication of entry point, e.g. S-CSCF) is sent from the HSS to the I-CSCF.

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism and then shall send the de-register information flow (P-CSCF address/name, ~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, UE IP address, I-CSCF(THIG) in case network configuration hiding is desired) to the S-CSCF.

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

7. Based on operator choice the S-CSCF can send either Cx-Put (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, clear S-CSCF name) or Cx-Put (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, keep S-CSCF name), and the ~~public user identit~~Public User Identity is no longer considered registered in the S-CSCF. In case the user has (originating – see 5.6.5, or terminating – see 5.12) services related to unregistered state, the S-CSCF sends Cx-Put (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, keep S-CSCF name) in order to keep the S-CSCF name in the HSS for these services.

   The HSS then either clears or keeps the S-CSCF name for that ~~public user identit~~Public User Identity according to the Cx-Put request. In both cases the state of the ~~public user identit~~Public User Identity is stored as unregistered in the HSS. If the S-CSCF name is kept, then the HSS shall be able to clear the serving S-CSCF name at any time.

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

9. The S-CSCF shall return the 200 OK information flow to the I-CSCF. The S-CSCF may release all registration information regarding this specific registration of the ~~public user identit~~Public User Identity after sending information flow 200 OK.

10. The I-CSCF shall send information flow 200 OK to the P-CSCF.

11. The P-CSCF shall send information flow 200 OK to the UE. The P-CSCF releases all registration information regarding this specific registration of the ~~public user identit~~Public User Identity after sending information flow 200 OK.

5.3.2 Network initiated de-registration

5.3.2.0 General

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

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

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

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

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

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

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

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

- To deal with registrations expirations.

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

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

The following flow shows a network initiated IM CN subsystem terminal application (SIP) de-registration based on a registration timeout. A timer value is provided at initial registration and is refreshed by subsequent re-registrations. The flow assumes that the timer has expired. The locations (home or visited network) of the P-CSCF and S-CSCF are not indicated as the scenario remains the same for all cases.
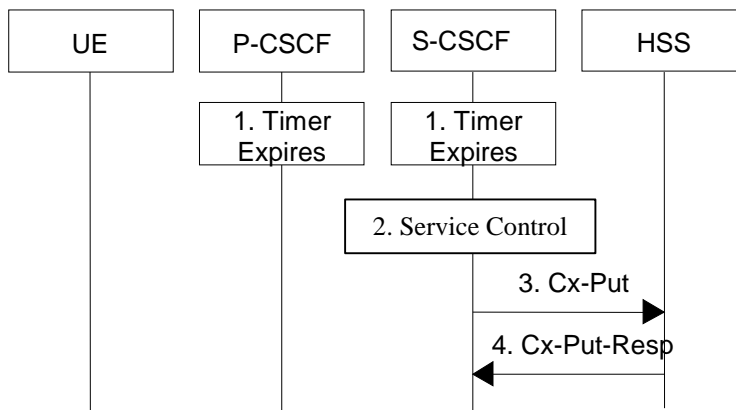
Figure 5.4: Network initiated application de-registration, registration timeout

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

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

3. Based on operator choice the S-CSCF can send either Cx-Put (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, clear S-CSCF name) or Cx-Put (~~public user identit~~Public User Identity, ~~private user identit~~Private User Identity, keep S-CSCF name), and the ~~public user identit~~Public User Identity is no longer considered registered in the S-CSCF. In case the user has (originating – see 5.6.5, or terminating – see 5.12) services related to unregistered state, the S-CSCF sends Cx-Put (~~public user identit~~Public User Identity, ~~private user identit~~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 identit~~Public User Identity according to Cx-Put the request. In both cases the state of the ~~public user identit~~Public User Identity is stored as unregistered in the HSS. If the S-CSCF name is kept, then the HSS shall be able to clear the serving S-CSCF name at any time.

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

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

5.4.3 Interworking with PSTN

The S-CSCF, possibly in conjunction with an ~~application server~~Application Server, shall determine that the session should be forwarded to the PSTN. The S-CSCF will forward the Invite information flow to the BGCF in the same network.

The BGCF selects the network in which the interworking should occur, and the selection of the interworking network is based on local policy.

If the BGCF determines that the interworking should occur in the same network, then the BGCF selects the MGCF which will perform the interworking, otherwise the BGCF forward the invite information flow to the BGCF in the selected network.

The MGCF will perform the interworking to the PSTN and control the MG for the media conversions.

The high level overview of the network initiated PSTN interworking process is shown in figure 5.6.
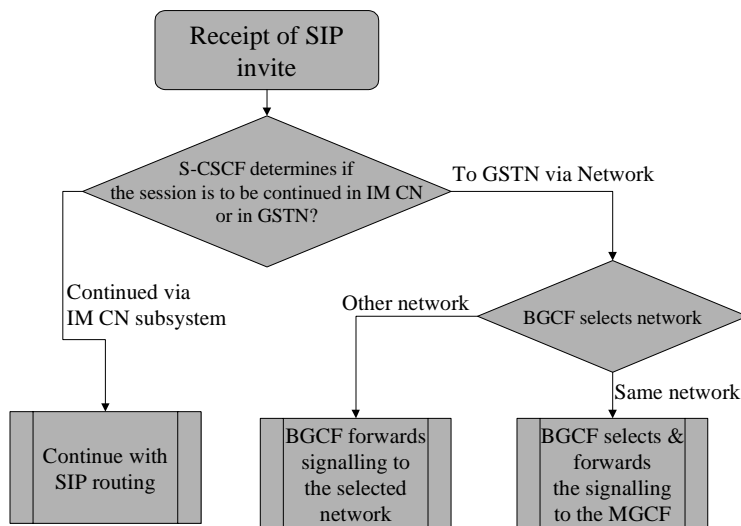

Figure 5.6: Network based PSTN interworking breakout process

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

5.4.9 Event and information distribution

5.4.9.0 General

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

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

This mechanism considers the following issues:

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

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

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

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

Figure 5.8: Providing service event related information to related endpoint

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

2. P-CSCF forwards the message request.

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

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

5. P-CSCF forwards the response.

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

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

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

## 5.4.11	Signalling Transport Interworking

A Signalling gateway function (SGW) is used to interconnect different signalling networks i.e. SCTP/IP based signalling networks and SS7 signalling networks. The signalling gateway function may be implemented as a stand alone entity or inside another entity [1]. The session flows in this specification do not show the SGW, but when interworking with PSTN/CS domain, it is assumed that there is a SGW for signalling transport conversion.

## 5.4.12	Configuration and Routing principles for Public Service Identities

### 5.4.12.0	General

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

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

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

### 5.4.12.1	PSIs on the originating side

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

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

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

### 5.4.12.2	PSIs on the terminating side

The ~~application server~~Application Server hosting the PSI may be invoked as a terminating ~~application server~~Application Server via information stored in the HSS. Such PSIs are globally routable and can be made available to users within and outside the operator domain, and can take the following form:

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

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

can be created and deleted by users using the Ut interface to the AS hosting the wildcarded range, or by the operator via O&M mechanisms.

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

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

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

The AS hosting the PSI in combination with its entry in the HSS is referred to as "PSI user".

Figure 5.~~4.12.~~9a depicts a routing example for incoming session where the session request is routed directly to the AS hosting the PSI.

Figure 5.~~4.12.~~9a Incoming session, direct route towards the AS

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

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

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

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

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

8-9. Session setup continues as per existing procedures.

Figure 5.~~4.12.~~9b depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.
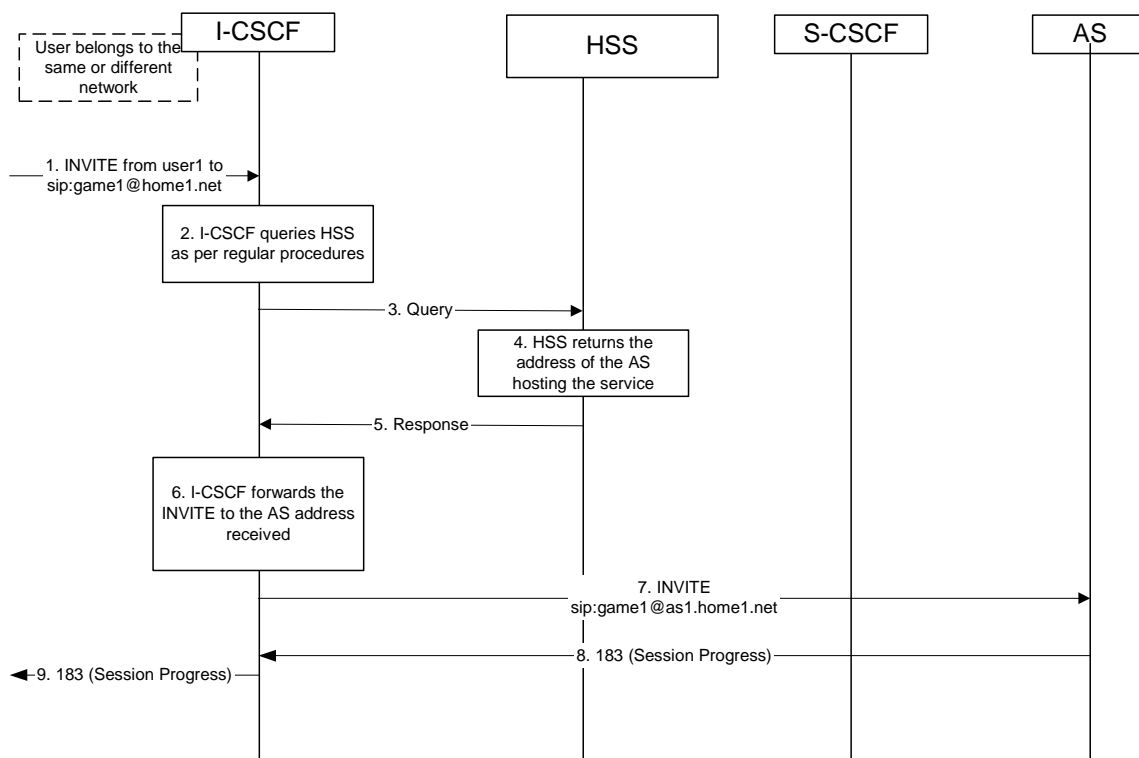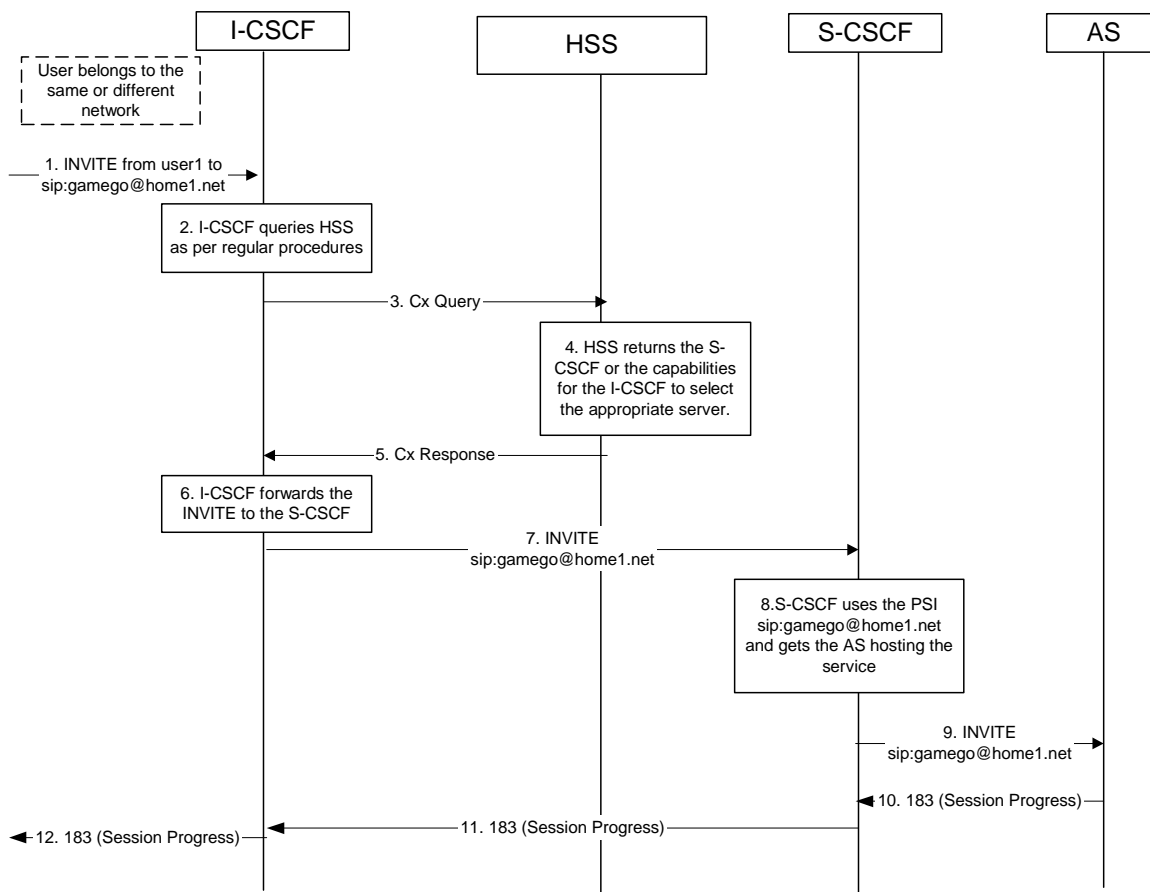
Figure 5.~~4.12.~~9b: Incoming session, indirect route to AS via S-CSCF

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

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

4. HSS determines the routing information, which is the S-CSCF defined for the"PSI user".

5. HSS returns the S-CSCF address/capabilities to the I-CSCF.

6-7.   I-CSCF, as per existing procedures, forwards the request towards the entity (i.e., S-CSCF) received from the query, or the I-CSCF selects a new S-CSCF if required.

8. S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.

9. The request is then routed towards the AS identified by the filter criteria.

10-12. Session setup continues as per existing procedures.

5.4.12.3   Subdomain based PSIs

Subdomains defined for PSIs allow both operators and users to define specific PSIs within subdomains for specific applications. For this purpose, subdomains can be defined by the operator in the DNS infrastructure. Specific PSIs within a subdomain can be created and deleted by users using the Ut interface to the AS hosting the subdomain, or by the operator via O&M mechanisms.

Subdomain based PSIs are globally routable and can be made available to users within and outside the operator domain.

In this case, there are two ways to route towards the AS hosting the PSI:

a) When the subdomain name is defined in the global DNS, then the originating S-CSCF receives the IP address of the AS hosting the PSI, when it queries DNS. The principles defined in RFC 3263 ~~"Session Initiation Protocol (SIP): Locating SIP Servers"~~ [44] may be used. For example, a NAPTR query and then a SRV query may be used to get the IP address of the AS.

b) The PSI is resolved by the global DNS to an I-CSCF address in the domain where the AS hosting the PSI is located. The I-CSCF recognises the subdomain (and thus does not query the HSS). It resolves the same PSI to the address of the actual destination AS hosting the PSI using an internal DNS mechanism, and forwards the requests directly to the AS.

Figure 5.4.12.9c shows an example of DNS based routing of an incoming session from an external network. The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.

Figure 5.4.12.9c:　Incoming session, direct route to AS using DNS

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

2. I-CSCF has been configured with the list of supported domains/network names, or it may have been configured to directly query a local DNS server.

3. In this case the I-CSCF checks the list and finds a match.

4. I-CSCF sends DNS query to find the route.

5. DNS server returns the IP address of the AS hosting the PSI.

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

8-9.　Session setup continues as per existing procedures.

5.4.12.4　PSI configuration in the HSS

In order to support configuration of an AS hosting a PSI, the distinct PSIs and/or wildcarded PSI ranges hosted in the AS need to be configured in the HSS. The configuration shall include procedures to allow:

- Distinct PSIs and wildcarded PSI ranges to be configured in the HSS via operation and maintenance procedures,

- Authorization and verification of access as "PSI user" with the Public Service Identity hosted by the AS, e.g. for AS-originating requests,

- Access to "PSI user" information (e.g. the S-CSCF assigned) over the Cx reference point from the CSCF nodes,

- Defining the "PSI user" similar to the principle of IMS user, without requiring any subscription/access information (e.g. CS/PS domain data) that are required for IMS user.

Further functional requirements such as how S-CSCF is provisioned with the PSI data need to be studied.

Note that the PSI configuration in the HSS does not affect the filter criteria based access to an AS as defined in the user profiles.

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

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.

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

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.

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

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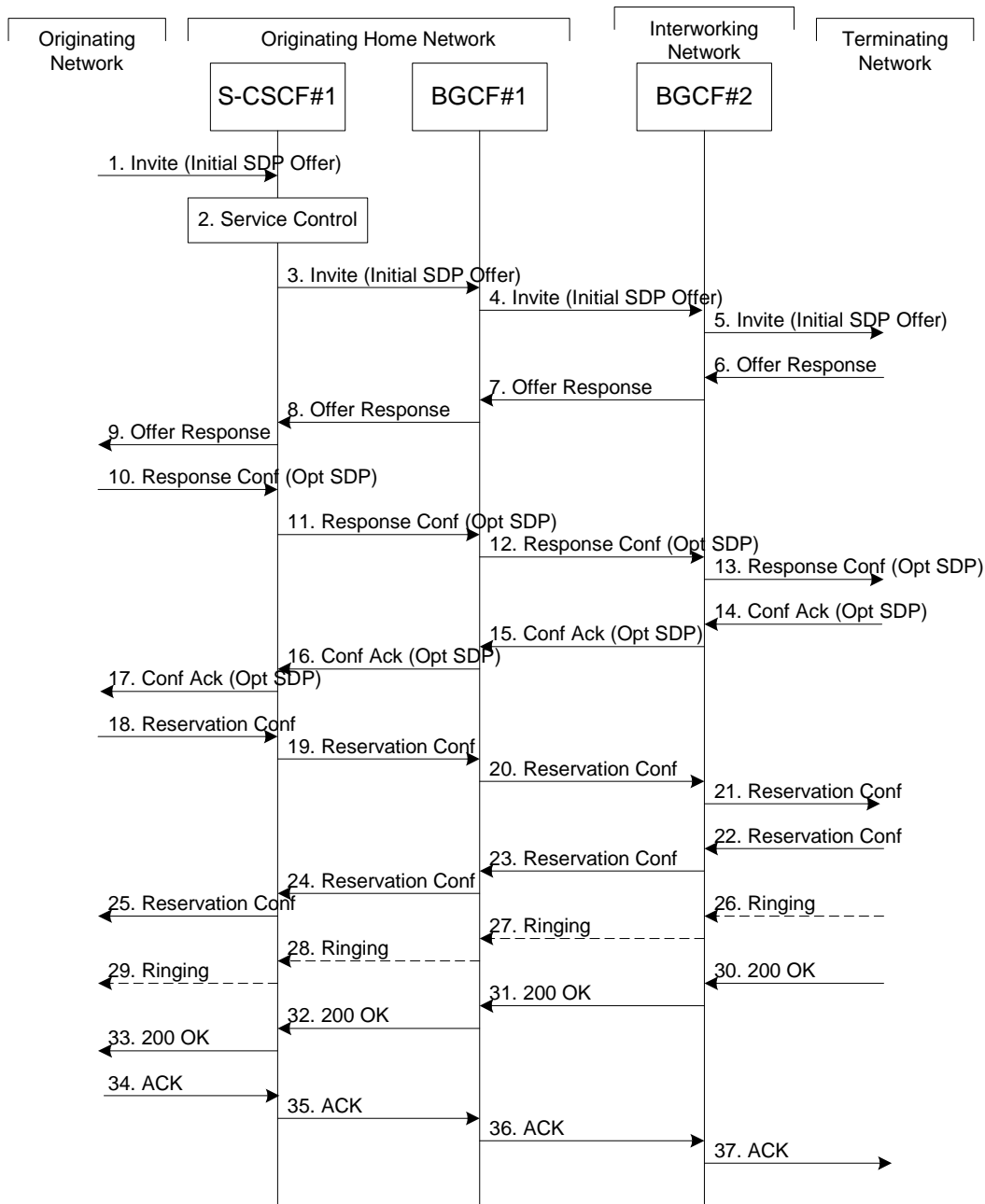
Figure 5.13: Serving to PSTN procedure - different operator

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 ~~originating end~~destination party answers the session.

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

5.6 Origination procedures

5.6.0 General

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

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

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

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

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

Sessions originated in the PSTN to a mobile destination are a special case of the Origination procedures. The MGCF uses H.248 [~~19~~18] to control a Media Gateway, and communicates with the SS7 network. The MGCF initiates the SIP request, and subsequent nodes consider the signalling as if it came from a S-CSCF.

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

5.6.5 Application Server origination

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.
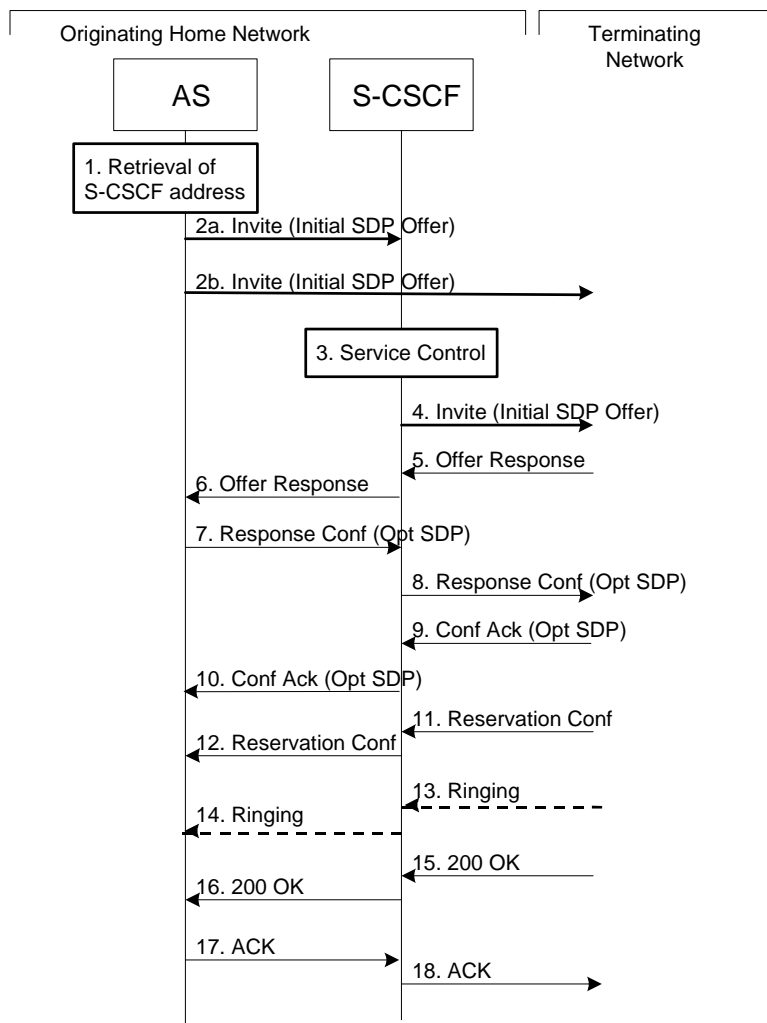

Figure 5.16d: Application Server origination procedure

Procedure for Application Server origination is as follows:

1. The Application Server acquires the address of the S-CSCF (if not available already) for the Public User Identity or the Public Service Identity on whose behalf the AS intends to originate the session. The AS may then proceed in the following way:

   - If the AS could not acquire a S-CSCF address for the Public User Identity, the AS shall not initiate a session on behalf of the user.

   - If the Public Service Identity on whose behalf the AS intends to generate the session does not have a S-CSCF address allocated, the AS sends the session initiation request directly towards the terminating network. In this case the AS may use the principles defined in RFC 3263 ~~"Session Initiation Protocol (SIP): Locating SIP Servers"~~[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 occured.

13-14. The destination UE may optionally perform alerting. If so, it signals this to the originating party by a provisional response indicating Ringing. This message is sent to the AS along the signaling path.

15-16. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating end.

17-18. The AS responds to the 200 OK with an ACK message which is passed along the signalling path to the terminating end.

******* 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.

Figure 5.19c. 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~~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~~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 by the PDF.

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 by the PDF.

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.

5.8 Procedures related to routing information interrogation

5.8.0 General

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

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

5.8.1 User identity to HSS resolution

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

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

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

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

The Dx interface provides:

- an operation to query the subscription locator from the I-CSCF or from the S-CSCF, respectively

- a response to provide the HSS name towards the I-CSCF or towards the S-CSCF, respectively.

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

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

The Dh interface provides:

- an operation to query the subscription locator from the AS

- a response to provide the HSS name towards the AS.

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

Subclause 5.8.4 presents the message flow on the Dh interface.
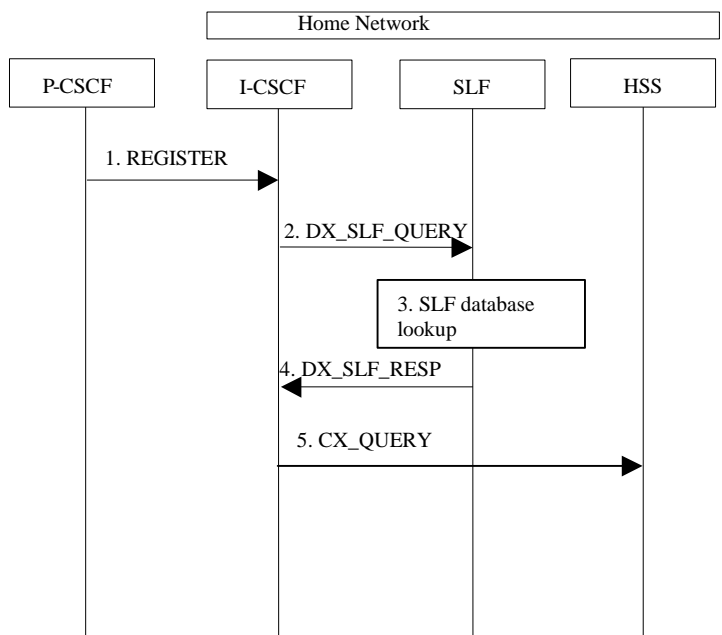
5.8.2 SLF on register

Figure 5.20: SLF on register (1st case)

1. I-CSCF receives a REGISTER request and now has to query for the location of the user's subscription data.

2. The I-CSCF sends a DX_SLF_QUERY to the SLF and includes as parameter the user identity which is stated in the REGISTER 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.

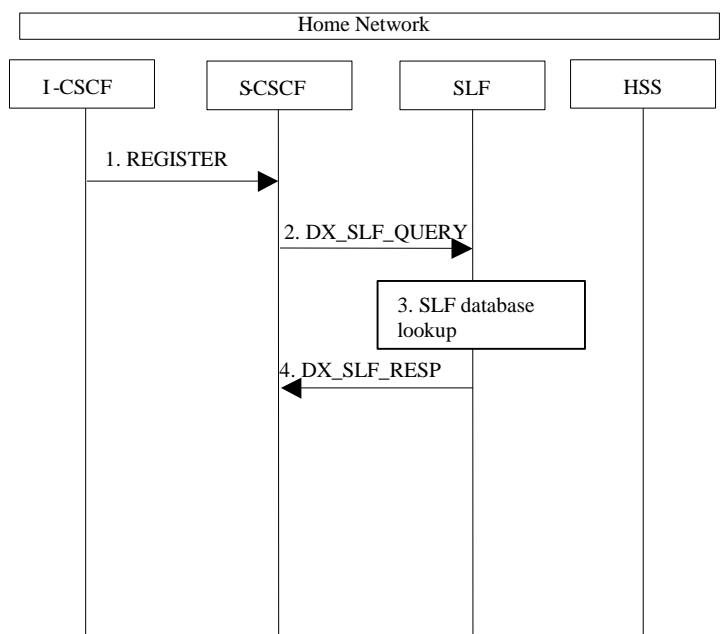5. The I-CSCF can proceed by querying the appropriate HSS.

Figure 5.20a: SLF on register (2nd case)

1. I-CSCF sends a REGISTER request to the S-CSCF. This now has to query for the location of the user's subscription data.

2. The S-CSCF sends a DX_SLF_QUERY to the SLF and includes as parameter the user identity which is stated in the REGISTER 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.
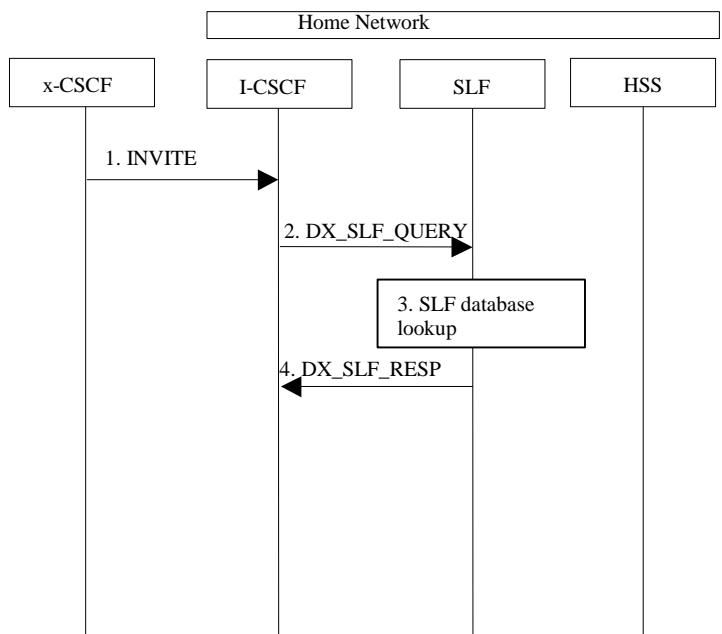
5.8.3 SLF on UE invite

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.

Figure 5.21: 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 identit~~Public User Identity.

2.　The SLF looks up its database for the queried ~~public user identit~~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.

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

5.10.2　PSTN initiated session release

The following flow shows a PSTN terminal initiated IM CN subsystem application (SIP) session release. It is assumed that the session is active and that the bearer was established to the PSTN from the Home Network (the visited network could be the Home network in this case). Furthermore, this flow assumes that service-based local policy is used.

Figure 5.23: PSTN initiated session release

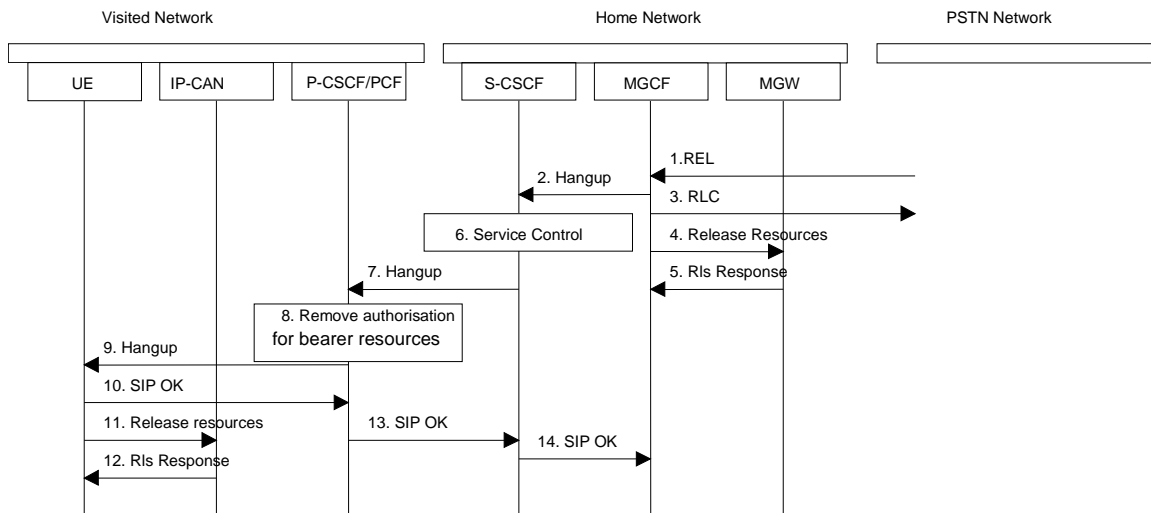1. PSTN party hangs up, which generates an ISUP REL message to the MGCF.

2. The MGCF sends a Hangup (Bye message in SIP) to the S-CSCF to notify the mobile that the far end party has disconnected.

3. Step 3 may be done in parallel with Step 2. Depending on the GSTN network type Step 3 may need to wait until after step 14. The MGCF notes the reception of the REL and acknowledges it with an RLC. This is consistent with the ISUP protocol.

4. The MGCF requests the MGW to release the vocoder and ISUP trunk using the H.248/MEGACO Transaction Request (subtract). This also results in disconnecting the two parties in the H.248 context. The IP network resources that were reserved for the message receive path to the PSTN for this session are now released. This is initiated from the MGW. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would be invoked here.

5. The MGW sends an acknowledgement to the MGCF upon completion of ~~step 6~~step 4.

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

7. The S-CSCF forwards the Hangup to the P-CSCF.

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

9. The P-CSCF forwards the Hangup to the UE.

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

11. Steps 11and 12 may be done in parallel with step 10. The UE initiates the release of the IP-CAN bearer .

12. The IP-CAN releases the IP-CAN bearer. The IP network resources that had been reserved for the message receive path to the mobile for this session are now released. This is initiated from the IP-CAN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.

13. The SIP OK message is sent to the S-CSCF.

14. The S-CSCF forwards the message to the MGCF.

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

5.11.3.1 Codec and media characteristics flow negotiation during initial session establishment

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

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

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

Once the session is established, the procedures of section 5.11.3.2 may be used by either endpoint to change to a different media characteristic (e.g. codec) that was included in the initial session description, and for which no additional resources are required for media transport. The procedures of section 5.11.3.3 may be used by either endpoint to change the session, which requires resources beyond those allocated to the existing session.

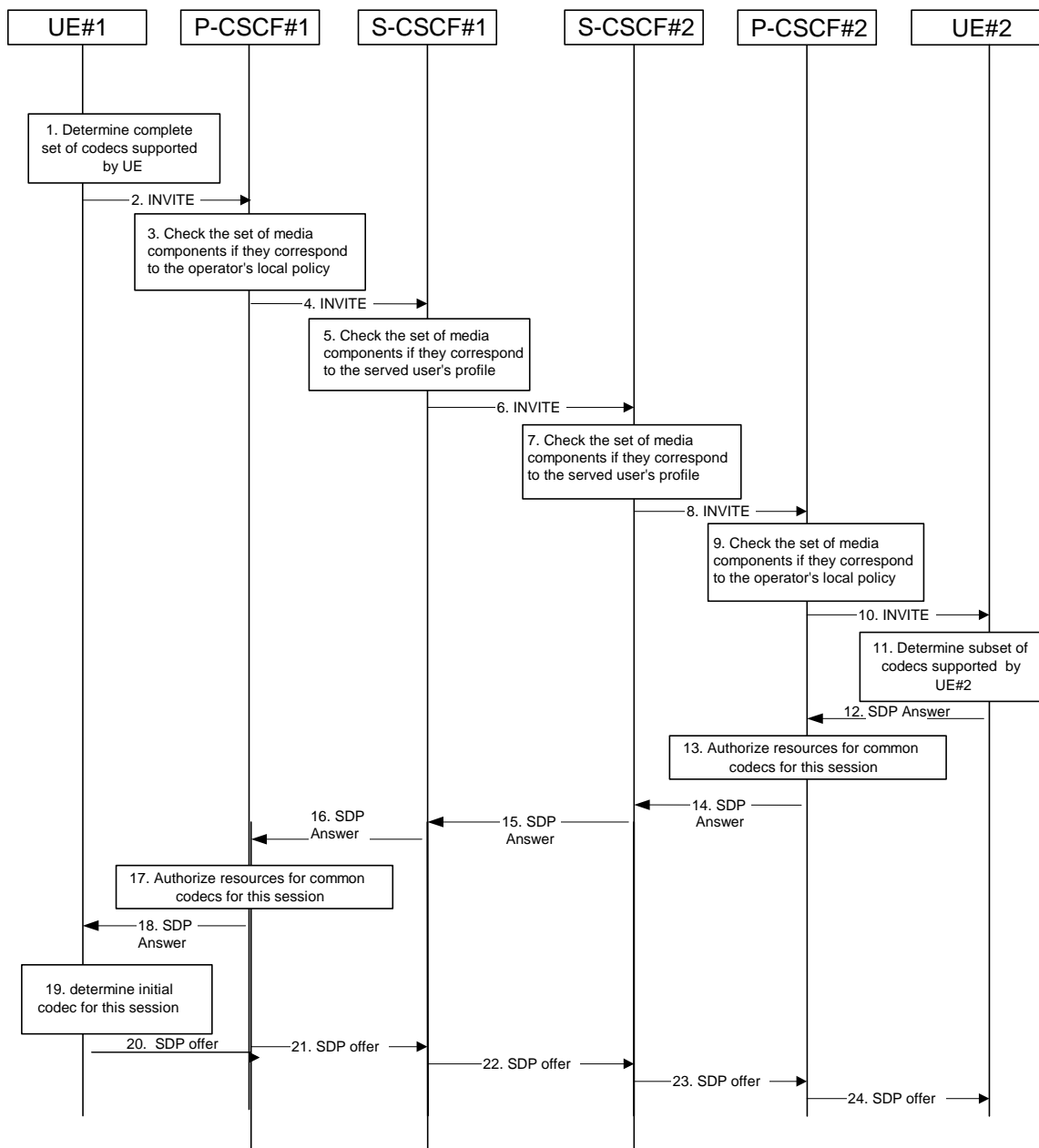The flow presented here assumes that service-based local policy is in use.

Figure 5.30: Codec negotiation during initial session establishment

The detailed procedure is as follows:

1. UE#1 inserts the codec(s) to a SDP payload. The inserted codec(s) shall reflect the UE#1's terminal capabilities and user preferences for the session capable of supporting for this 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 the initial 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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the P-CSCF#1 allows the initial session initiation attempt to continue.
The Authorisation token is generated by the PDF.

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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the S-CSCF#1 allows the initial session initiation 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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the S-CSCF#2 allows the initial session initiation attempt to continue.

8. S-CSCF#2 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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the P-CSCF#2 allows the initial session initiation attempt to continue.
    The Authorization-Token is generated by the PDF.

10. The Authorization-Token is included in the INVITE message. 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

13. P-CSCF#2 authorises the QoS resources for the remaining media flows and codec choices.

14. P-CSCF#2 forwards the SDP response to S-CSCF#2.

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. P-CSCF#1 authorises the QoS resources for the remaining media flows and codec choices.

18. The Authorization-Token is included in the SDP message. P-CSCF#1 forwards the SDP response to UE#1

19. 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 need to renegotiate the codecs by sending another offer to reduce codec to one with the UE#2.

20-24. ~~UE#2~~ UE#1 sends the "Offered SDP" message to ~~UE#1~~UE#2, along the signalling path established by the INVITE request

The remainder of the multi-media session completes identically to a single media/single codec session, if the negotiation results in a single codec per media.

5.11.3.2 Codec or media characteristics flow change within the existing reservation

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 flows. If the change is within the resources already reserved, then it is only necessary to synchronise the change with the other endpoint. Note that an admission control decision will not fail if the new resource request is within the existing reservation.

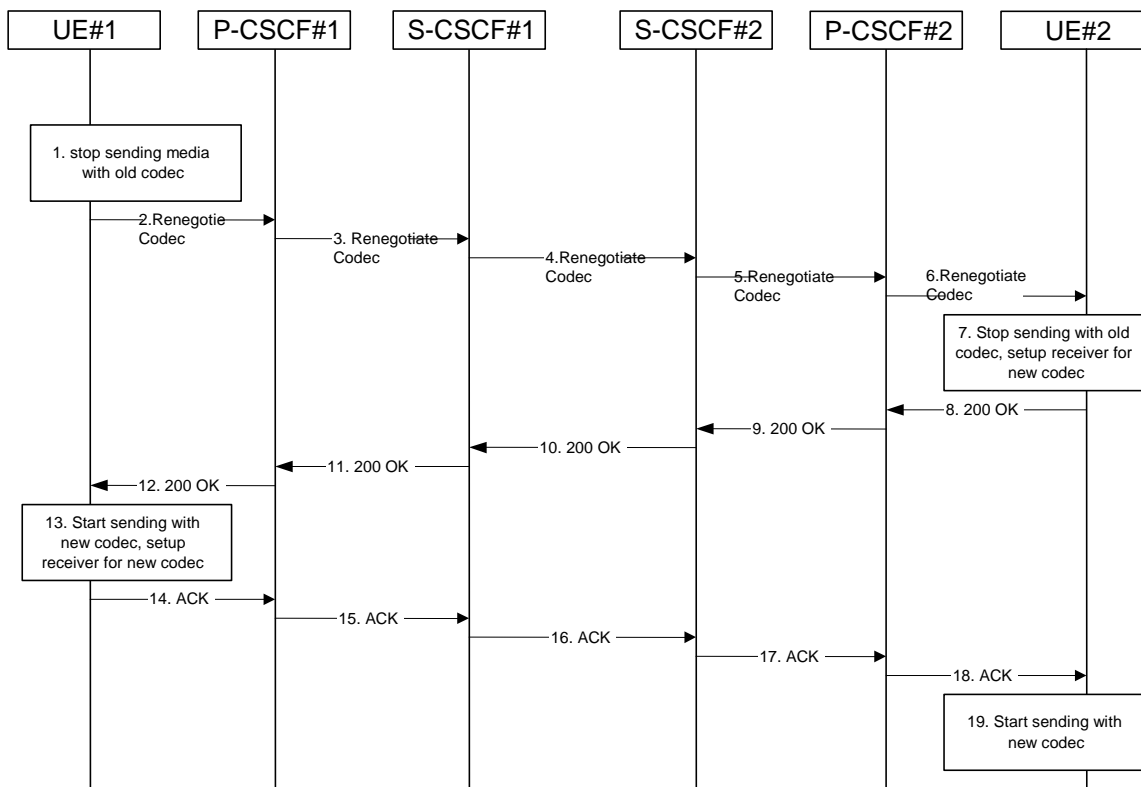The flow presented here assumes that service-based local policy is in use.

Figure 5.31: Codec or media flow change - same reservation

The detailed procedure is as follows:

1. UE#1 determines that a new media stream is desired, or that a change is needed in the codec in use for an existing media stream. UE#1 evaluates the impact of this change, and determines the existing resources reserved for the session are adequate. UE#1 builds a revised SDP that includes all the common media flows determined by the initial negotiation, but assigns a codec and port number only to those to be used onward. UE#1 stops transmitting media streams on those to be dropped from the session.

2-6. UE#1 sends an INVITE message through the signalling path to UE#2. At each step along the way, the CSCFs recognise the SDP is a proper subset of that previously authorised, and take no further action.

7. UE#2 receives the INVITE message, and agrees that it is a change within the previous resource reservation. (If not, it would respond with a SDP message, following the procedures of 5.11.3.1). UE#2 stops sending the media streams to be deleted, and initialises its media receivers for the new codec.

8-12. UE#2 forwards a 200-OK final response to the INVITE message along the signalling path back to UE#1.

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

14-18. UE#1 sends the SIP final acknowledgement, ACK, to UE#2.

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

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.

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.

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

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

19. 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. UE#1 sends the offered SDP message to UE#2, including the SDP from step #19 if needed.

25. 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.

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

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

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

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

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

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

38-~~40~~42.   UE#1 sends the SIP final acknowledgement, ACK, to UE#2 along the signalling path

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

5.11.3.4   Sample MM session flow - addition of another media

For this end-to-end session flow, we assume the originator is a UE located within the service area of the network operator to whom the UE is subscribed. The UE has already established an IM CN session and is generating an invite to add another media (e.g., video to a voice call) to the already established session. Note that the invite to add media to an existing session could be originated by either end. The invite, and subsequent flows, are assumed to follow the path determined when the initial session was established. Any I-CSCFs that were included in the initial session would be included in this session.

The originating party addresses a destination that is a subscriber of the same network operator.

The destination party is a UE located within the service area of the network operator to which it is subscribed.

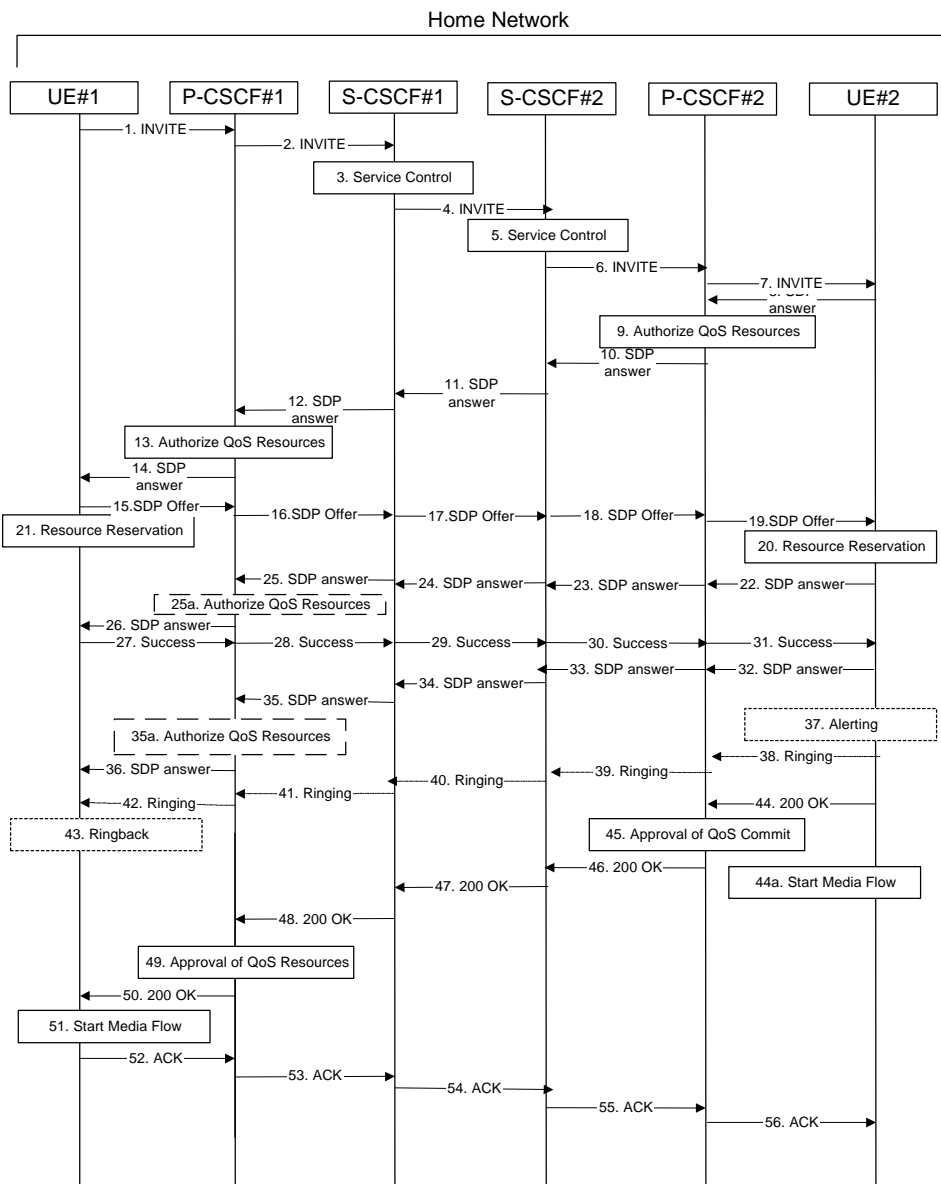The flow presented here assumes that service-based local policy is in use.

Figure 5.33: Multimedia session flow - addition of another media

Step-by-step processing of this end-to-end session flow is as follows:

1. UE#1 sends a SIP INVITE request, containing new SDP for the new media and including the original SDP, to P-CSCF#1, which was obtained from the CSCF discovery procedures.

2. P-CSCF#1 forwards the INVITE to the next hop name/address, as determined from the registration procedures. In this case the next hop is S-CSCF#1 within the same operator's network.

3. S-CSCF#1 validates the service profile, and invokes whatever service logic is appropriate for this session attempt.

4. S-CSCF#1 recognises that this invite applies to an existing session. It therefore forwards the INVITE along the existing path to S-CSCF#2.

5. S-CSCF#2 validates the service profile, and invokes whatever service logic is appropriate for this session attempt.

6. S-CSCF#2 remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to P-CSCF#2 in the home network.

7. P-CSCF#2 remembers (from the registration procedure) the address of UE#2 and forwards the INVITE to UE#2.

8. UE#2 returns the media stream capabilities of the destination to the session originator, along the signalling path established by the INVITE message.

9. P-CSCF#2 authorises the QoS resources required for this additional media.

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

11. S-CSCF#2 forwards the SDP to S-CSCF#1.

12. S-CSCF#1 forwards the SDP message to P-CSCF#1.

13. P-CSCF#1 authorises the additional resources necessary for this new media.

14. P-CSCF#1 forwards the SDP message to the originating endpoint, UE#1.

15-19. The originator decides the offered set of media streams for this media addition, and sends the offered SDP to P-CSCF#1.

20. UE#2 initiates the resource reservation procedures for the resources necessary for this additional media.

21. After determining the offered set of media streams for this additional media, step #15 above, UE#1 initiates the reservation procedures for the additional resources needed for this new media.

22-25. When UE#2 has successfully reserved the needed resources, it sends the "reservation successful" message to ~~UE#2~~UE#1 along the signaling path established by the INVITE message. The message is sent first to P-CSCF#1.

25a.   P-CSCF#1 authorises any additional media for the proposed SDP.

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

27-31. UE#1 sends the final agreed SDP to UE#2 via the established path.

32-35. UE#2 responds to the offered final media.

35a.   P-CSCF#1 authorises the media agreed.

36. The response is forwarded to UE#1.

37. UE#2 may optionally delay the session establishment in order to alert the user to the incoming additional media.

38. If UE#2 performs alerting, it sends a ringing indication to the originator via the signalling path. The message is sent first to P-CSCF#2.

39. P-CSCF#2 forwards the ringing message to S-CSCF#2.

~~40.~~ S-CSCF#2 invokes whatever service logic is appropriate for this ringing flow.

~~41~~40. S-CSCF#2 forwards the message to S-CSCF#1.

~~32.~~   41. S-CSCF#1 forwards the message to P-CSCF#1.

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

43.   UE#1 indicates to the originator that the media addition is being delayed due to alerting. Typically this involves playing a ringback sequence.

44. When the destination party accepts the additional media, UE#2 sends a SIP 200-OK final response along the signalling path back to the originator. The message is sent first to P-CSCF#2.

44a.   After sending the 200-OK, UE#2 may initiate the new media flow(s).

45. P-CSCF#2 approves the commitment of the QoS resources for this additional media.

46. P-CSCF#2 forwards the final response to S-CSCF#2.

47. S-CSCF#2 forwards the final response to S-CSCF#1.

48. S-CSCF#1 forwards the final response to P-CSCF#1.

49. P-CSCF#1 approves the commitment of the QoS resources for this additional media.

50. P-CSCF#1 forwards the final response to UE#1.

51. UE#1 starts the media flow(s) for this additional media.

52. UE#1 responds to the final response with a SIP ACK message, which is passed to the destination via the signalling path. The message is sent first to P-CSCF#1.

53. P-CSCF#1 forwards the ACK to S-CSCF#1

54. S-CSCF#1 forwards the ACK to S-CSCF#2.

55. S-CSCF#2 forwards the ACK to P-CSCF#2.

56. P-CSCF#2 forwards the ACK to UE#2.

5.11.4 Procedures for providing or blocking identity

5.11.4.0 General

Identity is composed of a ~~public user identit~~Public User Identity and an optional display name:

- The ~~public user identit~~Public User Identity is used by any user for requesting communications to other users (see section 4.3.3.2).

- The display name is the user's name if available, an indication of privacy or unavailability otherwise. The display name is a text string which may identify the subscriber, the user or the terminal.

This section gives information flows for the procedures for providing the authenticated ~~public user identit~~Public User Identity and the optional display Name information of the originating party to the terminating party. It also describes the mechanisms for blocking the display of ~~public user identit~~Public User Identity and optional display name if requested by the originating party.

5.11.4.1 Procedures for providing the authenticated identity of the originating party

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

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

In the following call flow, it is assumed that no privacy has been required by UE#1.If the ~~public user identit~~Public User Identity supplied by UE#1 in the INVITE request is incorrect, the P-CSCF may reject the request, or may overwrite with the correct URL.
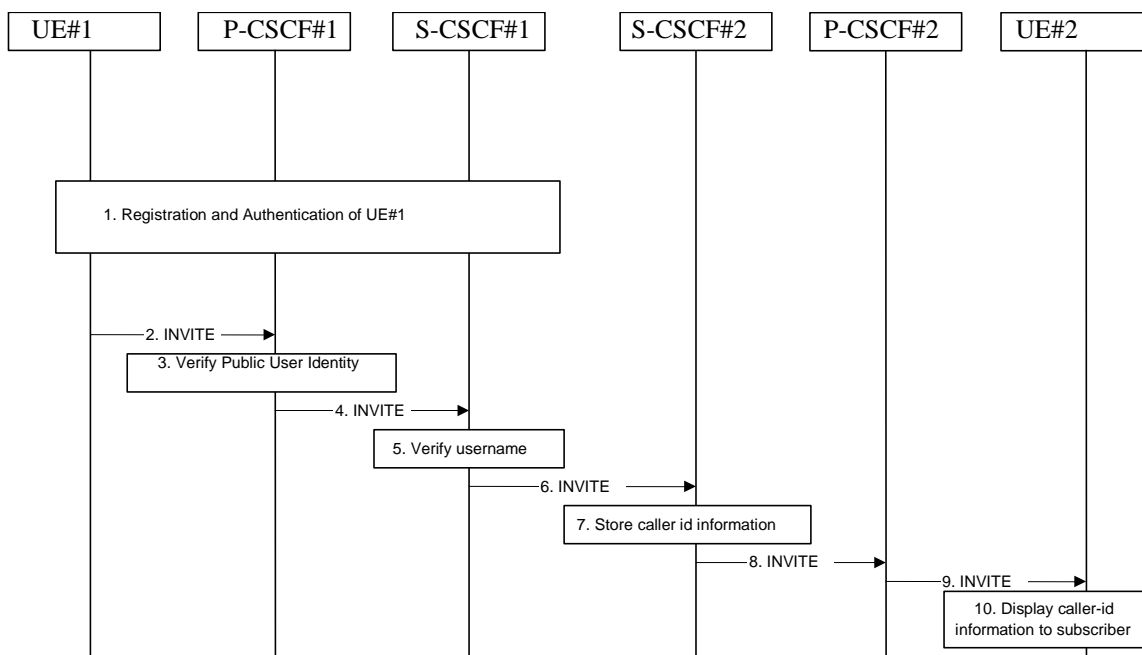
Figure 5.34: Providing the authenticated Identity of the originating party

The detailed procedure is as follows:

1. Registration and authentication of UE#1 is performed.

2. UE#1 initiates a new multi-media session, by sending an INVITE request to P-CSCF#1. This INVITE request includes a ~~public user identit~~Public User Identity, and may include a display name that may identify the specific person using the UE.

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

4. P-CSCF#1 forwards the INVITE request, with the verified ~~public user identit~~Public User Identity , to S-CSCF#1.

5. S-CSCF#1 invokes whatever service logic is appropriate for this session set up attempt to check in particular that no identity restriction is active.

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

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

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

10. UE#2 displays the ~~public user identit~~Public User Identity and the display name information (i.e. user-name if available, indication of privacy or unavailability otherwise) to the terminating party.

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 identit~~Public User Identity (i.e. 'id' privacy) .
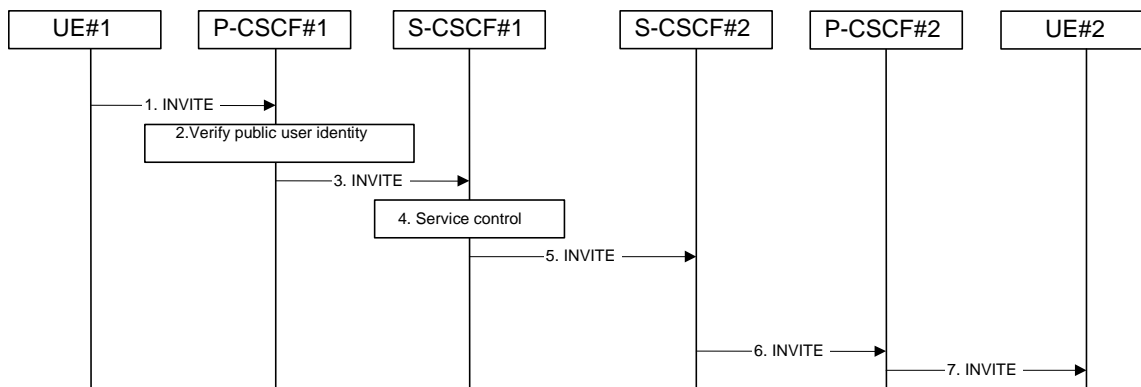
Figure 5.35: Blocking the identity of the originating party

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 identit~~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 identit~~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 identit~~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 identit~~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 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 identit~~Public User Identity from the message before forwarding the INVITE request to UE#2.

5.11.5 Session Redirection Procedures

5.11.5.0 General

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

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

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

5.11.5.1 Session Redirection initiated by S-CSCF to IMS

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

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

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

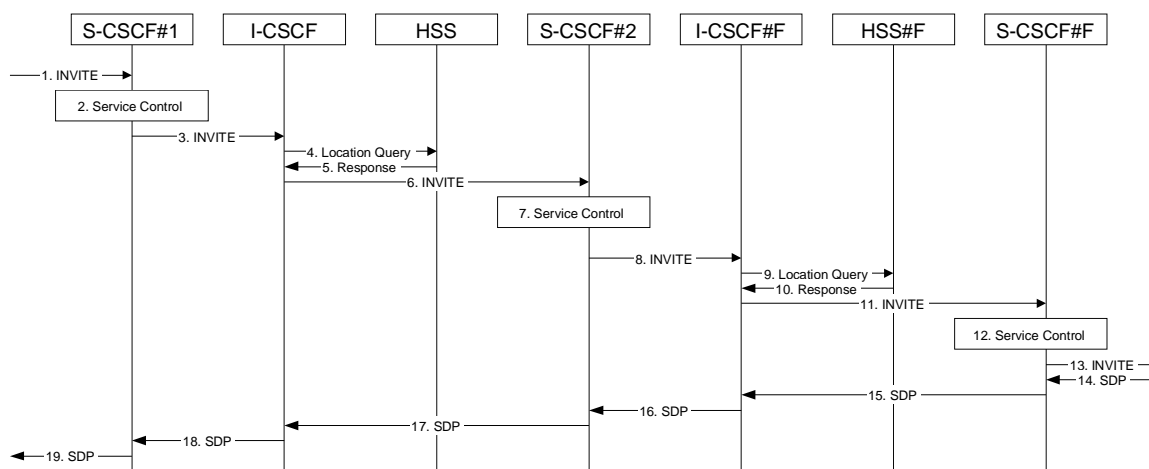This is shown in the following information flow:

Figure 5.36: Session redirection initiated by S-CSCF to IMS

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.

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 destination subscriber belongs. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a new destination URL within the IP Multimedia Subsystem. Based on operator policy and the user profile, S-CSCF#2 may restrict the media streams allowed in the redirected session.

8. S-CSCF#2 sends a SIP INVITE request to an I-CSCF (I-CSCF#F) for the network operator to whom the forwarded destination subscribes. This INVITE request may optionally go through an I-CSCF(THIG) if S-CSCF#2 is in a different operator's network than I-CSCF#F.

9. I-CSCF#F queries the HSS (HSS#F) for current location information of the destination user.

10. HSS#F responds with the address of the current Serving CSCF (S-CSCF#F) for the terminating user.

11. I-CSCF forwards the INVITE request to S-CSCF#F, who will handle the session termination.

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

13. S-CSCF#F forwards the INVITE toward the destination UE, according to the procedures of the terminating flow.

14-19. The destination UE responds with the SDP message, and the session establishment proceeds normally.

5.11.5.2 Session Redirection to PSTN Termination (S-CSCF #2 forwards INVITE)

The S-CSCF of the destination user (S-CSCF#2) may determine that the session is to be redirected to a PSTN Termination; e.g. CS-domain endpoint, or to the PSTN. For session redirection to PSTN termination where the S-CSCF of the called party (S-CSCF#2) wishes to remain in the path of SIP signalling, the S-CSCF forwards the INVITE to a BGCF. Then the BGCF (in the local network or in another network) will forward the INVITE to a MGCF, which will forward towards the destination according to the termination flow.

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

Handling of redirection to a PSTN Termination where the S-CSCF#2 forwards the INVITE is shown in the figure 5.37:
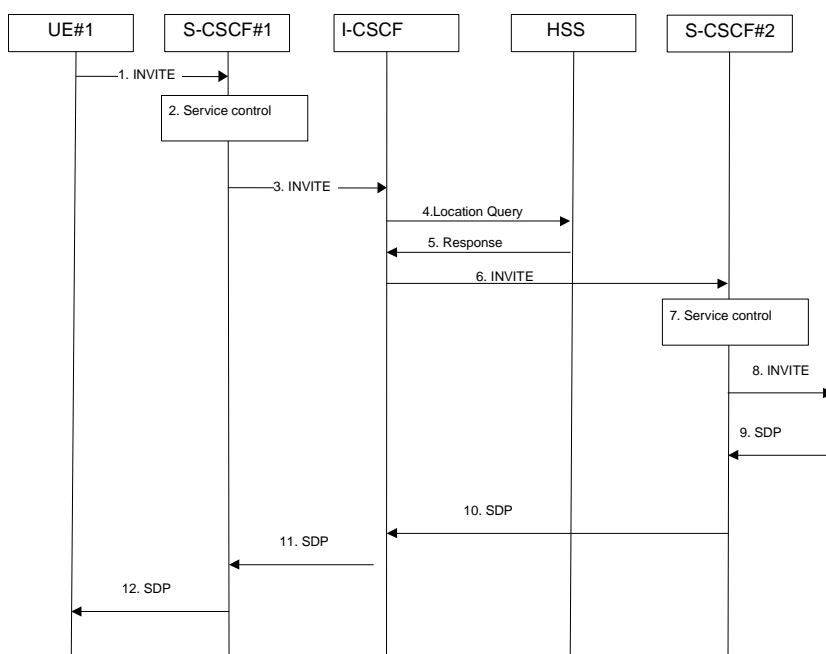

Figure 5.37: Session redirection to PSTN Termination (S-CSCF #2 forwards INVITE)

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE #1 to S-CSCF#1 by the procedures of the originating flow.

2. S-CSCF#1 performs whatever service control 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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a PSTN termination. . S-CSCF#2 determines that it wishes to remain in the path of the SIP signalling.

8. S-CSCF#2 forwards the INVITE using the Serving to Serving procedures S-S#3 or S-S#4. The PSTN terminating flows are then followed.

9-12. The destination responds with the SDP message, and the session establishment proceeds normally.

5.11.5.2a   Session Redirection to PSTN Termination (REDIRECT to originating UE#1)

The S-CSCF of the destination user (S-CSCF#2) may determine that the session is to be redirected to a PSTN Termination; e.g. CS-domain endpoint, or to the PSTN. For session redirection to PSTN termination where the S-CSCF of the called party (S-CSCF#2) wishes to use the SIP REDIRECT method, the S-CSCF#2 will pass the new destination information (the PSTN Termination information) to the originator (UE#1). The originator (UE#1) can then initiate a new session to the redirected to destination denoted by S-CSCF#2.

Handling of redirection to a PSTN Termination where the S-CSCF#2 REDIRECTS to the originating UE#1 is shown in the figure 5.37a:
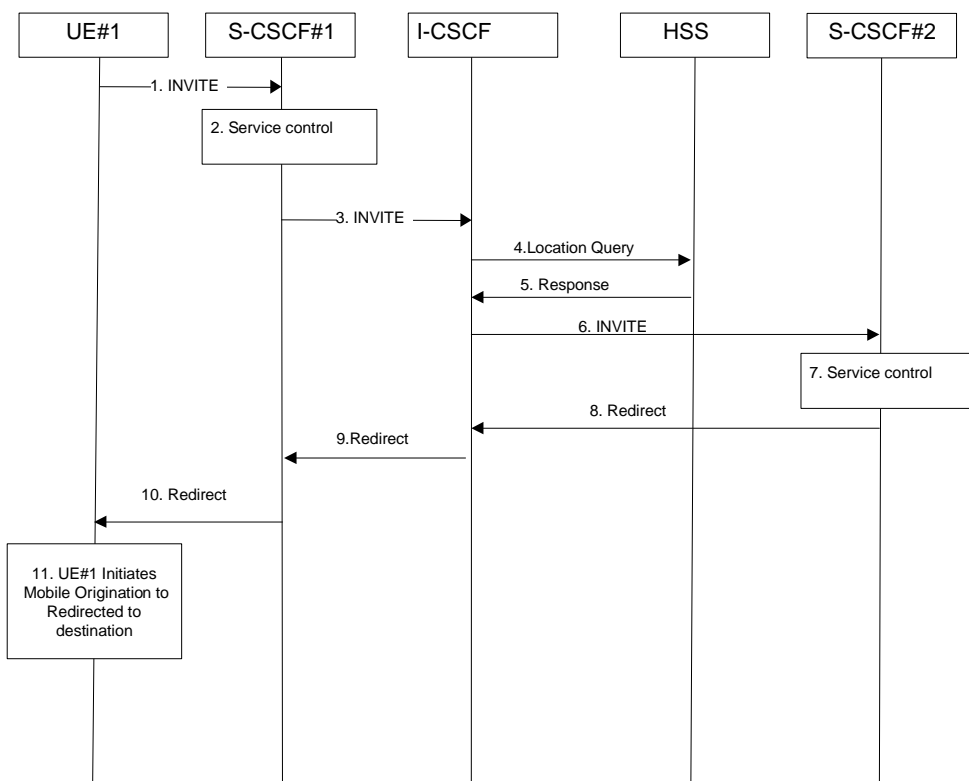

Figure 5.37a: Session redirection to PSTN Termination (REDIRECT to originating UE#1)

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE#1 to S-CSCF#1 by the procedures of the originating flow.

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. The INVITE message is sent to an I-CSCF for that operator, and may optionally go through an I-CSCF(THIG) if S-CSCF#1 is in a different operator's network than I-CSCF.

4. I-CSCF queries the HSS for current location information of the destination user.

5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.

6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a PSTN termination. S-CSCF#2 determines that it wishes to use the SIP REDIRECT method to pass the redirection destination information (the 'redirected-to PSTN Termination' information) to the originator (UE#1).

8. S-CSCF#2 sends a SIP Redirect response to I-CSCF with the redirection destination.

9. I-CSCF sends a Redirect response to S-CSCF#1, containing the redirection destination.

10. S-CSCF#2 forwards the Redirect response to UE#1, containing the redirection destination

11. UE#1 initiates a session to the 'redirected-to PSTN Termination' according to the mobile origination procedures supported in the UE (e.g. CS, IMS).

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

5.11.5.6　Session Redirection initiated by originating UE#1 after Bearer Establishment (REDIRECT to originating UE#1)

The UE of the destination user may request the session be redirected after a customer-specified ringing interval. The UE may also implement customer-specific feature processing, and base its decision to redirect this session on such things as identity of caller, current sessions in progress, other applications currently being accessed, etc. UE sends the SIP Redirect response to its P-CSCF, who forwards back along the signaling path to the originating endpoint, who initiates a session to the new destination.

The service implemented by this information flow is typically "Session Forward No Answer".

Redirect to another IMS endpoint (e.g. a sip: URL) is shown in the following information flow:

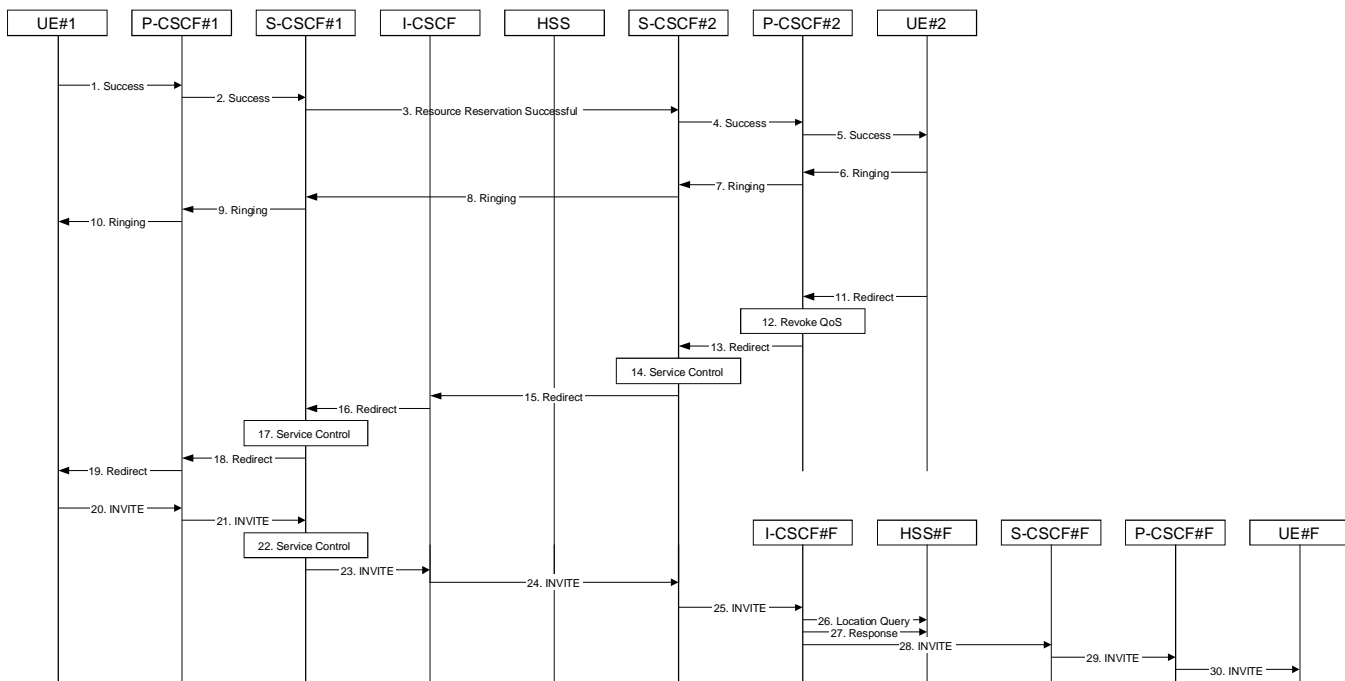The flow presented here assumes that service-based local policy is in use.

Figure 5.41: Session redirection after bearer establishment

Step-by-step processing is as follows:

1-10.   Normal handling of a basic session establishment, up through establishment of the bearer channel and alerting of the destination user or by a previous session redirection after bearer establishment procedure.

11. Based on a timeout or other indications, UE#2 decides the current session should be redirected to a new destination URL. This new destination URL may be a phone number, an email address, a web page, or anything else that can be expressed as a URL. The Redirect response is sent to P-CSCF#2.

12. P-CSCF#2 shall revoke any authorisation for QoS for the current session.

13. P-CSCF#2 forwards the Redirect response to S-CSCF#2.

14. S-CSCF#2 invokes whatever service logic is appropriate for this session redirection. If UE#2 does not subscribe to session redirection service, or did not supply a new destination URL, S-CSCF#2 may supply one or may terminate the session setup attempt with a failure response. The new destination URL may be a phone number, an email address, a web page, or anything else that can be expressed as a URL. S-CSCF#2 generates a private URL, addressed to itself, containing the new destination.

15. S-CSCF#2 sends a SIP Redirect response back to I-CSCF, containing the private URL addressed to S-CSCF#2.

16. I-CSCF sends a Redirect response back to S-CSCF#1, containing the redirection destination.

17. S-CSCF#1 checks the number of redirections that have occurred for this session setup attempt, and if excessive, aborts the session. S-CSCF#1 stores the new destination information, generates a private URL addressed to itself pointing to the stored information, and generates a modified Redirect response with the private URL.

18. S-CSCF#1 sends the modified Redirect response to P-CSCF#1

19. P-CSCF#1 shall revoke any authorisation for QoS for the current session and sends the Redirect response to UE#1.

20. UE#1 initiates a new INVITE request to the address provided in the Redirect response. The new INVITE request is sent to P-CSCF#1

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

22. S-CSCF#1 retrieves the destination information saved in step #17, and invokes whatever other service logic is appropriate for this new session setup attempt.

23. S-CSCF#1 determines the network operator of the new destination address. The INVITE message is sent to I-CSCF#2, the I-CSCF for S-CSCF#2.

24. I-CSCF forwards the INVITE to S-CSCF#2

25. S-CSCF#2 decodes the private URL, determines the network operator of the new destination, and sends the INVITE request to the I-CSCF for that network operator.

26-30. The remainder of this session completes as normal.

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

5.12.2   Mobile Terminating call procedures to unregistered Public User Identity that has no services related to unregistered state

In the example information flow the Public User Identity of the user is unregistered and the Public User Identity has no services related to unregistered state.

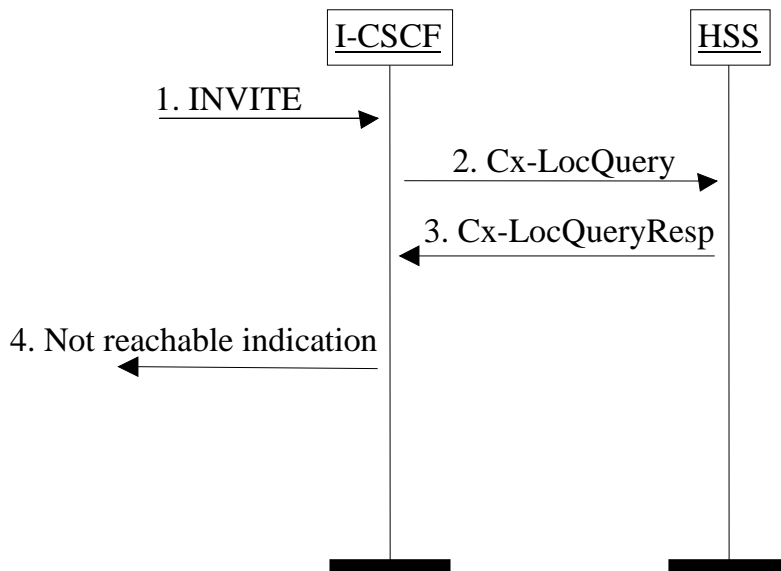This is shown in the following information flow (figure 5.44):

Figure 5.44: Mobile Terminating call procedures to unregistered Public User Identity that has no services related to unregistered state

1. I-CSCF receives an INVITE message.

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

3. HSS responds with an indication that the Public User Identity is unregistered, but no services are related to unregistered state.

4. I-CSCF responds to the origin of the request that the user is not reachable at the moment.

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

5.16.1 Immediate Messaging

5.16.1.0 General

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

5.16.1.1 Procedures to enable Immediate Messaging

5.16.1.1.0 General

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

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.~~xxx~~ 141 [37]

If the message size exceeds the size limit for MESSAGE requests, the UE shall use alternative means to deliver the content of the Immediate Message. Session based messaging specified in subclause 5.16.2 provides such means. RFC 3428[43] presents guidelines for the selection of transport mechanism for an Immediate Message. The message size limitations described above are meant to be applicable for Immediate Messages sent over end-to-end congestion safe transport, i.e. are not necessarily equal to the limitations specified for MESSAGE over congestion-unsafe transport by RFC 3428 [43].

Note:	The actual size limit is part of stage-3 design.

If the size limit for a terminating MESSAGE request is exceeded, the network may refuse the request or respond to the sender with an indication that the size of the message is too large.

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

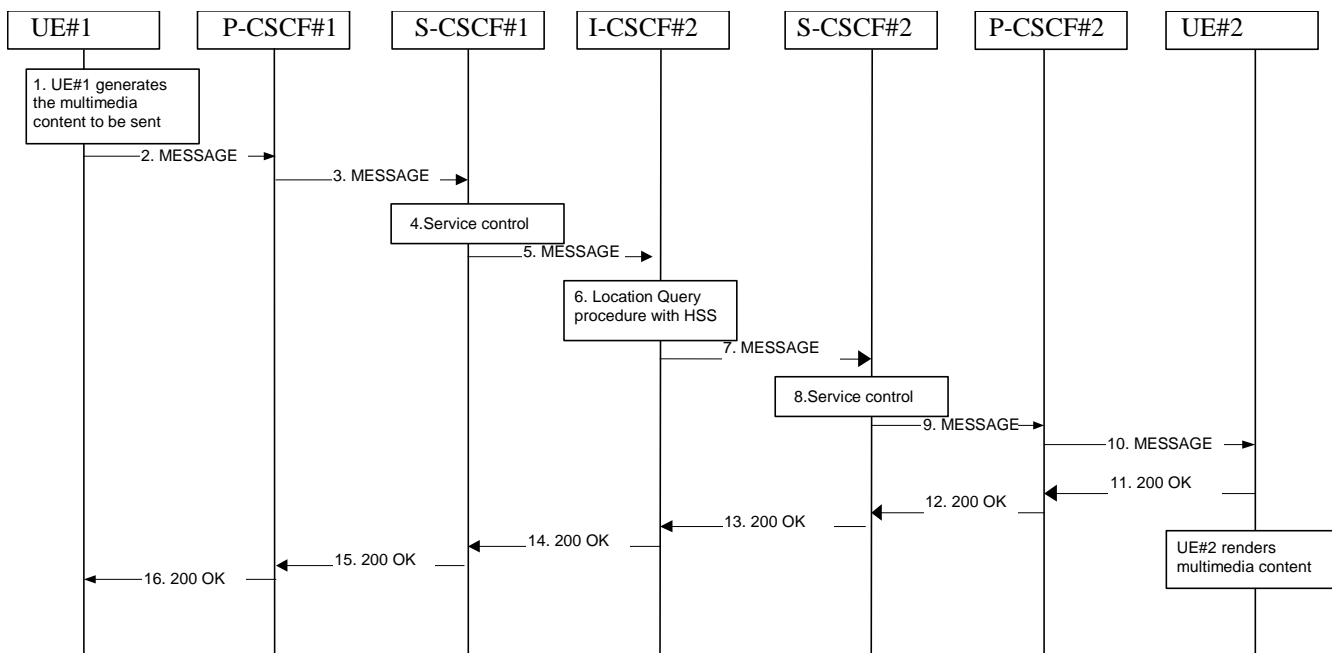### 5.16.1.1.1 Immediate messaging procedure to registered ~~public user identit~~Public User Identity

Figure 5.47: Immediate Messaging procedure to registered ~~public user identit~~Public User Identity

1. UE#1 generates the multimedia content intended to be sent to UE#2.

2. UE#1 sends the MESSAGE request to P-CSCF#1 that includes the multimedia content in the message body.

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

4. Based on operator policy S-CSCF#1 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF#1 invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an ~~application server~~Application Server, which processes the request further on.

5. S-CSC#1 forwards the MESSAGE request to I-CSCF#2.

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

7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.

8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF#2 invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an ~~application server~~Application Server, which processes the request further on.
For example, the UE#2 may have a service activated that blocks the delivery of incoming messages that fullfill criterias set by the user. The AS may then respond to the MESSAGE request with an appropriate error response.

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

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

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

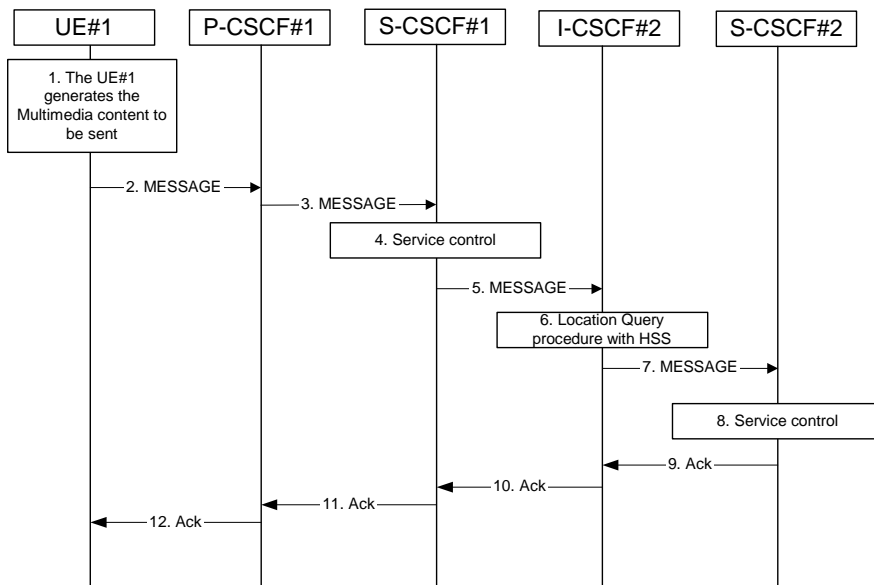### 5.16.1.1.2 Immediate messaging procedure to unregistered ~~public user identit~~Public User Identity

Figure 5.48: Immediate messaging to unregistered ~~public user identit~~Public User Identity, service control invoked

1-5. The same actions apply as for when the Public user identity is registered, see step 1-5 in clause 5.16.1.1.1.

6. I-CSCF#2 interacts with the HSS as per the terminating procedures defined for unregistered ~~public user identit~~Public User Identities in clause 5.12.1. If the ~~public user identit~~Public User Identity has no services related to unregistered state activated the interaction with HSS would be as per the procedure defined in clause 5.12.2.

7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.

8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable or the UE#2 does not have a service activated that temporarily hold the MESSAGE request in the network.

S-CSCF#2 invokes whatever service control logic appropriate for this MESSAGE request. This may include routing the MESSAGE request to an ~~application server~~Application Server, which processes the request further on.

For example, the UE#2 may have a service activated that allows delivery of any pending MESSAGE request. The AS may then hold the MESSAGE request and deliver the MESSAGE request when the UE#2 becomes reachable. In this case, depending on user settings UE#2 controls the delivery of the pending MESSAGEs.

9-12. The MESSAGE request is acknowledged with an appropriate acknowledgement response. The acknowledgement response traverses the transaction path back to UE#1.

5.16.1.2 Immediate messages with multiple recipients

IMS users shall be able to send a single immediate message to multiple recipients, as specified in 3GPP TS 22.340 [29a]. The following means are supported to achieve this:

- A PSI identifying a new group is created in the appropriate Application Server, and members are added to this group (e.g. by the user via the Ut interface or by the operator via O&M mechanisms). Immediate messages addressed to this PSI will be routed to the AS hosting the PSI, and this AS shall create and send immediate messages addressed to a group member of the group identified by the PSI.

- The user can send an immediate message by indicating the individual addresses (Public User Identities for IMS recipients) of the intended recipients as part of the immediate message. The AS of the user shall then create and send immediate messages addressed to each one of the intended recipients.

5.16.2 Session-based Messaging

5.16.2.0 General

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

5.16.2.1 Architectural principles

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

As the messaging media component usually does not require QoS beyond best-effort, use of the preconditions mechanism as defined in RFC 3312[41] is not required for session based messaging establishment that only includes a messaging media component.

NOTE: Pre-conditions mechanism may still be required for session establishment with additional media components that require the establishment of additional IP-CAN bearers.

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

The invited UE shall host the message session (accept a connection for the message session from the other endpoint). In order to host the message session the UE needs an appropriate IP-CAN bearer, on which it can accept the connection for the message media component. This IP-CAN bearer may be e.g. a general purpose bearer available prior to starting the session initiation or a dedicated bearer that is established during session establishment. Messages within a message session should be transported over a connection-oriented reliable transport protocol. Message sessions may be either established end to end between two UEs or may involve one or more intermediate nodes (e.g. a chat server for multi party chat or an ~~application server~~Application Server to perform per message charging).

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

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

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

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

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

- Support for indication of maximum message content size that a UA will accept to be received.

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

- Support for messaging-only sessions.

If charging mechanisms like charging based on the message content, message type or number of sent and/or received messages (see TS 22.340 [29a]) are required, then an intermediate node (messaging AS) shall be involved, which is able to inspect the SIP signalling as well as the exchanged messages and their content. Such an intermediate node may also provide support for time- and/or volume based charging.

5.16.2.2 Procedures to enable Session based Messaging

5.16.2.2.0 General

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

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

5.16.2.2.1 Session based messaging procedure to registered ~~public user identit~~Public User Identity

The following procedure shows the establishment of a message session between two registered UEs where the UEs are able to exchange messages end-to-end. The signaling flow is based on the general flow shown in chapter 5.7a of this specification.
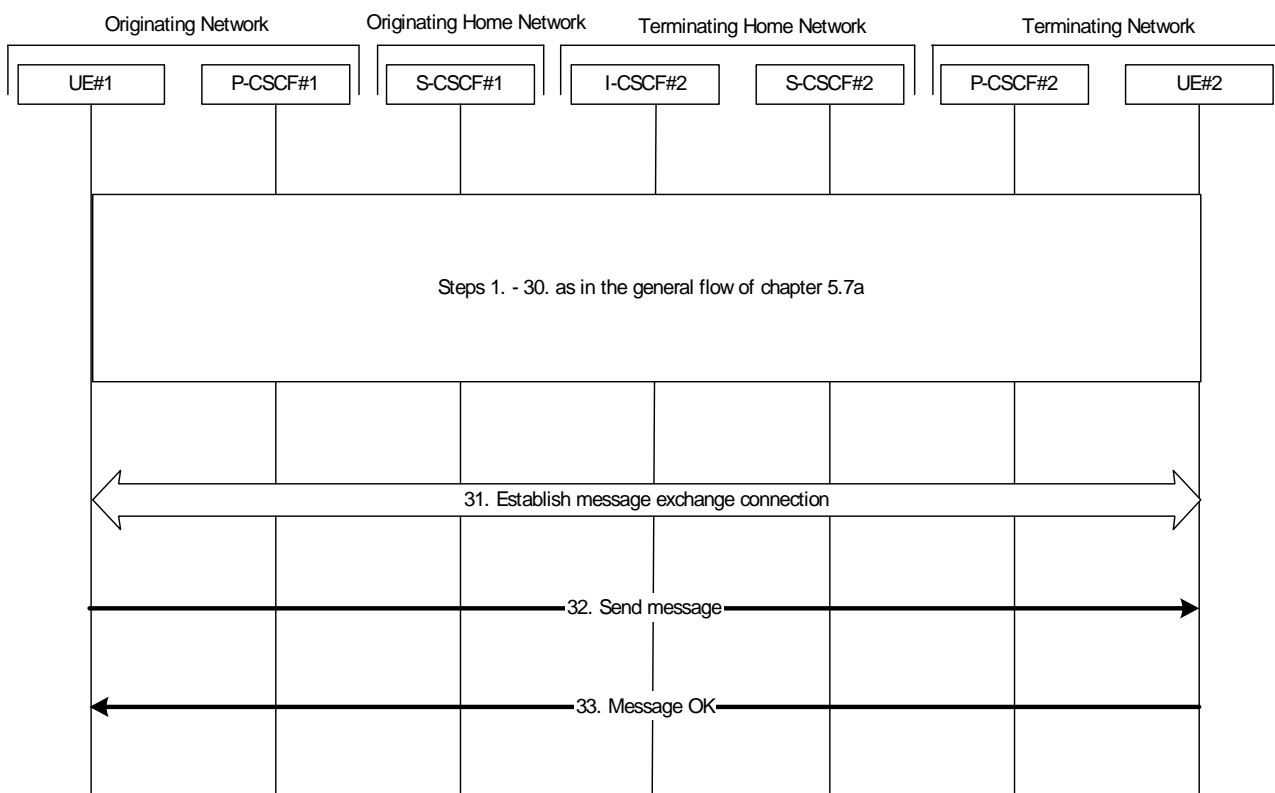
Figure 5.48a: Message session establishment

1-30.   These steps are identical to the steps 1 to 30 in the flow of chapter 5.7a. After that the message session is established. For session based messaging the SDP offer in the first INVITE request may indicate the maximum message size UE#1 accepts to receive and the 200 OK (Offer response) to the INVITE request may indicate the maximum message size UE#2 accepts to receive.

31. UE#1 establishes a reliable end-to-end connection with UE#2 to exchange the message media.

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

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

Further messages may be exchanged in either direction between UE#1 and UE#2 using the established connection. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and UE#2 respectively.

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

5.16.2.2.3 Session based messaging procedure with an intermediate node

The following procedure shows the originating session based messaging involving an intermediate node. An optional ringing response from AS to the UE or vice versa is not shown in the following procedure.
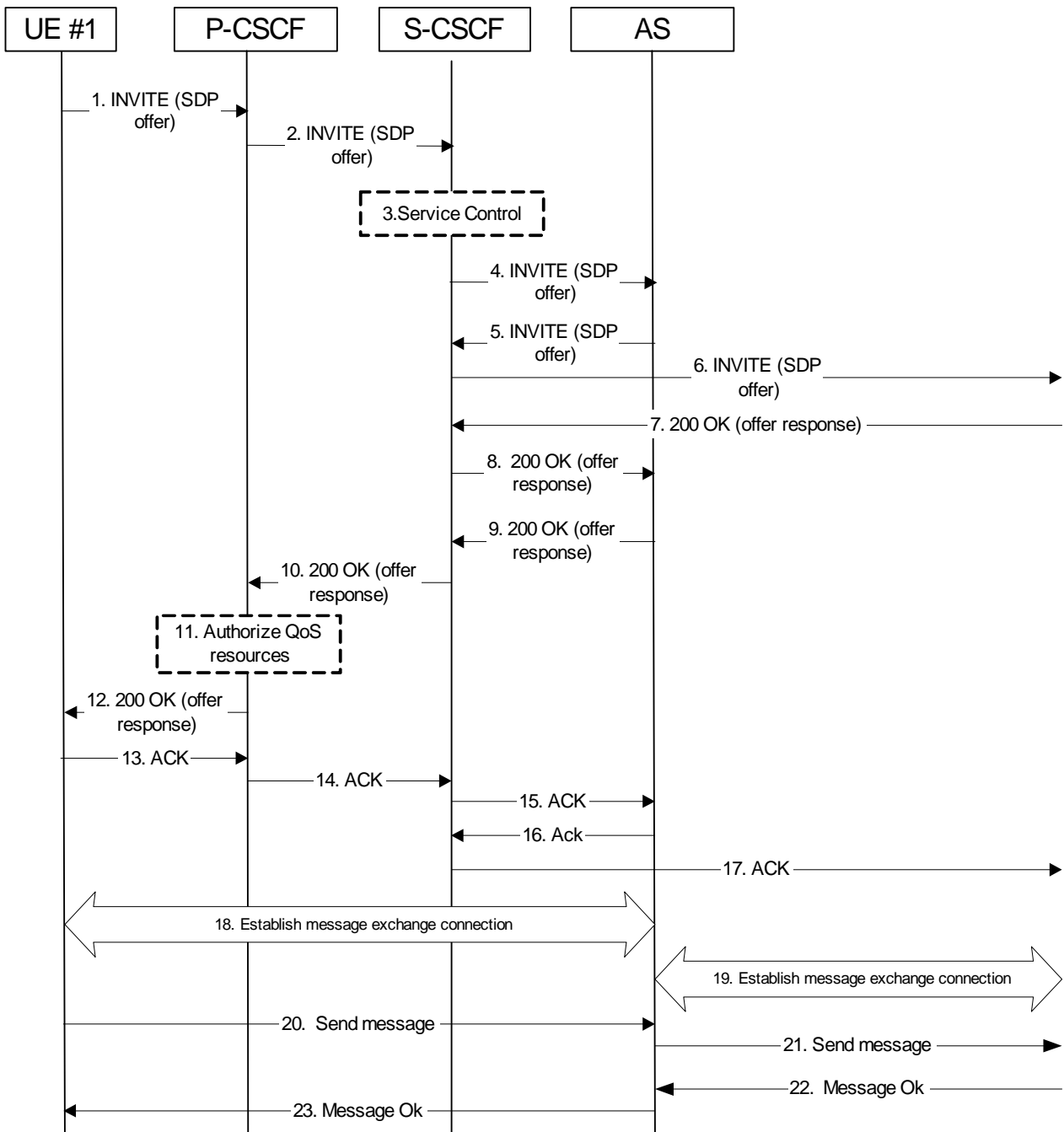
Figure 5.48c: Session based messaging with an intermediate node

1. UE#1 sends the SIP INVITE request addressed to UE#2, containing an initial SDP, to the P-CSCF. The SDP offer may indicate the maximum message size UE#1 accepts to receive.

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

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

4. The S-CSCF forwards the INVITE request to the AS. The AS may modify the content of the SDP (such as IP address/port numbers). Based on operator policy the AS may either reject the session set-up or decrease the maximum message size indication.

5. The AS sends the INVITE request to the S-CSCF.

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

7–8. The UE or AS in the terminating network accepts the INVITE request with a 200 OK response. The 200 OK response is forwarded by the S-CSCF to the AS. The 200 OK (Offer response) may indicate the maximum message size UE#2 accepts to receive, possibly decreased by the AS.

9, 10 and 12. The AS accepts the message session with a 200 OK response. The 200 OK response traverses back to UE#1.

11. Based on operator policy P-CSCF/PDF may authorize the resources necessary for this session. The media authorization token is generated by the PDF and sent in the 200 OK to UE#1.

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

16. - 17. The AS acknowledges the 200 OK response from the terminating network with an ACK, which traverses back to the UE or AS in the terminating network via the S-CSCF. Based on AS implementation sending of the ACK may happen sometimes after step 8.

18. UE#1 establishes a reliable end-to-end connection with the AS to exchange the message media.

19. The AS establishes a reliable end-to-end connection with the UE or AS in the terminating network to exchange the message media.

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

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

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

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

Further messages may be exchanged in either direction between UE#1 and the terminating network using the established message connection via the AS. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and UE#2 respectively, possibly decreased by the AS.

******* End of Changes *******

CR-Form-v7

CHANGE REQUEST

⌘   **23.228** CR **458**   ⌘ **rev** **1** ⌘   Current version: **6.7.0** ⌘

*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: ⌘	Removal of support for local services	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	IMS2	***Date:*** ⌘ 15/11/2004
Category: ⌘	**F**	***Release:*** ⌘ Rel-6

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

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

Reason for change: ⌘	Support for local services has been removed from Release 6. The text in 23.228 should be returned to that of Release 5. The text related to PSI use needs to be retained however.
Summary of change: ⌘	Replace the new text on local services with Release 5 text. Move the PSI related text to the section on PSIs.
Consequences if not approved: ⌘	Confusion over whether or not the feature is supported.

Clauses affected: ⌘	4.2.2, 4.3.6

	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 ******

4.2.2 ~~Support of Local Services in the IMS~~Void

~~Visited network provided services offer an opportunity for revenue generation by allowing access to services of a local nature to visiting users (inbound roamers). There shall be a standardised means to access local services. The mechanism to access local services shall be the same for home users and inbound roamers.~~

~~A local service may be identified by a globally routable public service identity (PSI); see subclause 4.3.6 for the definition of a PSI. In this case the routing principles in subclause 5.4.12 apply.~~

~~However, in some cases it is necessary to identify a local service by an identifier, which is not globally routable, e.g. using a local addressing plan. In this case access to local services shall be provided in the following manner:~~

~~1. It shall be possible for the HPLMN to determine whether the roaming user is requesting a local service, or is "dialing" an address according to the local addressing plan. This shall be based upon an indication received from the UE. The same indication shall be used to access local services as well as to use the local addressing plan. This indication shall be included in the Request URI of the SIP Invite.~~

~~2. The P-CSCF shall route the session towards the S-CSCF as per the session origination procedures.~~

~~3. Processing the SIP URI (e.g. address analysis and potential modification such as translation into globally routable format, e.g. a globally routable PSI) shall be performed by an Application Server in the subscriber's Home Network. The S-CSCF routes the session towards this Home Network Application Server based upon filter criteria which are triggered by the 'local indication' received from the UE. If required, the AS may need to identify the VPLMN, e.g. from information in SIP signalling or via the Sh interface.~~

~~4. The AS passes the session request back to the S-CSCF and the S-CSCF routes the session, via normal IMS routing principles, towards its destination (e.g. a server in the VPLMN identified by a PSI). Note that the ISC interface is not used as an inter-operator interface.~~

~~There shall be a standardised mechanism for the UE that is registered in the IM Subsystem, to receive and/or retrieve information about the available local services. It shall be possible to advertise local services to a registered UE independent of whether the UE has an active SIP session. Local services may be presented e.g. by directing the user to a web page.~~

~~Note: For users who have roamed, services relevant to the locality of the user may also be provided by the home network.~~

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

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 URL as defined in RFC 3261 [12] and RFC 2396 [13] or the "tel:"-URL format as defined in RFC 2806 [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.

The IM CN Subsystem shall provide capability of routing IMS messages using Public Service Identity.

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **452** | ⌘ **rev** | **3** | ⌘ | Current version: | **6.7.0** | ⌘ |

*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: ⌘	Addition of Application Server termination section	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	IMS2	***Date:*** ⌘ 15/11/2004

Category: ⌘ **F**	***Release:*** ⌘ Rel-6
Use one of the following categories: **F** *(correction)* **A** *(corresponds to a correction in an earlier release)* **B** *(addition of feature),* **C** *(functional modification of feature)* **D** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.	*Use one of the following releases:* 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 scenario in which a session targeted to a end user is terminated by an application server based on service logic instead of allowing it to continue to the end user is incorrectly handled in TS 23.228. While it is generally understood that such a scenario should be allowed, the existing error in the handling of this case in this stage 2 document implies this case will fail. This description should be corrected to complete the description of possible terminating scenarios.
Summary of change: ⌘	A new clause is added to describe the scenario in which a session is terminated by an Application Server based on service logic instead of allowing the session to continue to the targeted end user.
Consequences if not approved: ⌘	Not including this scenario erroneously implies that such a scenario is not allowed.

Clauses affected: ⌘	5.6.5, Add new subclause 5.7.8.

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

Other comments: ⌘	The proposed sub-clause and figure numbering has dependencies on CR461.

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.

PROPOSED CHANGE

5.6.5 (AS-O) Origination at Application Server ~~origination~~

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.~~16d~~16c: Application Server origination procedure

Procedure for Application Server origination is as follows:

1. The Application Server acquires the address of the S-CSCF (if not available already) for the Public User Identity or the Public Service Identity on whose behalf the AS intends to originate the session. The AS may then proceed in the following way:

   - If the AS could not acquire a S-CSCF address for the Public User Identity, the AS shall not initiate a session on behalf of the user.

- If the Public Service Identity on whose behalf the AS intends to generate the session does not have a S-CSCF address allocated, the AS sends the session initiation request directly towards the terminating network. In this case the AS may use the principles defined in RFC 3263 "Session Initiation Protocol (SIP): Locating SIP Servers" (see step 2b) to route the session initiation request.

- If the AS has acquired a S-CSCF address for the Public Service Identity or the Public User Identity, the AS sends the session initiation request to the S-CSCF (see step 2a).

2a. The AS sends the SIP INVITE request, containing an initial SDP, to the S-CSCF.
    The initial SDP may represent one or more media for a multi-media session.

2b. The AS sends the SIP INVITE request, containing an initial SDP, to the terminating network.

   The subsequent steps assume that the session initiation procedure involves the S-CSCF, i.e. they show the continuation of step 2a.

3. S-CSCF identifies the incoming request as an originating request, and invokes any origination service logic required for this Public User Identity / Public Service Identity. The S-CSCF handles the incoming request as an authenticated and authorized request, as it was originated by a trusted entity within the network.

4. S-CSCF forwards the request, as specified by the S-S procedures.

5-6.   The media stream capabilities of the destination are returned along the signalling path.

7-8.   The AS decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation along the signaling path towards the destination network. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response or a subset. The AS is free to continue to offer new media on this operation or on subsequent exchanges using the Update method.

9-10.   The terminating end point responds to the originating end with an acknowledgement, which is forwarded along the session signaling path. If Optional SDP is contained in the Response Confirmation, the Confirmation Acknowledge will also contain an SDP response.

11-12. The terminating endpoint responds to the originating end when successful resource reservation has occured.

13-14. The destination UE may optionally perform alerting. If so, it signals this to the originating party by a provisional response indicating Ringing. This message is sent to the AS along the signaling path.

15-16. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating end.

17-18. The AS responds to the 200 OK with an ACK message which is passed along the signalling path to the terminating end.

PROPOSED CHANGE

5.7.8   (AST#4) Termination at Application Server based on service logic

This termination procedure applies to an Application Server that terminates a session. In this case the addressed user is a UE and is not hosted by the AS. Based on the invoked service logic at the Application Server the session is terminated at the AS.

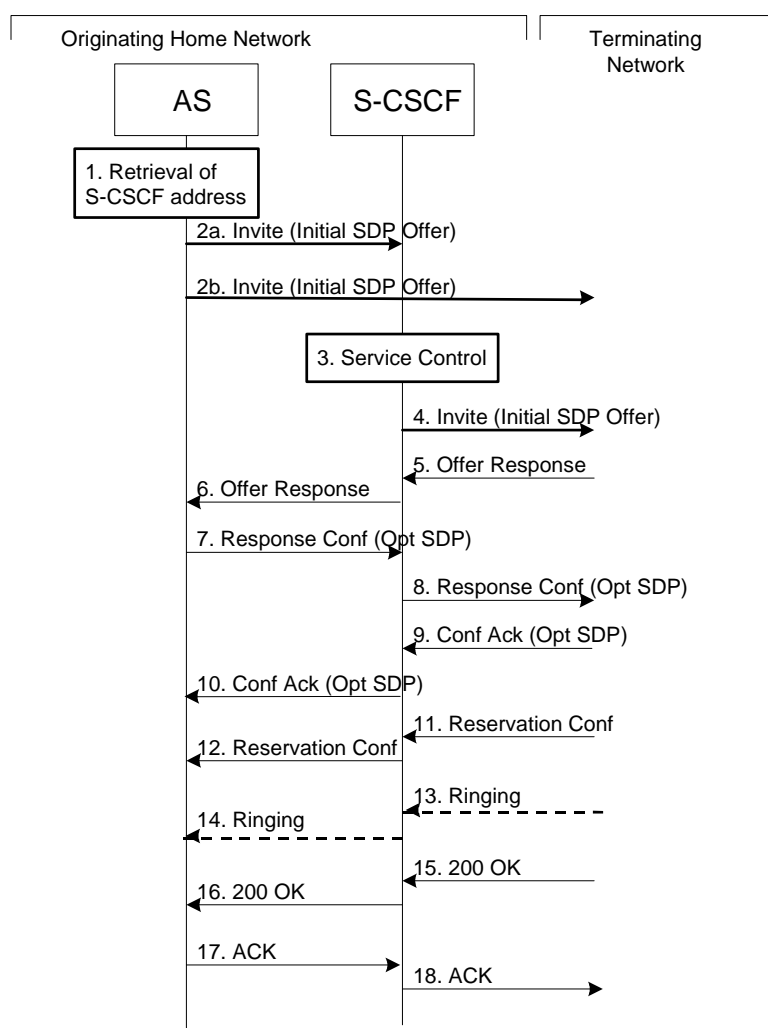The procedure described below assumes that the Application Server takes care of the user plane connection.

Figure 5.19g: Application Server termination

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

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

4. HSS determines the routing information, which is the S-CSCF defined for the user.

5. HSS returns the S-CSCF address/capabilities to the I-CSCF.

6-7. I-CSCF, as per existing procedures, forwards the request to S-CSCF that will handle the session termination.

8. S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.

9. The request is then routed towards the AS identified by the filter criteria. The AS terminates the session instead of allowing it to continue on to the address end user.

10-12. Session setup continues as per existing procedures.

CR-Form-v7

CHANGE REQUEST

⌘   **23.228** CR **462**   ⌘**rev** **1** ⌘   Current version: **6.7.0** ⌘

*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:	⌘	Changes for commonality in regards to token generation
Source:	⌘	Lucent Technologies
Work item code:⌘		IMSCOOP ***Date:*** ⌘ 15/11/2004

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 <u>TR 21.900</u>.

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)

Reason for change:	⌘	Support for commonality of IMS across different access networks indicates that the specifics of Service Based Local Policy should be described in the SBLP documents. The specific procedures for token generation are covered in other documents such as TS 23.207 and are not needed in 23.228.
Summary of change:⌘		Details regarding the specific entity responsible for token generation are removed.
Consequences if not approved:	⌘	The core IMS specifications at Stage-2 contains material that is not common across access networks.

Clauses affected:	⌘	5.6.1, 5.6.2, 5.7.1, 5.7.2, 5.7a, 5.11.3.1, 5.16.2.2.2, 5.16.2.2.3

	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.

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

5.6.1 (MO#1) Mobile origination, roaming

This origination procedure applies to roaming users.

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

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

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

Figure 5.14: Mobile origination procedure - roaming

Procedure MO#1 is as follows:

1. UE sends the SIP INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session.

2. The Authorization-Token is generated ~~by the PDF~~at this step and stored in the P-CSCF. P-CSCF remembers (from the registration procedure) the next hop CSCF for this UE.

This next hop is either the S-CSCF that is serving the visiting UE (choice (a)), or an I-CSCF(THIG) within the home network that is performing the configuration hiding function for the home network operator (choice (b)).

(2a) If the home network operator does not desire to keep their network configuration hidden, the name/address of the S-CSCF was provided during registration, and the INVITE request is forwarded directly to the S-CSCF.

(2b) If the home network operator desires to keep their network configuration hidden, the name/address of an I-CSCF(THIG) in the home network was provided during registration, and the INVITE request is forwarded through this I-CSCF(THIG) to the S-CSCF.

    (2b1) P-CSCF forwards the INVITE request to I-CSCF(THIG)

    (2b2) I-CSCF(THIG) forwards the INVITE request to S-CSCF

3. S-CSCF validates the service profile, and invokes any origination service logic required for this user. This includes authorisation of the requested SDP based on the user's subscription for multi-media services.

4. S-CSCF forwards the request, as specified by the S-S procedures.

5. The media stream capabilities of the destination are returned along the signalling path, per the S-S procedures.

6. S-CSCF forwards the Offer Response message to P-CSCF. Based on the choice made in step #2 above, this may be sent directly to P-CSCF (6a) or may be sent through I-CSCF(THIG) (6b1 and 6b2).

7. P-CSCF authorises the resources necessary for this session.

8. The Authorization-Token is included in the Offer Response message. P-CSCF forwards the message to the originating endpoint

9. UE decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation to the P-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 8 or a subset. If new media are defined by this SDP, a new authorization (as in Step 7) will be done by the P-CSCF(PDF) following Step 14. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method. Each offer/answer exchange will cause the P-CSCF(PDF) to repeat the Authorization step (Step 7) again.

10. After determining the needed resources in step 8, UE initiates the reservation procedures for the resources needed for this session.

11. P-CSCF forwards the Response Confirmation to S-CSCF. This may possibly be routed through the I-CSCF depending on operator configuration of the I-CSCF. Step 11 may be similar to Step 2 depending on whether or not configuration hiding is used.

12. S-CSCF forwards this message to the terminating endpoint, as per the S-S procedure.

13-15. The terminating end point responds to the originating end with an acknowledgement. If Optional SDP is contained in the Response Confirmation, the Confirmation Acknowledge will also contain an SDP response. If the SDP has changed, the P-CSCF validates that the resources are allowed to be used. Step 14 may be similar to Step 6 depending on whether or not configuration hiding is used.

16-18. When the resource reservation is completed, UE sends the successful Resource Reservation   message to the terminating endpoint, via the signalling path established by the INVITE message. The message is sent first to P-CSCF. Step 17 may be similar to Step 2 depending on whether or not configuration hiding is used.

19-21. The terminating end point responds to the originating end when successful resource reservation has occured. If the SDP has changed, the P-CSCF authorizes that the resources are allowed to be used. Step 20 may be similar to Step 6 depending on whether or not configuration hiding is used.

22-24. Terminating end point may generate ringing and it is then forwarded via the session path to the UE. Step 23 may be similar to Step 6 depending on whether or not configuration hiding is used.

25. UE indicates to the originating user that the destination is ringing

26. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response, as specified by the termination procedures and the S-S procedures, to S-CSCF.

27. S-CSCF sends a SIP 200-OK final response along the signalling path back to P-CSCF. Step 27 may be similar to Step 6 depending on whether or not configuration hiding is used.

28. P-CSCF indicates the resources reserved for this session should now be approved for use.

29. P-CSCF sends a SIP 200-OK final response to the session originator

30. UE starts the media flow(s) for this session

31-33. UE responds to the 200 OK with a SIP ACK message sent along the signalling path. Step 32 may be similar to Step 2 depending on whether or not configuration hiding is used.

5.6.2 (MO#2) Mobile origination, home

This origination procedure applies to users located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedure described in section 5.1.1. During registration, the home network allocates an S-CSCF in the home network.

When registration is complete, P-CSCF knows the name/address of S-CSCF.

Figure 5.15: Mobile origination procedure - home

Procedure MO#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session.

2. The Authorization-Token is generated ~~by the PDF~~at this step and stored in the P-CSCF. P-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. In this case it forwards the INVITE to the S-CSCF in the home network.

3. S-CSCF validates the service profile, and invokes any origination service logic required for this user. This includes authorisation of the requested SDP based on the user's subscription for multi-media services.

4. S-CSCF forwards the request, as specified by the S-S procedures.

5. The media stream capabilities of the destination are returned along the signalling path, per the S-S procedures.

6. S-CSCF forwards the Offer Response message to P-CSCF

7. P-CSCF authorises the resources necessary for this session.

8. The Authorization-Token is included in the Offer Response message. P-CSCF forwards the message to the originating endpoint.

9. UE decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation to P-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 8 or a subset. If new media are defined by this SDP, a new authorization (as in Step 7) will be done by the P-CSCF(PDF) following Step 14. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method. Each offer/answer exchange will cause the P-CSCF(PDF) to repeat the Authorization step (Step 7) again.

10. UE initiates resource reservation for the offered media.

11. P-CSCF forwards this message to S-CSCF

12. S-CSCF forwards this message to the terminating endpoint, as per the S-S procedure.

13-14. The terminating end point responds to the originating end with an acknowledgement. If Optional SDP is contained in the Response Confirmation, the Confirmation Acknowledge will also contain an SDP response. If the SDP has changed, the PCSCF authorises the media.

15. PCSCF forwards the answered media towards the UE.

16-18. When the resource reservation is completed, UE sends the successful Resource Reservation message to the terminating endpoint, via the signalling path established by the INVITE message. The message is sent first to P-CSCF.

19-21. The terminating end point responds to the originating end when successful resource reservation has occured. If the SDP has changed, the P-CSCF again authorizes that the resources are allowed to be used.

22-24. 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 S-CSCF per the S-S procedure. It is sent from there toward the originating end along the signalling path.

25. UE indicates to the originating user that the destination is ringing.

26-27. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating end, as specified by the termination procedures and the S-S procedures, to S-CSCF.

28. P-CSCF indicates the resources reserved for this session should now be approved for use.

29. P-CSCF passes the 200-OK response back to UE

30. UE starts the media flow(s) for this session.

31-33. UE responds to the 200 OK with an ACK message which is sent to P-CSCF and passed along the signalling path to the terminating end.

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

5.7.1 (MT#1) Mobile termination, roaming

This termination procedure applies to roaming users.

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

When registration is complete, S-CSCF knows the name/address of its next hop in the signalling path, either I-CSCF or P-CSCF, I-CSCF (if it exists) knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.
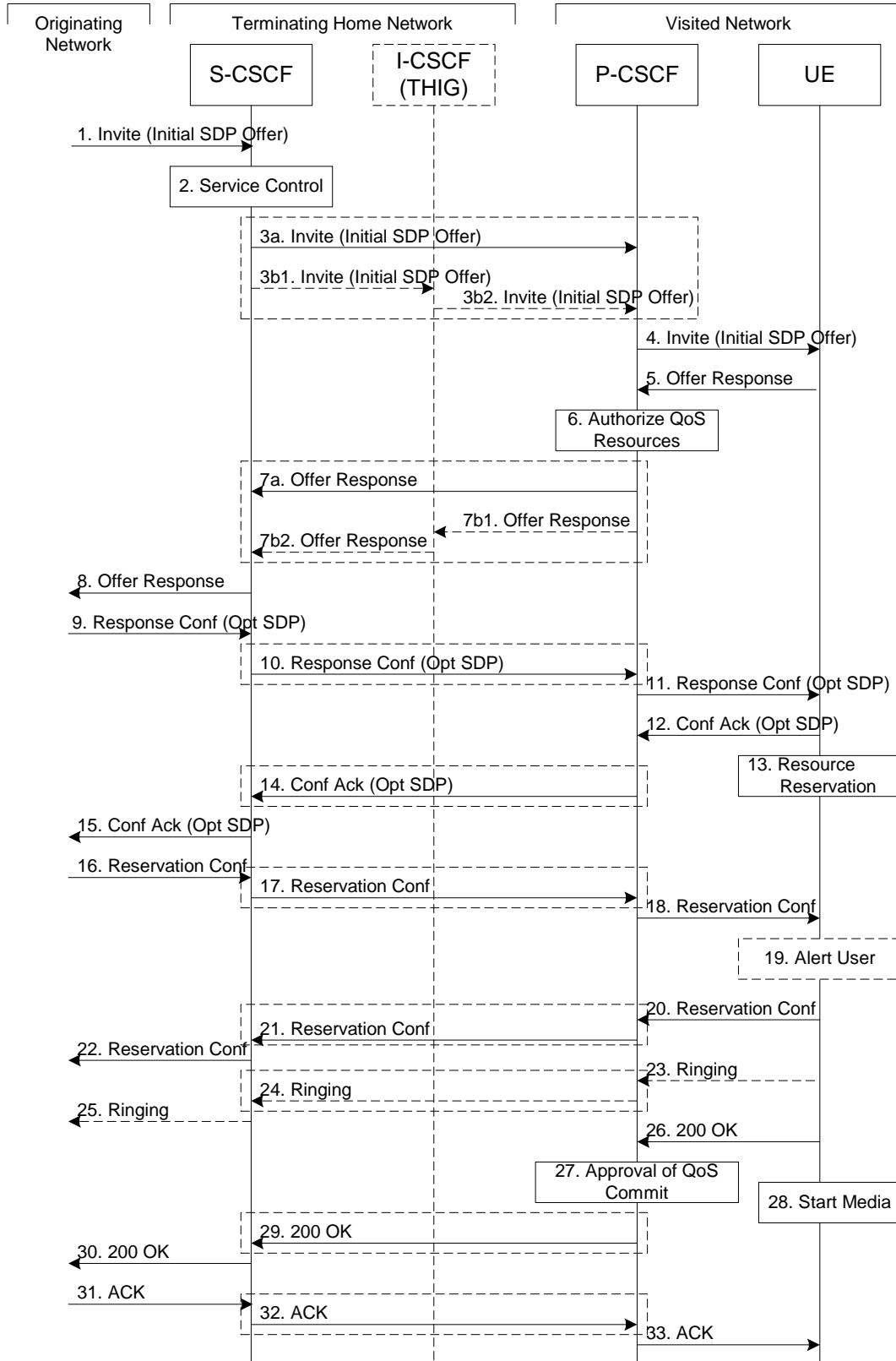
Figure 5.17: Mobile termination procedure - roaming

Procedure MT#1 is as follows:

1. The originating party sends the SIP INVITE request, containing an initial SDP, via one of the origination procedures, and via one of the Inter-Serving procedures, to the Serving-CSCF for the terminating users.

2. S-CSCF validates the service profile, and invokes any termination service logic required for this user. This includes authorisation of the requested SDP based on the user's subscription for multi-media services.

3. S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF in the visited network, possibly through an I-CSCF.

    This next hop is either the P-CSCF that is serving the visiting UE (choice (a)), or an I-CSCF(THIG) within the home network that is performing the configuration hiding function for the home network operator (choice (b)).

    (3a) If the home network operator does not desire to keep their network configuration hidden, the INVITE request is forwarded directly to the P-CSCF.

    (3b) If the home network operator desires to keep their network configuration hidden, the INVITE request is forwarded through an I-CSCF(THIG) to the P-CSCF.

        (3b1)   S-CSCF forwards the INVITE request to I-CSCF(THIG)

        (3b2)   I-CSCF(THIG) forwards the INVITE request to P-CSCF

4. The Authorization-Token is generated ~~by the PDF~~at this step and included in the INVITE message. P-CSCF remembers (from the registration procedure) the UE address, and forwards the INVITE to the UE.

5. UE determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. The SDP may represent one or more media for a multi-media session. This response is sent to P-CSCF.

6. P-CSCF authorises the resources necessary for this session.

7. P-CSCF forwards the Offer Response message to S-CSCF. Based on the choice made in step #3 above, this may be sent directly to S-CSCF (7a) or may be sent through I-CSCF(THIG) (7b1 and 7b2).

8. S-CSCF forwards the Offer Response message to the originator, per the S-S procedure.

9. The originating endpoint sends a Response Confirmation via the S-S procedure, to S-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in Step 8 or a subset. If new media are defined by this SDP, a new authorization (as in Step 6) will be done by the P-CSCF(PDF) following Step 12. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method. Each offer/answer exchange will cause the P-CSCF(PDF) to repeat the Authorization step (Step 6) again.

10. S-CSCF forwards the Response Confirmation to P-CSCF. This may possibly be routed through the I-CSCF depending on operator configuration of the I-CSCF. Step 10 may be similar to Step 3 depending on whether or not configuration hiding is used.

11. P-CSCF forwards the Response Confirmation to UE.

12. UE responds to the Response Confirmation with an acknowledgement. If Optional SDP is contained in the Response Confirmation, the Confirmation Ack will also contain an SDP response. If the SDP has changed, the P-CSCF authorizes that the resources are allowed to be used.

13. UE initiates the reservation procedures for the resources needed for this session.

14-15. PCSCF forwards the Confirmation Ack to the S-CSCF and then to the originating end point via session path. Step 14 may be similar to Step 7 depending on whether or not configuration hiding is used.

16-18. When the originating endpoint has completed its resource reservation, it sends the successful Resource Reservation message to S-CSCF, via the S-S procedures. The S-CSCF forwards the message toward the terminating endpoint along the signalling path. Step 17 may be similar to Step 3 depending on whether or not configuration hiding is used.

19. UE#2 alerts the destination user of an incoming session setup attempt.

20-22. UE#2 responds to the successful resource reservation towards the originating end point. Step 21 may be similar to Step 7 depending on whether or not configuration hiding is used.

23-25. UE may alert the user and wait for an indication from the user before completing the session setup. If so, it indicates this to the originating party by a provisional response indicating Ringing. This message is sent to P-CSCF and along the signalling path to the originating end. Step 24 may be similar to Step 7 depending on whether or not configuration hiding is used.

26. When the destination party answers, the UE sends a SIP 200-OK final response to P-CSCF.

27. P-CSCF indicates the resources reserved for this session should now be committed.

28. UE starts the media flow(s) for this session

29-30. P-CSCF sends a SIP 200-OK final response along the signalling path back to the S-CSCF Step 29 may be similar to Step 7 depending on whether or not configuration hiding is used.

31-33. The originating party responds to the 200-OK final response with a SIP ACK message that is sent to S-CSCF via the S-S procedure and forwarded to the terminating end along the signalling path. Step 32 may be similar to Step 3 depending on whether or not configuration hiding is used.

5.7.2　(MT#2) Mobile termination, home

This termination procedure applies to users located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedures described in section 5.1.1.

When registration is complete, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.
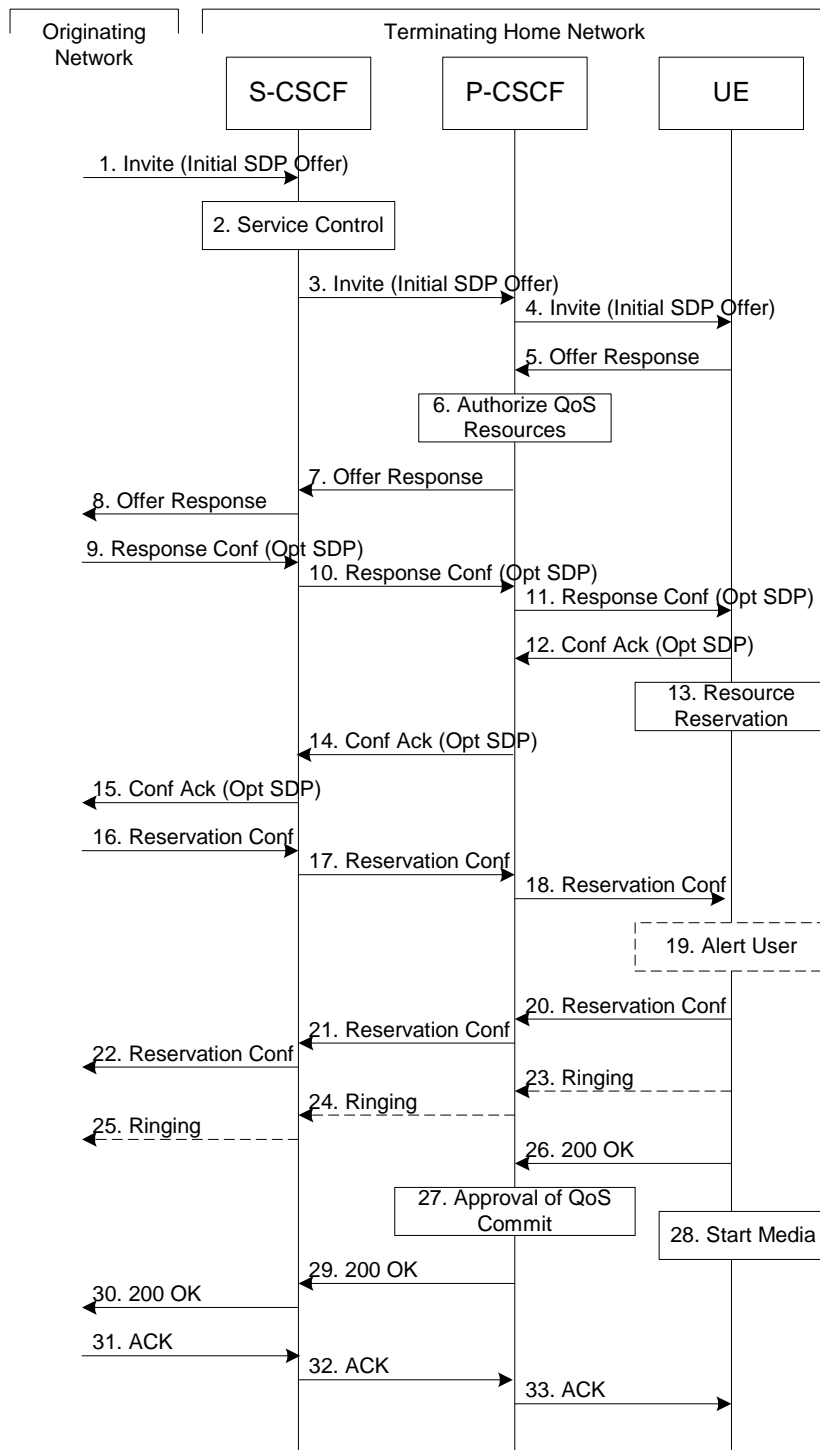
Figure 5.18: Mobile termination procedure - home

Procedure MT#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, via one of the origination procedures, and via one of the Serving to Serving-CSCF procedures, to the Serving-CSCF for the terminating user.

2. S-CSCF validates the service profile, and invokes any termination service logic required for this user. This includes authorisation of the requested SDP based on the user's subscription for multi-media services.

3. S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF in the home network.

4. The Authorization-Token is generated ~~by the PDF~~at this step and included in the INVITE message. P-CSCF remembers (from the registration procedure) the UE address, and forwards the INVITE to the UE.

5. UE determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. The SDP may represent one or more media for a multi-media session. This response is sent to P-CSCF.

6. P-CSCF authorises the resources necessary for this session.

7. P-CSCF forwards the Offer Response message to S-CSCF.

8. S-CSCF forwards the Offer Response message to the originator, per the S-S procedure.

9. The originating endpoint sends a Response Confirmation via the S-S procedure, to S-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in Step 8 or a subset. If new media are defined by this SDP, a new authorization (as in Step 6) will be done by the P-CSCF(PDF) following Step 12. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method. Each offer/answer exchange will cause the P-CSCF(PDF) to repeat the Authorization step (Step 6) again.

10. S-CSCF forwards the Response Confirmation to P-CSCF.

11. P-CSCF forwards the Response Confirmation to UE.

12. UE responds to the Response Confirmation with an acknowledgement. If Optional SDP is contained in the Response Confirmation, the Confirmation Ack will also contain an SDP response. If the SDP has changed, the P-CSCF authorizes that the resources are allowed to be used.

13. UE initiates the reservation procedures for the resources needed for this session.

14-15. The response is forwarded to the originating end point.

16-18. When the originating endpoint has completed its resource reservation, it sends the successful Resource Reservation message to S-CSCF, via the S-S procedures. The S-CSCF forwards the message toward the terminating endpoint along the signalling path.

19. UE#2 alerts the destination user of an incoming session setup attempt.

20-22. UE#2 responds to the successful resource reservation and the message is forwarded to the originating end.

23-25. UE may alert the user and wait for an indication from the user before completing the session. If so, it indicates this to the originating party by a provisional response indicating Ringing. This message is sent to P-CSCF and along the signalling path to the originating end.

26. When the destination party answers, UE sends a SIP 200-OK final response to P-CSCF.

27. P-CSCF indicates the resources reserved for this session should now be committed.

28. UE starts the media flow(s) for this session.

29-30. P-CSCF forwards the 200-OK to S-CSCF, following the signaling path.

31-33. The session originator responds to the 200-OK by sending the ACK message to S-CSCF via the S-S procedure and it is forwarded to the terminating end along the signalling path..

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

This termination procedure applies to a user registered for CS services, either in the home network or in a visited network. The user has both IMS and CS subscriptions but is unregistered for IMS services
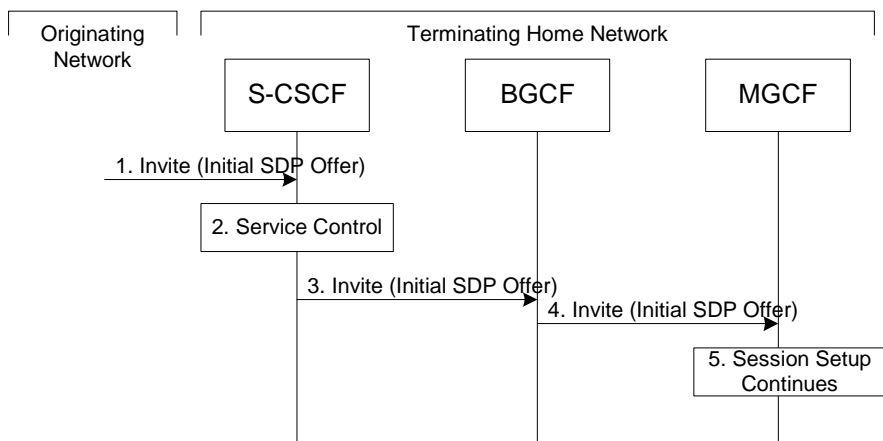
Figure 5.18a: Mobile Terminating procedures to a user that is unregistered for IMS services but is registered for CS services

1. In case the terminating user does not have an S-CSCF allocated, the session attempt is routed according to the section 5.12.1 (Mobile Terminating procedures to unregistered IMS user that has services related to unregistered state).

2. S-CSCF invokes service control appropriate for this session setup attempt, which may result in e.g. re-routing the session to a messaging service, or continued routing towards the user's CS domain termination address (e.g. E.164).

3. S-CSCF performs whatever further actions are appropriate for this session setup attempt. In case of routing towards the user's CS domain termination address, the S-CSCF performs an analysis of this address. From the analysis of the destination address, S-CSCF determines that this is for the CS domain, and passes the request to the BGCF.

4. The BGCF forwards the SIP INVITE message to the appropriate MGCF in the home network, or to a BGCF in another network. This depends on the PSTN interworking configuration of the IMS network. Eventually, the session initiation arrives to an MGCF.

5. Normal session setup continues according to PSTN-T flow as described in Section 5.7.3

5.7.3 (PSTN-T) PSTN termination

The MGCF in the IM CN subsystem is a SIP endpoint that initiates and receives requests on behalf of the PSTN and Media Gateway (MGW).Other nodes consider the signalling as if it came from a S-CSCF. The MGCF incorporates the network security functionality of the S-CSCF.

PSTN termination may be done in the same operator's network as the S-CSCF of the session originator. Therefore, the location of the MGCF/MGW are given only as "Terminating Network" rather than "Home Network" or "Visited Network."

Further, agreements between network operators may allow PSTN termination in a network other than the originator's visited network or home network. This may be done, for example, to avoid long distance or international tariffs.

This termination procedure can be used for any of the inter-serving procedures, in place of the S-CSCF.
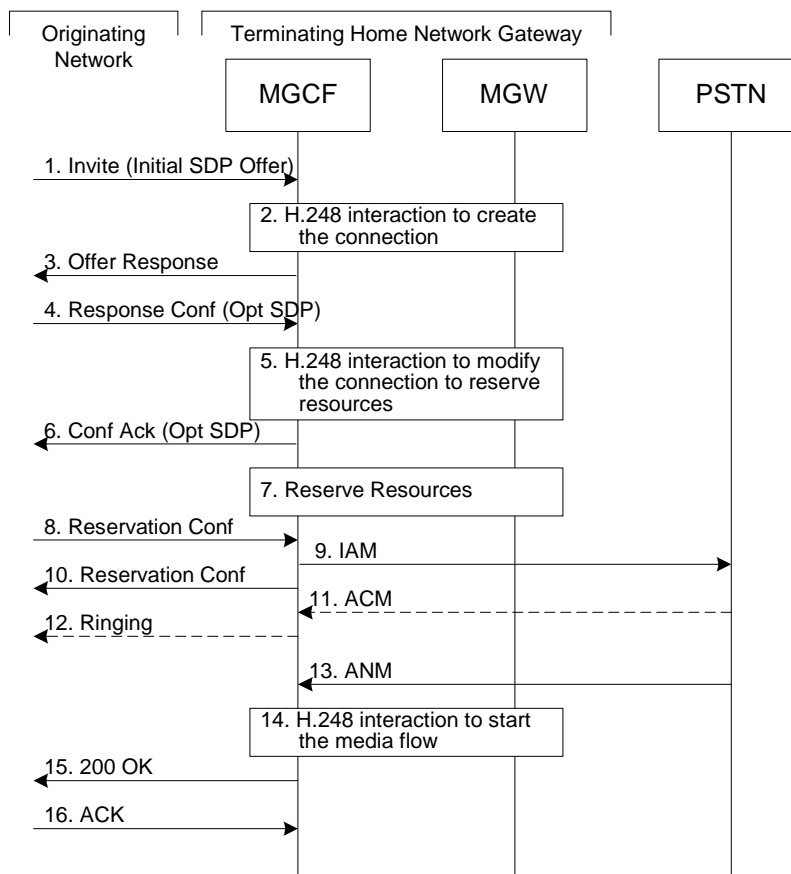
Figure 5.19: PSTN termination procedure

The PSTN termination procedure is as follows:

1. MGCF receives an INVITE request, containing an initial SDP, through one of the origination procedures and via one of the inter-serving procedures.

2. MGCF initiates a H.248 interaction to pick an outgoing channel and determine media capabilities of the MGW.

3. MGCF determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. This response is sent via the S-S procedure.

4. The originating endpoint sends a Response Confirmation. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in Step 3 or a subset. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method.

5. MGCF initiates a H.248 interaction to modify the connection established in step #2 and instruct MGW to reserve the resources necessary for the media streams.

6. MGCF responds to the offered media towards the originating party.

7. GW reserved the resources necessary for the media streams.

8. When the originating endpoint has completed its resource reservation, it sends the successful Resource Reservation   message to MGCF, via the S-S procedures.

9. MGCF sends an IAM message to the PSTN

10. MGCF sends response to the successful resource reservation towards originating end.

11. The PSTN establishes the path to the destination. It may optionally alert the destination user before completing the session. If so, it responds with an ACM message.

12. If the PSTN is alerting the destination user, MGCF indicates this to the originating party by a provisional response indicating Ringing. This message is sent via the S-S procedures.

13. When the destination party answers, the PSTN sends an ANM message to MGCF

14. MGCF initiates a H.248 interaction to make the connection in the MGW bi-directional.

15. MGCF sends a SIP 200-OK final response along the signalling path back to the session originator

16. The Originating party acknowledges the final response with a SIP ACK message

5.7.4 Mobile Termination from an external SIP client

This clause describes the terminating session setup procedures 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 parameters have been negotiated and accepted. Session flows 5.19a and 5.19b show 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 clause 5.7.2. The same principles apply in roaming cases, i.e. analogous variants of MT#1 defined in clause 5.7.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
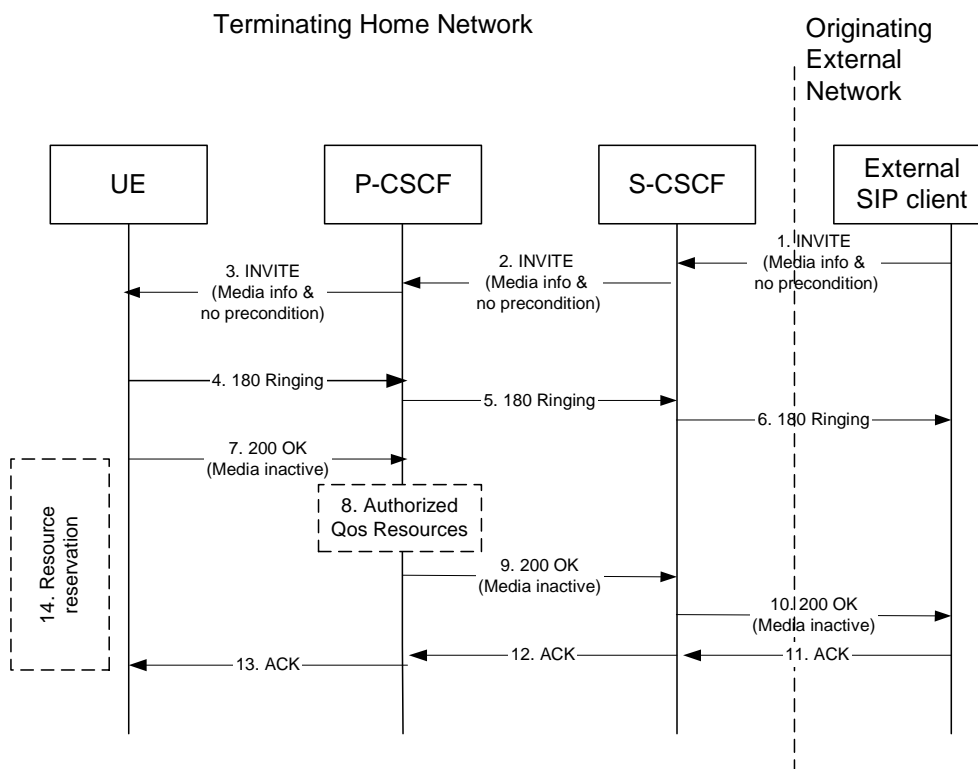

Figure 5.19a. Terminating session from external SIP client, detection & initial setup with media not allowed

1-3. A session arrives at the UE in the IMS network with media information but without requiring precondition capability.

4-6. Ringing information is sent end to end towards the originating party.

7-10. The UE begins the resource reservation according to the session and media parameters. The P-CSCF/PDF may authorise the media parameters being negotiated and the originating party is notified of the session setup details with all media components set to inactive.

11-13. The originating party acknowledges the session.

14. When the UE has completed the resource reservation procedures, the UE continues with the session setup according to flow 5.19b. The UE sets the media components to active state.
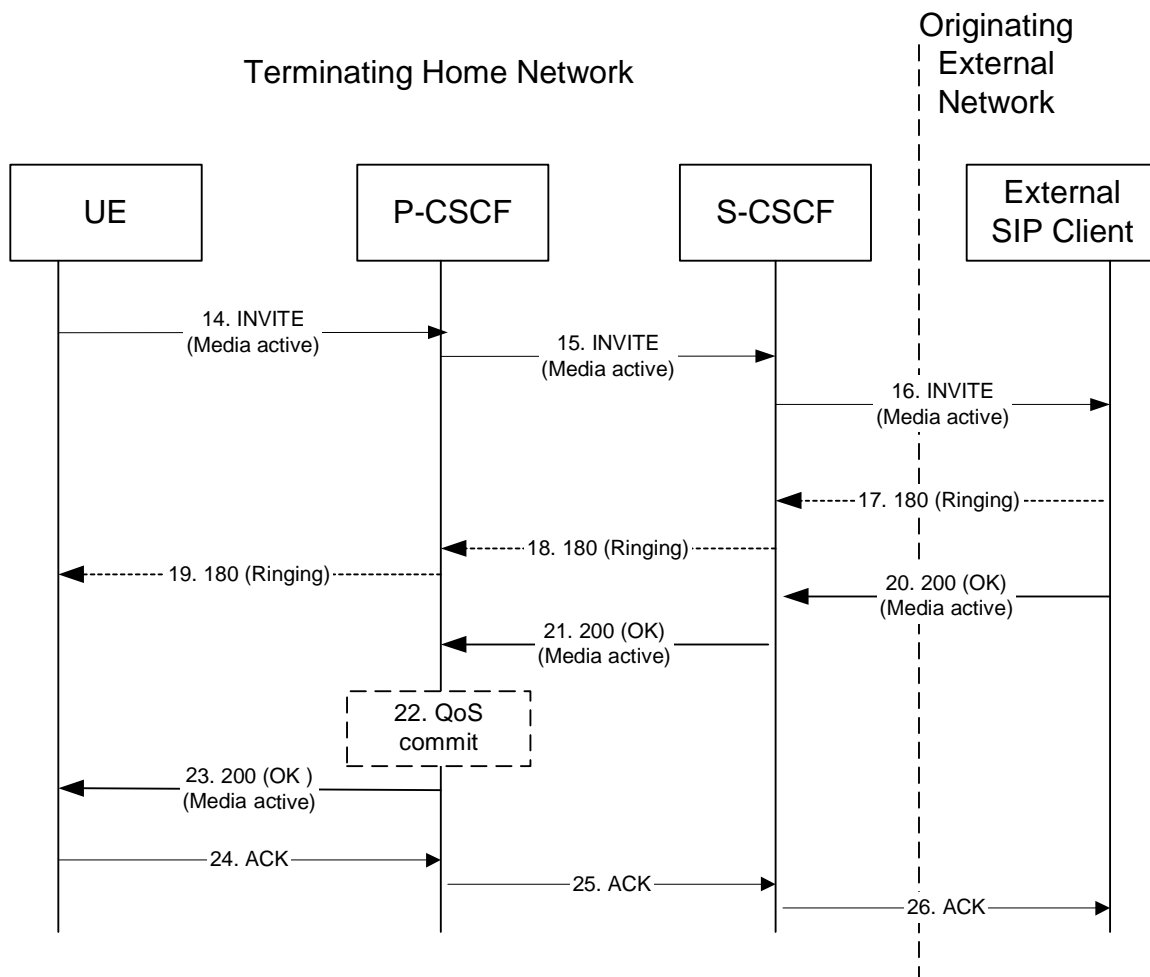

Figure 5.19b. Continuation of terminating session from external SIP client, session setup with active media

14-16. By sending a re-INVITE indicating the support for the precondition capability, the terminating UE initiates setting of media components to active.

17-19. Ringing Information may be sent from an external SIP entity (in this case the originating party) through the session path towards the terminating UE.

20-23. The originating SIP client accepts the re-INVITE with the active media streams. In step 22, The P-CSCF/PDF may commit/approve the resources authorised for the session.

24-26. Session is acknowledged end-to-end.

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.

Figure 5.19c. 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 ~~by the PDF~~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 ~~by the PDF~~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******

5.11.3   Procedures for codec and media characteristics flow negotiations

5.11.3.0   General

This section gives information flows for:

- -   the procedures for determining the set of negotiated characteristics between the endpoints of a multi-media session, determining the initial media characteristics (including common codecs) to be used for the multi-media session, and

- -   the procedures for modifying a session within the existing resources reservation or with a new resources reservation (adding/deleting a media flow, changing media characteristics including codecs, changing bandwidth requirements)   when the session is already established.

5.11.3.1   Codec and media characteristics flow negotiation during initial session establishment

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

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

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

Once the session is established, the procedures of section 5.11.3.2 may be used by either endpoint to change to a different media characteristic (e.g. codec) that was included in the initial session description, and for which no additional resources are required for media transport. The procedures of section 5.11.3.3 may be used by either endpoint to change the session, which requires resources beyond those allocated to the existing session.

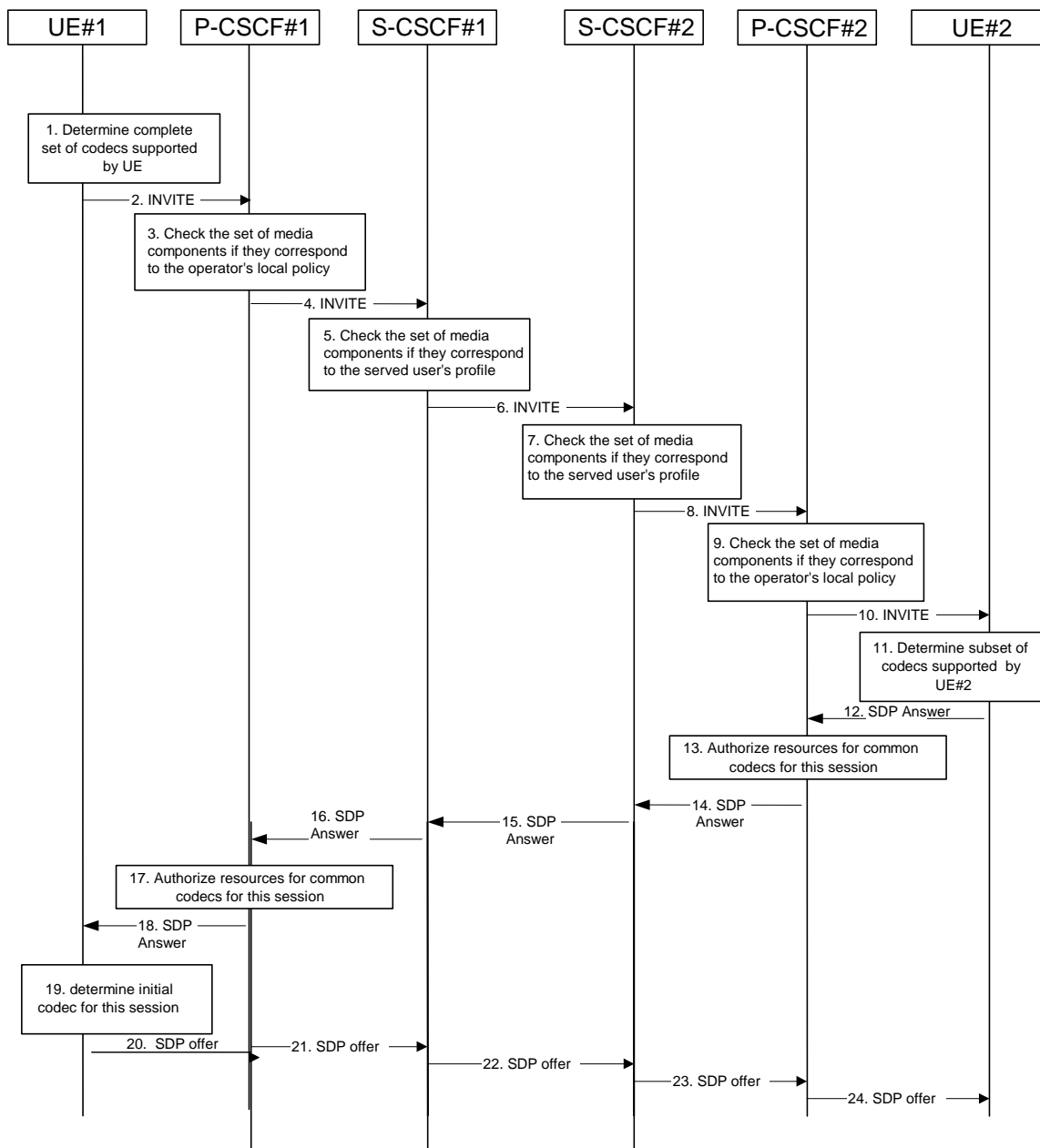The flow presented here assumes that service-based local policy is in use.

Figure 5.30: Codec negotiation during initial session establishment

The detailed procedure is as follows:

1. UE#1 inserts the codec(s) to a SDP payload. The inserted codec(s) shall reflect the UE#1's terminal capabilities and user preferences for the session capable of supporting for this 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 the initial 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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the P-CSCF#1 allows the initial session initiation attempt to continue.
The Authorisation token is generated ~~by the PDF~~at this step.

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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the S-CSCF#1 allows the initial session initiation 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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the S-CSCF#2 allows the initial session initiation attempt to continue.

8. S-CSCF#2 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 initiation attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session initiation 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 5.30 above the P-CSCF#2 allows the initial session initiation attempt to continue.
    The Authorization-Token is generated ~~by the PDF~~at this step.

10. The Authorization-Token is included in the INVITE message. 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

13. P-CSCF#2 authorises the QoS resources for the remaining media flows and codec choices.

14. P-CSCF#2 forwards the SDP response to S-CSCF#2.

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. P-CSCF#1 authorises the QoS resources for the remaining media flows and codec choices.

18. The Authorization-Token is included in the SDP message. P-CSCF#1 forwards the SDP response to UE#1

19. 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 need to renegotiate the codecs by sending another offer to reduce codec to one with the UE#2.

20-24. UE#2 sends the "Offered SDP" message to UE#1, along the signalling path established by the INVITE request

The remainder of the multi-media session completes identically to a single media/single codec session, if the negotiation results in a single codec per media.

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

5.16.2.2.2   Session based messaging procedure using multiple UEs

Session based messaging between more than two UEs require the establishment of a session based messaging conference.

Within session based messaging conferences including multiple UEs (e.g. multiparty chat conferences) an MRFC/MRFP or an IMS AS shall be used to control the media resources.

When MRFC/MRFP are used, then conferencing principles are used to provide the chat service:

- MRFP must be able to establish message connections with all involved parties.

- MRFC/MRFP must be able to receive messages from conference participants and to distribute messages to all or some of the participants.

- In order to enable the UE managing information related to the session based messaging conference the MRFC may be co-located with an IMS AS.

- MRFC/MRFP roles and interactions with an AS are described in more detail in chapters 4.7 and 5.14.1 and 5.14.2.

- The interface for session based messaging between MRFC and MRFP is not standardised in this release. When an AS is used, then the IMS service control architecture is used to provide the chat service. Both signalling and user plane are then supported by the AS. For more details, see section 4.2.

The following flow shows the originating session based messaging set up using an intermediate server for a chat service. In this case the intermediate chat server is addressed by the UE#1 using a PSI. It is assumed that UE#1 is the first UE entering the chat session.

NOTE: Interactions between MRFC and MRFP are not shown in the flows below since these interactions are not standardized. An optional ringing response from MRFC/AS to the UE is not shown in the following procedure.
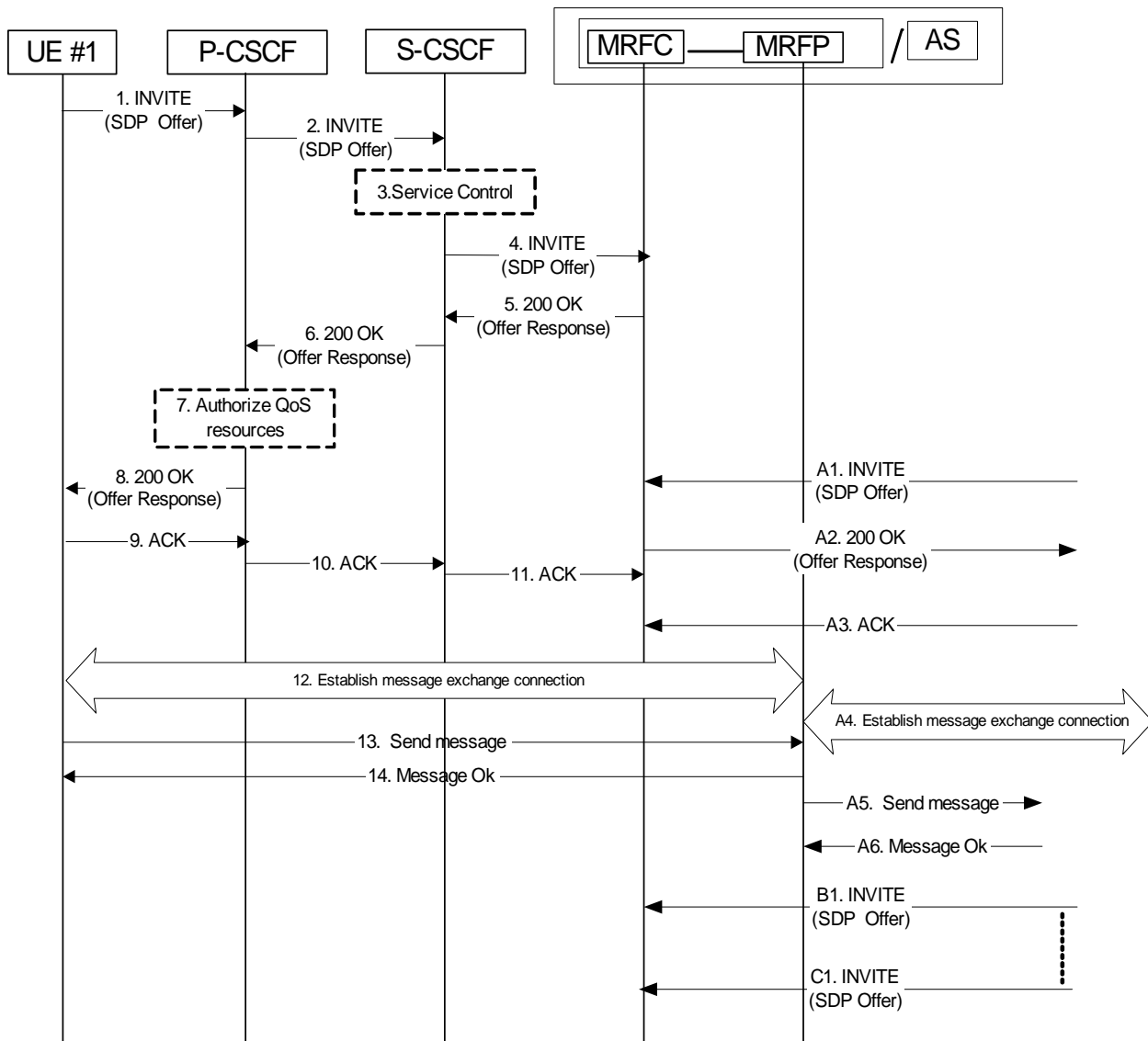
****** Next Change******

Figure 5.48b: Session based messaging using a chat server

1. UE #1 sends the SIP INVITE request addressed to a conferencing or chat PSI to the P-CSCF. The SDP offer indicates that UE#1 wants to establish a message session and contains all necessary information to do that. The SDP offer may indicate the maximum message size UE#1 accepts to receive.

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

3. S-CSCF may invoke service control logic for UE#1.

4. S-CSCF forwards the INVITE request to the MRFC/AS.

5., 6. and 8. MRFC/AS acknowledges the INVITE with a 200 OK, which traverses back to UE#1. The 200 OK (Offer response) may indicate the maximum message size the host of the PSI accepts to receive.

7. Based on operator policy P-CSCF/PDF may authorize the resources necessary for this session. The media authorization token is generated ~~by the PDF~~at this step and sent in the 200 OK to UE#1.

9.-11. UE#1 acknowledges the establishment of the messaging session with an ACK towards MRFC/AS.

12. UE#1 establishes a reliable end-to-end connection with MRFP/AS to exchange the message media.

13. UE#1 sends a message towards MRFP/AS.

14. MRFP/AS acknowledges the message.

A1.   Another UE (UE#2) sends an INVITE request addressed to the same conferencing or chat PSI. The initial SDP indicates that the UE wants to establish a message session and contains all necessary information to do that.

A2.   MRFC/AS acknowledges the INVITE request with a 200 OK.

A3.   UE#2 acknowledges the 200 OK with an ACK.

A4.   UE#2 establishes a reliable end-to-end connection with MRFP/AS to exchange the message media.

A5.   MRFP/AS forwards the message to all recipients, e.g. all participants in the chat room.

A6. The recipients acknowledge the message towards MRFP/AS.

B1. and C1.   Further INVITE requests from new possible participants may arrive at any time.

Further messages may be exchanged in either direction between the participating UEs using the established connection via the MRFC/MRFP or AS. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and the host of the PSI respectively.

5.16.2.2.3   Session based messaging procedure with an intermediate node

The following procedure shows the originating session based messaging involving an intermediate node. An optional ringing response from AS to the UE or vice versa is not shown in the following procedure.
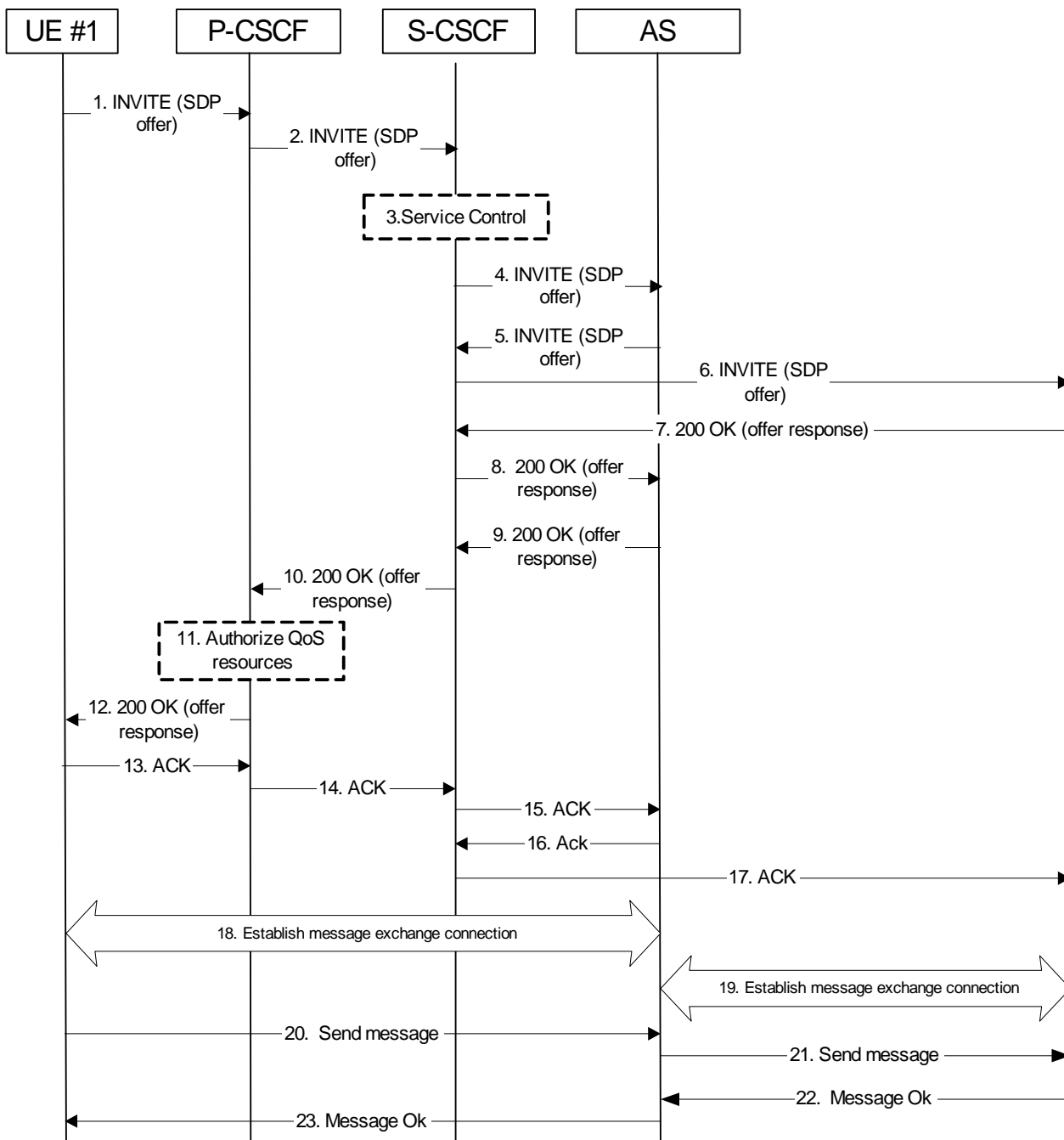
Figure 5.48c: Session based messaging with an intermediate node

1. UE#1 sends the SIP INVITE request addressed to UE#2, containing an initial SDP, to the P-CSCF. The SDP offer may indicate the maximum message size UE#1 accepts to receive.

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

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

4. The S-CSCF forwards the INVITE request to the AS. The AS may modify the content of the SDP (such as IP address/port numbers). Based on operator policy the AS may either reject the session set-up or decrease the maximum message size indication.

5. The AS sends the INVITE request to the S-CSCF.

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

7–8. The UE or AS in the terminating network accepts the INVITE request with a 200 OK response. The 200 OK response is forwarded by the S-CSCF to the AS. The 200 OK (Offer response) may indicate the maximum message size UE#2 accepts to receive, possibly decreased by the AS.

9, 10 and 12. The AS accepts the message session with a 200 OK response. The 200 OK response traverses back to UE#1.

11. Based on operator policy P-CSCF/PDF may authorize the resources necessary for this session. The media authorization token is generated ~~by the PDF~~at this step and sent in the 200 OK to UE#1.

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

16. - 17. The AS acknowledges the 200 OK response from the terminating network with an ACK, which traverses back to the UE or AS in the terminating network via the S-CSCF. Based on AS implementation sending of the ACK may happen sometimes after step 8.

18. UE#1 establishes a reliable end-to-end connection with the AS to exchange the message media.

19. The AS establishes a reliable end-to-end connection with the UE or AS in the terminating network to exchange the message media.

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

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

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

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

Further messages may be exchanged in either direction between UE#1 and the terminating network using the established message connection via the AS. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and UE#2 respectively, possibly decreased by the AS.

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **464** | ⌘**rev** | **1** | ⌘ | Current version: | **6.7.0** | ⌘ |

*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: ⌘	Tel-URI related reference updates	
Source: ⌘	Nokia	
Work item code:⌘	IMS2	***Date:*** ⌘ 07/11/2004
Category: ⌘ **D**		***Release:*** ⌘ Rel-6

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

Use *one* of the following releases:
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: ⌘	RFC 2916 is obsoleted by RFC 3761, and the internet draft http://www.ietf.org/internet-drafts/draft-ietf-iptel-rfc2806bis-09.txt was approved by the IESG.
Summary of change:⌘	References to obsoleted RFCs replaced.
Consequences if not approved: ⌘	Reference to obsoleted RFCs (RFC2806, RFC 2916) in TS.

Clauses affected: ⌘	2	

	Y	N		
Other specs ⌘	X		Other core specifications ⌘	22.228, 24.229
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.

======FIRST CHANGE======

2 References

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

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

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1]   3GPP TS 23.002: "Network Architecture".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[42]   draft-ietf-sip-callerprefs-10 (October 2003): "Caller Preferences for the Session Initiation Protocol (SIP)"

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

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

=======END OF CHANGE=======

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **467** | ⌘ **rev** | **1** | ⌘ | Current version: | **6.7.0** | ⌘ |

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:	⌘	Informing AS on Registration
Source:	⌘	Siemens
Work item code:⌘	IMS2	**Date:** ⌘ 18/11/2004

Category:	⌘	**F**		**Release:** ⌘ Rel-6

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

Use one of the following releases:
   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: ⌘	Subclause 5.2.1 describes, among others that the S-CSCF may inform Application Servers upon registration time. However the current text is not precise.
Summary of change:⌘	Clarify that the S-CSCF may inform more than one AS and clarify that this information takes place for each registration (not per user). The latter changes makes the text generic enough to also cover both implicit registration and for shared public user identities.
Consequences if not approved: ⌘	Specification may be misleading.

Clauses affected:	⌘	5.2.1

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

Other comments:	⌘	

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

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

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

5.2.1　　Requirements considered for registration

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

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

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

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

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

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

6. The Serving-CSCF is able to retrieve a service profile of the user who has IMS subscription. The S-CSCF shall check the registration request against the filter information and if necessary inform ~~the~~ application servers about the registration; i. ~~It~~ shall be possible for the filter information to allow either just the initial registrations or also subsequent re-registrations ~~of the user~~ to be communicated to the application servers. The Serving-CSCF knows how to reach the Proxy-CSCF currently serving the user who is registered.

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

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

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

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

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

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

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

13. The UE may indicate its capabilities and characteristics in terms of SIP User Agent capabilities and characteristics described in "draft-ietf-sip-callee-caps-01" [38] during IMS registration. The UE may also update its capabilities by initiating a re-registration when the capabilities are changed on the UE.

3GPP TSG-SA WG2 Meeting #43
Seoul, Korea.15th - 19th November 2004.

Tdoc ⌘*S2-043842*

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.228 CR 453** ⌘**rev 4** ⌘ Current version: **6.7.0** ⌘

*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: ⌘	Revision of session set-up from external SIP client	
Source: ⌘	Ericsson	
Work item code: ⌘	IMS 2	***Date:*** ⌘ 18/11/2004
Category: ⌘ **F**		***Release:*** ⌘ Rel-6

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

Use *one* of the following releases:
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 present procedure is unnecessarily complex. The procedure also leads to more complex charging analysis, since the 200 OK either is sent too early or sent from the incorrect user.
Summary of change: ⌘	The proposal aligns the fall back case with the normal non precondition session set-up procedure.
Consequences if not approved: ⌘	1) Unnecessarily complex procedure. 2) Unnecessarily complex charging analysis.

Clauses affected: ⌘	5.6.4

	Y	N		
Other specs Affected: ⌘	X		Other core specifications ⌘	24.229
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘	

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

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

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

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

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

This subclause 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 5.16a shows 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 subclause 5.7.2. The same principles apply in roaming cases, i.e. analogous variants of MT#1 defined in subclause 5.7.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.

External Orig Networ

External S Client

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.

This clause describes the originating session setup procedures from 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. Below figures 5.16.a, 5.16.b and 5.16.c 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 clause 5.6.2. The same principles apply in roaming cases, i.e. analogous variants of MO#1 defined in clause 5.6.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
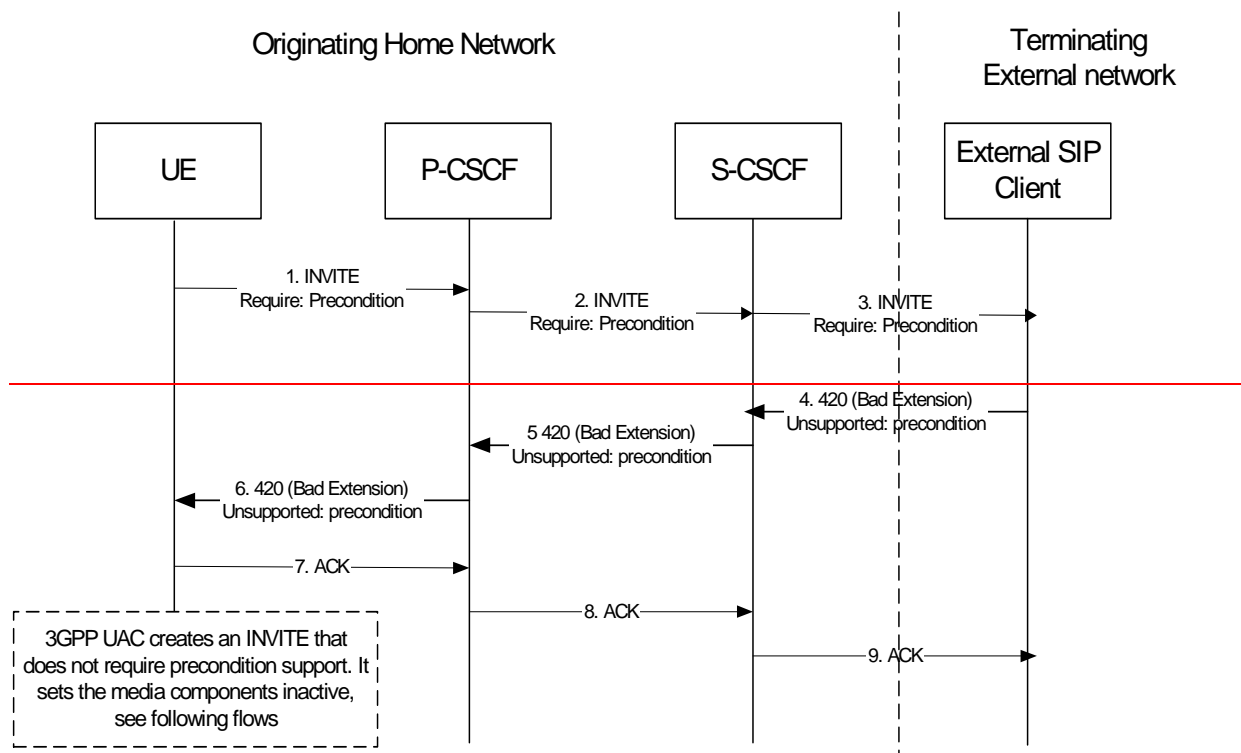

Figure 5.16a. Originating session towards external SIP client, detection phase

The Originating 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.

Originating Home Network
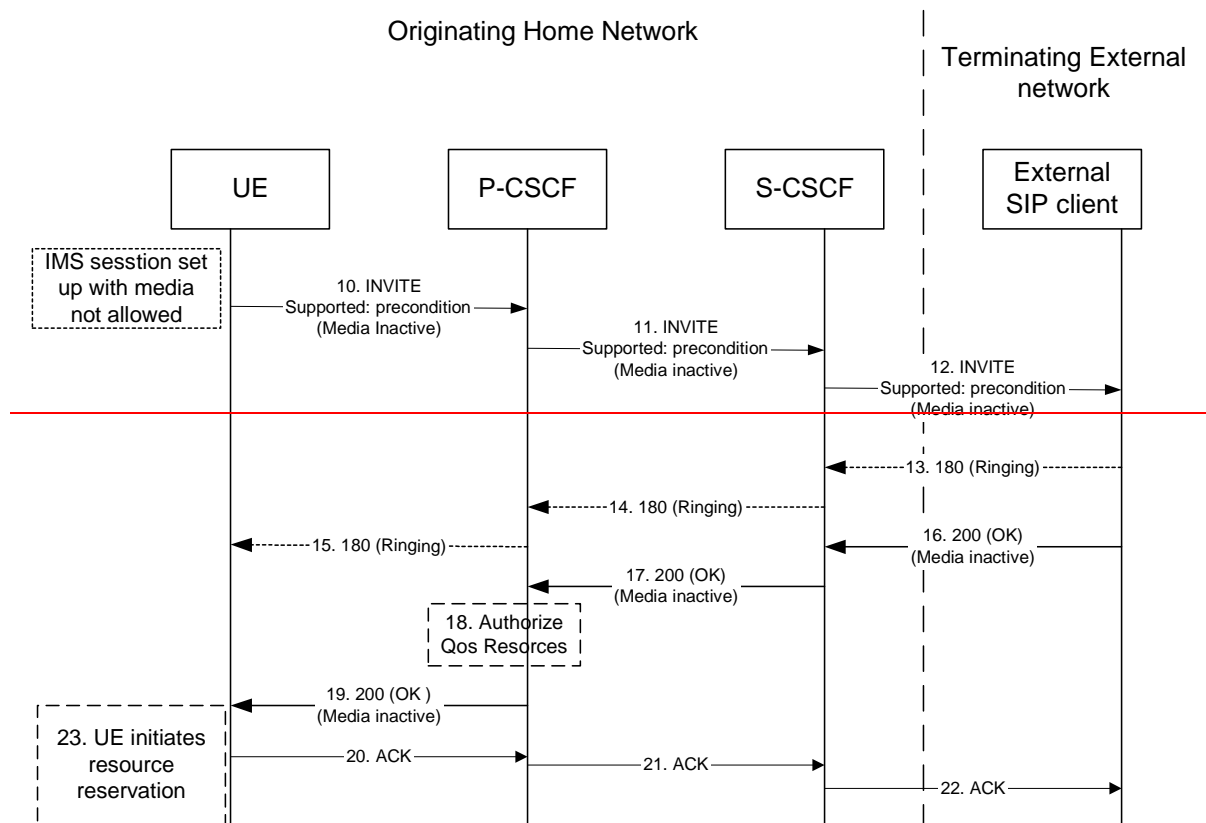
Terminating External network

Figure 5.16b. Originating 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 5.16b & 5.16c.

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.

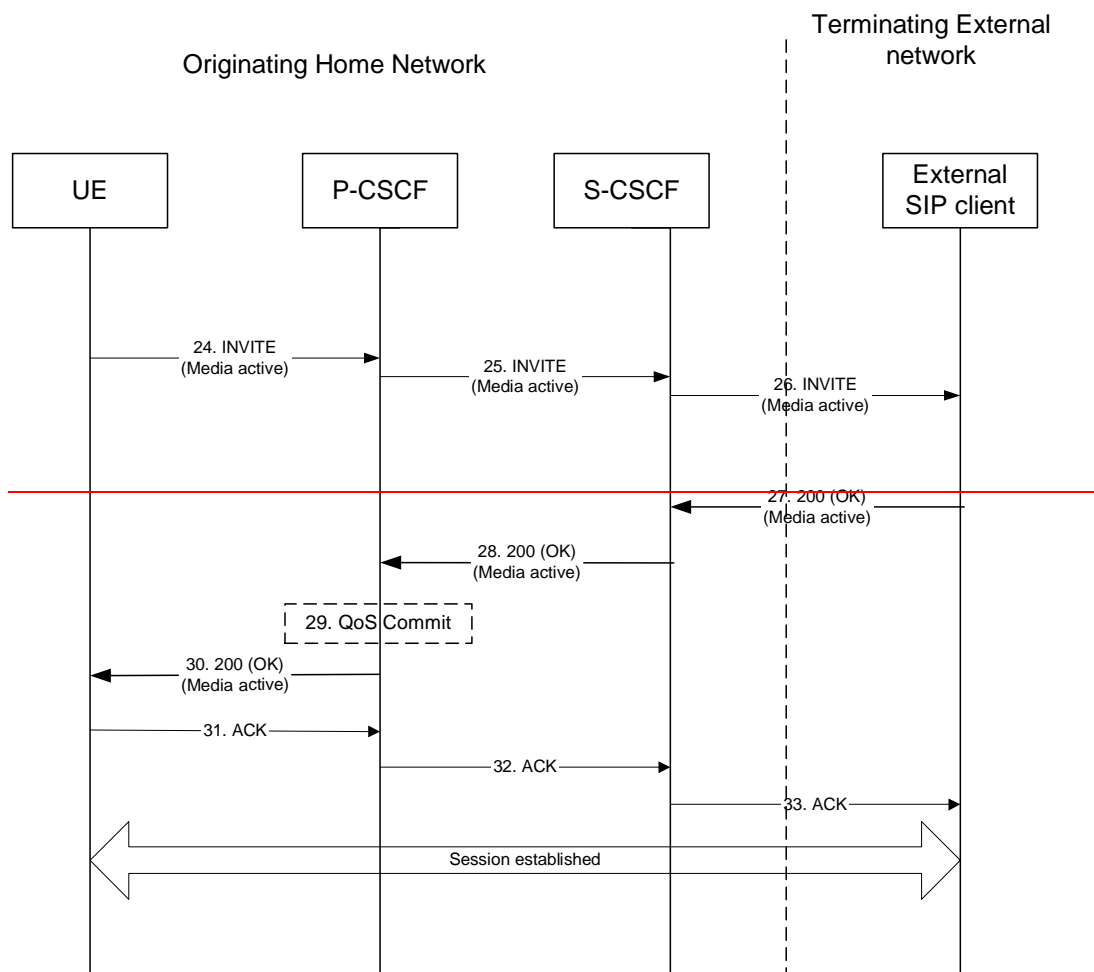23. The UE starts the resource reservation for the media.

Figure 5.16c. Continuation of originating 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 5.16c.

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.

CR-Form-v7

CHANGE REQUEST

⌘ **23.228 CR 461** ⌘**rev 2** ⌘ Current version: **6.7.0** ⌘

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: ⌘	Reorganization and clarification of session flows	
Source: ⌘	Lucent Technologies	
Work item code:⌘	IMS2	***Date:*** ⌘ 15/11/2004
Category: ⌘ **F**		***Release:*** ⌘ Rel-6

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

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

Reason for change: ⌘	Several new sub-clauses introduced as part of Release 6 have been put places that do not fit with the original flow of procedures in 23.228. This makes the document very difficult to understand and suggests that there is a difference in procedures where none exists.

The addition of new origination and termination procedures haven't been fully integrated into the text of sub-clause 5.4.10 and 5.5. This means that the full range of end to end sessions may not be understood from reading the specification.

Also the sub-clauses describing the interworking of IMS with non-IMS SIP networks have been placed in the wrong sub-clauses in clause 5. Specifically, 5.6.4 describes a procedure where the non-IMS SIP network is terminating a session yet it has been placed in sub-clause 5.6, Origination procedures. Likewise 5.7.4 describes a procedure where the non-IMS SIP network originates a session but it has been placed in sub-clause 5.7, Termination procedures. The confusion seems to have arisen because the procedures have been interpreted from the IMS UE's point of view rather than from the non-IMS SIP network's point of view. See 5.6.3 for an example of the correct way to categorise a procedure involving IMS interworking to a non-IMS network. |
| ***Summary of change:***⌘ | The changes are to relocate sections related to session flow overview and session termination scenarios. The origination and termination procedures that have already been added are now named in 5.4.10 and included in table 5.2. Sub-clause 5.4.10 is moved to 5.4a so that the overview immediately precedes |

the section with the procedures. In addition, clause 5 is updated to ensure the definition of which origination and termination procedures use which S-CSCF to S-CSCF procedures are only defined in one place (in table 5.2).

In addition, existing sub-clauses 5.6.4 and 5.7.4 are swapped. The original clause titles have been changed to clarify the meaning of the procedures and minor wording changes made to the first paragraph in each case. Figure numbers and titles have been amended as necessary.

The changes to sub-clause 5.6.4 are contained in CR 453R4.

This CR incorporates the changes approved in CR 448 and CR 449 and replaces these CRs.

Consequences if not approved:	⌘	Incorrect interpretation of the session flow procedures.

Clauses affected:	⌘	5.4.10, 5.4.12.2, 5.4.12.3, 5.4a (new), 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.7.4, 5.7.5 (new), 5.7.6 (new), and 5.7.7 (new).

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

Other comments:	⌘	

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

5.4.10   ~~Overview of session flow procedures~~Void

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

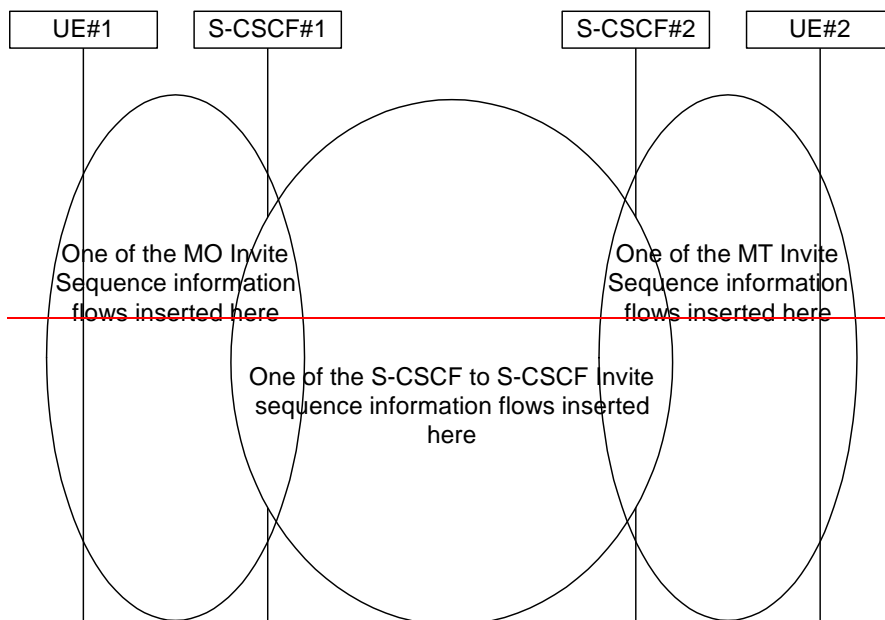~~For an IP Multi-Media Subsystem session, the session flow procedures are shown in the following diagram.~~

~~**Figure 5.9: Overview of Session Flow Sections**~~

~~The following procedures are defined:~~

~~For the origination sequence:~~

~~(MO#1) Mobile origination, roaming~~

~~(MO#2) Mobile origination, home~~

~~(PSTN-O) PSTN origination~~

~~For the termination sequence:~~

~~(MT#1) Mobile termination, roaming~~

~~(MT#2) Mobile termination, home~~

~~(MT#3) Mobile termination, CS Domain roaming~~

~~(PSTN-T) PSTN termination~~

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

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

~~(S-S#2) Session origination and termination are served by the same operator.~~

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

~~(S-S#4) Session origination with PSTN termination in a different network to the S-CSCF~~

~~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.	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.

In addition, variants of MO#1, MO#2, MT#1 and MT#2 are supported for interworking with external SIP clients, which do not support the SIP extensions required for IMS end points. These variants are not used in combination with any other session procedure.

5.4.11   Signalling Transport Interworking

A Signalling gateway function (SGW) is used to interconnect different signalling networks i.e. SCTP/IP based signalling networks and SS7 signalling networks. The signalling gateway function may be implemented as a stand alone entity or inside another entity [1]. The session flows in this specification do not show the SGW, but when interworking with PSTN/CS domain, it is assumed that there is a SGW for signalling transport conversion.

5.4.12   Configuration and Routing principles for Public Service Identities

5.4.12.0   General

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

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

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

## 5.4.12.1	PSIs on the originating side

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

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

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

## 5.4.12.2	PSIs on the terminating side

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

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

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

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

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

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

The AS hosting the PSI in combination with its entry in the HSS is referred to as "PSI user".

Figure ~~5.4.12.a~~5.19d depicts a routing example for incoming session where the session request is routed directly to the ~~~~AS hosting the PSI.

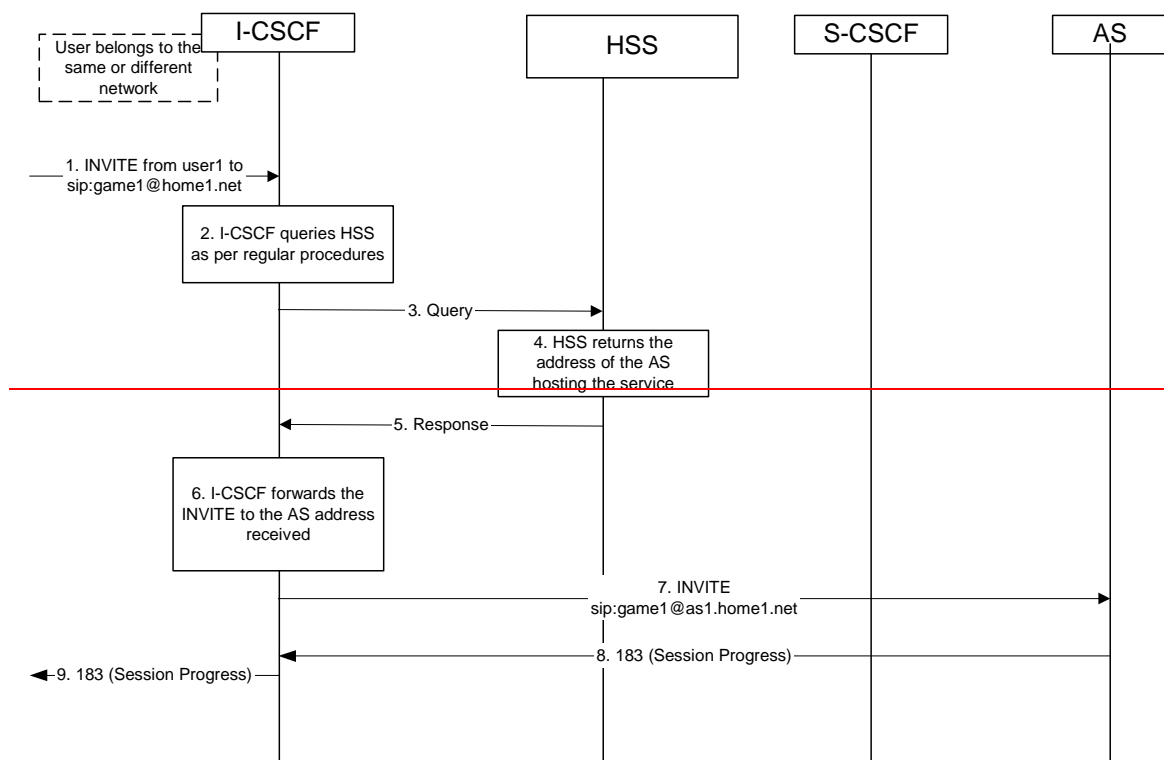Figure 5.19e depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.

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

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

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

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

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

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

8 9.   Session setup continues as per existing procedures.

Figure 5.4.12.b depicts an example routing scenario where the basic IMS routing via S CSCF is used to route the session.
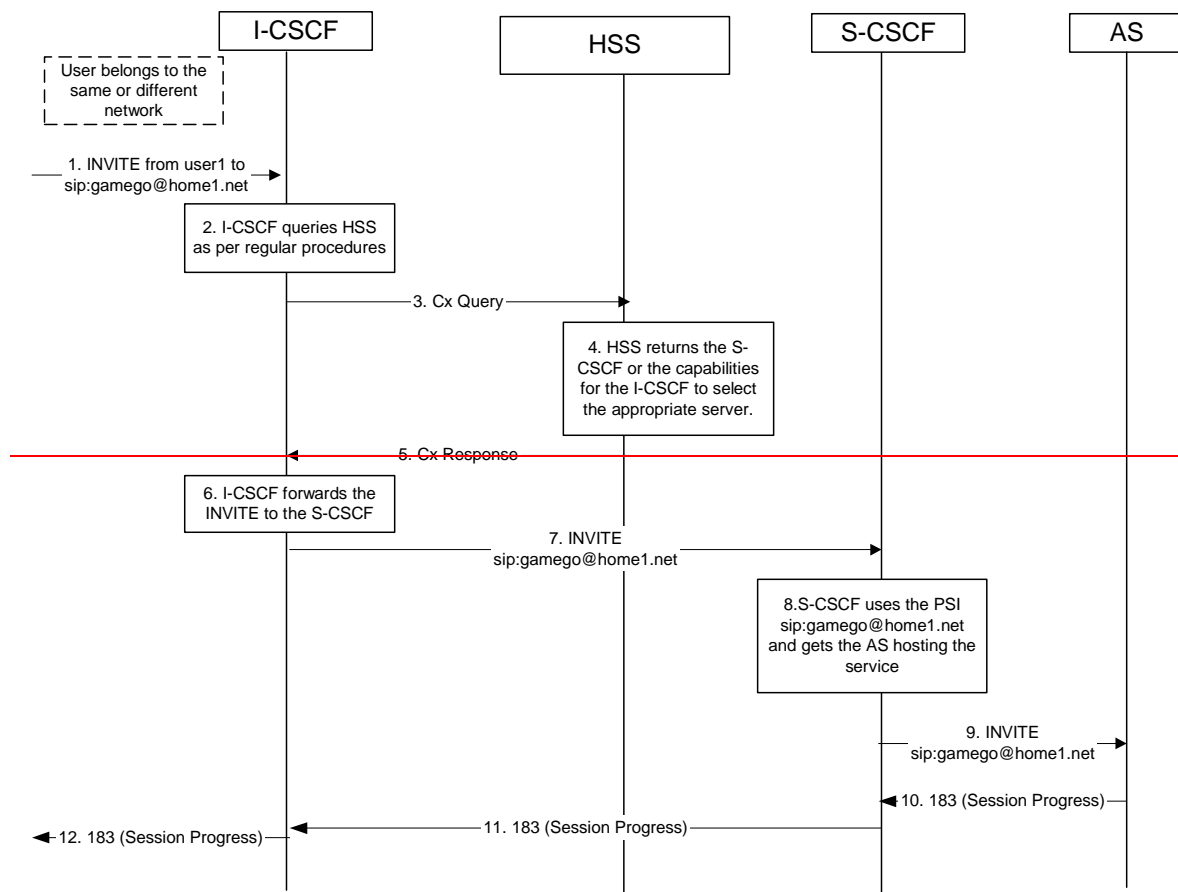
Figure 5.4.12.b: ~~Incoming session, indirect route to AS via S-CSCF~~

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

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

4. ~~HSS determines the routing information, which is the S-CSCF defined for the "PSI user".~~

5. ~~HSS returns the S-CSCF address/capabilities to the I-CSCF.~~

6-7. ~~I CSCF, as per existing procedures, forwards the request towards the entity (i.e., S-CSCF) received from the query, or the I CSCF selects a new S-CSCF if required.~~

8. ~~S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.~~

9. ~~The request is then routed towards the AS identified by the filter criteria.~~

10-12. ~~Session setup continues as per existing procedures.~~

5.4.12.3   Subdomain based PSIs

Subdomains defined for PSIs allow both operators and users to define specific PSIs within subdomains for specific applications. For this purpose, subdomains can be defined by the operator in the DNS infrastructure. Specific PSIs within a subdomain can be created and deleted by users using the Ut interface to the AS hosting the subdomain, or by the operator via O&M mechanisms.

Subdomain based PSIs are globally routable and can be made available to users within and outside the operator domain.

In this case, there are two ways to route towards the AS hosting the PSI:

a) When the subdomain name is defined in the global DNS, then the originating S-CSCF receives the IP address of the AS hosting the PSI, when it queries DNS. The principles defined in RFC 3263 "Session Initiation Protocol (SIP): Locating SIP Servers" may be used. For example, a NAPTR query and then a SRV query may be used to get the IP address of the AS.

b) The PSI is resolved by the global DNS to an I-CSCF address in the domain where the AS hosting the PSI is located. The I-CSCF recognises the subdomain (and thus does not query the HSS). It resolves the same PSI to the address of the actual destination AS hosting the PSI using an internal DNS mechanism, and forwards the requests directly to the AS.

Figure 5.4.12.c5.19f shows an example of DNS based routing of an incoming session from an external network. The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.
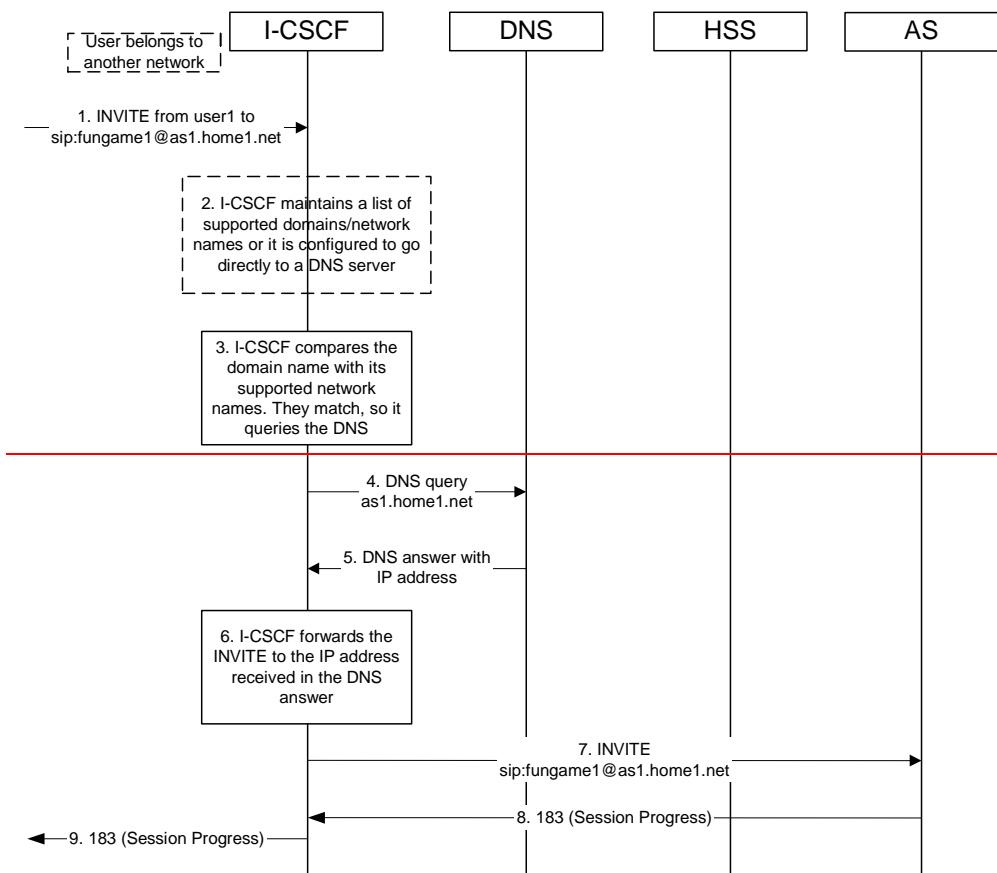

Figure 5.4.12.c: Incoming session, direct route to AS using DNS

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

2. I-CSCF has been configured with the list of supported domains/network names, or it may have been configured to directly query a local DNS server.

3. In this case the I-CSCF checks the list and finds a match.

4. I-CSCF sends DNS query to find the route.

5. DNS server returns the IP address of the AS hosting the PSI.

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

8-9. Session setup continues as per existing procedures.

5.4.12.4 PSI configuration in the HSS

In order to support configuration of an AS hosting a PSI, the distinct PSIs and/or wildcarded PSI ranges hosted in the AS need to be configured in the HSS. The configuration shall include procedures to allow:

- Distinct PSIs and wildcarded PSI ranges to be configured in the HSS via operation and maintenance procedures,

- Authorization and verification of access as "PSI user" with the Public Service Identity hosted by the AS, e.g. for AS-originating requests,

- Access to "PSI user" information (e.g. the S-CSCF assigned) over the Cx reference point from the CSCF nodes,

- Defining the "PSI user" similar to the principle of IMS user, without requiring any subscription/access information (e.g. CS/PS domain data) that are required for IMS user.

Further functional requirements such as how S-CSCF is provisioned with the PSI data need to be studied.

Note that the PSI configuration in the HSS does not affect the filter criteria based access to an AS as defined in the user profiles.

5.4.12.5 Requests originated by the AS hosting the PSI

The AS hosting the PSI may originate requests with the PSI as the originating party. For such originating requests, the home IMS network shall be capable to perform the following functions:

- In case network configuration hiding is to be applied, the request shall be routed as per the principles described in sub-clause 4.6.2.1. This means that the last hop within the originating IMS is an I-CSCF (THIG), which processes the request further on and routes it towards the destination network.

- Network Domain Security [20] shall be used where applicable.

- Charging requirements such as providing appropriate accounting and charging functions via the charging entities shall be supported according to 3GPP TS 32.200 [25].

- In case the target identity is a tel: URL, ENUM translation needs to be performed, and the request shall be routed based on the translation result.

Routing from the Originating AS hosting the PSI can be performed as follows:

a) The AS may forward the originating request to the destination network without involving a S-CSCF. If this option is applied where the target identity is a tel: URL, the AS performs an ENUM query and routes the request based on the translation result. ENUM support for an AS is optional. If an AS does not support ENUM, it shall be configured to use b) at least in case of tel: URLs.

b) In case the PSI has a S-CSCF assigned, the AS forwards the originating request to this S-CSCF, which then processes the request as per regular originating S-CSCF procedures.

To prevent fraudulent or unsecure IMS traffic possibly caused by AS originated requests, security and authentication procedures may be performed towards the AS.

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.
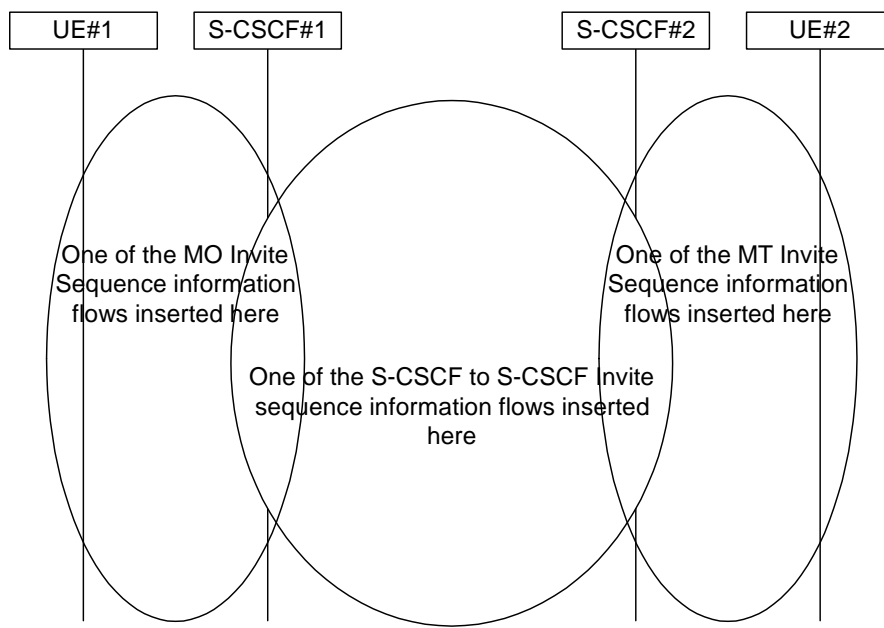
Figure 5.9: Overview of Session Flow Sections

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 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 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 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,	S-S#1 Different network operators	MT#1 Mobile termination,

roaming, home control of services (2). MO#2 Mobile origination, located in home service area. PSTN-O PSTN origination.	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.	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 subclause 5.4a to see which ~~Origination~~ origination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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-O PSTN origination. The ~~"~~"Originating Network~~"~~" of S-S#1 is the home network. The element labeled S-CSCF#1 is the MGCF of the PSTN-O procedure.

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

NI-O　　Non-IMS network origination. The external SIP client of figure 5.16a 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 subclause 5.4a to see which ~~Termination~~ termination sequences ~~that~~ share this common S-S procedure.~~ are:~~ 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 of figure 5.10.

NI-T　　Non-IMS network terminations. The external SIPclient of figure 5.19a 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 subclause 5.4a to see which ~~Origination~~ origination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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-O PSTN 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 5.16c.

Refer to table 5.2 in subclause 5.4a to see which ~~Termination~~ termination sequences ~~that~~ share this common S-S procedure ~~are~~:. 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 of figure 5.11.
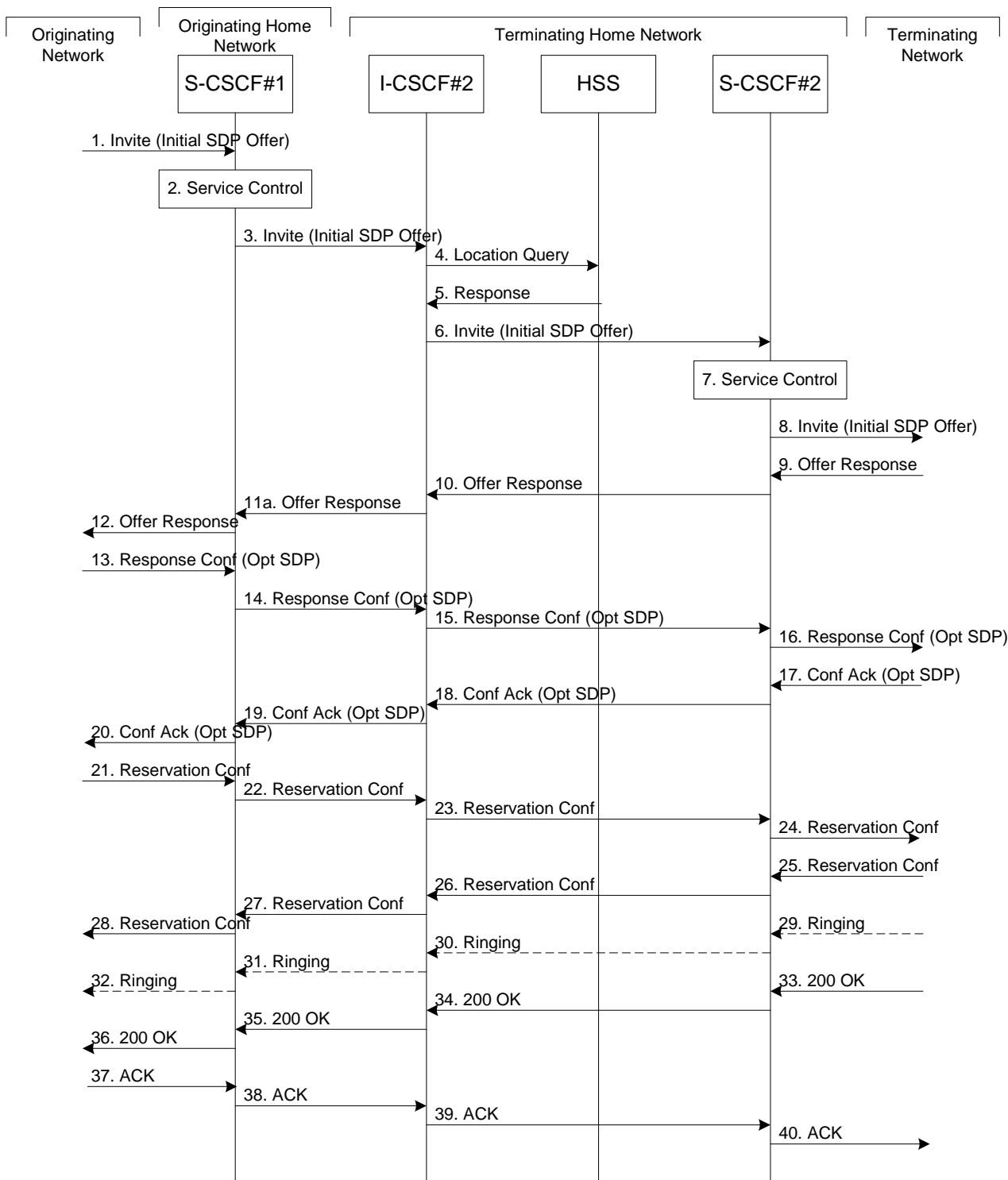
Figure 5.11: Serving to serving procedure - same operator

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 subclause 5.4a to see which oOrigination sequences that share this common S-S procedure are:. 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-OPSTN origination. The "Originating Network" of S-S#3 is the home network. The element labeled 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 5.16c.

Refer to table 5.2 in subclause 5.4a to see which Termination termination sequences that share this common S-S procedure are:. 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.
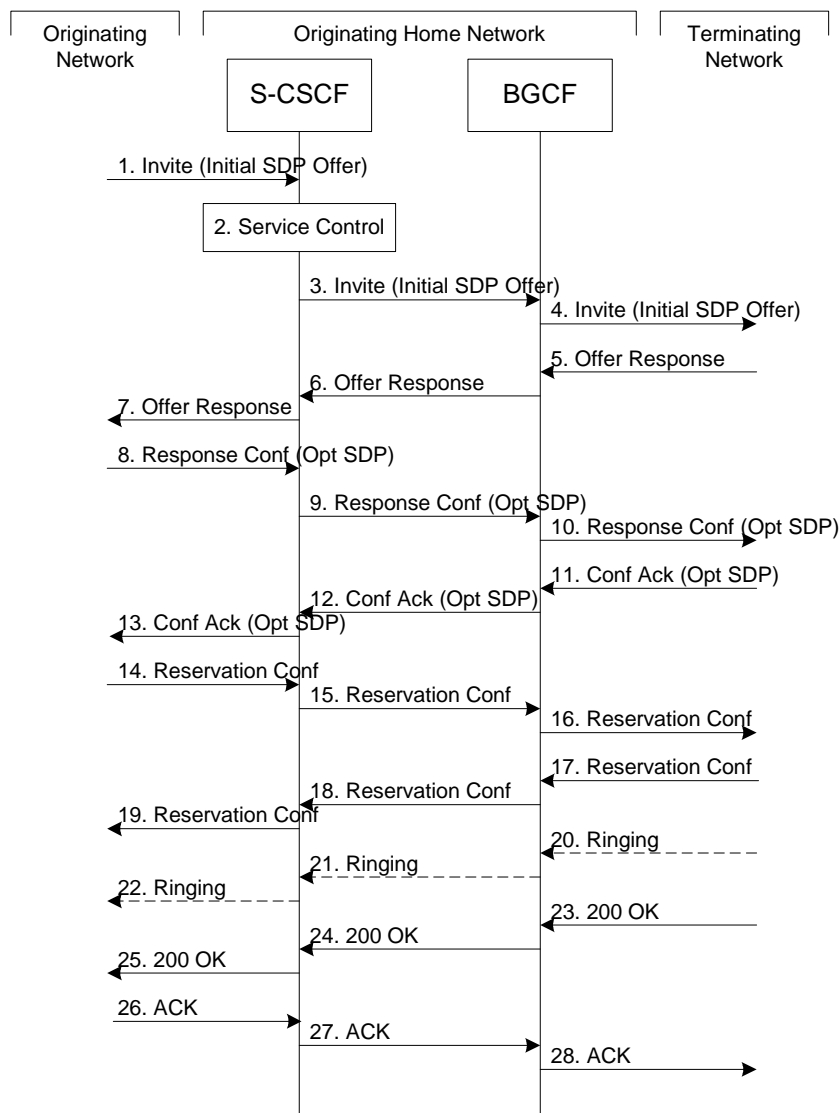
Figure 5.12: Serving to PSTN procedure - same operator

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 subclause 5.4a to see which ~~Origination~~ origination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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 5.16c.

NI-O   Non-IMS network origination. The external SIP client of figure 5.16a 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 5.4a to see which ~~Termination~~ termination sequences ~~that~~ share this common S-S procedure ~~are:~~. 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.
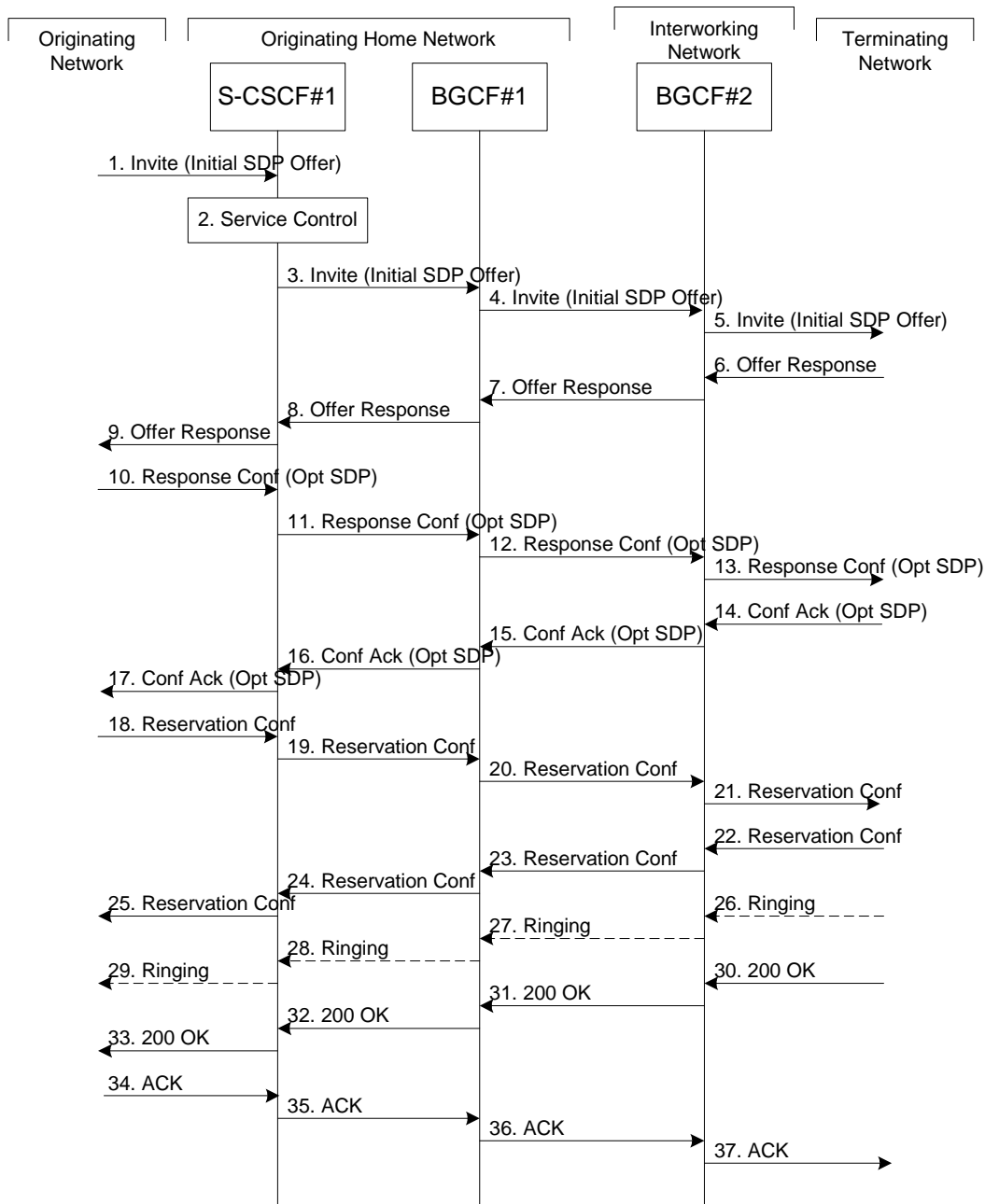
Figure 5.13: Serving to PSTN procedure - different operator

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 originating end answers the session.

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

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

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

This subclause 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 5.19a, 5.19b and 5.19c 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 subclause 5.6.2. The same principles apply in roaming cases, i.e. analogous variants of MO#1 defined in subclause 5.6.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
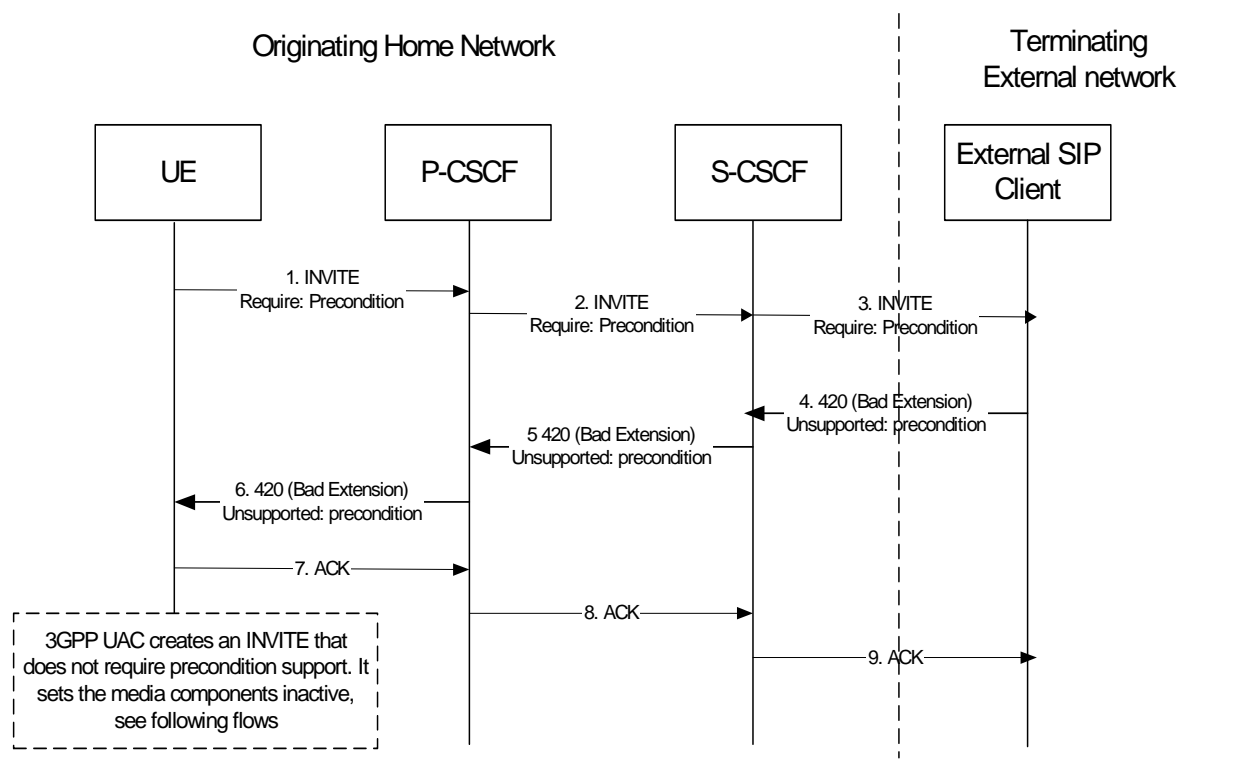
Figure 5.19a: Terminating session towards external SIP client, detection phase

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 5.19b: 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 figures 5.19b & 5.19c.

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.

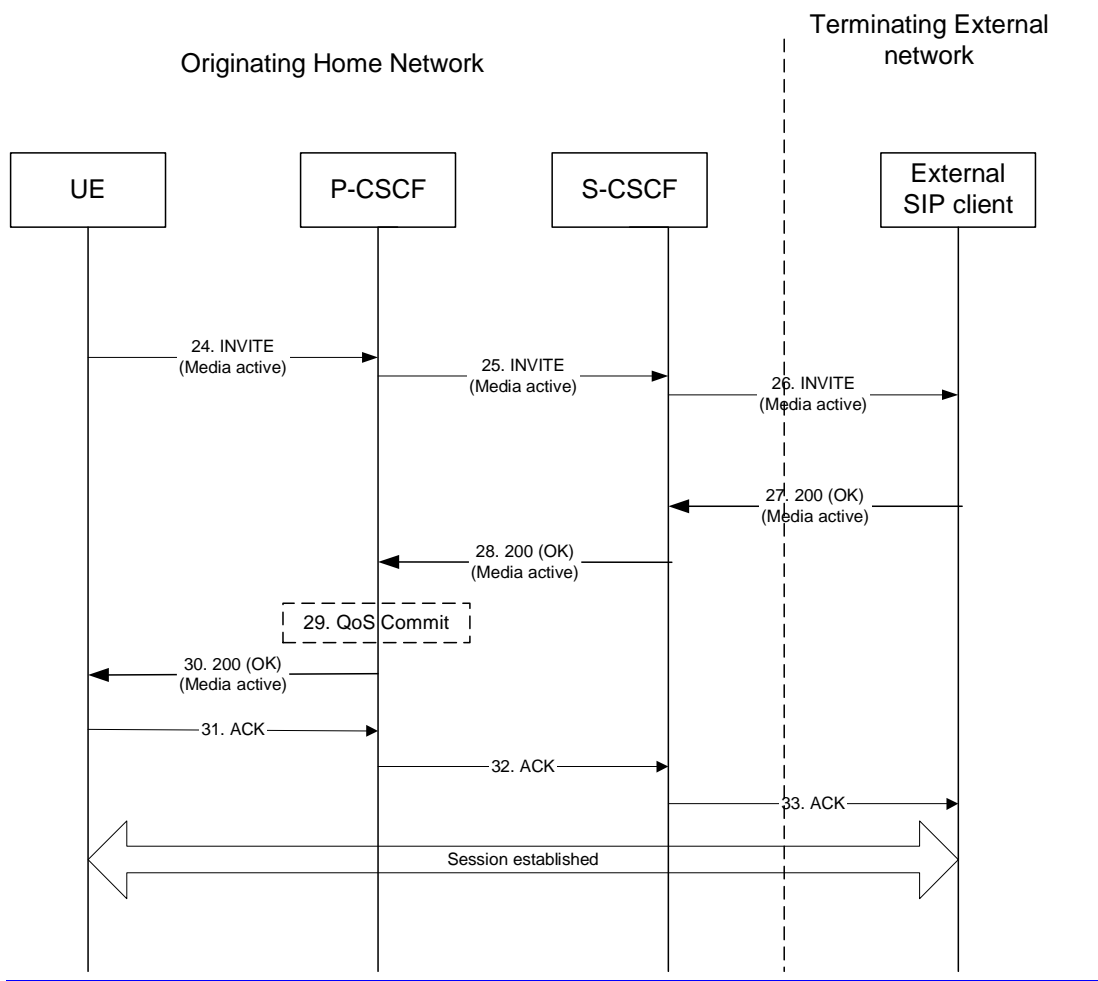23. The UE starts the resource reservation for the media.

Figure 5.19c: 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 5.19c.

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.

This clause describes the terminating session setup procedures 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 parameters have been negotiated and accepted. Session flows 5.19a and 5.19b show 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 clause 5.7.2. The same principles apply in roaming cases, i.e. analogous variants of MT#1 defined in clause 5.7.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
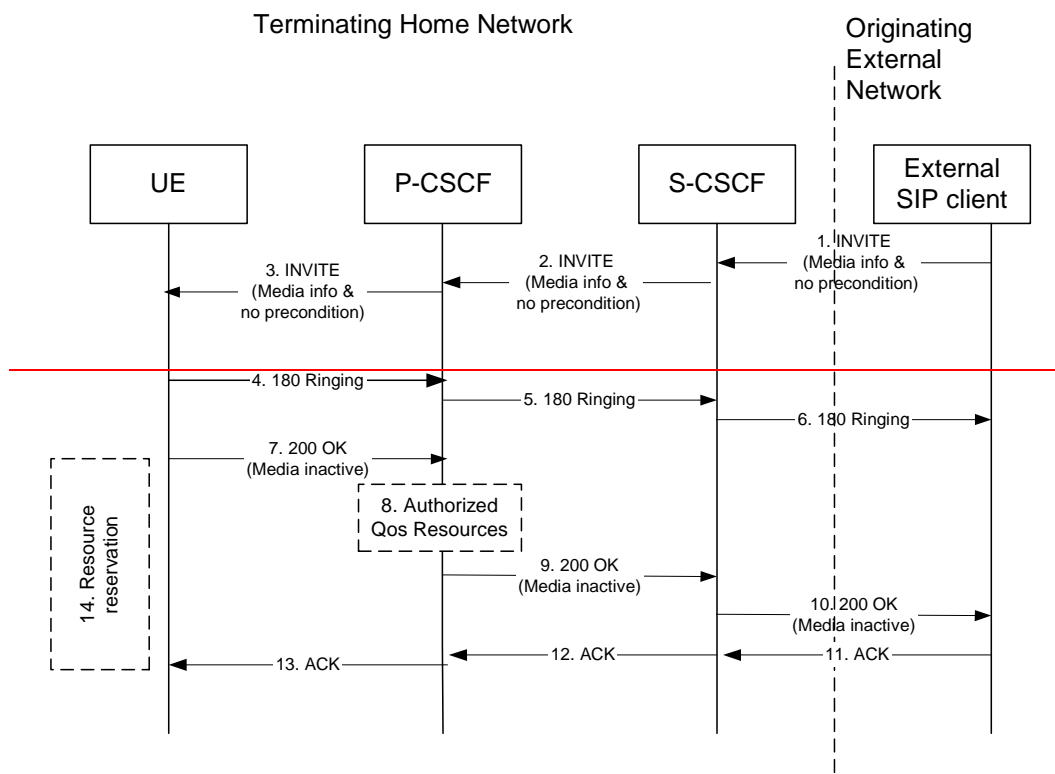
Terminating Home Network

Originating External Network

Figure 5.19a. Terminating session from external SIP client, detection & initial setup with media not allowed

1-3.   A session arrives at the UE in the IMS network with media information but without requiring precondition capability.

4-6.   Ringing information is sent end to end towards the originating party.

7-10.   The UE begins the resource reservation according to the session and media parameters. The P-CSCF/PDF may authorise the media parameters being negotiated and the originating party is notified of the session setup details with all media components set to inactive.

11-13. The originating party acknowledges the session.

14. When the UE has completed the resource reservation procedures, the UE continues with the session setup according to flow 5.19b. The UE sets the media components to active state.
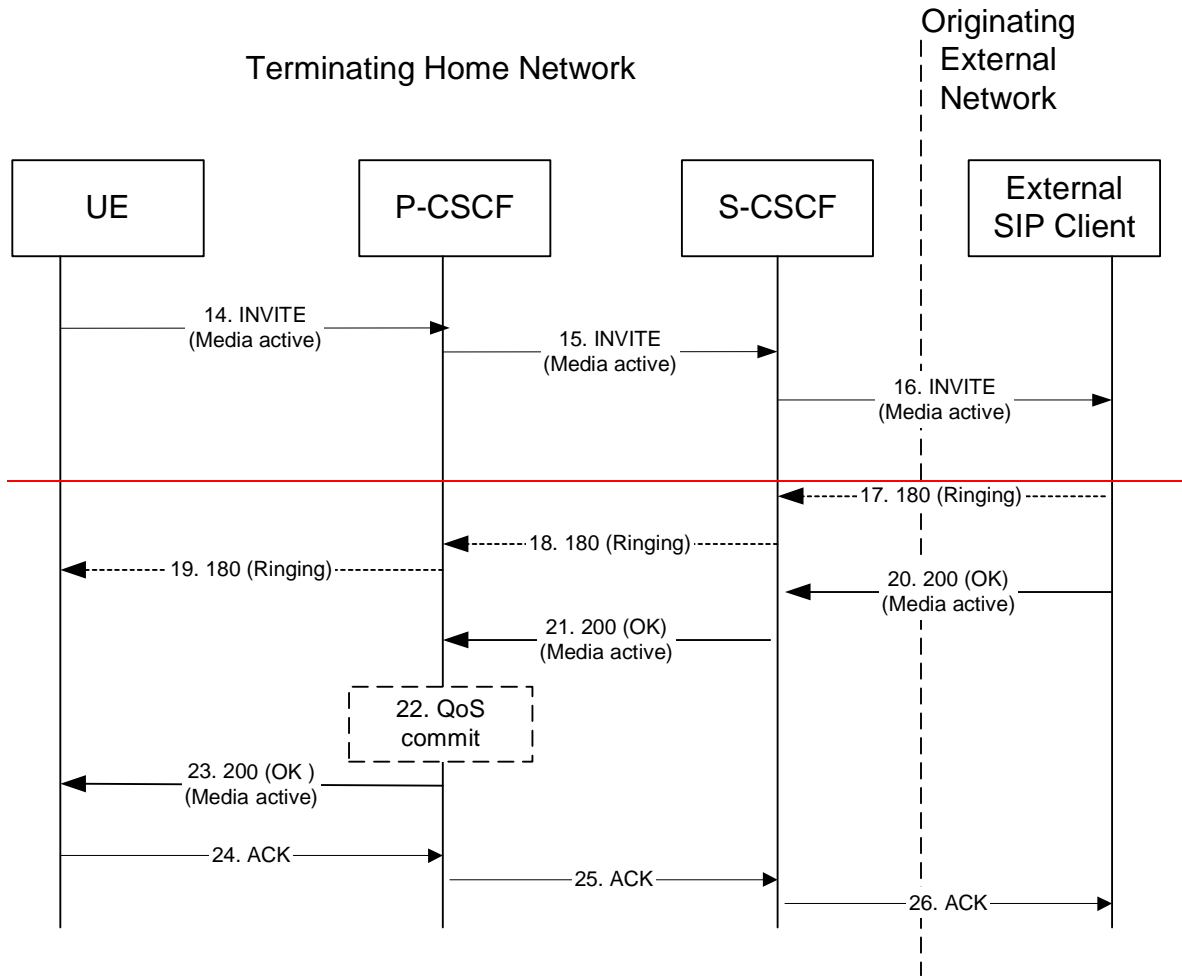
14-16. By sending a re-INVITE indicating the support for the precondition capability, the terminating UE initiates setting of media components to active.

17-19. Ringing Information may be sent from an external SIP entity (in this case the originating party) through the session path towards the terminating UE.

20-23. The originating SIP client accepts the re-INVITE with the active media streams. In step 22, The P-CSCF/PDF may commit/approve the resources authorised for the session.

24-26. Session is acknowledged end-to-end.

5.7.5 (AS-T#1) PSI based Application Server termination – direct

This section depicts a routing example for incoming session where the session request is routed directly to the AS hosting the PSI.
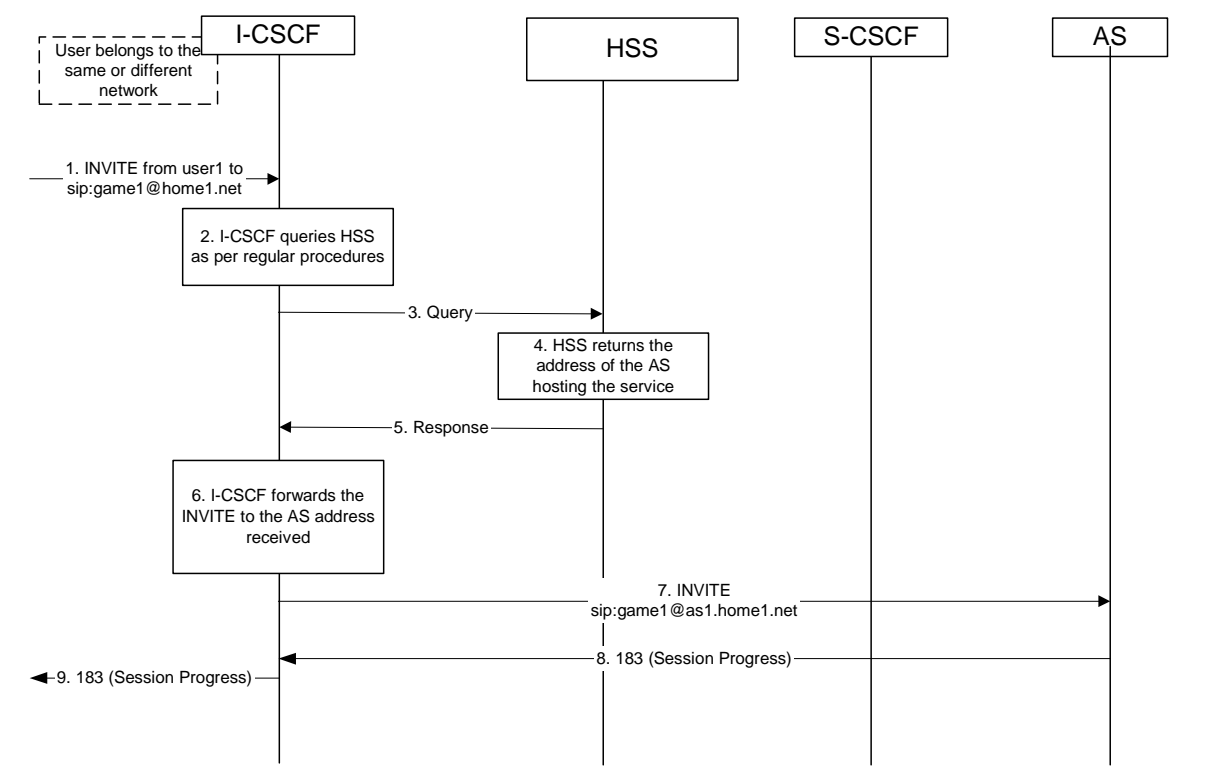
Figure 5.19d Incoming session, direct route towards the AS

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

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

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

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

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

8-9. Session setup continues as per existing procedures.

5.7.6   (AS-T#2) PSI based Application Server termination – indirect

This section depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.
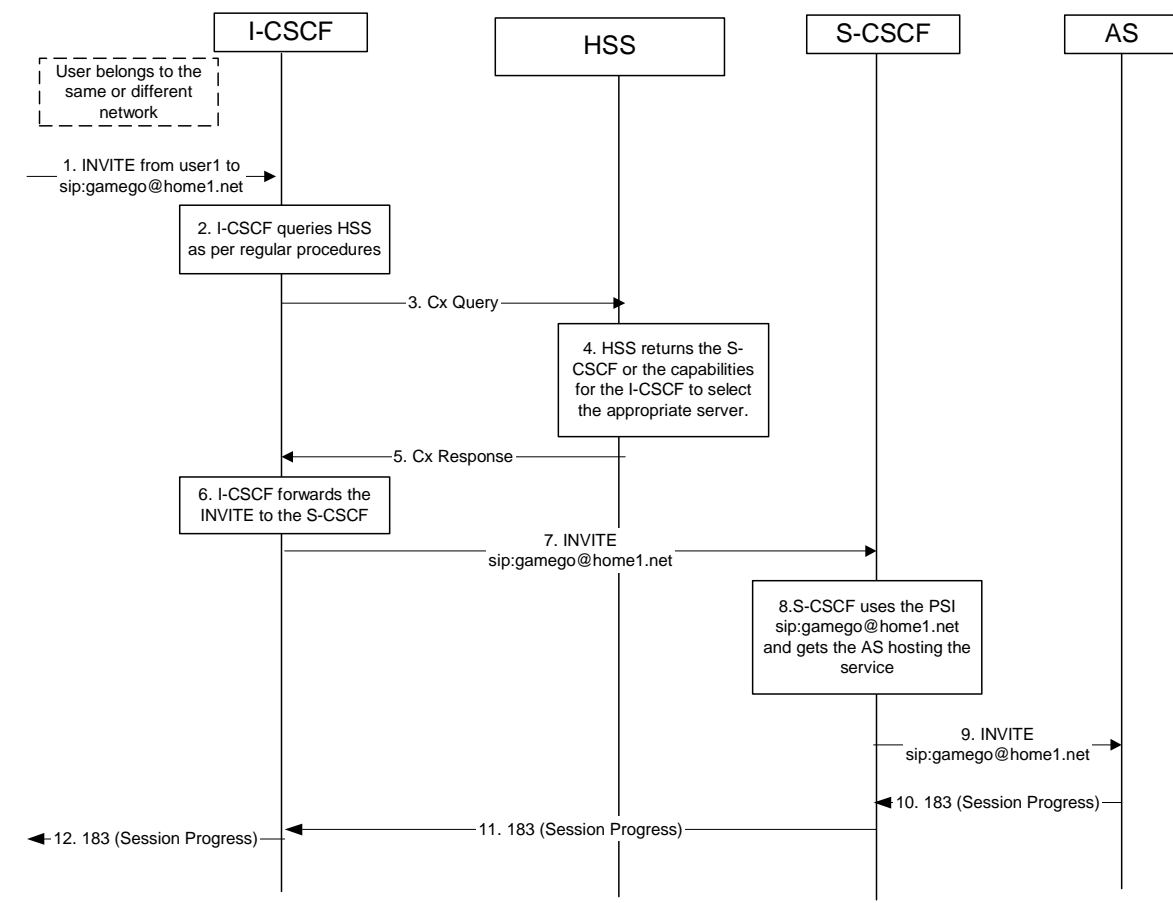
Figure 5.19e: Incoming session, indirect route to AS via S-CSCF

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

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

4. HSS determines the routing information, which is the S-CSCF defined for the "PSI user".

5. HSS returns the S-CSCF address/capabilities to the I-CSCF.

6-7.   I-CSCF, as per existing procedures, forwards the request towards the entity (i.e., S-CSCF) received from the query, or the I-CSCF selects a new S-CSCF if required.

8. S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.

9. The request is then routed towards the AS identified by the filter criteria.

10-12. Session setup continues as per existing procedures.

5.7.7   (AS-T#3) PSI based Application Server termination – DNS routing

This section shows an example of DNS based routing of an incoming session from an external network. The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.
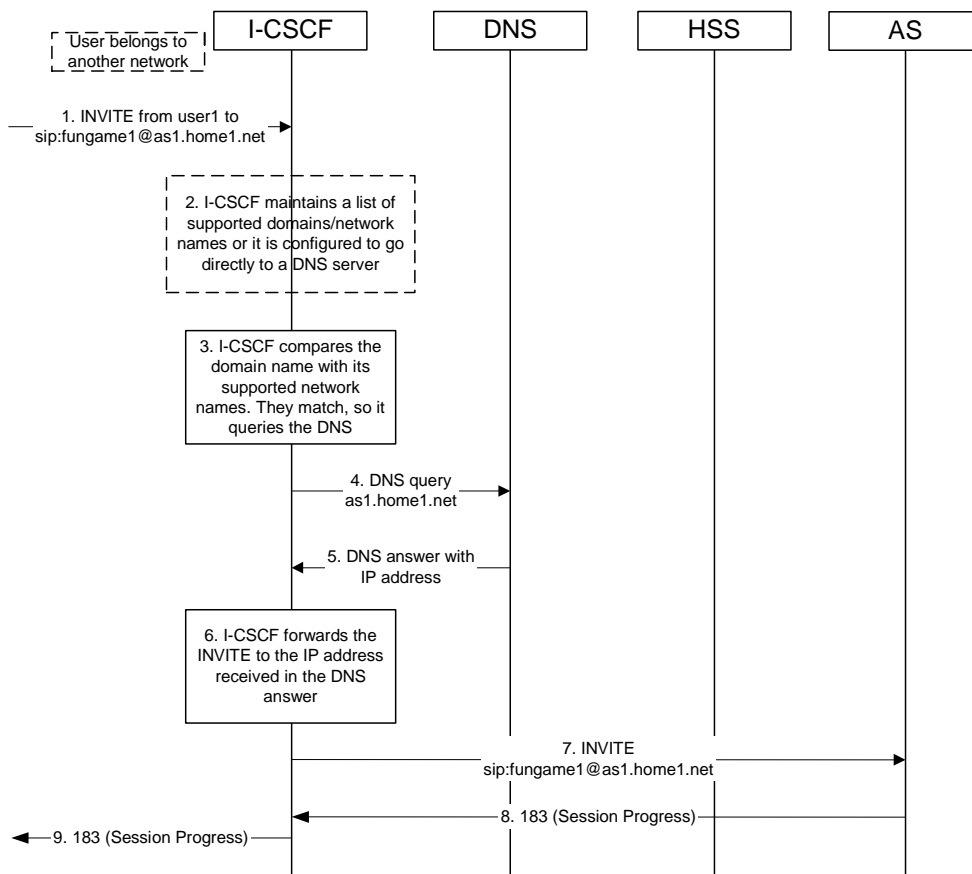
Figure 5.19f: Incoming session, direct route to AS using DNS

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

2. I-CSCF has been configured with the list of supported domains/network names, or it may have been configured to directly query a local DNS server.

3. In this case the I-CSCF checks the list and finds a match.

4. I-CSCF sends DNS query to find the route.

5. DNS server returns the IP address of the AS hosting the PSI.

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

8-9. Session setup continues as per existing procedures.