3GPP TSG-SA Meeting #19
Birmingham, UK, 17-20.3.2003

SP-030181
(revised SP-030172)

CR-Formv7

CHANGE REQUEST

✍ **23.228** **CR** **280** ✍**rev** **3** ✍ Current version: **6.0.1** ✍

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

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

Title:	✍	Combined CR for CR#264 and CR#280rev1
Source:	✍	Ericsson, Lucent, Nokia, Nortel, Qualcomm, Siemens
Work item code:	✍	IMS2 and IMSCOOP
Date:	✍	17/03/2003
Category:	✍	**D**
Release:	✍	Rel-6

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

Use one of the following releases:

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

Reason for change: ✍

CR#264 and CR#280rev1 approved at SA2#29 and SA2#30, respectively, have some parts that overlap with eachother. TheCR#280rev3 resolves these overlaps by combining the CRs.

CR280r1: As the basic stage-2 IMS specification, TS 23.228 defines the architectural description for the IP Multimedia Core Network Subsystem (IMS). It also covers the Access Network functionality and GPRS aspects to the extent as they relate to providing IMS services.

To better facilitate the documentation aspects of interoperability and commonality between IP Multimedia Systems using different IP-Connectivity Access Networks, there is a need to clearly separate the specification of Access Network (GPRS) specific functionality.

CR264: The call flows for the P-CSCF initiated session release have to be updated and clarified due to the following reasons:

- GPRS and SBLP specific mechanisms are already covered by other specifications (23.060 and 23.207).
- The P-CSCF decision on the session release should be shown as a separate step due to a variety of impacts (e.g. type of service, timers, policies).
- A separation of P-CSCF actions related to the indication from GPRS and actions related to the potential session release is necessary.

Some minor updates are necessary to utilize the GPRS and SBLP specific mechansims in the correct way.

Summary of change: ✍ The changes brought in by CR#264 are incorporated into CR#280r1, the result is the present CR#280rev3.

	CR280r1: A new normative annex has been created for documenting the GPRS-access specific concepts that relate to the provisioning of IMS services. The relevant text from throughout clause 1-5 of the TS has been moved into this annex or to TS 23.221. In clauses defining IMS-level concepts (1-5), the GPRS-specific terminology has been changed to a more generic terminology where applicable. CR 264: The following changes are proposed: - A sentence is added to section 5.10.3.0 correlating this section with the network initiated session release mechanisms. - Some minor additions and corrections to the text of section 5.10.3.1 are made. - The call flows for the P-CSCF initiated session release are updated by deleting interactions already described by 23.060 and 23.207. - A new step is added in which the P-CSCF decides about the session release. The actions of the P-CSCF/PDF related to the received indication and the potential session release are separated and completed.
Consequences if not approved:	CRs 264 and 280r1 would be overlapping. CR280r1: The goal of specifying interoperability and commonality between IP Multimedia Systems using different "IP-Connectivity Access Networks" required by the corresponding Work Item would be impossible to achieve. CR264: Duplication of desciptions in different specifications may lead to inexactness and maintenance difficulties. The existing call flows do not cover possible dependencies between different bearers as well as the resulting actions. Furthermore, the actions necessary after the decision for a session release are incomplete.

Clauses affected:	Contents, 4, 4.2.1.2, 4.2.3, 4.2.5, 4.2.5.1, 4.2.6, 4.3.1, 4.3.3.1, 4.3.3.2, 4.3.3.4, 4.5, 4.6.1, 5.1.0, 5.1.1, 5.1.1.1, 5.1.1.2, 5.2.1, 5.2.2.2, 5.2.2.3, 5.3.2.1, 5.3.2.2, 5.4.1, 5.4.4, 5.4.6.3, 5.4.7, 5.4.7.1, 5.4.7.1a, 5.4.7.2, 5.4.7.3, 5.4.7.4, 5.4.7.5, 5.4.7.6, 5.4.7.7, 5.4.8, 5.6, 5.6.1, 5.6.2, 5.6.3, 5.7, 5.7.1, 5.7.2, 5.7.3, 5.10.1, 5.10.2, 5.10.3.0, 5.10.3.1, 5.10.3.1.1, 5.10.3.1.2, 5.10.3.2, 5.11.1.1, 5.11.1.2, 5.11.3.1, 5.11.3.2, 5.11.3.3, 5.11.3.4, 5.11.5.6, 5.13 New Clause created with several sub-clauses: Annex X (normative)			
Other specs Affected:	**Y**	**N**		
	X		Other core specifications	TS 23.221
		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

3GPP TS 23.228 V6.0.1 (2003-01)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
IP Multimedia Subsystem (IMS);
Stage 2
(Release 6)

Keywords
UMTS, multimedia, packet mode, IP

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

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 ~~in UMTS~~. 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 ~~or GPRS aspects~~ except as they relate to provision of IM services, these aspects are covered in the normative Annex X. The 3GPP TS 23.060 contains GPRS Access Network description and the 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] RFC 3261: "SIP: Session Initiation Protocol"

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

Refer to TS 23.002 [1] for the definitions of some terms used in this document.

For the purposes of the present document the following additional definitions apply.

IP-Connectivity Access Network: refers to the collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities. ~~: refers to any reference points in the architecture that provide IP connectivity between any two or more IP capable nodes; e.g. Gm, Gi, Mw.~~ An example of an "IP-Connectivity Access Network" is GPRS.

Subscriber: A Subscriber is an entity (comprising one or more users) that is engaged in a Subscription with a service provider. The subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of user authorised to enjoy these services, and also to set the limits relative to the use that users make of these services.

3.2 Symbols

For the purposes of the present document the following symbols apply:

Cx	Reference Point between a CSCF and an HSS.
Dx	Reference Point between an I-CSCF and an SLF.
Gi	Reference point between GPRS and an external packet data network Gm Reference Point between a UE and a P-CSCF.
ISC	Reference Point between a CSCF and an Application Server.Iu Interface between the RNS and the core network. It is also considered as a reference point.
Le	Reference Point between an AS and a GMLC
Mb	Reference Point to IPv6 network services.
Mg	Reference Point between an MGCF and a CSCF.
Mi	Reference Point between a CSCF and a BGCF.
Mj	Reference Point beetween a BGCF and an MGCF.
Mk	Reference Point betweeen a BGCF and another BGCF.
Mm	Reference Point between a CSCF and an IP multimedia network.
Mr	Reference Point between an CSCF and an MRFC.
Mw	Reference Point between a CSCF and another CSCF.
Sh	Reference Point between an AS (SIP-AS or OSA-CSCF) and an HSS.
Si	Reference Point between an IM-SSF and an HSS.

3.3 Abbreviations

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

AMR	Adaptive Multi-rate
API	Application Program Interface
AS	Application Server
BCSM	Basic Call State Model
BG	Border Gateway
BGCF	Breakout Gateway Control Function
BS	Bearer Service
CAMEL	Customised Application Mobile Enhanced Logic
CAP	Camel Application Part
CDR	Charging DataRecord
CN	Core Network
CS	Circuit Switched
CSCF	Call Session Control Function
CSE	CAMEL Service Environment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENUM	E.164 Number
GGSN	Gateway GPRS Support Node
GMLC	Gateway Mobile Location Centre
HSS	Home Subscriber Server
I-CSCF	Interrogating-CSCF
IETF	Internet Engineering Task Force
IM	IP Multimedia
IM CN SS	IP Multimedia Core Network Subsystem
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IP-CAN	IP-Connectivity Access Network
ISDN	Integrated Services Digital Network
ISIM	IMS SIM
ISP	Internet Service Provider
ISUP	ISDN User Part
MAP	Mobile Application Part
MGCF	Media Gateway Control Function

MGF	Media Gateway Function
NAI	Network Access Identifier
OSA	Open Services Architecture
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PDN	Packet Data Network
PDP	Packet Data Protocol e.g., IP
PEF	Policy Enforcement Function
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAB	Radio Access Bearer
RFC	Request for Comments
SCS	Service Capability Server
S-CSCF	Serving-CSCF
SGSN	Serving GPRS Support Node
SLF	Subscription Locator Function
SSF	Service Switching Function
SS7	Signalling System 7
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SGW	Signalling Gateway
THIG	Topology Hiding Inter-network Gateway
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URL	Universal Resource Locator
USIM	UMTS SIM

4 IP multimedia subsystem concepts

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

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

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

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

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

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

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

4.2 IMS services concepts

4.2.1 Home-network based services

4.2.1.1 Support of CAMEL

It shall be possible for an operator to offer access to services based on the CSE for its IM CN subsystem subscribers. It should be noted that there is no requirement for any operator to support CAMEL services for their IM CN subsystem subscribers or for inbound roamers.

For more information refer to section 4.2.4.

4.2.1.2 Support of OSA

It shall be possible for an operator to offer access to services based on OSA for its IM CN subsystem subscribers. This shall be supported by an OSA API between the Application Server (AS) and the network.

For more information refer to section 4.2.4.

4.2.2 Support of Local Services in the IMS

Visited network provided services offer an opportunity for revenue generation by allowing access to services of a local nature to visiting users (inbound roamers). There shall be a standardised means to access local services. The mechanism to access local services shall be exactly the same for home users and inbound roamers.

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) 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.

4. The S-CSCF routes the session, via normal SIP routing, towards its destination (eg a server in the VPLMN). 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.

4.2.3 Support of roaming users

The architecture shall be based on the principle that the service control for Home subscribed services for a roaming subscriber is in the Home network, e.g., the Serving-CSCF is located in the Home network.

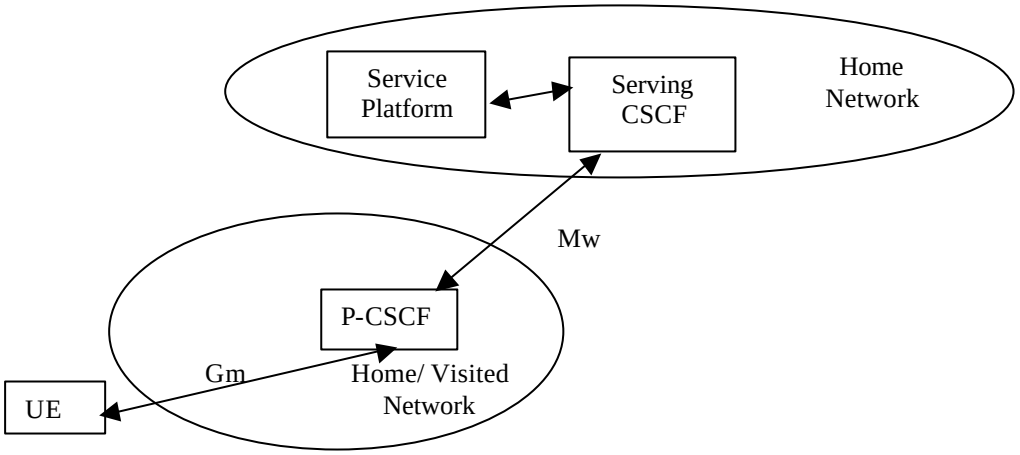


Figure 4-1: Service Platform in Home Network

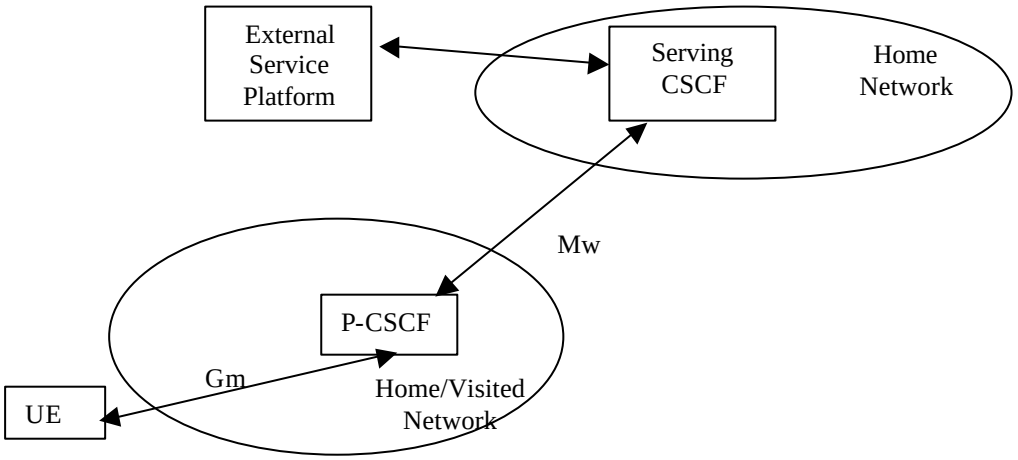


Figure 4-2: External Service Platform

There are two possible scenarios to provide services:

- via the service platform in the Home Network

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

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

The roles that the CSCF plays are described below.

- ~~The Proxy-CSCF is located in the same network as the GGSN.~~ The Proxy-CSCF shall enable the session control to be passed to the Serving-CSCF.

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

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

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

Network initiated Proxy-CSCF reassignment is not a requirement.

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

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 S-CSCF shall decide whether an Application Server is required to receive information related to an incoming SIP session 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.

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.

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.

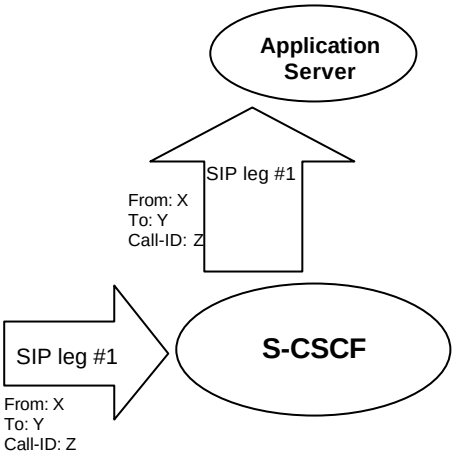


Figure 4.3a: Application Server acting as terminating UA, or redirect server

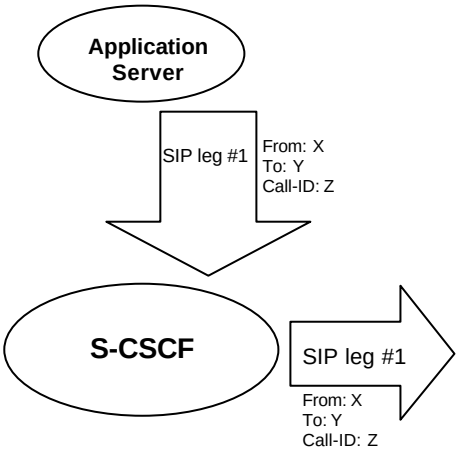


Figure 4.3b: Application Server acting as originating UA

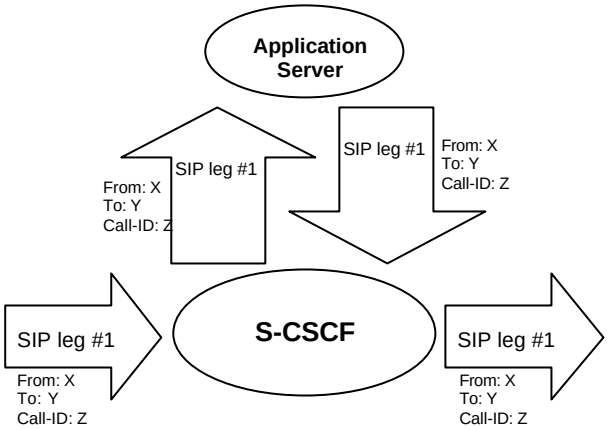


Figure 4.3c: Application Server acting as a SIP proxy

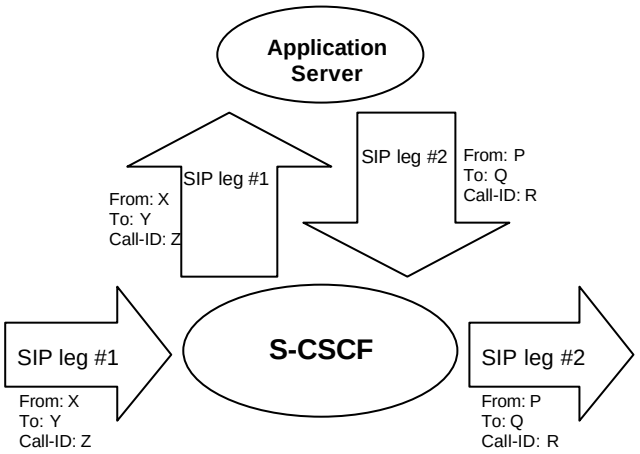


Figure 4.3d: Application Server performing 3rd party call control

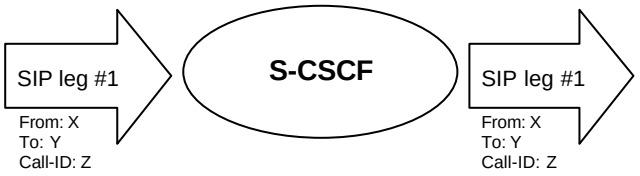


Figure 4.3e: A SIP leg is passed through the S-CSCF without Application Server involvement

4.2.4a HSS to service platform Interface

The "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" 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.

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.

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

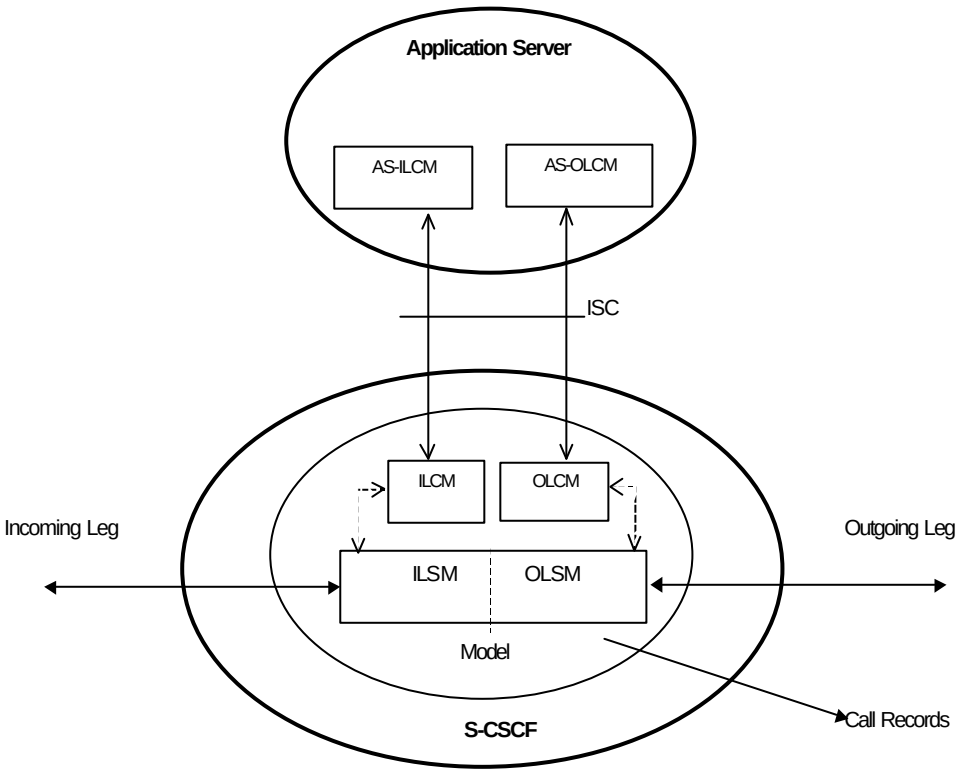


Figure 4.3f: Service Control Model with Incoming Leg Control and Outgoing Leg Control

Figure 1 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 1) 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 1) 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 ~~services or the Background QoS Class~~.

~~3. QoS Signalling at Different Bearer Service Control Levels~~

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

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

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

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

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

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

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

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

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 ~~UMTS BS~~IP-Connectivity Access Network (i.e. layer-2) Level

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

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

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

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

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

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

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

7. The Efficiency of QoS Signalling and Resource Allocation

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

8. Dynamic QoS Negotiation and Resource Allocation

   Changes (upgrading or downgrading) of QoS provided to an active IMS session shall be supported based on either the request from the IM application or the current network loads or ~~radio~~ 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 ~~GPRS~~ 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 ~~GPRS~~ packet data and circuit switched services.

4.2.5.1 ~~Relation of IMS media components and PDP contexts carrying IMS media~~Void

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

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

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

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

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

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

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

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

4.2.6 QoS Requirements for IM CN subsystem signalling

The UE shall be able to establish ~~a~~ dedicated ~~signalling PDP Context~~ IP-CAN bearer for IM Subsystem related signalling or utilize a general-purpose ~~PDP context~~ IP-CAN bearer for IM subsystem signalling traffic. ~~The application level signalling flag is used to indicate the dedicated signalling PDP context. If the network operator does not support a dedicated signalling PDP context, the network will consider the PDP context as a general purpose PDP context.~~

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

~~.~~ If ~~the the~~ a dedicated ~~signalling PDP context~~ 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 ~~GGSN~~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 ~~Release 5~~this Release for providing the information about the restrictions back to the UE, the available set of rules and restrictions in this Release ~~5~~ is the set of capabilities as defined below.

The dedicated ~~signalling PDP context is~~ IP-CAN bearer is subject to restrictions, the capabilities to be applied ~~is~~ are defined as follows: all messages from the UE ~~on the Signalling PDP Context~~ that use a dedicated 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 ~~GGSN and~~ P-CSCF ~~are~~ is located.

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

4.2.7 Support of SIP forking

SIP forking is the ability of a SIP proxy server to fork SIP request messages to multiple destinations according to [12]. ~~3GPP~~ CSCFs and ASes that behave according to this version of the specification shall not fork any request.

Other networks outside the IM CN Subsystem are able to perform SIP forking. Hence, ~~3GPP~~ UEs 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 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 shall acknowledge the 200 OK and cancel other early dialogues that may have been established. The UE may require updating the allocated resources according to the resources needed. In case the UE receives a subsequent 200 OK, the UE shall acknowledge the dialogue and immediately send a BYE to drop the dialog.

The UE shall be able to include preferences, in INVITE's, indicating that proxies should not fork the INVITE request.

On the terminating side, a UE shall be able to receive, as specified in [12], several requests for the same dialog that were forked by a previous SIP entity.

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].

~~According to the procedures defined in TS 23.060 [23], w~~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, any change to the IP address that is used to access the IM CN subsystem shall trigger automatic registration in order to update the UE's IP address.

~~The ability of the User plane and the Control Plane for a single session being able to pass through different GGSNs is not defined in this release.~~

4.3.2 Void

Figure 4.4: Void

4.3.3 Identification of users

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

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 (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 Identitys 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).

~~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 (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.~~

4.3.3.3 Routing of SIP signalling within the IP multimedia subsystem

Routing of SIP signalling within the IMS shall use SIP URLs. 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 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 dialing plan and prefix. The IMS will interpret the phone number with a leading '+' to be fully defined international number.

Support for local services and local dialling plans are not specified in the present document.

4.3.3.4 Relationship of private and public user identities

The home network operator is responsible for the assignment of the private user identifier, and public user identifiers; other identities that are not defined by the operator may also exist.

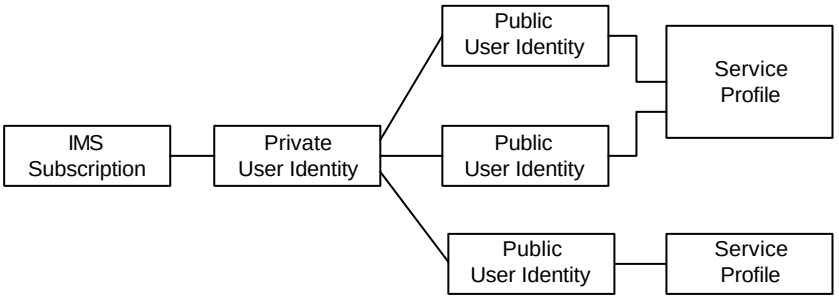


Figure 4.5: Relationship of the private user identity and public user identities

The IMS Service Profile is a collection of service and user related data as defined in 3GPP TS 29.228 [30]. The Service Profile is independent from the Implicit Registration Set, e.g. IMPUs with different Service Profiles may belong to the

same Implicit Registration Set. Initial filter criteria in the service profile provide a simple service logic comprising of user / operator preferences that are of static nature i.e. they do not get changed on a frequent basis.

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

The IMS Service profile is defined and maintained in the HSS and its scope is limited to IM CN Subsystem. The service profile is downloaded from the HSS to the S-CSCF.Only one service profile per Public user identity is downloaded to the S-CSCF at a given time (such as at registration, update of a profile etc.) based on the Public user identities being served by the S-CSCF. Nothing precludes that multiple service profiles can be defined in the HSS for a subscription. Each Public user identity is associated with one and only one Service Profile. Each service profile is associated with one or more Public user identities.

All Service Profiles that share the same Private user identity are associated to the same S-CSCF. Later releases may allow different Service Profiles that share the same Private user identity to be associated with different S-CSCFs.

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.

~~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].~~

It is not a requirement for a user to be able to register on behalf of another user 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.

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 Name to address 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.

4.4 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 CSCF and BGCF (Mi)

- Between BGCF and MGCF (Mj)
- 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 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.

4.5 Mobility related concepts

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

The following procedures are supported by an UE when accessing IMS:

?? Connect to the IP-CAN ~~core network using GPRS procedures~~ and acquire the necessary IP address ~~via activation of a PDP context~~, which includes, or is followed by, the P-CSCF discovery procedure;

?? Register to the IM subsystem as defined by the IMS registration procedures;

?? If an UE explicitly deactivates ~~a PDP context~~ the IP-CAN bearer ~~-~~ that is being used for IMS signalling, it shall first de-register from the IMS (while there is no IMS session in progress);

?? If an UE explicitly deactivates ~~a PDP context~~ the IP-CAN bearer ~~-~~ that is being used for IMS signalling while an IMS session is in progress, the UE must first release the session and de-register from the IMS and then deactivate the ~~PDP context~~ IP-CAN bearers;

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

?? In order to be able to deliver an incoming IMS session, the ~~PDP context~~ IP-CAN bearer ~~-~~ that is being used for IMS signalling need to remain active as long as the UE is registered in the IM CN subsystem;

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

4.6 Roles of Session Control Functions

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

4.6.1 Proxy-CSCF

The Proxy-CSCF (P-CSCF) is the first contact point within the IM CN subsystem. Its address is discovered by UEs ~~following PDP context activation~~, using the mechanism described in section "Procedures related to Local CSCF Discovery ". The P-CSCF behaves like a Proxy (as defined in RFC 3261 [12] or subsequent versions), i.e. it accepts requests and services them internally or forwards them on. The P-CSCF shall not modify the Request URI in the SIP

INVITE message. The P-CSCF may behave as a User Agent (as defined in the RFC 3261 [12] or subsequent versions), i.e. in abnormal conditions it may terminate and independently generate SIP transactions.

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

The functions performed by the P-CSCF are:

- Forward the SIP register request received from the UE to an I-CSCF determined using the home domain name, as provided by the UE.
- Forward SIP messages received from the UE to the SIP server (e.g. S-CSCF) whose name the P-CSCF has received as a result of the registration procedure.
- Forward the SIP request or response to the UE.
- Detect and handle an emergency session establishment request as per error handling procedures defined by stage-3.
- Generation of CDRs.
- Maintain a Security Association between itself and each UE, as defined in TS 33.203 [19].
- Should perform SIP message compression/decompression.
- Authorisation of bearer resources and QoS management. For details see TS 23.207 [9].

4.6.2 Interrogating-CSCF

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

Registration

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

Session-related and session-unrelated flows

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

Charging and resource utilisation:

- Generation of CDRs.

4.6.2.1 Topology Hiding Inter-network Gateway

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

4.6.3 Serving-CSCF

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

Registration

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

Session-related and session-unrelated flows

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

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

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

- Interaction with Services Platforms for the support of Services

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

- On behalf of an originating endpoint (i.e. the originating user/UE)

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

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

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

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

- On behalf of a destination endpoint (i.e. the terminating user/UE)

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

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

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

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

Charging and resource utilisation:

- Generation of CDRs.

4.6.4 Breakout Gateway Control Function

The Breakout Gateway control function (BGCF) selects the network in which PSTN/CS Domain breakout is to occur. If the BGCF determines that the breakout is to occur in the same network in which the BGCF is located within, then the BGCF shall select a MGCF which will be responsible for the interworking with the PSTN/CS Domain. If the break out is in another network, the BGCF will forward this session signalling to another BGCF in the selected network.

The functions performed by the BGCF are:

- Receives request from S-CSCF to select appropriate PSTN/CS Domain break out point for the session

- Select the network in which the interworking with the PSTN/CS Domain is to occur. If the interworking is in another network, then the BGCF will forward the SIP signalling to the BGCF of that network. If the

interworking is in another network and network hiding is required by the operator, the BGCF will forward the SIP signaling via an I-CSCF(THIG) toward the BGCF of the other network.

- Select the MGCF in the network in which the interworking with PSTN/CS Domain is to occur and forward the SIP signalling to that MGCF. This may not apply if the interworking is a different network.

- Generation of CDRs.

The BGCF may make use of information received from other protocols, or may make use of administrative information, when making the choice of which network the interworking shall occur.

4.7 Multimedia Resource Function

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

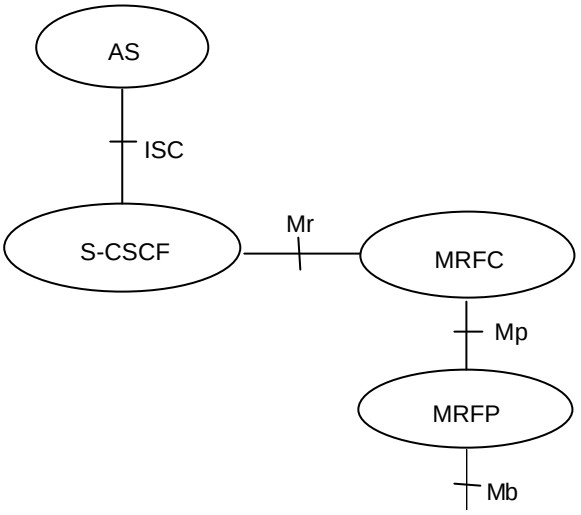


Figure 4.5a: Architecture of MRF

The MRF is split into Multimedia Resource Function Controller (MRFC) and Multimedia Resource Function Processor (MRFP).

Tasks of the MRFC are the following:

- Control the media stream resources in the MRFP.
- Interpret information coming from an AS and S-CSCF (e.g session identifier) and control MRFP accordingly.
- Generate of CDRs.

Tasks of the MRFP are the following:

- Control of the bearer on the Mb reference point .
- Provide resources to be controlled by the MRFC.
- Mixing of incoming media streams (e.g for multiple parties).
- Media stream source (for multimedia announcements).
- Media stream processing (e.g. audio transcoding, media analysis).

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

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

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

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

The Mp reference point has the following properties:

- Full compliance with the H.248 standard.
- Open architecture where extensions (packages) definition work on the interface may be carried out.

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

4.8 Security Concepts

IM CN Subsystem functional elements provide security, as needed, by security methods defined in 3GPP TS 32.203[19] and TS 33.210 [20]. If interacting with external Networks, Security Associations are provided in accordance with operator policy.

4.9 Charging Concepts

IM CN subsystem functional elements provide support for offline and online charging. This includes support for charging correlation, e.g. between IM CN subsystem and PS domain. The charging architecture, charging principles and charging data for IM CN subsystem are described in 3GPP TS 32.200 [25] and 3GPP TS 32.225 [26]. The charging correlation information between IM CN subsystem and PS domain are also described in 3GPP TS 24.229 [10a] and 3GPP TS 29.207 [11a].

5 IP multimedia subsystem procedures

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

5.0 Session-unrelated procedures

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

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

5.1 CSCF related procedures

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

Before the UE can request IM services, appropriate IP-CAN bearer ~~a PDP context~~ must be available ~~activated~~ to carry IM Subsystem related signalling.

~~It shall be possible for the UE to convey to the network the intention of using the PDP context for IM Subsystem related signalling. For this purpose it uses the mechanism for 'PDP Context Used for Application Level Signalling Transport' as described in TS23.207. A signalling flag determines any rules and restrictions that shall apply at the GGSN for that PDP context, as described in section 4.2.6. It shall not be possible to modify a general purpose PDP context into a dedicated PDP context for IM Subsystem related signalling and vice versa.~~

~~The QoS profile parameters for this PDP context are appropriate for IM Subsystem related signalling. The QoS profile parameters are detailed in TS23.107. The signalling flag and the QoS profile parameters may be used independently of each other.~~

5.1.1 Procedures related to local CSCF discovery

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

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

- Alternatively, the P-CSCF discovery may be perfomed after the IP connectivity has been established. To enable P-CSCF discovery after the establishment of IP connectivity, the IP-Connectivity Access Network shall provide the following P-CSCF discovery option to the UE:~~after GPRS attach and after or as part of a successful activation of a PDP context for IMS signalling using one of the following mechanisms~~:

  ~~1.~~ Use of DHCP to provide the UE with the domain name of a Proxy-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the Proxy-CSCF name, as described below in clause 5.1.1.1.

~~2. Transfer a Proxy-CSCF address within the PDP Context Activation signalling to the UE, as described below in clause 5.1.1.2. The UE shall request the P-CSCF address(es) from the GGSN when activating the PDP context. The GGSN shall send the P-CSCF address(es) to the UE when accepting the PDP context activation. Both the P-CSCF address(es) request and the P-CSCF address(es) shall be sent transparently through the SGSN.~~

5.1.1.1 DHCP/DNS procedure for P-CSCF discovery

The DHCP relay agent within the IP-Connectivity Access Network ~~GGSN acts as a DHCP Relay Agent, relaying~~ relays DHCP messages between UE and the DHCP server.

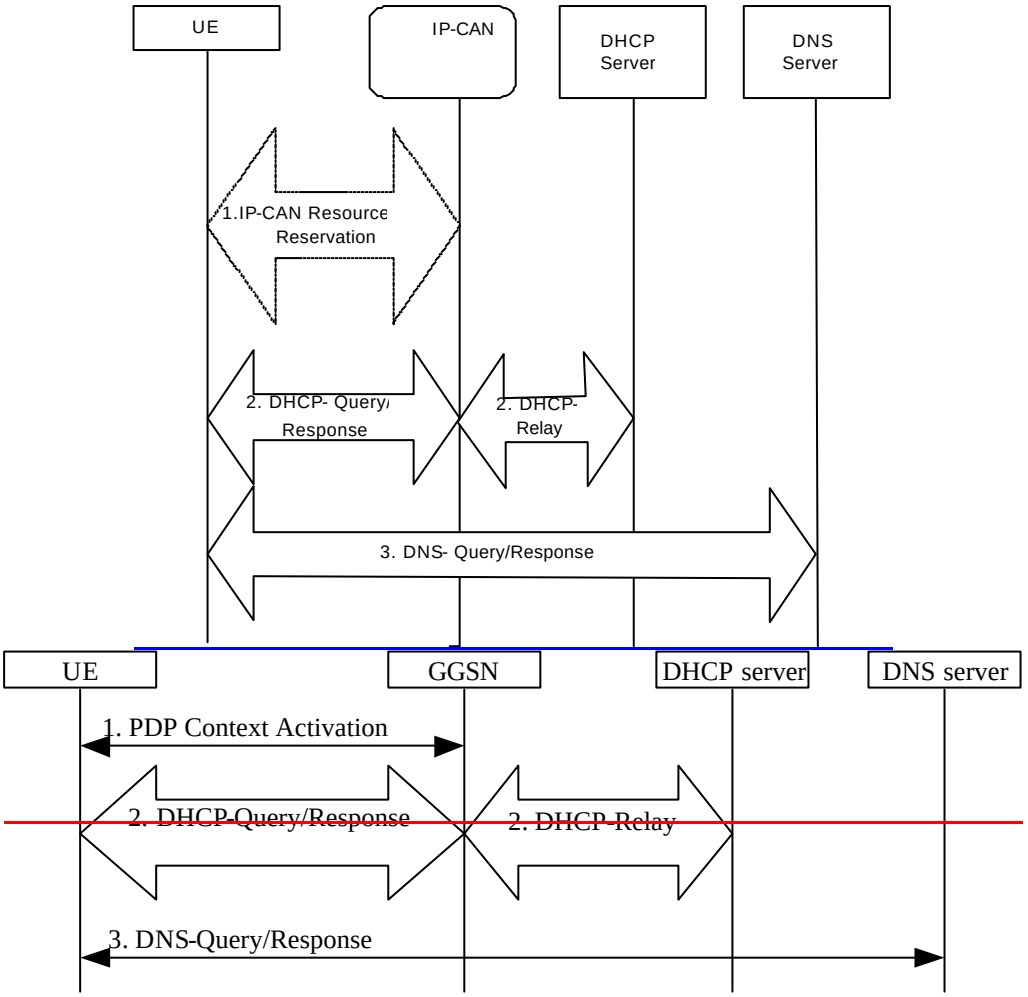


Figure 5.0a: P-CSCF discovery using DHCP and DNS

1. ~~Create~~Reserve ~~PDP context~~ IP-Connectivity Access Network bearer if not already available ~~bearer~~ by using the procedures ~~as specified in TS 23.060~~available in the IP-Connectivity Access Network.

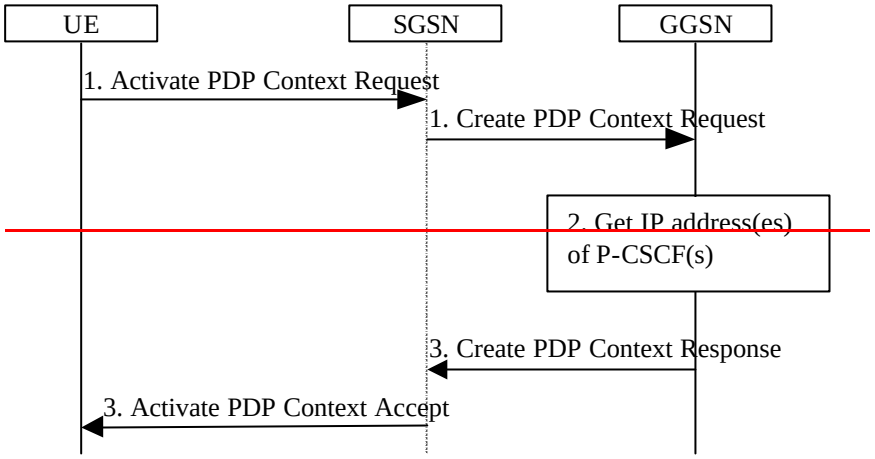
2. The UE requests a DHCP server and additionally requests the domain name of the P-CSCF and IP addresses of DNS servers. It may require a multiple DHCP Query/Response message exchange to retrieve the requested information.

3. The UE performs a DNS query to retrieve a list of P-CSCF(s) IP addresses from which one is selected. If the response does not contain the IP addresses, an additional DNS query is needed to resolve a Fully Qualified Domain Name (FQDN) to an IP address.

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

5.1.1.2 ~~GPRS procedure for P-CSCF discovery~~Void

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



~~**Figure 5.0b: P-CSCF discovery using PDP Context Activation signalling**~~

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

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

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

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

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

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 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, 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. supplementary service parameters, application server address, triggers etc.

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

- 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 supplementary 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

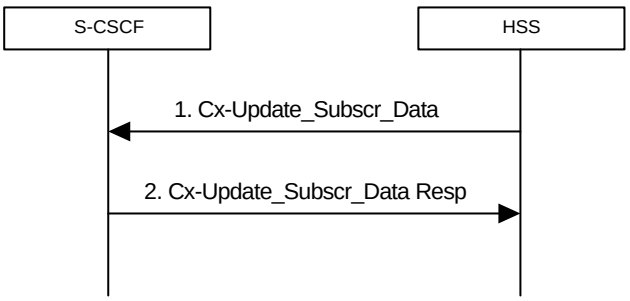
The routing of the SIP registration information flows shall not take into account previous registrations (i.e., registration state). The routing of the session information flows (e.g., INVITE) shall take into account the information received during the registration process.

5.1.5 Subscription Updating Procedures

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

5.1.5.1 Subscription updating information flow

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



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

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

5.2 Application level registration procedures

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 understands a service profile and the address of the functionality of the Proxy-CSCF.

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.

~~-In order to support pre-Rel-5 UICC accessing IMS services, a temporary public user identity is generated using IMSI. It is strongly recommended that the temporary public user identity be set to barred for IMS non-registration procedures.~~

~~8. 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~~

~~9~~8. It shall be possible to register multiple public identities via single IMS registration procedure from the UE.

5.2.1a Implicit Registration

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

?? HSS has the set of public user identities that are part of implicit registration.

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

?? When one of the public user identities within the set is registered, all Public user identities associated with the implicit registration are registered at the same time.

?? When one of the public user identities within the set is de-registered, all public user identities that have been implicitly registered are de-registered at the same time.

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

?? When a public user identity belongs to an implicit registration set, it can not be registered or de-registered individually without the public user identity being removed from the implicit registration list.

?? All IMS related registration timers should apply to the set of implicitly registered public user identities

?? S-CSCF, P-CSCF and UE shall be notified of the set of public user identities belonging to the implicitly registered function. Session set up shall not be allowed for the implicitly registered public user identities until the entities are updated, except for the explicitly registered public user identity.

?? When a public user identity is barred from IMS communications, only the HSS and S-CSCF shall have access to this public user identity,

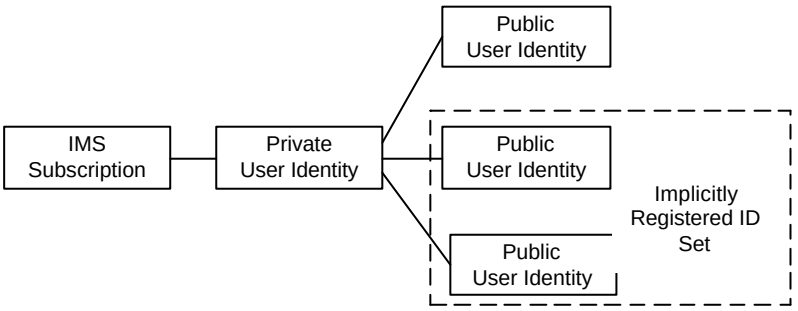


Figure 5.2.1a Relationship of public user identities when implicitly registered

5.2.1a.1 Implicit Registration for UE without ISIM

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

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

?? It shall be defined in HSS that if the user does not have implicit registration activated then the user shall not be allowed to register in the IMS using the Temporary public user identity.

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 ~~Radio~~ bearer~~s are~~ 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) 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.

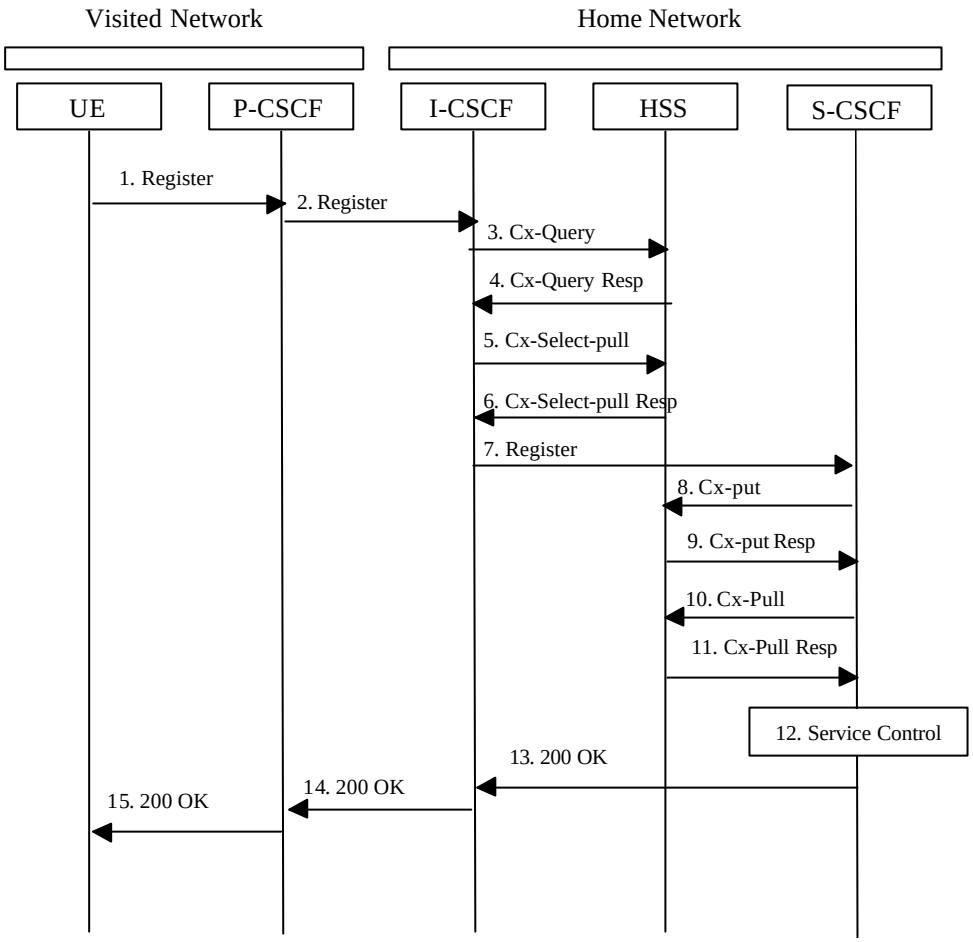


Figure 5.1: Registration – User not registered

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

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

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

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

4. Cx-Query Resp 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 will continue proceeding according to step 5. If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt.

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

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

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

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

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

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

11. The HSS shall return the information flow 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.

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

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

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

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

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

5.2.2.4 Re-Registration information flow – User currently registered

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

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

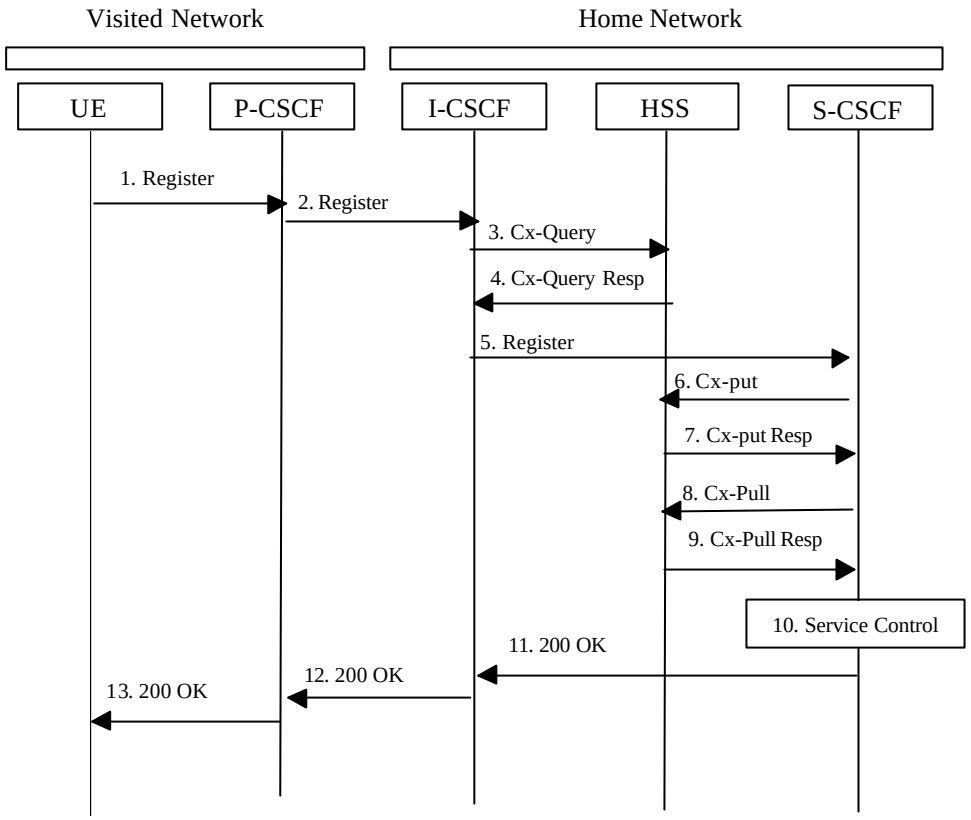


Figure 5.2: Re-registration - user currently registered

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

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

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

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

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

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

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

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

9. The HSS shall return the information flow Cx-Pull-Resp (user information) to the S-CSCF. The S-CSCF shall store the user information for that indicated user.

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

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

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

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

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

5.2.2.5 Stored information.

Table 5.1 provides an indication of the information stored in the indicated nodes during and after the registration process.

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 Same as before registration
Proxy-CSCF - in local 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”.

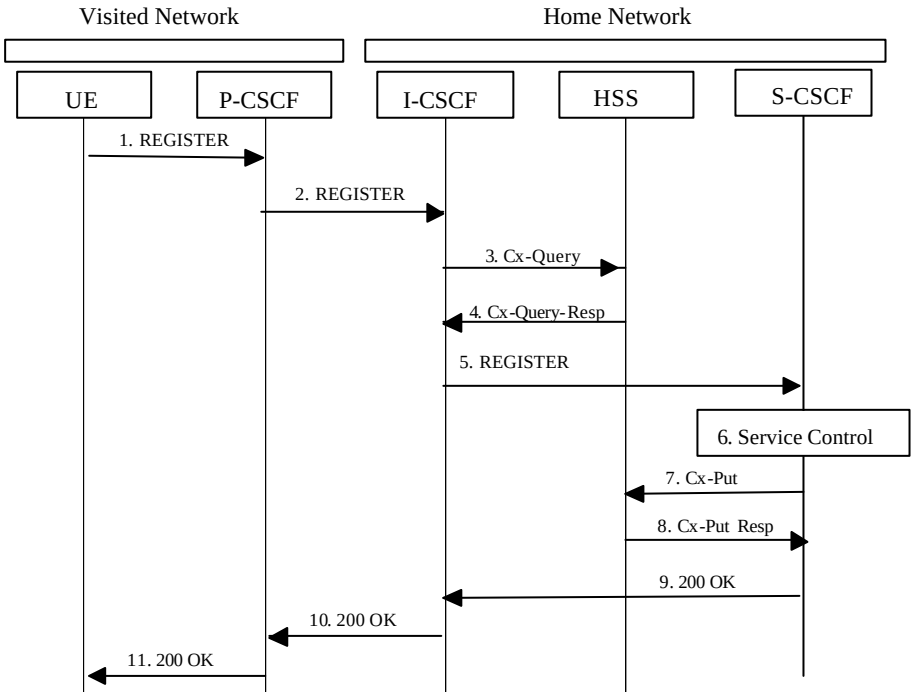


Figure 5.3: De-registration - user currently registered

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 identity, private user identity, home network domain name, UE IP address).

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

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

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

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

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

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

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

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

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

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

5.3.2 Network initiated de-registration

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

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

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

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

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

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

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

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

- To deal with registrations expirations.

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

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

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

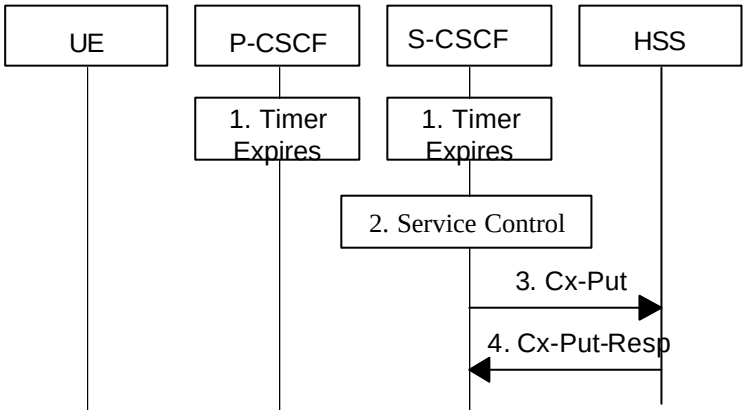


Figure 5.4: Network initiated application de-registration, registration timeout

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

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

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

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

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

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

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

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

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

5.3.2.2.1 Network Initiated De-registration by HSS, administrative

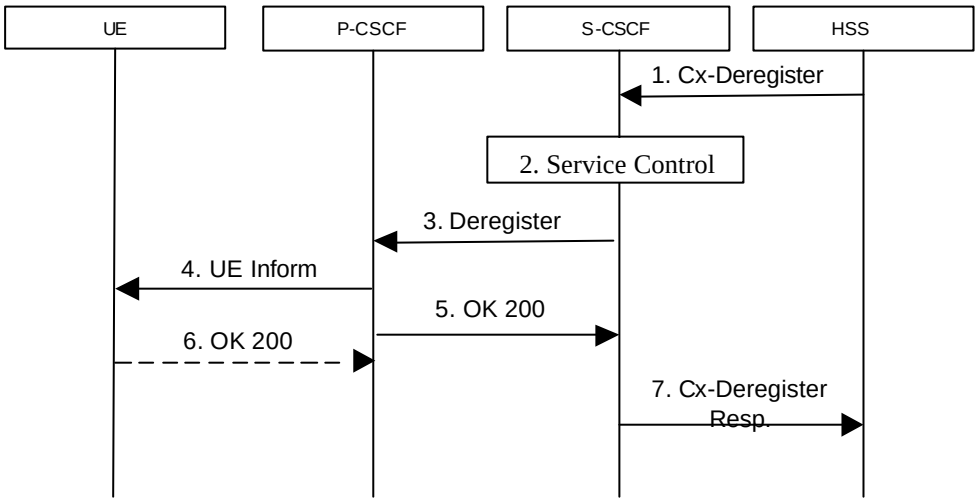


Figure 5.5: Network initiated application de-registration by HSS, administrative

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

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

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

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

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

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

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

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

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

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

5.3.2.2.2 Network Initiated De-registration by S-CSCF

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

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

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

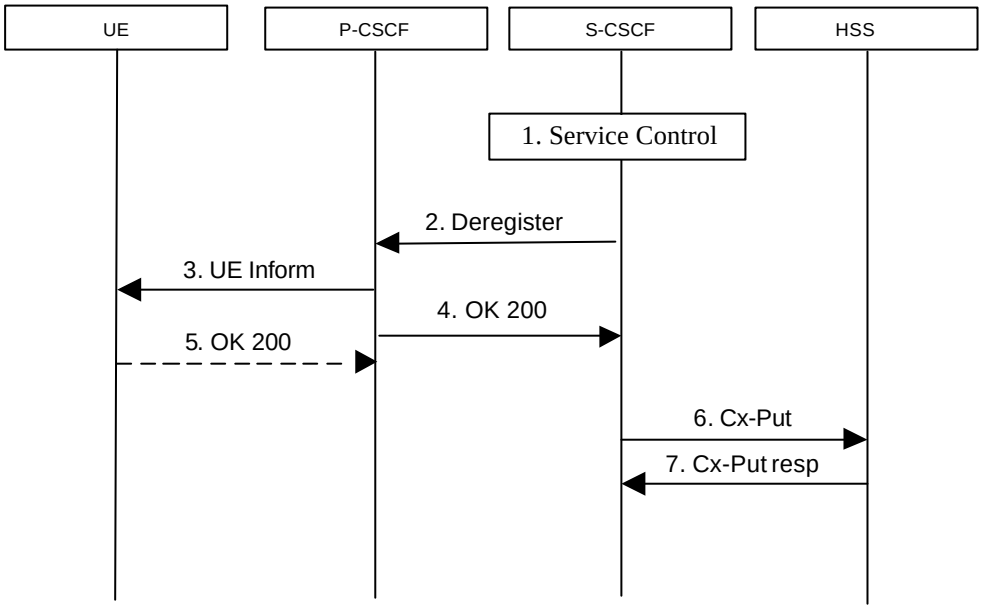


Figure 5.5a: Network initiated application de-registration, service platform

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

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

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

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

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

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

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

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

7. The HSS confirms the update.

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

5.4 Procedures for IP multi-media sessions

Basic sessions between mobile users will always involve two S-CSCFs (one S-CSCF for each). A basic session between a user and a PSTN endpoint involves an S-CSCF for the UE, a BGCF to select the PSTN gateway, and an MGCF for the PSTN.

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

5.4.1 Bearer interworking concepts

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

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

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

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

5.4.2 Interworking with Internet

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

5.4.3 Interworking with PSTN

The S-CSCF, possibly in conjunction with an 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.

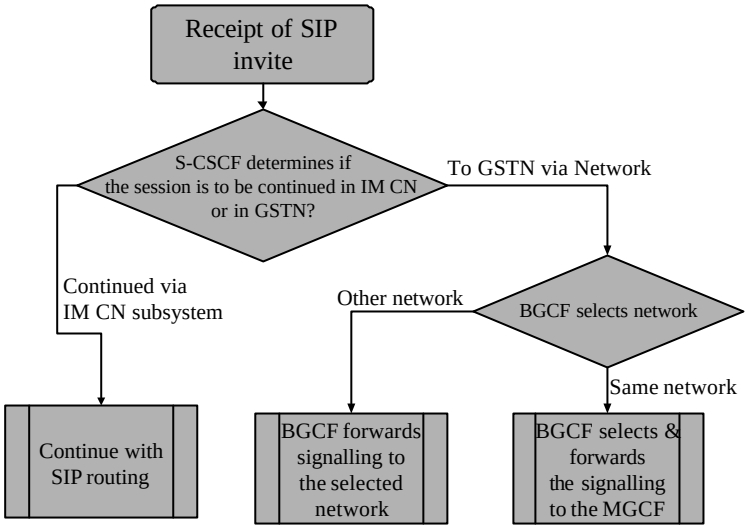


Figure 5.6: Network based PSTN interworking breakout process

5.4.4 Requirements for IP multi-media session control

In order for operators to be able to offer a "carrier-grade" IP multimedia service, and to require bearers whose features (e.g. Bandwidth) are coherent with the media components negotiated through CSCFs, the following features shall be offered:

1. Both end points of the session shall be able to negotiate (according to service /UE settings,) which resources (i.e. which media components) need to be established before the destination party is alerted. The session signalling shall ensure that these resources (including IP-Connectivity Access Network resources and IP multimedia backbone resources) are made available or reserved before the destination UE rings.

   This should nevertheless not prevent the UE from offering to the end-user the choice of accepting or rejecting the components of the session before establishing the bearers.

2. Depending on regulatory requirements, the IP multimedia service shall be able to charge the originating party for the ~~Access IP connectivity~~IP-Connectivity Access Network ~~-~~service of both originating and destination side or when reverse charging applies to charge the terminating party for the IP-Connectivity Access Network ~~Access IP connectivity~~ service of both originating and terminating side. This implies that it should be easy to correlate CDR held by the IP-Connectivity Access Network ~~Access IP connectivity~~ service (e.g. GPRS) with a session.

3. The session control function of IP multimedia network of an operator (CSCF) shall be able (according to operator choice) to have a strict control (e.g. on source /destination IP address, QoS) on the flows associated with session established through SIP entering the IP multimedia bearer network from IP-Connectivity Access Network ~~Access IP connectivity~~ service. This does not mean that CSCF is the enforcement point (which actually is the Gateway between the ~~Access IP connectivity service~~IP-Connectivity Access Network and the IP multimedia network~~, i.e. the GGSN in GPRS case~~) but that the CSCF may be the final decision point for this control.

4. The session control and bearer control mechanisms shall allow the session control to decide when user plane traffic between end-points of a SIP session may start/shall stop. This allows this traffic to start/stop in synchronisation with the start/stop of charging for a session.

5. The ~~Access IP connectivity service~~IP-Connectivity Access Network service shall be able to notify the IP multimedia session control when ~~Access IP connectivity~~the IP-Connectivity Access Network ~~-~~service has either modified or suspend\ed or released the bearer(s) of a~~n~~ user associated with a session (because e.g. the user is no longer reachable).

6. The solution shall comply with the architectural rules relating to separation of bearer level, session control level, and service level expressed in 23.221[7].

5.4.5 Storing of session path information

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

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

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

5.4.6 End-user preferences and terminal capabilities

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

5.4.6.1 Objectives

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

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

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

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

- The available resources in the network play an important role, as certain media streams, consuming high bandwidth, may be denied. Therefore, before the user is alerted that the session set up is successful, it is assumed that the network has guaranteed and has reserved the needed resources for one or several media streams of the session. This does not preclude the possibility for the user to indicate his/her preferences regarding the session also after the alerting, in which case the initial resource reservations may have to be modified.

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

5.4.6.2 End-user expectations

From the end-user point of view the following user interactions can be listed:

- For outgoing sessions, it is assumed that the user would like to select certain parameters that define the proposed session. This can be pre-configured as preferences or defined on a per session basis.

- For incoming sessions, it is assumed that the terminal will establish a dialogue with the user. Such dialogue allows the user to manually accept some of the proposed parameters by the originator. This is typically media type (audio, video, whiteboard) and different quality parameters per media type. As an alternative, the user preferences may be pre-configured.

- Before establishing or accepting a new session, the user may define or agree on the following parameters. Some of these parameters may be pre-configured and others are defined on a per session basis.

    1. Type of media, i.e. audio, video, whiteboard, etc. This represents the user preferences of media types.

2. Combination of QoS attributes and selection of codec. This represents the quality of the media component, the cost and the probability of availability of resources both in the access network and in the core network.

3. Subset of capabilities used in the terminal. Terminals can have different set of capabilities. However, the user may or may not want to use the maximum set of capabilities. For instance, a user might want to establish a low cost video session with a small window on the screen.

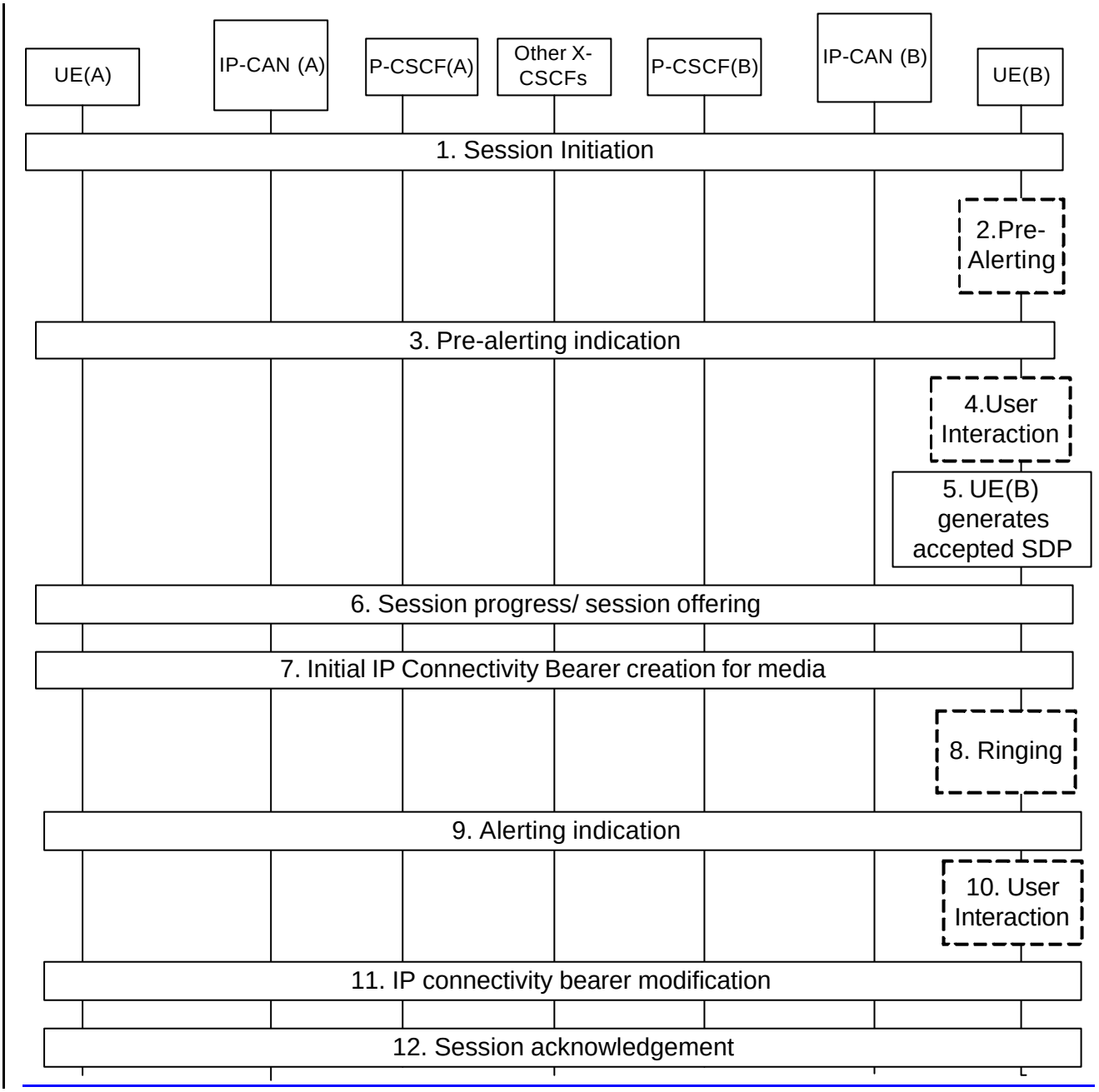
4. End-to-end quality of service. For certain media streams, the user may want assured end-to-end QoS while for other streams the QoS may be optional or even not desired at all (best effort).

5.4.6.3 Mechanism for bearer establishment

In order to fulfil the above requirements, it is needed that the destination user can be pre-alerted before the bearer establishment and negotiation and ~~PDP context~~ IP-Connectivity Access Network bearer ~~-~~ activation has taken place. This gives room for the destination user to choose the media streams and codecs required before an expensive resource (as the air interface is) is established.

Figure 5.7 shows the mechanism for the bearer establishment in which the pre-alerting occurs before the initial bearer creation procedures are performed. Furthermore, a user interaction may also occur after the initial bearers are created as shown in figure 5.7. If the session originator receives multiple provisional responses for the same session indicating that the session has been forked in the network, the UE may choose to process a pre-configured number of responses. In the case of multiple responses, the resources requested by the UE shall be the “logical OR” (i.e. least upper bound) of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE shall never request more resources then was originally proposed in the Original INVITE.

The "Other x-CSCFs" entity in figure 5.7 comprises several CSCFs: I-CSCF and S-CSCFs. For the sake of simplicity only the IP-Connectivity Access Network is shown, ~~GGSNs are presented from the UMTS access network~~ and the Policy Decision Functions have been omitted from the diagram.


UE(A)
IP-CAN (A)
P-CSCF(A)
Other X-CSCFs
P-CSCF(B)
IP-CAN (B)
UE(B)
1. Session Initiation
2.Pre-Alerting
3. Pre-alerting indication
4.User Interaction
5. UE(B) generates accepted SDP
6. Session progress/ session offering
7. Initial IP Connectivity Bearer creation for media
8. Ringing
9. Alerting indication
10. User Interaction
11. IP connectivity bearer modification
12. Session acknowledgement

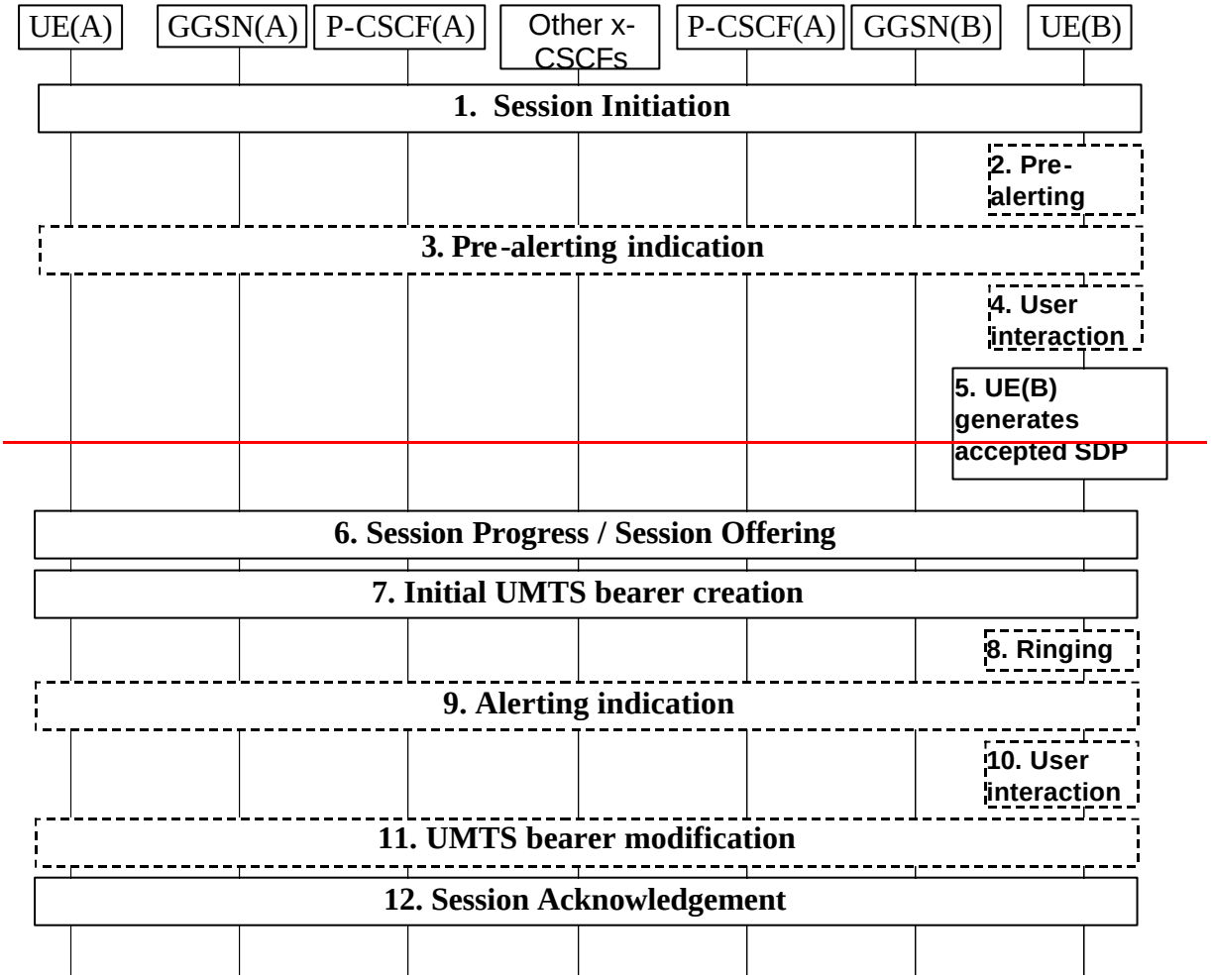


Figure 5.7: Bearer establishment showing optional pre-alerting

1. UE(A) starts a Session Initiation procedure to UE(B) that includes an SDP proposal.

The steps 2-4 are optional and may depend on terminal implementation and/or terminal pre-configured settings.

2. The user at UE(B) is pre-alerted.
3. An indication of the pre-alerting may be sent towards UE(A).
4. User at UE(B) will then interact and express his/her wishes regarding the actual session.
5. UE(B) generates accepted SDP based on terminal settings, terminal pre-configured profiles and optionally the user's wishes.
6. The accepted SDP is forwarded to UE(A) in the payload of a reliable SIP response.
7. If the media requires separate IP-CAN bearer, ~~i~~Initial bearer creation procedure is performed. During this bearer creation step the resources in the UE(A)'s and UE(B)'s IP-CANs ~~access network~~ are reserved ~~with PDP context procedures~~. Bearer resources in external networks may also be reserved at this point.

The steps 8-10 are also optional and may be skipped.

8. Terminal at UE(B) starts ringing.
9. The alerting indication is sent towards UE(A).
10. User at UE(B) may interact and express his/her wishes regarding the actual session.

11. UE(A) and UE(B) may perform bearer modification procedure at this point, if the initial bearers reserved in step 7 and the wishes of user at UE(B) are different. During this bearer modification step the resources in the UE(A)'s and UE(B)'s access network may be modified ~~by modifying the PDP context~~, and the resource reservation in the external network may also be modified.

12. Session initiation procedure is acknowledged.

5.4.6.4 Session progress indication to the originating UE

The pre-alerting or alerting indications returned to the originating UE shall enable the

originating UE to inform the calling user of the session progress prior to the arrival of the incoming media (for example the originating UE may synthesise ringing locally).

5.4.7 Interaction between QoS and session signalling

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

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

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

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

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

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

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

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

5.4.7.1 Authorize QoS Resources

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

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

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

5.4.7.1a Resource Reservation with Service-based Local Policy

The ~~GGSN~~ IP-CAN ~~serves as~~ provides the Policy Enforcement Point that implements the policy decisions for performing admission control and authorising the ~~GPRS~~ IP-CAN and IP BS QoS Resource request, and policing IP flows entering the external IP network.

Authorisation of IP-CAN ~~GPRS~~ and IP QoS Resources shall be required for access to the IP Multimedia Subsystem. The ~~GGSN~~ IP-CAN shall determine the need for authorisation, possibly based on provisioning and/or based on the requested APN ~~of the PDP context~~.

Resource Reservation shall be initiated by the UE, and shall take place only after successful authorisation of QoS resources by the PDF. Resource reservation requests from the UE shall contain the binding information received from the P-CSCF during IMS signaling which ~~. The use of this binding information~~ enables the ~~GGSN~~ IP-CAN to correctly match the reservation request to the corresponding authorisation. The authorisation shall be 'Pulled' from the PDF by the ~~GGSN~~ Policy Enforcement Function within the IP-CAN when the reservation request is received from the UE. When a UE combines multiple media flows onto a single ~~PDP context~~ IP-CAN bearer, all of the binding information related to those media flows shall be provided in the resource reservation request.

With a request for IP-CAN ~~GPRS~~ QoS resources, the Policy Enforcement Function within the IP-CAN ~~GGSN~~ shall verify the request is less than the sum of the authorised IP resources (within the error tolerance of the conversion mechanism) for all of the combined media flows. With a request for IP QoS resources, the Policy Enforcement Function within the IP-CAN ~~GGSN~~ shall verify the request is less than the authorised IP resources.

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

5.4.7.2 Approval of QoS Commit

The PDF makes policy decisions and provides an indication to the ~~GGSN~~ Policy Enforcement Function within the IP-CAN that the user is now allowed to use the allocated QoS resources for per-session authorisations unless this was done based on service based local policy at the time of the Resource Reservation procedure. If there is more than one response for the same session, indicating that the session has been forked in the network, the PDF may authorise the “logical OR” of the resources requested in the responses. When the session established indication has been received, if the PDF earlier have authorised the "logical OR" of the resources then the PDF will modify the authorisation and commit to resources according to the session established indication.

The ~~GGSN~~ Policy Enforcement Function within the IP-CAN enforces the policy decisions. The ~~GGSN~~ IP-CAN may restrict any use of the ~~GPRS~~ IP-CAN resources prior to this indication from the PDF. The IP-CAN ~~GGSN~~ shall restrict any use of the IP resources prior to this indication from the PDF, e.g. by open the gate and enabling the use of resources for the media flow. Based on local policy, IP-CAN ~~GPRS~~ and/or IP resources may beallowed to be used by the user at the time they are authorised by the PDF.

5.4.7.3 Removal of QoS Commit

The PDF makes policy decisions and provides an indication to the Policy Enforcement Function within the IP-CAN ~~GGSN~~ about revoking the user's capacity to use ~~-~~the allocated QoS resources for per-session authorisations. Removal of QoS Commit for IP-CAN ~~GPRS~~ and IP resources shall be sent as a separate decision to the Policy Enforcement Function within the IP-CAN~~GGSN~~ corresponding to the previous "Approval of QoS commit" request.

The ~~GGSN~~ Policy Enforcement Function within the IP-CAN enforces the policy decisions. The ~~GGSN~~ IP-CAN may restrict any use of the ~~GPRS~~ IP-CAN~~-~~ resources after this indication from the PDF. The IP-CAN ~~GGSN~~ shall restrict any use of the IP resources after this indication from the PDF, e.g. by closing the gate and blocking the media flow.

5.4.7.4 Revoke Authorisation for IP-Connectivity Access Network~~GPRS~~ and IP Resources

At IP multimedia session release, the UE should deactivate the ~~PDP context~~ IP-CAN bearer(s) used for the IP multimedia session. In various cases~~, such as loss of signal from the mobile,~~ the UE will be unable to perform this release itself. The Policy Decision Function provides indication to the ~~GGSN~~ Policy Enforcement Function within the IP-CAN when the resources previous authorised, and possibly allocated by the UE, are to be released. The ~~GGSNshall~~ IP-CAN shall deactivate the ~~PDP context~~ IP-CAN bearer used for the IP multimedia session.

5.4.7.5 Indication of ~~PDP Context~~ IP-Connectivity Access Network bearer release

Any release of ~~a PDP Context~~ IP-CAN bearer(s) that ~~was~~ were established based on authorisation from the PDF shall be reported to the PDF by the ~~GGSN~~ IP-CAN.

This indication may be used by the PDF to initiate a session release towards the remote endpoint.

5.4.7.6 Authorization of ~~PDP Context~~ IP-Connectivity Access Network bearer modification

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

If the ~~GGSN~~ Policy Enforcement Function within the IP-CAN does not have sufficient information to authorize the ~~PDP context modification~~ IP-CAN bearer modification request, the ~~GGSN~~ Policy Enforcement Function within the IP-CAN shall send an authorization request to the PDF.

5.4.7.7 Indication of ~~PDP Context~~ IP-Connectivity Access Network bearer modification

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

This indication may be used by the PDF to initiate a session release towards the remote endpoint.

5.4.8 QoS-Assured Preconditions

This section contains concepts for the relation between the resource reservation procedure and the procedure for end-to-end sessions.
A precondition is a set of constraints about the session, which are introduced during the session initiation. The recipient of the session generates an answer, but does not alert the user or otherwise proceed with session establishment until the preconditions are met. This can be known through a local event (such as a confirmation of a resource reservation), or through a new set of constraints sent by the caller.

A "QoS-Assured" session will not complete until required resources have been allocated to the session. In a QoS-Assured session, the UE must succeed in establishing the QoS bearer for the media stream according to the QoS preconditions defined at the session level before it may indicate a successful response to complete the session and alert the other end point. The principles for when a UE shall regard QoS preconditions to be met are:

- A minimum requirement to meet the QoS preconditions defined for a media stream in a certain direction, is that an appropriate IP-CAN bearer ~~PDP context is~~ established at the local access for that direction.

- Segmented resource reservation is performed since the end points are responsible to make access network resource reservations via local mechanisms.

- The end points shall offer the resources it may want to support for the session and negotiate to an agreed set. Multiple negotiation steps may be needed in order to agree on a set of media for the session. The final agreed set is then updated between the end points.

- The action to take in case a UE fails to fulfil the pre-conditions (e.g. failure in establishment of an RSVP session) depends on the reason for failure. If the reason is lack of resources in the network (e.g. an admission control function in the network rejects the request for resources), the UE shall fail to complete the session. For other reasons (e.g. lack of RSVP host or proxy along the path) the action to take is local decision within the UE. It may for example 1) choose to fail to complete the session, 2) attempt to complete the session by no longer requiring some of the additional actions ~~(e.g. fall back to establishment of PDP context only)~~.

The flows of sections 5.5, 5.6 and 5.7 depict the case where both UEs require confirmation from the other of the fulfilment of the pre-conditions. Other cases are possible according to the SIP specifications. For example, the pre-conditions may already be fulfilled (according to the principles above) when the INVITE is sent, or the UE may not require explicit confirmation from the other SIP endpoint when the pre-conditions are fulfilled. One example of such SIP endpoint is the MGCF used for PSTN interworking. In these cases, one or both of the reservation confirmation messages may not be sent.

5.4.9 Event and information distribution

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

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

This mechanism considers the following issues:

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

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

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

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

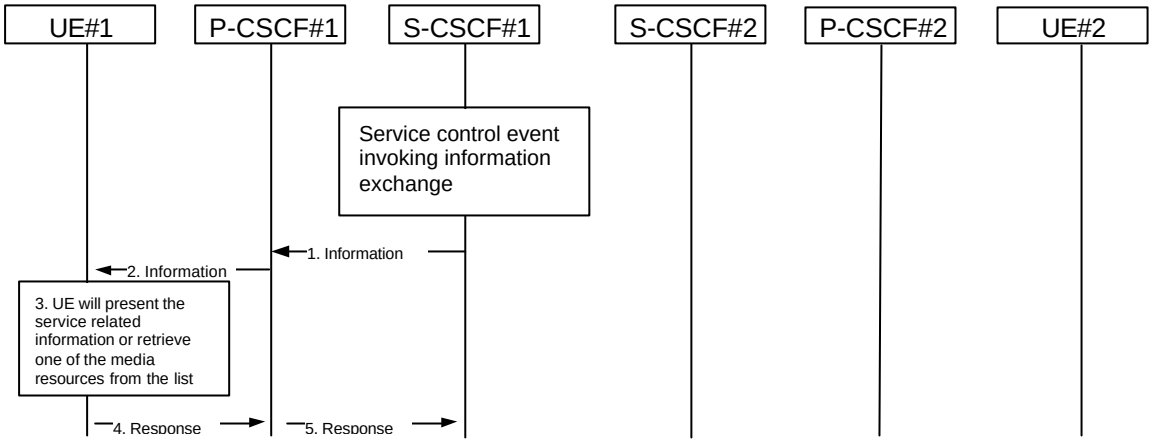


Figure 5.8: Providing service event related information to related endpoint

1. When a service event occurs that the S-CSCF or the Application Server wishes to inform an endpoint about, the S-CSCF or the Application Server generates a message request containing information to be presented to the user. The contents may include text describing the service event, a list of URI(s) or other service modification information.
2. P-CSCF forwards the message request.
3. UE presents the service-related information, to the extent that it conforms to its capabilities and configuration, to the user.
4. Possibly after interaction with the user, the UE will be able to include information in the response to the S-CSCF.
5. P-CSCF forwards the response.

Note 1: The UE may retrieve service event related information using ~~PS Domain~~IP or IMS procedures.

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

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.

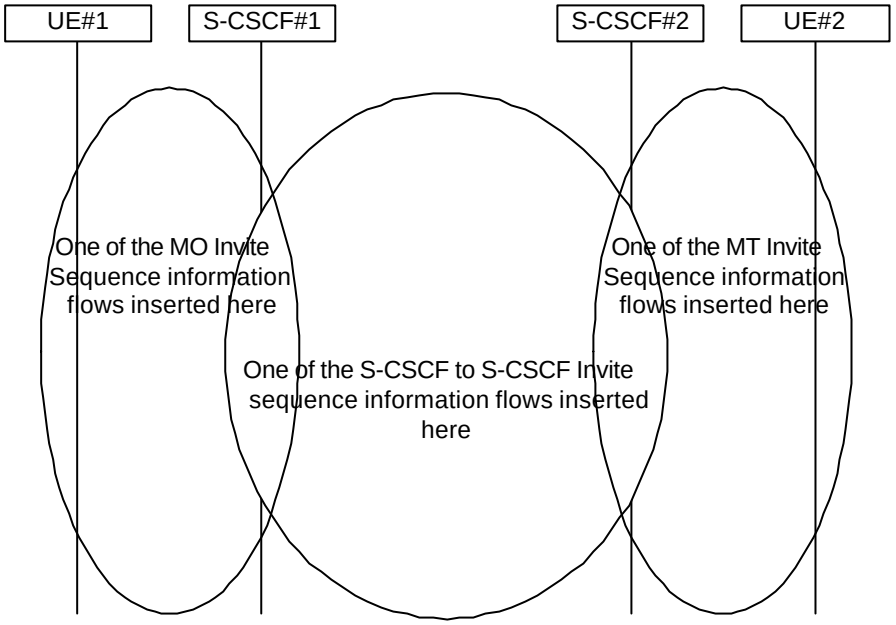


Figure 5.9: Overview of Session Flow Sections

The following procedures are defined:

For the origination sequence:

?? (MO#1) Mobile origination, roaming

?? (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.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

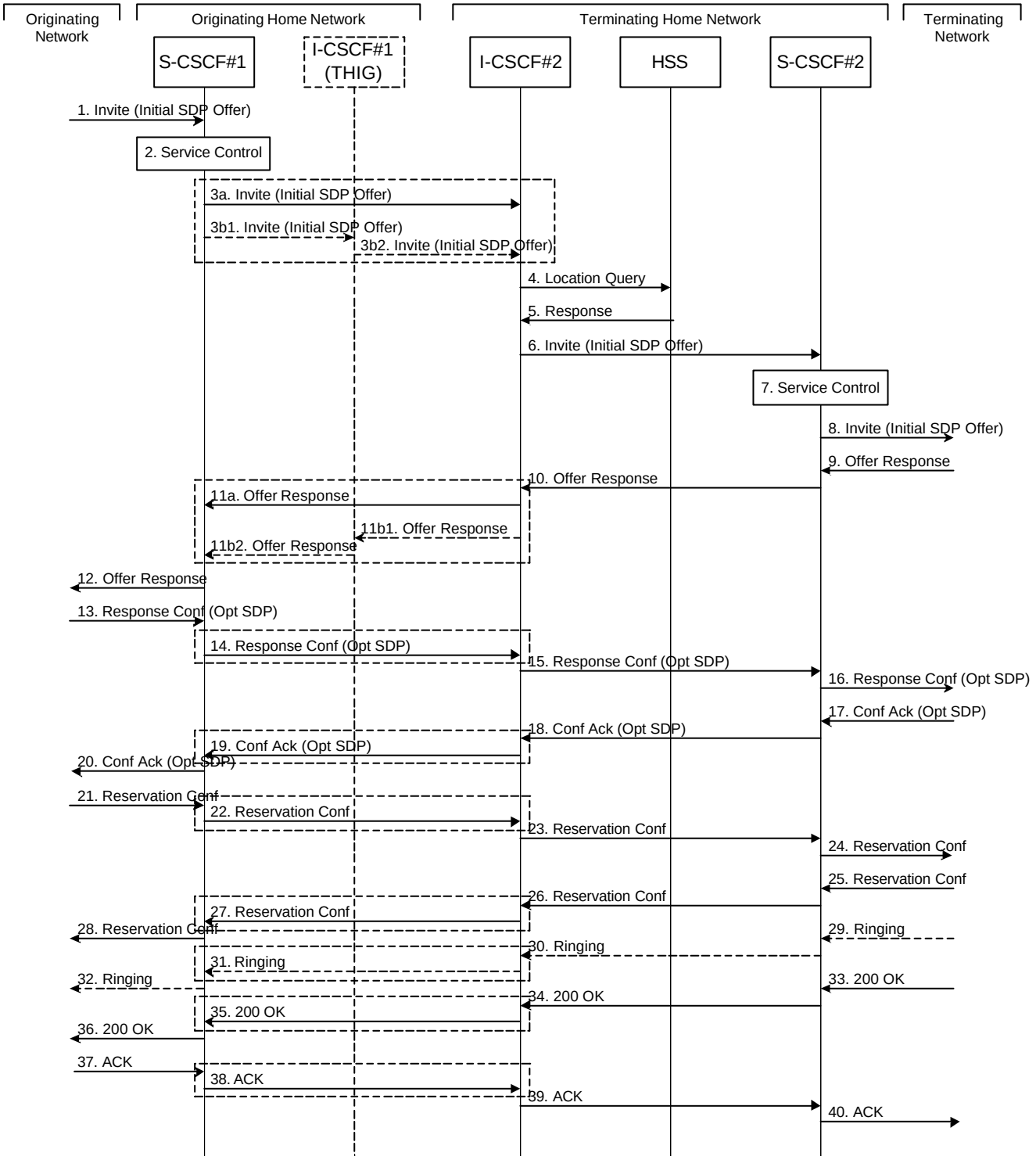


Figure 5.10: Serving to serving procedure - different operators

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) may query the HSS for current location information. If I-CSCF#2 cannot determine, based on analysis of the destination number, that the HSS query will fail, then it will send "Cx-location-query" to the HSS to obtain the location information for the destination. If I-CSCF#2 can determine, based on analysis of the destination number, that the HSS query will fail, it will not send the "Cx-location-query" message, allocate a MGCF for a PSTN termination, and continue with step #6.

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.

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

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.

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

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.

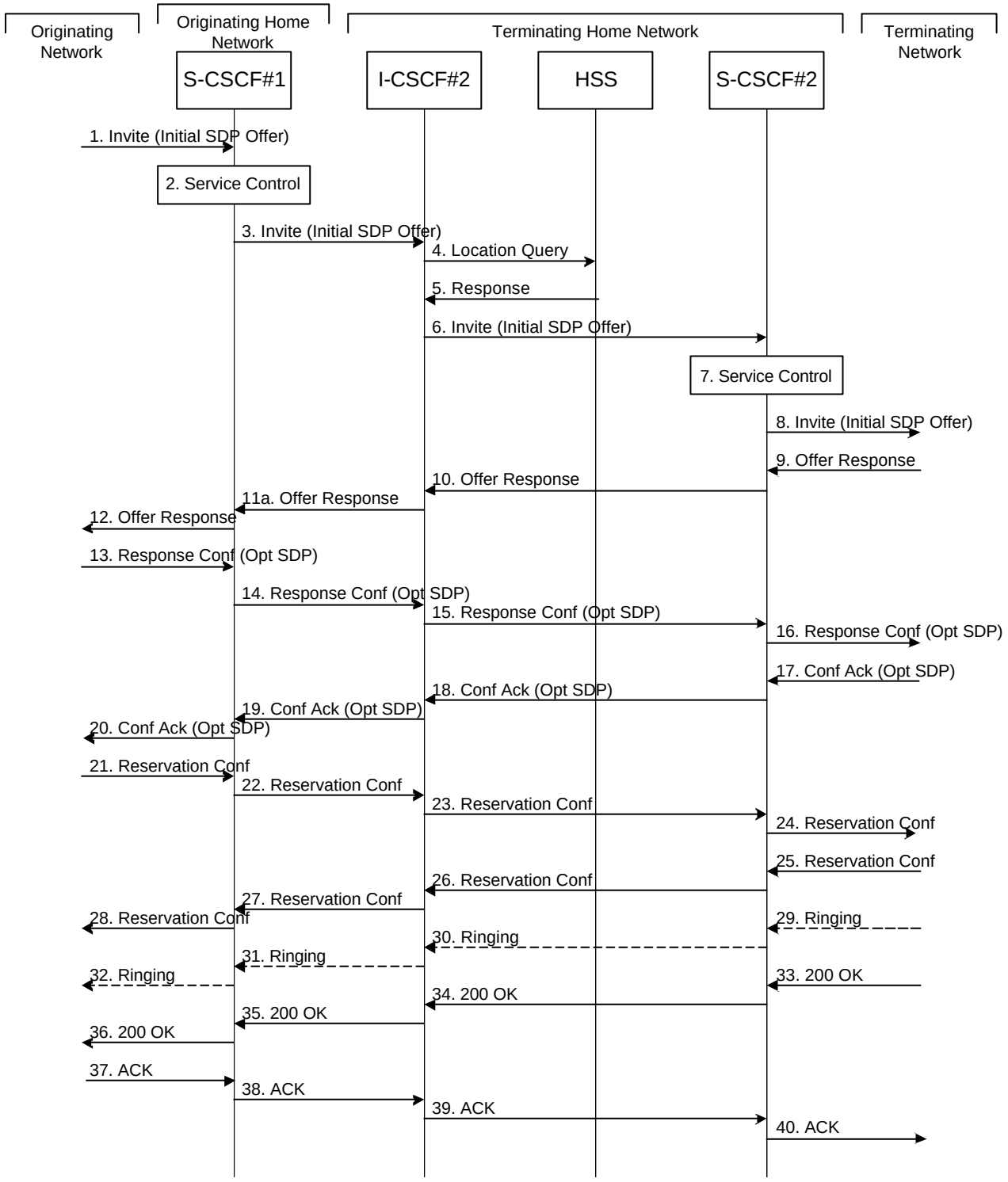


Figure 5.11: Serving to serving procedure - same operator

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 may query the HSS for current location information. If I-CSCF cannot determine, based on analysis of the destination number, that the HSS query will fail, then it will send “Cx-location-query” to the HSS to obtain

the location information for the destination. If I-CSCF can determine, based on analysis of the destination number, that the HSS query will fail, it will not send the "Cx-location-query" message, allocate a MGCF for a PSTN termination, and continue with step #6.

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.

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

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.

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

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

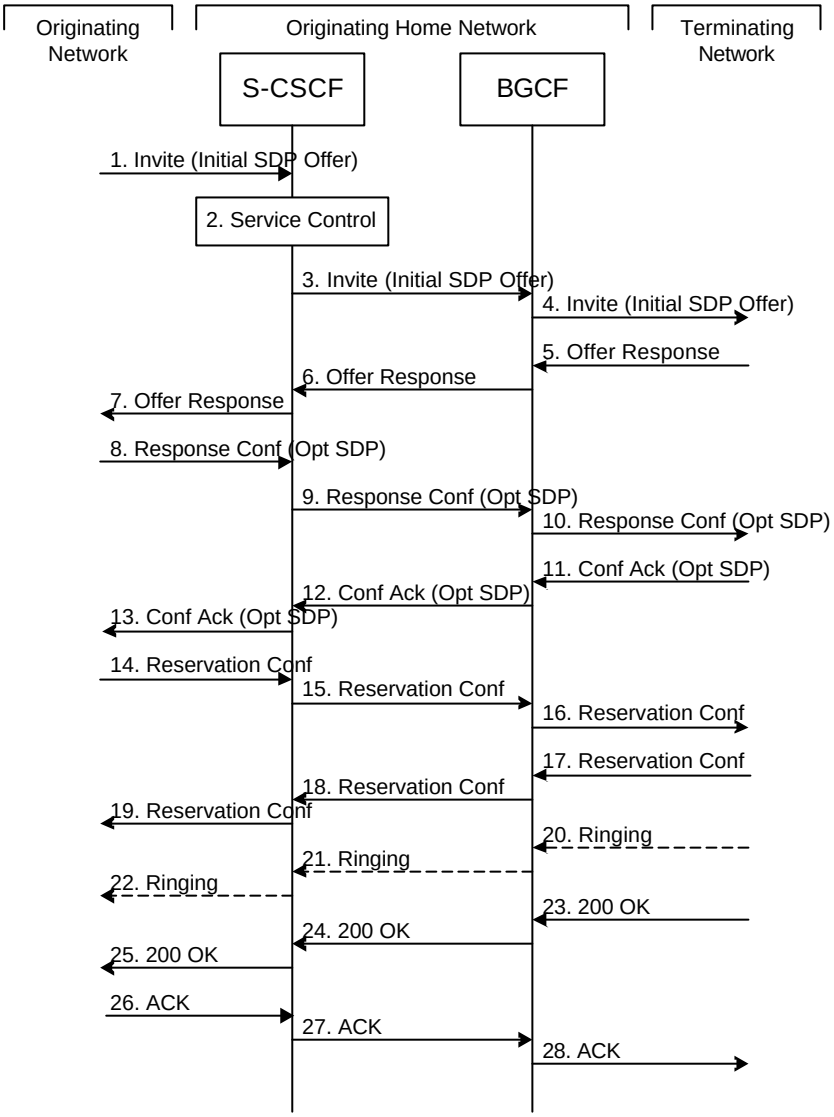


Figure 5.12: Serving to PSTN procedure - same operator

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.

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 the same network as the S-CSCF.

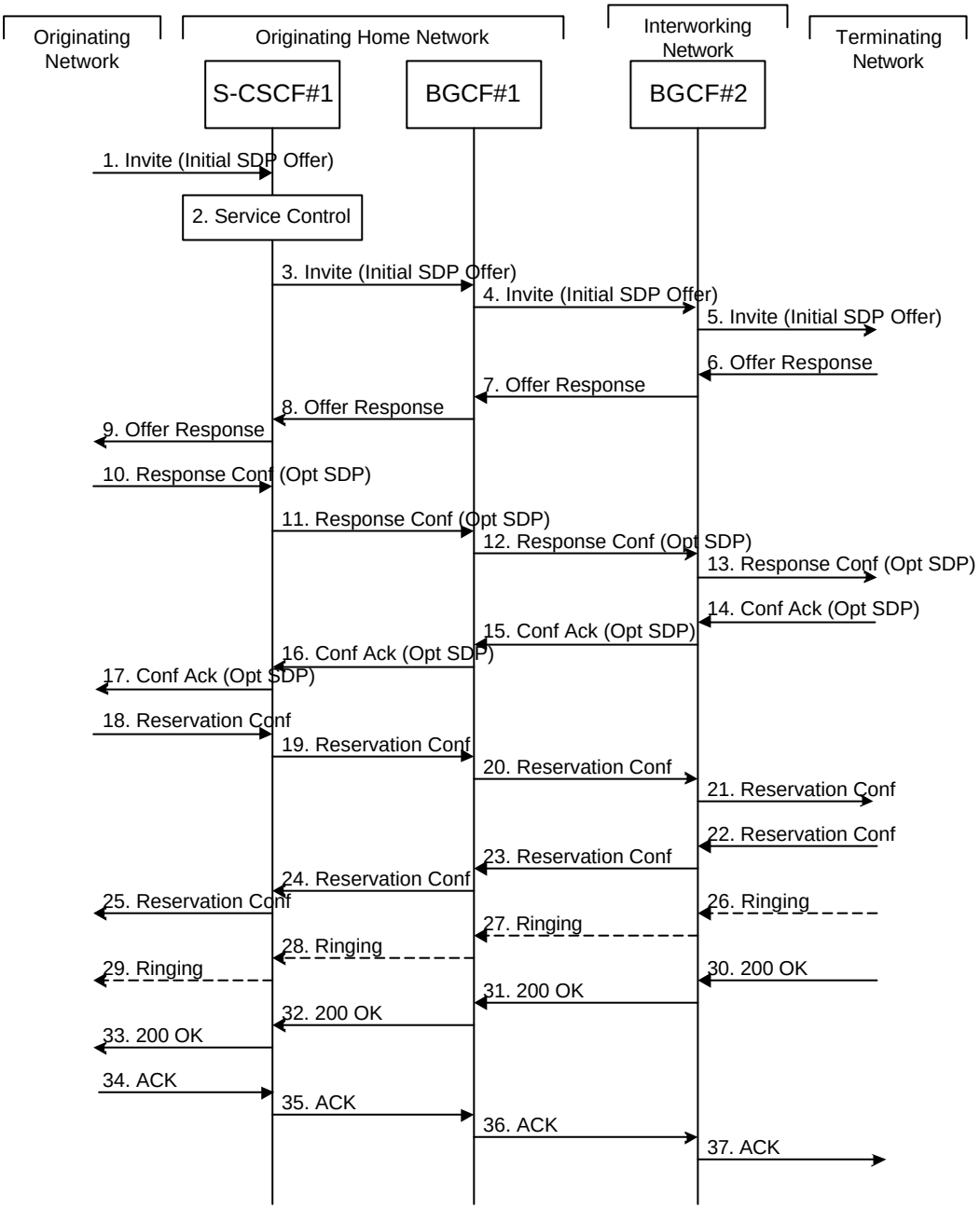


Figure 5.13: Serving to PSTN procedure - different operator

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.

5.6 Origination procedures

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 ~~is located in the same network as the GGSN,~~ performs resource authorisation, and may have additional functions in handling of emergency sessions. The P-CSCF is determined by the CSCF discovery process, described in Section 5.1.1 (Local CSCF Discovery).

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

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

5.6.1 (MO#1) Mobile origination, roaming

This origination procedure applies to roaming users.

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

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

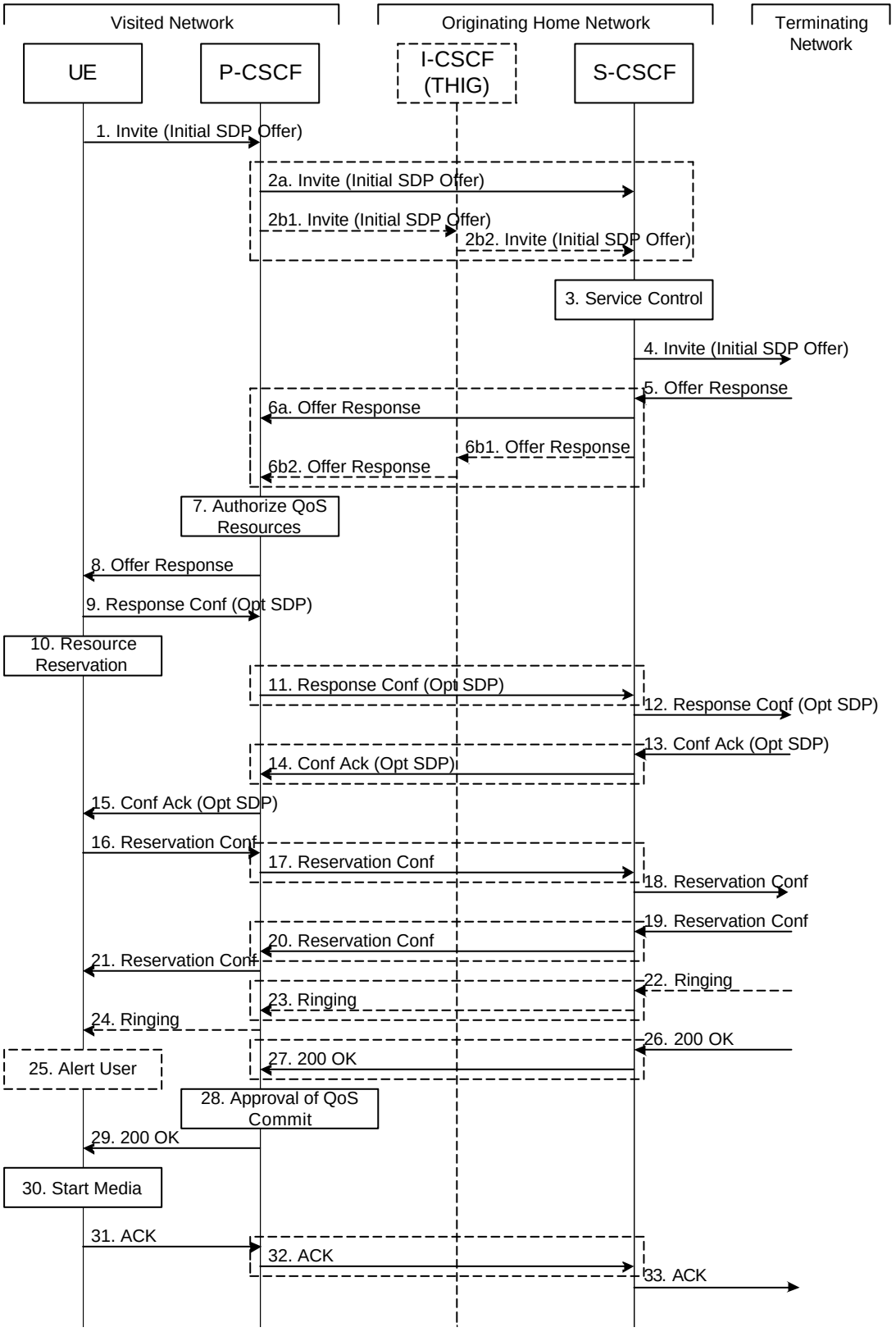


Figure 5.14: Mobile origination procedure - roaming

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. 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. The Authorization-Token is generated by the PDF.

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.

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 invokes whatever service logic is appropriate for the completed session setup.

27. S-CSCF sends a SIP 200-OK final response along the signalling path back to P-CSCF. Step 23 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.

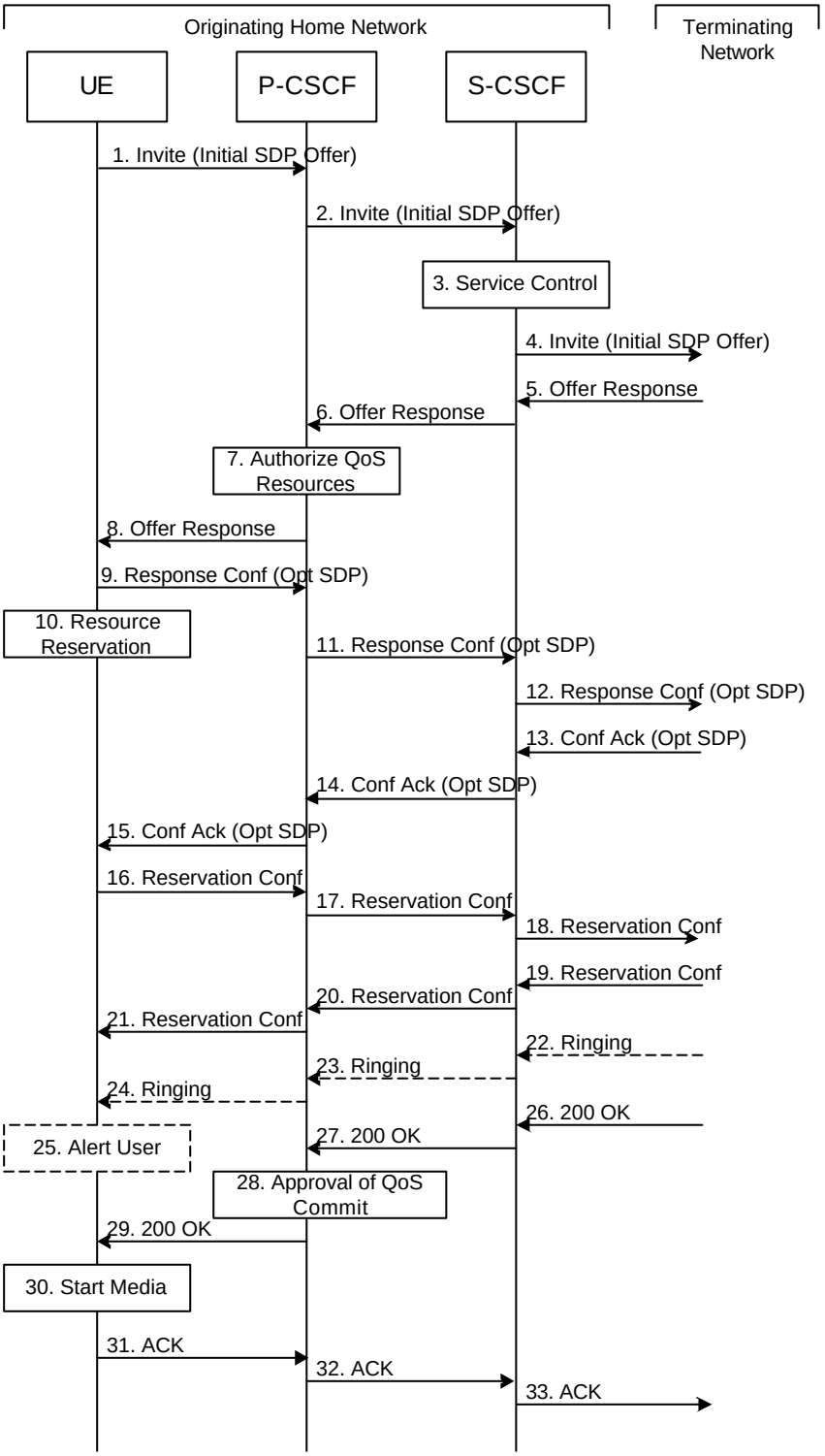


Figure 5.15: Mobile origination procedure - home

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. 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. The Authorization-Token is generated by the PDF.

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.

5.6.3 (PSTN-O) PSTN origination

The MGCF in the IM CN subsystem is a SIP endpoint that initiates requests on behalf of the PSTN and Media Gateway. The subsequent nodes consider the signalling as if it came from a S-CSCF. The MGCF incorporates the network security functionality of the S-CSCF. This MGCF does not invoke Service Control, as this may be carried out in the GSTN or at the terminating S-CSCF. This origination procedure can be used for any of the S-S procedures.

Due to routing of sessions within the PSTN, this origination procedure will only occur in the home network of the destination subscriber. However due to cases of session forwarding and electronic surveillance, the destination of the session through the IM CN subsystem may actually be another PSTN termination.

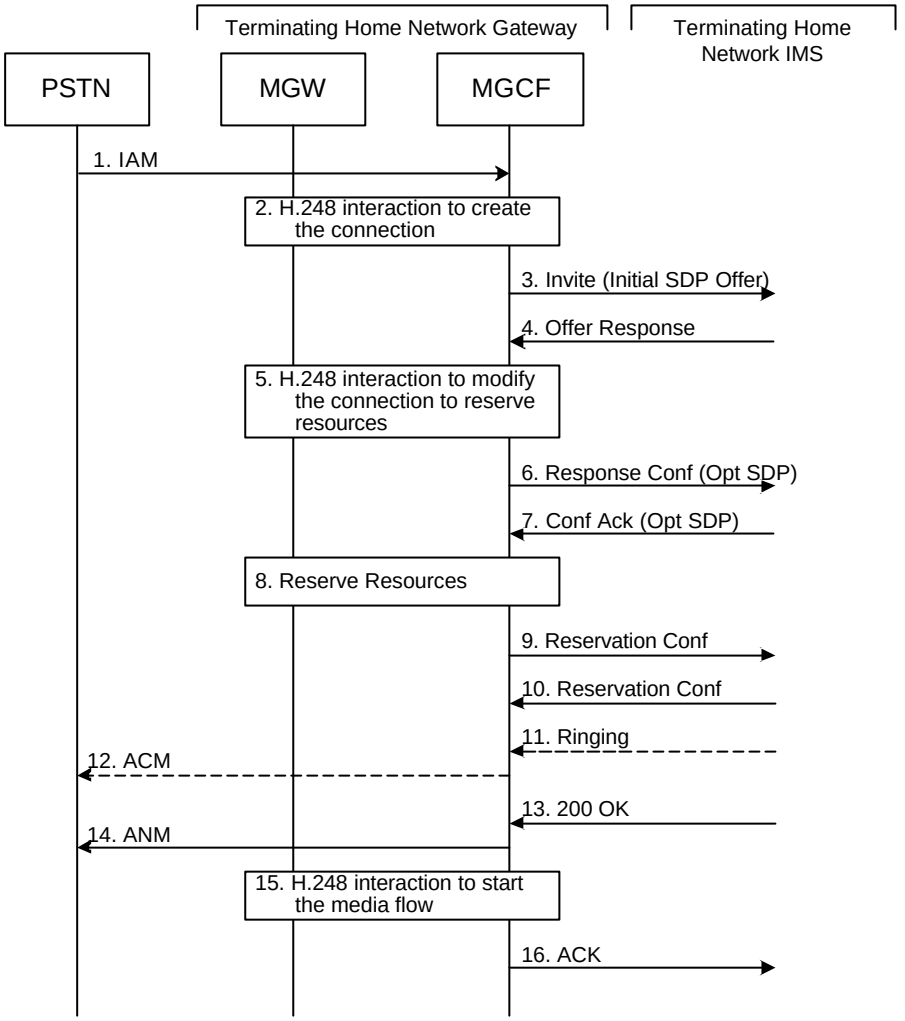


Figure 5.16: PSTN origination procedure

The PSTN Origination procedure is as follows:

1. The PSTN establishes a bearer path to the MGW, and signals to the MGCF with a IAM message, giving the trunk identity and destination information

2. The MGCF initiates a H.248 command, to seize the trunk and an IP port.

3. The MGCF initiates a SIP INVITE request, containing an initial SDP, as per the proper S-S procedure.

4. The media stream capabilities of the destination are returned along the signalling path, per the S-S procedures.

5. MGCF initiates a H.248 command to modify the connection parameters and instruct the MGW to reserve the resources needed for the session.

6. MGCF decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation per the S-S procedures.

7. Terminating end point responds to the Response Confirmation. If Optional SDP is contained in the Response Confirmation, the Confirmation Acknowledge will also contain an SDP response.

8. MGW reserves the resources needed for the session

9. When the resource reservation is completed, MGCF sends the successful Resource Reservation message to the terminating endpoint, per the S-S procedures.

10. Terminating end point responds to the successful media resource reservation.

11. The destination endpoint may optionally perform alerting. If so, it signals this to the originating party by a provisional response indicating Ringing. This message is sent to MGCF per the S-S procedure.

12. If alerting is being performed, the MGCF forwards an ACM message to PSTN

13. When the destination party answers, the terminating and S-S procedures result in a SIP 200-OK final response being sent to MGCF

14. MGCF forwards an ANM message to to the PSTN

15. MGCF initiates a H.248 command to alter the connection at MGW to make it bi-6directional

16. MGCF acknowledges the SIP final response with a SIP ACK message

5.7 Termination procedures

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

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

The session termination procedures specify the signalling path between the Serving-CSCF assigned to perform the session termination service and the UE. This signalling path is determined at the time of UE registration, and remains fixed for the life of the registration. This signalling path is the reverse of the session initiation signalling path of Section 5.6. Therefore there is a one-to-one correspondence between the origination procedures of section 5.6 and the termination procedures of this section.

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

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

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

5.7.1 (MT#1) Mobile termination, roaming

This termination procedure applies to roaming users.

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

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

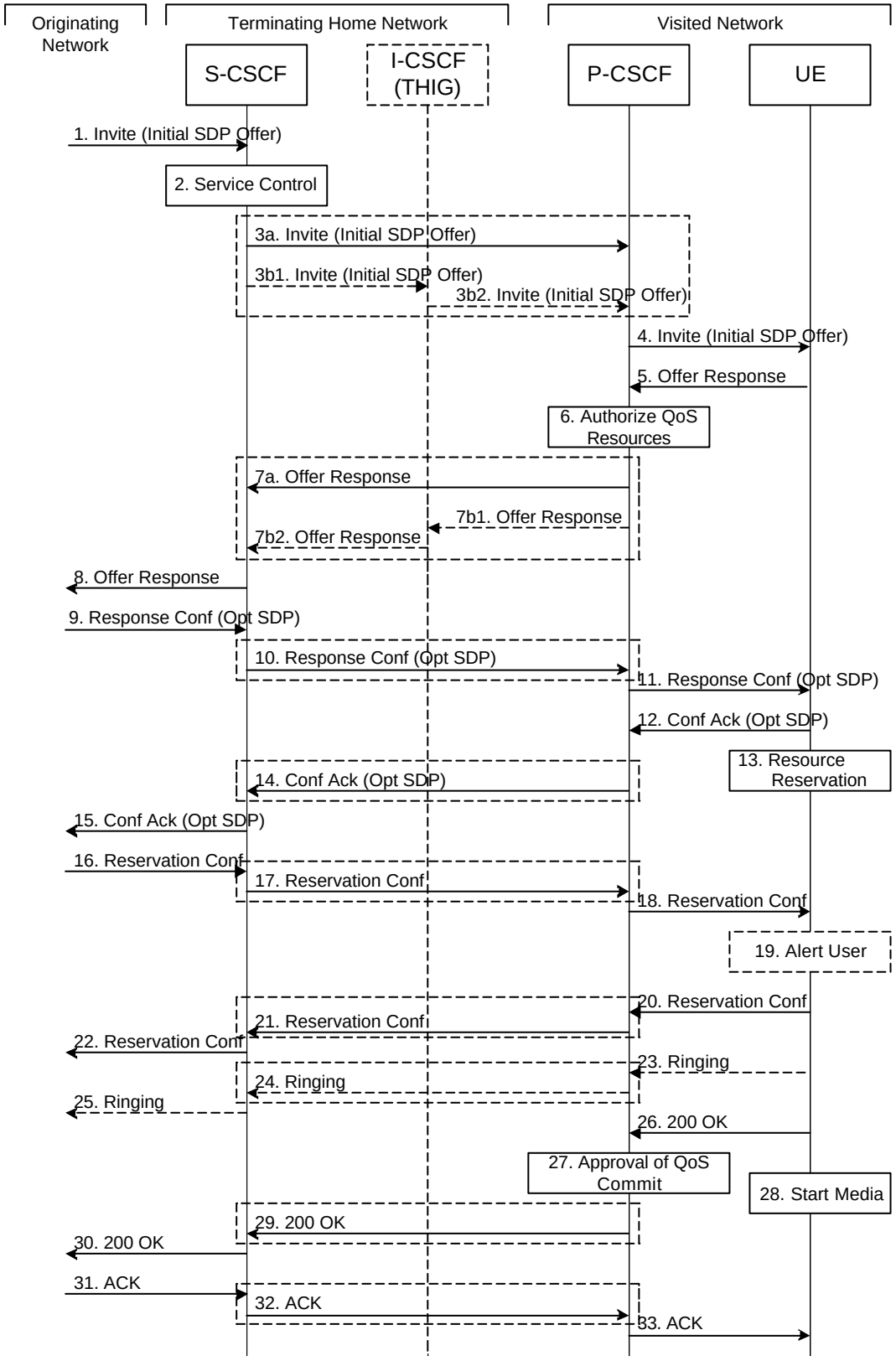


Figure 5.17: Mobile termination procedure - roaming

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 PDFand 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.

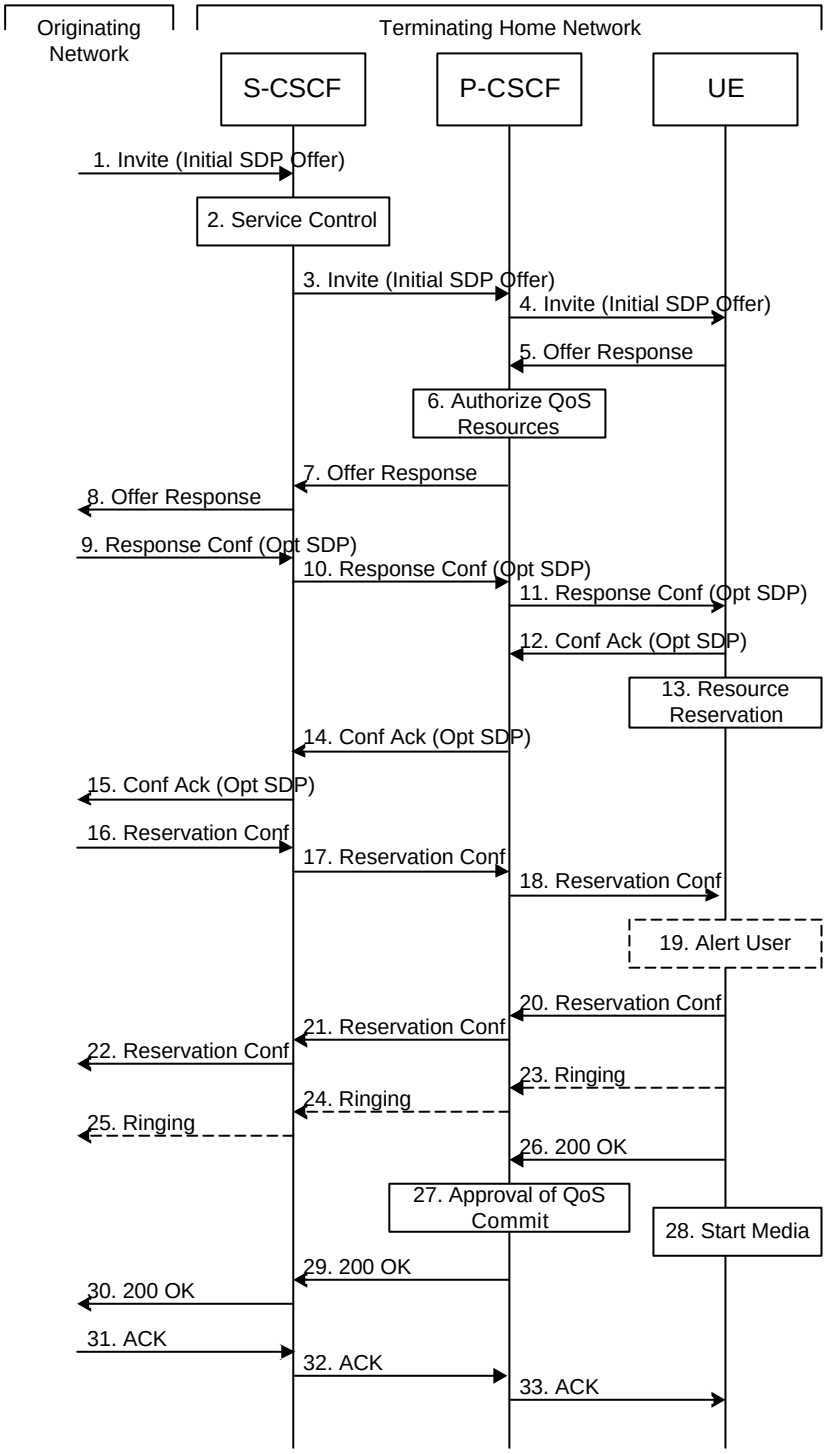


Figure 5.18: Mobile termination procedure - home

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 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

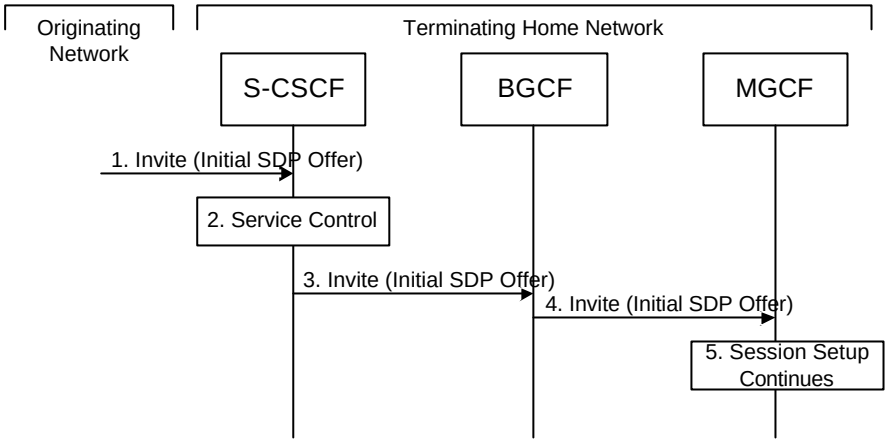


Figure 5.18a: Mobile Terminating procedures to a user that is unregistered for IMS services but is registered for CS services

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.

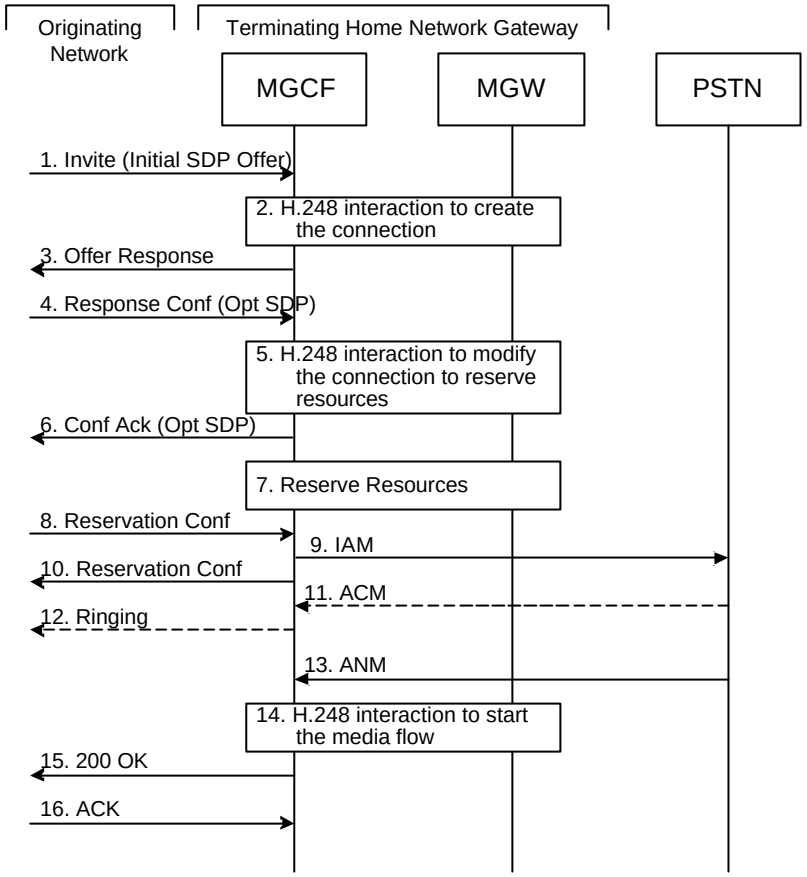


Figure 5.19: PSTN termination procedure

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. MGW 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

5.8 Procedures related to routing information interrogation

The mobile terminated sessions for a user shall be routed either to a Serving-CSCF or to a MGCF (if the user is roaming in a legacy network). When a mobile terminated session set-up arrives at a CSCF that is authorised to route sessions, the CSCF interrogates the HSS for routing information.

The Cx reference point shall support retrieval of routing information from HSS to CSCF. The resulting routing information can be either Serving-CSCF signalling transport parameters (e.g. IP-address).

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.

5.8.2 SLF on register

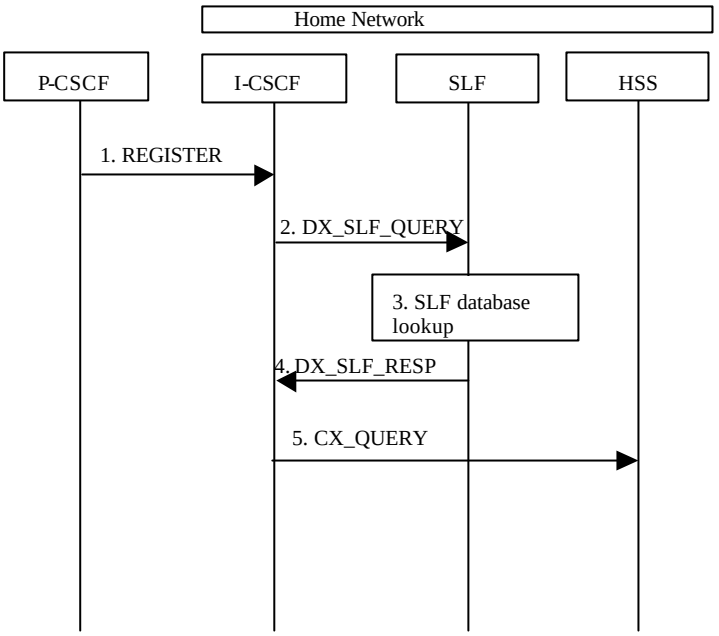


Figure 5.20: SLF on register (1st case)

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.

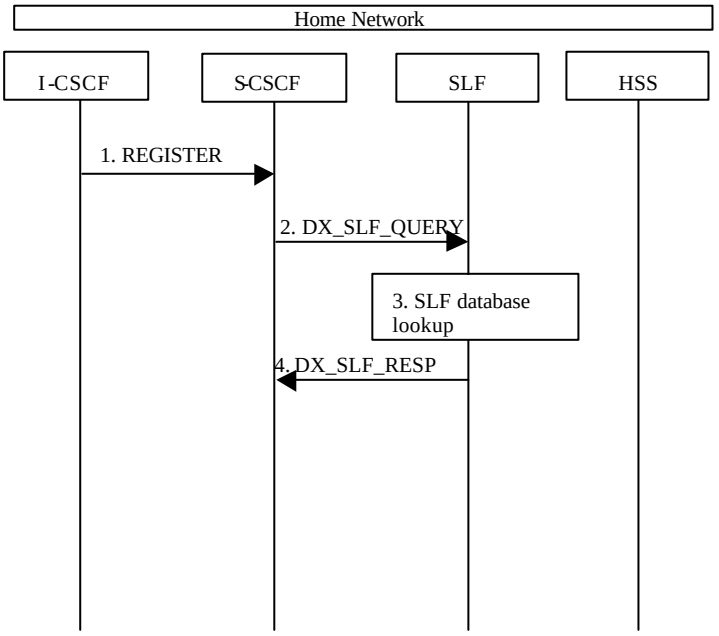


Figure 5.20a: SLF on register (2nd case)

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

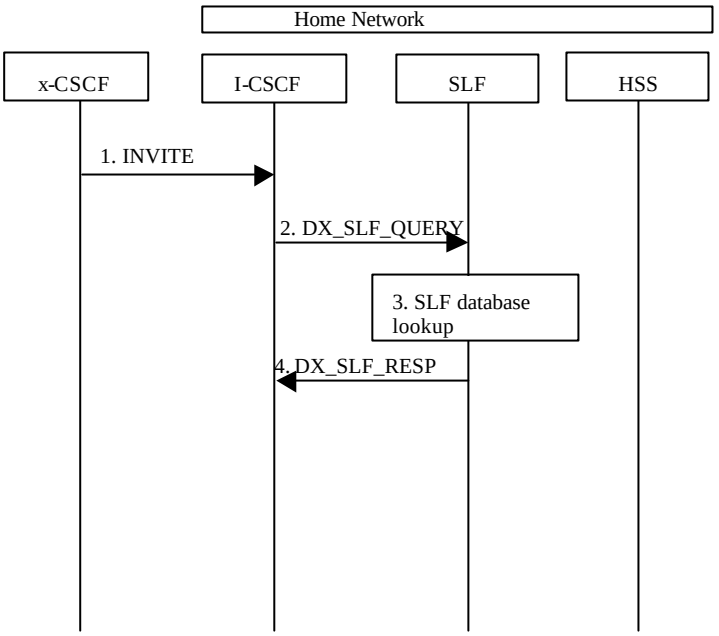


Figure 5.21: SLF on UE invite

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.

The synchronisation between the SLF and the different HSSs is an O&M issue.

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.

5.9 Routing of mid-session signalling

During the signalling exchanges that occur to establish an IM Session, the following elements must ensure future signalling messages related to this session are routed through them:

?? P-CSCF serving the originating UE, in order to generate the CDR record in the roaming case, and to force release of the resources used for the session

?? S-CSCF serving the originating UE, in order to invoke any service logic required at session setup completion, and to generate the CDR record at session termination

?? S-CSCF serving the terminating UE, in order to invoke any service logic required at session setup completion, and to generate the CDR record at session termination

?? P-CSCF serving the terminating UE, in order to generate the CDR record in the roaming case, and to force release of the resources used for the session

Other CSCFs (e.g. I-CSCFs) may optionally request this as well, for example if they perform some function needed in handling mid-session changes or session clearing operations.

All signalling message from the UE related to IMS sessions shall be sent to the P-CSCF.

5.10 Session release procedures

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

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

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

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

5.10.1 Mobile terminal initiated session release

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

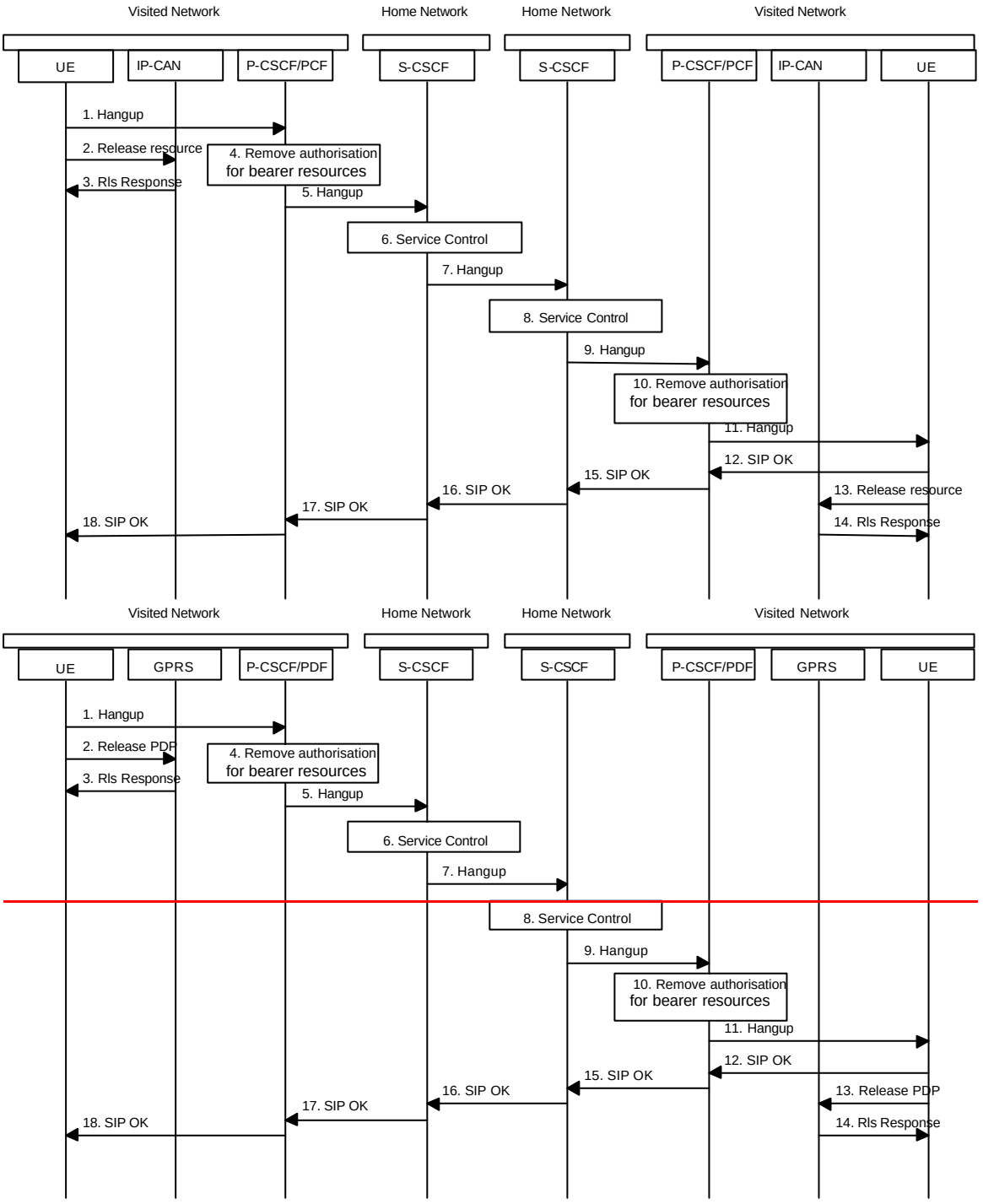


Figure 5.22: Mobile initiated session release

1. One mobile party hangs up, which generates a message (Bye message in SIP) from the UE to the P-CSCF.

2. Steps 2 and 3 may take place before or after Step 1 and in parallel with Step 4. The UE initiates the release of the ~~bearer~~ IP-CAN bearer ~~PDP context~~. The IP-CAN ~~GPRS subsystem~~ releases the ~~PDP context~~ 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 ~~GGSN~~ IP-CAN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.

3. The IP-CAN ~~GPRS subsystem~~ responds to the UE's bearer release request.

4. The P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this session. This step will also result in a release indication to the IP-CAN ~~GPRS subsystem~~ to confirm that the IP bearers associated with the session have been deleted

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

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.

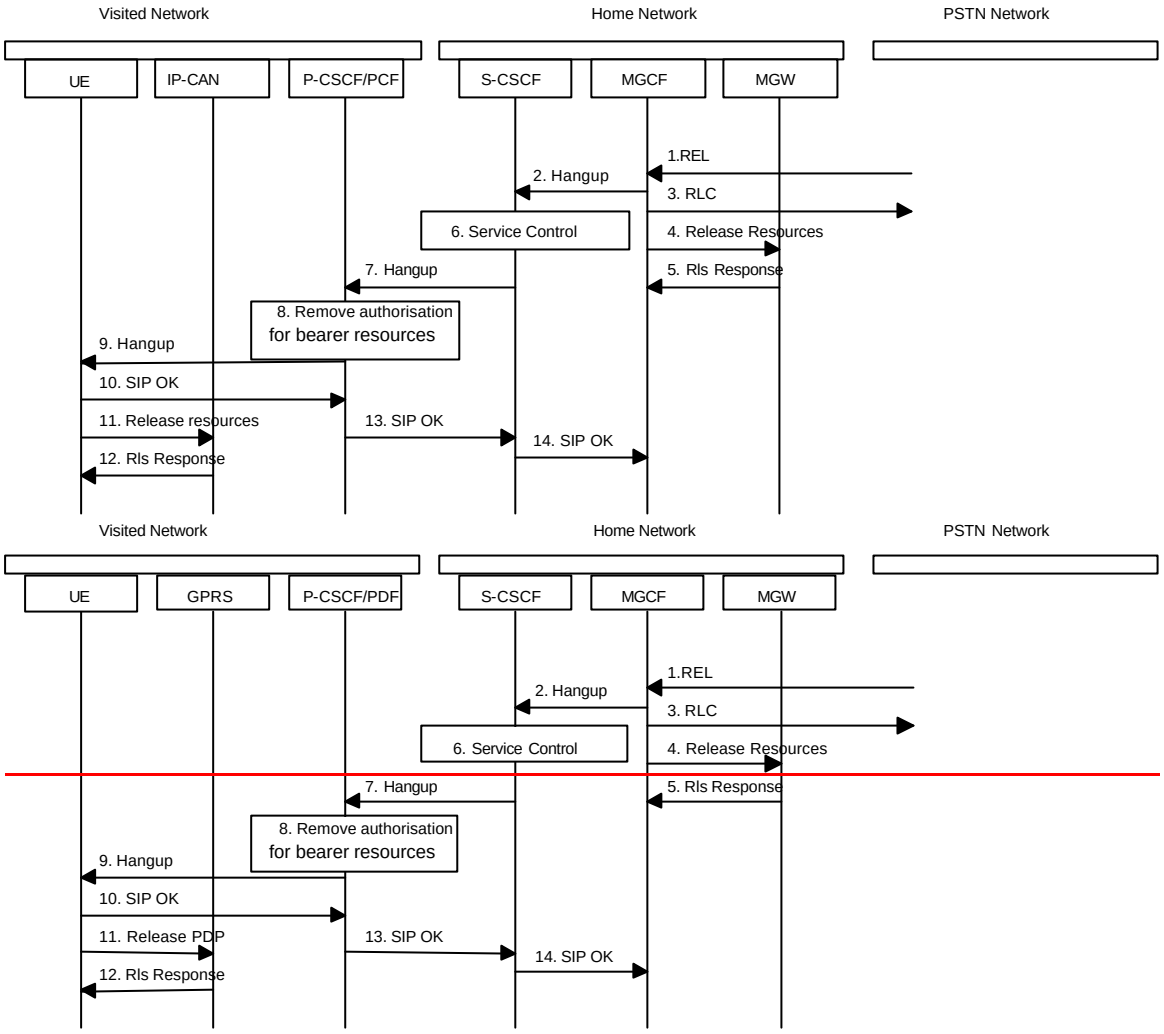


Figure 5.23: PSTN initiated session release

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.
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 ~~GPRS subsystem~~ 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 ~~Mobile~~ UE initiates the release of the IP-CAN bearer ~~PDP context~~.

12. The IP-CAN ~~GPRS subsystem~~ releases the ~~PDP context~~ 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.

5.10.3 Network initiated session release

5.10.3.0 ~~Deletion~~ Removal of ~~PDP context~~ IP-CAN bearer used to transport IMS SIP signalling

It is possible that the IP-CAN ~~GPRS subsystem~~ ~~deletes~~ removes the IP-CAN bearer ~~PDP context~~ used to transport IMS SIP signalling (e.g. due to ~~routing area update,~~ overload situations).

In this case the UE shall initiate a procedure to re-establish an IP-CAN bearer ~~PDP context~~ to transport IMS SIP signalling. ~~If there are any IMS related PDP contexts active the re-establishment of the PDP context to transport IMS signalling shall be perfomed by using the Secondary PDP Context Activation Procedure as defined in TS 23.060 [23].~~ If re-establishment fails then the UE shall de-activate all other IMS related ~~PDP context~~ IP-CAN bearer(s) ~~(s)~~. The deactivation of the IP-CAN bearer(s) results in the P-CSCF/PDF being informed of the bearer release which may, depending on policy, lead to a network initiated session release (initiated by the P-CSCF) as described in 5.10.3.1.

5.10.3.1 Network initiated session release - P-CSCF initiated

This clause assumes that service-based local policy is applied

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

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

~~In the event of loss of coverage, 3G TS 23.060 defines the Iu or RAB Release procedures. In case of PDP context with streaming or conversational class the maximum bitrate of the GTP tunnel between SGSN and GGSN is modified to 0 kbit/s. This is indicated to the P-CSCF / PDF by performing the 'PDP Context Modification' procedure (see 3GPP TS 23.207) as shown in Figure 5.25. For loss of coverage in case of other PDP contexts (background or interactive traffic class), the PDP context is preserved with no modifications.~~

Other network initiated session release scenarios are of course possible. ~~In particular such scenarios initiated in the home network for administrative reasons might begin with an S-CSCF.~~

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

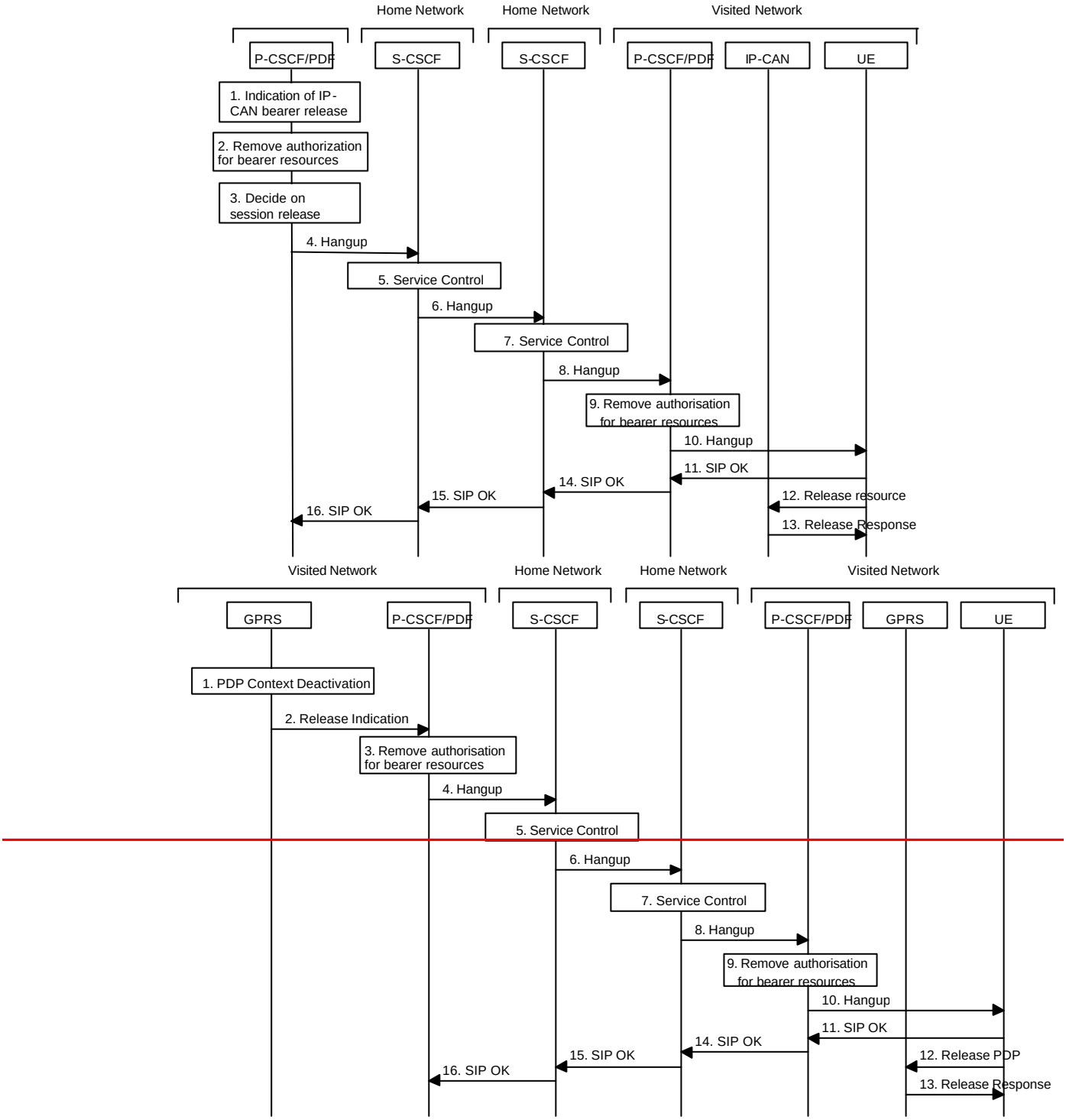


Figure 5.26: Network initiated session release - P-CSCF initiated ~~-~~– after removal of IP-CAN bearer~~PDP context~~

~~1. A bearer related to the session is terminated, for example, triggered by a mobile power down, etc. This is noted by the GPRS subsystem.~~

~~2. If a request state was created in the PDF at PDP context activation, the GGSN shall send a release indication to the P-CSCF/PDF for the disconnected bearer. The P-CSCF might also note the release due to a SIP Session Timeout.~~

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

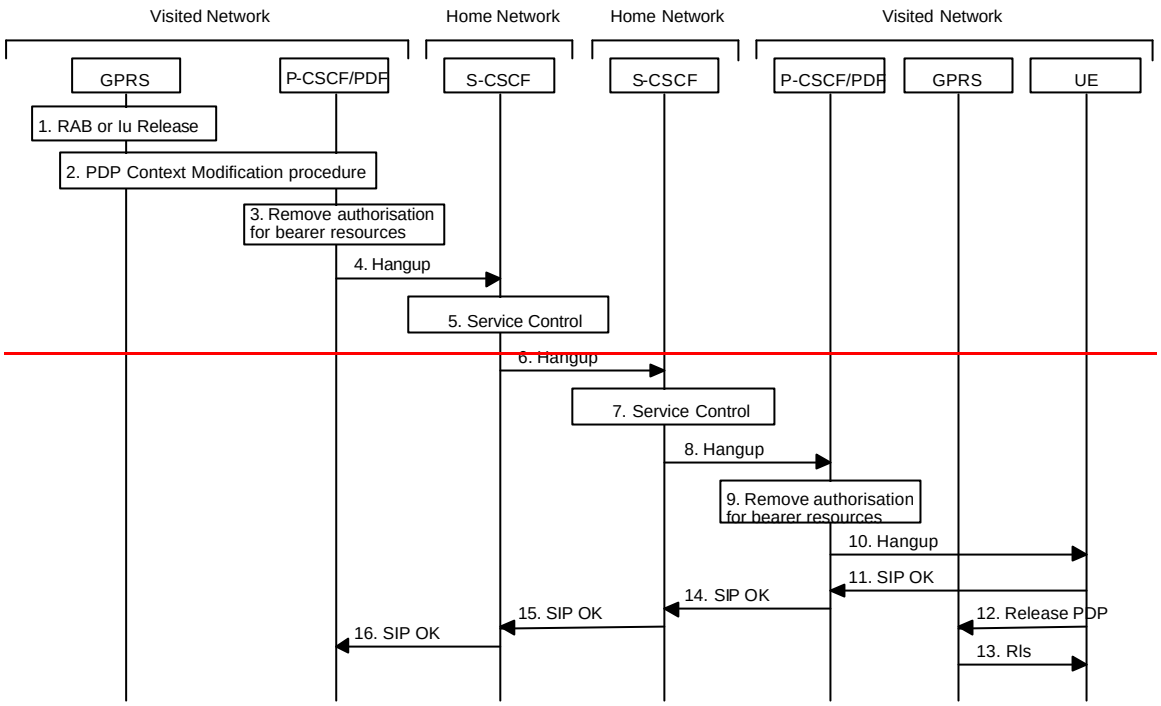
2~~3~~. The P-CSCF/PDF removes the authorisation for resources related to the released bearer that had previously been issued for this endpoint for this session. It is optional for the P-CSCF/PDF to deactivate additional IP-CAN bearers (e.g. an IP-CAN bearer for chat could still be allowed). For these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

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

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

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

5.10.3.1.2 ~~P-CSCF initiated session release after loss of radio coverage~~Void



~~Figure 5.26a: P-CSCF initiated session release after loss of radio coverage~~

~~1. In the event of loss of radio coverage the Iu connection or RAB(s) are released. In case of PDP context with streaming or conversational class the maximum bitrate of the GTP tunnel between SGSN and GGSN is modified to 0 kbit/s by PDP Context Modification procedures. For PDP contexts using background or interactive traffic class, the PDP context is preserved with no modifications.~~

~~2. If a request state was created in the PDF at PDP context activation, the GGSN shall initiate the PDP context modification procedure by sending a modify indication to the P-CSCF/PDF for the affected bearers in order to indicate the change of the maximum bitrate to 0 kbit/s. The P-CSCF/PDF shall accept this modification.~~

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

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

~~4. The P-CSCF generates a Hangup (Bye message in SIP) to the S-CSCF of the releasing party. It is noted that this message should be able to carry a cause value to indicate the reason for the generation of the hangup.~~

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

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

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

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

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

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

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

~~12. Steps 12 and 13 may be done in parallel with step 11. The Mobile initiates the release of the bearer PDP context.~~

~~13. The GPRS subsystem releases the PDP context. The IP network resources that had been reserved for the message receive path to the mobile for this session are now released. This is initiated from the GGSN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.~~

~~14. The SIP OK message is sent to the S-CSCF.~~

~~15. The S-CSCF of the other party forwards the OK to the S-CSCF of the releasing party.~~

~~16. The S-CSCF of the releasing party forwards the OK to the P-CSCF of the releasing party.~~

5.10.3.2 Network initiated session release - S-CSCF Initiated

The following flow shows a network-initiated IM CN subsystem application session release, where the release is initiated by the S-CSCF. This can occur in various service scenarios, e.g. administrative, or prepaid.

The procedures for clearing a session, when initiated by an S-CSCF, are as shown in the following information flow. The flow assumes that service-based local policy is in use.

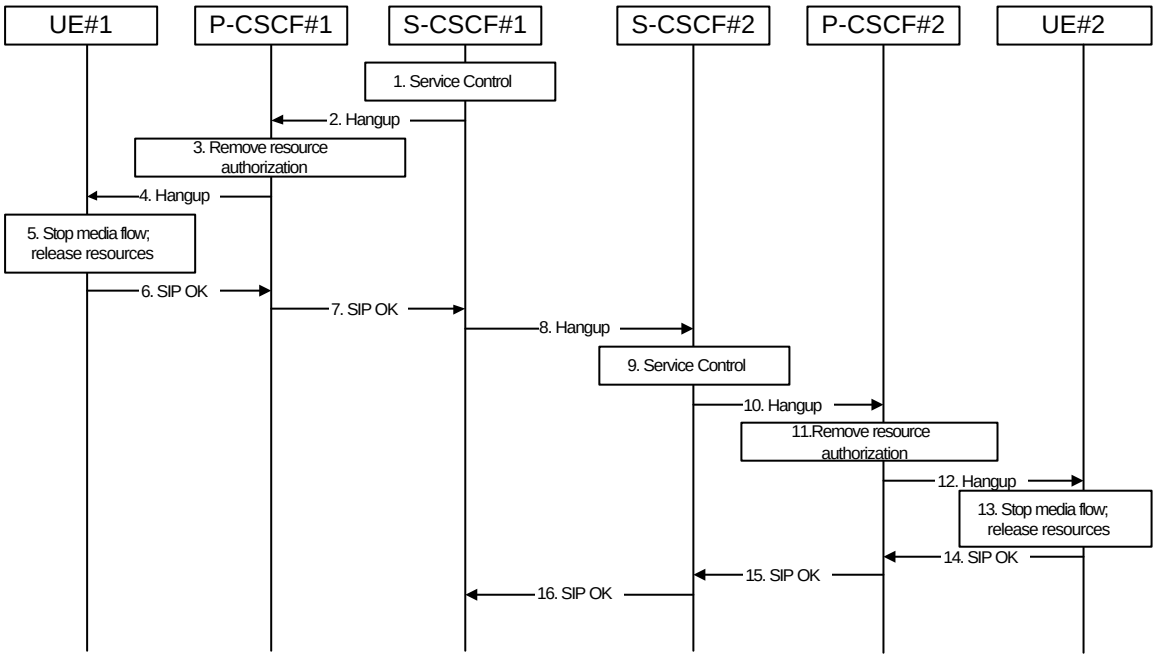


Figure 5.27: Network initiated session release - S-CSCF initiated

Information flow procedures are as follows:

1. S-CSCF#1 decides the session should be terminated, due to administrative reasons or due to service expiration.
2. S-CSCF#1 sends a Hangup message to P-CSCF#1
3. P-CSCF#1 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 ~~GPRS subsystem~~ to confirm that the IP bearers associated with the session have been deleted for UE#1.
4. P-CSCF#1 forwards the Hangup message to UE#1.
5. UE#1 stops sending the media stream to the remote endpoint, and releases the resources used for the session.
6. UE#1 responds with a SIP-OK message to its proxy, P-CSCF#1.
7. P-CSCF#1 forwards the SIP-OK message to S-CSCF#1.
8. S-CSCF#1 sends a Hangup message to S-CSCF#2. This is done at the same time as flow#2
9. S-CSCF#2 invokes whatever service logic procedures are appropriate for this ending session.

10. S-CSCF#2 forwards the Hangup message to P-CSCF#2.
11. P-CSCF#2 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 ~~GPRS subsystem~~ to confirm that the IP bearers associated with the session have been deleted for UE#2.
12. P-CSCF#2 forwards the Hangup message to UE#2.
13. UE#2 stops sending the media stream to the remote endpoint, and releases the resources used for the session.
14. UE#2 acknowledges receipt of the Hangup message with a SIP-OK final response, send to P-CSCF#2.
15. P-CSCF#2 forwards the SIP-OK final response to S-CSCF#2.
16. S-CSCF#2 forwards the SIP-OK final response to S-CSCF#1.

5.11 Procedures to enable enhanced multimedia services

5.11.1 Session Hold and Resume Procedures

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

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

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

5.11.1.1 Mobile-to-Mobile Session Hold and Resume Procedures

An IMS session was previously established between an initiating UE and a terminating UE. Each of these UEs has an associated P-CSCF ~~in the same network as their GGSN IP Connectivity Netwroks are located~~, and a S-CSCF assigned in their home network. These functional elements co-operate to clear the session, and the procedures are independent of whether they are located in the home or visited networks.

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

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

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

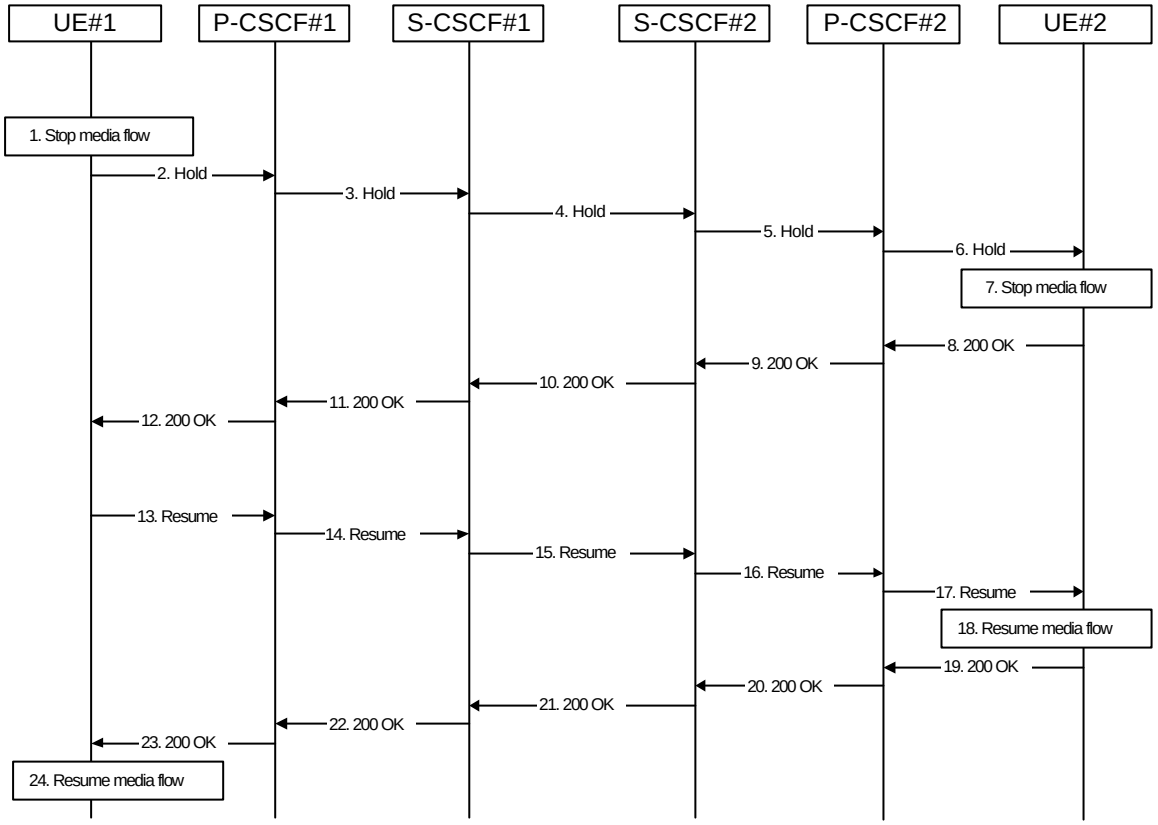


Figure 5.28: Mobile to Mobile session hold and resume

Information flow procedures are as follows:

1. UE#1 detects a request from the user to place a media stream on hold. UE#1 stops sending the media stream to the remote endpoint, but keeps the resources for the session reserved.

2. UE#1 sends a Hold message to its proxy, P-CSCF#1.

3. P-CSCF#1 forwards the Hold message to S-CSCF#1.

4. S-CSCF#1 forwards the Hold message to S-CSCF#2.

5. S-CSCF#2 forwards the Hold message to P-CSCF#2.

6. P-CSCF#2 forwards the Hold message to UE#2.

7. UE#2 stops sending the media stream to the remote endpoint, but keeps the resources for the session reserved.

8. UE#2 acknowledges receipt of the Hold message with a 200-OK final response, send to P-CSCF#2.

9. P-CSCF#2 forwards the 200 OK final response to S-CSCF#2.

10. S-CSCF#2 forwards the 200 OK final response to S-CSCF#1.

11. S-CSCF#1 forwards the 200 OK final response to P-CSCF#1.

12. P-CSCF#1 forwards the 200 OK final response to UE#1.

13. UE#1 detects a request from the user to resume the media stream previously placed on hold. UE#1 sends a Resume message to its proxy, P-CSCF#1.

14. P-CSCF#1 forwards the Resume message to S-CSCF#1.

15. S-CSCF#1 forwards the Resume message to S-CSCF#2.

16. S-CSCF#2 forwards the Resume message to P-CSCF#2.

17. P-CSCF#2 forwards the Resume message to UE#2.

18. UE#2 resumes sending the media stream to the remote endpoint.

19. UE#2 acknowledges receipt of the Resume message with a 200-OK final response, sent to P-CSCF#2.

20. P-CSCF#2 forwards the 200 OK final response to S-CSCF#2.

21. S-CSCF#2 forwards the 200 OK final response to S-CSCF#1.

22. S-CSCF#1 forwards the 200 OK final response to P-CSCF#1.

23. P-CSCF#1 forwards the 200 OK final response to UE#1.

24. UE#1 resumes sending the media stream to the remote endpoint.

5.11.1.2 Mobile-initiated Hold and Resume of a Mobile-PSTN Session

An IMS session was previously established between an initiating UE and a MGCF acting as a gateway for a session terminating on the PSTN, or between an initiating MGCF acting as a gateway for a session originating on the PSTN to a terminating UE. The UE has an associated P-CSCF ~~in the same network as its GGSN is located~~, an S-CSCF assigned in its home network, and a BGCF that chooses the MGCF. These functional elements co-operate to clear the session, and the procedures are independent of whether they are located in the subscriber's home or visited networks. Therefore there is no distinction in this section of home network vs. visited network.

The session hold and resume procedure is similar whether the UE initiated the session to the PSTN, or if the PSTN initiated the session to the UE. The only difference is the optional presence of the BGCF in the case of a session initiated by the UE. Note that the BGCF might or might not be present in the signalling path after the first INVITE is routed.

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

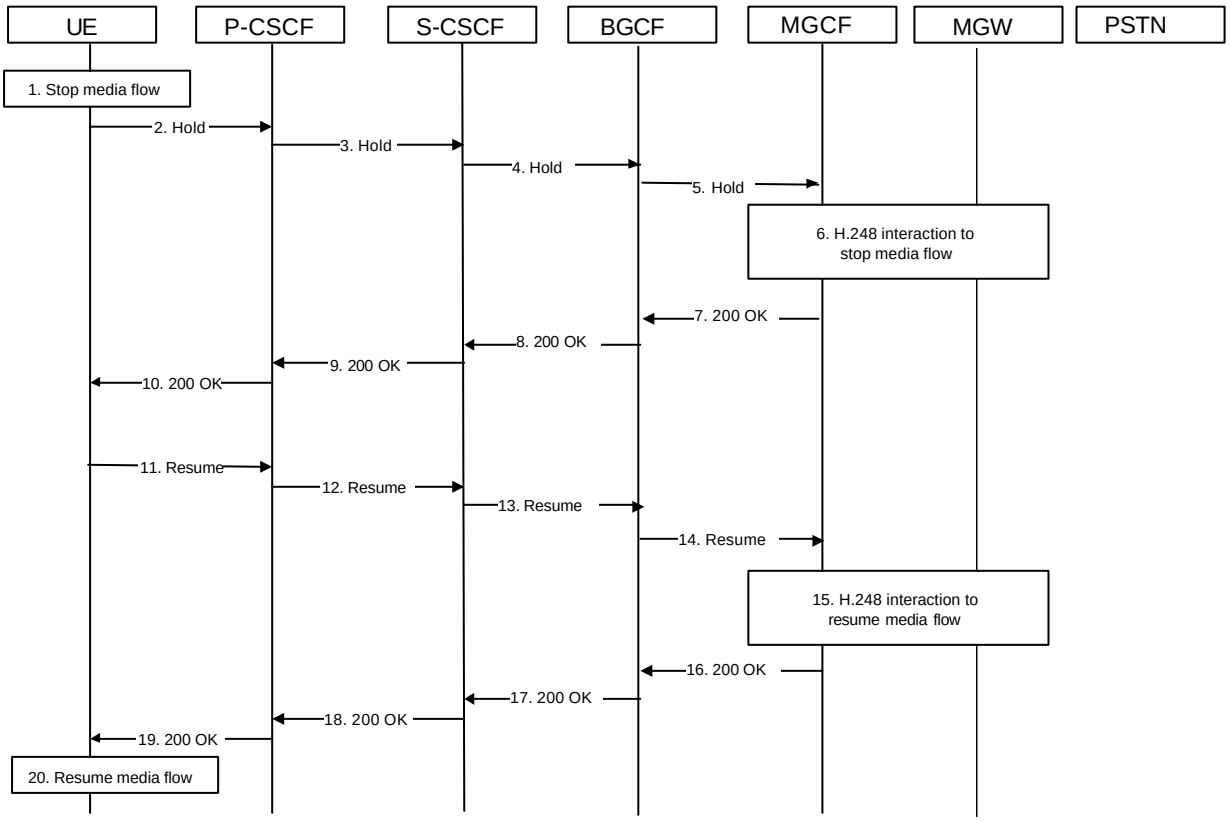


Figure 5.29: Mobile to PSTN session hold and resume

Information flow procedures are as follows:

1. UE detects a request from the user to place a media stream on hold. UE#1 stops sending the media stream to the remote endpoint, but keeps the resources for the session reserved.

2. UE sends a Hold message to its proxy, P-CSCF.
3. P-CSCF forwards the Hold message to S-CSCF.
4. S-CSCF forwards the Hold message to BGCF.
5. BGCF forwards the Hold message to MGCF.
6. MGCF initiates a H.248 interaction with MGW instructing it to stop sending the media stream, but to keep the resources for the session reserved.
7. MGCF acknowledges receipt of the Hold message with a 200-OK final response, send to BGCF.
8. BGCF forwards the 200-OK to the S-CSCF.
9. S-CSCF forwards the 200 OK final response to P-CSCF.
10. P-CSCF forwards the 200 OK final response to UE.
11. UE detects a request from the user to resume the media stream previously placed on hold. UE sends a Resume message to its proxy, P-CSCF.
12. P-CSCF forwards the Resume message to S-CSCF.
13. S-CSCF forwards the Resume message to BGCF.
14. BGCF forwards the Resume message to MGCF.
15. MGCF initiates a H.248 interaction with MGW instructing it to resume sending the media stream.
16. MGCF acknowledges receipt of the Resume message with a 200-OK final response, sent to BGCF.
17. BGCF forwards the 200 OK final response to the S-CSCF.
18. S-CSCF forwards the 200 OK final response to P-CSCF.
19. P-CSCF forwards the 200 OK final response to UE.
20. UE resumes sending the media stream to the remote endpoint.

5.11.2 Procedures for anonymous session establishment

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

5.11.2.1 Signalling requirements for anonymous session establishment

If the user requests the session to be anonymous, the UE must not reveal any identity information other than that required in the Remote-Party-ID header.

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

5.11.2.2 Bearer path requirements for anonymous session establishment

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

5.11.3 Procedures for codec and media characteristics flow negotiations

This section gives information flows for:

- the procedures for determining the set of negotiated characteritics between the endpoints of a multi-media session, determining the initial media characteristics (including common codecs) to be used for the multi-media session, and

- the procedures for modifying a session within the existing resources reservation or with a new resources reservation (adding/deleting a media flow, changing media characteristics including codecs, changing bandwidth requirements) when the session is already established.

5.11.3.1 Codec and media characteristics flow negotiation during initial session establishment

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

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

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

Once the session is established, the procedures of section 5.11.3.2 may be used by either endpoint to change to a different media characteristic (e.g. codec) that was included in the initial session description, and for which no additional resources are required for media transport. The procedures of section 5.11.3.3 may be used by either endpoint to change the session, which requires resources beyond those allocated to the existing session.

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

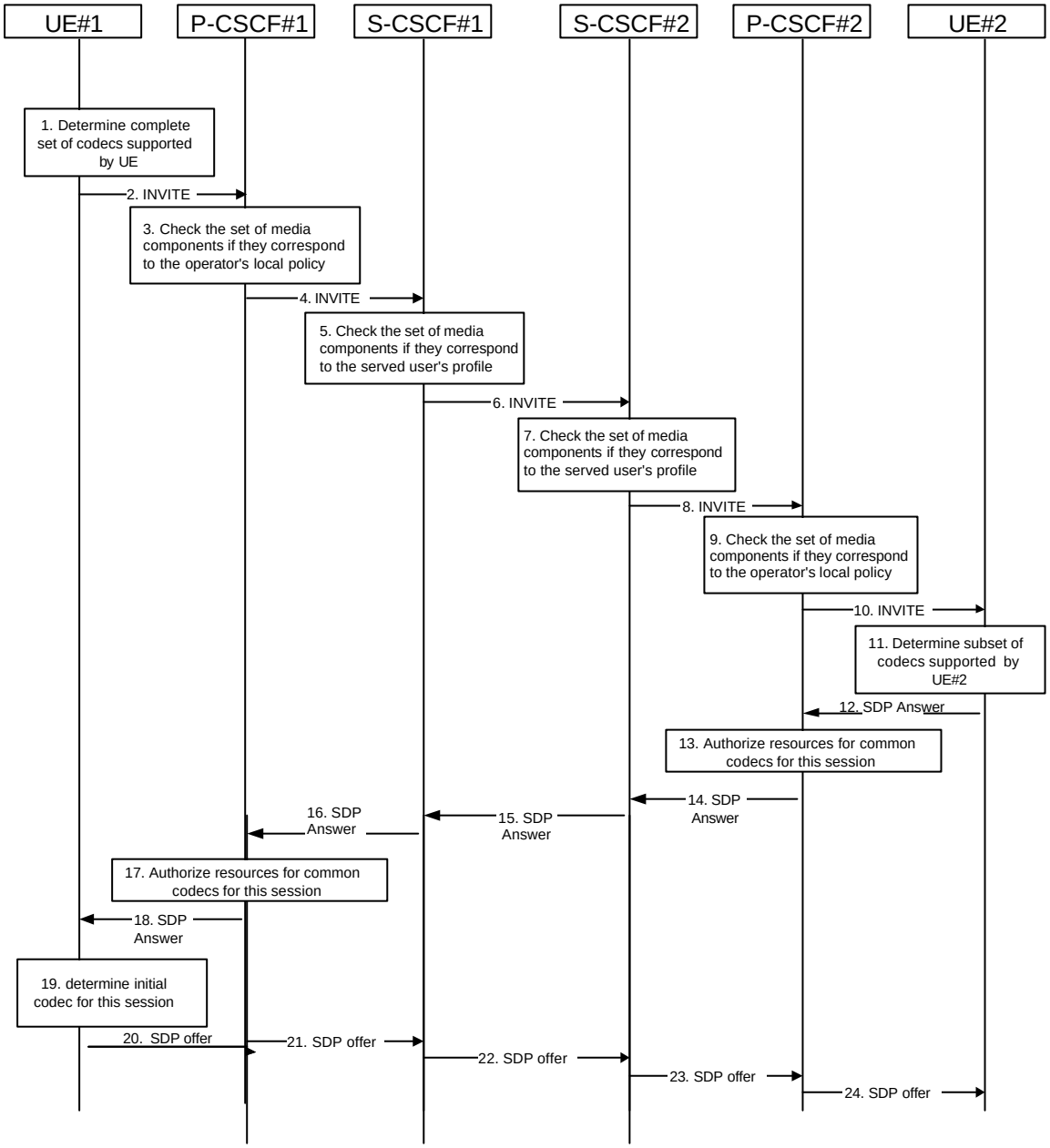


Figure 5.30: Codec negotiation during initial session establishment

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 that local policy 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 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.

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 that local policy 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 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. The Authorization-Token is generated by the PDF.

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.

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.

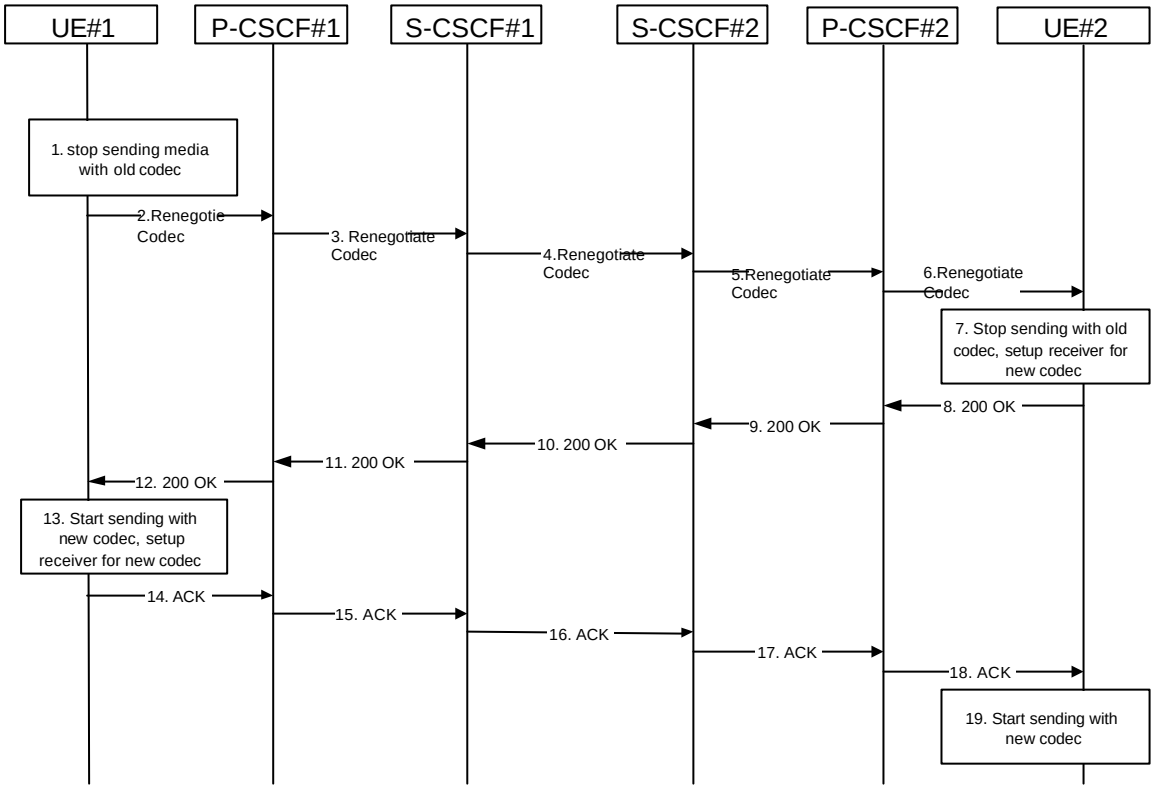


Figure 5.31: Codec or media flow change - same reservation

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.

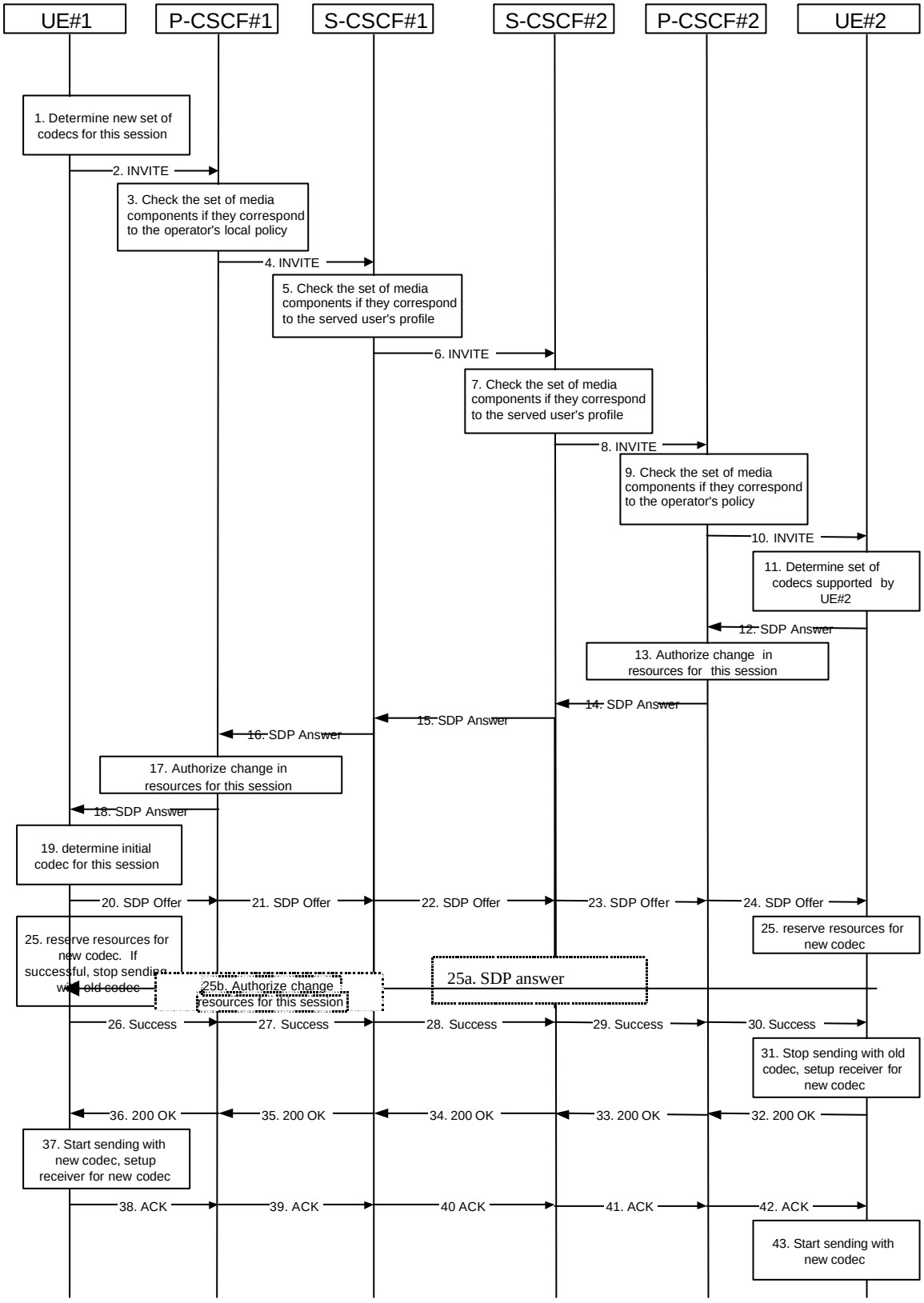


Figure 5.32: Codec or media flow change - new reservation

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 that local policy 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 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 that local policy 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 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. 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.

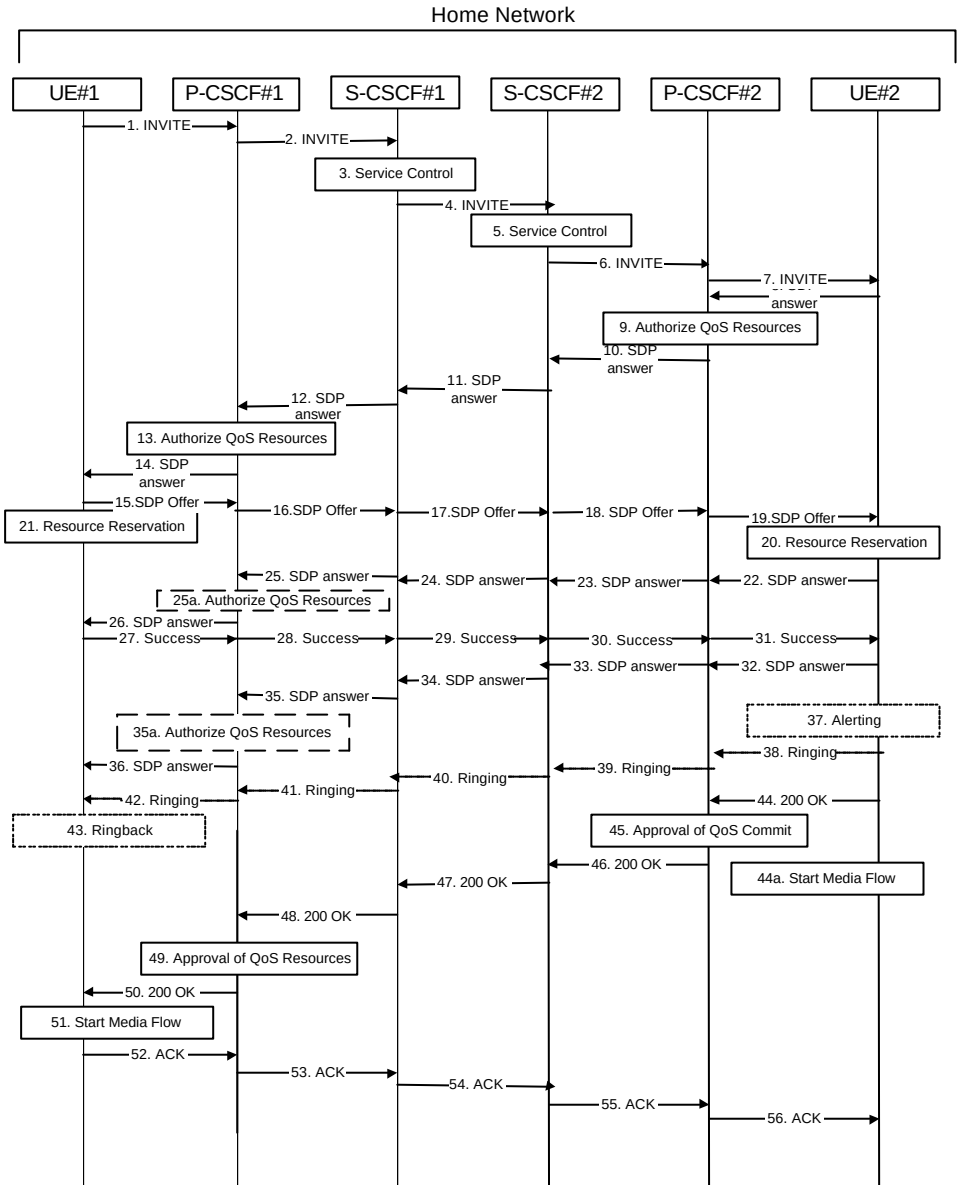


Figure 5.33: Multimedia session flow - addition of another media

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 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. 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.

9. 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

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

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

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

5.11.4.1 Procedures for providing the authenticated identity of the originating party

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

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

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

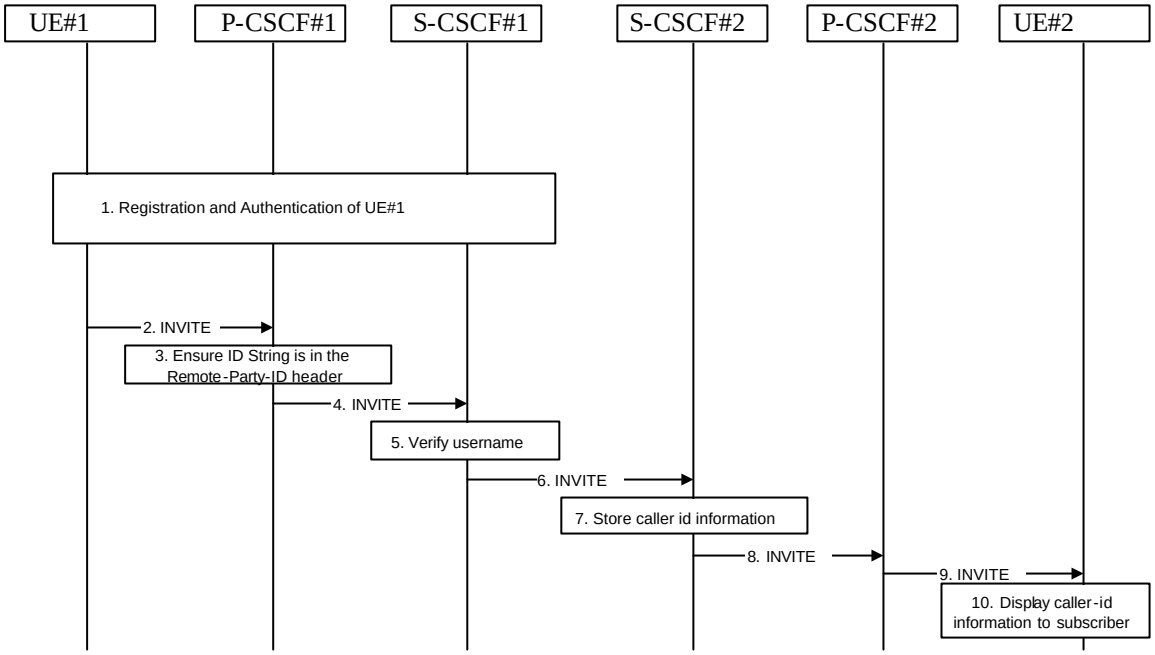


Figure 5.34: Providing the authenticated Identity of the originating party

The detailed procedure is as follows:

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

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

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

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

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

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

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

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

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

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) .

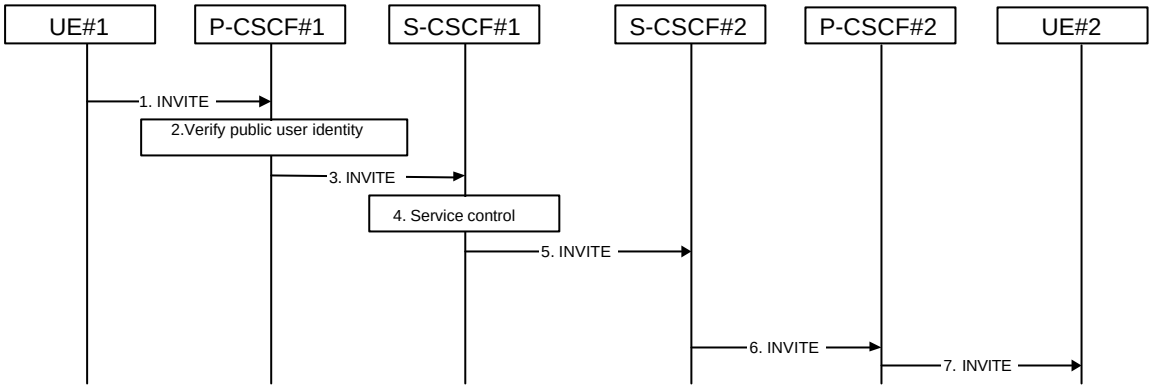


Figure 5.35: Blocking the identity of the originating party

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

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:

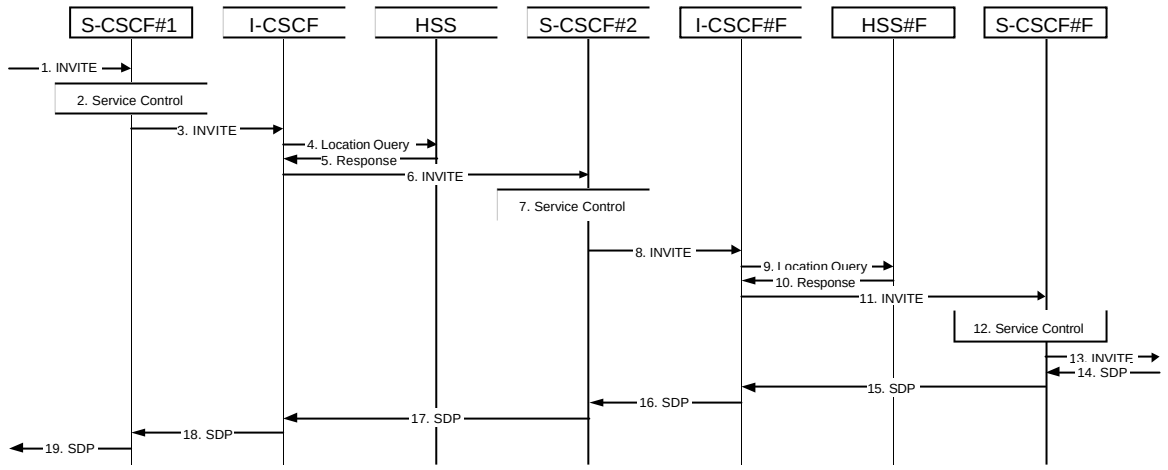


Figure 5.36: Session redirection initiated by S-CSCF to IMS

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. 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:

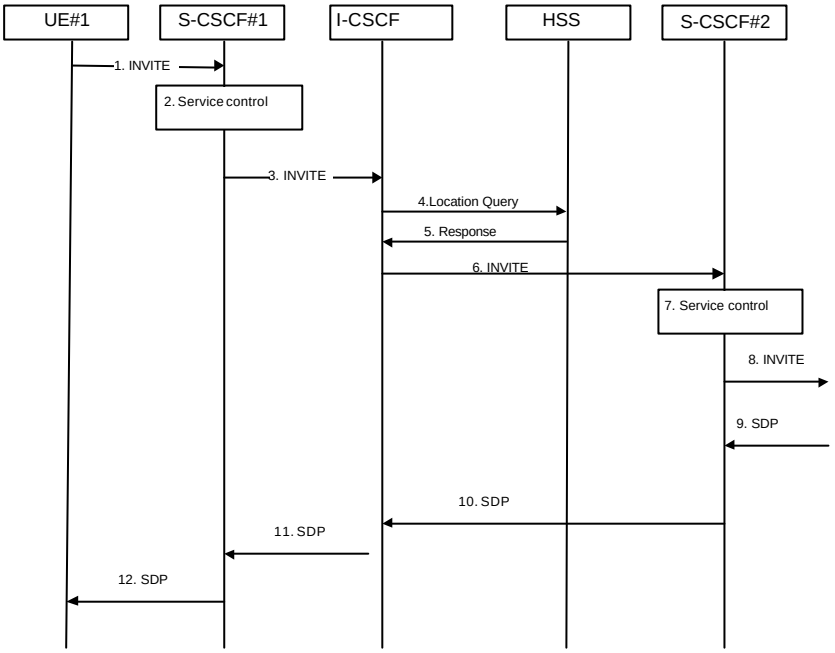


Figure 5.37: Session redirection to PSTN Termination (S-CSCF #2 forwards INVITE)

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 establshment 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:

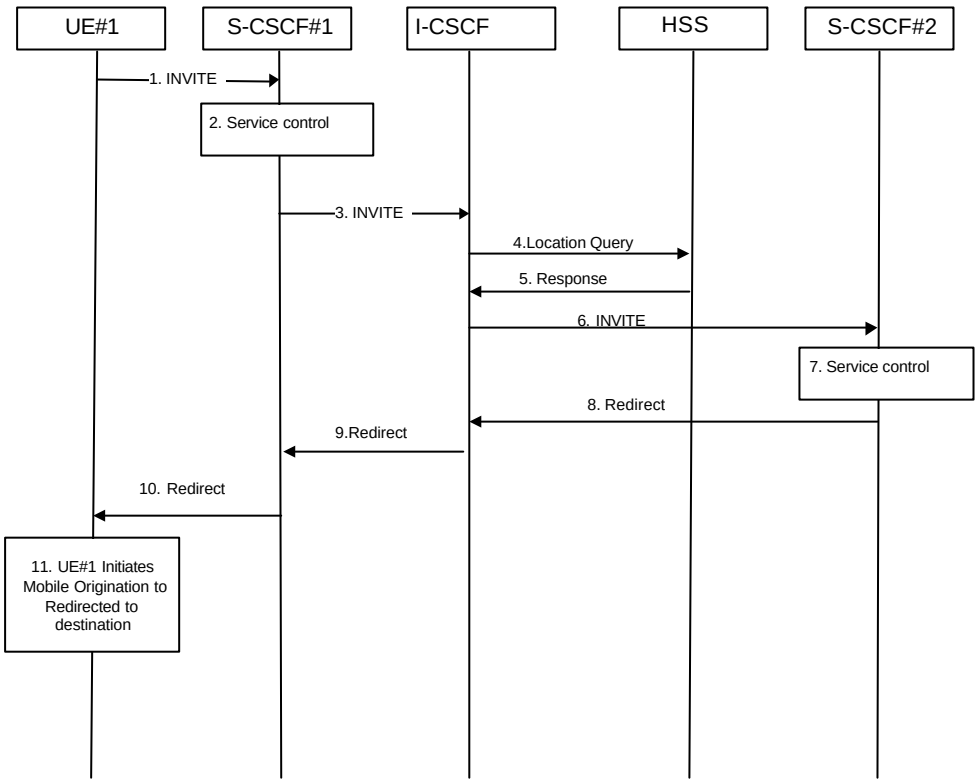


Figure 5.37a: Session redirection to PSTN Termination (REDIRECT to originating UE#1)

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 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.

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

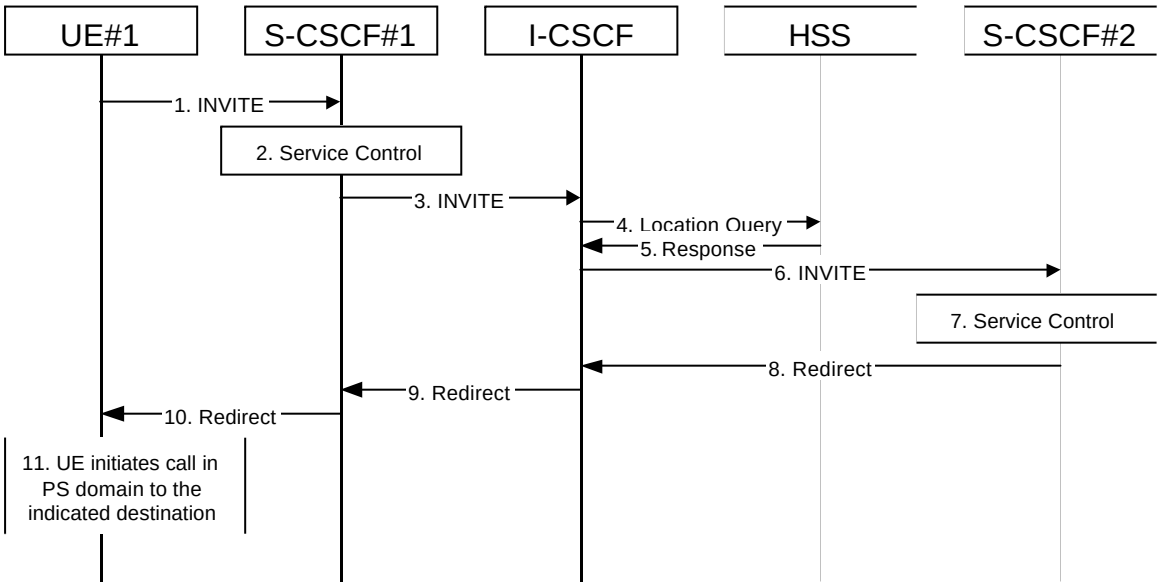


Figure 5.38: Session redirection initiated by S-CSCF to general endpoint

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.

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:

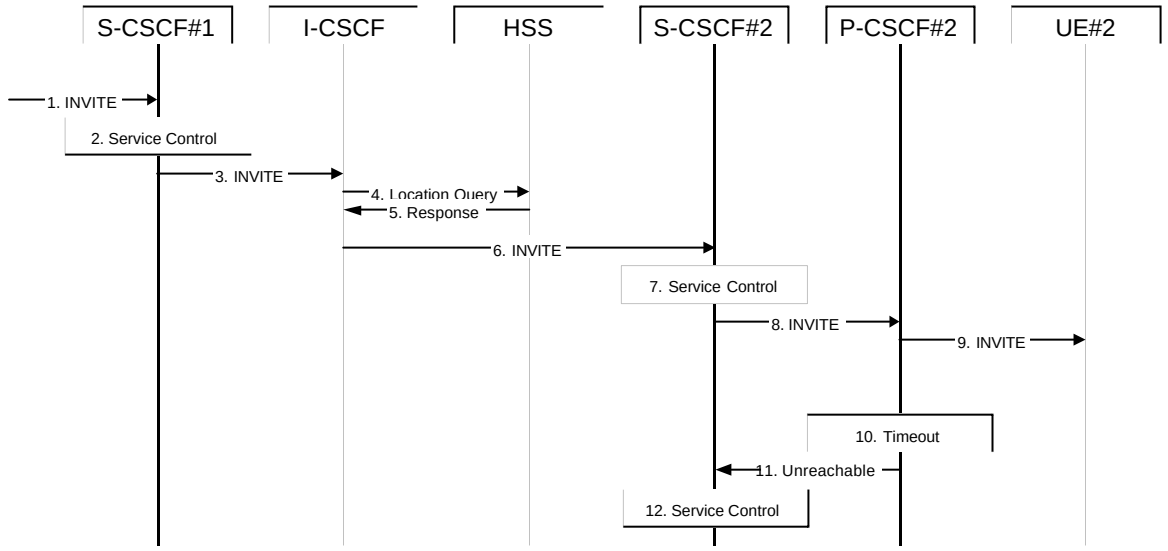


Figure 5.39: Session redirection initiated by P-CSCF

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, which may be a phone number, an email address, a web page, or anything else that can be expressed as a URL. Processing continues according to subsections 1, 2, or 3 above, based on the type of destination URL.

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:

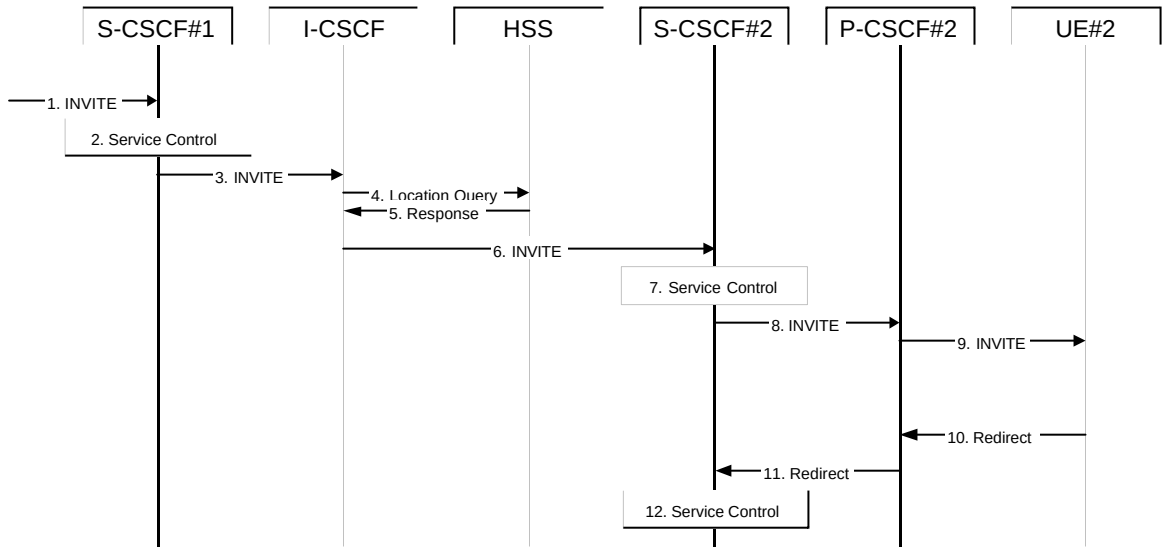


Figure 5.40: Session redirection initiated by UE

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. 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

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, 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. The procedures of subsection 1, 2, or 3 given above are followed, based on the type of URL.

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.

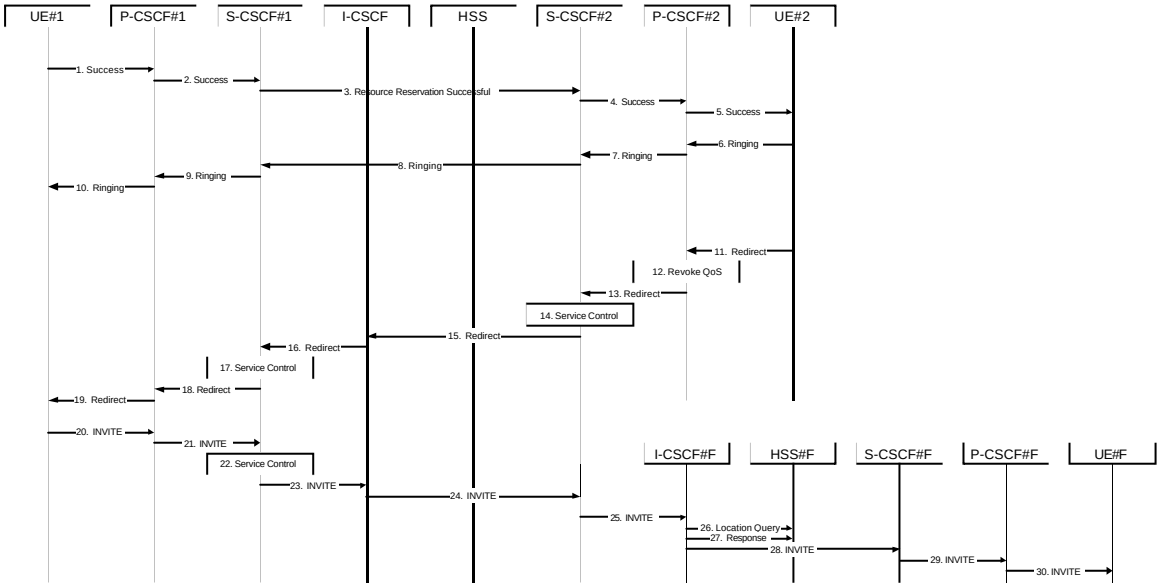


Figure 5.41: Session redirection after bearer establishment

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. The remainder of this session completes as normal.

5.11.6 Session Transfer Procedures

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

5.11.6.1 Refer operation

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

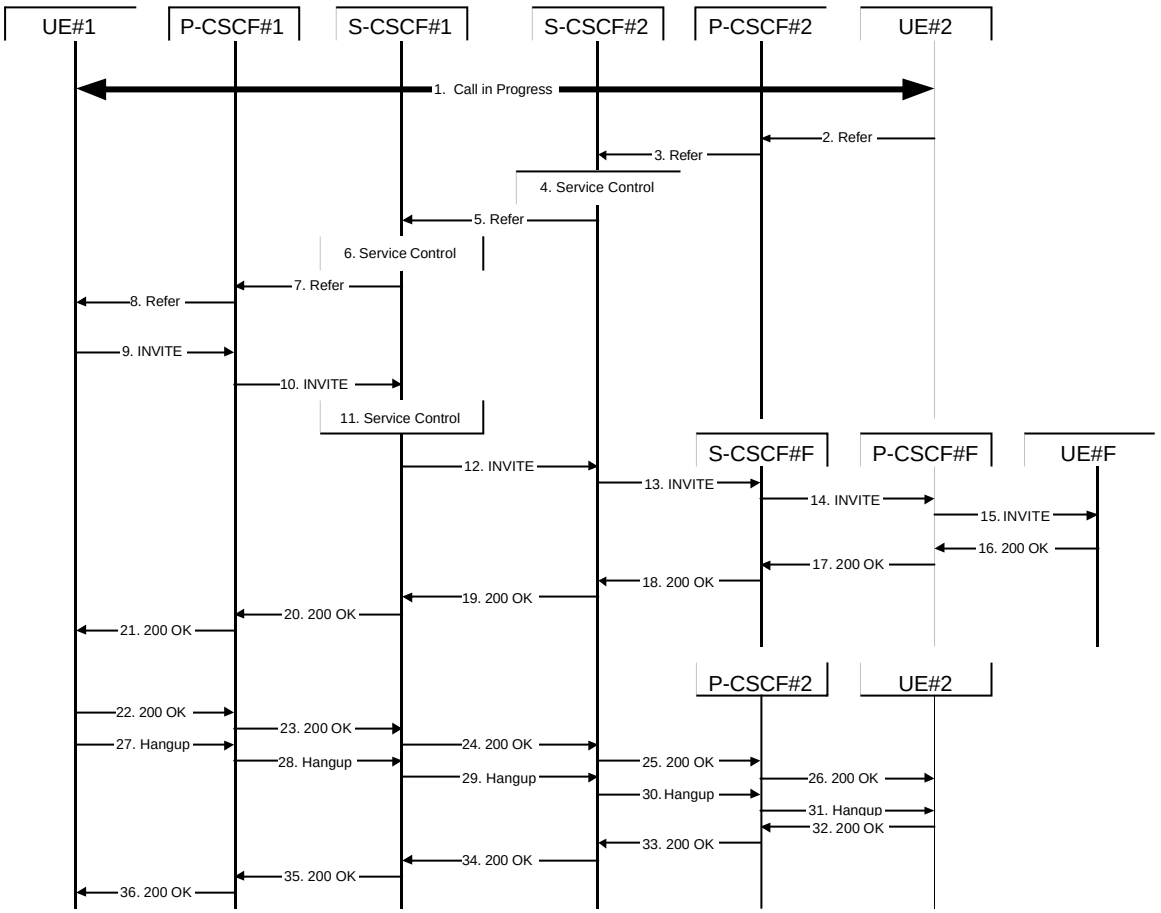


Figure 5.42: Refer operation

Step-by-step description of the information flow:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

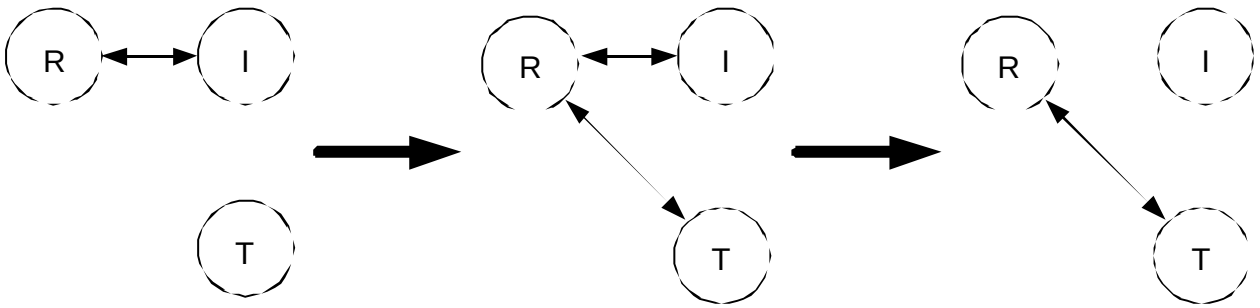
5.11.6.2 Application to Session Transfer Services

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

5.11.6.2.1 Blind Transfer and Assured Transfer

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

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

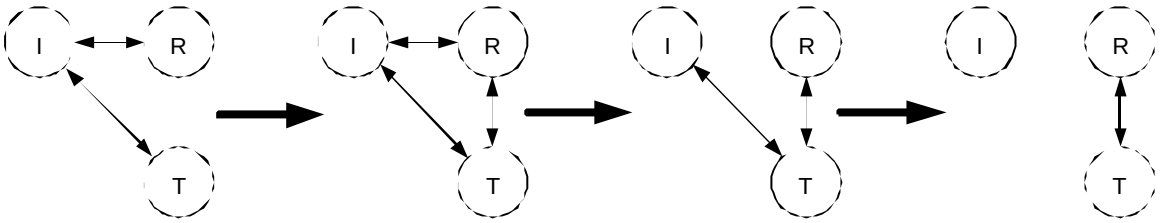


An Assured Transfer is identical to the above, except that I waits until the Refer successfully completes before issuing the BYE message to terminate its connection with R. If the new session from R to T were to fail, R would still have a session with I.

5.11.6.2.2 Consultative Transfer

A Consultative Transfer again starts with an existing session, established from the Initiator (I) to the Recipient (R). The Initiator first consults with the Target (T), then decides to transfer the original session to T.

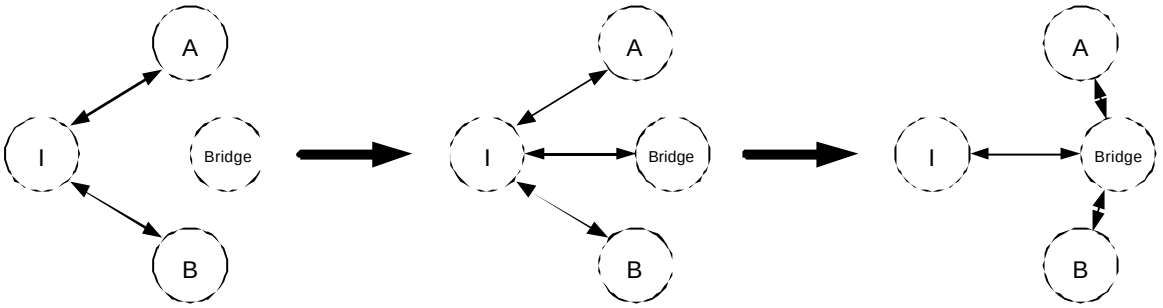
From the starting configuration, as shown in the leftmost diagram in the previous section, I places the session with R on hold and establishes a new session with T. This is shown in the leftmost diagram below. I then sends a Refer message to T, causing T to establish a session with R. This is shown in the second diagram. When the Refer operation completes, I clears its two active sessions, first with R (leaving the configuration as shown in the third diagram) then with T. The end configuration is shown in the rightmost diagram.



5.11.6.2.3 Three-way Session

A three-way session starts with an existing session, between the Initiator (I) and party (A). The initiator places this session on hold, and establishes a second session with party (B). The initiator then decides to create an ad-hoc conference of all three parties.

From the point where the initiator decides to create the ad-hoc conference, shown in the leftmost diagram below, the initiator establishes another session with a third-party conference bridge service. This is shown in the center diagram. The initiator then transfers both of the existing sessions, I->A and I->B, to the bridge, ending in the configuration shown in the rightmost diagram.



The conference bridge service is in control of the termination sequence. On termination of one of the three sessions, it may either terminate the other two sessions by use of the session clearing procedures of section 5.11, or may utilize the procedures of subsection 1 above to transfer one of the remaining endpoints to the other, resulting in a simple two-party session.

5.12 Mobile Terminating call procedures to unregistered Public User Identities

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

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

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

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

In Figure 5.43 below the Public User Identity is unregistered for IMS and the Public User Identity has services related to unregistered state. In this case, the HSS responds back to I-CSCF with an indication that I-CSCF should select S-CSCF for this MT call to the unregistered Public User Identity of the user or provide the I-CSCF with the previously allocated S-CSCF name. Before S-CSCF selection, I-CSCF shall query HSS for the information related to the required S-CSCF capabilities. I-CSCF selects a S-CSCF to invoke service logic and I-CSCF routes the call further to the selected destination. If the S-CSCF does not have the relevant information from the user profile then the S-CSCF shall download

the relevant information from HSS before it invokes service logic and any further actions in the call attempt. The service implemented by this information flow could be e.g. “Call Forward Unconditional.”

This is shown by the information flow in Figure 5.43:

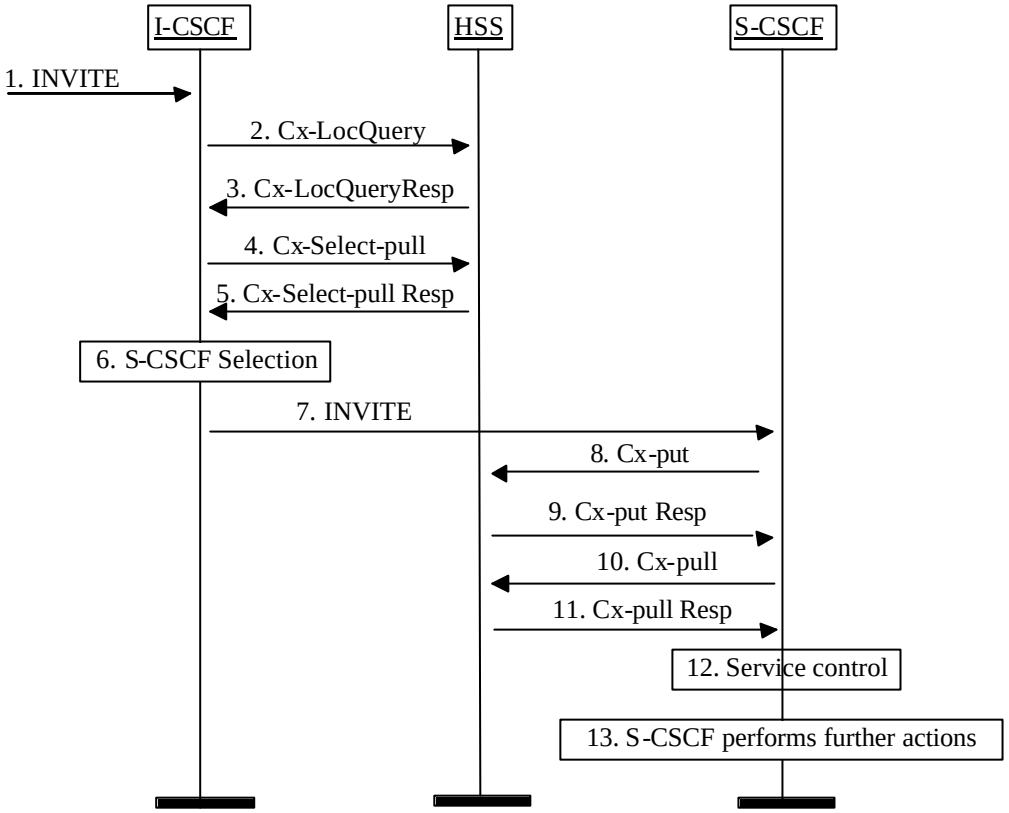


Figure 5.43: Mobile Terminating call procedures to unregistered IMS Public User Identity that has services related to unregistered state

1. I-CSCF receives an INVITE message.
2. I-CSCF queries the HSS for current location information.
3. HSS either responds with an indication that the Public User Identity is unregistered for IMS and I-CSCF should select a S-CSCF for the unregistered Public User Identity of the user or provides the I-CSCF with the previously allocated S-CSCF name for that user.
4. If the I-CSCF has not been provided with the location of the S-CSCF, the I-CSCF may send Cx-Select-Pull (unregistered, Public User Identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function. This query is optional.
5. The HSS shall send Cx-Select-Pull Resp (required S-CSCF capabilities) to the I-CSCF.
6. If the I-CSCF has not been provided with the location of the S-CSCF, the I-CSCF selects an S-CSCF for the unregistered Public User Identity of the user.
7. I-CSCF forwards the INVITE request to the S-CSCF.
8. The S-CSCF sends Cx-Put (Public User Identity, S-CSCF name) to the HSS. When multiple and separately addressable HSSs have been deployed by the network operator, then the S-CSCF needs to query the SLF to resolve the HSS. The HSS stores the S-CSCF name for unregistered Public User Identities of that user. This will result in all terminating traffic for unregistered Public User Identities of that user being routed to this particular S-CSCF until the registration period expires or the user attaches the Public User Identity to the network. Note: Optionally the S-CSCF can omit the Cx-Put request if it has the relevant information from the user profile.
9. The HSS shall send Cx-Put Resp to the I-CSCF to acknowledge the sending of Cx-Put.

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

11. The HSS shall return the information flow Cx-Pull Resp (user information) to the S-CSCF. The S-CSCF shall store it for that indicated Public User Identity.

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

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

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

5.12.2 Mobile Terminating call procedures to unregistered Public User Identitythat 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 Identityhas no services related to unregistered state.

This is shown in the following information flow (figure 5.44):

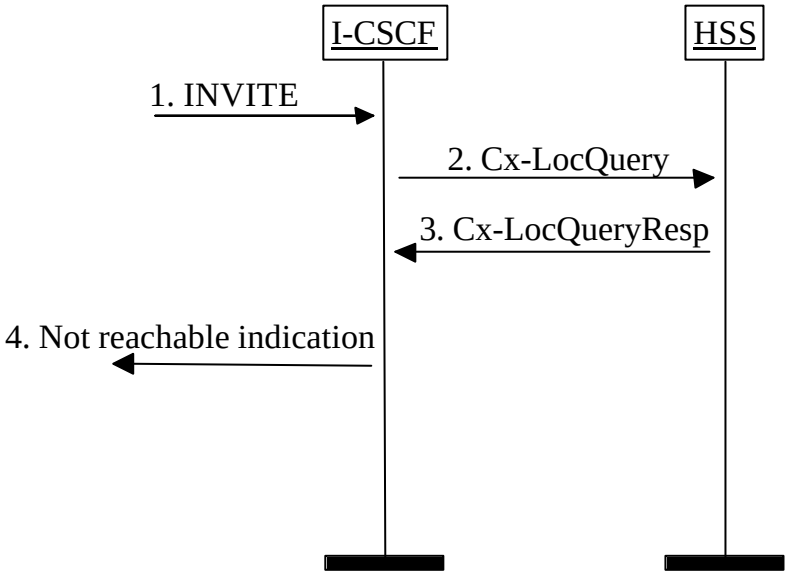


Figure 5.44: Mobile Terminating call procedures to unregistered Public User Identity that has no services related to unregistered state

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.

I-CSCF responds to the origin of the request that the user is not reachable at the moment.

5.13 IMS Emergency Sessions

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

5.13.1 Requirements for IMS Emergency Sessions

A CS capable UE shall use the CS domain for emergency services.

5.13.2 Procedures for SIP Emergency Session Establishment

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

5.13.3 Procedures for IMS Emergency Session Establishment

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

~~It shall be possible for the network to identify that a PDP context to be activated is for emergency use (signalling and media context). It allows to apply special treatment (e.g. with respect to filtering, higher priority, routing, QoS) of IMS emergency sessions.~~

~~If the UE is not attached to GPRS network, then it shall first perform a GPRS attach. It shall be possible for the network to discriminate between a normal Attach and an Attach for emergency use.~~

5.14 Interactions involving the MRFC/MRFP

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

5.14.1 Interactions between the UE and the MRFC

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

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

5.14.2 Service control based interactions with the MRFC

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

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

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

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

specific service such as identification of the announcement to be played or identification of the specific transcoding requirements.

5.15 Mobile Terminating session procedure for unknown user

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

5.15.1 Unknown user determined in the HSS.

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

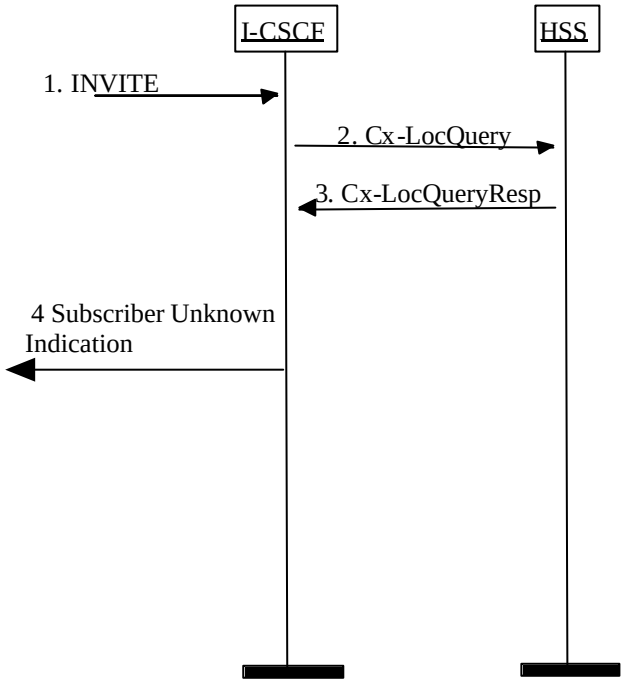


Figure 5.45 HSS determination of unknown user.

1) I-CSCF receives an INVITE.

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

3) HSS responds with an indication that the user is unknown

4) The I-CSCF responds to the origin of the request that the user is unknown.

5.15.2 Unknown user determined in the SLF

In Figure 5.46 the unknown status of the requested party is determined in the SLF. The I-CSCF requests information on the user to be reached and the SLF responds back to the I-CSCF with an indication that the user is unknown. The I-CSCF uses the indication that the user is unknown returned from the SLF to formulate the correct SIP message back towards the originating party to inform them that the user is unknown.

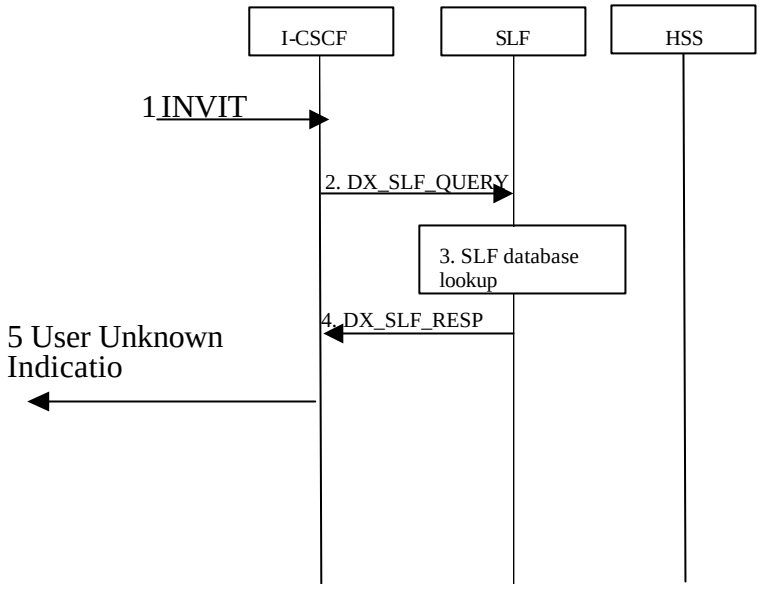


Figure 5.46 SLF determination of unknown user.

1) The ICSCF receives an INVITE request and now has to query for the location of the user's subscription data.

2) The I-CSCF sends a DX_SLF_QUERY to the SLF and includes as parameter the user identity which is stated in the INVITE request.

3) The SLF looks up its database for the queried user identity.

4) The SLF answers with an indication that the user is unknown.

5) The I-CSCF responds to the origin of the request that the user is unknown.

5.16 IMS messaging concepts and procedures

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

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

5.16.1 Immediate Messaging

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

5.16.1.1 Procedures to enable Immediate Messaging

IMS users shall be able to exchange immediate messages with each other by using the procedure described in this sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions on message length, FFS).

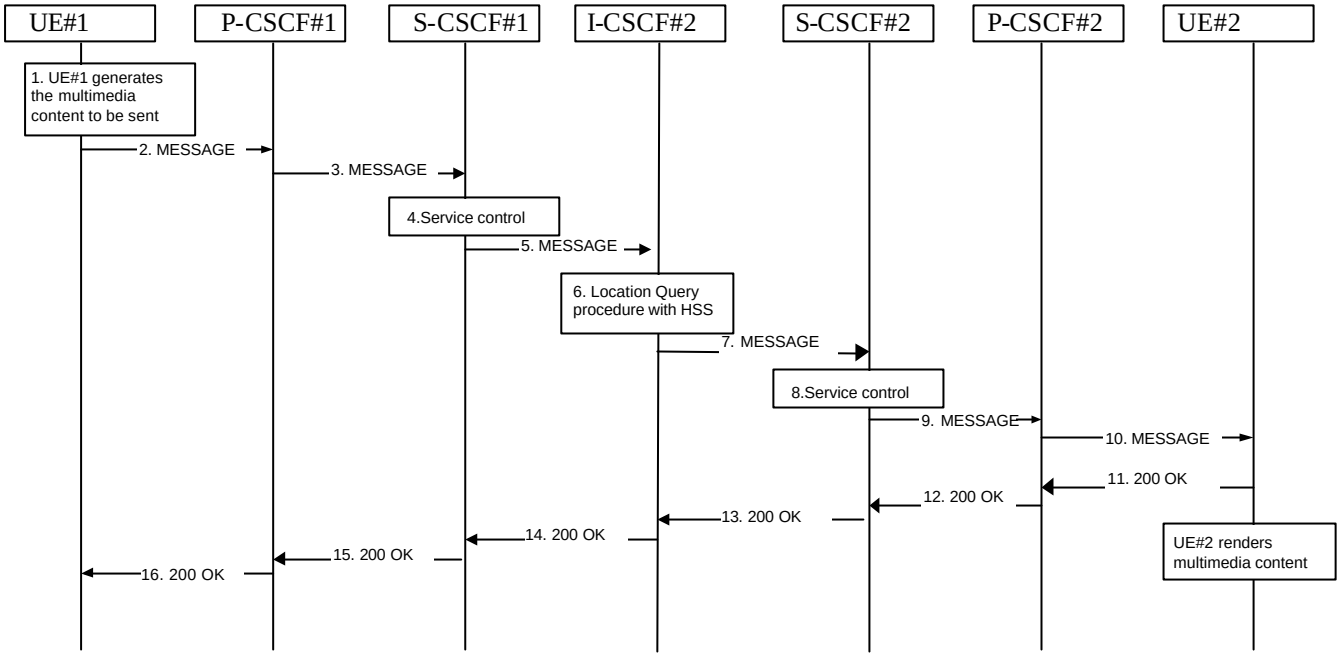


Figure 5.47: Immediate Messaging procedure

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. S-CSCF#1 performs whatever service control logic is appropriate for this MESSAGE request.
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. S-CSCF#2 performs whatever service control logic is appropriate for this MESSA GE request.
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 200OK response. The 200OK response traverses the transaction path back to UE#1.

5.16.2 Session-based Messaging

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

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. The details of the impacts of Session-based Messaging in IMS are for further study."

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

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

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

X.1 Mobility related concepts

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

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

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

X.1.1 Procedures for P-CSCF discovery

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

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

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

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

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

X.1.1.1 GPRS procedure for P-CSCF discovery

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

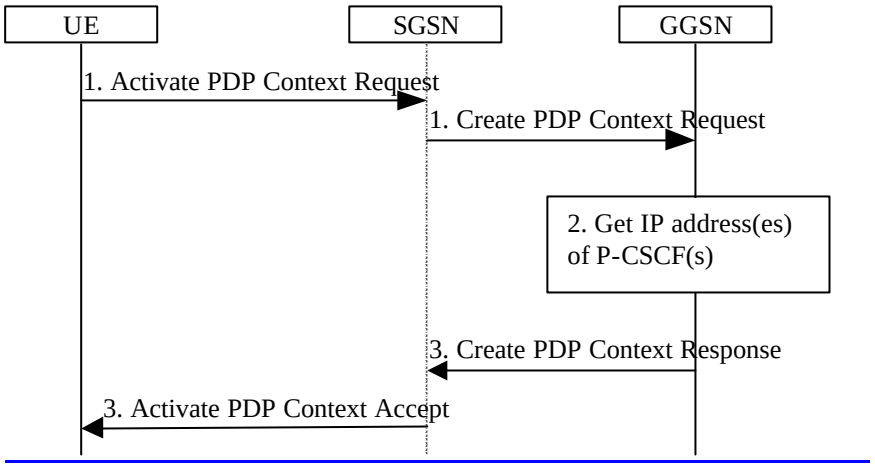


Figure X.1: P-CSCF discovery using PDP Context Activation signalling

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

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

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

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

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

X.2 QoS related concepts

X.2.1 QoS Requirements for IM CN subsystem signalling

When the UE uses GPRS-access for IMS services, it shall be able to establish a dedicated signalling PDP-Context for IM Subsystem related signalling or utilize a general-purpose PDP context for IM subsystem signalling traffic. The application level signalling flag is used to indicate the dedicated signalling PDP context. If the network-operator does not support a dedicated signalling PDP context, the network will consider the PDP context as a general-purpose PDP context.

A dedicated signalling PDP context provides dedicated IP-Connectivity Access Network bearers for IM CN subsystem signaling traffic, hence architectural requirements described in clause 4.2.6 for the usage of dedicated bearer resources shall be applied. The UE is not trusted to implement these restrictions, therefore the restrictions are enforced in the GGSN by the operator of the GGSN.

X.2.1.1 Establishing PDP Context for IM CN Subsystem Related Signalling

It shall be possible for the UE to convey to the network the intention of using the PDP context for IM Subsystem related signalling. For this purpose it uses the mechanism for 'PDP Context Used for Application Level Signalling Transport' as described in TS23.207. A signalling flag determines any rules and restrictions that shall apply at the GGSN for that PDP context, these rules and restrictions are described in section 4.2.6. It shall not be possible to modify a general purpose PDP context into a dedicated PDP context for IM Subsystem related signalling and vice versa.

The QoS profile parameters for this PDP context are appropriate for IM Subsystem related signalling. The QoS profile parameters are detailed in TS23.107. The signalling flag and the QoS profile parameters may be used independently of each other.

X.2.1.2 Deletion of PDP Context used to transport IMS SIP signaling

In case the GPRS subsystem deletes the PDP Context used to transport IMS SIP signaling, then according to clause 5.10.3.0 the UE shall initiate a procedure to re-establish a PDP Context for IMS signaling transport. If there are any IMS related PDP contexts active, the re-establishment of the PDP context to transport IMS signalling shall be perfomed by using the Secondary PDP Context Activation Procedure as defined in TS 23.060 [23].

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

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

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

1. QoS Signalling at Different Bearer Service Control Levels

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

X.2.3 Interaction between GPRS QoS and session signaling

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

At PDP context setup the user shall have access to either GPRS without service-based local policy, or GPRS with service-based local policy.

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

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

The GGSN contains a Policy Enforcement Function (PEF).

X.2.3.1 Resource Reservation with Service-based Local Policy

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

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

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

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

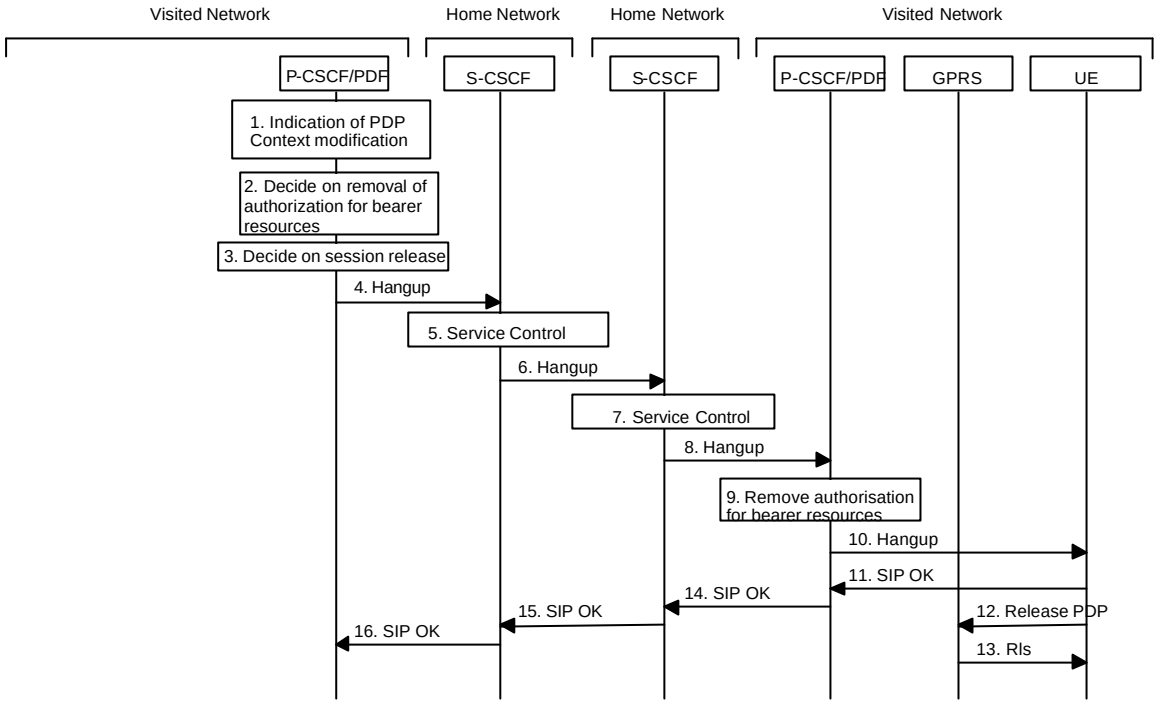


Figure X.2: Network initiated session release - P-CSCF initiated after loss of radio coverage

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

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

3. The P-CSCF decides on the termination of the session. If the P-CSCF decides to terminate the session then the P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this session. The P-CSCF/PDF shall perform the 'Revoke Authorization for UMTS and IP Resources' procedure (see 3GPP TS 23.207) in case that all IP bearers associated with the session have not been deleted yet.

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

4. The P-CSCF generates a Hangup (Bye message in SIP) to the S-CSCF of the releasing party. It is noted that this message should be able to carry a cause value to indicate the reason for the generation of the hangup.

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

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

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

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

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

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

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

12. Steps 12 and 13 may be done in parallel with step 11. The UE initiates the release of the bearer PDP context.

13. The GPRS subsystem releases the PDP context. The IP network resources that had been reserved for the message receive path to the UE for this session are now released. This is initiated from the GGSN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.

14. The SIP OK message is sent to the S-CSCF.

15. The S-CSCF of the other party forwards the OK to the S-CSCF of the releasing party.

16. The S-CSCF of the releasing party forwards the OK to the P-CSCF of the releasing party.

X.3 Address and identity management concepts

X.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 (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 .

X.4 IMS Emergency sessions

It shall be possible for the network to identify that a PDP context to be activated is for emergency use (signalling and media context). It allows to apply special treatment (e.g. with respect to filtering, higher priority, routing, QoS) of IMS emergency sessions.

If the UE is not attached to GPRS network, then it shall first perform a GPRS attach. It shall be possible for the network to discriminate between a normal Attach and an Attach for emergency use.

Annex A (Informative): Information flow template

This section describes the template used in developing information flow (IF) procedures.

X.Y.Z "Name of procedure (e.g., Terminal location registration)"

In this section, provide a brief prose description of the service or network capability. The "X.Y.Z." refers to the section heading number.

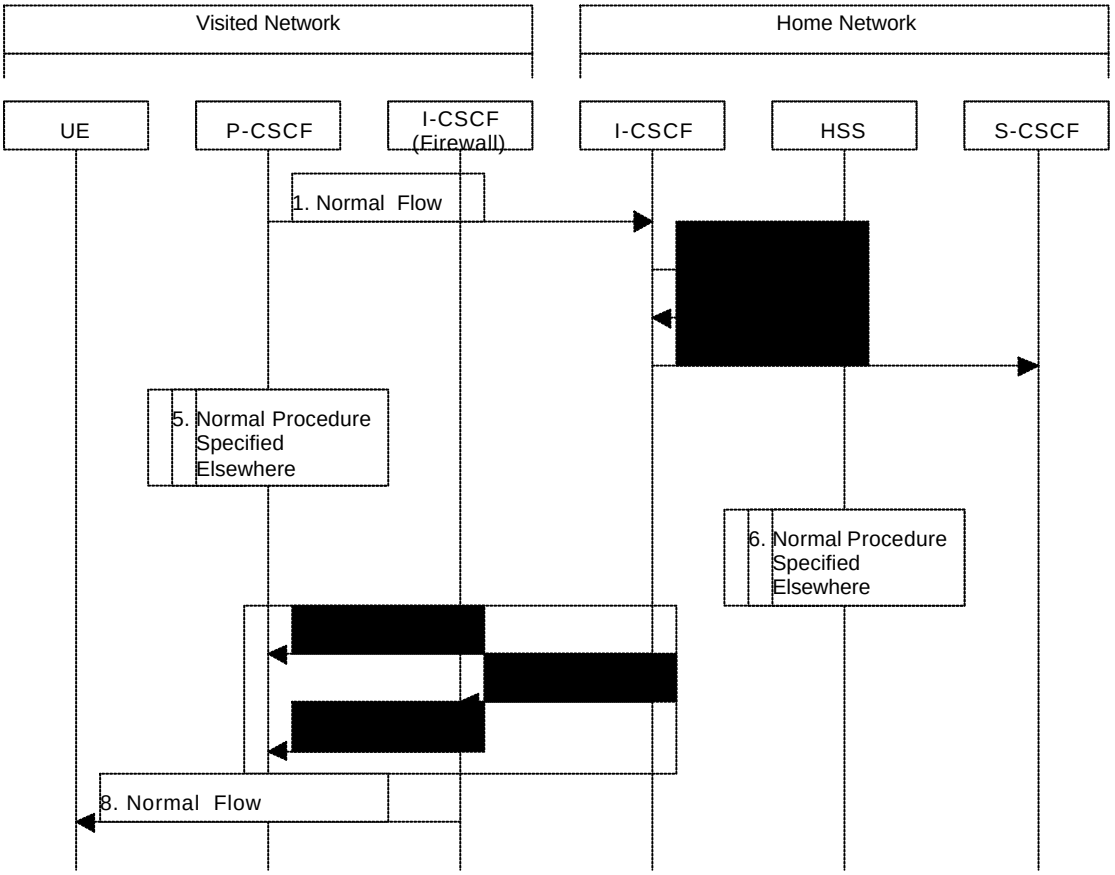


Figure A.1: Information Flow Template

This sub-section consists of subparagraphs each dedicated to one information flow of the IF diagram. For each information flow, a detailed description is provided on the information flow name, certain information elements (IEs) within the information flow, whether the IE is mandatory or optional (M/O), in the sequence as shown in the IF diagram. FE actions (FEA) are also provided in this section. This sub-section format is proposed as follows:

1. Initial information flow: One should normally describe the initiating FE Action (FEA) leading to the first flow. Any information that is specifically required to support the operation should be mentioned (e.g. this flow conveys the user identity to the HSS).

2. Each paragraph should contain a brief description of the flow and any specific start and end FEAs. When information to be conveyed is optional, the conditions for its inclusion should be specified and the response to its presence when received should also be specified (e.g., Include IP Address when condition xyz occurs). For an information flow that is required, the description should indicate whether a response is required based on successful outcome to the received IF, failed outcome, both or neither. e.g., "Response is required indicating Success or Failure".

3. Flows may occur in either direction but not both at the same time. To indicate a shorthand for multiple flows, use a procedure box as in flow 5 or 6.

4. Flows that are an optional part of the procedure should be shown as dotted arrows as in flow 4. These may appear in either direction.

5. A set of flows, representing a common procedure, is shown by a box. The procedure should be numbered and named with a name that corresponds to the procedure as described elsewhere. The location of the box on an entity represents the start of the common procedure regardless of the number of the entities involved in the procedure.

6. An optional set of flows is represented as a dashed box. Otherwise the use is the same as in flow 5.

7. A small number of alternative flows may be shown within a dashed box. The alternatives are shown by a letter immediately following the flow number, e.g. 7a, 7b, 7c, etc. Where a single alternative results in multiple flows, they must be shown with an indication of the proper sequence, e.g. 7b1, 7b2. The subparagraph describing the information flow must describe the decision process taken in choice of alternatives.

   7a. Alternative (a) is described. If alternative (a) is a single information flow, the contents and purpose of that information flow is included here.

   7b. Alternative (b) is described.

      7b1. The first information flow of alternative (b) is described

      7b2. The second information flow of alternative (b) is described. Etc.

8. The final flow in a procedure may provide additional information regarding other procedures that might follow it but such information is not required.

The general characteristics of the information flow template are as follows:

- All relevant functional entities are contained in the flow diagram. Only relevant entities need be shown.

- When an element occurs only in an information flows for which several alternatives exist, the description box for the functional entity and the vertical line shall be dashed lines.

- The specific network affiliation of functional entities may be shown using a labelled bracket over the specific entities as shown in the figure (e.g., Home Network). Such labelling is not required unless the flow would not be clear without it.

- The number associated with each flow provides a “handle” to the functional entity action (FEA) executed by the FE receiving the flow. This number is known only within the scope of the specific information flow diagram. The description of this functional entity action (FEA) immediately follows the information flow description.

- Common Procedures described elsewhere can be used in the information flows in order to simplify the diagram. These may be either required or optional.

- Each common procedure is treated as a single action and therefore is given a unique number.

- An optional flows (flows 4 and 6) are indicated by a dashed arrow or box.

- Co-ordinated flows or flows that illustrate parallel actions are indicated by the flow text description. For example one might see a description such as: "flows 5 and 6 may be initiated any time after flow 3".

- Sequential operation is assumed unless indicated otherwise.

Annex B (Informative):
[void]

Annex C (informative): Optional configuration independence between operator networks

The I-CSCF (THIG) functionality may be used to hide the network topology from other operators. It shall be possible 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.

The specific mechanism chosen needs to take into account the following separate aspects:

Network management. In the case that network details (i.e. S-CSCF addresses) are visible by other external network elements, any (temporary or permanent) changes to the network topology need to be propagated to network elements outside of the operator's network. This is highly undesirable from a network management perspective.

Network scalability. Establishing security associations on a pair-wise basis among all CSCFs is likely to be unscalable. The security associations shall be independent of the number of network elements.

Competitivity aspects. The operational details of an operator's network are sensitive business information that operators are reluctant to share with their competitors. While there may be situations (partnerships or other business relations) where the sharing of such information is appropriate, the possibility should exist for an operator to determine whether or not the internals of its network need to be hidden.

Security aspects. Network element hiding may help to reduce the vulnerability of the overall system to external attacks (e.g. denial of service attacks). Further work is needed in this area.

Annex D (informative): Change history

Date	TSG #	TSG Doc.	CR#	Rev	Subject/Comment	In	Out
2001-04	SA#11	SP-010121	-		Creation of version 5.0.0	2.0.0	5.0.0
2001-06	SA#12	SP-010335	038	1	Combined Services Architecture	5.0.0	5.1.0
2001-06	SA#12	SP-010335	040	1	Security functional roles for Roles of Session Control	5.0.0	5.1.0
2001-06	SA#12	SP-010335	009	1	Registration of users with multiple public identifiers: avoiding useless registration messages	5.0.0	5.1.0
2001-06	SA#12	SP-010335	020	1	Registration information removal from S-CSCF	5.0.0	5.1.0
2001-06	SA#12	SP-010335	028	1	SLF Mechanism for all kinds of CSCF types	5.0.0	5.1.0
2001-06	SA#12	SP-010335	014	1	Registration flows	5.0.0	5.1.0
2001-06	SA#12	SP-010335	042		Definition of default codec in 23.228	5.0.0	5.1.0
2001-06	SA#12	SP-010335	023	1	Changes for DTMF ToneInterworking	5.0.0	5.1.0
2001-06	SA#12	SP-010335	044		Session handling in IM (Redirection)	5.0.0	5.1.0
2001-06	SA#12	SP-010335	015	1	MT call procedures for unregistered subscriber	5.0.0	5.1.0
2001-06	SA#12	SP-010335	017	1	Providing local services in the IM Subsystem	5.0.0	5.1.0
2001-06	SA#12	SP-010335	018	1	Emergency call handling in the IMS	5.0.0	5.1.0
2001-06	SA#12	SP-010335	046		Subscription Updating Procedure	5.0.0	5.1.0
2001-06	SA#12	SP-010335	036	1	23.228 Additional information on the service control architecture	5.0.0	5.1.0
2001-09	SA#13	SP-010553	010		CR on “23.228 Correction for the usage of CAMEL services on top of IMS”	5.1.0	5.2.0
2001-09	SA#13	SP-010553	011	2	QoS-Assured Preconditions	5.1.0	5.2.0
2001-09	SA#13	SP-010553	019	1	SIP Compression	5.1.0	5.2.0
2001-09	SA#13	SP-010553	022		CR on “Incorrect text on interworking with ISUP”	5.1.0	5.2.0
2001-09	SA#13	SP-010553	025		Corrections to 23.228 V5.0.0	5.1.0	5.2.0
2001-09	SA#13	SP-010553	032		CR on “Correct information related to IPv4 handling”	5.1.0	5.2.0
2001-09	SA#13	SP-010553	045		CR on “MRF functionality and architecture”	5.1.0	5.2.0
2001-09	SA#13	SP-010553	049	2	Awareness of local SIP services in the IM Subsystem	5.1.0	5.2.0
2001-09	SA#13	SP-010553	050		Token generation at the PCF	5.1.0	5.2.0
2001-09	SA#13	SP-010553	051	2	SIP protocol on the SIP+ (ISC) interface	5.1.0	5.2.0
2001-09	SA#13	SP-010553	052	2	CR on “Emergency sessions”	5.1.0	5.2.0
2001-09	SA#13	SP-010553	055	2	CR on “Network Initiated De-registration procedure”	5.1.0	5.2.0
2001-09	SA#13	SP-010553	058	1	Terminology Change from SIP+ to ISC for Service Control interface	5.1.0	5.2.0
2001-09	SA#13	SP-010553	061	3	Clarification of P-CSCF discovery	5.1.0	5.2.0
2001-09	SA#13	SP-010553	081		P-CSCF and PCF Clarifications	5.1.0	5.2.0
2001-09	SA#13	SP-010553	083		Service control during registration and de-registration	5.1.0	5.2.0
2001-12	SA#14	SP-010714	012	2	Requirement to indicate to UE what to do on alerting	5.2.0	5.3.0
2001-12	SA#14	SP-010714	044	2	Miscellanous BGCF impacts to 23.228	5.2.0	5.3.0
2001-12	SA#14	SP-010714	051	1	Generation of CDRs at BGCF	5.2.0	5.3.0
2001-12	SA#14	SP-010714	052		BGCF to MGCF interface	5.2.0	5.3.0
2001-12	SA#14	SP-010714	053	1	THIG usage in 23.228	5.2.0	5.3.0
2001-12	SA#14	SP-010714	053	2	Routing IMS voice calls to CS domain	5.2.0	5.3.0
2001-12	SA#14	SP-010714	060	2	Removal of T-SGW in 23.228	5.2.0	5.3.0
2001-12	SA#14	SP-010714	067	3	SLF query on UE invite	5.2.0	5.3.0
2001-12	SA#14	SP-010714	070		Registration and Re-registration flow, editorial correction	5.2.0	5.3.0
2001-12	SA#14	SP-010714	071		Clarification to Emergency sessions	5.2.0	5.3.0
2001-12	SA#14	SP-010714	075	1	Subscriber profile updating	5.2.0	5.3.0
2001-12	SA#14	SP-010714	082	2	Sh Interface for CAMEL	5.2.0	5.3.0
2001-12	SA#14	SP-010714	084		Revisiting ISC requirements	5.2.0	5.3.0
2001-12	SA#14	SP-010714	085	2	P-CSCF in same network as GGSN	5.2.0	5.3.0
2001-12	SA#14	SP-010714	119		Network Configuration Independence	5.2.0	5.3.0
2001-12	SA#14	SP-010714	086	1	Network Determination of Local Services in IM Subsystem	5.2.0	5.3.0
2001-12	SA#14	SP-010714	089	2	Local services for IMS	5.2.0	5.3.0
2001-12	SA#14	SP-010714	089	1	Local service for IMS	5.2.0	5.3.0
2001-12	SA#14	SP-010714	090	2	PDP context & IMS procedure clarification	5.2.0	5.3.0
2001-12	SA#14	SP-010714	091	1	Mobility related concept clean up	5.2.0	5.3.0
2001-12	SA#14	SP-010714	092	1	Relation of IMS user identities and the Service Profiles	5.2.0	5.3.0
2001-12	SA#14	SP-010714	096		P-CSCF network identifier	5.2.0	5.3.0
2001-12	SA#14	SP-010714	098	1	Service control managed MRFC session legs	5.2.0	5.3.0

2001-12	SA#14	SP-010714	100	2	Alignment of 23.060 and 23.228 for the handling of the PDP contexts in case of Iu release or RAB release	5.2.0	5.3.0
2001-12	SA#14	SP-010714	101		Event and information distribution within IMS	5.2.0	5.3.0
2001-12	SA#14	SP-010714	102		Session unrelated procedures	5.2.0	5.3.0
2001-12	SA#14	SP-010714	103		Correction for acronym “CDR”	5.2.0	5.3.0
2001-12	SA#14	SP-010714	104		Clarification of address resolution for IMS	5.2.0	5.3.0
2001-12	SA#14	SP-010714	105		Codec knowledge in IMS, draft CR to 23.228	5.2.0	5.3.0
2001-12	SA#14	SP-010714	106		Unknown subscriber handling in IMS	5.2.0	5.3.0
2001-12	SA#14	SP-010714	107	1	Correction of 23.228 with regard to security procedures defined in 33.210	5.2.0	5.3.0
2001-12	SA#14	SP-010714	108	2	UE informed of the reason for de-registration	5.2.0	5.3.0
2001-12	SA#14	SP-010714	117	1	Corrections to network initiated session release procedures	5.2.0	5.3.0
2001-12	SA#14	SP-010714	118	2	THIG for the BGCF	5.2.0	5.3.0
2001-12	SA#14	SP-010714	048	2	PDP Context Used for IM Subsystem Related Signalling	5.2.0	5.3.0
2001-12	SA#14	SP-010714	109	2	Clean up of the emergency service sections in 23.228	5.2.0	5.3.0
2002-03	SA#15	SP-020153	152		Correction of references to obsolete SIP RFC 2543 IETF specification	5.3.0	5.4.0
2002-03	SA#15	SP-020136	086		IMS Session Procedure Errors	5.3.0	5.4.0
2002-03	SA#15	SP-020136	115		Introduction of an IMS bearer reference point	5.3.0	5.4.0
2002-03	SA#15	SP-020136	120	2	Clarifications to text on handling of the PDP contexts in case of Iu release or RAB release	5.3.0	5.4.0
2002-03	SA#15	SP-020136	121	1	Corrections to codec negotiation	5.3.0	5.4.0
2002-03	SA#15	SP-020136	122	1	Interaction between QoS and session signalling	5.3.0	5.4.0
2002-03	SA#15	SP-020136	127	2	Requirement to register Public Id before usage	5.3.0	5.4.0
2002-03	SA#15	SP-020136	129	1	Corrections to List of Symbols	5.3.0	5.4.0
2002-03	SA#15	SP-020136	130	1	Authorization of QoS Resources	5.3.0	5.4.0
2002-03	SA#15	SP-020136	131	1	S-CSCF change	5.3.0	5.4.0
2002-03	SA#15	SP-020136	133		P-CSCF discovery	5.3.0	5.4.0
2002-03	SA#15	SP-020136	134	2	Number of media components per PDP Context	5.3.0	5.4.0
2002-03	SA#15	SP-020136	135	1	Registration Parameter Corrections	5.3.0	5.4.0
2002-03	SA#15	SP-020136	136	1	Removal of Editor's Notes	5.3.0	5.4.0
2002-03	SA#15	SP-020136	137	1	Clarification on Sh interface definition	5.3.0	5.4.0
2002-03	SA#15	SP-020136	138		Extend support of information transfer between SIP end points	5.3.0	5.4.0
2002-03	SA#15	SP-020136	139	1	Clean-up of MT Unregistered procedures	5.3.0	5.4.0
2002-03	SA#15	SP-020136	141	2	IP privacy requires re-registration	5.3.0	5.4.0
2002-03	SA#15	SP-020136	144		Corrections for Section 5.4.7 Interaction between QoS and session signalling	5.3.0	5.4.0
2002-03	SA#15	SP-020136	147		Corrections on P-CSCF initiated session release after loss of radio coverage	5.3.0	5.4.0
2002-03	SA#15	SP-020189	148	2	Use of R99 USIM for IMS	5.3.0	5.4.0
2002-03	SA#15	SP-020136	149	1	Provision of ‘VPLMN provided services’ in IMS	5.3.0	5.4.0
2002-03	SA#15	SP-020136	150		Corrections to P-CSCF’s functions	5.3.0	5.4.0
2002-03	SA#15	SP-020136	151		Removal of Sr Interface for R5	5.3.0	5.4.0
2002-03	SA#15	SP-020136	067	3	SLF query on UE invite	5.3.0	5.4.0
2002-04	SA#15	SP-020189	148	3	Resolution of a problem with CR 148: SP-020189.zip approved at SA#15 contains both 148Rev2 and 148Rev3. Rev3 was meant to be approved but Rev2 was implemented in v.5.4.0. V.5.4.1 is created to incorporate the delta between 148rev2 and 148rev3.	5.4.0	5.4.1
2002-06	SA#16	SP-020317	125	1	E.164 numbers as public user identifiers	5.4.1	5.5.0
2002-06	SA#16	SP-020317	161		Consistent and correct use of destination subscriber & fix a fault of changing destination to originating subscriber	5.4.1	5.5.0
2002-06	SA#16	SP-020317	167		Corrections to architecture of MRF	5.4.1	5.5.0
2002-06	SA#16	SP-020317	170		External Application Servers	5.4.1	5.5.0
2002-06	SA#16	SP-020317	157	1	Correct stage 2 text following IETF changes	5.4.1	5.5.0
2002-06	SA#16	SP-020317	155	1	Clarifying function of barring IMPU as a function	5.4.1	5.5.0
2002-06	SA#16	SP-020317	156	1	Clarification of the relation between Public User Identities and Service Profiles	5.4.1	5.5.0
2002-06	SA#16	SP-020317	160	1	IMS call redirected towards the PSTN/CS domain	5.4.1	5.5.0
2002-06	SA#16	SP-020317	173	1	Media negotiation	5.4.1	5.5.0
2002-06	SA#16	SP-020317	168	1	S-CSCF allocation	5.4.1	5.5.0
2002-06	SA#16	SP-020317	169	1	Registration flow	5.4.1	5.5.0
2002-06	SA#16	SP-020317	164	1	Clarification on the filter criteria for ASs	5.4.1	5.5.0
2002-06	SA#16	SP-020317	158	1	Forking In IMS	5.4.1	5.5.0
2002-06	SA#16	SP-020317	162	2	Clarification on the charging concept with stage 3	5.4.1	5.5.0
2002-06	SA#16	SP-020317	171	3	Restrictions of the Signalling PDP context	5.4.1	5.5.0

2002-06	SA#16	SP-020317	174	3	Number of media components per PDP Context	5.4.1	5.5.0
2002-06	SA#16	SP-020317	153	2	Deriving IMS parameters from the USIM	5.4.1	5.5.0
2002-06	SA#16	SP-020317	154	2	Clarification of the function “Implicit Registration”	5.4.1	5.5.0
2002-09	SA#17	SP-020534	175	1	The use of the Secondary PDP Context Activation Procedure for IMS	5.5.0	5.6.0
2002-09	SA#17	SP-020534	176	2	Modification of IMS Signalling PDP context	5.5.0	5.6.0
2002-09	SA#17	SP-020534	178	2	Clarification on terminology in 23.228: user and subscriber	5.5.0	5.6.0
2002-09	SA#17	SP-020534	179		Clarification on registration procedures	5.5.0	5.6.0
2002-09	SA#17	SP-020534	180	1	Procedures for providing or blocking identity	5.5.0	5.6.0
2002-09	SA#17	SP-020534	181	1	Corrections on session redirection procedures	5.5.0	5.6.0
2002-09	SA#17	SP-020534	182	1	Policy control procedures on PDP context modification	5.5.0	5.6.0
2002-09	SA#17	SP-020534	183	5	Location information in IMS	5.5.0	5.6.0
2002-09	SA#17	SP-020534	185	1	Re-registration procedures	5.5.0	5.6.0
2002-09	SA#17	SP-020534	187		Deletion of ISC interface support for control of timers	5.5.0	5.6.0
2002-09	SA#17	SP-020534	188	2	Support of Originated Requests from Application Servers	5.5.0	5.6.0
2002-09	SA#17	SP-020534	195	2	Updates to unify draft changes	5.5.0	5.6.0
2002-09	SA#17	SP-020534	197		Private ID cleanup	5.5.0	5.6.0
2002-09	SA#17	SP-020534	198	1	ISC cleanup	5.5.0	5.6.0
2002-09	SA#17	SP-020534	199	1	Emergency sessions	5.5.0	5.6.0
2002-09	SA#17	SP-020534	202	1	Clarification on Filter Criteria	5.5.0	5.6.0
2002-12	SA#18	SP-020776	203	1	Clarification on charging concepts	5.6.0	5.7.0
2002-12	SA#18	SP-020776	204	4	Clarification on MRFP reference point	5.6.0	5.7.0
2002-12	SA#18	SP-020776	207	1	Clarification on subclause 5.4.4	5.6.0	5.7.0
2002-12	SA#18	SP-020776	210	1	Removal of duplicate text	5.6.0	5.7.0
2002-12	SA#18	SP-020776	211	1	Movement of service architecture	5.6.0	5.7.0
2002-12	SA#18	SP-020776	213	1	Description of “Service Profile”	5.6.0	5.7.0
2002-12	SA#18	SP-020776	216	2	Correction to services concepts	5.6.0	5.7.0
2002-12	SA#18	SP-020776	221	1	Clarification on the ISC interface	5.6.0	5.7.0
2002-12	SA#18	SP-020776	223		PCF to PDF Changes	5.6.0	5.7.0
2002-12	SA#18	SP-020828	225	1	Service Invocation	5.6.0	5.7.0
2002-12	SA#18	SP-020776	226		Separation of media components in relation to forking	5.6.0	5.7.0
2002-12	SA#18	SP-020776	227	1	Number internationalisation clarification	5.6.0	5.7.0
2002-12	SA#18	SP-020776	228	1	S-CSCF re-assignment	5.6.0	5.7.0
2002-12	SA#18	SP-020776	229	1	Cleanup and alignment to stage 3 of 23.228	5.6.0	5.7.0
2002-12	SA#18	SP-020776	230		P-CSCF at home or visited	5.6.0	5.7.0
2002-12	SA#18	SP-020776	231	1	Clean up of 23.228 in general to make the spec accurate	5.6.0	5.7.0
2002-12	SA#18	SP-020776	232	1	Stripping of headers in the P-CSCF	5.6.0	5.7.0
2002-12	SA#18	SP-020776	233	1	Resource reservation	5.6.0	5.7.0
2002-12	SA#18	SP-020776	235	1	Clarification on Network Configuration Hiding	5.6.0	5.7.0
2002-12	SA#18	SP-020776	236	1	Clarification on grouping of media components to PDP Contexts	5.6.0	5.7.0
2002-12	SA#18	SP-020838	237	4	Handling of SDP manipulation issue in stage-2 specifications	5.6.0	5.7.0
2003-01	SA#18	SP-020776	217	5	Incorporating Messaging aspects to 23.228	5.7.0	6.0.0
2003-01	SA#18	SP-020776	241	1	Local services	5.7.0	6.0.0
2003-01	SA#18	SP-020776	242	1	Cleaning up of IMS emergency session requirement	5.7.0	6.0.0