ETSI TS 123 228 V16.4.0 (2020-10)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
IP Multimedia Subsystem (IMS);
Stage 2
(3GPP TS 23.228 version 16.4.0 Release 16)

Reference
RTS/TSGS-0223228vg40

Keywords
GSM,LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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. ITU-T Recommendation I.130 [4] describes a three-stage method for characterisation of telecommunication services, and ITU-T Recommendation Q.65 [3] defines stage 2 of the method.

This document does not cover the Access Network functionality except as they relate to provision of IM services, these aspects are covered in the normative Annexes.

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] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] Void.

[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] Void.

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

[11] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

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

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

[13] IETF RFC 3986: "Uniform Resource Identifiers (URI): Generic Syntax".

[14] IETF RFC 4282: "The Network Access Identifier".

[15] IETF RFC 3966: "The tel URI for Telephone Numbers".

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

[16a] IETF RFC 4941: "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] Void.

[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 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[26] 3GPP TS 32.260: "Telecommunication Management; Charging Management; IP Multimedia Subsystem (IMS) charging".

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

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

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

[29a] 3GPP TS 22.340: "IMS Messaging; Stage 1".

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

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

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

[33] IETF RFC 2766: "Network Address Translation-Protocol Translation (NAT-PT)".

[34] IETF RFC 2663: "IP Network Address Translator (NAT) Terminology and Considerations".

[35] Void.

[36] 3GPP TS 23.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service".

[37] Void.

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

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

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

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

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

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

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

[45] IETF RFC 5245: "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[46] IETF RFC 5766: "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)".

[47] IETF RFC 5389: "Session Traversal Utilities for NAT (STUN)".

[48] IETF RFC 5626: "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".

[49] IETF RFC 5627: "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".

[50] IETF RFC 5628: "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUUs)".

[51] IETF RFC 4787: "Network Address Translation (NAT) Behavioural Requirements for Unicast UDP".

[52] 3GPP TS 23.279: "Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services; Stage 2".

[53] 3GPP TS 22.173: "IMS Multimedia Telephony Service and supplementary services; Stage 1".

[54] 3GPP TS 23.203: "Policy and Charging Control architecture".

[55] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[56] 3GPP TS 23.204: "Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access".

[57] IETF RFC 4769: "IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information".

[58] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[59] 3GPP TS 29.333: "Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp Interface; Stage 3".

[60] 3GPP2 X.S0011: "cdma2000 Wireless IP Network Standard".

[61] 3GPP2 C.S0001-D: "Introduction to cdma2000 Spread Spectrum Systems - Revision D".

[62] 3GPP2 C.S0024-A: "cdma2000 High Rate Packet Data Air Interface Standard, April 2004".

[63] 3GPP2 C.S0084-000: "Overview for Ultra Mobile Broadband (UMB) Air Interface Specification".

[64] 3GPP TS 24.167: "3GPP IMS Management Object (MO); Stage 3".

[65] IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)".

[66] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services".

[67] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity".

[68] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[69] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[70] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[71] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[72] IETF RFC 3264: "An Offer/Answer Model with Session Description Protocol".

[73] 3GPP TS 23.333: "Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp interface: Procedures Descriptions".

[74] 3GPP TS 23.334: " IMS Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW) interface: Procedures Descriptions".

[75] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[76] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[77] 3GPP TS 22.153: "Multimedia priority service".

[78] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[79] 3GPP TS 29.328: "IP Multimedia (IM) Subsystem Sh Interface; Signalling flows and message contents".

[80] 3GPP TS 23.380: "IP Multimedia Subsystem (IMS); IMS Restoration Procedures".

[81] 3GPP TS 24.525: "Business trunking; Architecture and functional description".

[82] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses".

[83] 3GPP TS 33.328: "IP Multimedia (IM) Subsystem media plane security".

[84] IETF Draft, draft-ietf-rtcweb-overview-13 "Overview: Real Time Protocols for Brower-based Applications".

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

[85] W3C: "WebRTC 1.0: Real-time Communication Between Browsers", W3C Working Draft, 10 September 2013, http://www.w3.org/TR/2013/WD-webrtc-20130910/.

Editor's note: The above document cannot be formally referenced until it is published as a candidate recommendation.

[86] W3C: "Cross-Origin Resource Sharing", W3C Proposed Recommendation, 05 December 2013, http://www.w3.org/TR/2013/PR-cors-20131205/.

[87] ITU-T Recommendation T.140: "Protocol for multimedia application text conversation".

[88] IETF RFC 6455: "The WebSocket Protocol".

[89] IETF RFC 7118: "The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)".

[90] IETF RFC 4571: "Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport".

[91] 3GPP TS 24.610: "Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem".

[92] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2".

[93] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[94] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[95] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[96] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[97] 3GPP TS 23.632: "User data interworking, coexistence and migration; Stage 2".

[98] 3GPP TS 29.563: "5G System (5GS); Home Subscriber Server (HSS) services for interworking with Unified Data Management (UDM); Stage 3".

[99] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description".

[100] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[101] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description".

[102] 3GPP TS 38.321: "NR; Medium Access Control (MAC) protocol specification".

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 terms and definitions given in TR 21.905 [68] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [68].

For the purposes of the present document, the following terms and definitions given in TS 23.003 [24] apply:

Distinct Public Service Identity

Public User Identity

Wildcarded Public User Identity

Wildcarded Service User Identity

Alias Public User Identities: A set of Public User Identities that belong to the same alias group as specified in TS 29.228 [30].

ALG: Application Level Gateway (ALG) is an application specific functional entity that allows communication between disparate address realm or IP versions, e.g. an IPv6 node to communicate with an IPv4 node and vice versa, when certain applications carry network addresses in the payloads like SIP/SDP. NA(P)T-PT or NA(P)T is application unaware whereas ALGs are application specific translation entities that allow a host running an application to communicate transparently with another host running the same application but in a different IP version or IP address realm. See IETF RFC 2663 [34] for more details.

> For IMS, an IMS ALG provides the necessary application function for SIP/SDP protocols in order to communicate between different address realms or IP versions, e.g. IPv6 and IPv4 SIP applications.

Distinct Public User Identity: used in relation to wildcarded Public User/Service Identities to denote an explicitly provisioned Public User/Service Identity. See more details in TS 23.003 [24].

Entry point: In the case that border control concepts are to be applied in an IM CN subsystem, then these are to be provided by capabilities within the IBCF, and the IBCF acts as an entry point for this network (instead of the I-CSCF). In this case the IBCF and the I-CSCF can be co-located as a single physical node. If border control concepts are not applied, then the I-CSCF is considered as an entry point of a network. If the P-CSCF is in the home network, then the I-CSCF is considered as an entry point for this document.

Exit point: If operator preference requires the application of border control concepts then these are to be provided by capabilities within the IBCF, and requests sent towards another network are routed via a local network exit point (IBCF), which will then forward the request to the other network (discovering the entry point if necessary).

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**.** An example of an "IP-Connectivity Access Network" is GPRS.

Business trunking: as defined in TS 24.525 [81].

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 authorized to enjoy these services, and also to set the limits relative to the use that users make of these services.

Inter-IMS Network to Network Interface: The interface which is used to interconnect two IM CN subsystem networks. This interface is not constrained to a single protocol.

Network Address Translation (NA(P)T): method by which IP addresses are mapped from one group to another, transparently to end users. Network Address Port Translation, or NA(P)T is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. See RFC 3022 [65] for further details.

NAT-PT/NAPT-PT: NAT-PT uses a pool of globally unique IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across the IP version boundaries. NAT-PT binds addresses in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing between the two IP domains without requiring any changes to end points, like the UE. NAT-PT needs to track the sessions it supports and mandates that inbound and outbound data for a specific session traverse the same NAT-PT router.

> NAPT-PT provides additional translation of transport identifier (e.g., TCP and UDP port numbers, ICMP query identifiers). This allows the transport identifiers of a number of IPv6 hosts to be multiplexed into the transport identifiers of a single assigned IPv4 address. See IETF RFC 2766 [33] for more details.

Transport address: A unique identifier of transport-layer address, i.e. a combination of a network address, protocol identifier and port number. For example an IP address and a UDP port.

IMS application: An IMS application is an application that uses an IMS communication service(s) in order to provide a specific service to the end-user. An IMS application utilises the IMS communication service(s) as they are specified without extending the definition of the IMS communication service(s).

IMS application reference: An IMS application reference is the means by which an IMS communication service identifies an IMS application.

IMS communication service: An IMS communication service is a type of communication defined by a service definition that specifies the rules and procedures and allowed medias for a specific type of communication and that utilises the IMS enablers.

IMS communication service identifier: An IMS communication service identifier uniquely identifies the IMS communication service associated with the particular IMS request.

IMC: IMS Credentials as defined in TR 21.905 [68].

IMS enabler: An IMS enabler is a set of IMS procedures that fulfils specific function. An IMS enabler may be used in conjunction with other IMS enablers in order to provide an IMS communication service.

Instance identifier: An identifier, that uniquely identifies a specific UE amongst all other UEs registered with the same Public User Identity.

Local Service Number: A local service number is a telephone number in non international format. A local service number is used to access a service that may be located in the home network of the user (home local service number) or the roamed network of the user (geo-local service number).

Geo-local service number: A local service number that is used to access a service in the roamed network (a local service where the subscriber is located).

Geographical Identifier: A Geographical Identifier identifies a geographical area within a country or territory. See more details in clause E.8.

Home local service number: A local service number is used to access a service that is located in the home network of the user.

HSS Group ID: This refers to one or more SBI capable HSS instances managing a specific set of IMPIs/IMPUs.

IP Flow: Unidirectional flow of IP packets with the following properties:

- same source IP address and port number;
- same destination IP address and port number;
- same transport protocol (port numbers are only applicable if used by the transport protocol).

IP-SM-GW (IP short message gateway): An IP-SM-GW is an AS providing the support of Short Message Service of the IMS domain. See more details in TS 23.204 [56].

Media Flow: One or more IP flows carrying a single media instance, e.g., an audio stream or a video stream. In the context of this specification the term Media Flow is used instead of IP Flow regardless of whether the actual IP packet corresponds to media plane information (e.g. audio RTP flow) or control signalling (e.g. RTCP or SIP Signalling).

MPS: Based on TS 22.153 [77]. Multimedia Priority Service allows authorized users to obtain and maintain radio and network resources with priority, also during national security or emergency situations when PLMN congestion may occur.

MPS session: A session (e.g., voice, video, data session) for which priority treatment is applied for allocating and maintaining radio and network resources.

MPS-subscribed UE: A UE having a USIM with MPS subscription.

Outbound: Managing Client Initiated Connections in the Session Initiation Protocol (Outbound) defines behaviours for User Agents, registrars and proxy servers that allow requests to be delivered on existing connections established by the User Agent. See RFC 5626 [48] for further details.

Preferred Circuit Carrier Selection: An IMS service that allows the subscriber to select a long distance circuit carrier per call when dialling a call origination.

Preferred Circuit Carrier Access: An IMS service that allows a specific long distance circuit carrier to be selected for a long distance call.

Service User: According to TS 22.153 [77].

STUN: Simple Traversal of UDP Through NAT (STUN), provides a toolkit of functions. These functions allow entities behind a NAT to learn the address bindings allocated by the NAT, to keep those bindings open, and communicate with other STUN-aware devices to validate connectivity. See RFC 5389 [47] for further details.

STUN Relay: Is a usage of STUN, that allows a client to request an address on the STUN server itself, so that the STUN server acts as a relay. See IETF RFC 5766 [46] for further details.

STUN Keep-alive: Is a usage of STUN, to keep NAT bindings open.

3.2 Symbols

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

Cr	Reference Point between an AS and an MRFC for media control.
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 or between an IP-PBX and a P-CSCF.
ISC	Reference Point between a CSCF and an Application Server and between a CSCF and an MRB.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
Ix	Reference Point between IBCF and TrGW.
Ici	Reference Point between an IBCF and another IBCF belonging to a different IM CN subsystem network or between an IBCF and an IP-PBX.
Izi	Reference Point between a TrGW and another TrGW belonging to a different IM CN subsystem network.
Le	Reference Point between an AS and a GMLC.
Ma	Reference Point between an AS and an I-CSCF.
Mb	Reference Point used for IMS media transport to IP network services.
Mf	Reference Point between a transit function and AS.
Mg	Reference Point between an MGCF and a CSCF.

Mi Reference Point between a CSCF and a BGCF.
Mj Reference Point between a BGCF and an MGCF.
Mk Reference Point between a BGCF/IMS ALG and another BGCF.
Mm Reference Point between a IBCF/CSCF/BGCF/IMS ALG and an IP multimedia network.
Mr Reference Point between an CSCF and an MRFC.
Mr′ Reference Point between an AS and an MRFC for session control.
Mp Reference Point between MRFP and MRFC.
Ms Reference point between an IBCF and Application Server
Mw Reference Point between a CSCF and another CSCF.
Mx Reference Point between a CSCF/BGCF and IBCF.
Rc Reference Point between an AS and an MRB.
Sh Reference Point between an AS (SIP-AS or OSA-CSCF) and an HSS.
Si Reference Point between an IM-SSF and an HSS.
Ut Reference Point between UE and an Application Server.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [68] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [68].

5GS 5G System
API Application Program Interface
APN Access Point Name
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 Data Record
CN Core Network
CS Circuit Switched
CSCF Call Session Control Function
CSE CAMEL Service Environment
DHCP Dynamic Host Configuration Protocol
DNN Data Network Name
DNS Domain Name System
ECN Explicit Congestion Notification
ENUM E.164 Number Mapping
GGSN Gateway GPRS Support Node
GLMS Group and List Management Server
GMLC Gateway Mobile Location Centre
GRUU Globally Routable User Agent URI
GUP Generic User Profile
HSS Home Subscriber Server
IBCF Interconnection Border Control Function
I-CSCF Interrogating-CSCF
IETF Internet Engineering Task Force
IM IP Multimedia
IMC IMS Credentials
IMS IP Multimedia Core Network Subsystem
IMS ALG IMS Application Level Gateway
IMSI International Mobile Subscriber Identifier
IN Intelligent Network
IP Internet Protocol
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
IP-CAN IP-Connectivity Access Network
IP-SM-GW IP Short Message Gateway

ISDN	Integrated Services Digital Network
ISIM	IMS SIM
ISP	Internet Service Provider
ISUP	ISDN User Part
IWF	Interworking Function
NP	Number portability
MAP	Mobile Application Part
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MRB	Media Resource Broker
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
NAI	Network Access Identifier
NAPT	Network Address Port Translation
NAT	Network Address Translation
NA(P)T-PT	Network Address (Port-Multiplexing) Translation-Protocol Translation
II-NNI	Inter-IMS Network to Network Interface
OSA	Open Services Architecture
P-CSCF	Proxy-CSCF
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDP	Packet Data Protocol e.g., IP
P-GRUU	Public Globally Routable User Agent URI
PLMN	Public Land Mobile Network
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAB	Radio Access Bearer
RFC	Request for Comments
SCS	Service Capability Server
S-CSCF	Serving-CSCF
SDP	Session Description Protocol
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
S-GW	Signalling Gateway
TAS	Telephony Application Server
T-GRUU	Temporary Globally Routable User Agent URI
THIG	Topology Hiding Inter-network Gateway
TrGW	Transition Gateway
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URL	Universal Resource Locator
USIM	UMTS SIM

4 IP multimedia subsystem concepts

4.0 General

The IP Multimedia CN subsystem comprises all CN elements for provision of multimedia services. This includes the collection of signalling and media 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 transport capabilities, utilises the IP-Connectivity Access Network (this may include an equivalent set of services to the relevant subset of CS Services).

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

The IP multimedia core network (IM CN) subsystem enables operators to offer their subscribers multimedia services. The IM CN subsystem should enable the convergence of, and access to, voice, video, messaging, data and web-based technologies for the wireless and wireline user.

The complete solution for the support of IP multimedia applications consists of terminals, IP-Connectivity Access Networks (IP-CAN), and the specific functional elements of the IM CN subsystem described in this technical specification. Examples of IP-Connectivity Access Network are:

- the GPRS core network with GERAN and/or UTRAN radio access networks; and
- EPC core network and E-UTRAN radio access network; and
- 5GS access network.

Figure 4.0 below represents the IMS reference architecture including interfaces towards CS network and other IP based multimedia Networks. Details of the roles of these nodes are described in clauses 4.6, 4.7 and 4.7a.

NOTE 1: Some entities defined as part of the IMS Subsystem can also be used by other subsystems.

NOTE 2: The Ici and Izi reference points are only applicable for IP Multimedia Networks that are IMS subsystems.

NOTE 3: In certain configuration, two entities can exchange SIP messages directly with each other without a reference point being defined between them (e.g., intermediate entitie(s) not record-routed).

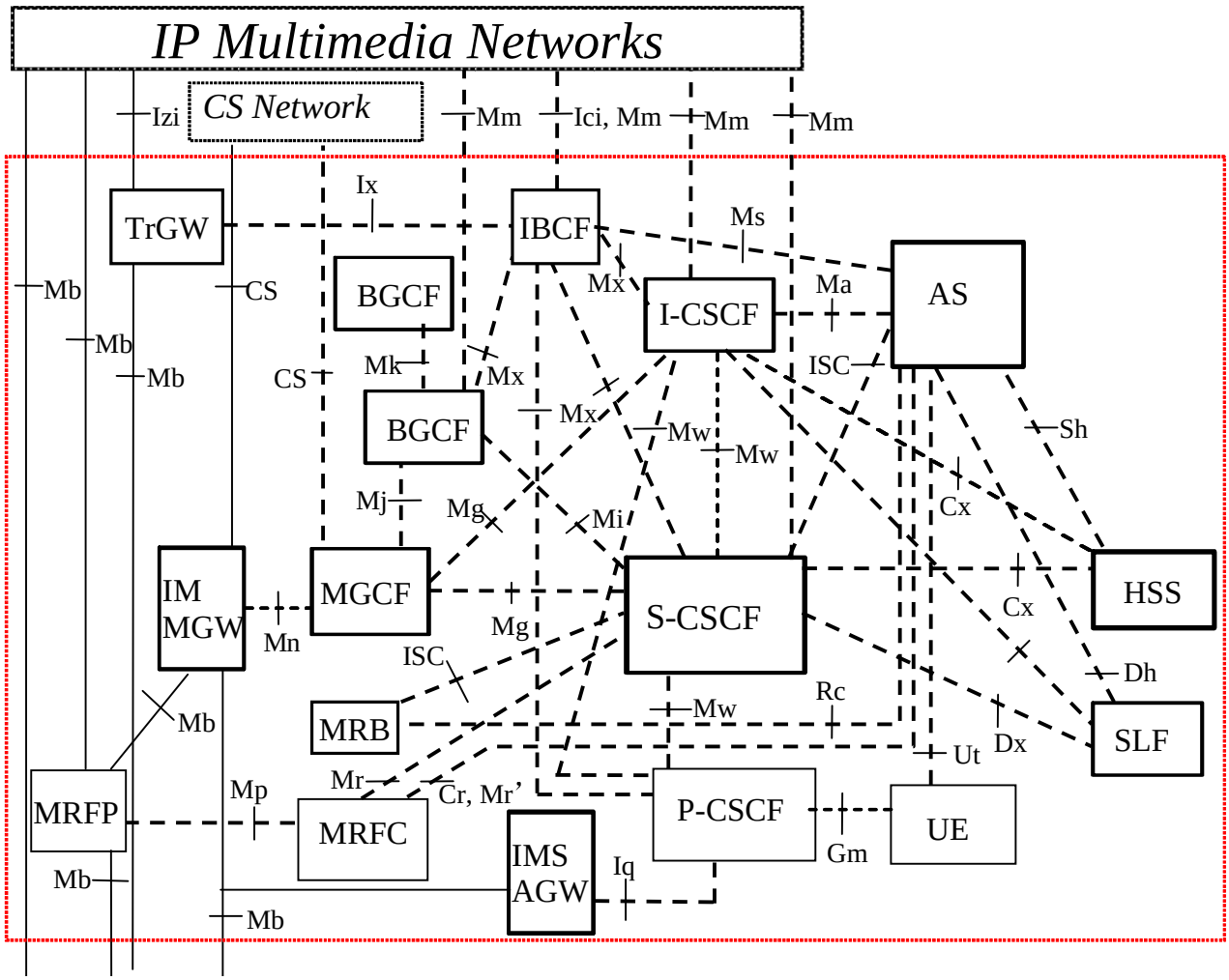


Figure 4.0: Reference Architecture of the IP Multimedia Core Network Subsystem

A description of the functional entities can be found in TS 23.002 [1].

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

The IP multimedia subsystem utilizes the IP-CAN to transport multimedia signalling and bearer traffic. IP-CANs that maintain the service while the terminal moves, hide 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 or IN

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

For more information refer to clause 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 clause 4.2.4.

4.2.1.3 Dynamic services interactions handling

4.2.1.3.1 Service information exchanged between Application Servers

To avoid conflicting interactions between services they execute, different ASs involved in the same IMS session (within an operator network or across networks) shall be able to exchange the following service interaction information:

- indication of services that have been performed, and
- optionally, additional indication of services that should be further avoided.

4.2.1.3.2 Handling by the Application Server

If an AS provides one or more services, the AS may include service interaction information in SIP signalling, identifying the service that it has executed.

If an AS provides one or more services which are known to be negatively impacted by the subsequent execution of a service by another AS, the AS may include, in addition to the an indication of the services executed, service interaction information in SIP signalling, indicating the services that should be avoided.

An AS receiving a SIP message containing an indication

- that a service has been executed previously, and/or
- that a service should be avoided,

may, depending on local policy, take this information into account. The service interaction information shall be such that an AS receiving this information should not be able to misinterpret the information and shall ignore such information that it does not recognize.

Service interaction information for standardized services shall be standardized but there shall also be the ability to exchange globally unique service information for non-standardized services.

4.2.1.3.3 Deletion of services interaction information

The service interaction information shall be removed when it is sent to the UE via P-CSCF or to an entity outside the trust domain or when it is not in compliance with service level agreements with other domains.

4.2.2 Support of numbers in non-international format in the IMS

Phone or telephone numbers which are not in the international format can allow the access of the visited services (local service numbers) and the access of numbers in a local addressing plan. Since numbers in non-international format are widely used in legacy fixed and mobile CS networks the seamless co-operation with these networks require the support of numbers in non-international format (including local service numbers) in the IMS. It is up to the operator's policy when and which type of numbers in non-international format can be used. In the rest of this clause the term 'visited access network' is used to indicate the network in which the user is physically located. In the case of GPRS access this is the VPLMN. In the case of other access types this is most probably the IP-CAN provider.

The use of numbers in non-international format including local service numbers shall be provided in the following manner:

1. It shall be possible for the HPLMN to determine whether a user is using a number in non-international format according to an addressing plan used in the visited network or a geo-local service number. 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 a local addressing plan. This indication shall be included in the Request URI of the SIP request. If a user intends to use a number according to an addressing plan used at his/her current physical location or a local service number at his/her current physical location, then there shall be information about the visited access network independently from the location of the P-CSCF included in the Request-URI of the SIP request.

2. The P-CSCF shall route the session towards the S-CSCF as per the session origination procedures.

   Processing the Request URI (e.g. address analysis and potential modification such as translation into globally routable format, e.g. a globally routable PSI) shall be performed by an Application Server in the subscriber's Home Network. The S-CSCF routes the SIP request towards this Home Network Application Server based upon filter criteria which are triggered by the information in the 'local indication' received from the UE. The AS may need to identify the visited access network, e.g. from information in SIP signalling or via the Sh interface.

   When clause 4.15a (Roaming Architecture for Voice over IMS with Local Breakout) is in use, and the Home Network decides to loop-back the call to the visited network, and when the indication is received that the number is in accordance with the visited network numbering plan the Home network can choose to not translate numbers in non-international format, and pass on the non-international number as received, to the VPLMN.

   When clause 4.15b (Roaming Architecture for Voice over IMS with home routed traffic) is in use, a translation to an international routable number may be needed, but this is beyond the scope of this specification e.g. an implementation specific NNI to the VPLMN (or other 3rd party in the visited country) is needed.

3. Then the AS passes the session request back to the S-CSCF with Request URI that contains either a globally routable SIP URI or a Tel URI with number in international format, or a Tel URI with number in non-international format if clause 4.15a (Roaming Architecture for Voice over IMS with Local Breakout) is in use and the Home network does not translate the number in non-international format. The SIP request shall contain enough information to route to the network hosting the service or using the addressing plan and allow the terminating network to identify the intended end point (e.g. service).

4. The S-CSCF routes the SIP request, via normal IMS routing principles, towards its destination (e.g. a server in the visited access network identified by a PSI) using the Mw or Mm interfaces.

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.

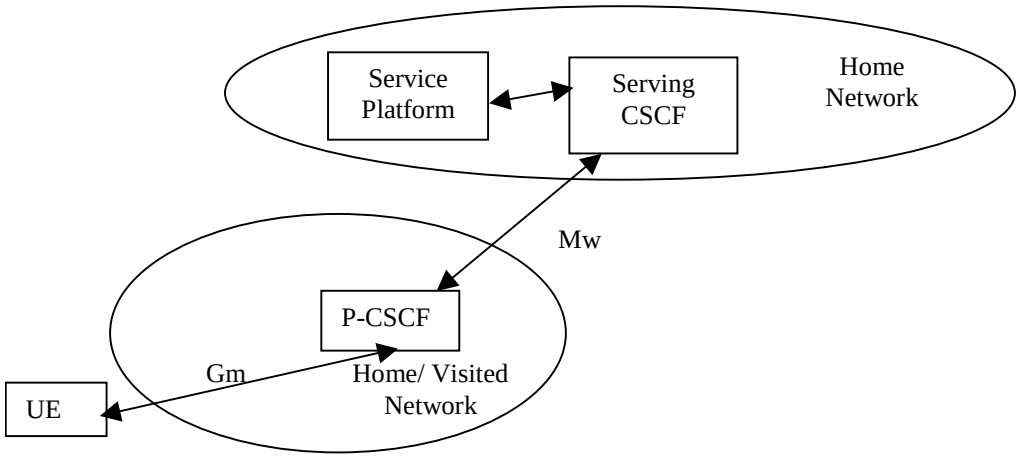


Figure 4.1: Service Platform in Home Network

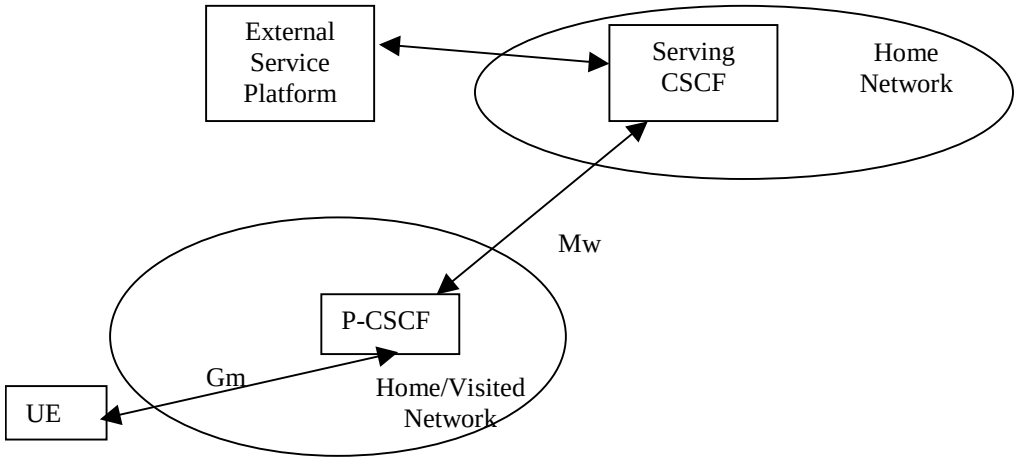


Figure 4.2: External Service Platform

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 clause 4.2.4.

The roles that the CSCF plays are described below.

- The Proxy-CSCF shall enable the session control to be passed to the Serving-CSCF.
- The Serving-CSCF is located in the home network. The Serving-CSCF shall invoke service logic.

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

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

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

Network initiated Proxy-CSCF reassignment is not a requirement.

The use of additional elements to be included in the SIP signalling path is optional. Such additional elements may provide functions as described in clause 4.14 and Annex I.

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 be able to supply the AS with information to allow it to execute multiple services in order within a single SIP transaction.

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

The S-CSCF shall decide whether an Application Server is required to receive information related to an incoming initial SIP request to ensure appropriate service handling. The decision at the S-CSCF is based on (filter) information received from the HSS. This filter information is stored and conveyed on a per Application Server basis for each user. It shall be possible to include a service indication in the filter information, which is used to identify services and the order that they are executed on an Application Server within a single SIP transaction. The name(s)/address(es) information of the Application Server (s) are received from the HSS.

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

The S-CSCF does not handle service interaction issues.

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

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

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

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

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

It shall be possible for an Application Server to generate SIP requests and dialogs on behalf of users. Requests originating sessions on behalf of a user are forwarded to the S-CSCF serving the user, if the AS has knowledge of the S-CSCF assigned to that user and the S-CSCF shall perform regular originating procedures for these requests.

Originating requests on behalf of registered and unregistered users 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 TS 32.240 [25] and TS 32.260 [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 IETF RFC 3261 [12], other relevant IETF RFC's, and additional enhancements introduced to support 3GPP´s needs on the Mw, Mm, Mg interfaces).

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 IETF 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 4.3a – 4.3e below.

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

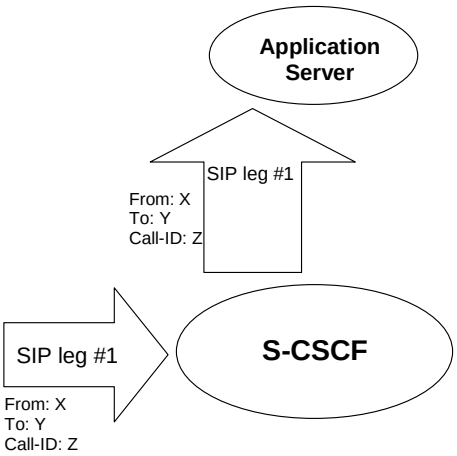


Figure 4.3a: Application Server acting as terminating UA, or redirect server

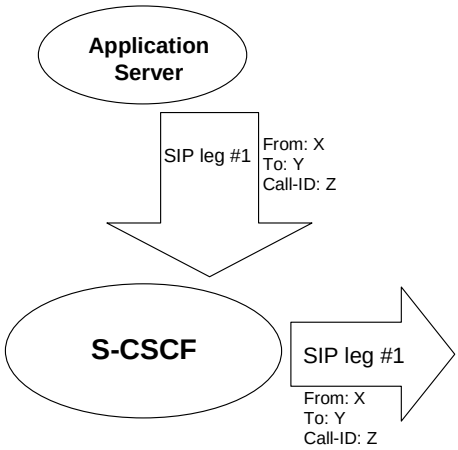


Figure 4.3b: Application Server acting as originating UA

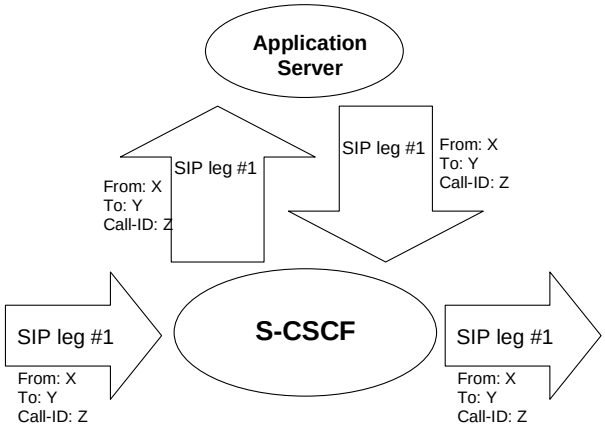


Figure 4.3c: Application Server acting as a SIP proxy

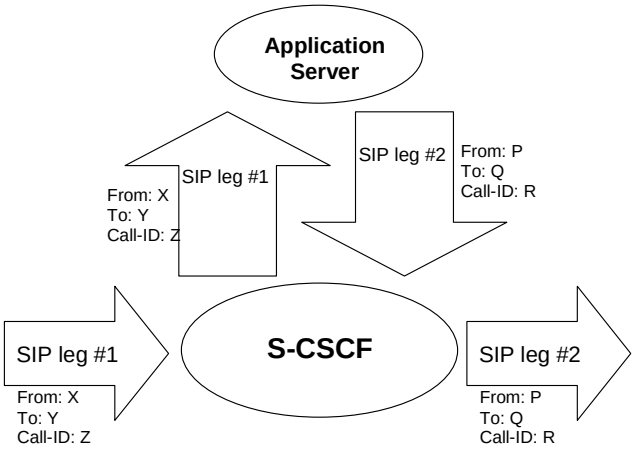


Figure 4.3d: Application Server performing 3rd party call control

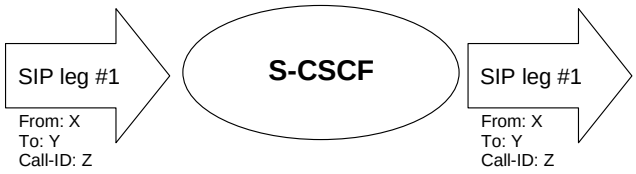


Figure 4.3e: A SIP leg is passed through the S-CSCF without Application Server involvement

4.2.4a HSS to service platform Interface

The Application Server (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, etc.
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, UE Time Zone and user location information (e.g. cell global ID/Service Area ID or the address of the serving network element, VPLMN ID, etc.)). The Sh interface supports retrieving the Private User Identities using the same Public User Identity. In the case of a Public User Identity being shared across multiple Private User Identities within the same IMS subscription, the Sh interface supports the transfer of the Private User Identities that share the Public User Identity.

NOTE 1: 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 TS 22.071 [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 [28]) instead of using the Sh interface.

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

6. The Sh interface also supports mechanisms that allow Application Servers to activate/deactivate their own existing initial filter criteria stored in the HSS on a per subscriber basis.

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.

NOTE 2: CAMEL subscription data can also be transferred from the HSS to the IM-SSF via the Sh interface.

4.2.4b S-CSCF Service Control Model

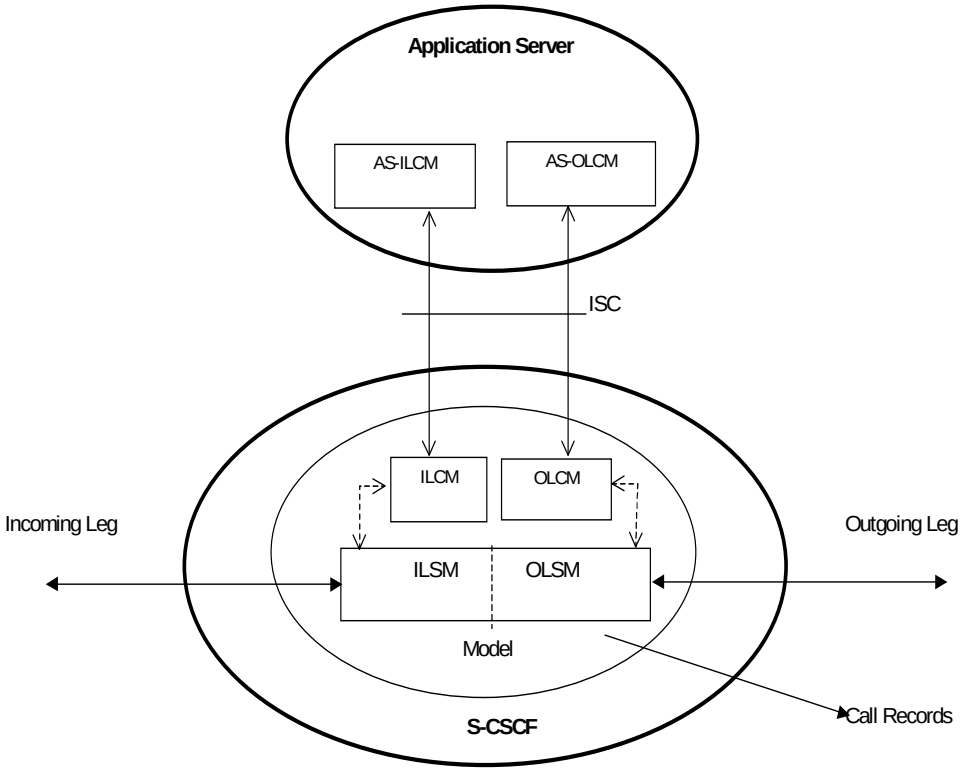


Figure 4.3f: Service Control Model with Incoming Leg Control and Outgoing Leg Control

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

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

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

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

The definitions used in the model are:

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

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

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

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

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

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

4.2.4c I-CSCF to AS reference point (Ma)

The Ma reference point is between the Interrogating CSCF and the service platform(s).

The Interrogating-CSCF to AS reference point is used to:

- forward SIP requests destined to a Public Service Identity hosted by an Application Server directly to the Application Server;
- originate a session on behalf of a user or Public Service Identity, if the AS has no knowledge of a S CSCF assigned to that user or Public Service Identity.

It shall be possible for an Application Server to originate a session on behalf of users or Public Service Identities. If the AS has no knowledge of the serving S-CSCF for that user or Public Service Identity, such requests are forwarded to an I-CSCF, and the I CSCF shall perform regular originating procedures for these requests.

Session origination requests on behalf of registered and unregistered users shall be supported.

The Ma reference point shall be able to convey charging information according to TS 32.240 [25] and TS 32.260 [26].

The protocol to be used on the Ma reference point shall be SIP (as defined by RFC 3261 [12], other relevant IETF RFCs, and additional enhancements introduced to support 3GPP´s needs on the Mw, Mm, Mg reference points).

Concerning the relationship between the SIP legs of the Ma reference point and the SIP legs of the Mw, Mm, and Mg reference points the I-CSCF acts as a SIP proxy, as shown in Figures 4.3f and 4.3g below.

Figures 4.3f and 4.3g below depict the possible high-level interactions envisioned between the I-CSCF and the Application Server.

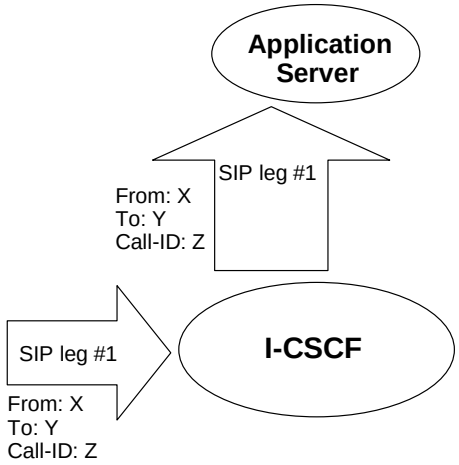


Figure 4.3f: I-CSCF forwarding a SIP request destined to a Public Service Identity to an Application Server hosting this Public Service Identity

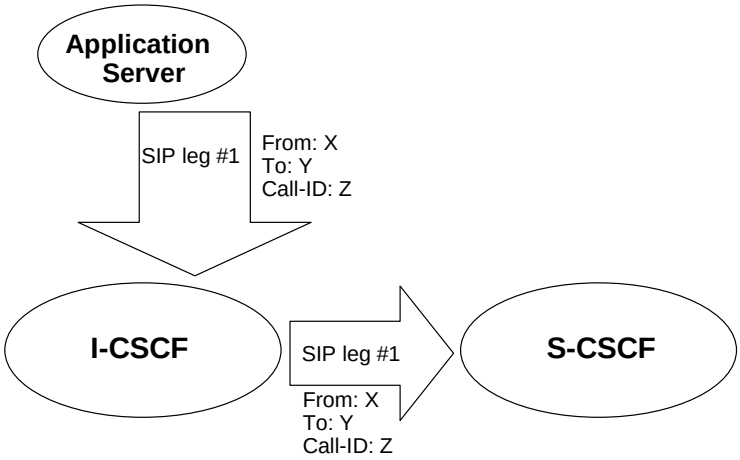


Figure 4.3g: Application Server originating a session on behalf of a user or a Public Service Identity, having no knowledge of the S-CSCF to use

4.2.5 The QoS requirements for an IM CN subsystem session

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

1. Independence between QoS signalling and Session Control

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

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

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

3. Void.

4. Restricted Resource Access at the IP BS Level

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

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

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

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

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

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

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

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

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

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

7. The Efficiency of QoS Signalling and Resource Allocation

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

8. Dynamic QoS Negotiation and Resource Allocation

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

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

9. Prevention of Theft of Service

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

10. Prevention of Denial of Service

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

4.2.6 QoS Requirements for IM CN subsystem signalling

Depending on the bearer establishment mode, the UE or the IP-CAN shall be able to establish a dedicated signalling IP-CAN bearer for IM Subsystem related signalling or utilize a general-purpose IP-CAN bearer for IM subsystem signalling traffic.

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

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

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

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

- the P-CSCF assigned for this UE, or to any one of the set of possible P-CSCFs that may be assigned to this UE.
- and towards DHCP and DNS servers within the IMS operator's domain where the P-CSCF is located.

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

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

4.2.7 Support of SIP forking

4.2.7.1 SIP Forking

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

4.2.7.2 Forking within and outside the IM CN Subsystem

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

- The S-CSCF shall support the ability for a Public User Identity to be registered from multiple contact addresses, as defined in IETF RFC 3261 [12]. The S-CSCF shall support forking so that an incoming SIP request addressed to a Public User Identity is proxied to multiple registered contact addresses. This allows forking across multiple contact addresses of the same Public User Identity.
- When multiple contact addresses have been registered, then the S-CSCF shall exhibit the following behaviour with regards to forking the incoming SIP request:

    1. If the UE has indicated capability information upon IMS registration in terms of SIP User Agent capabilities and characteristics described in IETF RFC 3840 [38], then the S-CSCF shall use it to generate a target contact set using the matching mechanism described in IETF RFC 3841 [42]. If the UE has not indicated any capabilities for the contact addresses upon registration, then the S-CSCF may still use the preference information, if indicated for the contact addresses upon registration, as described in the following bullet point below.

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

- Application Servers in the IMS shall not act as a forking proxy towards the S-CSCF in the sense of IETF RFC 3261 [12].

NOTE 1: The AS may subscribe to the registration event package to retrieve the contact address(es) of the UE. Based on this information the AS may act as a forking proxy in the sense of IETF RFC 3261 [12] towards other nodes than the S-CSCF.

NOTE 2: The AS may initiate multiple requests towards the registered Public User Identities of a user, however, this is not considered as forking in the sense of IETF RFC 3261 [12].

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

4.2.7.3 Support for forked requests

UE and MGCF shall be ready to receive responses generated due to a forked request and behave according to the procedures specified in IETF RFC 3261 [12] and in this clause.

The UE and MGCF may accept or reject early dialogues from different terminations as described in IETF RFC 3261 [12], for example if the UE is only capable of supporting a limited number of simultaneous dialogs.

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

NOTE: Upon the reception of a first final 200 OK (for INVITE), the UE or MGCF may terminate the early dialogue, as specified in IETF RFC 3261 [12].

The UE and MGCF may include preferences according to IETF RFC 3841 [42], in INVITE's, indicating that proxies should not fork the INVITE request. The S-CSCF and AS should follow the preferences, if included in the INVITE request. On the terminating side, UE and MGCF shall be able to receive, as specified in IETF RFC 3261 [12], several requests for the same dialog that were forked by a previous SIP entity.

Application Servers and MRFCs shall be capable to handle forked requests according to the procedures specified in IETF RFC 3261 [12].

4.3 Naming and addressing concepts

4.3.1 Address management

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

When a UE is assigned an IPv6 prefix, it can change the global IPv6 address it is currently using via the mechanism defined in IETF RFC 4941 [16a], or similar means. When a UE is registered in the IM CN Subsystem with an IP address, any change to this IP address that is used to access the IM CN subsystem will result in dropping the active SIP dialogs, and shall trigger automatic registration. This automatic registration updates the UE's IP address and security association. To avoid disruption of ongoing IM CN subsystem services, the UE should not change the IP address that it uses to access the IM CN subsystem while engaged in active SIP dialogs (e.g. INVITE or SUBSCRIBE-NOTIFY dialogs).

4.3.2 Void

Figure 4.4: Void

4.3.3 Identification of users

4.3.3.0 General

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

4.3.3.1 Private User Identities

Every IM CN subsystem user shall have one or more Private User Identities. The private identity is assigned by the home network operator, and used, for example, for Registration, Authorization, Administration, and Accounting purposes. This identity shall take the form of a Network Access Identifier (NAI) as defined in IETF RFC 4282 [14]. It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

- The Private User Identity is not used for routing of SIP messages.
- The Private User Identity shall be contained in all Registration requests, (including Re-registration and De-registration requests) passed from the UE to the home network.
- An ISIM application shall securely store one Private User Identity. For UEs supporting only non-3GPP accesses, if neither ISIM nor USIM is present, but IMC is present, the Private User Identity shall be stored in IMC. It shall not be possible for the UE to modify the Private User Identity information stored on the ISIM application or IMC.
- The Private User Identity is a unique global identity defined by the Home Network Operator, which may be used within the home network to identify the user's subscription (e.g. IM service capability) from a network perspective. The Private User Identity identifies the subscription, not the user.
- The Private User Identity shall be permanently allocated to a user's subscription (it is not a dynamic identity), and is valid for the duration of the user's subscription with the home network.
- The Private User Identity is used to identify the user's information (for example authentication information) stored within the HSS (for use for example during Registration).
- The Private User Identity may be present in charging records based on operator policies.
- The Private User Identity is authenticated only during registration of the user, (including re-registration and de-registration).
- The HSS needs to store the Private User Identity.
- The S-CSCF needs to obtain and store the Private User Identity upon registration and unregistered termination.
- If mobile terminated short message service without MSISDN as defined in TS 23.204 [56] is required then the Private User Identity shall be based on the IMSI according to TS 23.003 [24], clause 13.3.

4.3.3.2 Public User Identities

Every IM CN subsystem user shall have one or more Public User Identities (see TS 22.228 [8]), including at least one taking the form of a SIP URI (see IETF RFC 3261 [12]). The Public User Identity is 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 shall take the form as defined in TS 23.003 [24].
- An ISIM application shall securely store at least one Public User Identity. For UEs supporting only non-3GPP accesses, if neither ISIM nor USIM is present, but IMC is present, the Public User Identity shall be stored in IMC. 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 or IMC.
- A Public User Identity shall be registered either explicitly or implicitly before originating IMS sessions and originating IMS session unrelated procedures can be established by a UE using the Public User Identity. Subscriber-specific services for unregistered users may nevertheless be executed as described in clause 5.6.5. Each implicit registration set shall contain at least one Public User Identity taking the form of a SIP URI.

NOTE: An implicit registration set can contain Public User Identities of more than one service profile. When sending a third party registration request (for details see clause 5.4.1.7 in TS 24.229 [10a]) to an AS based on an initial filter criteria in a service profile, the third party registration request will include a Public User Identity taking the form of a SIP URI from that service profile within the implicit registration set.

- It shall be possible to identify Alias Public User Identities. For such a group of Public User Identities, operations that enable changes to the service profile and the service data configured shall apply to all the Public User Identities within the group. This grouping information shall be stored in the HSS. It shall be possible to make this grouping information available to the AS via the Sh interface, and Sh operations are applicable to all of the Public User Identities within the same Alias Public User Identity group. It shall be possible to make this information available to the S-CSCF via the Cx interface. It shall be possible to make this information available to the UE via the Gm interface.

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

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

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

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

4.3.3.2a Globally Routable User Agent URI (GRUU)

A Globally Routable User Agent URI (GRUU) is an identity that identifies a unique combination of Public User Identity and UE instance that allows a UE to address a SIP request to a specific Public User Identity UE combination instance, as opposed to a Public User Identity, in order to ensure that the SIP request is not forked to another registered UE of the same Public User Identity. There are two types of GRUUs; Public GRUUs (P-GRUUs) and Temporary GRUUs (T-GRUUs). P-GRUUs are GRUUs that reveal the Public User Identity of the user and are very long lived. T-GRUUs are GRUUs that contain a URI that do not reveal the Public User Identity of the user and are valid until the contact is explicitly de-registered or the current registration expires. The IM CN subsystem shall support the capability for IMS UEs to obtain both T-GRUUs and P-GRUUs when performing IMS registration, exchange GRUUs using SIP requests and responses and use GRUUs to address SIP requests to specific UEs according to RFC 5627 [49].

4.3.3.2a.1 Architecture Requirements

The following architectural requirements shall apply to support of GRUU in the IMS:

0. If a UE could become engaged in a service (e.g. telephony supplementary service) that potentially requires the ability to identify and interact with a specific UE even when multiple UEs share the same single Public User Identity then the UE should support GRUU.

1. A GRUU shall be registered in the IMS network with a unique combination of specific Public User Identity and UE.

2. If a UE supports GRUU, it shall indicate support for a GRUU that is associated with a specific Public User Identity at the time of registration of the Public User Identity. The UE shall use the same instance ID for all registration requests regardless of the access network used for registration. A function that registers on behalf of a UE shall use the same Instance ID as if that UE had performed the registration itself.

NOTE 1: If the UICC is replaced the UE is still considered to be same UE instance and so the UE instance ID is not changed by using a different UICC.

3. The IMS network shall be able to receive an indication of support for GRUU for a specific Public User Identity at a specific UE instance and be able to generate both P-GRUU's and T-GRUU's and return them back to the UE that indicated support for GRUU.

NOTE 2: The UE may have a registration request that indicates GRUU support, but the GRUU will not be returned if IMS network does not support generation of GRUUs.

4. When the IMS network receives indication of GRUU support for a specific Public User Identity from the UE during a registration request, the IMS network shall also generate P-GRUU's and T-GRUU's for all implicitly registered Public User Identities belonging to the same implicit registration set. The IMS network shall communicate all these other GRUUs to the UE.

5. Registrations of all GRUUs associated with a specific Public User Identity shall also be directed to the same S-CSCF.

6. The IMS network will be able to generate GRUU's for any UE registered with a valid SIP URI.

7. The IMS network shall generate the same P-GRUU for a given Public User Identity and Instance Identifier combination.

8. The IMS network shall generate a different T-GRUU for a given Public User Identity and Instance Identifier combination for each registration and re-registration.

9. The IMS network shall be able to derive the Public User Identity directly from the P-GRUU. The Public User Identity derived from the P-GRUU used to identify the contact address of the sender shall be same as the Public User Identity used to identify the initiator or an associated Public User Identity. If the URI in the SIP Contact header of the sender carries a parameter indicating that it is a GRUU but does not comply with the stated requirement or if there is no registration corresponding to the GRUU, then the IMS network should reject the request.

10. The IMS network shall be able to route requests destined to a GRUU to the UE instance registered with that GRUU.

11. The IMS network shall not fork SIP requests addressed to a GRUU to separate UEs.

12. A UE that is capable of supporting GRUUs shall be able to differentiate between a GRUU and a Public User Identity.

13. The IMS network shall support establishment of session or non-session related communication using a GRUU.

14. A UE supporting GRUUs shall be able to inter-work with an IMS network not supporting GRUUs.

15. A UE supporting GRUUs shall be able to inter-work with a UE not supporting GRUUs per RFC 5627 [49].

16. A UE or network that supports GRUUs shall not negatively affect networks or UEs that do not support GRUUs.

17. It shall be possible to define iFCs that match the Public User Identity part of a GRUU.

18. It shall be possible for iFCs to determine whether the Request URI of a message contains a GRUU, and then trigger to Application Servers that are only applicable for GRUUs.

19. It shall be possible to provide terminating services to a GRUU associated with a currently unregistered subscriber.

NOTE 3: The network may not be able to validate the unregistered GRUU of a currently unregistered or registered subscriber, such that operator policy might restrict the services available to the GRUU under these conditions.

20. It shall be possible to apply same level of privacy irrespective whether GRUU is used or not.

4.3.3.2b Wildcarded Public User Identity

It shall be possible to support a wildcarded Public User Identity. A wildcarded Public User Identity expresses a set of Public User Identities grouped together. It shall be possible to include and express the wildcarded Public User Identity in the implicit registration set according to clause 5.2.1a.

Only distinct Public User Identities shall be used for explicit registration. The implicit registration of a wildcarded Public User Identity shall be handled in the same manner as the implicit registration of a distinct Public User Identity from a network perspective, with only one service profile associated to the wildcarded Public User Identity.

It shall be possible for a user to have a distinct Public User Identity even if it matches a wildcarded Public User Identity. Such a distinct Public User Identity may have a different service profile than the wildcarded Public User Identity.

Editor's Note: It is to TBD if a distinct Public User Identity shall be included in the same implicit registration or not. If stage 3 protocol solution found for this issue, then they can be in separate implicit registration set.

The matching of a distinct Public User Identity shall take precedence over matching of wildcarded Public User Identity. When the value of a Public User Identity matches what is expressed as an implicitly registered wildcarded Public User Identity and there is no better match, then the procedures are the same as in the case that the identifier matches an implicitly registered distinct Public User Identity.

4.3.3.3 Routing of SIP signalling within the IP multimedia subsystem

Routing of SIP signalling within the IMS shall use SIP URIs or other (non SIP) AbsoluteURIs. AbsoluteURIs are defined in IETF RFC 3986 [13]. Routing of SIP signalling within the IMS using AbsoluteURI (non SIP) shall only be

supported for IMS signalling from IMS user to external networks. E.164 [2] format Public User Identities shall not be used for routing within the IMS, and session requests based upon E.164 format Public User Identities will require conversion into SIP URI format for internal IMS usage.

4.3.3.3a Handling of dialled number formats

When using a phone number as the dialled address, the UE can provide this number in the form of a SIP URI or a TEL URI. This phone number can be in the form of E.164 format (prefixed with a '+' sign), or a local format using local dialling plan and prefix. The IMS will interpret the phone number with a leading '+' to be a fully defined international number.

4.3.3.3b Termination of session with the TEL URI format Public User Identity

If a terminating session with a TEL URI is used, the HSS and the SLF (in the case that more than one independently addressable HSS is utilized by a network operator) shall support the TEL URI format Public User Identity.

4.3.3.4 Relationship of Private and Public User Identities

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

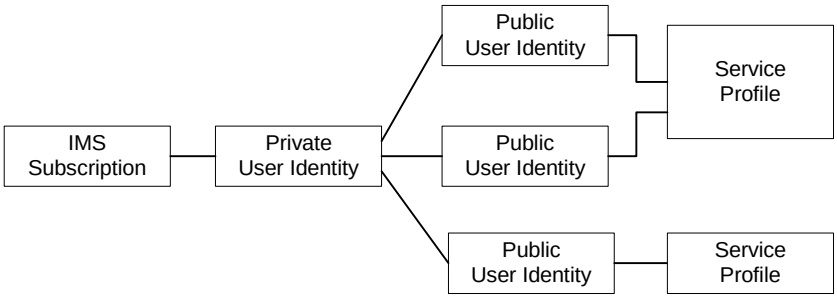


Figure 4.5: Relationship of the Private User Identity and Public User Identities

The IMS Service Profile is a collection of service and user related data as defined in TS 29.228 [30]. The Service Profile is independent from the Implicit Registration Set, e.g. Public User Identities with different Service Profiles may belong to the same Implicit Registration Set. Initial filter criteria in the service profile provide a simple service logic comprising of user / operator preferences that are of static nature i.e. they do not get changed on a frequent basis. It shall be possible to identify Alias Public User Identities. See clause 4.3.3.2 for more details.

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

The IMS service profile is defined and maintained in the HSS and its scope is limited to IM CN Subsystem. A Public User Identity shall be registered at a single S-CSCF at one time. All Public User Identities of an IMS subscription shall be registered at the same S-CSCF. The service profile is downloaded from the HSS to the S-CSCF. Only one service profile shall be associated with a Public User Identity at the S-CSCF at a given time. Multiple service profiles may be defined in the HSS for a subscription. Each Public User Identity is associated with one and only one service profile. Each service profile is associated with one or more Public User Identities.

An ISIM application shall securely store the home domain name of the subscriber. For UEs supporting only non-3GPP accesses, if neither ISIM nor USIM is present, but IMC is present, the home domain name shall be stored in IMC. It shall not be possible for the UE to modify the information from which the home domain name is derived.

It is not a requirement for a user to be able to register on behalf of another user which is third party registration specified in IETF RFC 3261 [12] or for a device to be able to register on behalf of another device or for combinations of the above for the IM CN subsystem for this release.

Public User Identities may be shared across multiple Private User Identities within the same IMS subscription. Hence, a particular Public User Identity may be simultaneously registered from multiple UEs that use different Private User Identities and different contact addresses. If a Public User Identity is shared among the Private User Identities of a subscription, then it is assumed that all Private User Identities in the IMS subscription share the Public User Identity.

The relationship for a shared Public User Identity with Private User Identities, and the resulting relationship with service profiles and IMS subscription, is depicted in Figure 4.6.

An IMS subscription may support multiple IMS users.

NOTE 1: The Public User Identity sharing mechanism described above is not intended to support sharing of identities across large numbers of Private User Identities, since this would result in all these users being forced to be associated with the same IMS subscription and hence the same S-CSCF.

NOTE 2: Subscription data is assumed to indicate which Public User Identities within a subscription are shared and which are not.

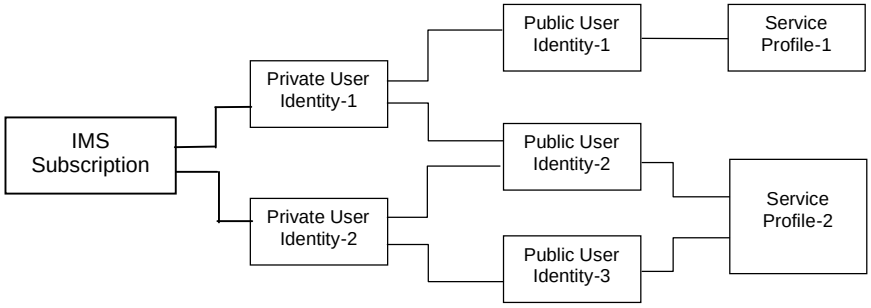


Figure 4.6: The relation of a shared Public User Identity (Public-ID-2) and Private User Identities

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

4.3.3.5 Relationship of Public User Identities, GRUUs, and UEs

Each Public User Identity may have one or more Globally Routable User Agent URIs (GRUUs). There are two types of GRUU, P-GRUUs and T-GRUUs which are associated with Public User Identities and are generated and assigned to the UE together during registrations and re-registration in a pair of one P-GRUU and one T-GRUU. Each pair of a P-GRUU and a T-GRUU is associated with one Public User Identity and one UE. During subsequent re-registrations the same P-GRUU will be assigned to the UE but a new and different T-GRUU will be generated and assigned. After a re-registration all the previous T-GRUUs generated during the period of this registration are all still valid. A UE may retain some or all of the previous T-GRUUs obtained during the initial registration or previous re-registrations along with the new T-GRUU or the UE may replace some or all of the previous T-GRUUs with the new T-GRUU. The current set of the P-GRUU and all T-GRUUs which are currently valid during this registration period is referred to here as the GRUU set. This relationship is depicted in figure 4.6a. If a UE registers (explicitly or implicitly) with multiple Public User Identities, a separate GRUU set is associated with each. If different UEs register with the same Public User Identity, a different GRUU set is associated with each.

NOTE: If the UICC is replaced the UE is still considered to be same UE instance and if that UE instance with a different UICC registers the same Public User Identity as was registered with the previous UICC the same P-GRUU will be assigned for that Public User Identity UE instance combination.

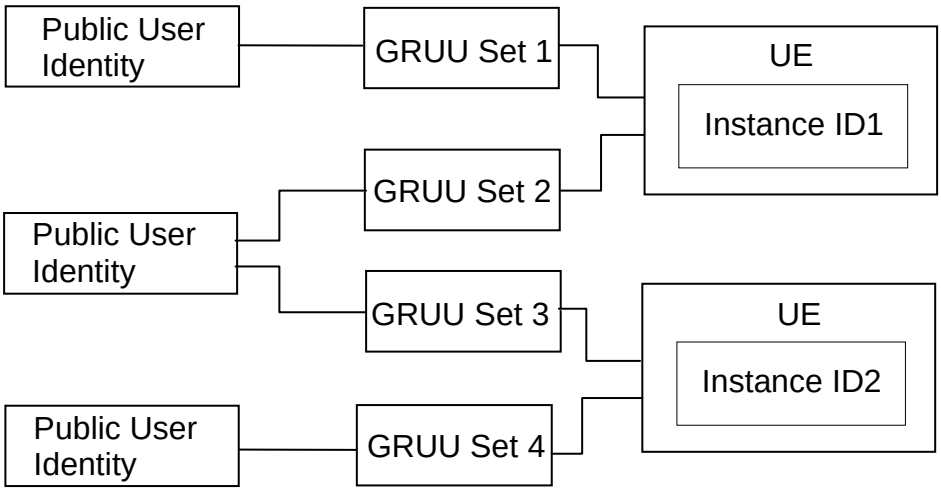


Figure 4.6a: The relationship of Public User Identities, GRUUs, and UEs

4.3.4 Identification of network nodes

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

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

4.3.5.1 ENUM/DNS translation mechanism

The ENUM/DNS translation mechanism as specified in IETF RFC 3761 [16] can be used by all IMS nodes that require E.164 address to SIP URI resolution. The actual ENUM/DNS database(s) used to perform address translations are outside the scope of 3GPP and are therefore a matter for the network operator. There is no requirement that the universal ENUM service on the Internet be used. As such, it is possible that the ENUM/DNS mechanism uses a different top level domain to that of "e164.arpa." (as mandated in IETF RFC 3761 [16], clause 1.2), therefore, the top level domain to be used for ENUM domain names shall be a network operator configurable option in all IMS nodes that can perform ENUM/DNS resolution.

In some scenarios, owners of ENUM servers may require information on who is the querying IMS operator, to determine an appropriate response (including whether to respond at all). This capability is required on the egress of the IMS network, particularly in the presence of shared network elements and intermediary IMS network(s) between the originating IMS operator and target ENUM/DNS server(s).

ENUM databases may contain Number Portability information. Number Portability is further described in clause 4.18.1.

4.3.5.2 Handling of Tel URIs

The S-CSCF shall support the ability to translate the E.164 address contained in a Request-URI in the Tel: URI format (as specified in IETF RFC 3966 [15]) to a SIP routable SIP URI using the ENUM/DNS translation mechanism as specified in clause 4.3.5.1. If this translation succeeds, then the session shall be routed according to the returned SIP URI. If this translation fails, then the session may be forwarded to a BGCF for further routing (e.g. to the PSTN) as described in clause 5.19 or appropriate notification shall be sent to the originating session endpoint, depending on network operator configuration.

When clause 4.15a (Roaming Architecture for Voice over IMS with Local Breakout) is in use, and the Home Network decides to loop-back the call to the visited network, the Home network can choose not to translate the E.164 address in the Request URI to a globally routable SIP URI, and leave it to the visited network.

4.3.5.3 Handling of SIP URIs representing a telephone number

Per network operator policy, the network may attempt to resolve and route a SIP URI representing a telephone number and a domain that does not own the target user using the ENUM/DNS translation mechanism specified in clause 4.3.5.1. The need for address resolution may be triggered by the S-CSCF, and the I-CSCF or transit function, as determined by network operator configuration. Procedures applied to the S-CSCF, I-CSCF and transit functions are outlined below.

When an originating S-CSCF receives an originating request with a Request-URI containing the SIP representation of an E.164 number, network operator policy shall dictate whether the procedure shall be carried out for all the domains of the SIP URI where those domains belong to the home network, or not at all. If operator policy indicates that the procedure is to be performed, then the S-CSCF shall reuse the procedure specified in clause 4.3.5.for handling of Tel URIs.

If the operator policy at the originating S-CSCF dictates that the procedure shall not be performed or the SIP URI containing the representation of an E.164 number contains a domain that does not belong to the home network, then the S-CSCF shall handle and route the request in the same manner as a SIP URI.

Prior to an HSS Location Query, the I-CSCF shall translate a SIP URI representing a telephone number contained in a Request-URI into the Tel: URI format specified in IETF RFC 3966 [15]. The resultant Tel URI shall then be used for performing the HSS Location Query.

If the HSS Location Query response indicates that the user does not exist, and if configured by operator policy, the I-CSCF shall invoke the portion of transit functionality that translates the E.164 address contained in the Tel URI in the Request-URI into a routable SIP URI, reusing the procedure specified in 4.3.5.2 for handling of Tel URIs.

NOTE: The entire transit functionality is not required for this purpose.

4.3.6 Public Service Identities

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

Public Service Identities shall take the form as defined in TS 23.003 [24].

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

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

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

4.4 Signalling concepts

A Single session control between the UE and CSCF:

- For Multi-Media type services delivered via the IP-CAN 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 IETF RFC 3261 [12], other relevant IETF RFC's, and additional enhancements required to support 3GPP's needs).

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

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

- MGCF and CSCF (Mg),
- between CSCFs (Mw),
- between a CSCF/IMS ALG and external IP networks (Mm),
- between CSCF and BGCF (Mi),
- between BGCF and MGCF (Mj),
- between BGCF/IMS ALG and BGCF (Mk), and
- between BGCF/CSCF and IBCF (Mx).

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

- The single session control protocol applied to these interfaces will be based on SIP (as defined by IETF RFC 3261 [12], other relevant IETF 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 than SIP based signalling between the UE and the CSCF.

Based on operator preference, border control functions may be applied between two IM CN subsystem networks or between an IM CN subsystem network and other SIP based multimedia network, see clause 4.14 and Annex I for details.

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 following procedures are supported by an UE when accessing IMS:

- Connect to the IP-CAN and acquire the necessary IP address, which includes, or is followed by, the P-CSCF discovery procedure. The mobility related procedures and IP address management principles for the IP-CAN are described in the relevant IP-CAN specifications;
- Register to the IM subsystem as defined by the IMS registration procedures;
- If an UE explicitly deactivates 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 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 IP-CAN bearers;
- If an UE changes its IP address according to IP-CAN procedures (e.g. TS 23.221 [7]), the UE shall re- register in the IMS by executing the IMS registration;
- If an UE acquires an additional IP address due to establishing an additional IP-CAN bearer through a different access network, the UE may perform an IMS registration using this IP address as the contact address. If IMS registration is performed, this IMS registration may co-exist with the previous IMS registration from this UE and the UE shall be notified that this IMS registration results in multiple simultaneous registrations.
- In order to be able to deliver an incoming IMS session, the 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;

4.6 Roles of Session Control Functions

4.6.0 General

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

4.6.1 Proxy-CSCF

The Proxy-CSCF (P-CSCF) is the first contact point within the IM CN subsystem. Its address is discovered by UEs using the mechanism described in the clause "Procedures related to Local CSCF Discovery". The P-CSCF behaves like a Proxy (as defined in IETF 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 IETF RFC 3261 [12] or subsequent versions), i.e. in abnormal conditions it may terminate and independently generate SIP transactions.

NOTE 1: When requests are sent towards another domain they may, if required, be routed via a local network exit point (IBCF), which will then forward the request to the entry point of the other domain. More details on this can be found in clause 4.14 and Annex I.

The P-CSCF in the role of an AF may interact with the Policy and Charging Architecture; the P-CSCF may interact over the Rx interface (see TS 29.214 [11]) with the the Policy and Charging Architecture defined in TS 23.203 [54]; the P-CSCF may interact over the Rx interface (see TS 29.214 [11]) or over the N5 interface (using the Npcf_PolicyAutorization service, see TS 29.514 [96]) with the the Policy and Charging Architecture defined in TS 23.503 [95].

The functions performed by the P-CSCF are:

- Forward the SIP register request received from the UE to an entry point 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.

- Ensure that the SIP messages received from the UE to the SIP server (e.g. S-CSCF) contain the correct or up to date information about the access network type currently used by the UE, when the information is available from the access network. Depending on operator policies, the P-CSCF may insert in any SIP message (request or response) the access network type currently used by the UE, when the information is available from the access network.

NOTE 2: For the 3GPP access network, the P-CSCF can derive information about the access network type currently used by the UE using PCC mechanisms as specified in TS 23.203 [54] and in TS 29.214 [11], or in TS 23.503 [95] and in TS 29.514 [96].

NOTE 3: IMS entities other than P-CSCF will not be informed by this mechanism of the change in the access network unless SIP messages are exchanged.

- Based on operator policies, and the availability of the user location information and/or UE Time Zone from the access network, ensure that relevant SIP messages contain the correct or up to date information about the user location information, and/or UE Time Zone provided by the access network currently used by the UE.

NOTE 4: For the 3GPP access networks and for TWAN access (as defined in clause 16 of TS 23.402 [82]), the P-CSCF can retrieve user location information and/or UE Time Zone related to the access network currently used by the UE using PCC mechanisms, as specified in TS 23.203 [54] and in TS 29.214 [11], or in TS 23.503 [95] and in TS 29.514 [96].

- Forward the SIP request or response to the UE.

  Detect and handle an emergency session establishment request.

- 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.
- Authorization of bearer resources and QoS management. For details see TS 23.203 [54] and TS 23.503 [95].
- Detection and handling of an originating or terminating IMS MPS session establishment request (see also clause 5.21).
- May support the Paging Policy Differentiation for IMS conversational voice as described in clause E.9 and clause Y.9.
- May subscribe to notification of changes in the type of access network using PCC mechanisms as specified in TS 23.203 [54] and in TS 29.214 [11] or in TS 23.503 [95] and in TS 29.514 [96].

4.6.2 Interrogating-CSCF

4.6.2.0 General

Interrogating-CSCF (I-CSCF) is the contact point within an operator's network for all connections destined to a user of that network operator, or a roaming user currently located within that network operator's service area.

NOTE- 1: If border control concepts are applied, the contact point within an operator's network may be different, see clause 4.14 and Annex I for details.

NOTE 2: When requests are sent towards another domain they may, if required, be routed via a local network exit point (IBCF), which will then forward the request to the entry point of the other domain. More details on this can be found in clause 4.14 and Annex I.

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 the clause 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.
- Translate the E.164 address contained in all Request-URIs having the SIP URI with user=phone parameter format into the Tel: URI format of IETF RFC 3966 [15] before performing the HSS Location Query. In the event the user does not exist, and if configured by operator policy, the I-CSCF may invoke the portion of the transit functionality that translates the E.164 address contained in the Request-URI of the Tel: URI format to a routable SIP URI.
- Obtain from HSS the Address of the S-CSCF.
- Forward the SIP request or response to the S-CSCF determined by the step above

Based on local configuration, the I-CSCF may perform transit routing functions (see clause 5.19). If the I-CSCF determines, based on an HSS query, that the destination of the session is not within the IMS, it may forward the request or it may return with a failure response toward the originating endpoint.

Charging and resource utilisation:

- Generation of CDRs.

4.6.2.1 Void

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:

For Registration:

- May behave as a Registrar as defined in IETF RFC 3261 [12] or subsequent versions, i.e. it accepts registration requests and makes its information available through the location server (e.g. HSS).
- When a registration request includes an Instance ID with the contact being registered and indicates support for GRUU, the S-CSCF shall assign a unique P-GRUU and a new and unique T-GRUU to the combination of Public User Identity and Instance ID.
- If a registration request indicates support for GRUU, the S-CSCF shall return the GRUU set assigned to each currently registered Instance ID.
- The S-CSCF shall notify subscribers about registration changes, including the GRUU sets assigned to registered instances.
- During registration process, the S-CSCF shall provide policy information, if available, for a Public User Identity from the HSS to the P-CSCF and/or UE.

NOTE 1: For example, the policy information includes MPS IMS Subscription status and policy applicable to enterprise network subscribers.

For 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 clause 5.2.1.
- May behave as a Proxy Server as defined in IETF 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 IETF RFC 3261 [12] or subsequent versions, i.e. it may terminate and independently generate SIP transactions.
- Based on the determined served user, handle interaction with Services Platforms for the support of Services
- Provide endpoints with service event related information (e.g. notification of tones/announcement together with location of additional media resources, billing notification)
- For an originating endpoint (i.e. the originating user/UE, or originating AS)
    - Obtain from a database the Address of the entry point for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URI), when the destination user is a customer of a different network operator, and forward the SIP request or response to that entry point.

      If a GRUU is received as the contact, ensures that the Public User Identity of the served user in the request and the Public User Identity encapsulated in the P-GRUU or associated with the T-GRUU belongs to the same service profile.
    - When the destination name of the destination user (e.g. dialled phone number or SIP URI), and the originating user is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.
    - Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.
    - Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.
    - Ensure the originating end point is subscribed to the determined IMS communication service.

- Ensure that the content of the SIP request or response (e.g. value included in Content-Type SIP header, media lines included in SDP) sent or received by the originating endpoint matches the determined IMS communication service definition, based on originating user's subscription.

- When the INVITE message includes an MPS code or an MPS input string, forward the INVITE, including the Service User's priority level if available.

- When an MPS user is authorized by an AS for priority service, include the Service User's priority level received from the AS in the INVITE and forward the INVITE.

NOTE 2: The mechanism to provide authorisation by an AS for priority service is out of scope of this specification.

- Attestation of the identity of the originating subscriber if configured through operator policies. Optionally the S-CSCF can invoke an AS for attestation of the identity of originating subscriber, if configured through operator policies.

NOTE 3: Only one network element performs attestation for an originating subscriber in the originating network.

- If the request is an originating request from an Application Server:

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

  - Process and proceed with the request even if the served user on whose behalf the AS had generated the request is unregistered. If the served user is unregistered, the S-CSCF shall execute any unregistered origination service logic on behalf of the served user before forwarding requests from an AS.

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

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

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

  - Forward the SIP request or response to a P-CSCF.

  - Modify the SIP request for routing an incoming session to CS domain according to HSS and service control interactions, if 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.

  - Ensure the terminating end point is subscribed to the determined IMS communication service.

  - Ensure that the content of SIP request or response (e.g. value included in Content-Type SIP header, media lines included in SDP) sent or received by the destination end point matches the determined IMS communication service definition, based on terminating user's subscription.

  - If the SIP request contains preferences for characteristics of the destination endpoint, perform preference and capability matching as specified in IETF RFC 3312 [41].

  - Optionally for a redirected session, if configured through operator policies, performs attestation of the identity of the diverting subscriber initiating the diversion.

  - Proxies a terminating request to an AS associated with the terminating user for signature verification if signature verification is required.

NOTE 4: The S-CSCF would normally proxy any terminating request to an AS via ISC for additional processing.

- For an originating request with a Request URI containing the SIP representation of an E.164 number, and configured per operator policy:

  - the S-CSCF attempts translation of the E.164 address in the SIP URI to a globally routable SIP URI using the procedures specified in clause 4.3.5. As stated in clause 4.3.5, if the E.164 address translation fails, the request may be forwarded to a BGCF to allow routing to the PSTN and if the translation succeeds, the Request URI is updated and the request is routed based on the SIP URI that was obtained.

NOTE 5: When requests are sent towards another domain they may, if required, be routed via a local network exit point (IBCF), which will then forward the request to the entry point of the other domain. More details on this can be found in clause 4.14 and Annex I.

Based on local configuration, the S-CSCF may be provisioned as the contact point within an operator's network for transit IMS scenarios and may perform transit routing functions (see clause 5.19).

Charging and resource utilisation:

- Generation of CDRs

4.6.4 Breakout Gateway Control Function

Based on local configuration, the Breakout Gateway Control Function (BGCF) may be provisioned as the contact point within an operator's network for transit IMS scenarios as described in clause 5.19. Otherwise the BGCF processes requests for routing from an S-CSCF for the case were the S-CSCF has determined that the session cannot be routed using DNS or ENUM/DNS (see clauses 5.4.3, 5.19 and 4.3.5 for more information).

The BGCF determines the next hop for routing the SIP message. This determination may be based on information received in the protocol, administrative information, and/or database access. For PSTN terminations, the BGCF determines the network in which PSTN/CS Domain breakout is to occur. If the routing determination is such that the breakout is to occur in the same network in which the BGCF is located, then the BGCF shall select a MGCF that will be responsible for the interworking with the PSTN/CS Domain. If the routing determination results in break out in another network, the BGCF will forward this session signalling to another BGCF in the selected network. If the routing determination results in the session being destined for another IMS network, the BGCF forwards the message to an I-CSCF in this IMS network. If the BGCF determines that there is another IP destination for the next hop, it forwards the message to that contact point.

There may be multiple BGCFs within an operator's network. The functions performed by the BGCF are:

- Determines the next hop for SIP routing.
- For PSTN terminations, 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.
- For PSTN terminations, 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

NOTE: When requests are sent towards another domain they may, if required, be routed via a local network exit point (IBCF), which will then forward the request to the entry point of the other domain. More details on this can be found in clause 4.14 and Annex I.

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.

4.6.5 Void

4.7 Multimedia Resource Function

The architecture concerning the Multimedia Resource Function is presented in Figure 4.7 below.

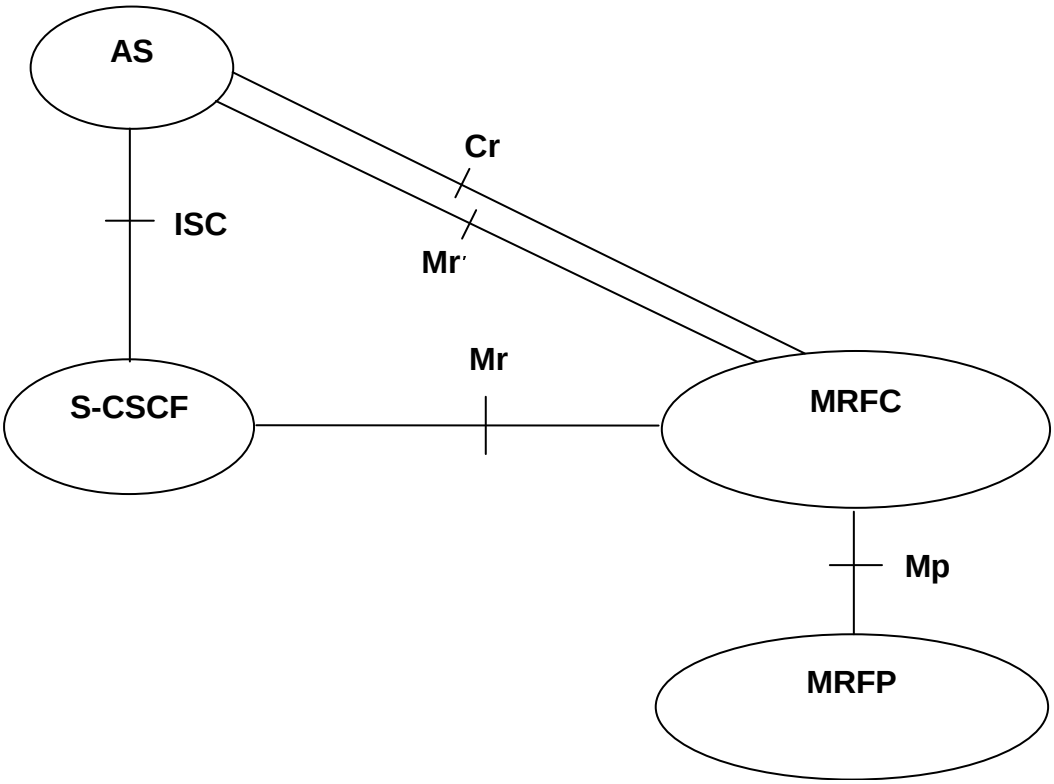


Figure 4.7: Architecture of MRF

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

Tasks of the MRFC are the following:

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

Tasks of the MRFP include the following:

- Control of the bearer on the Mb reference point.
- Provide resources to be controlled by the MRFC.
- Mixing of incoming media streams (e.g. for multiple parties).
- Media stream source (for multimedia announcements).
- Media stream processing (e.g. audio transcoding, media analysis).
- Floor Control (i.e. manage access rights to shared resources in a conferencing environment).

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

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

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

The Cr reference point allows interaction between an Application Server and an MRFC for media control. Further information on the Cr reference point is provided in TS 23.218 [71].

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

The Mp reference point has the following properties:

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

The protocol for the Mp reference point is described in TS 29.333 [59].

4.7a Media Resource Broker

The MRB supports the sharing of a pool of heterogeneous MRF resources by multiple heterogeneous applications. The MRB assigns (and later releases) specific suitable MRF resources to calls as requested by the consuming applications, based on MRF attributes specified by the applications as well as other criteria. For more information see TS 23.218 [71].

4.8 Security Concepts

IM CN Subsystem functional elements provide security, as needed, by security methods defined in TS 33.203 [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 TS 32.240 [25] and TS 32.260 [26]. The charging correlation information between IM CN subsystem and PS domain are also described in TS 24.229 [10a] and TS 29.207 [11a].

4.10 IMS group management concepts

4.10.0 General

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

4.10.1 IMS group administration

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

The Ut reference point shall support a scenario where one single Application Server is used to create groups that can be utilized for different services, possibly hosted by different ASes.

NOTE: Such an Application Server is sometimes referred to as a Group and List Management Server (GLMS).

4.10.2 Group identifiers

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

4.11 Relationship to 3GPP Generic User Profile (GUP)

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

4.12 Network Address Translation traversal in access network

It shall be possible to support the scenario where a NAT(-PT)/NAPT(-PT) residing between the IMS functionality in the UE and the P-CSCF has to be traversed for IMS communication. This shall include at least the types of NATs that implement address and port dependent mapping together with address and port dependent filtering, RFC 4787 [51].

NOTE: The UE may be one piece of equipment, or it may be a network of elements located on a end-user's physical premises.

4.13 Identification of IMS communication Services

4.13.1 General

This clause describes the architectural requirements for the identification of IMS communication services.

4.13.2 Identification of IMS communication Services

An IMS Communication Service Identifier (ICSI) provides a framework for the identification of IMS communication services utilising the IMS enablers. An IMS communication service is provided via the use of the IMS enablers. At terminals, the use of a communication service identifier is similar to the use of the port concept in TCP/IP, in that it allows applications in a terminal and the network that use SIP for communication purposes to be identified. In the terminal this means dispatching a SIP message to the correct application, and in the network it means selection of the correct application server over ISC. Examples of IMS based applications and communication services are OMA messaging and OMA PoC.

An IMS communication service defines restrictions to which SIP procedures are possible within a single SIP session or standalone transaction and how those SIP procedures are used. The IMS communication service contains an aggregation of zero, one, or several media components and the service logic managing the aggregation, represented in the protocols used. Its behaviour and characteristics may be standardized as done for the two examples above, or proprietary and specific for e.g. an operator or an enterprise.

A service description specifies this behaviour and states e.g. the allowed media combinations and state transitions as a consequence of signalling and use of IMS enablers in the network and terminals.

NOTE 1: The application server(s) required to support the IMS communication service are required to be included in the path of the standalone transaction or SIP session at the establishment of the SIP dialogue and therefore can not be linked in after the initial SIP request, i.e. once a SIP session has been established, it is not possible to change the IMS communication service for that session. A UE can establish a new SIP session with another IMS communication service identifier if it is required to add a media that is not supported by the existing IMS communication service.

The need of applying a service identifier is to be taken within the specification of each individual service.

The communication service identifier identifies IMS communication services and shall be included in the relevant SIP methods.

The IMS communication service identifier shall fulfil the following requirements:

1. It shall be possible for the UE and an Application Server (AS) to set the IMS communication service identifier in a SIP request, e.g. in the REGISTER and INVITE request.

2. Based on operator policy the S-CSCF or an AS shall be able to validate an IMS communication service identifier in a SIP request. This includes e.g. to check the syntactical correctness of a service identifier, and policing the usage of a communication service identifier. It shall also be possible for the S-CSCF and an AS to indicate that the value of the IMS communication service is validated. An asserted IMS communication service identifier shall be able to be indicated by the service in SIP responses to the SIP request along with information that the IMS communication service identifier is asserted.

NOTE 2: If the asserted IMS communication service provided in the SIP response differs from the requested IMS communication service, the UE can make a local decision on whether it wish to continue the session. The UE will ignore any IMS communication service it does not support. User interaction is not needed.

NOTE 3: If the asserted IMS communication service provided in the SIP response differs from the requested IMS communication service, the VPLMN can make a local decision on whether it wish to continue the session. If continuing, the asserted IMS communication service is used in VPLMN for the remainder of the session (e.g. to provide service aware charging).

3. It shall be possible, e.g. for the UE, S-CSCF and AS, to identify an IMS service uniquely by the IMS communication service identifier.

4. It shall be possible for the S-CSCF to invoke appropriate service logic based on the IMS communication service identifier contained in a SIP request, e.g. route a SIP request containing a service identifier based on initial filter criteria to the correct AS.

5. It shall be possible for the UE to invoke appropriate application based on the IMS communication service identifier contained in a received SIP request.

6. It shall be possible for the UE to indicate its service capabilities to the network, e.g. during registration, using the IMS communication service identifier.

NOTE 4: The UE does not need to indicate all the service capabilities it supports to the network.

7. It shall be possible for the network to inform the UE about service capabilities, represented by ICSIs, of the network.

8. The structure of the IMS communication service identifier shall be as simple as possible, i.e. the IMS communication service identifier shall be limited to identify a service.

9. Based on operator policy S-CSCF and AS shall consider the IMS communication service identifier for online and offline charging, e.g. put appropriate data into call detailed records.

10. The communication service identifier shall be capable of being an input into the policy control and charging rules.

11. It shall be possible to use the IMS communication service identifier as a means to authorize whether a subscriber is allowed to initiate or receive request for a communication service.

12. The communication service identifier shall be taken into account when selecting the correct UE(s), if multiple UEs are registered for the same Public User Identity(s).

13. The usage of communication service identifiers shall not adversely affect interoperability between IMS networks and interoperability with external SIP networks and CS networks. The behaviour of a network receiving the IMS requests without an IMS communication service identifier is a matter of operator policy. Usage of communication service identifiers shall not decrease the level of interoperability with networks and UEs that are unaware of the communication service identifier.

14. It shall be possible for the IMS network and UE to support communications that do not use a communication service identifier. In the case that an IMS communication service identifier is not present then the network may assume a particular IMS communication service.

15. The usage of communication service identifiers shall not restrict the inherent capabilities of SIP.

16. The usage of communication service identifiers shall not require additional user interaction, i.e. the communication service identifier is assumed to be "added" by the UE that initiates the communication.

17. Where a communication service needs to be identified, one requested IMS communication service identifier shall be included by the originator of the session in the SIP method that initiates a SIP dialogue or standalone transaction. In addition to the requested IMS communication service, the supported IMS communication services may be included.

18. This version of the specification does not require the capability to use multiple requested IMS communication service identifiers in the SIP method that initiates a SIP dialogue or standalone transaction. However, the protocol implementation shall nonetheless be prepared to transport more than one requested IMS communication service identifier and the network shall be prepared to handle the situation if multiple IMS communication service identifiers are received but the network is only required to take action on one of the values. The same applies for the UE.

19. To facilitate service aware charging for roaming, it shall be possible to provide an asserted IMS communication identifier service to the VPLMN.

The network and the terminal shall be able to continue operation as defined in 3GPP Release 5 and 3GPP Release 6.

The communication service identifier shall be available at least in the following interfaces:

- ISC, Gm, Ma, Mi, Mj, Mk, Mw, Mg, Mr, Mr′;
- Cx; Dx (e.g. as part of the iFC);
- Rx, N5;
- Rf, Ro.

NOTE 5: The communication service identifier does not replace the public service identity (PSI). The communication service identifier would be used to indicate the communication service used to access the service addressed via a PSI, and is required to identify the communication service even when SIP requests are sent towards another entity without using a PSI.

4.13.3 Identification of IMS applications

An IMS application is an application that uses an IMS communication service(s) in order to provide a specific service to the end-user. The IMS application uses specific IMS Communication Service(s) and provides the end user service through the reuse of the SIP communication part of service. The IMS application does not extend the definition of the IMS communication service. The IMS application reference identifies the application utilising the IMS communication service.

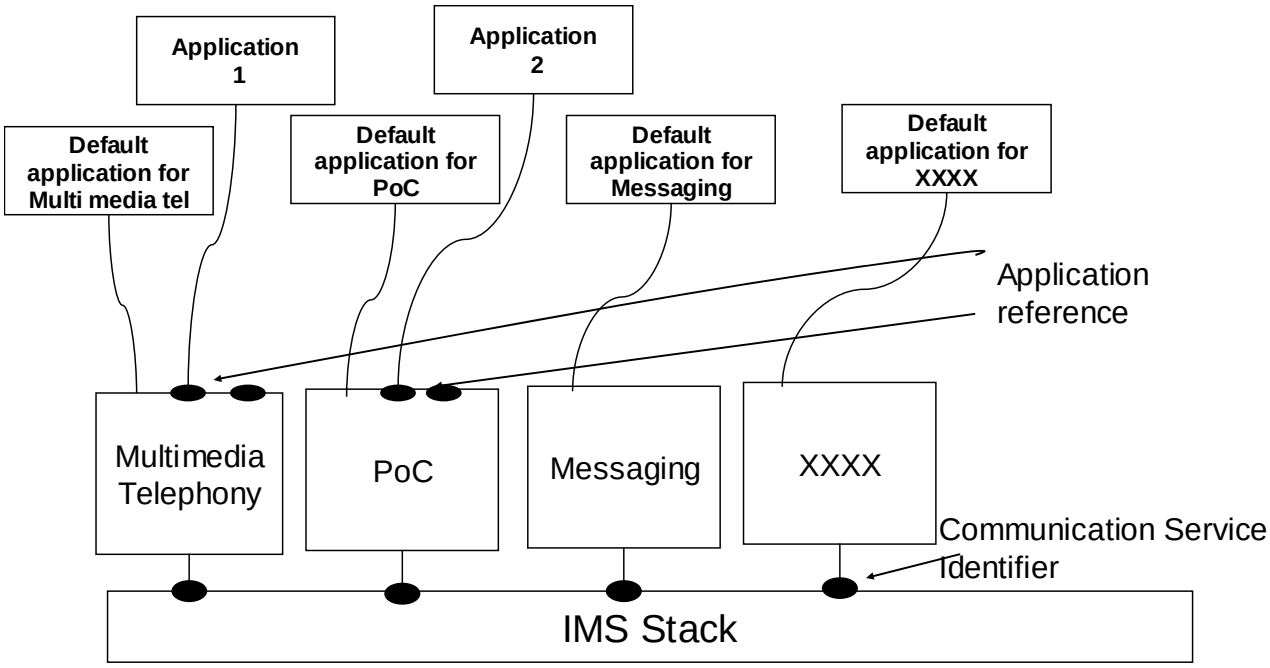


Figure 4.13-1: IMS applications on top of an IMS communication service

The IMS application reference is used to identify the IMS applications other than the default for the IMS communication service. The IMS application reference has significance at the UE and the SIP AS behaving as SIP endpoints. The means to transport the IMS application reference is defined within the IMS communication services. When used, it shall be possible to transport the IMS application reference on at least on the following interfaces:

- ISC, Gm, Ma; Mi, Mj, Mk, Mw, Mg, Mr, Mr′, Rx, N5, Rf, Ro.

It shall be possible to register the IMS application reference. The IMS application reference can be taken into account when selecting the correct UE(s), if multiple UEs are registered for the same Public User Identity(s).

4.14 Border Control concepts

Based on operator preference, border control functions may be applied between two IM CN subsystem networks or between an IM CN subsystem network and other SIP based multimedia network. These functions are provided by the IBCF and include:

- Controlling transport plane functions;
- Supporting functions to allow establishing communication between disparate address realms' SIP applications;
- Supporting functions to allow establishing communication between IM CN subsystems using different media codecs based on the interworking agreement and session information;
- Providing network configuration hiding 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, etc;

NOTE 1: Network configuration hiding was not intended to be invoked in IMS roaming scenarios when the P-CSCF and IBCF are both located in the visited network as information available in certain SIP headers may be used by the home network for further processing of signalling messages.

- Screening SIP signalling information based on source/destination and operator policy (e.g. remove information that is of local significance to an operator) and optionally, for an IBCF located in the home network, policing the IMS Communication Service ID;
- Generation of CDRs;
- Invoking an IWF when interworking between different SIP profiles or different protocols (e.g., SIP and H.323) is necessary; in this case the IWF acts as an entry point for the IMS network;

NOTE 2: IWF and IBCF may be co-located. The IWF is not specified within this release of the specification.

- Selecting the appropriate signalling interconnect.
- Indicating whether an incoming SIP request is to be handled as an originating request by subsequent nodes in the IMS network.
- For an originating session leaving an IBCF, the IBCF of the originating network, if configured through operator policies, invokes an AS for the signing of attestation and identity information if available in the incoming request. The IBCF includes the signed information in the outgoing request.
- For a terminating session entering the IBCF without attestation information, the IBCF adds, if configured through policies, gateway attestation information based on the network from which the request was received.
- For a terminating session entering the IBCF with signed attestation information, the IBCF, if configured through policies, invokes an AS for signature verification.

If border control concepts are to be applied in an IMS network, the IBCF acts as an entry point for this network (instead of the I-CSCF), and also acts as an exit point for this network.

NOTE 3: In this case the IBCF and I-CSCF may be co-located as a single physical node.

Based on local configuration, the IBCF may perform transit routing functions (see clause 5.19).

More detailed description of these functions is provided in Annex I.

4.15 IMS in transit network scenarios

4.15.1 General concepts

IMS generally provides services to end user customers of a network operator by directly supporting multimedia communications services to or from that operator's customers. However IMS may also be used in a number of other configurations where the capabilities of IMS are used to support CS domain customers of an IMS operator or in various other kinds of business arrangements where the capabilities may be used to support interconnection of other networks.

Clause 4.15.2 describes several types of configurations in which IMS might be used to support such network interconnection. These are not intended to represent all possible applications of IMS, but rather provide some basis for the mechanisms by which IMS provides these transit functionalities. Further description of IMS transit network procedures are found in Clauses 5.4a.2 and 5.19.

Clause 4.15.3 describes the cases in which IMS application services can be provided in relation to the IMS transit traffic.

4.15.2 IMS transit network configurations

There are at least three general cases in which IMS may be used for transit network support. These could be classified as in the following:

a) IMS operator providing transit functionality for its own, non-IMS (CS domain), customers:
In this case the operator is serving its own customers, some of which have been migrated to IMS while others are still CS Domain subscribers. In this case SIP traffic arrives at a configured entry point and PSTN traffic arrives at the operator's MGCF. This is similar to the normal Mobile Terminating cases for IMS, but in this case the CS domain subscribers do not have an IMS subscription. For the case where the destination user is not an IMS subscriber, the operator needs to route the session to the CS domain.

b) IMS operator providing transit functionality to enterprise networks:
In this case the operator is serving as a transit network for an enterprise IP network and provides connectivity to both PSTN and IP endpoints. Traffic from the enterprise network arrives at a provisioned routing entity and needs to be routed to either an IP network or to the PSTN depending on the terminating endpoint.

c) IMS operator providing transit functionality to other network operators:
In this case the operator is serving as an IMS session based routing backbone for a PSTN operator or another IP network and provides connectivity to both PSTN and IP endpoints (PSTN <-> PSTN, IP <-> IP, PSTN <-> IP). Traffic from the PSTN operator arrives at configured MGCFs for translation to SIP. IMS traffic arrives at a configured entry point. In either case the operator needs to route the traffic to either an IP network or to the PSTN depending on the terminating endpoint.

An IMS operator can provide transit functionality as above in addition to (originating or terminating) IMS services. In these situations analysis of an incoming SIP request is required before it can be determined whether transit or terminating services need to be provided for this request.

4.15.3 Providing IMS application services in transit network scenarios

When IMS provides transit functionality to other network operators or enterprise networks, the IMS may also provide IMS applications services to the network operator or enterprise network.

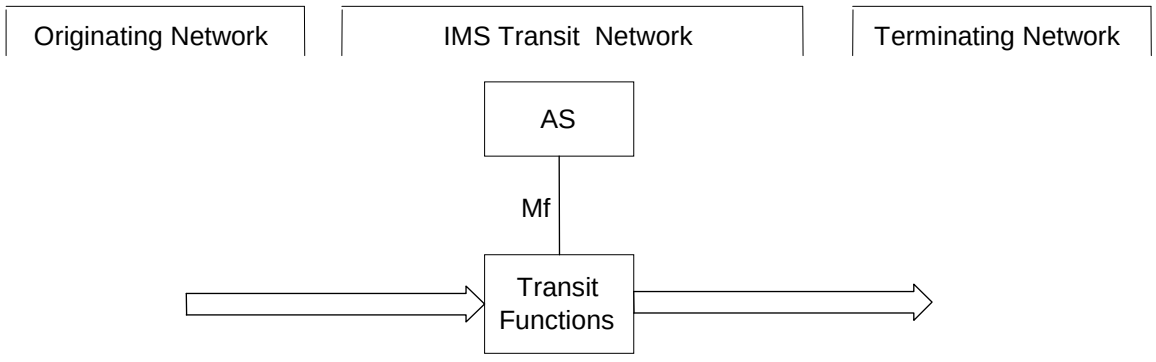


Figure 4.15.3-1: IMS application services reference point for transit network scenarios

The Transit service invocation shall be performed based on local configured Transit invocation criteria that are provided for the specific transit scenario.

The Transit invocation criteria for invocation shall have the possibility to take into account,

- (served) preceding network,
- (served) succeeding network, and
- other additional session information.

NOTE: The Transit invocation criteria are intended to be per served interconnected network basis and not per subscriber basis.

Similar to the initial filter criteria for a user profile, the Transit invocation criteria may have service point triggers based on different information in the request, such as source/destination, SIP method, session case, SIP header, and SIP body. The service invocation procedure shall support suppression/avoidance of conflicting services, multiple invocations of the same service and loopback scenarios.

The IMS application services provided can be classified as:

a) Originating IMS application services:

In this case the IMS operator provides IMS application services for SIP traffic being received from the served network operator or enterprise network. The application services, appropriate for the received SIP traffic, will be invoked when received from the served network, after which the traffic is routed towards the destination endpoint.

b) Terminating IMS application services:

In this case the IMS operator provides IMS application services for SIP traffic destined to a served network operator or enterprise network. The application services, appropriate for the received SIP traffic, will be invoked when the served network has been identified as the next network, or when the traffic has been identified as destined to the served network.

4.15a Roaming Architecture for Voice over IMS with Local Breakout

The Transit and Roaming Function is the combined functionalities of the transit network functions as defined in clause 4.15 and the roaming specific functions defined in this clause.

The following architectural requirements apply:

- The P-CSCF, S-CSCF, the Transit and Roaming Function, and other nodes performing routing procedures in different networks may control the application of OMR procedures by indicating in the signalling whether an IBCF/TrGW should not apply OMR.
- In order to allow scenarios where the media is not routed through the originating HPLMN, IBCFs handling incoming requests to the network should support OMR and allow bypass of TrGWs. Anchoring of media may be controlled via outgoing IBCFs.
- The HPLMN shall decide whether to perform the loopback procedure based on local policy and on knowledge of the support of the procedure in the VPLMN.
- The VPLMN shall be provided by the HPLMN with enough information to determine whether home routing has been applied (or has not been applied):
  - The HPLMN shall send an indication to the VPLMN that this session set-up is a loopback to allow differentiation from any other incoming call. By this means the VPLMN is able to apply the correct treatment for this looped incoming leg incl. charging and routing decisions.
- If local policy requires access to BGCF routing data to make the loopback decision for a particular originating INVITE request, then the loopback decision should be performed in the BGCF. Else it should be performed in the S-CSCF.
- The Transit and Roaming Function shall perform call routing towards the terminating network by selecting appropriate egress point (e.g., MGCF for CS/PSTN, IBCF to other IMS networks, or I-CSCF for termination in own network). The Transit and Roaming Function may use information such as originating UE location information to select a nearby egress point for media anchoring.

- The VPLMN may provide the HPLMN with a reference to the preferred Transit and Roaming Function to steer the selection of the Transit and Roaming Function. If the VPLMN does not provide the Transit and Roaming Function address then the HPLMN shall use the default derived address for the VPLMN.

- When the HPLMN operator does not use loopback to the Transit and Roaming Function in VPLMN, the HPLMN shall be able to anchor the media. This ensures that the signalling and media are routed together.

An overview of the principles and flows of the Roaming Architecture for Voice over IMS with Local Breakout are depicted in Annex M, clause M.3.

4.15b Roaming Architecture for Voice over IMS with home routed traffic

In this scenario, the anchor point for the IP address for both the IMS signalling and media traffic is in the home network for a roaming UE, i.e. for 3GPP systems, the GGSN, PGW or UPF for a roaming UE is in the HPLMN of the UE.

The following architecture requirements apply:

- The P-CSCF is located in the HPLMN

Additional architecture requirements and functions that are needed to support IMS services with home routed traffic are depicted in Annex W for EPS and in Annex Y for 5GS.

4.16 Support of multimedia telephony

4.16.1 Telephony Application Server

The Telephony Application Server is a SIP AS providing the network support for the multimedia telephony service, TS 22.173 [53]. If specific procedures and message flows include or require media interaction, the TAS and MRFC may be collocated.

NOTE: The support of multimedia telephony services may be allocated to one or more Application Servers.

4.16.2 Identification of multimedia telephony

The multimedia telephony communication service shall be associated with a communication service identifier to allow easy identification of the service.

When multimedia telephony is supported in a network, Voice/video calls originating from the PSTN/CS domain shall be marked with the communication service identifier associated with multimedia telephony communication service.

4.16.3 Session setup principles

When establishment of UE initiated IP-CAN bearer(s) for the media is required it is recommended to reserve IP-CAN bearer(s) at the reception of the SDP answer. If the UE has been made aware of the operator policies with regards to allowed media for the multimedia telephony service, then the UE may reserve IP-CAN bearer(s) at the sending of the SIP INVITE request. For multimedia telephony, the UE should only mark resource reservation as required for voice and video.

When there are no requirements for resource reservation or when required resources are available on the originating side, the P-CSCF on the terminating side may send available session information to the PCRF/PCF at the reception of the SDP offer, as in such cases the UE can attempt resource reservation before sending the SDP answer.

If configured through policies, the telephony AS, or any other AS, may perform for originating requests attestation of the identity of the originating subscriber.

If configured through operator policies, the telephony AS may perform for diverted sessions attestation of the identity of the diverting subscriber initiating the diversion,

In addition, and if configured through policies, the telephony AS, or any other AS, may perform for terminating requests signature verification, if one is included.

NOTE: Only one network element performs attestation for an originating subscriber in the originating network.

4.17 Support of short message service

4.17.1 IP Short Message Gateway (IP-SM-GW)

The IP-SM-GW acts as an SIP-AS in the IMS domain to provide the protocol interworking for the delivery of the short message between the UE and the Service Centre. All functionalities and interfaces of IP-SM-GW are defined in TS 23.204 [56].

4.18 Support of Number portability

4.18.1 Number portability

Number portability (NP) allows a user to retain their E.164 number when changing subscriptions from one network operator to another. As such, NP applies to TEL URIs and SIP URIs representing E.164 addresses. NP is subject to regional requirements and is accomplished through the retrieval of ported data from those databases. The specification of these databases is out of the scope of this document, but the NP data may be accessed through ENUM/DNS or accessed via existing (PSTN- and CS-domain) NP databases using the legacy PSTN/CS-domain protocols, such as TCAP.

Support of NP within a network and the exact means to make the number portability data available to IMS, is subject to and configured per operator policy. NP is not mandated by this specification on any network operator.

As configured per operator policy, IMS ENUM interfaces can be updated to support handling of the PSTN ENUM service per IETF RFC 4769 [57], which provides a URI containing an E.164 number with NP routing information and NP dip indicators. The IMS entity receiving NP information as a result of an ENUM/DNS query (e.g. S-CSCF), needs to support NP protocol parameters retrieved as part of ENUM/DNS procedures contained in clause 4.3.5. This IMS entity and any subsequent IMS entities/network elements used to process the call to the PSTN shall not remove the NP protocol parameters inserted in SIP messaging as part of the NP data retrieval procedure.

NP data can also be made available by means of direct access to PSTN/CS-domain NP Databases using the legacy PSTN/CS-Domain interfaces and protocols. To support this existing interface within the network, the requesting and subsequent network elements need to support, or not remove, NP protocol parameters within SIP messages that result from the NP data retrieval procedures. The procedures to retrieve the NP data using the legacy PSTN/CS-domain interfaces are out of scope of this specification.

Alternatively, per operator policy, the BGCF can retrieve NP data as part of the procedures to select an MGCF for PSTN connection. The interface used at the BGCF to retrieve the NP data is out of scope of this specification.

When clause 4.15a (Roaming Architecture for Voice over IMS with Local Breakout) is in use, and the Home Network decides to loop-back the call to the visited network, the Home network can choose not to retrieve NP data, and leave it to the visited network.

Alternatively, per operator policy, the MGCF may support legacy interfaces to retrieve number portability data.

NOTE: Although legacy protocols are used to access the number portability database, this does not imply that the IMS nodes (CSCFs, BGCFs) need to implement such protocols.

4.19 Support of Preferred Circuit Carrier Access and Per Call Circuit Carrier Selection

4.19.1 Preferred Circuit Carrier Access and Per Call Circuit Carrier Selection

Preferred Circuit Carrier Access allows the network operator to configure a preferred long distance circuit carrier for a subscriber, set of subscribers or all subscribers on the network. All long distance calls from a subscriber are routed to the long distance circuit carrier when preferred circuit carrier access applies. A SIP message parameter indicates the preferred circuit carrier selected. This parameter can be delivered to the PSTN. An application server can be used to insert preferred circuit carrier parameters. The BGCF needs to consider, and can insert, the preferred circuit carrier parameters when routing calls towards an MGCF.

Preferred Circuit Carrier Selection per call, also known as Dial-around, allows the subscriber to request a long distance carrier for a specific call. A dial-around request is dialled by the subscriber along with the called party number at call origination. As configured per operator policy, the dial-around circuit carrier selection can take precedence over other preferred circuit carrier selection that can be configured in the network. Therefore, based on operator policy, the preferred circuit carrier parameter is not to be replaced if already present in a SIP message with a dial-around indicator. A SIP message parameter indicates the preferred circuit carrier selected with a dial-around indicator. This parameter is delivered to the PSTN.

Support of preferred circuit carrier access and dial-around is optional within a network and is subject to, and configured per, operator policy.

4.20 Support of IMS Service Centralization and Continuity

IMS Service Centralization, defined in TS 23.292 [66] provides communication services such that all services, and service control, are based on IMS mechanisms and enablers. It enables IMS services when using CS access as bearer for the media.

IMS Service Continuity, defined in TS 23.237 [67] provides Session Transfer mechanisms to maintain service continuity in the event of access transfer for the case when such events are not hidden from the IMS session layer and thus service continuity could not otherwise be maintained.

All functionalities and reference points are defined in TS 23.292 [66] and TS 23.237 [67].

4.21 Support of Overlap Signalling

The support of overlap signalling consists of the functionality for conversion between overlap and en-bloc, as well as the functionality for digit collection.

The above mentioned functionalities may be implemented in different network nodes depending on the operator's deployment strategy (e.g. AS, IBCF, MGCF).

NOTE 1: Support for overlap signalling in the IMS is an option limited to the interworking function located within the PSTN/ISDN networks that use overlap signalling.

NOTE 2: Digit collection limits the number of messages with incomplete number and to find another node that support overlap signalling.

4.22 Support of Explicit Congestion Notification (ECN)

4.22.1 General

The ECN profile used to trigger codec rate adaptation for Multimedia Telephony is defined in TS 26.114 [76] and affects the following IMS entities: UE, MGCF/IM-MGW, IBCF/TrGW, IMS-ALG/ IMS-AGW, MRFP/MRFC, and the MSC Server enhanced for ICS/MSC Server enhanced for SRVCC with SIP/CS-MGW.

As specified in TS 26.114 [76]:

- an MGCF/IM-MGW can be used for inter-working between an ECN-capable client in a 3GPP network that properly handles ECN-marked packets and a CS network;
- an IBCF/TrGW supporting Multimedia Telephony can be used for interworking between an ECN-capable entity in a 3GPP network that properly handles ECN-marked packets, and:
  - a remote entity that does not use ECN;
  - a remote entity that supports ECN in different way than what is specified for Multimedia Telephony clients;
  - a network which does not handle ECN-marked packets properly.

A UE supporting Multimedia Telephony and ECN shall support the procedures described in TS 26.114 [76].

4.22.2 CS GERAN/UTRAN Interworking at MGCF/IM-MGW

If MGCF/IM-MGW supports Multimedia Telephony compliant ECN, it shall:

- support ECN Multimedia Telephony client procedures as described in TS 26.114 [76], except that the MGCF and IM-MGW do not determine whether ECN can be used based on the Radio Access Technology that is used towards the client; the MGCF/ IM-MGW act as an ECN endpoint towards the Multimedia Telephony terminal;
- support SDP ability to negotiate to ECN according to TS 26.114 [76];
- be capable of enabling end-to-end rate adaptation between Multimedia Telephony terminal and the CS terminal or IM-MGW by performing the following:
  - negotiate the use of ECN with the Multimedia Telephony terminal, if it can be confirmed that the network used towards the Multimedia Telephony terminal properly handles ECN-marked packets;

NOTE 1: An operator can ensure that the network used towards the Multimedia Telephony terminal properly handles ECN-marked packets by setting corresponding requirements on network equipment, and verifying that those requirements are met. No active signalling ("probing") during normal operation is required to ensure this.

  - trigger rate adaptation request towards the Multimedia Telephony terminal when receiving in the incoming IMS media flow IP packets marked with ECN-CE, regardless of whether the IM-MGW applies or does not apply transcoding;
  - inter-work adaptation requests between the Multimedia Telephony terminal and the CS GERAN/UTRAN when the IM-MGW bridges compatible codec configurations between the interfaces without applying a transcoding function; if the IM-MGW prefers to receive a lower codec mode rate from the Multimedia Telephony terminal than what the CS network indicates, e.g. after having received IP packets with ECN-CE, the IM-MGW may replace the codec mode requested from the CS side with the codec mode that the IM-MGW prefers;
  - perform media adaptation (e.g. reduce media bit-rate) towards the Multimedia Telephony terminal when receiving from the latter an adaptation request and the IM-MGW applies transcoding.

NOTE 2: For CS interworking the MGCF/MGW does not have to perform transcoding if the same codec is selected on the CS and PS network.

4.22.3 Interworking with non-ECN IP network and/or terminal at IBCF/TrGW

An IBCF/TrGW may support Multimedia Telephony using ECN and can be used to enable ECN within the local network when either the remote network cannot be confirmed to properly handle ECN-marked packets or the remote entity does not support or use ECN.

In order to support Multimedia Telephony using ECN when interworking with a remote network that cannot be confirmed to properly handle ECN-marked packets and/or with a remote terminal does not support or use ECN, the IBCF/TrGW shall:

- determine from local configuration if the remote network properly handles ECN-marked packets;
- determine with SDP offer/answer procedures if the remote entity supports ECN;
- support SDP ability to negotiate to ECN according to TS 26.114 [76];
- be capable of enabling end-to-end rate adaptation between the local Multimedia Telephony terminal and the remote entity or TrGW by performing the following towards the local Multimedia Telephony terminal:
  - negotiate the use of ECN;
  - support ECN Multimedia Telephony client procedures as described in TS 26.114 [76], except that the IBCF/TrGW does not determine whether ECN can be used based on the Radio Access Technology; the IBCF/TrGW acts as an ECN endpoint towards the ECN capable Multimedia Telephony terminal;
  - trigger rate adaptation request towards the Multimedia Telephony terminal when receiving in the incoming IMS media flow IP packets marked with ECN-CE, regardless of whether the TrGW applies or does not apply transcoding; this requires that the IBCF provides the TrGW with the media configuration, even if transcoding is not supported or applied, when the IP termination is configured with ECN;
  - forward adaptation requests between the Multimedia Telephony terminal and the remote entity when the TrGW bridges compatible codec configurations between the interfaces without applying a transcoding function; if the TrGW prefers to receive a lower codec mode rate from the Multimedia Telephony terminal than what the other SIP network indicates, e.g. after having received IP packets with ECN-CE, the TrGW may replace the codec mode requested from the other SIP network with the codec mode that the TrGW prefers;
  - perform media adaptation (e.g. reduce media bit-rate) towards the Multimedia Telephony terminal when receiving from the latter an adaptation request and the TrGW applies transcoding.

NOTE: For this interworking the IBCF/TrGW does not have to perform transcoding if the same codec is selected on both sides of the TrGW.

4.22.4 Interworking with non-3GPP ECN IP terminal at IBCF/TrGW

An IBCF/TrGW supporting Multimedia Telephony compliant ECN can also be used to enable ECN end-to-end if the remote entity uses ECN in a different way than what is described in TS 26.114 [76], e.g. if the remote entity only supports probing for the ECN initiation phase or it needs the ECN feedback.

NOTE: For this interworking the IBCF/TrGW does not have to perform transcoding if the same codec is selected between both terminals.

4.22.5 ECN support at IMS-ALG/IMS-AGW

The P-CSCF shall be able to disallow the negotiation of ECN during SDP offer/answer exchanges if the IMS-AGW does not support transparent forwarding of the ECN bits or if the IMS core network or the access network used towards the Multimedia Telephony terminal do not properly handle ECN-marked packets.

An IMS-AGW supporting ECN shall be able to forward the ECN bits as instructed by the IMS-ALG.

The IMS-ALG/IMS-AGW may act as an ECN endpoint towards the access network and/or the IMS Core Network to enable ECN when the ECN connection cannot be established or maintained transparently (e.g. after PS-CS Access Transfer).

When acting as an ECN endpoint the IMS-AGW shall support end-to-end rate adaptation between the local terminal and the remote entity by performing the following:

- trigger rate adaptation request towards the ECN-capable peer when receiving in the incoming IMS media flow IP packets marked with ECN-CE, regardless of whether the IMS-AGW applies or does not apply transcoding;
- forward adaptation requests between the local and the remote peer when the IMS-AGW bridges compatible codec configurations between the interfaces without applying a transcoding function;

- perform media adaptation (e.g. reduce media bit-rate) towards the ECN-capable peer when receiving from the latter an adaptation request and the IMS-AGW applies transcoding.

4.22.6 ECN support at MRFC/MRFP

An MRFC/MRFP may support Multimedia Telephony using ECN and may act as an ECN endpoint to enable ECN with a local ECN-capable terminal within a local network that properly handles ECN-marked packets (see TS 23.333 [73]).

This requires that the MRFC/MRFP performs the following:

- support SDP ability to negotiate to ECN according to TS 26.114 [76];
- be capable of enabling end-to-end rate adaptation between the local Multimedia Telephony terminal and the MRFP by performing the following towards the local Multimedia Telephony terminal:
  - negotiate the use of ECN;
  - support ECN Multimedia Telephony client procedures as described in TS 26.114 [76], except that the MRFC/MRFP does not determine whether ECN can be used based on the Radio Access Technology; the MRFC/MRFP acts as an ECN endpoint towards the ECN capable Multimedia Telephony terminal;
  - trigger rate adaptation request towards the Multimedia Telephony terminal when receiving in the incoming IMS media flow IP packets marked with ECN-CE;
  - perform media adaptation (e.g. reduce media bit-rate) towards the Multimedia Telephony terminal when receiving from the latter an adaptation request.

4.22.7 CS GERAN/UTRAN Interworking at the MSC Server enhanced for ICS/MSC Server enhanced for SRVCC with SIP/CS-MGW

If the MSC Server enhanced for ICS/MSC Server enhanced for SRVCC with SIP/CS-MGW supports Multimedia Telephony compliant ECN, it shall support the procedures specified in clause 4.22.2 respectively for the MGCF and IM-MGW.

4.23 Support of Load Balancing

4.23.1 General

An IMS network may implement functionality for IMS serving network nodes (S-CSCF, Transit Function) to handle load balancing, i.e. the technique to distribute workload evenly across two or more network nodes implementing the same functions, in order to get optimal resource utilization.

For S-CSCFs, load balancing may be applied for received initial registration requests (see clause 4.23.2).

For Transit Functions, load balancing may be applied for received service requests, i.e. initial SIP requests requesting a service (see clause 4.23.3).

4.23.2 Registration-based load balancing of S-CSCFs

Load balancing of S-CSCFs for received initial registration requests may be based on load balancing functionality performed by an I-CSCF or it may be based on mechanisms outside IMS functional entities (such as DNS). An example of the DNS-based load balancing approach is the use of functionality that collects load information of S-CSCFs, applies a load balancing algorithm and provides the outcome to a (Dynamic) DNS, which subsequently is used implicitly by I-CSCFs.

An I-CSCF that performs load balancing of S-CSCFs for initial registration requests shall assign a received registration request to one of the available and suitable S-CSCFs using a load balancing algorithm. Such load balancing algorithm may take load information of the S-CSCFs into consideration if available. Load information may be obtained via management interfaces, via proprietary interfaces, or via other mechanisms.

4.23.3 Registration independent load balancing of Transit Functions

Load balancing of Transit Functions for received service requests may be based on load balancing functionality performed by an IMS functional entity that is the immediate source of the service request to the Transit Function (e.g. an IBCF or an I-CSCF), or it may be based on mechanisms outside IMS functional entities (such as DNS). An example of the DNS-based load balancing approach is the use of functionality that collects load information of Transit Functions, applies a load balancing algorithm and provides the outcome to a (Dynamic) DNS, which subsequently is used implicitly by IMS functional entities that require the IP-address of a Transit Function for routing a service request.

An IMS functional entity that performs load balancing of Transit Functions for service requests shall assign a received service request to one of the available and suitable Transit Functions using a load balancing algorithm. Such load balancing algorithm may take load information of the Transit Functions into consideration if available. Load information may be obtained via management interfaces, via proprietary interfaces, or via other mechanisms.

4.24 Support of Restoration Procedures

An I-CSCF that performs recovery of S-CSCFs for registration requests shall determine failure of an S-CSCF implicitly (i.e. via a timeout) or explicitly (i.e. via a failure message) and shall reroute the registration request to another S-CSCF based on the restoration procedures as defined in TS 23.380 [80].

4.25 Support of Overload Control

4.25.1 General

Network elements within the IP Multimedia CN subsystem may have to cope with high volume of signalling traffic with significant traffic peaks. An IMS network may therefore implement overload control functionality in IMS network elements to prevent overload situations.

For that purpose, two different mechanisms are provided:

- A mechanism based on next-hop monitoring of overload, where an IMS node acting as a SIP server may provide overload control feedback to its neighbours. This mechanism is described in clause 4.25.2.

NOTE 1: This mechanism is well suited for preventing overload of core network servers (CSCF) where overload is not due to calls to a specific application/destination.

- A filter-based mechanism where an IMS node acting as SIP server, may send load control filters to another IMS node that has subscribed for receiving this information. This mechanism is described in clause 4.25.3.

NOTE 2: This mechanism is particularly well suited for application servers when the source of overload is due to calls to a specific destination (e.g. a 800 application overloaded by mass calling to a particular destination).

Emergency calls shall not be affected by the overload traffic restrictions due to overload control and MPS priority information shall be taken into account when applying by the overload traffic restrictions based on received indications.

4.25.2 Next-hop monitoring of overload

For IMS entities supporting next-hop monitoring of overload, these IMS entities shall support a mechanism for monitoring overload of neighbour nodes with minimal overhead, to enable scenarios where the overload status needs to be adjusted frequently.

IMS entities supporting SIP, e.g. S-CSCF, shall be able to provide overload control feedback to their neighbours by providing load reduction directives within SIP responses. The neighbour nodes shall be able to adapt the traffic sent to the overloaded node by restricting the traffic offered to the overloaded neighbour node in accordance with the overload status information received.

It is recommended that when next-hop monitoring of overload is deployed for a specific function, all neighbour nodes also support the feedback of overload control status and support the overload traffic restriction procedures towards the specific function being monitored.

The next hop monitoring of overload procedures should at least be possible to use for the following scenarios:

- Network internal overload control between core functions, e.g., between different CSCFs.
- Application Server overload control (i.e., between CSCF and AS).
- Roaming and Interconnect (e.g., between IBCFs of two different networks).
- Transit scenarios (e.g., between IBCF and Transit function).

4.25.3 Filter based Overload Control

When filter based Overload Control is deployed, an IMS entity supporting SIP overload control (e.g. originating AS or S-CSCF) may subscribe to traffic filter information of specific IMS SIP server destination which may be subject to overload (e.g. an 800 application overloaded by mass calling to a specific number), and perform overload traffic restriction according to the information received. Alternatively, when the destination is not in IMS, the IMS entity performing the overload traffic restrictions may subscribe to an IMS SIP server providing traffic filter information related to the destination, or can have configured overload traffic filter information for the specific destination.

IMS entities supporting this mechanism shall match all SIP requests they send against received traffic filter information.

If such a filter based mechanism is used, it is recommended that the function performing the overload traffic restrictions be as close to originating party as possible, while still having sufficiently aggregated traffic to perform restrictions on, e.g., by allowing the originating AS/S-CSCF to subscribe to the traffic filter information from a terminating AS.

4.26 Support for Business Trunking

An IMS network may support business trunking for IP-PBXs in two different modes.

- Registration mode, or
- Static mode.

In both modes, the IP-PBX can be provisioned as a subscriber in the HSS.

In registration mode, the IP-PBX registers to and receives service from the IMS network in same manner as an ordinary subscriber.

In static mode, the IP-PBX does not perform any registration procedures.

Description on the support for IP-PBX business trunking is provided in Annex S and TS 24.525 [81]. The support for business trunking in static mode is provided by either an IBCF or a P-CSCF and clarified in Annex S.

5 IP multimedia subsystem procedures

5.0 General

This clause 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.

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

5.0a Session-unrelated procedures

The IM CN Subsystem provides means to conduct session-unrelated interactions between users, e.g. OPTIONS query, outband REFER. These interactions are described in IETF RFC 3261 [12], and other possible IETF RFCs. The generic capability exchange mechanism is defined in TS 23.279 [52].

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 clauses and specifications.

5.1 CSCF related procedures

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

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

For a UE using the IMS Local Breakout procedure as shown in Annex M, the IP address of the UE obtained from the local Gateway (i.e. single IP address) is used for both IM Subsystem related signalling and media.

5.1.1 Procedures related to Proxy-CSCF discovery

5.1.1.0 General

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

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

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

  - Use of DHCP to provide the UE with the domain name and/or IP address 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.

- The UE may be configured (e.g. during initial provisioning or via a 3GPP IMS Management Object (MO), TS 24.167 [64] or in the ISIM, TS 31.103 [69]) to know the fully qualified domain name (FQDN) of the P-CSCF or its IP address. If the domain name is known, DNS resolution is used to obtain the IP address.

If DNS is used to obtain the IP address of the P-CSCF, the name-address resolution mechanism is allowed to take the load information of the P-CSCFs (e.g. obtained using network management procedures) into consideration when deciding the address of the P-CSCF for the UE.

In the case where UE is aware of more than one P-CSCF address, the selection shall be based on home operator configured policy to select the P-CSCF.

NOTE: Subject to home operator policy, the UE selects the Home P-CSCF to be used by either using a pre-configured Home P-CSCF FQDN or according to TS 24.167 [64]. This can be done without the UE first performing the local P-CSCF discovery (e.g. DHCP).

5.1.1.1 DHCP/DNS procedure for P-CSCF discovery

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

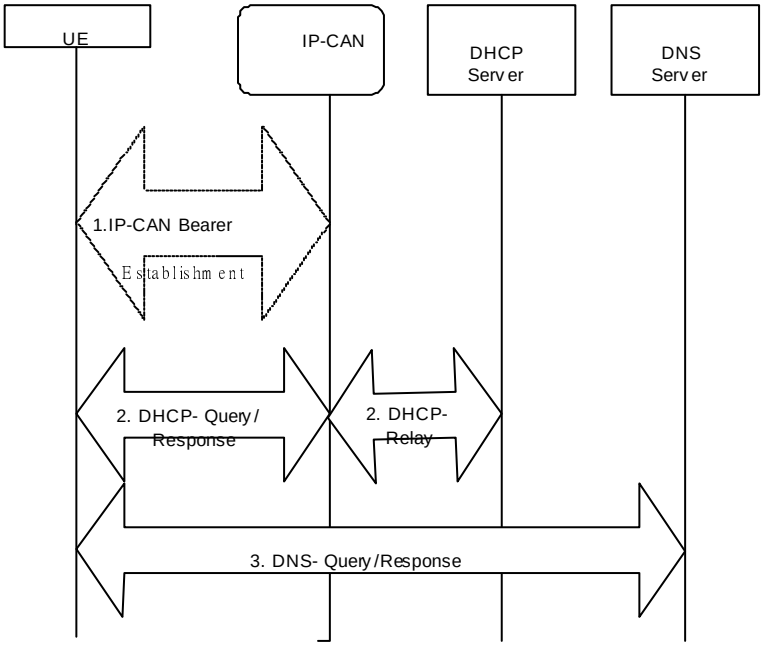


Figure 5.0a: P-CSCF discovery using DHCP and DNS

1. Establish an IP-Connectivity Access Network bearer if not already available by using the procedures available in the IP-Connectivity Access Network.

2. The UE requests a DHCP server and additionally requests the domain name and/or IP address 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 Void

5.1.2 Procedures related to Serving-CSCF assignment

5.1.2.1 Assigning a Serving-CSCF for a user

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1.2.2 Cancelling the Serving-CSCF assignment

Cancellation of the assigned Serving CSCF is either:

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

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

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

5.1.2.3 Void

5.1.3 Procedures related to Interrogating-CSCF

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

5.1.4 Procedures related to Proxy-CSCF

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

5.1.5 Subscription Updating Procedures

5.1.5.0 General

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

5.1.5.1 Subscription updating information flow

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

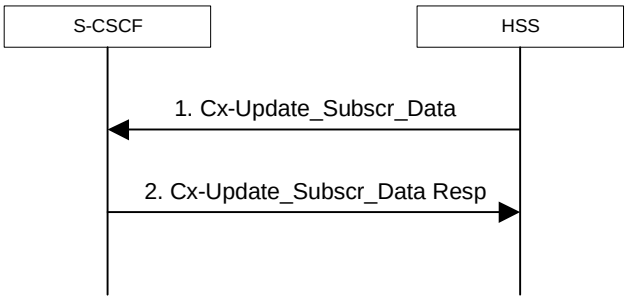


Figure 5.0b: Subscription data updating

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

5.2 Application level registration procedures

5.2.0 General

The following clauses 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 registers with the IM CN subsystem.

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

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

   - Currently it is required that at least one Public User Identity shall be stored in the ISIM application or, for UEs supporting only non-3GPP accesses, in the IMC, if IMC is present. If 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 or IMC directly.

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

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

10. It shall be possible to register a Public User Identity that is simultaneously shared across multiple contact addresses (at the same or via separate UEs) via IMS registration procedures. However, each registration and each de-registration process always relates to a particular contact address and a particular Private User Identity.

    The number of allowed simultaneous registrations is defined by home operator policy, e.g. locally configured at the S-CSCF or, when registration is requested via separate UEs, per subscribed value if received from the HSS.

10a. It shall be possible for the UE to indicate to the network whether the registration adds a new contact to an existing registration from the same UE.

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

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

13. The UE may indicate its capabilities and characteristics in terms of SIP User Agent capabilities and characteristics described in IETF RFC 3840 [38] during IMS registration. The UE may also update its capabilities by initiating a re-registration when the capabilities are changed on the UE.

14. If a UE supports GRUU, the UE shall indicate its support for GRUUs and obtain a P-GRUU and a T-GRUU for each registered Public User Identity during IMS registration as described in RFC 5627 [49].

15. The P-CSCF may subscribe to notifications of the status of the IMS Signalling connectivity after successful initial user IMS Registration.

16. When the access network type information is available from the access network, the P-CSCF shall ensure that the IMS registration request received from the UE to the SIP server (e.g. S-CSCF) contains the correct information. The P-CSCF may subscribe to notification of changes in the type of access network.

17. The P-CSCF shall cancel any active subscription e.g. to notifications of the status of the IMS Signalling connectivity and/or of the change of access network type when the user is de-Registered from the IM CN subsystem.

18. When the UE determines that the radio conditions are suitable for IMS PS voice/video services (e.g. UE is in normal coverage or in CE mode A as defined in Annex E, clause E.1.2) then UE may register for IMS voice/video services.

5.2.1a Implicit Registration

5.2.1a.0 General

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

- HSS has the set of Public User Identities that are part of implicit registration.
- Cx reference point between S-CSCF and HSS shall support download of all Public User Identities associated with the implicit registration, during registration of any of the single Public User Identities within the set.
- All Public User Identities of an Implicit Registration set must be associated to the same Private User Identities. See figure 5.0d for the detailed relationship between the public and private user entities within an Implicit Registration set.
- When one of the Public User Identities within the set is registered, all Public User Identities associated with the implicit registration set are registered at the same time.
- When one of the Public User Identities within the set is de-registered, all Public User Identities that have been implicitly registered are de-registered at the same time.
- Registration and de-registration always relates to a particular contact address and a particular Private User Identity. A Public User Identity that has been registered (including when implicitly registered) with different contact addresses remains registered in relation to those contact addresses that have not been de-registered.
- Public User Identities belonging to an implicit registration set may point to different service profiles; or some of these Public User Identities may point to the same service profile.
- When a Public User Identity belongs to an implicit registration set, it cannot be registered or de-registered individually without the Public User Identity being removed from the implicit registration list.
- All IMS related registration timers should apply to the set of implicitly registered Public User Identities
- S-CSCF, P-CSCF and UE shall be notified of the set of Public User Identities belonging to the implicitly registered function. Session set up shall not be allowed for the implicitly registered Public User Identities until the entities are updated, except for the explicitly registered Public User Identity.
- The S-CSCF shall store during registration all the Service profiles corresponding to the Public User Identities being registered.
- When a Public User Identity is barred from IMS communications, only the HSS and S-CSCF shall have access to this Public User Identity.

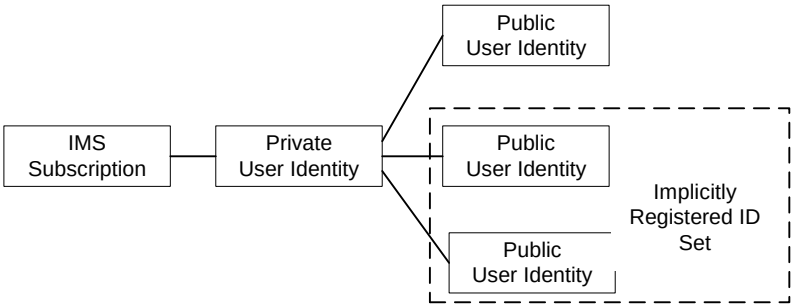


Figure 5.0c: Relationship of Public User Identities when implicitly registered

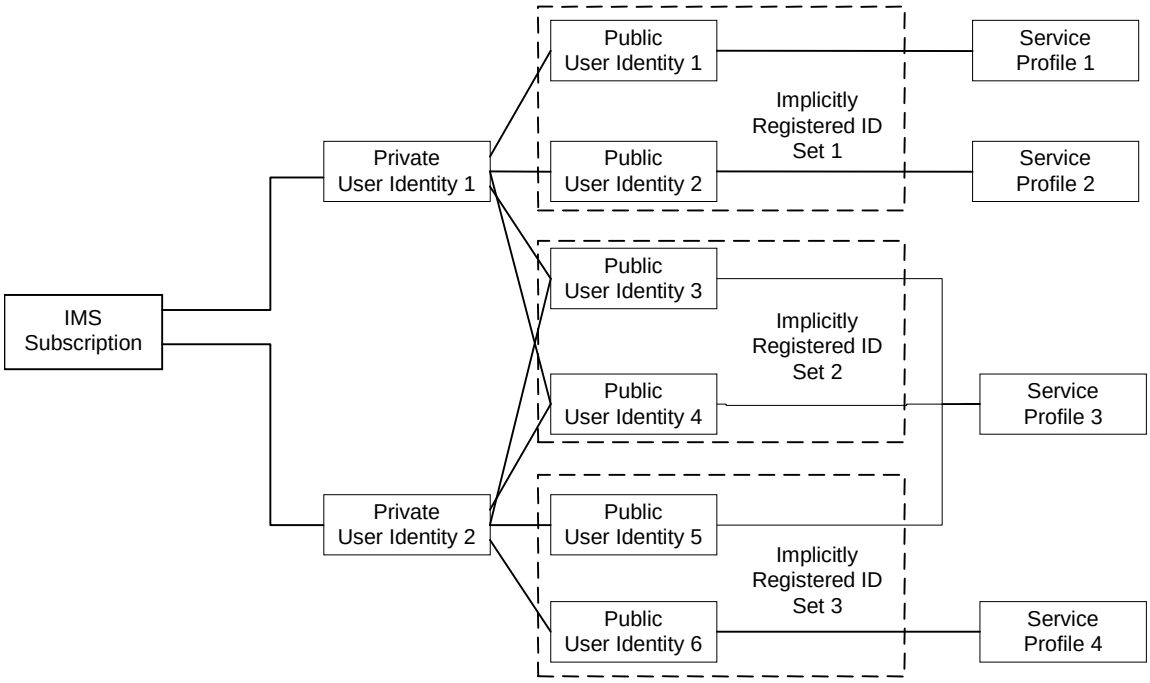


Figure 5.0d: The relation of two shared Public User Identities (Public-ID-3 and 4) and Private User Identities

5.2.1a.1 Implicit Registration for UE without ISIM or IMC

If an UE is registering in the IMS without ISIM or, for UEs supporting only non-3GPP accesses, without IMC, it shall require the network's assistance to register at least 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 or IMC-less UEs to register the Public User Identity(s). In addition to the functions defined in clause 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 clause 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 clause 5.3.2.3:

1. IP-CAN bearer is already established for signalling and a mechanism exists for the first REGISTER message to be forwarded to the proxy.
2. The I-CSCF shall use a mechanism for determining the Serving-CSCF address based on the required capabilities. The I-CSCF obtains the name of the S-CSCF from its role as an S-CSCF selector (Figure 5.1) 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 clauses 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 TS 33.203 [19].

5.2.2.3 Registration information flow – User not registered

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

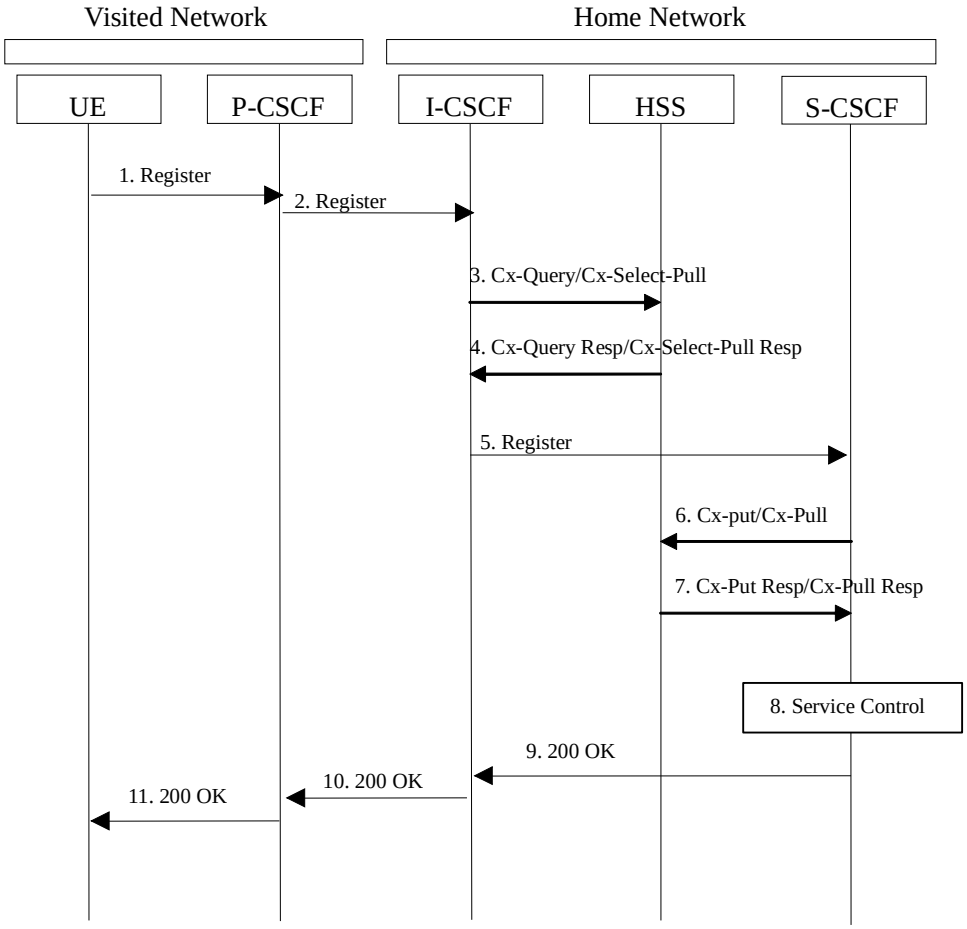


Figure 5.1: Registration – User not registered

1. After the UE has obtained IP connectivity, it can perform the IM registration. To do so, the UE sends the Register information flow to the proxy (Public User Identity, Private User Identity, home network domain name, UE IP address, Instance Identifier, GRUU Support Indication).

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

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

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

4. Cx-Query Resp/Cx-Select-Pull Resp is sent from the HSS to the I-CSCF. It shall contain the S-CSCF name, if it is known by the HSS, or the S-CSCF capabilities, if it is necessary to select a new S-CSCF. When capabilities are returned, the I-CSCF shall construct a name from the capabilities returned.

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

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. The name-address resolution mechanism is allowed to take the load information of the S-CSCFs (e.g. obtained using network management procedures) into consideration when deciding the address of the S-CSCF. The I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. 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 to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiation signalling to the home network.

   The S-CSCF shall reject the registration if the number of registered contact addresses for a Public User Identity from the same UE exceeds the limit of simultaneous registrations configured at the S-CSCF. The S-CSCF shall also reject the registration from separate UEs if the allowed number of simultaneous registrations according to the S-CSCF configuration or per subscribed value for a Public User Identity received from the HSS exceeds the limit of simultaneous registrations. The S-CSCF shall store the P-CSCF address/name, as supplied by the visited network. This represents the address/name that the home network forwards the subsequent terminating session signalling to the UE. The S-CSCF shall store the P-CSCF Network ID information.

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

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

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

9. The S-CSCF shall return the 200 OK information flow (home network contact information, a GRUU set) to the I-CSCF.

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

11. The P-CSCF shall store the home network contact information, and shall send information flow 200 OK (a GRUU set) to the UE. The P-CSCF may subscribe to notifications of the status of the IMS Signalling connectivity from PCRF/PCF (see TS 23.203 [54] and TS 23.503 [95] for more details).

    If the S-CSCF receives the priority information of the MPS subscribed-UE as a part of user profile from the HSS, the S-CSCF provides the priority information to the P-CSCF and the P-CSCF stores this information for the MPS-subscribed UE.

5.2.2.4 Re-Registration information flow – User currently registered

Periodic application level re-registration is initiated by the UE either to refresh an existing registration or in response to a change in the registration status of the UE. A re-registration procedure can also be initiated when the capabilities of the UE have changed or the IP-CAN has changed. The UE should perform IMS re-registration when the IP-CAN used by the UE changes between 3GPP access and WLAN access.

Re-registration follows the same process as defined in clause 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 1: if the UE does not re-register, any active sessions may be deactivated.

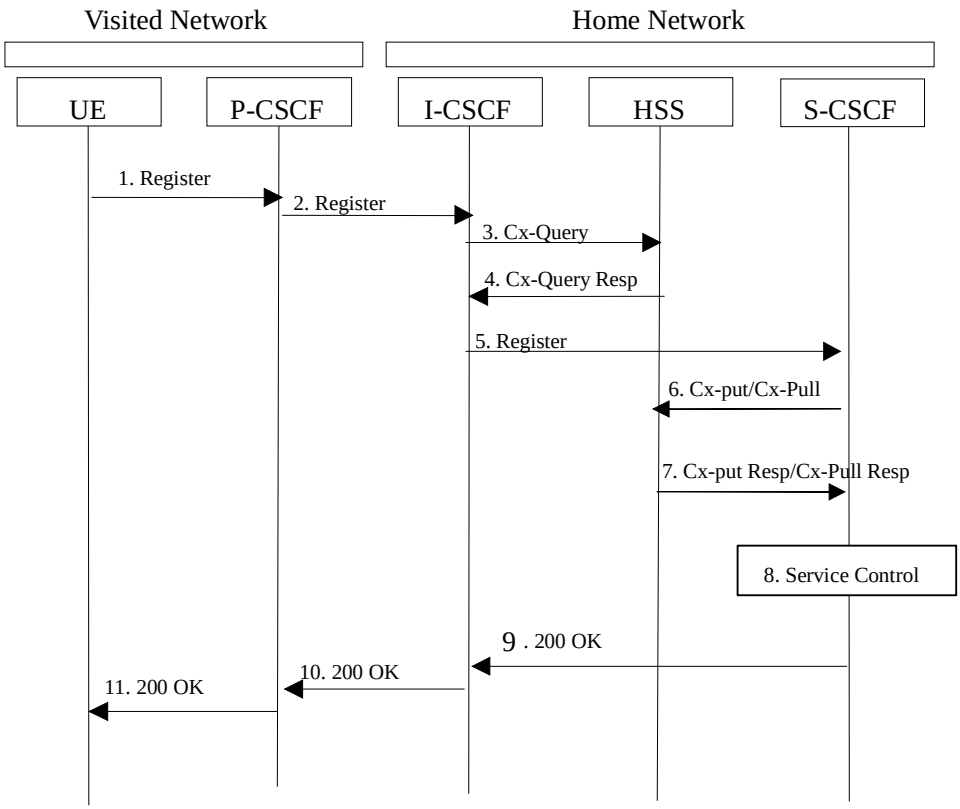


Figure 5.2: Re-registration - user currently registered

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

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).

NOTE 2: The P-CSCF may force the UE to attempt initial registration with another P-CSCF, instead of forwarding its re-registration request. This is useful e.g. to move users from a P-CSCF to another P-CSCF without interrupting the service to these users.

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. 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 to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiation signalling to the home network.

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

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

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

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

NOTE 3: The service control environment can be notified of the current IP-CAN type serving the UE via this procedure.

9. The S-CSCF shall return the 200 OK information flow (home network contact information, a GRUU set) to the I-CSCF.

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

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

    If the S-CSCF receives the priority information of the MPS subscribed-UE as a part of user profile from the HSS, the S-CSCF provides the priority information to the P-CSCF and the P-CSCF stores this information for the MPS-subscribed UE.

5.2.2.5 Stored information.

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

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

Node	Before Registration	During Registration	After Registration
UE - in local network	Credentials Home Domain Proxy Name/Address	Same as before registration	Credentials Home Domain Proxy Name/Address UE P-GRUU At least one T-GRUU
Proxy-CSCF - in Home or Visited network	Routing Function	Initial Network Entry point UE Address Public and Private User IDs Access Network Type	Final Network Entry point UE Address Public and Private User IDs Access Network Type
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 UE P-GRUU UE T-GRUU	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 clause 5.2.2.3 "Registration Information Flow – User not registered".

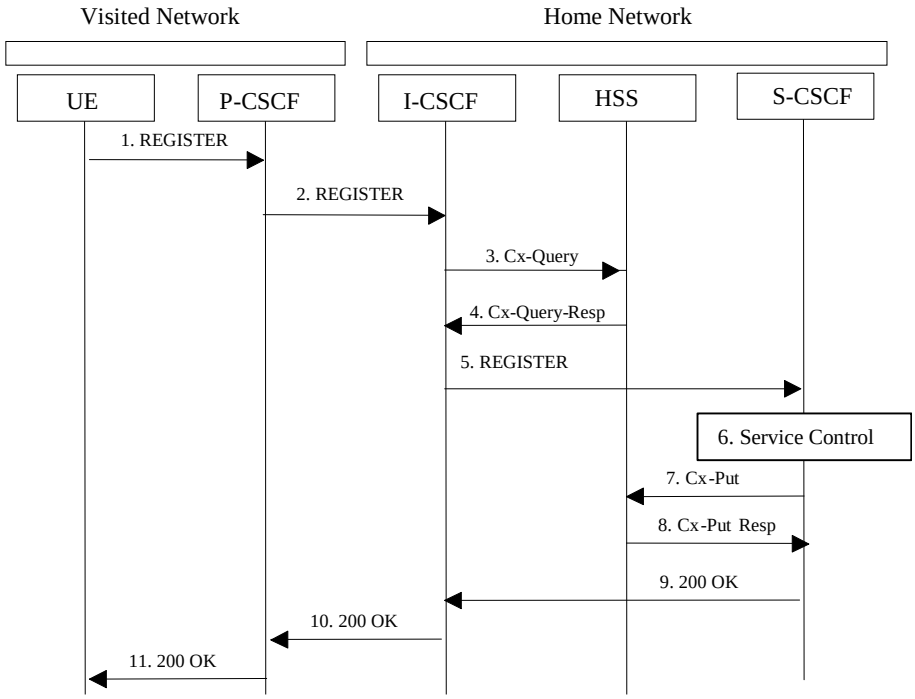


Figure 5.3: De-registration - user currently registered

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 Identity is currently registered. The Cx-Query Resp (indication of entry point, e.g. S-CSCF) is sent from the HSS to the I-CSCF.

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism and then shall send the de-register information flow (P-CSCF address/name, Public User Identity, Private User Identity, UE IP address) 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. If the user has (originating – see 5.6.5, or terminating – see 5.12) services related to unregistered state, the S-CSCF sends Cx-Put (Public User Identity, Private User Identity, keep S-CSCF name) in order to keep the S-CSCF name in the HSS for these services.

The HSS then either clears or keeps the S-CSCF name for that Public User Identity according to the Cx-Put request. If the S-CSCF name is kept, then the HSS shall be able to clear the serving S-CSCF name at any time.

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

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

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

11. The P-CSCF shall send information flow 200 OK to the UE. The P-CSCF releases all registration information regarding this specific registration of the Public User Identity after sending information flow 200 OK. If the P-CSCF has an active subscription to notifications of the status of the IMS Signalling connectivity, the P-CSCF shall cancel the subscription (see TS 23.203 [54] and TS 23.503 [95] for more details).

5.3.2 Network initiated de-registration

5.3.2.0 General

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

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

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

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

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

- Subscription Management
  The operator must be able to restrict user access to the IM CN subsystem upon detection of contract expiration, removal of IM subscription, fraud detection, etc. In the 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 clauses provide scenarios showing SIP application de-registration. Note that these flows have avoided the strict use of specific SIP protocol message names. This is in an attempt to focus on the architectural aspects rather than the protocol.

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

- To deal with registrations expirations.

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

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

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

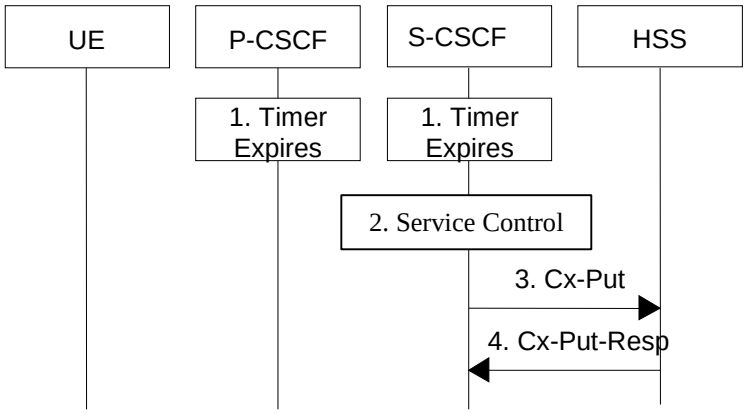


Figure 5.4: Network initiated application de-registration, registration timeout

1. The registration timers in the P-CSCF and in the S-CSCF expire. The timers are assumed to be close enough that no external synchronisation is required. The P-CSCF updates its internal databases to remove the Public User Identity from being registered. It is assumed that any cleanup of IP-Connectivity Access Network resources will be handled by independent means. If the P-CSCF has an active subscription to notifications of the status of the IMS Signalling connectivity, the P-CSCF shall cancel the subscription (see TS 23.203 [54] and TS 23.503 [95] for more details).

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. If the user has (originating – see 5.6.5, or terminating – see 5.12) services related to unregistered state, the S-CSCF sends Cx-Put (Public User Identity, Private User Identity, keep S-CSCF name) in order to keep the S-CSCF name in the HSS for these services.

   The HSS then either clears or keeps S-CSCF name for that Public User Identity according to Cx-Put the request. If the S-CSCF name is kept, then the HSS shall be able to clear the serving S-CSCF name at any time.

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

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

5.3.2.2.0 General

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

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

The following flow shows a network initiated IM CN subsystem terminal application (SIP) de-registration based on an administrative action for example. The IP transport infrastructure is not notified. If complete packet access is to be denied, a transport layer administrative mechanism would be used. This scenario does not address the administrative

mechanisms used for updating any subscriber records, EIR records, access authorization, 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 clause 5.10.3.

5.3.2.2.1 Network Initiated De-registration by HSS, administrative

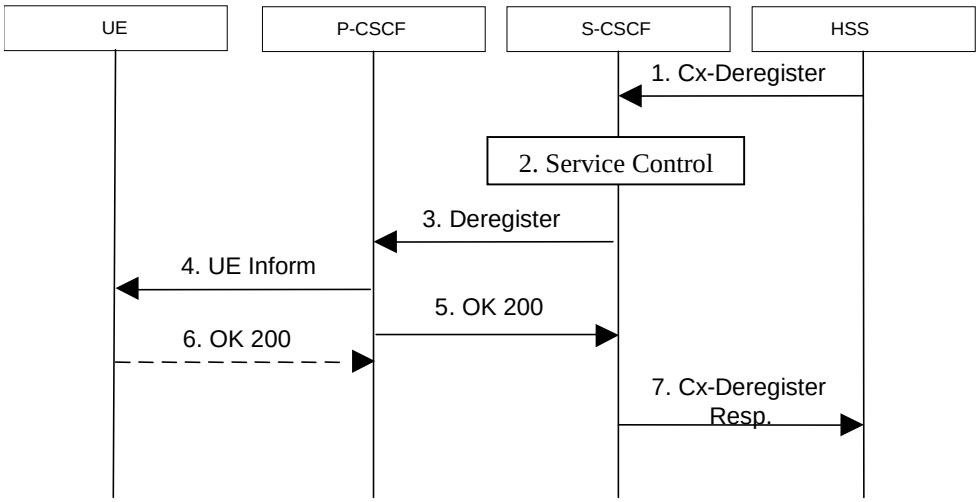


Figure 5.5: Network initiated application de-registration by HSS, administrative

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. If the P-CSCF has an active subscription to notifications of the status of the IMS Signalling connectivity, the P-CSCF shall cancel the subscription (see TS 23.203 [54] for more details).

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 1: 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 2: Another trusted/secured party may also request for de-registration via HSS through administrative mechanisms provided by the operator.

5.3.2.2.2 Network Initiated De-registration by Service Platform

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.

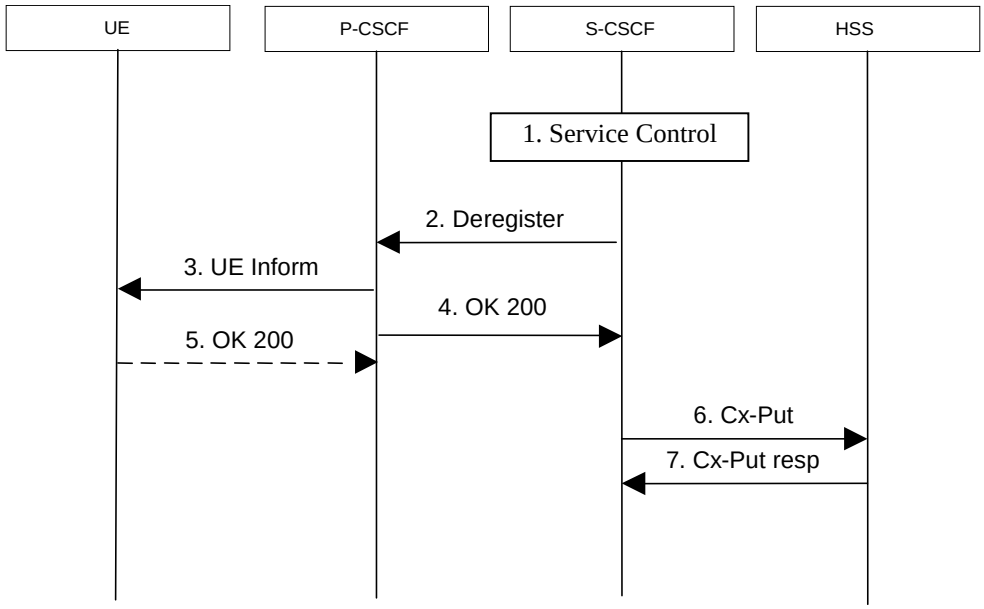


Figure 5.5a: Network initiated application de-registration, service platform

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. If the P-CSCF has an active subscription to notifications of the status of the IMS Signalling connectivity, the P-CSCF shall cancel the subscription (see TS 23.203 [54] for more details).

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 1: 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. Based on operator choice the S-CSCF can send either Cx-Put (Public User Identity, Private User Identity, clear S-CSCF name) or Cx-Put (Public User Identity, Private User Identity, keep S-CSCF name). In both cases the Public User Identity is no longer considered registered in the S-CSCF. If the user has (originating - see 5.6.5, or terminating - see 5.12) services related to unregistered state, the S-CSCF may send Cx-Put (Public User Identity, Private User Identity, keep S-CSCF name) in order to keep the S-CSCF name in the HSS for these services.

   The HSS then either clears or keeps S-CSCF name for that Public User Identity according to Cx-Put the request.

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

NOTE 2: Another trusted/secured party may also initiate the de-registration, for example, by issuing a third party SIP registration with timer set to 0 via S-CSCF.

5.4 Procedures for IP multi-media sessions

5.4.0 General

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

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

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

5.4.1 Bearer interworking concepts

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

Default codecs to be supported within the UE are IP-CAN dependent and hence are defined in the respective IP-CAN specific documents. 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 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 IMS supports endpoints (e.g., UE, MRFP, MGCF for interworking with the PSTN) able to send or receive DTMF tone indications using the bearer, i.e. inband signalling. An additional element for bearer interworking is the interworking of these DTMF tones and out-of-band signalling between one network and another. In such a case, the MGW shall provide tone generation and may provide detection 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.

It is possible that the external SIP client does not support one or more of the SIP extensions required for IMS end points to set up IMS sessions (e.g. Preconditions, Update, 100Rel) as described in TS 24.229 [10a], then the UE or other SIP user agents within the IMS should be able to fall back to SIP procedures which allow interworking towards the external client. Depending on the home network operator policy, the network may restrict session initiation requests towards and from external SIP clients without the support of SIP extensions defined for IMS sessions.

5.4.2a IP version interworking

Following interworking scenarios exist:

Application Level Interworking

It should be possible for users connected to an IMS network to communicate with users that are connected to SIP based networks that use a different IP version via interworking or that are in a separate addressing range (e.g. NA(P)T

functionality is set at the border of the IMS). Annex I describes in more detail how such interworking is performed for IMS.

Transport Level Interworking

Inter-working also includes tunnelling level interconnection of IMS networks via transit networks that use a different IP version using for example, configured tunnels as described in TS 23.221 [7]. Figure 5.5b below shows an example configuration scenario where two IPv6 IMS networks are connected via an IPv4 network.

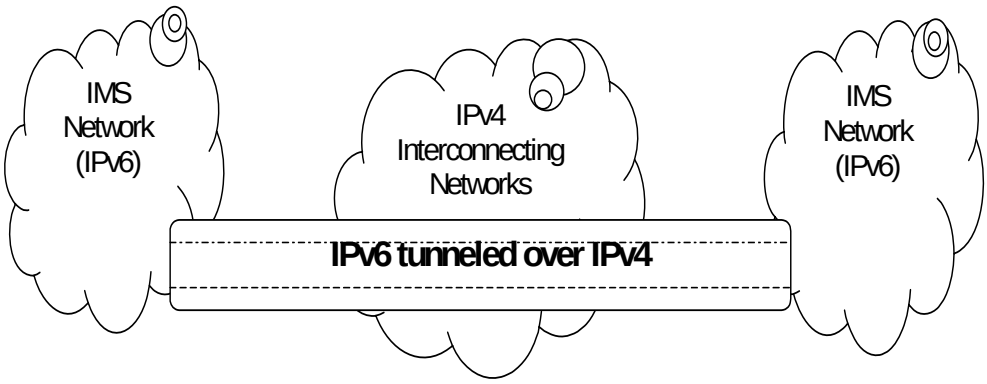


Figure 5.5b: Example tunnelling of IPv6 traffic over IPv4 networks

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.

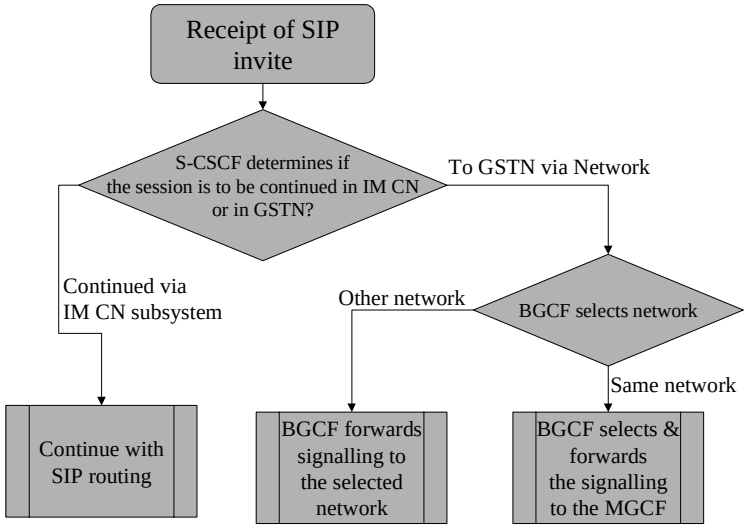


Figure 5.6: Network based PSTN interworking breakout process

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 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 service of both originating and terminating side. This implies that it should be easy to correlate CDR held by the IP-Connectivity Access Network service 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 service. This does not mean that CSCF is the enforcement point (which actually is the Gateway between the IP-Connectivity Access Network and the IP multimedia network) 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 IP-Connectivity Access Network service shall be able to notify the IP multimedia session control when the IP-Connectivity Access Network service has either modified or suspended or released the bearer(s) of a 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.

5.4.5 Session Path Information

5.4.5.1 Session Path Information during Registration and Session Initiation

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

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

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

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

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

5.4.5.2 P-CSCF in the Session Path

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

5.4.5.3 S-CSCF in the Session Path

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

See also Annex F for background information.

5.4.6 End-user preferences and terminal capabilities

5.4.6.0 General

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

5.4.6.1 Objectives

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

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

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

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

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

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

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 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, and the Policy Decision Functions have been omitted from the diagram.

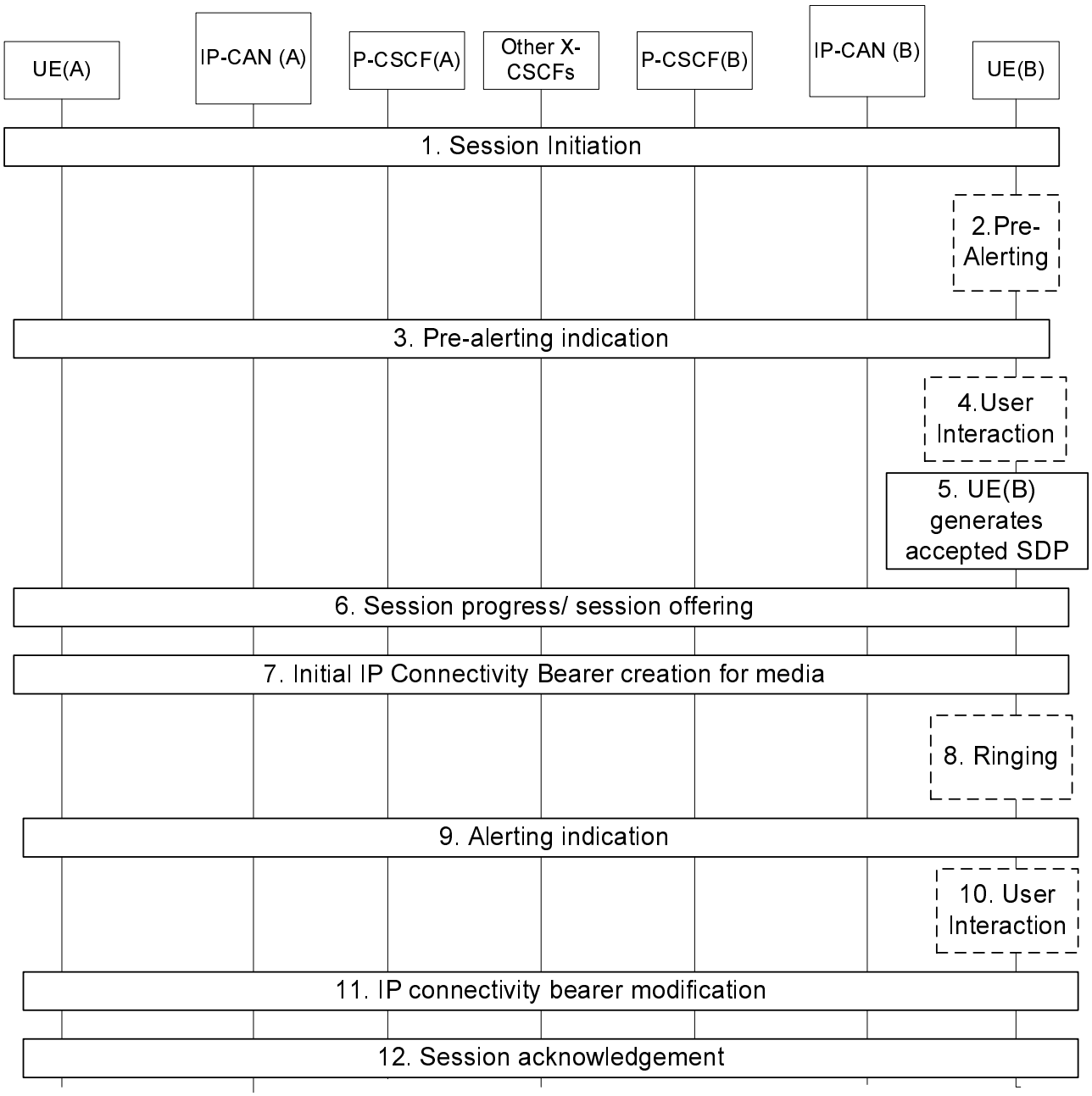


Figure 5.7: Bearer establishment showing optional pre-alerting

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. Initial bearer creation procedure is performed. During this bearer creation step the resources in the UE(A)'s and UE(B)'s IP-CANs are reserved. 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 IP-CANs of UE(A) and UE(B) may be modified, 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

5.4.7.0 General

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

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

When using IP-CAN with Policy and Charging Control, PCC decisions (e.g., authorization and control) are also applied to the IP-CAN bearer.

The description in this clause and the following clauses (clauses 5.4.7.1 - 5.4.7.7) is applicable for the case when Policy and Charging Control is employed.

The IP-Connectivity Access Network contains a Policy and Charging Enforcement Function (PCEF, in 5GS corresponding to the combination of SMF and UPF) that has the capability of policing packet flow into the IP network, and restricting the set of IP destinations that may be reached from/through an IP-CAN bearer according to a packet classifier.

NOTE: How PCEF is distributed in SMF and UPF in 5GS is specified in TS 23.501 [93] and TS 23.203 [54].

This 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 PCRF/PCF (the interface between the PCRF/PCF and the P-CSCF is the Rx interface standardised in TS 23.203 [54] or the N5 interface (using the Npcf_PolicyAutorization service), standardised in TS 23.503 [95] and TS 29.514 [96]).

There are eight interactions defined for Policy and Charging Control:

1. Authorize QoS Resources.
2. Resource Reservation.
3. Enabling of media flows authorized in (1), e.g. 'open' the 'gate'.
4. Disabling of media flows authorized in (1), e.g. 'close' the 'gate'.
5. Revoke Authorization for IP-CAN and IP resources.
6. Indication of IP-CAN bearer release from the PCEF in the IP-Connectivity Access Network to the PCRF/PCF.

7. Authorization of IP-CAN bearer modification.

8. Indication of IP-CAN bearer modification from the PCEF in the IP-Connectivity Access Network to the PCRF/PCF.

These requirements and functional description of these interactions are explained further in the following clauses. The complete specification of the interface between the PCRF/PCF and the PCEF is contained in TS 23.203 [54] and TS 23.503 [95].

The Policy and Charging Control can also be used to enable the P-CSCF to retrieve the user location and/or UE Time Zone information from the access network as specified in TS 23.203 [54] and TS 23.503 [95].

5.4.7.1 Authorize QoS Resources

The Authorize QoS Resources procedure is used during an establishment and a modification of a SIP session. The P-CSCF shall use the SDP contained in the SIP signalling to derive the session information that is relevant for Policy and Charging Control and forwards it to the PCRF/PCF. The PCRF/PCF shall use the received information to calculate the proper authorization. This enables the PCRF/PCF to authorize the required QoS resources.

NOTE: Although session information is incomplete in the terminating side P-CSCF at the reception of the SDP offer, it can be sent to PCRF/PCF whenever the SDP offer (contained in the session establishment request or session modification request) indicates no requirements for resource reservation or that the required resources are already available on the originating side, as in such cases no SDP answer is received before the PCRF/PCF is requested to authorize the required QoS resources.

The authorization shall be expressed in terms of the IP resources to be authorized and shall include limits on media flows, and may include restrictions on IP destination address and port. The PCC shall authorize each SIP session independently (including additional parallel sessions, e.g. Call Waiting) and shall take into consideration the amount of IP resources the user's subscription allows.

5.4.7.1a Resource Reservation with Policy and Charging Control

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

Authorization of IP-CAN and IP QoS Resources shall be required for access to the IP Multimedia Subsystem. The IP-CAN shall determine the need for authorization, possibly based on provisioning and/or based on requested parameters, which may be IP-CAN specific.

Resource Reservation is initiated either by the UE or the IP-CAN depending on the bearer establishment mode selected for the IP-CAN session, see TS 23.203 [54] and TS 23.503 [95]:

- Resource reservation requests initiated from the UE shall (if possible for the used IP-CAN) contain the traffic mapping information which enables the IP-CAN to correctly match the reservation request to the corresponding authorization. The authorization is normally 'Pulled' from the PCRF/PCF by the PCEF within the IP-CAN when the reservation request is received from the UE.

NOTE: When a UE combines multiple media flows onto a single IP-CAN bearer, all the traffic mapping information related to those media flows are provided in the resource reservation request.

With a request for IP-CAN QoS resources, the PCEF within the IP-CAN shall verify the request is less than the sum of the authorized IP resources (within the error tolerance of the conversion mechanism) for all of the combined media flows.

- Resource reservation requests initiated by the IP-CAN take place after successful authorization of QoS resources. The PCRF/PCF "Pushes" the authorization for IP-CAN bearer resources to the PCEF within the IP-CAN, which then enforces the authorization by either modifying the characteristics of one existing IP-CAN bearer or requesting the establishment of a new one.

- Resource reservation requests initiated by the IP-CAN shall (if possible for the used IP-CAN) contain the traffic mapping information which enables the UE to correctly match the reservation request to the corresponding media of the SIP session.

5.4.7.2 Enabling of Media Flows

The PCRF/PCF makes policy decisions and provides an indication to the PCEF within the IP-CAN that the user is now allowed to use the allocated QoS resources for per-session authorizations unless this was done based on Policy and Charging Control 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 PCRF/PCF may authorize the "logical OR" of the resources requested in the responses. When the session established indication has been received, if the PCRF/PCF earlier have authorized the "logical OR" of the resources then the PCRF/PCF will modify the authorization and enable the corresponding media flows according to the session established indication.

The PCEF within the IP-CAN enforces the policy decisions. The IP-CAN shall restrict any use of the IP resources prior to this indication from the PCRF/PCF, e.g. by keeping the gate closed and disabling the use of resources for the media flow. Based on local policy, IP-CAN and/or IP resources may be allowed to be used by the user at the time they are authorized by the PCRF/PCF.

5.4.7.3 Disabling of Media Flows

The PCRF/PCF makes policy decisions and provides an indication to the PCEF within the IP-CAN about revoking the user's capacity to use the allocated QoS resources for per-session authorizations. The indication for disabling media flows shall be sent as a separate decision to the PCEF within the IP-CAN corresponding to the previous request to enable media flows.

The PCEF within the IP-CAN enforces the policy decisions. The IP-CAN shall restrict any use of the IP resources after this indication from the PCRF/PCF, e.g. by closing the gate and blocking the media flow.

5.4.7.4 Revoke Authorization for IP-Connectivity Access Network and IP Resources

At IP multimedia session release, the UE should deactivate the IP-CAN bearer(s) used for the IP multimedia session. In various cases the UE will be unable to perform this release itself. The PCRF/PCF provides indication to the PCEF within the IP-CAN when the resources previous authorized, and possibly allocated by the UE, are to be released. The IP-CAN shall deactivate the IP-CAN bearer used for the IP multimedia session.

5.4.7.5 Indication of IP-Connectivity Access Network bearer release

Any release of IP-CAN bearer(s) that were established based on authorization from the PCRF/PCF shall be reported to the PCRF/PCF by the PCEF within the IP-CAN.

This indication is forwarded to the P-CSCF and may be used by the P-CSCF to initiate a session release towards the remote endpoint e.g. if all IP-CAN bearer(s) associated with the session were released, the procedures in clause 5.10.3.1 can be executed.

NOTE: If only a subset of IP-CAN bearer(s) were released, then the UE can update the ongoing session with the remainder of allowed media flows or a subset of allowed media flows.

5.4.7.6 Authorization of IP-Connectivity Access Network bearer modification

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

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

When the P-CSCF sends an update of the session information and the bearer establishment is controlled by the IP-CAN, the PCRF/PCF shall send an updated authorization to the PCEF. The PCEF within the IP-CAN enforces the policy decision accordingly (e.g. by requesting the reservation of new IP-CAN bearer resources in the case of the addition of a new media component to the session or release of previously reserved resources if a media component has been removed from the IP Multimedia session).

5.4.7.7 Indication of IP-Connectivity Access Network bearer modification

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

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

5.4.7.8 Sharing of Resources for Network Detected Concurrent Sessions

5.4.7.8.1 Network Detected Concurrent Sessions

The following scenarios for concurrent sessions are subject to resource sharing:

- The UE is engaged in a session, puts the session on hold, then initiates a new session to a new UE.
- The UE is engaged in a session and receives an incoming session, puts the ongoing session on hold to accept the incoming session.
- The UE is engaged in multiple sessions, puts all sessions on hold and creates a conferencing session.

For a UE engaged in multiple sessions, with only one active session at any time, the network may be able to share resources for media components of the same type and that are common to these multiple sessions.

Resource sharing shall only be indicated for concurrent sessions that employ resource reservation based on TS 23.203 [54] or TS 23.503 [95].

When a UE puts a session on hold, it may put all or a subset of the media components of the session on hold. In such a case, the resource sharing applies only to the media components that are on hold and not to the rest of media components belonging to this IMS session

An emergency session shall not share resources with any other session.

NOTE: Resource sharing to be shared for any media component can be allowed for one direction as well as both directions. According to TS 24.229 [10a] and TS 24.610 [91] it is not prohibited that a UE may send media towards a held UE, i.e. uplink media can occur even when a UE puts a remote UE on hold. The P-CSCF or SIP AS can therefore be locally configured to allow resource sharing in both directions if the P-CSCF or SIP AS knows that the UE will not send media to a remote UE on hold.

5.4.7.8.2 Initiating Resource Sharing for Network Detected Concurrent Sessions

If the P-CSCF is configured to apply resource sharing, it may at establishment of a new Rx session or a new Npcf_PolicyAutorization application session context with the PCRF/PCF, indicate that resources may be shared in uplink and/or downlink direction by assigning an uplink and/or downlink tag to each media component of an IMS session unless it is an IMS emergency session.

NOTE: The assignment of tags to media components is regardless of any future sharing decision.

If this is the first IMS session of a UE, the P-CSCF shall assign new tags. Upon detection by the P-CSCF that a UE is engaged in multiple sessions, it shall determine if these sessions fulfil the criteria specified in clause 5.4.7.8.1 and have common media components that can share resources. If so, the P-CSCF may activate resource sharing by assigning the same existing tag to each media component whose resources can be shared amongst the IMS sessions. Otherwise, the P-CSCF shall assign new tags that are different from any tag previously assigned for this UE. The PCRF/PCF may then authorize resource sharing based on these tags. For further information, see TS 23.203 [54].

Whenever resource sharing is active, the P-CSCF shall ensure that the UE can only receive the media flow for one session at a time by closing the gates for all other media flows that can share the same resource, i.e. having the same tag.

SIP AS may indicate to a supporting P-CSCF to apply resource sharing to each media lines included in SDP of an IMS session. When SIP AS is used, P-CSCF, based on the local policy, may follow the resource sharing policy from SIP AS. The interaction between P-CSCF and SIP AS for handling Resource sharing procedure is defined in TS 24.229 [10a].

5.4.7.8.3 Void

5.4.7.9 Priority sharing for concurrent sessions

The P-CSCF may indicate to the PCRF/PCF that the resource allocation for a media flow is allowed to use the same priority as other media flows of the same media type for the UE engaged in multiple sessions by providing a priority sharing indicator and an optional pre-emption control information in addition to the application identifier and the service priority. For MCPTT, the service priority and the priority sharing indicator are defined in TS 23.179 [92]. The pre-emption control information is used to indicate to the PCRF/PCF how to perform pre-emption in accordance to TS 23.203 [54] and TS 23.503 [95].

The following scenario is subject to priority sharing:

-- The P-CSCF receives a priority sharing indicator associated with the media flow from the Application Server.

Upon detection by the P-CSCF that a session includes a priority sharing indicator for a media flow and may optionally include pre-emption control information, the P-CSCF shall convey to the PCRF/PCF the priority sharing indicator and, when available, the pre-emption control information as described in TS 23.203 [54] and TS 23.503 [95].

NOTE 1: The Application Server is not supposed to include the priority sharing indicator for an emergency session.

NOTE 2: The priority sharing enables the usage of one bearer per QCI/5QI for a UE having multiple sessions; otherwise sessions with different service priorities would end up in different bearers.

5.4.8 QoS-Assured Preconditions

This clause 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.

The set-up of a "QoS-Assured" session will not complete until required resources have been allocated to the session. In a QoS-Assured session, the QoS bearer for the media stream shall be successfully established according to the QoS preconditions defined at the session level before the UE 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 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 if 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.

NOTE 1: To avoid unwanted session setup delay and IP-CAN signalling load, QoS-Assured sessions needs to be used with care and it is decided per application which media that require resource reservation.

The following cases exist in the context of using "QoS-Assured" preconditions for IMS:

a. The IMS session requires the reservation of additional bearer resources, and the UE requires confirmation from the other endpoint of the fulfilment of the pre-conditions related to this resource reservation. An endpoint may not require the reservation of bearer resources, and may therefore immediately indicate the local fulfilment of the pre-conditions. One example of such SIP endpoint is the MGCF used for PSTN interworking. In these cases, one or both of the reservation confirmation messages may not be sent.

b. The IMS session does not require the reservation of additional bearer resources, and both endpoints indicate in their initial session setup message that the pre-conditions are fulfilled.

c. The IMS session does not require the reservation of additional bearer resources, and the endpoints do not use the mechanism to indicate "QoS-Assured" pre-conditions.

NOTE 2: The flows of clauses 5.5, 5.6 and 5.7 depict the case where both UEs require confirmation from each other of the fulfilment of the pre-conditions. The flow in clause 5.7a depicts the case where the IMS session does not require the reservation of additional bearer resources and the endpoints do not use pre-conditions.

5.4.9 Event and information distribution

5.4.9.0 General

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

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

This mechanism considers the following issues:

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

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

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

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

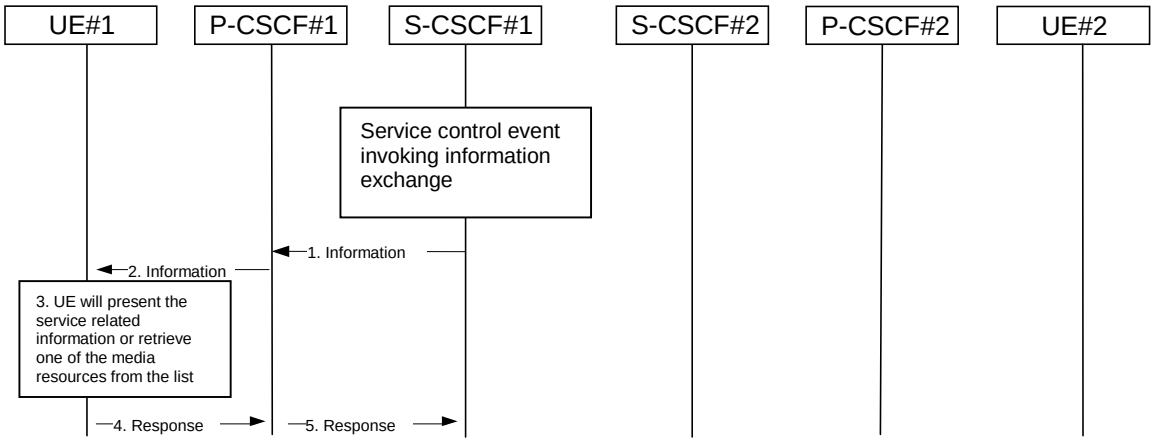


Figure 5.8: Providing service event related information to related endpoint

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

2. P-CSCF forwards the message request.

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

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

5. P-CSCF forwards the response.

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

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

5.4.9.1 Subscription to event notifications

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

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

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

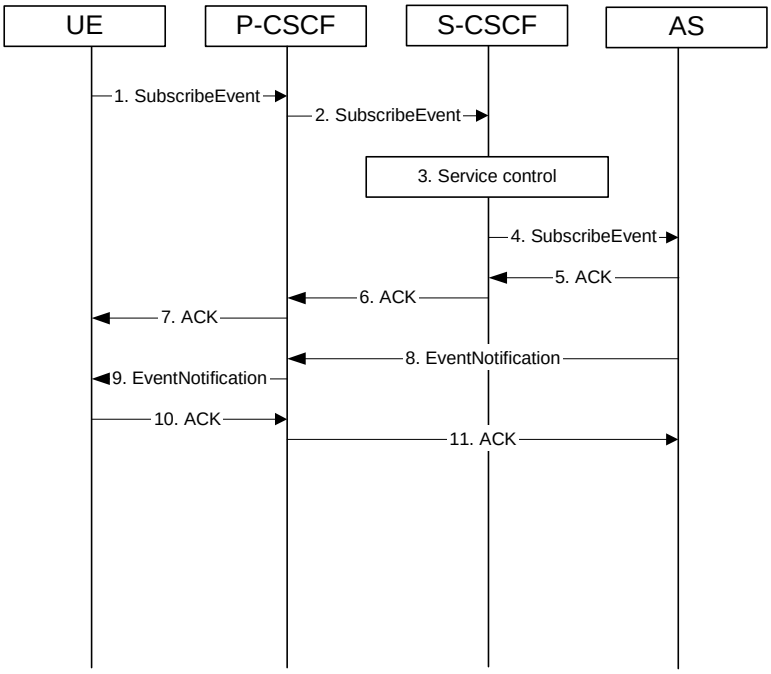


Figure 5.8a: Subscription to event in AS

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

5.4.10 Void

5.4.11 Signalling Transport Interworking

A Signalling gateway function (S-GW) 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 (see TS 23.002 [1]). The session flows in this specification do not show the S-GW, but when interworking with PSTN/CS domain, it is assumed that there is a S-GW for signalling transport conversion.

5.4.12 Configuration and Routing principles for Public Service Identities

5.4.12.0 General

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

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

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

5.4.12.1 PSIs on the originating side

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

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

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

5.4.12.2 PSIs on the terminating side

The Application Server hosting the PSI may be invoked as a terminating Application Server via information stored in the HSS. Such PSIs are globally routable and can be made available to users within and outside the operator domain, and can take the following form:

- Distinct PSIs are defined in TS 23.003 [24]. Distinct PSIs can be created, modified and deleted in the HSS by the operator via O&M mechanisms. Distinct PSIs can also be created and deleted by users using the Ut interface using the means described in clause 5.4.12.3 for subdomain-based PSIs.

- The distinct PSI may be activated in the HSS by the AS using the Sh interface.

- Wildcarded PSIs are defined in TS 23.003 [24]. Wildcarded PSI ranges can be created, modified and deleted in the HSS by the operator via O&M mechanisms. Specific PSIs within a wildcarded range can be created and deleted by users using the Ut interface to the AS hosting the wildcarded range, or by the operator via O&M mechanisms.

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

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

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

The AS hosting the PSI in combination with its entry in the HSS is referred to as "PSI user".

Figure 5. 19d depicts a routing example for incoming session where the session request is routed directly to the AS hosting the PSI.

Figure 5.19e depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.

5.4.12.3 Subdomain based PSIs

Subdomains defined for PSIs allow both operators and users to define specific PSIs within subdomains for specific applications. For this purpose, subdomains can be defined by the operator in the DNS infrastructure. Specific PSIs within a subdomain can be created and deleted by users using the Ut interface to the AS hosting the subdomain, or by the operator via O&M mechanisms.

Subdomain based PSIs are globally routable and can be made available to users within and outside the operator domain.

In this case, there are two ways to route towards the AS hosting the PSI:

a) When the subdomain name is defined in the global DNS, then the originating S-CSCF or a Transit Function receives the IP address of the AS hosting the PSI, when it queries DNS. The principles defined in IETF RFC 3263 [44] may be used. For example, a NAPTR query and then a SRV query may be used to get the IP address of the AS.

b) The PSI is resolved by the global DNS to an I-CSCF address in the domain where the AS hosting the PSI is located. The I-CSCF recognises the subdomain (and thus does not query the HSS). It resolves the same PSI to the address of the actual destination AS hosting the PSI using an internal DNS mechanism, and forwards the requests directly to the AS.

Figure 5.19f shows an example of DNS based routing of an incoming session from an external network. The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.

5.4.12.4 PSI configuration in the HSS

In order to support configuration of an AS hosting a PSI, the distinct PSIs and/or wildcarded PSI ranges hosted in the AS need to be configured in the HSS. The configuration shall include procedures to allow:

- Distinct PSIs and wildcarded PSI ranges to be configured in the HSS via operation and maintenance procedures,
- Authorization and verification of access as "PSI user" with the Public Service Identity hosted by the AS, e.g. for AS-originating requests,
- Access to "PSI user" information (e.g. the S-CSCF assigned) over the Cx reference point from the CSCF nodes,
- Defining the "PSI user" similar to the principle of IMS user, without requiring any subscription/access information (e.g. CS/PS domain data) that are required for IMS user.

Note that the PSI configuration in the HSS does not affect the filter criteria based access to an AS as defined in the user profiles.

5.4.12.5 Requests originated by the AS hosting the PSI

The AS hosting the PSI may originate requests with the PSI as the originating party. For such originating requests, the home IMS network shall be capable to perform the following functions:

- Network Domain Security, TS 33.210 [20], shall be used where applicable.
- Charging requirements such as providing appropriate accounting and charging functions via the charging entities shall be supported according to TS 32.240 [25].

- If the target identity is a Tel URI (as specified in IETF RFC 3966 [15]), ENUM translation needs to be performed as described in clause 4.3.5.2, and the request shall be routed based on the translation result appropriately.

Routing from the Originating AS hosting the PSI can be performed as follows:

a) If the AS supports routing capabilities (e.g. ENUM support, etc), the AS may forward the originating request to the destination network without involving a S-CSCF. If this option is applied where the target identity is a Tel URI, the AS shall perform an ENUM query and route the request based on the translation result.

b) If the AS does not support routing capabilities, the AS may forward the originating request to the IMS Transit Functions. The IMS Transit Functions will then route the session initiation request to the destination.

c) If the session requires the use of a S-CSCF: either the PSI has an S-CSCF assigned, in which case the AS forwards the originating request to this S-CSCF, which then processes the request as per regular originating S-CSCF procedures, or the PSI has no S-CSCF assigned, in which case the AS sends the session initiation request to an I-CSCF that will allocate an S-CSCF to the PSI.

To prevent fraudulent or unsecure IMS traffic possibly caused by AS originated requests, security and authentication procedures may be performed towards the AS.

5.4.13 Transcoding concepts

IMS control plane entities, including the P-CSCF, Application Servers or (for inter-domain sessions) the IBCF, may check the SDP offer/answer information associated with session requests and responses, to determine the need for transcoding. If such a need is determined to exist, media transcoding resources are reserved from the MRFP (via the MRFC), the IMS-AGW, or the TrGW.

Transcoding requires knowledge of the codecs supported by the end points and may be invoked at the originating or terminating network based on interworking agreements (e.g. local policy) or service level agreement (SLA).

For more details concerning transcoding involving MRFC/MRFP interworking see clause 5.14, Annex P and TS 23.218 [71], and for the IBCF/TrGW implementation consult clause 4.14 and Annex I, clause I.3.3.

5.4a Overview of session flow procedures

5.4a.1 End-to-End session flow procedures

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

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

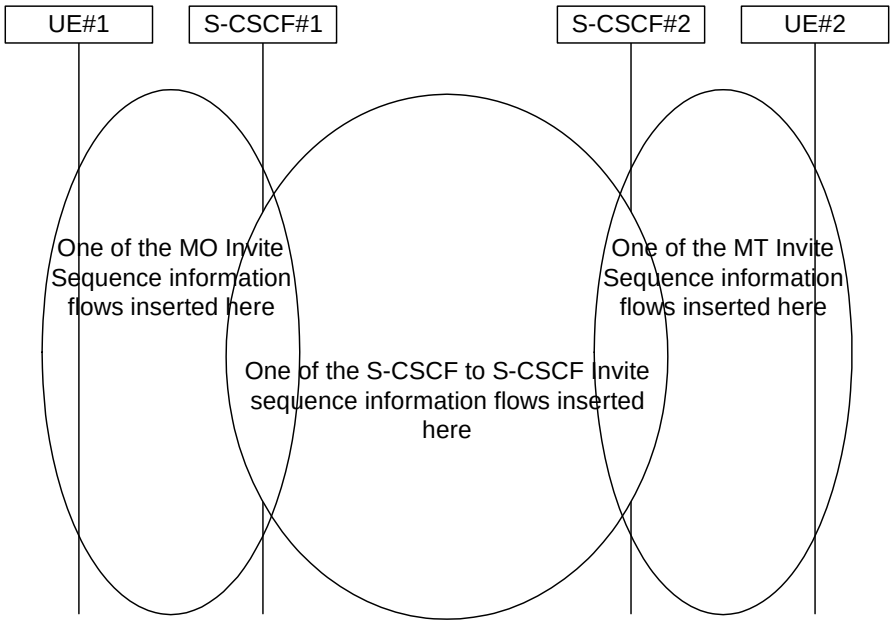


Figure 5.9: Overview of Session Flow Sections

The following procedures are defined:

For the origination sequences:

- (MO#1) Mobile origination, roaming , see clause 5.6.1;
- (MO#2) Mobile origination, home, see clause 5.6.2;
- (PSTN-O) PSTN origination, see clause 5.6.3;
- (NI-O) Non-IMS network origination (external SIP client), see clause 5.6.4;
- (AS-O) Application Server origination, see clause 5.6.5.

For the termination sequences:

- (MT#1) Mobile termination, roaming, see clause 5.7.1;
- (MT#2) Mobile termination, home, see clause 5.7.2;
- (MT#3) Mobile termination, CS Domain roaming, see clause 5.7.2a;
- (PSTN-T) PSTN termination, see clause 5.7.3;
- (NI-T) Non-IMS network termination (external SIP client), see clause 5.7.4;
- (AS-T#1) PSI based Application Server termination, direct, see clause 5.7.5;
- (AS-T#2) PSI based Application Server termination, indirect, see clause 5.7.6;
- (AS-T#3) PSI based Application Server termination, direct, using DNS, see clause 5.7.7;
- (AS-T#4) PUI based Application Server termination, indirect, see clause 5.7.8.

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

- (S-S#1) Session origination and termination are served by different network operators, see clause 5.5.1;
- (S-S#2) Session origination and termination are served by the same operator, see clause 5.5.2;
- (S-S#3) Session origination with PSTN termination in the same network as the S-CSCF, see clause 5.5.3;
- (S-S#4) Session origination with PSTN termination in a different network to the S-CSCF, see clause 5.5.4.

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

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

- (MO#2) Mobile origination, home,
- (S-S#2) Single network operator,
- (MT#2) Mobile termination, home.

There are a large number of end-to-end session flows defined by these procedures. They are built from combinations of origination, serving to serving, and termination procedures, as determined from the following table. For each row of the table, any one of the listed origination procedures can be combined with any one of the serving-serving procedures, which can be combined with any one of the termination procedures.

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.

The flows assume precondition mechanism is used, but as shown in clause 5.7a, a UE may originate a session without using preconditions.

Table 5.2: Combinations of session procedures

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

5.4a.2 Transit network session flow procedures

In addition to the combinations of flows constructed from the above scenarios, elements of an IMS network may be used by an operator in support of transit network scenarios. Figure 5.9a shows session flow combinations for transit network scenarios.

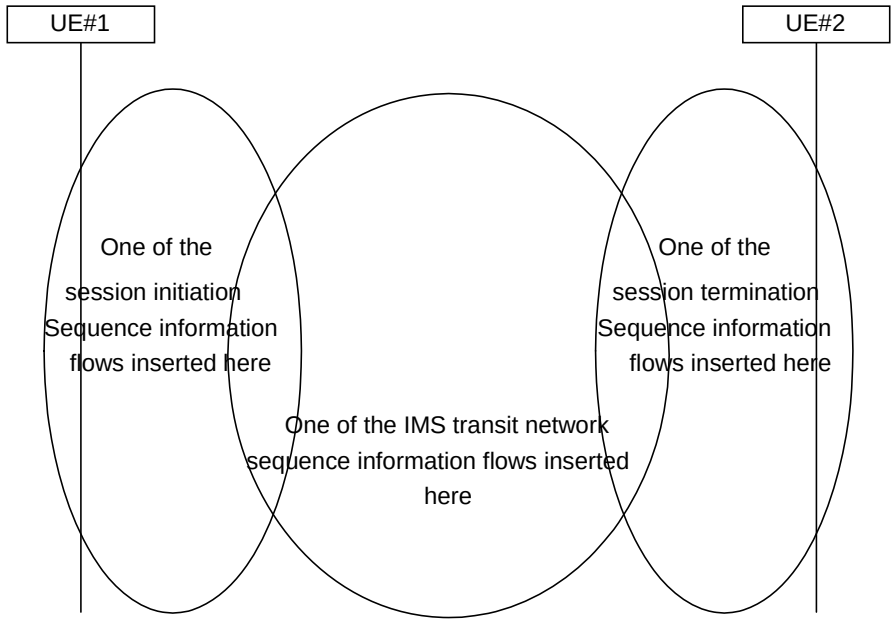


Figure 5.9a: Overview of Session Flow Sections for transit scenarios

Table 5.2a: Combinations of IMS transit network procedures

Origination Procedure (pick one)	IMS Transit Network Procedure	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. NI-O Non-IMS network origination	I-T IMS Transit Network	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. PSTN-T PSTN termination. NI-T Non-IMS network termination

The following procedures are defined:

For the origination sequences:

- (MO#1) Mobile origination, roaming , see clause 5.6.1;
- (MO#2) Mobile origination, home, see clause 5.6.2;
- (PSTN-O) PSTN origination, see clause 5.6.3;
- (NI-O) Non-IMS network origination (external SIP client), see clause 5.6.4;

For the termination sequences:

- (MT#1) Mobile termination, roaming, see clause 5.7.1;
- (MT#2) Mobile termination, home, see clause 5.7.2;
- (MT#3) Mobile termination, CS Domain roaming, see clause 5.7.2a;
- (PSTN-T) PSTN termination, see clause 5.7.3;
- (NI-T) Non-IMS network termination (external SIP client), see clause 5.7.4;

For the IMS transit network aspects see clause 5.19.

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

5.5.0 General

This clause presents the detailed application level flows to define the procedures for Serving-CSCF/MGCF to Serving-CSCF/MGCF.

In the IM CN subsystem the MGCF is considered as a SIP endpoint. It translates ISUP/BICC messages of the PSTN side to SIP signalling of the IM CN subsystem side and vice-versa. It should also be noted that the MGCF does not invoke Service Control.

This clause 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) 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 to a well-known entry point in the destination operator's network, the I-CSCF. The I-CSCF queries the HSS for current location information, and finds the user either located in the home service area, or roaming. The I-CSCF therefore forwards the request to the S-CSCF serving the destination user.

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

MO#1	Mobile origination, roaming. The "Originating Network" of S-S#1 is therefore a visited network.
MO#2	Mobile origination, home. The "Originating Network" of S-S#1 is therefore the home network.
PSTN-O	PSTN origination. The "Originating Network" of S-S#1 is the PSTN network. The elements of figure 5.16 replace all elements of the Originating network and Originating Home Network in figure 5.10.
AS-O	Application Server origination. The" Originating Network" of S-S#1 is the home network. The element labelled S-CSCF#1 corresponds to the S-SCSF in figure 5.16b.
NI-O	Non-IMS network origination. The external SIP client of figure 5. 16b replaces all elements of the Originating network and Originating Home Network in figure 5.10. There may be other non-IMS SIP servers on the path that are not shown.

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

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

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

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

NI-T Non-IMS network terminations. The external SIP client of figure5.19a replaces all elements of the Terminating Home Network and Terminating Network in figure 5.10. There may be other non-IMS SIP servers on the path that are not shown.

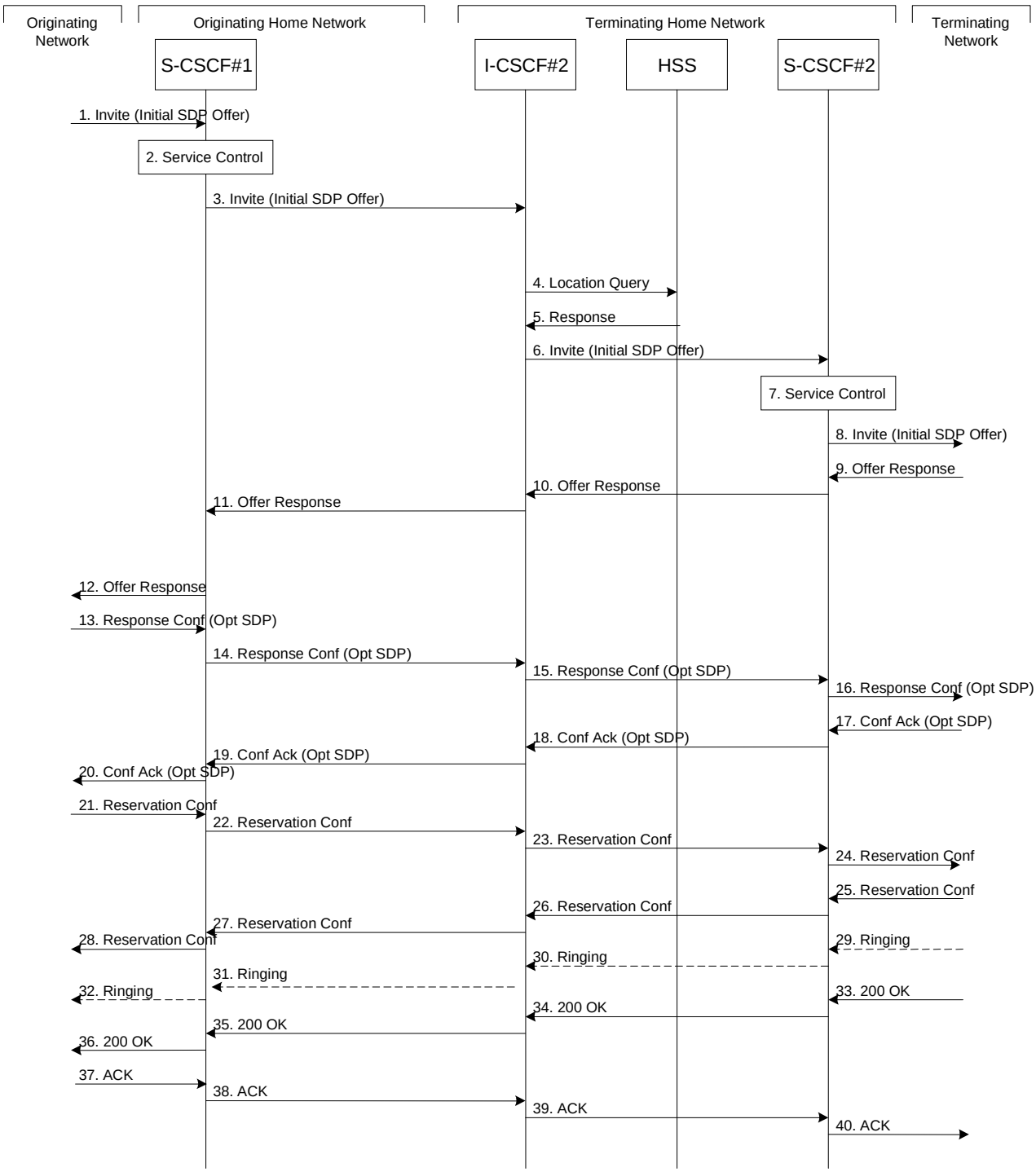


Figure 5.10: Serving to serving procedure - different operators

Procedure S-S#1 is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow. This message should contain the initial media description offer in the SDP.
2. S-CSCF#1 invokes whatever service logic is appropriate for this session attempt.
3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. For S-S#1, this flow is an inter-operator message to the I-CSCF entry point for the terminating user. S-CSCF#1 forwards the INVITE request directly to I-CSCF#2, the well-known entry point into the terminating user's network
4. I-CSCF#2 (at the border of the terminating user's network) shall query the HSS for current location information.
5. HSS responds with the address of the current Serving-CSCF for the terminating user.
6. I-CSCF#2 forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.
7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt
8. The sequence continues with the message flows determined by the termination procedure.
9. The media stream capabilities of the destination are returned along the signalling path, as per the termination procedure.
10. S-CSCF#2 forwards the SDP to I-CSCF#2
11. I-CSCF#2 forwards the SDP to S-CSCF#1.
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.

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.

21-24. Originating end point acknowledges successful resource reservation and the message is forwarded to the terminating end point.

25-28. Terminating end point acknowledges the response and this message is sent to the originating end point through the established session path.

29-32. Terminating end point then generates ringing and this message is sent to the originating end point through the established session path.

33-36. Terminating end point then sends 200 OK via the established session path to the originating end point.

37-40. Originating end point acknowledges the establishment of the session and sends to the terminating end point via the established session path.

5.5.2 (S-S#2) Single network operator performing origination and termination

The Serving-CSCF handling session origination performs an analysis of the destination address, and determines that it belongs to a subscriber of the same operator. The request is therefore forwarded to a local I-CSCF. The I-CSCF queries the HSS for current location information, and finds the user either located in the home service area, or roaming. The I-CSCF therefore forwards the request to the S-CSCF serving the destination user.

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

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

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

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

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

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

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

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

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

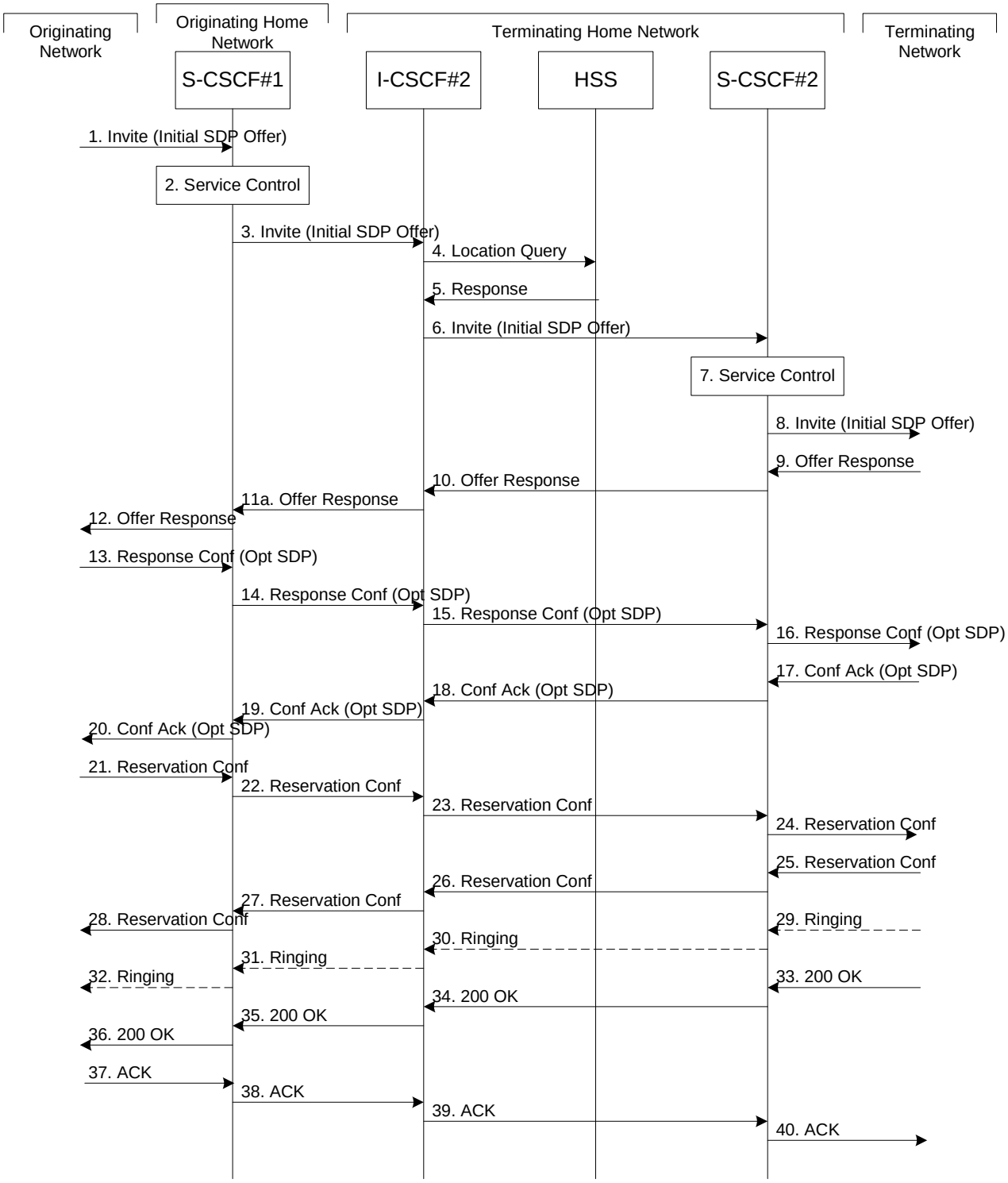


Figure 5.11: Serving to serving procedure - same operator

Procedure S-S#2 is as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

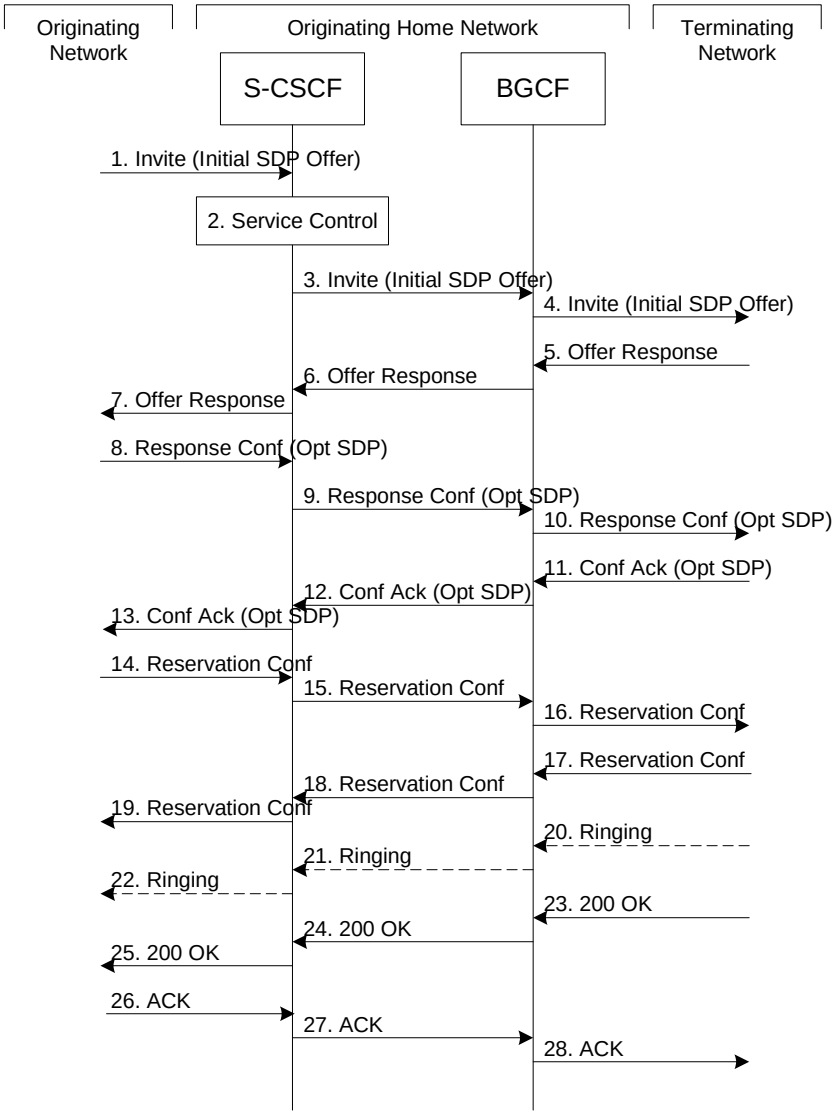


Figure 5.12: Serving to PSTN procedure - same operator

Procedure S-S#3 is as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MO#1	Mobile origination, roaming. The "Originating Network" of S-S#4 is therefore a visited network.
MO#2	Mobile origination, located in home service area. The "Originating Network" of S-S#4 is therefore the home network.
AS- O	Application Server origination. The" Originating Network" of S-S#1 is the home network. The element labelled S-CSCF#1 corresponds to the S-CSCF in figure 5.16b.

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

PSTN-T	PSTN termination. This occurs when the MGCF is selected to be in a different network than the S-CSCF.

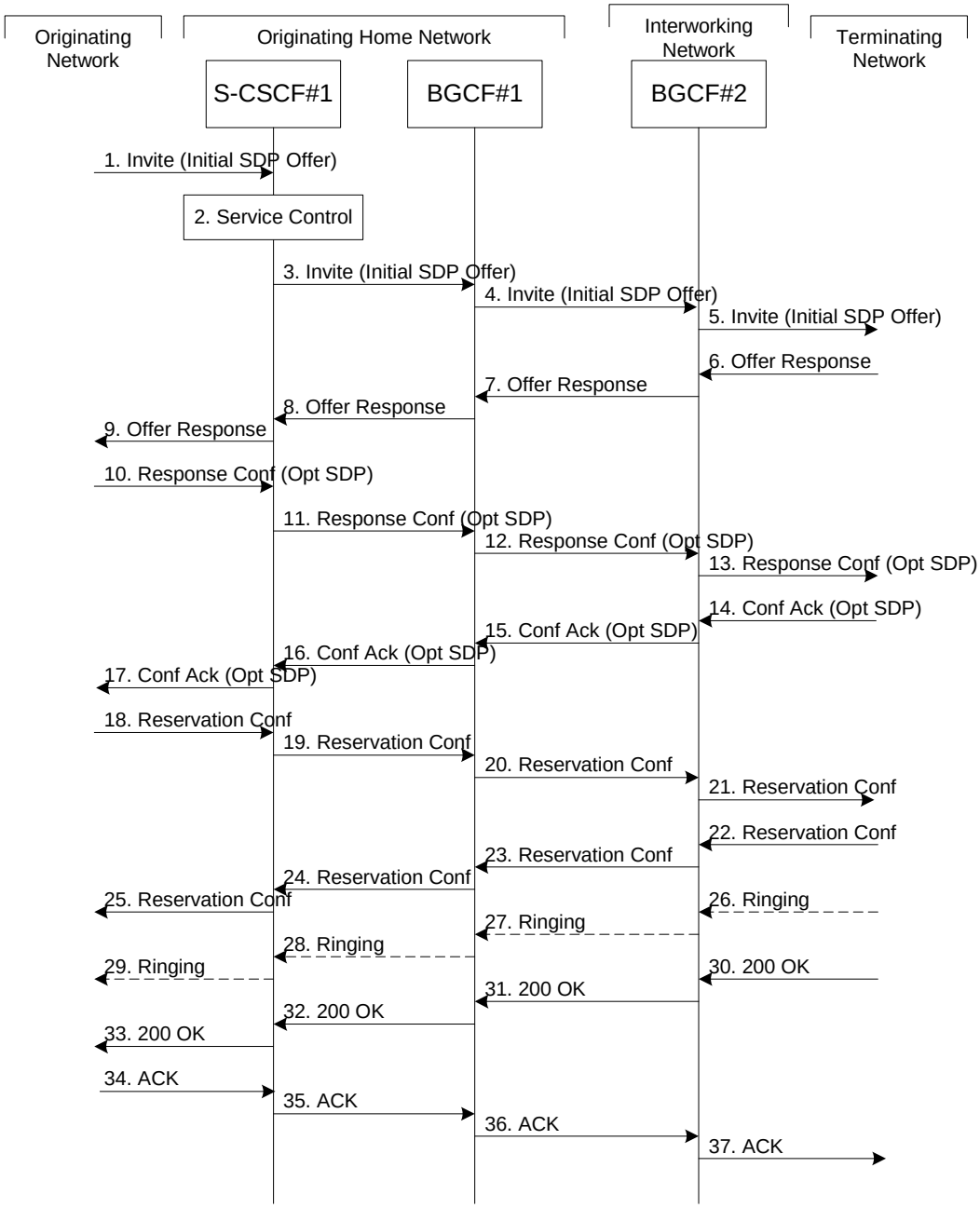


Figure 5.13: Serving to PSTN procedure - different operator

Procedure S-S#4 is as follows:

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

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

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

4. The BGCF#1 determines that the PSTN interworking should occur in interworking network, and forwards the request on to BGCF#2.

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

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

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

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

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

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

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

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

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

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

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

5.6 Origination procedures

5.6.0 General

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

The flows presented in the clause assume the use of Policy and Charging Control for the establishment of QoS-Assured Sessions.

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

A UE always has a proxy (P-CSCF) associated with it. This P-CSCF performs resource authorization, and may have additional functions in handling of emergency and priority sessions. The P-CSCF is determined by the CSCF discovery process, described in clause 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 (MO#1). These next-hop addresses could be IP addresses, or could be names that are translated via DNS to an IP address.

Sessions originated in the PSTN to a destination in an IMS network are a special case of the Origination procedures. The MGCF uses H.248 [18] to control a Media Gateway, and communicates with the SS7 network. The MGCF initiates the SIP request, and subsequent nodes consider the signalling as if it came from a S-CSCF.

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 clause 5.1.1. The home network advertises the S-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.

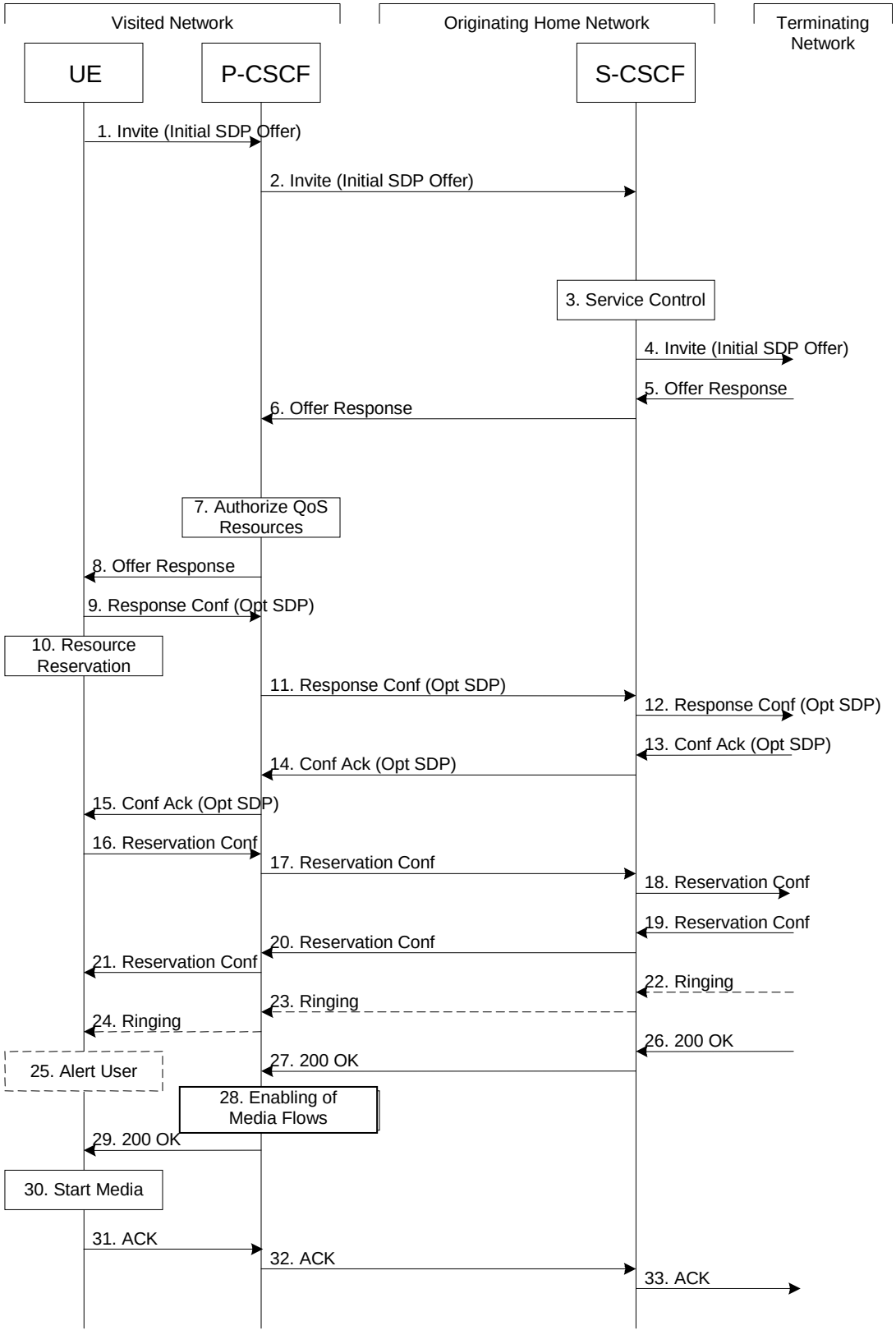


Figure 5.14: Mobile origination procedure - roaming

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.

P-CSCF determines whether the INVITE message requires priority handling based on user profile stored during the registration procedure and/or the priority requested by the user and/or MPS code/identifier included in the INVITE message. If the session is determined to require priority handling, then P-CSCF inserts/replaces the priority indication and forwards the INVITE to the S-CSCF.

3. S-CSCF validates the service profile, if a GRUU is received as the contact, ensures that the Public User Identity of the served user in the request and the Public User Identity associated with the GRUU belongs to the same service profile, and invokes any origination service logic required for this user. This includes authorization of the requested SDP based on the user's subscription for multi-media services. If the Request URI contains the SIP URI representation of an E.164 address then the procedure specified in clause 4.3.5.3 applies.

4. S-CSCF forwards the request, as specified by the S-S procedures. When the INVITE message includes priority indication, the S-CSCF forwards the INVITE, including the Service User's priority level if available.

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 instructs the PCRF/PCF to authorize the resources necessary for this session.

8. P-CSCF forwards the Offer Response 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 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 to instruct the PCRF/PCF to repeat the Authorization step (Step 7) again.

10. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. The UE initiates the reservation procedures for the resources needed for this session after determining the needed resources in step 8 as shown in Figure 5.14. Otherwise, the IP-CAN initiates the reservation of required resources after step 7.

11. P-CSCF forwards the Response Confirmation to S-CSCF.

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.

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 occurred. If the SDP has changed, the P-CSCF authorizes that the resources are allowed to be 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 sends a SIP 200-OK final response along the signalling path back to P-CSCF.

28. P-CSCF indicates that the media flows authorized for this session should now be enabled.

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.

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 clause 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.

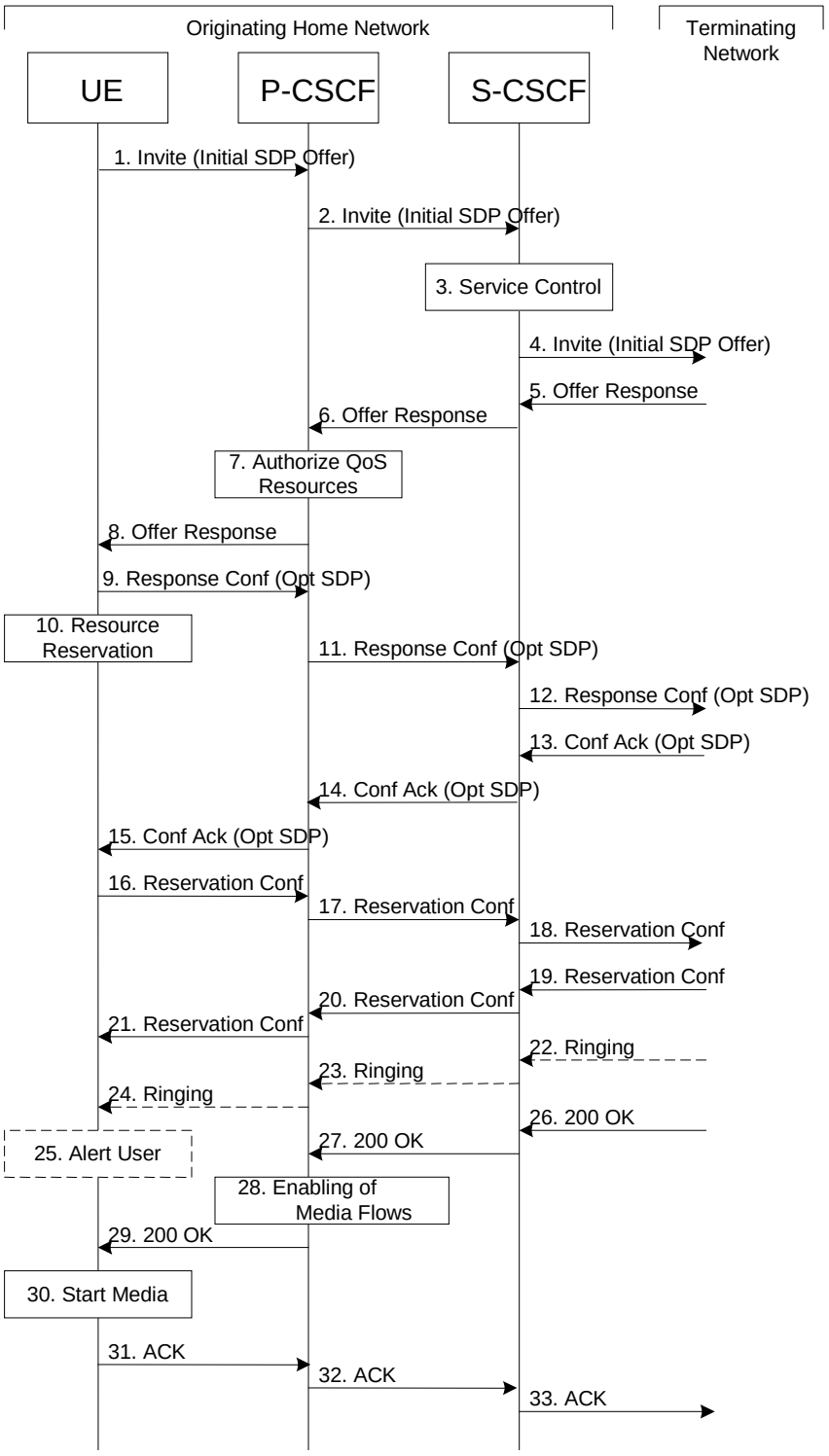


Figure 5.15: Mobile origination procedure - home

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.

   P-CSCF determines whether the INVITE message requires priority handling based on user profile stored during the registration procedure and/or the priority requested by the user and/or MPS code/identifier included in the INVITE message. If the session is determined to require priority handling, then P-CSCF inserts/replaces the priority indication and forwards the INVITE to the S-CSCF.

3. S-CSCF validates the service profile, if a GRUU is received as the contact, ensures that the Public User Identity of the served user in the request and the Public User Identity associated with the GRUU belong to the same service profile, and invokes any origination service logic required for this user. This includes authorization of the requested SDP based on the user's subscription for multi-media services. If the Request URI contains the SIP representation of an E.164 address then the procedure specified in clause 4.3.5.3 applies.

4. S-CSCF forwards the request, as specified by the S-S procedures. When the INVITE message includes priority indication, the S-CSCF forwards the INVITE, including the Service User's priority level if available.

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 instructs the PCRF/PCF to authorize the resources necessary for this session.

8. P-CSCF forwards the Offer Response 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 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 to repeat the Step 7 again.

10. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. The UE initiates resource reservation procedures for the offered media as shown in Figure 5.15. Otherwise, the IP-CAN initiates the reservation of required resources after step 7.

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 authorizes 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 occurred. 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 that the media flows authorized for this session should now be enabled.

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.

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.

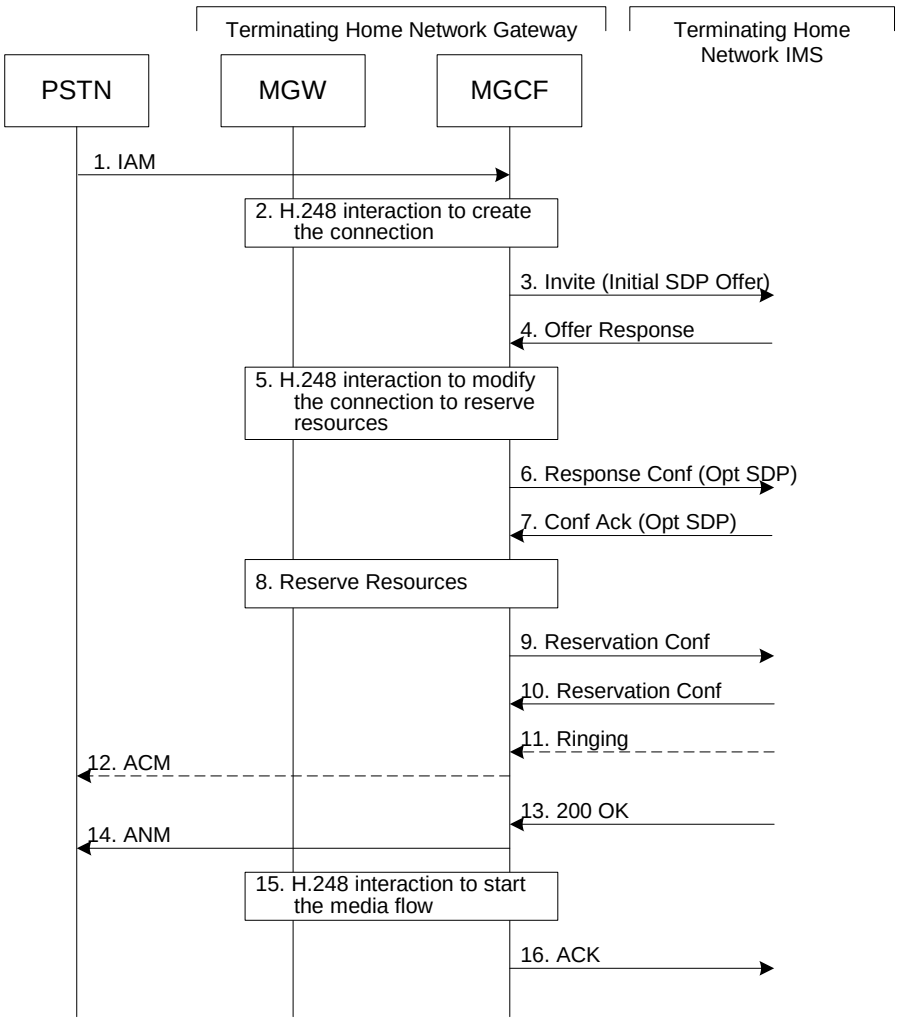


Figure 5.16: PSTN origination procedure

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 addressed to a tel URI or, if directed by operator's local policy, to a SIP URI (using an E.164 address in the user portion and the setting user=phone), includes an initial SDP in the INVITE request, and forwards the request to a configured I-CSCF, as per the proper S-S procedure. If configured through policies, the MGCF adds to the SIP INVITE attestation information based on the trunk identity or other sources of the request.
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 the PSTN.
15. MGCF initiates a H.248 command to alter the connection at MGW to make it bi-directional.
16. MGCF acknowledges the SIP final response with a SIP ACK message.

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

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

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

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

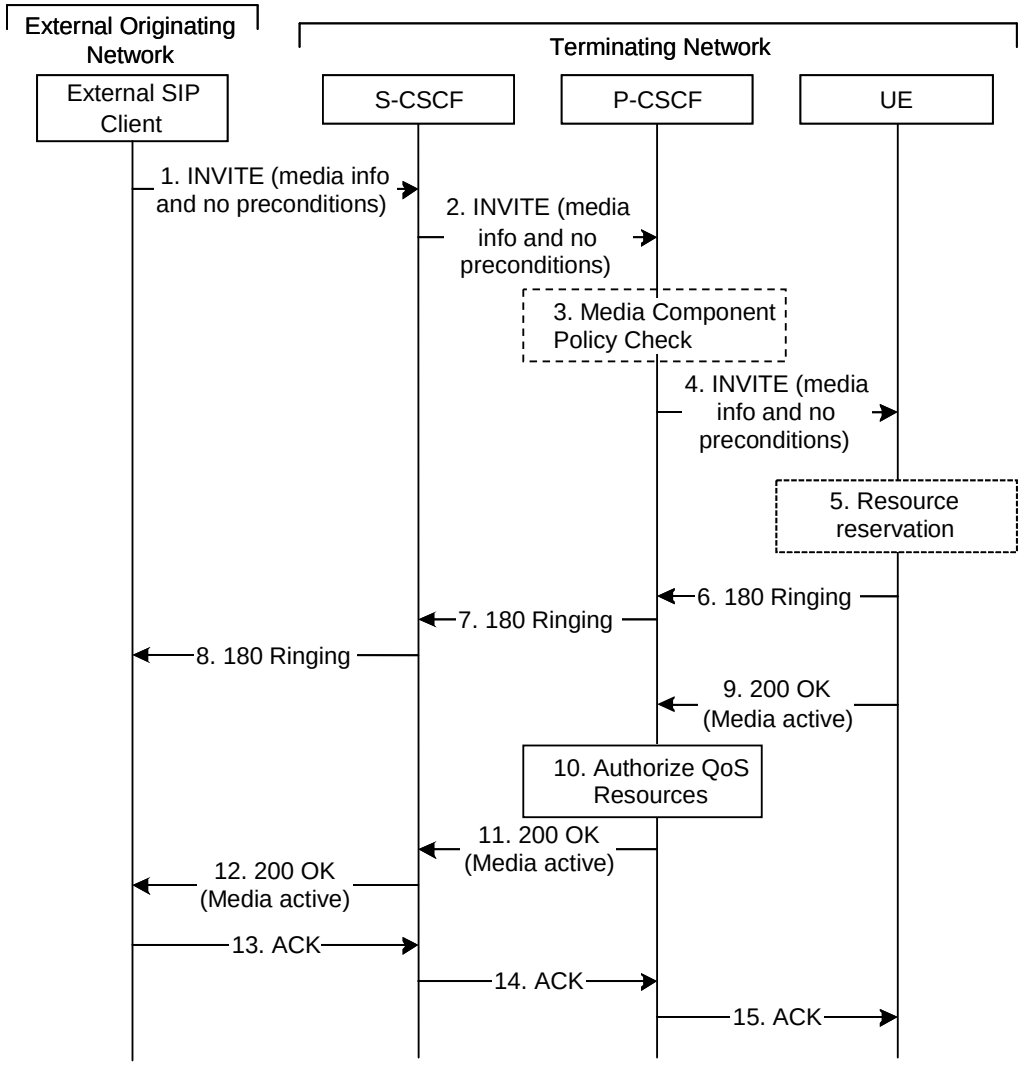


Figure 5.16a: Originating session from external SIP client

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

3. P-CSCF examines the media parameters. If P-CSCF finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies, or if available bandwidth authorization limitation information coming from the PCRF/PCF), it rejects the session initiation attempt.

NOTE 1: Whether the P-CSCF should interact with PCRF/PCF in this step is based on operator policy.

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

5. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. The UE begins the resource reservation according to the session and media parameters as shown in Figure 5.16a. Otherwise, the IP-CAN initiates the reservation of required resources after step 10.

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

9. The UE accepts the session with a 200 OK response.

10. Based on operator policy the P-CSCF may instruct the PCRF/PCF to authorize the resources necessary for this session.

11-12. The 200 OK response is forwarded to the originating party.

13-15. The originating party acknowledges the session.

5.6.5 Application Server Origination Procedure

5.6.5.1 (AS-O) Origination at Application Server

This origination procedure applies to an Application Server that initiates a session on behalf of a user or a Public Service Identity. If the AS initiates the session on behalf of a user, the user may be an IMS user (i.e. referred to by a Public User Identity) or a non-IMS user (i.e. with no profile in the HSS, e.g. a PSTN user). It will be referred as a non-IMS user. If the AS initiates the session on behalf of a user, the identity-related fields of the initial request are populated the same way as if the request was originated by the user himself.

In the case of originating unregistered procedures, the handling of the S-CSCF in the HSS will follow the same principle as terminating unregistered user handling.

In the case of originating unregistered procedures, the S-CSCF shall execute any unregistered origination service logic before forwarding requests from an AS on behalf of an IMS user (i.e. referred to by a Public User Identity) or a Public Service Identity, as specified by the S-S procedures. In order to allow an AS to retrieve the S-CSCF name via Sh interface the S-CSCF may keep its name in the HSS for Public User Identities that have services related to the unregistered state.

AS shall contact the S-CSCF only in the case that it has the knowledge of the serving S-CSCF based, e.g., on Sh query or third party registration. Otherwise, AS shall contact an I-CSCF to continue the session initiation.

The procedure described below assumes that the Application Server takes care of the user plane connection.

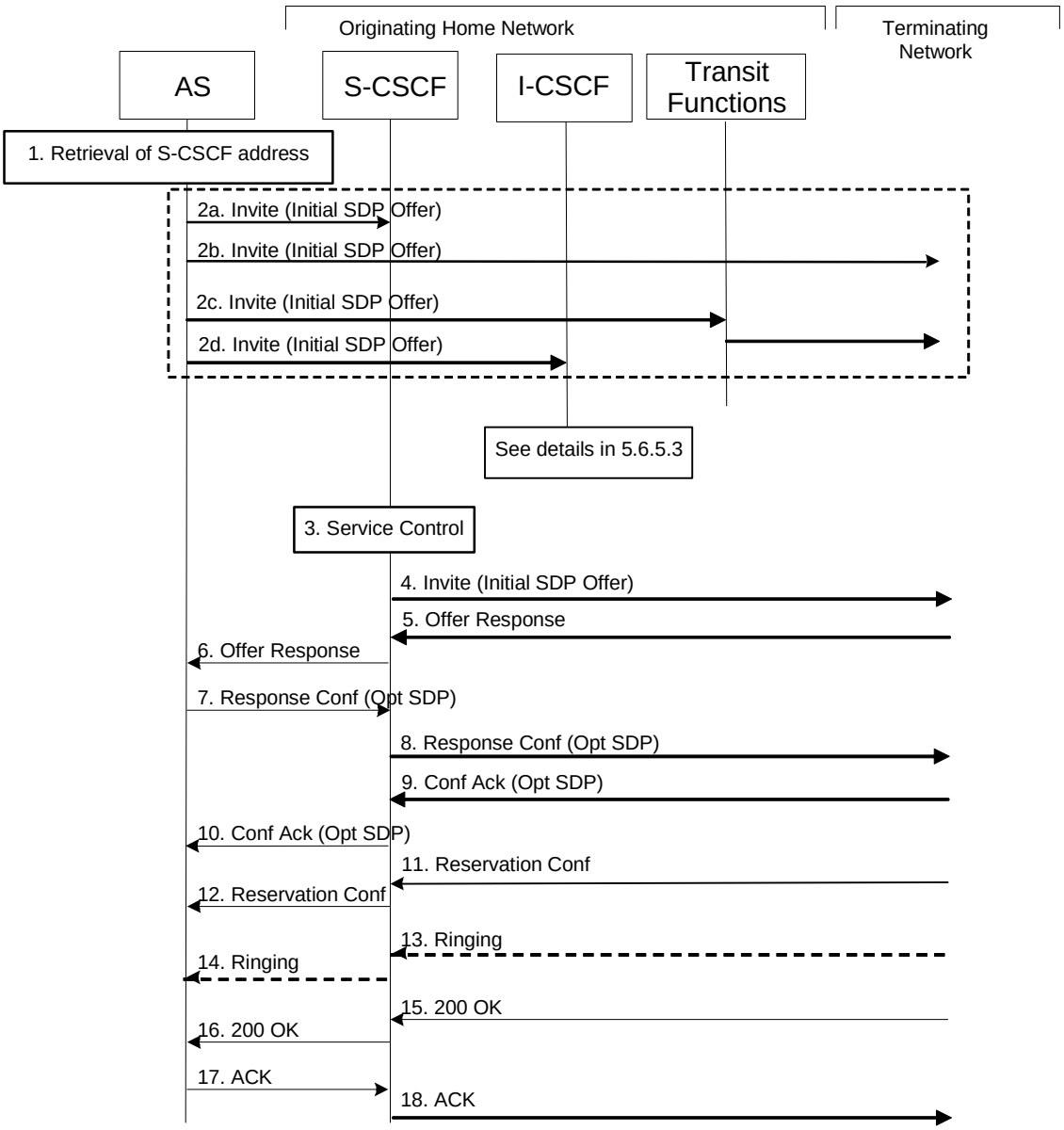


Figure 5.16b: Application Server origination procedure

Procedure for Application Server origination is as follows:

1. The AS may proceed in either of the following ways:

   - If the session requires the use of a S-CSCF and:

     - If the AS has acquired the address of the S-CSCF (if not available already) for the Public User Identity or the Public Service Identity on whose behalf the AS intends to originate the session, e.g. through Sh interface or based on third party registration, the AS sends the session initiation request to the S-CSCF (see step 2a)

     - If the AS could not acquire a S-CSCF address for the Public User Identity or the Public Service Identity, the AS sends the session initiation request to an I-CSCF (see step 2d).

   - If the Public Service Identity on whose behalf the AS intends to generate the session does not require the use of a S-CSCF or if the user on whose behalf the AS intends to generate the session is a non-IMS user:

     - If the AS supports routing capabilities (e.g. ENUM support, etc.), the AS sends the session initiation request directly towards the terminating network. In this case the AS may use the principles defined in IETF RFC 3263 [44] (see step 2b) to route the session initiation request.

- If the AS doesn't support routing capabilities, the AS shall send the session initiation request to the IMS Transit Functions (see step 2c). The IMS Transit Functions routes the session initiation request to the destination as described in clause 5.19.

2a. The AS sends the SIP INVITE request, containing an initial SDP, to the S-CSCF.
The initial SDP may represent one or more media for a multi-media session.

2b. The AS sends the SIP INVITE request, containing an initial SDP, to the terminating network.

The subsequent steps assume that the session initiation procedure involves the S-CSCF, i.e. they show the continuation of step 2a.

2c. The AS sends the SIP INVITE request, containing an initial SDP, to the IMS Transit Functions.

2d. The AS sends the SIP INVITE request, containing an initial SDP, to an I-CSCF indicating that it is an originating request. The I-CSCF selects the S-CSCF and forwards the SIP INVITE to that S-CSCF for further process. If the request is sent on behalf of the unregistered user, the procedure is described in clause 5.6.5.3.

3. S-CSCF identifies the incoming request as an originating request, and invokes any origination service logic required for this Public User Identity / Public Service Identity. The S-CSCF handles the incoming request as an authenticated and authorized request, as it was originated by a trusted entity within the network. If the Request URI contains the SIP representation of a telephone number then the procedure specified in clause 4.3.5.3 applies.

4. S-CSCF forwards the request, as specified by the S-S procedures.

5-6. The media stream capabilities of the destination are returned along the signalling path.

7-8. The AS decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation along the signalling path towards the destination network. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response or a subset. The AS is free to continue to offer new media on this operation or on subsequent exchanges using the Update method.

9-10. The terminating end point responds to the originating end with an acknowledgement, which is forwarded along the session signalling path. If Optional SDP is contained in the Response Confirmation, the Confirmation Acknowledge will also contain an SDP response.

11-12. The terminating endpoint responds to the originating end when successful resource reservation has occurred.

13-14. The destination UE may optionally perform alerting. If so, it signals this to the originating party by a provisional response indicating Ringing. This message is sent to the AS along the signalling path.

15-16. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating end.

17-18. The AS responds to the 200 OK with an ACK message which is passed along the signalling path to the terminating end.

5.6.5.2 Void

5.6.5.3 S-CSCF selection by I-CSCF for AS Originating call procedures

In figure 5.16c below the AS has no information of the serving S-CSCF, and therefore the AS sends the request to an I-CSCF as the entry point of the home network of the Public User Identity or the Public Service Identity. The AS finds an I-CSCF by using the same mechanism as the S-CSCF uses to find an I-CSCF of the terminating network (see clauses 5.5.1 and 5.5.2). The request shall indicate that it is an originating request sent on behalf of the Public User Identity or the Public Service Identity.

NOTE 1: If border control concepts are applied, the contact point within an operator's network may be different, see clause 4.14 and Annex I for details.

NOTE 2: The procedure described below can be used by an external AS that cannot access HSS data using the Sh interface.

The procedure described below assumes that the Application Server takes care of the user plane connection.

This is shown by the information flow in figure 5.16c:

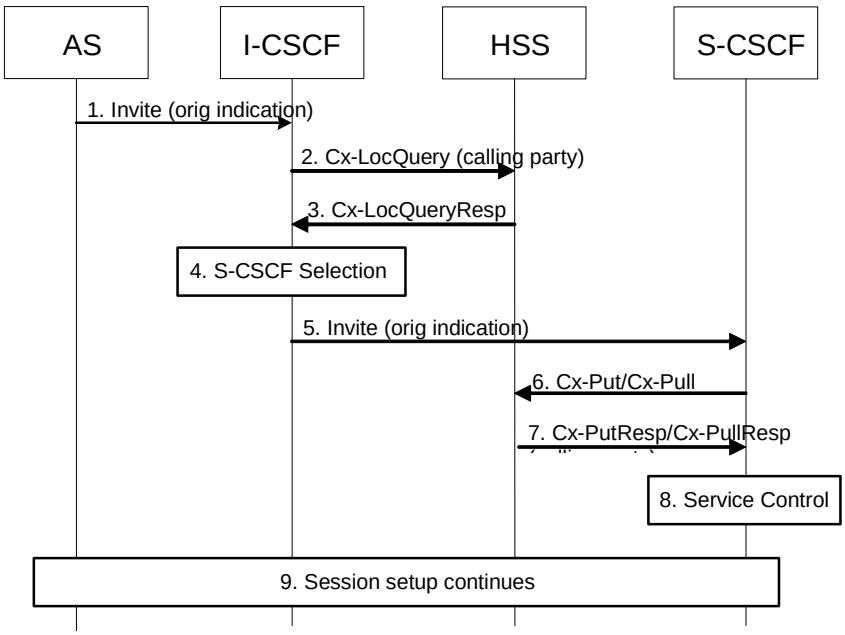


Figure 5.16c: S-CSCF selection by I-CSCF for AS Originating call procedure

1. The I-CSCF receives an INVITE message indicating that it is an AS originating procedure.

2. The I-CSCF queries the HSS for current location information of the Public User Identity/Public Service Identity on whose behalf the request is sent.

3. The HSS either responds with the required S-CSCF capabilities which the I-CSCF should use as an input to select a S-CSCF or provides the I-CSCF with the previously allocated S-CSCF name for that user or service.

NOTE 3: The HSS sends back the capabilities even if the Public User Identity/Public Service Identity is not registered and has no initial filter criteria related to the unregistered state.

4. If the I-CSCF has not been provided with the location of the S-CSCF, the I-CSCF selects a S-CSCF.

5. The I-CSCF forwards the INVITE request to the S-CSCF. The I-CSCF must indicate that it is an originating request sent on behalf of the Public User Identity/Public Service Identity.

6. The S-CSCF sends Cx-Put/Cx-Pull (Public User Identity/Public Service 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 Public Service Identity or Public User Identities of that user. This will result in all traffic related to the Public Service Identity or the 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 4: Optionally the S-CSCF can omit the Cx-Put/Cx-Pull request if it has the relevant information from the user profile.

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

8. The S-CSCF invokes whatever service logic is appropriate for this call attempt, if required.

NOTE 5: If the Public User Identity/Public Service Identity is not registered and has no initial filter criteria related to the unregistered state, the S-CSCF just routes the request further without invoking any service logic for this request.

9. The session setup continues as for normal origination procedures.

5.7 Termination procedures

5.7.0 General

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

The flows presented in the clause assume the use of Policy and Charging Control for the establishment of QoS-Assured Sessions.

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

A UE always has a proxy (P-CSCF) associated with it. This P-CSCF performs resource authorization for the sessions to the UE and may have additional functions in handling of priority sessions. The P-CSCF is determined by the CSCF discovery process, described in clause 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).

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 clause 5.1.1. The home network advertises the S-CSCF 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, the P-CSCF and P-CSCF knows the name/address of the UE.

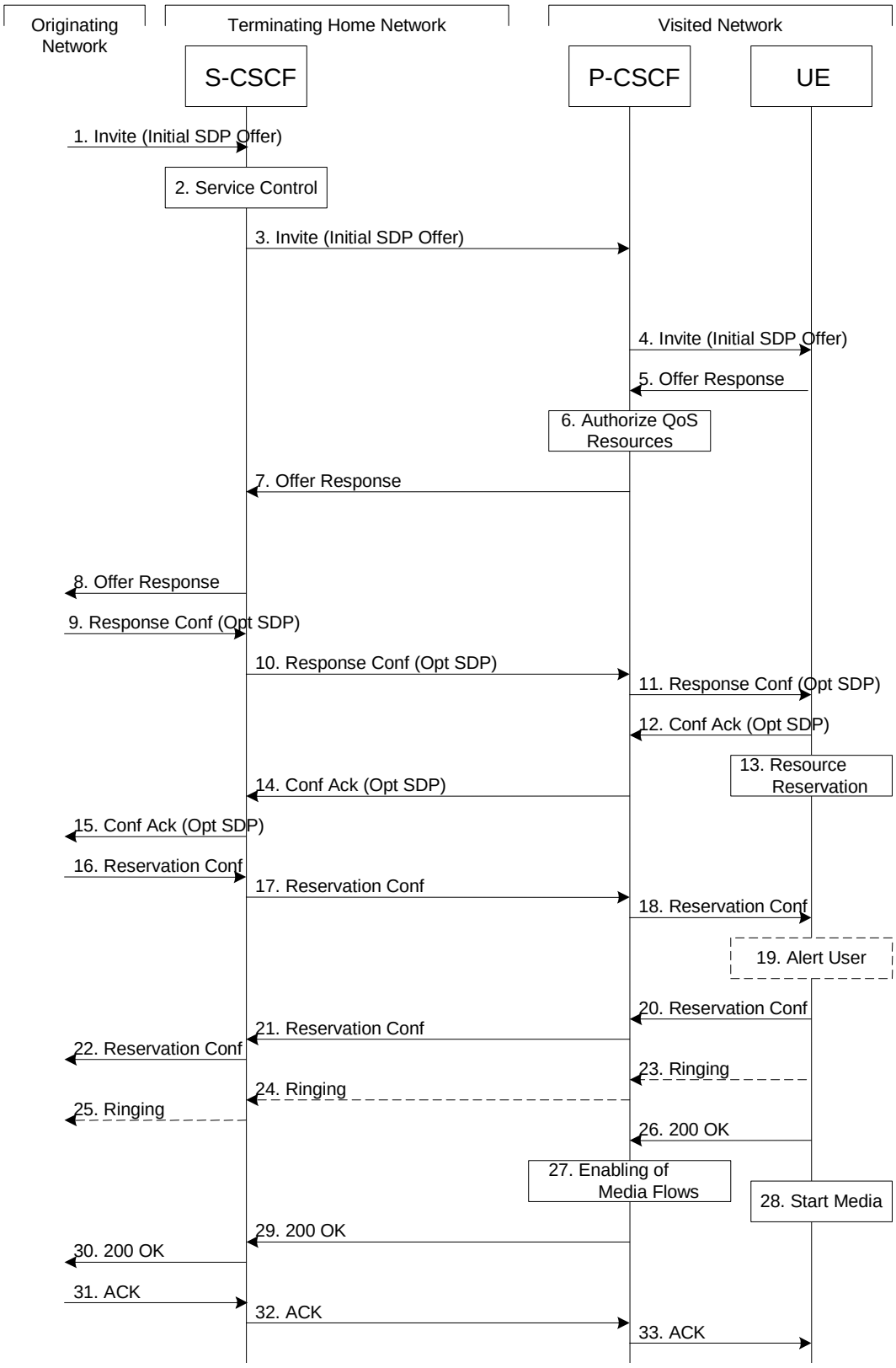


Figure 5.17: Mobile termination procedure - roaming

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 authorization 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.

4. If the P-CSCF determines that the termination is for an MPS session, the P-CSCF derives the session information and invokes dynamic policy sending the derived session information to the PCRF/PCF. The 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 instructs the PCRF/PCF to authorize the resources necessary for this session.

NOTE: P-CSCF can additionally authorize the resources in step 4 in scenarios where request indicates requirements for resource reservation or that the required resources are already available on the originating side, as in such cases no SDP answer is received before the PCRF/PCF is requested to authorize the required QoS resources.

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 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 to repeat the 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.

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. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. The UE initiates the reservation procedures for the resources needed for this session as shown in Figure 5.17. Otherwise, the IP-CAN initiates the reservation of required resources after step 6.

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.

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.

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.

26. When the destination party answers, the UE sends a SIP 200-OK final response to P-CSCF.

27. P-CSCF indicates to PCRF/PCF that the media flows for this session should now be enabled.

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.

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.

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 clause 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.

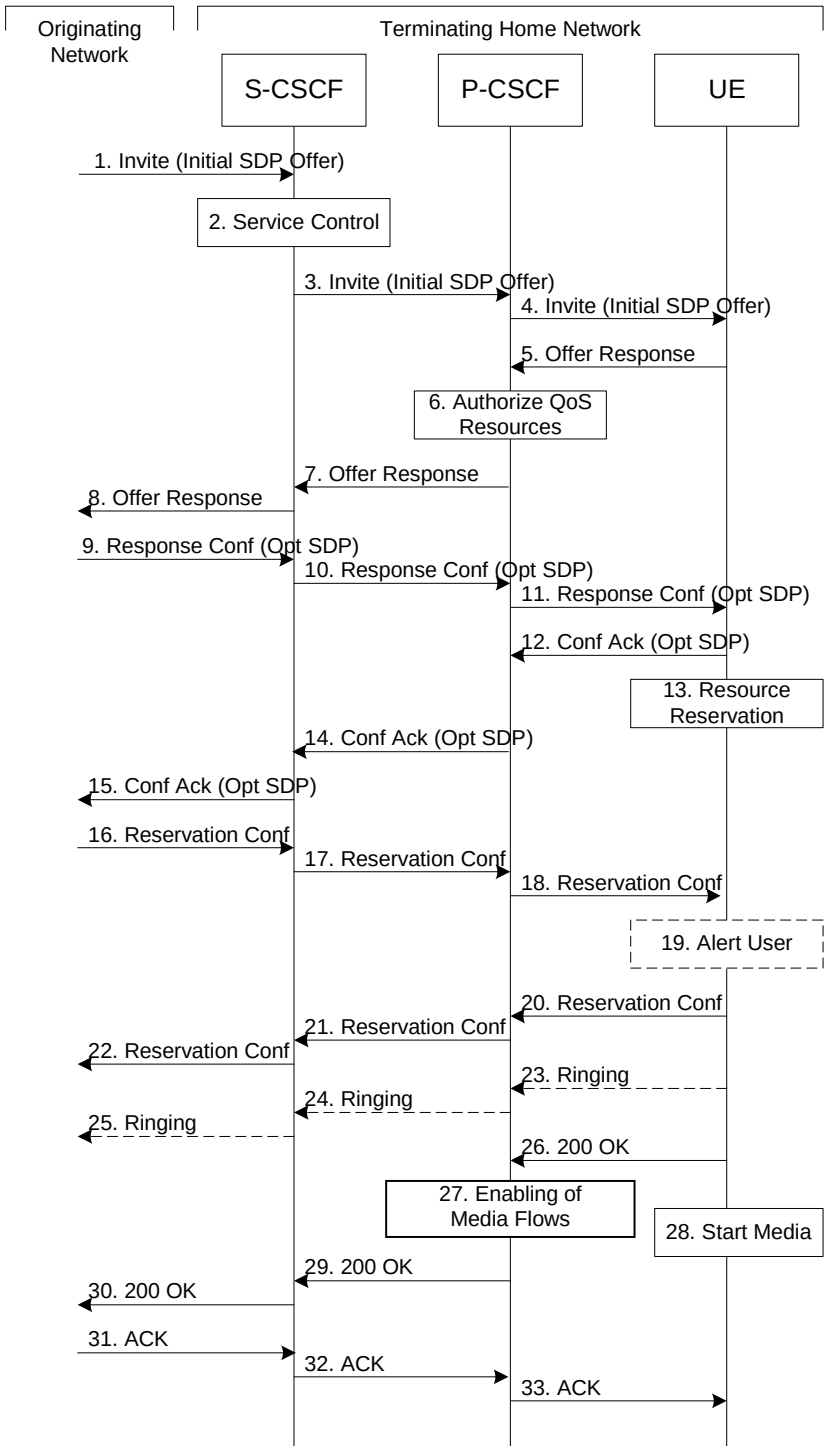


Figure 5.18: Mobile termination procedure - home

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 authorization 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. If the P-CSCF determines that the termination is for an MPS session, the P-CSCF derives the session information and invokes dynamic policy sending the derived session information to the PCRF/PCF. The 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 instructs PCRF/PCF to authorize the resources necessary for this session.

NOTE: P-CSCF can additionally authorize the resources in step 4 in scenarios where request indicates no requirements for resource reservation or that the required resources are already available on the originating side, as in such cases no SDP answer is received before the PCRF/PCF is requested to authorize the required QoS resources.

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 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 to repeat the 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. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. The UE initiates the reservation procedures for the resources needed for this session as shown in Figure 5.18. Otherwise, the IP-CAN initiates the reservation of required resources after step 6.

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 that the authorized media flows for this session should now be enabled.

28. UE starts the media flow(s) for this session.

29-30. P-CSCF forwards the 200-OK to S-CSCF, following the signalling 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

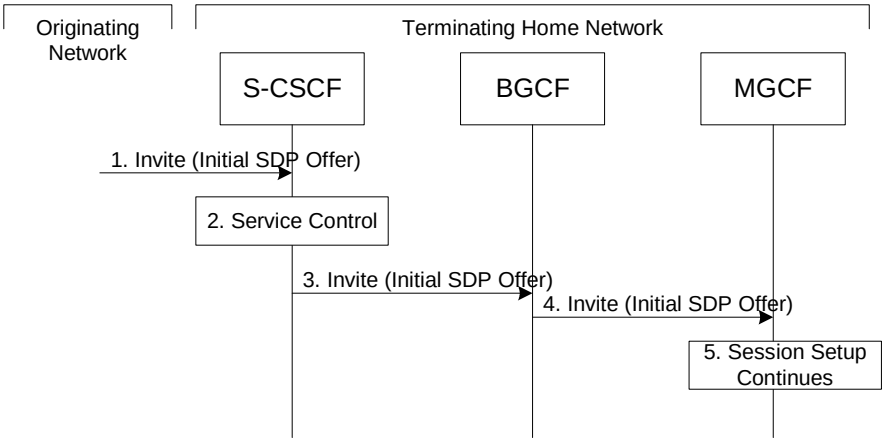


Figure 5.18a: Mobile Terminating procedures to a user that is unregistered for IMS services but is registered for CS services

1. If the terminating user does not have an S-CSCF allocated, the session attempt is routed according to the clause 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 the 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 clause 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.

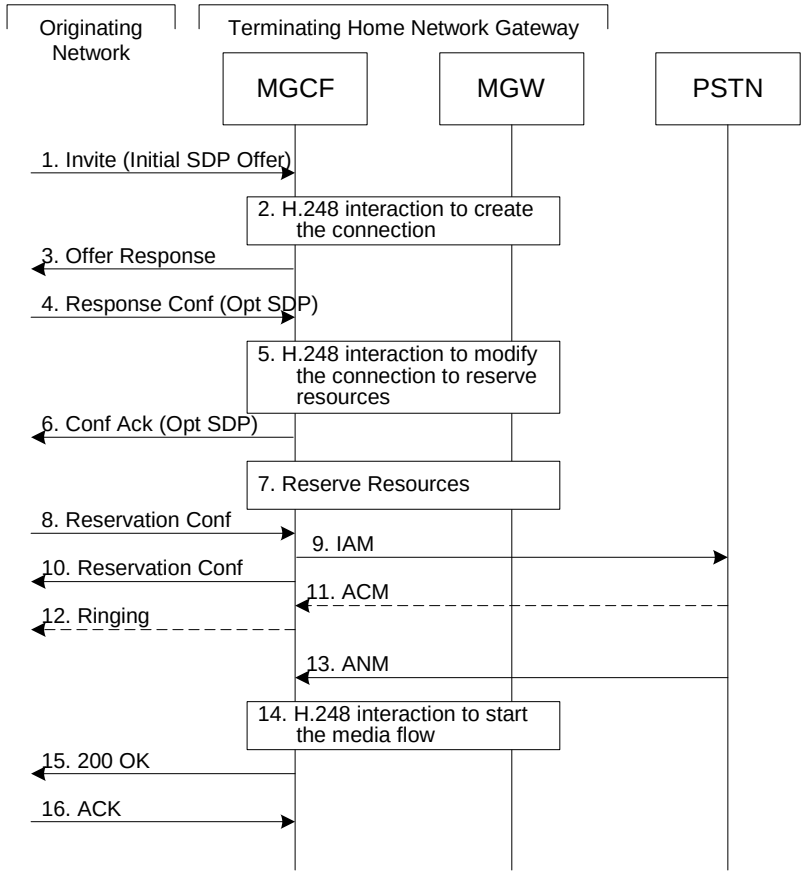


Figure 5.19: PSTN termination procedure

The PSTN termination procedure is as follows:

1. MGCF receives an INVITE request, containing an initial SDP, through one of the origination procedures and via one of the inter-serving procedures.
2. MGCF initiates a H.248 interaction to pick an outgoing channel and determine media capabilities of the MGW.
3. MGCF determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. This response is sent via the S-S procedure.
4. The originating endpoint sends a Response Confirmation. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in Step 3 or a subset. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method.
5. MGCF initiates a H.248 interaction to modify the connection established in step #2 and instruct MGW to reserve the resources necessary for the media streams.
6. MGCF responds to the offered media towards the originating party.
7. GW reserved the resources necessary for the media streams.
8. When the originating endpoint has completed its resource reservation, it sends the successful Resource Reservation message to MGCF, via the S-S procedures.
9. MGCF sends an IAM message to the PSTN
10. MGCF sends response to the successful resource reservation towards originating end.
11. The PSTN establishes the path to the destination. It may optionally alert the destination user before completing the session. If so, it responds with an ACM message.
12. If the PSTN is alerting the destination user, MGCF indicates this to the originating party by a provisional response indicating Ringing. This message is sent via the S-S procedures.

13. When the destination party answers, the PSTN sends an ANM message to MGCF
14. MGCF initiates a H.248 interaction to make the connection in the MGW bi-directional.
15. MGCF sends a SIP 200-OK final response along the signalling path back to the session originator
16. The Originating party acknowledges the final response with a SIP ACK message

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

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

In this scenario, the UE originates an IMS session without requiring the support for precondition capabilities, towards an external SIP entity that does not support those capabilities. Since required resources are not yet available at the UE, all the media components are set to inactive. In this example the external SIP client does not support the Precondition extension of SIP so the related precondition information within SIP/SDP is ignored.

When both parties have agreed to the session and media parameters and the UE has established resources for the media, the UE initiates session modification setting the status of the media components to active and is thus enabling the media transfer to start. Figures 5.19b and 5.19c together illustrate session flows for one possible originating session establishment towards a non-IMS client in an external network with QoS authorization and Policy and Charging Control support.

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

Figure 5.19a: Void

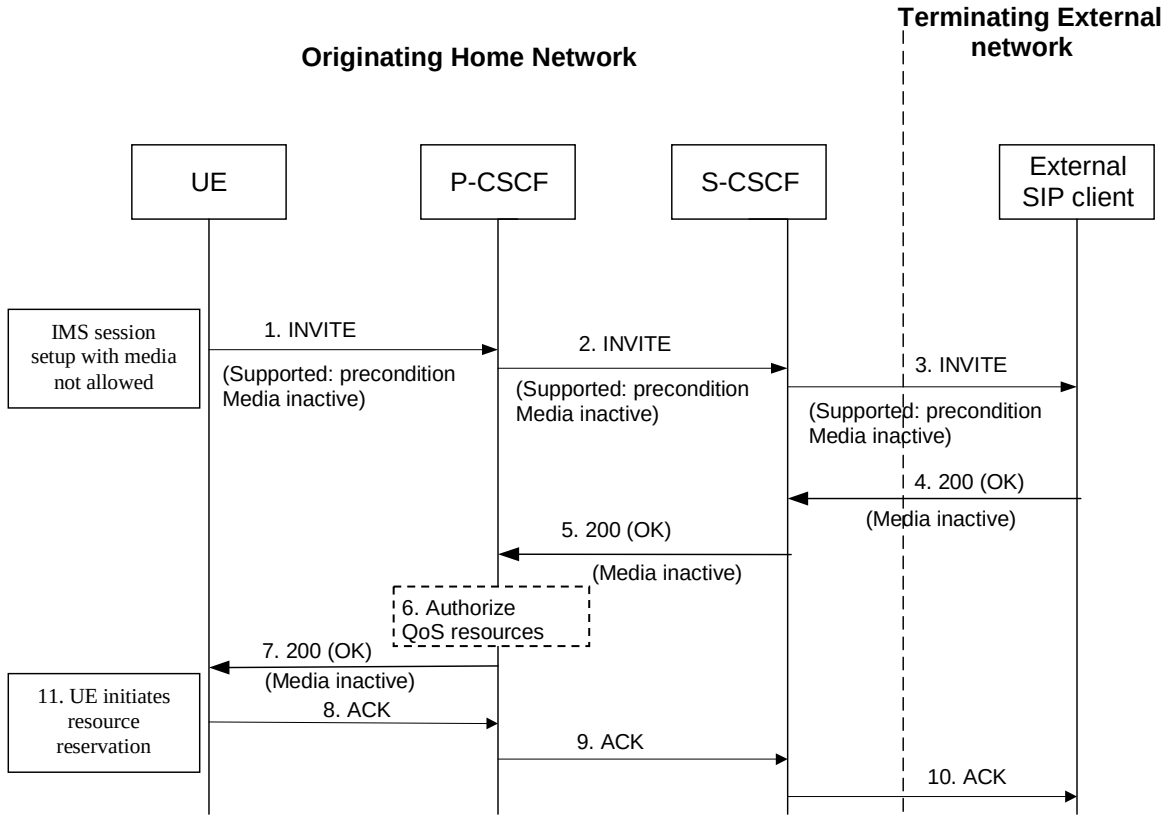


Figure 5.19b: Terminating session towards external SIP client, initiate session set up not requiring precondition capabilities and with inactive media

The UE initiates an INVITE message, which indicates the support of the precondition capability Since required resources are not yet available, the UE sets all media components to inactive state, as shown in figure 5.19b.

1-3. UE initiates a new IMS session indicating the support of the precondition capability and setting all media components to inactive state.

4-5. Acknowledgement of the session and media parameters are sent from the terminating side to the P-CSCF.

6. The P-CSCF may at this point instruct PCRF/PCF to authorize the resources being negotiated.

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

8-10. The session is established, but media transfer is not allowed yet.

11. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. The UE starts the resource reservation for the media as shown in Figure 5.19b. Otherwise, the IP-CAN initiates the reservation of required resources after step 6.

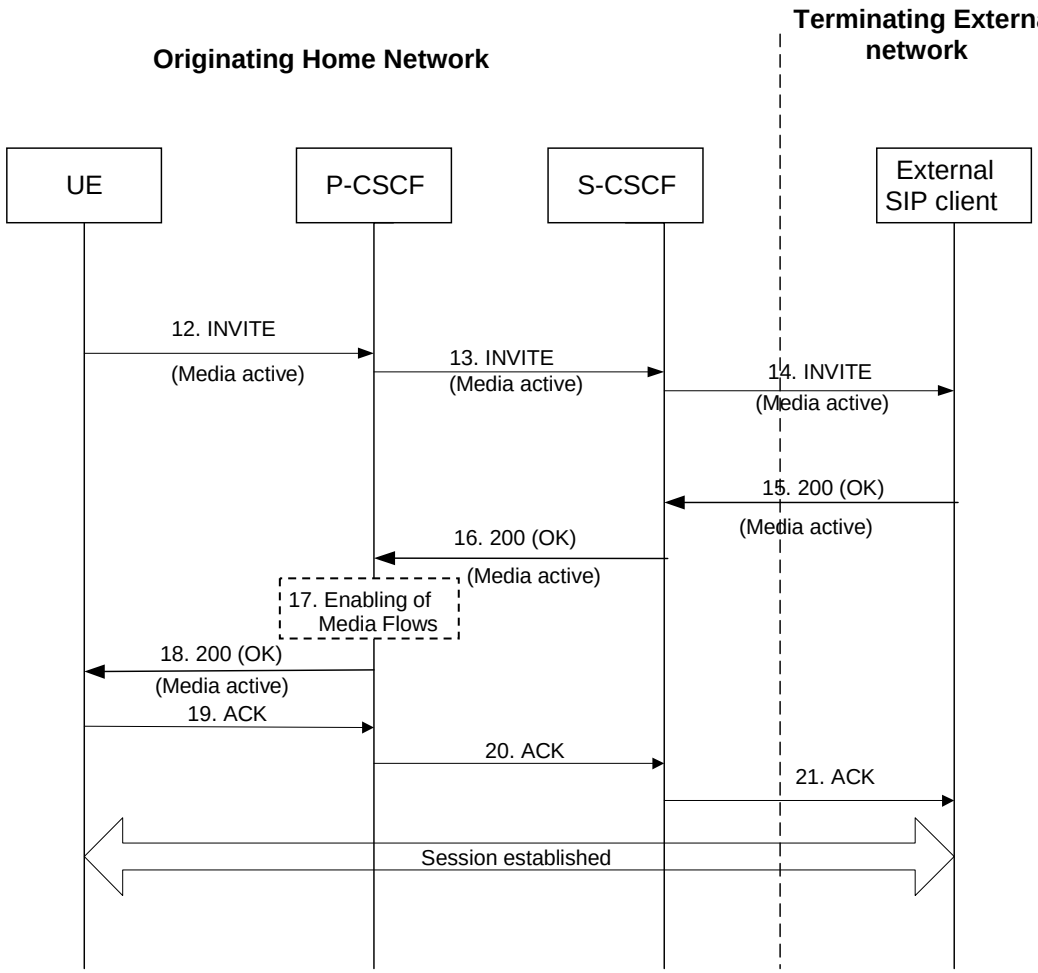


Figure 5.19c: Continuation of terminating session towards external SIP client, session set up with active media

Once the session parameters have been agreed and the UE has successfully reserved resources for the media components, the session set-up continues by setting the media components to active, as shown in session flow 5.19c.

12-14. UE initiates activation of media by initiating an INVITE procedure towards the terminating party.

15-16. The terminating party accepts media activation, and corresponding signalling is passed back towards the originating party along the session path.

17. The P-CSCF receives the acceptance of media activation. At this point, the P-CSCF may instruct the PCRF/PCF to enable the media flows that have been authorized for the session.

18. The P-CSCF forwards the signalling message to the originating UE indicating that the session setup can continue and activation of media is performed.

19-21. The Session establishment is then acknowledged through the session path.

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

5.7.5 (AS-T#1) PSI based Application Server termination – direct

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

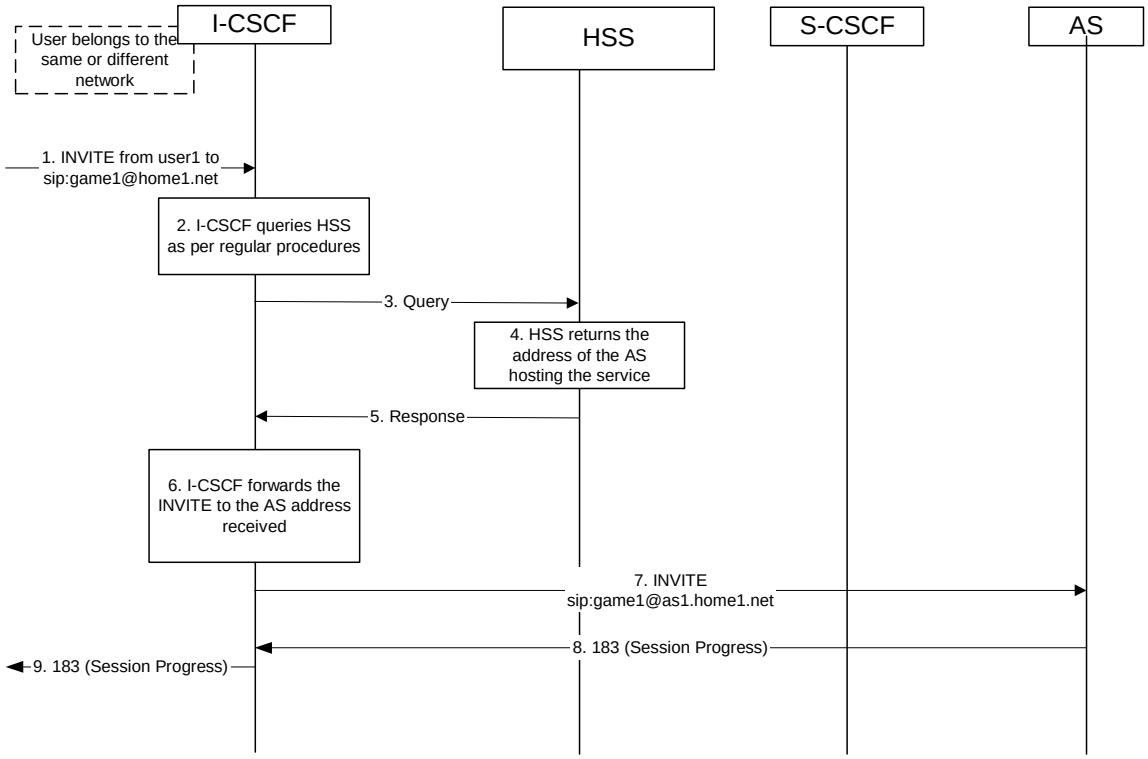


Figure 5.19d: Incoming session, direct route towards the AS

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

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

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

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

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

8-9. Session setup continues as per existing procedures.

5.7.6 (AS-T#2) PSI based Application Server termination – indirect

This clause depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.

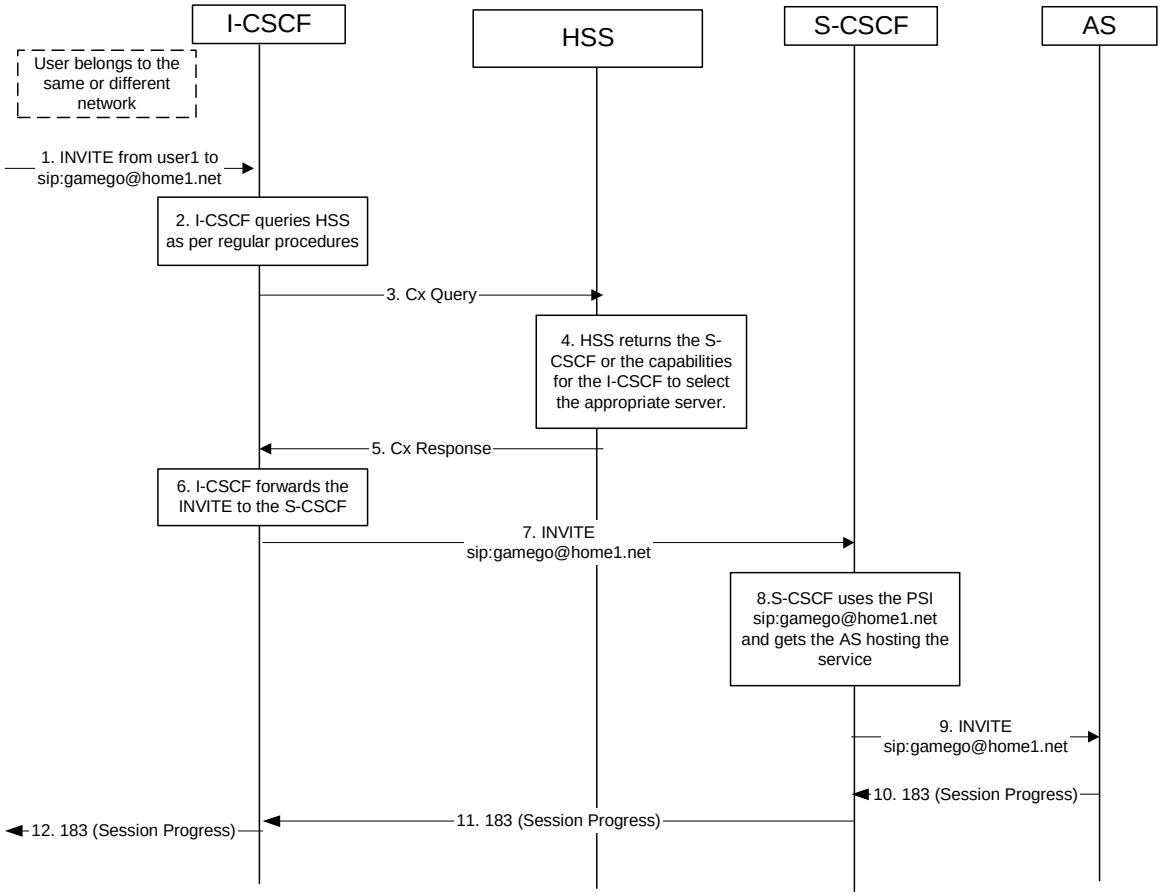


Figure 5.19e: Incoming session, indirect route to AS via S-CSCF

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

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

4. HSS determines the routing information, which is the S-CSCF defined for the "PSI user".

5. HSS returns the S-CSCF address/capabilities to the I-CSCF.

6-7. I-CSCF, as per existing procedures, forwards the request towards the entity (i.e., S-CSCF) received from the query, or the I-CSCF selects a new S-CSCF if required.

8. S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.

9. The request is then routed towards the AS identified by the filter criteria.

10-12. Session setup continues as per existing procedures.

5.7.7 (AS-T#3) PSI based Application Server termination – DNS routing

This clause shows an example of DNS based routing of an incoming session from an external network. The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.

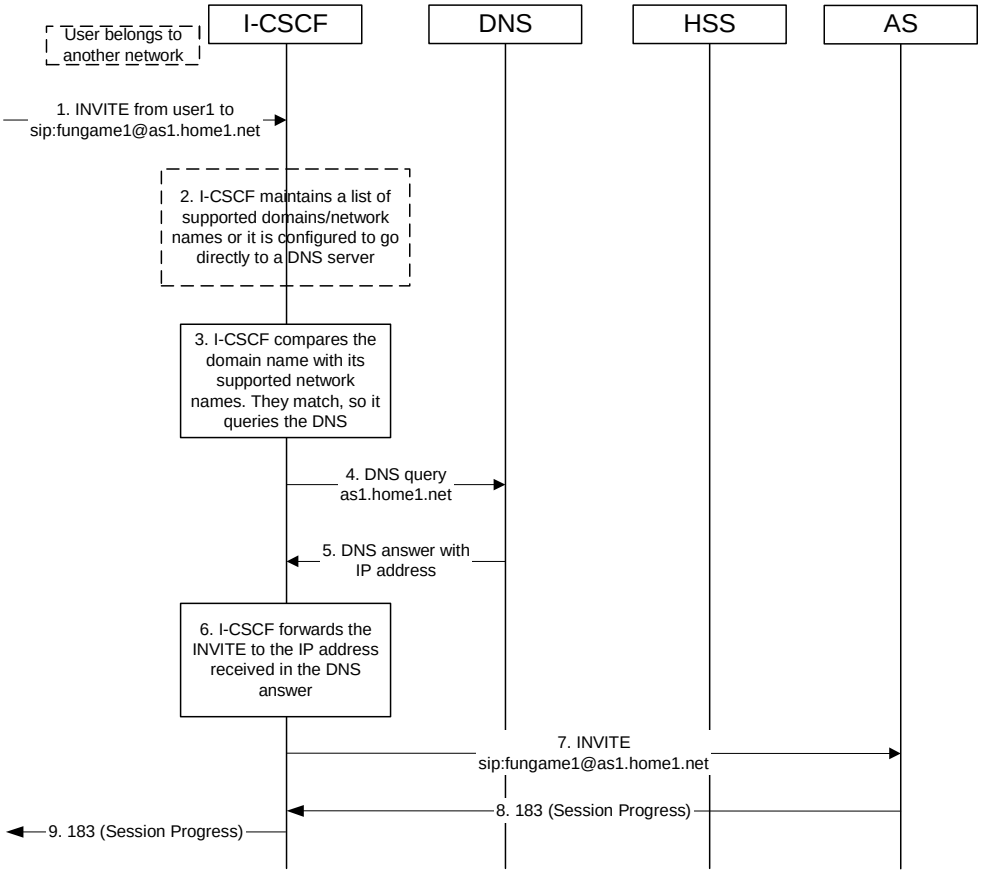


Figure 5.19f: Incoming session, direct route to AS using DNS

1. I-CSCF receives a request that is destined to the PSI.
2. I-CSCF has been configured with the list of supported domains/network names, or it may have been configured to directly query a local DNS server.
3. In this case the I-CSCF checks the list and finds a match.
4. I-CSCF sends DNS query to find the route.
5. DNS server returns the IP address of the AS hosting the PSI.

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

8-9. Session setup continues as per existing procedures.

5.7.8 (AST#4) Termination at Application Server based on service logic

This termination procedure applies to an Application Server that terminates a session. In this case the addressed user is a UE and is not hosted by the AS. Based on the invoked service logic at the Application Server the session is terminated at the AS.

The procedure described below assumes that the Application Server takes care of the user plane connection.

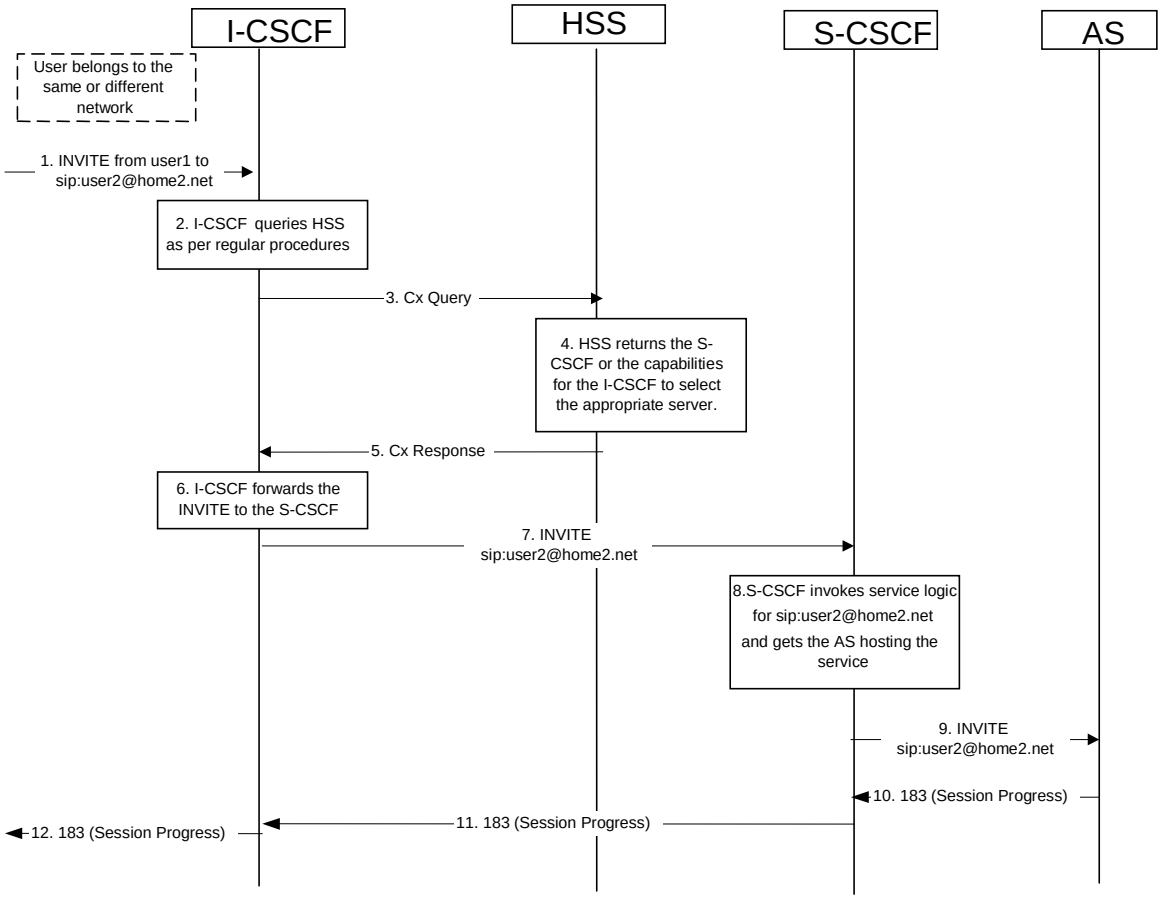


Figure 5.19g: Application Server termination

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

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

4. HSS determines the routing information, which is the S-CSCF defined for the user.

5. HSS returns the S-CSCF address/capabilities to the I-CSCF.

6-7. I-CSCF, as per existing procedures, forwards the request to S-CSCF that will handle the session termination.

8. S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.

9. The request is then routed towards the AS identified by the filter criteria. The AS terminates the session instead of allowing it to continue on to the address end user.

10-12. Session setup continues as per existing procedures.

5.7a Procedures for the establishment of sessions without preconditions

5.7a.1 General

These clauses present the general end-to-end session flow procedures without preconditions. The flow in clause 5.7a.2 is applicable to services without real-time QoS requirements before session becomes active, and thus do not need to set-up dedicated IP-CAN bearers but can use existing IP-CAN bearers, and to services which do not require that the terminating endpoint obtains a SIP-level notification when the originating endpoint's IP-CAN bearer becomes available.

NOTE: The flows in clauses 5.6 and 5.7 apply for services with real-time QoS requirements before session becomes active.

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

5.7a.2 Procedures for the establishment of sessions without preconditions - no resource reservation required before session becomes active

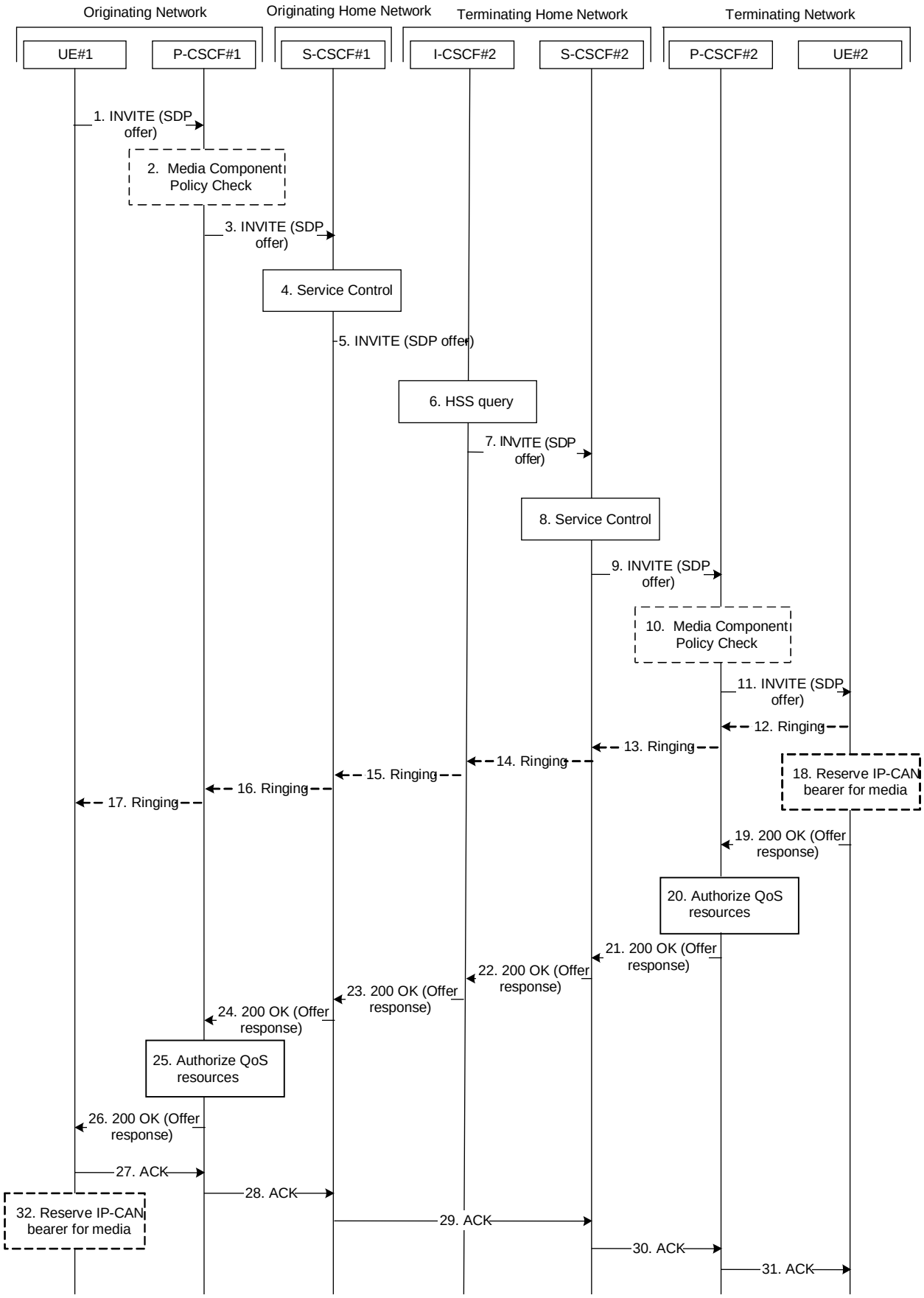


Figure 5.19h: End-to-end session flow procedure without preconditions - no resource reservation required before session becomes active

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

2. P-CSCF#1 examines the media parameters. If P-CSCF#1 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies, or if available bandwidth authorization limitation information coming from the PCRF/PCF), it rejects the session initiation attempt.

NOTE 0a: Whether the P-CSCF should interact with PCRF/PCF in this step is based on operator policy.

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

4. Based on operator policy S-CSCF#1 validates the user's service profile and may invoke whatever service control logic is appropriate for this INVITE request. This may include routing the INVITE request to an Application Server, which processes the request further on.

5. S-CSCF#1 forwards INVITE 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 INVITE request to S-CSCF#2.

8. Based on operator policy S-CSCF#2 validates the user's service profile and may invoke whatever service control logic is appropriate for this INVITE request. This may include routing the INVITE request to an Application Server, which processes the request further on.

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

10. P-CSCF#2 examines the media parameters. If P-CSCF#2 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies, or if available bandwidth authorization limitation information coming from the PCRF/PCF), it rejects the session initiation attempt.

NOTE 0b: Whether the P-CSCF should interact with PCRF/PCF in this step is based on operator policy.

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

12. - 17. UE#2 may optionally generate a ringing message towards UE#1.

18. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. UE#2 may reserve a dedicated IP-CAN bearer for media based on the media parameters received in the SDP offer as shown in Figure 5.19h. Otherwise, the IP-CAN#2 initiates the reservation of required resources after step 20 instead.

NOTE 1: The sequential ordering of 18 and 19 does not indicate that these steps are necessarily performed one after the other. If step 19 is performed before step 18 is finished, UE#2 shall use an existing IP-CAN bearer to send and receive media unless the application is such that a new bearer is not needed until some later point in time. If step 18 is performed successfully, media are sent and received by UE#2 on the dedicated IP-CAN bearer.

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

20. Based on operator policy P-CSCF#2 may instruct PCRF/PCF to authorize the resources necessary for this session.

21. - 24. The 200 OK response traverses back to UE#1.

25. Based on operator policy P-CSCF#1 may instruct the PCRF/PCF to authorize the resources necessary for this session.

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

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

32. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. UE#1 may reserve a dedicated IP-CAN bearer for media based on the media parameters received in the SDP answer as shown in Figure 5.19h. Otherwise, the IP-CAN#1 initiates the reservation of required resources after step 25.

NOTE 2: The sequential ordering of 27 and 32 does not indicate that these steps are necessarily performed one after the other. If step 32 is performed successfully, media are sent and received by UE#1 on the reserved dedicated IP-CAN bearer. UE#1 may also use an existing IP-CAN bearer to send and receive media.

5.7a.3 Void

5.8 Procedures related to routing information interrogation

5.8.0 General

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

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

5.8.1 User identity to HSS resolution

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

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

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

A way to use the SLF is described in the following.

The Dx interface provides:

- an operation to query the SLF 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. The I-CSCF may forward the HSS name towards the S-CSCF. The S-CSCF may use this name to find the subscriber's HSS.

Clause 5.8.2 presents the session flows on REGISTER and clause 5.8.3 on INVITE messages.

The Dh interface provides:

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

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

Clause 5.8.4 presents the message flow on the Dh interface.

5.8.2 SLF on register

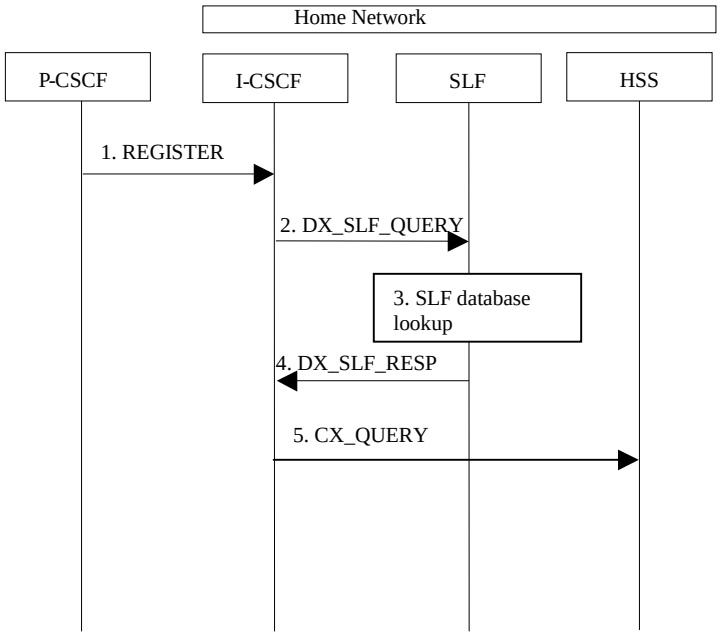


Figure 5.20: SLF on register (1st case)

1. I-CSCF receives a REGISTER request and now has to query for the location of the user's subscription data.
2. The I-CSCF sends a DX_SLF_QUERY to the SLF and includes as parameter the user identity which is stated in the REGISTER request.
3. The SLF looks up its database for the queried user identity.
4. The SLF answers with the HSS name in which the user's subscription data can be found.
5. The I-CSCF can proceed by querying the appropriate HSS.

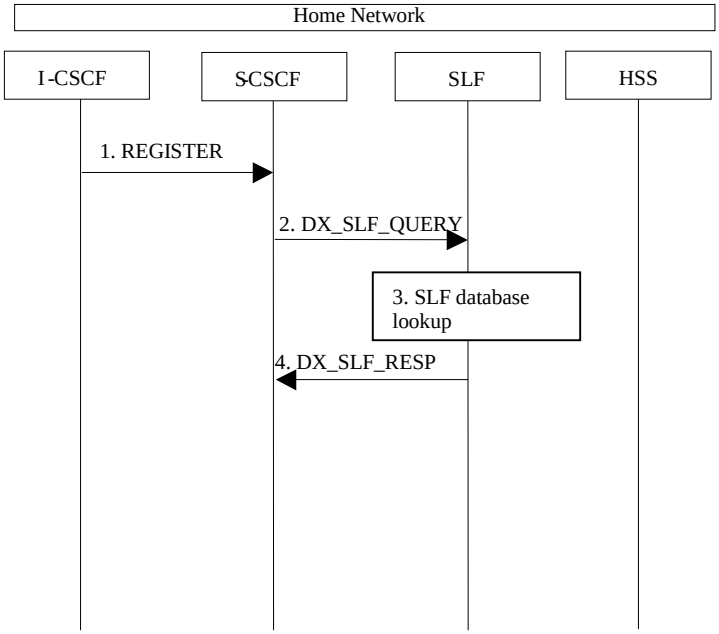


Figure 5.20a: SLF on register (2nd case)

1. I-CSCF sends a REGISTER request to the S-CSCF. This now has to query for the location of the user's subscription data.
2. The S-CSCF sends a DX_SLF_QUERY to the SLF and includes as parameter the user identity which is stated in the REGISTER request.
3. The SLF looks up its database for the queried user identity.
4. The SLF answers with the HSS name in which the user's subscription data can be found.

5.8.3 SLF on UE invite

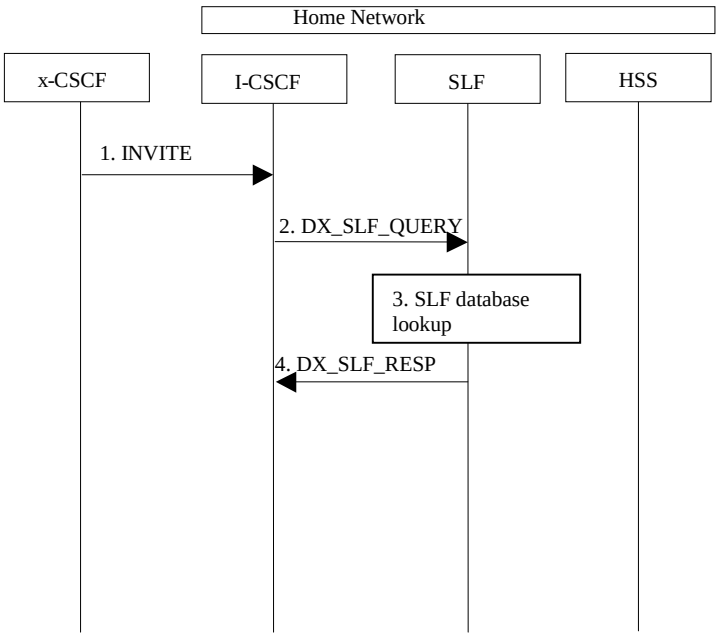


Figure 5.21: SLF on UE invite

1. I-CSCF receives an INVITE request and now has to query for the location of the user's subscription data.

2. The I-CSCF sends a DX_SLF_QUERY to the SLF and includes as parameter the user identity which is stated in the INVITE request. If the user identity is an E.164 number in the SIP URI with user=phone parameter format the I-CSCF shall first translate it into the Tel: URI format per IETF RFC 3966 [15] prior to sending to the SLF the DX_SLF_QUERY.

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

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

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

5.8.4 SLF on AS access to HSS

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

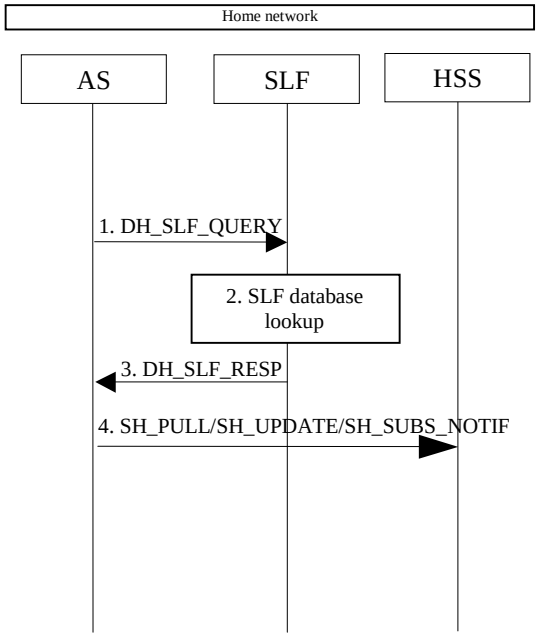


Figure 5.21a: SLF on AS access to HSS

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

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

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

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

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

5.10.0 General

This clause 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 Terminal initiated session release

The following flow shows a 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 Policy and Charging Control is in use.

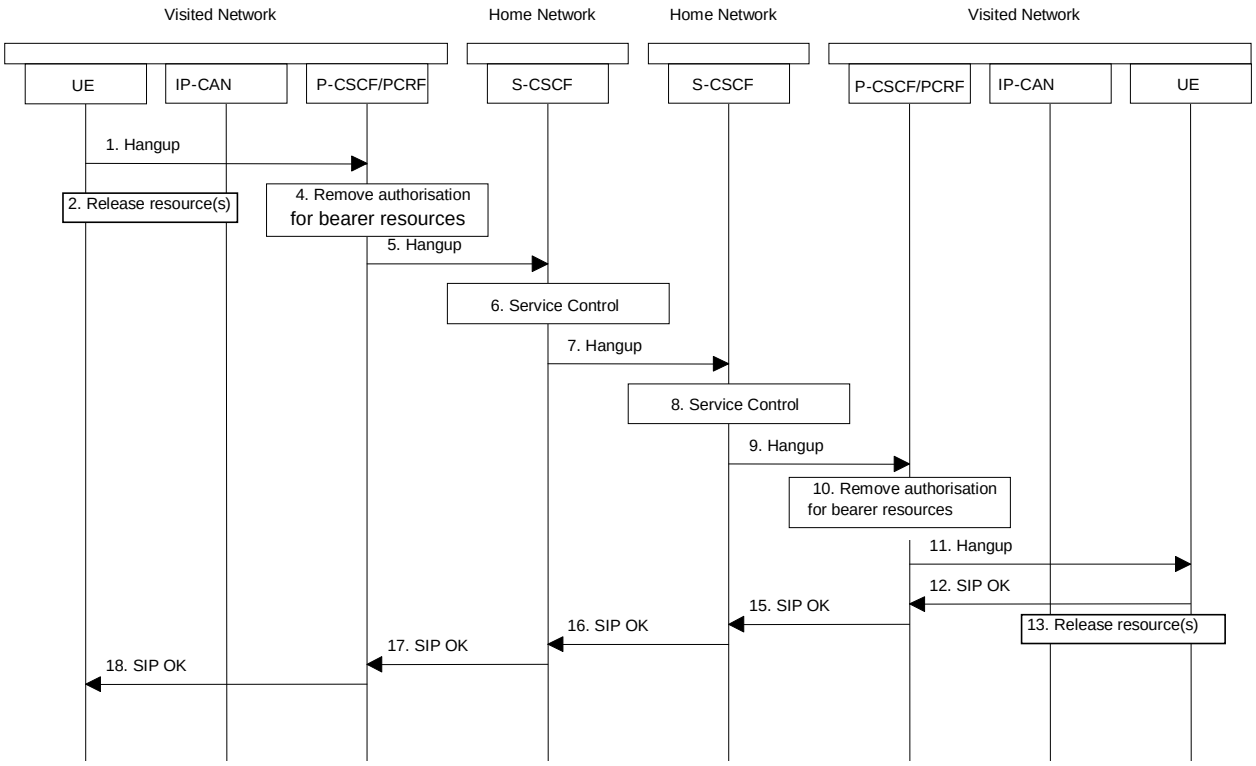


Figure 5.22: Terminal initiated session release

1. One party hangs up, which generates a message (Bye message in SIP) from the UE to the P-CSCF.
2. Depending on the bearer establishment mode selected for the IP-CAN session, release resource(s) shall be initiated either by the UE or by the IP-CAN itself. The UE initiates the release procedures for the resources used for this session as shown in Figure 5.22. Otherwise, the IP-CAN initiates the release of used resources after step 4.
3. Void.
4. The P-CSCF instruct the PCRF/PCF to remove the authorization for resources that had previously been issued for this endpoint for this session. This step will also result in a release indication to the IP-CAN to confirm that the IP bearers associated with the session have been deleted.
5. The P-CSCF sends a Hangup to the S-CSCF of the releasing party.
6. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.
7. The S-CSCF of the releasing party forwards the Hangup to the S-CSCF of the other party.
8. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.
9. The S-CSCF of the other party forwards the Hangup on to the P-CSCF.
10. The P-CSCF instructs the PCRF/PCF to remove the authorization for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the UE#2 session have been deleted.
11. The P-CSCF forwards the Hangup on to the UE.
12. The terminal responds with an acknowledgement, the SIP OK message (number 200), that is sent back to the P-CSCF.
13. Depending on the bearer establishment mode selected for the IP-CAN session, release resource(s) shall be initiated either by the UE or by the IP-CAN itself. The UE initiates the release procedures for the resources used for this session as shown in Figure 5.22. Otherwise, the IP-CAN initiates the release of used resources after step 11.

14 Void.

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 Policy and Charging Control is used.

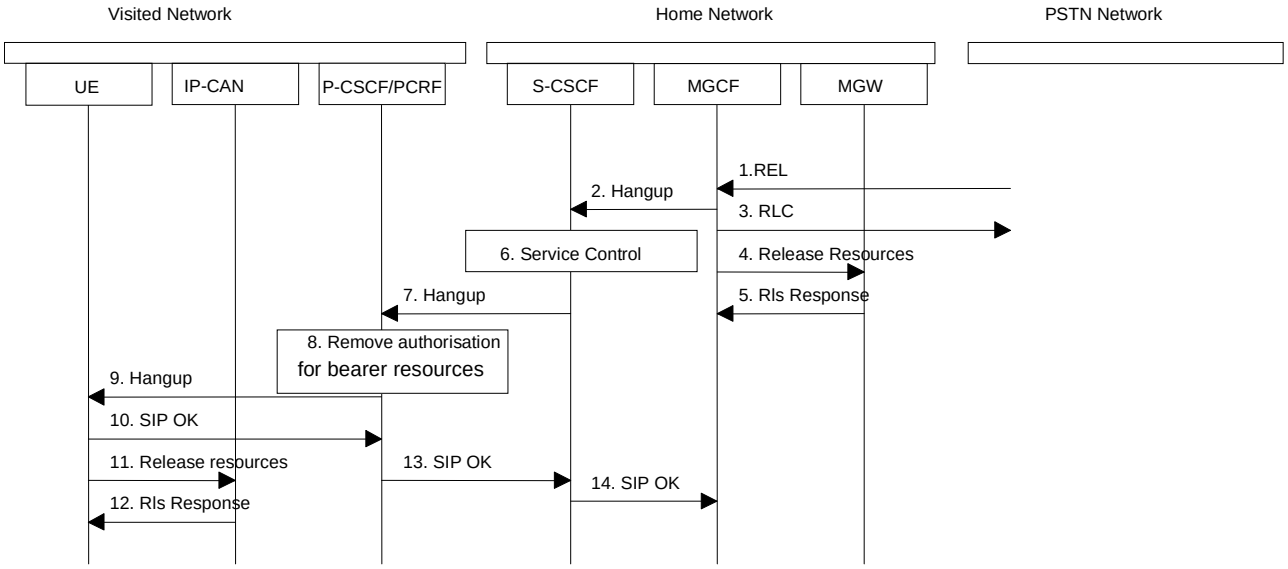


Figure 5.23: PSTN initiated session release

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 terminal 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 4.

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

7. The S-CSCF forwards the Hangup to the P-CSCF.

8. The P-CSCF instructs the PCRF/PCF to remove the authorization for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the UE#2 session have been deleted.

9. The P-CSCF forwards the Hangup to the UE.

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

11-12. The IP network resources that had been reserved for the message receive path to the endpoint for this session are released, taking into account the bearer establishment mode used for the IP-CAN session. Steps 11and 12 may be done in parallel with step 10. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would be 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 Removal of IP-CAN bearer used to transport IMS SIP signalling

It is possible that the IP-CAN removes the IP-CAN bearer used to transport IMS SIP signalling (e.g. due to overload situations).

In this case the UE or network shall initiate a procedure to re-establish (or modify where possible) an IP-CAN bearer to transport IMS SIP signalling. After the re-establishment of an IP-CAN bearer the UE should perform a re-registration to the IMS.

If the re-establishment (or the modification) fails then the UE or network shall de-activate all other IMS related IP-CAN bearer(s).

The deactivation of the IP-CAN bearer(s) results in the P-CSCF being informed via PCRF/PCF of the IP-CAN bearer release P-CSCF may, depending on policy, initiate a network initiated session release as described in clause 5.10.3.1.

The failure in re-establishing the ability to communicate towards the UE results also in the P-CSCF/PCRF/PCF being informed that the IMS SIP signalling transport to the UE is no longer possible which shall lead to a network initiated session release (initiated by the P-CSCF) as described in clause 5.10.3.1 if any IMS related session is still ongoing for that UE. Additionally, the P-CSCF shall reject subsequent incoming session requests towards the remote endpoint indicating that the user is not reachable, until either:

- the registration timer expires in P-CSCF and the user is de-registered from IMS.
- a new Register message from the UE is received providing an indication to the P-CSCF that the IMS SIP signalling transport for that user has become available again and session requests can be handled again.

The P-CSCF shall not assume that the IMS SIP signalling transport is lost unless the P-CSCF receives a notification of loss of signalling connectivity from the PCRF/PCF as defined in this clause. The P-CSCF shall not reject subsequent incoming session requests towards the remote endpoint based upon notification of other events e.g. upon PCRF/PCF notification of loss of a media bearer or upon the failure to deliver an INVITE message to the UE.

5.10.3.1 Network initiated session release - P-CSCF initiated

5.10.3.1.0 General

This clause assumes that Policy and Charging Control is applied

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

A bearer is removed e.g. triggered by a UE power down, due to a previous loss of coverage, or accidental/malicious removal, etc. In this case an IP-CAN session modification procedure (GW initiated) will be performed (see TS 23.203 [54] and TS 23.503 [95]). The flow for this case is shown in Figure 5.26.

Other network initiated session release scenarios are of course possible.

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

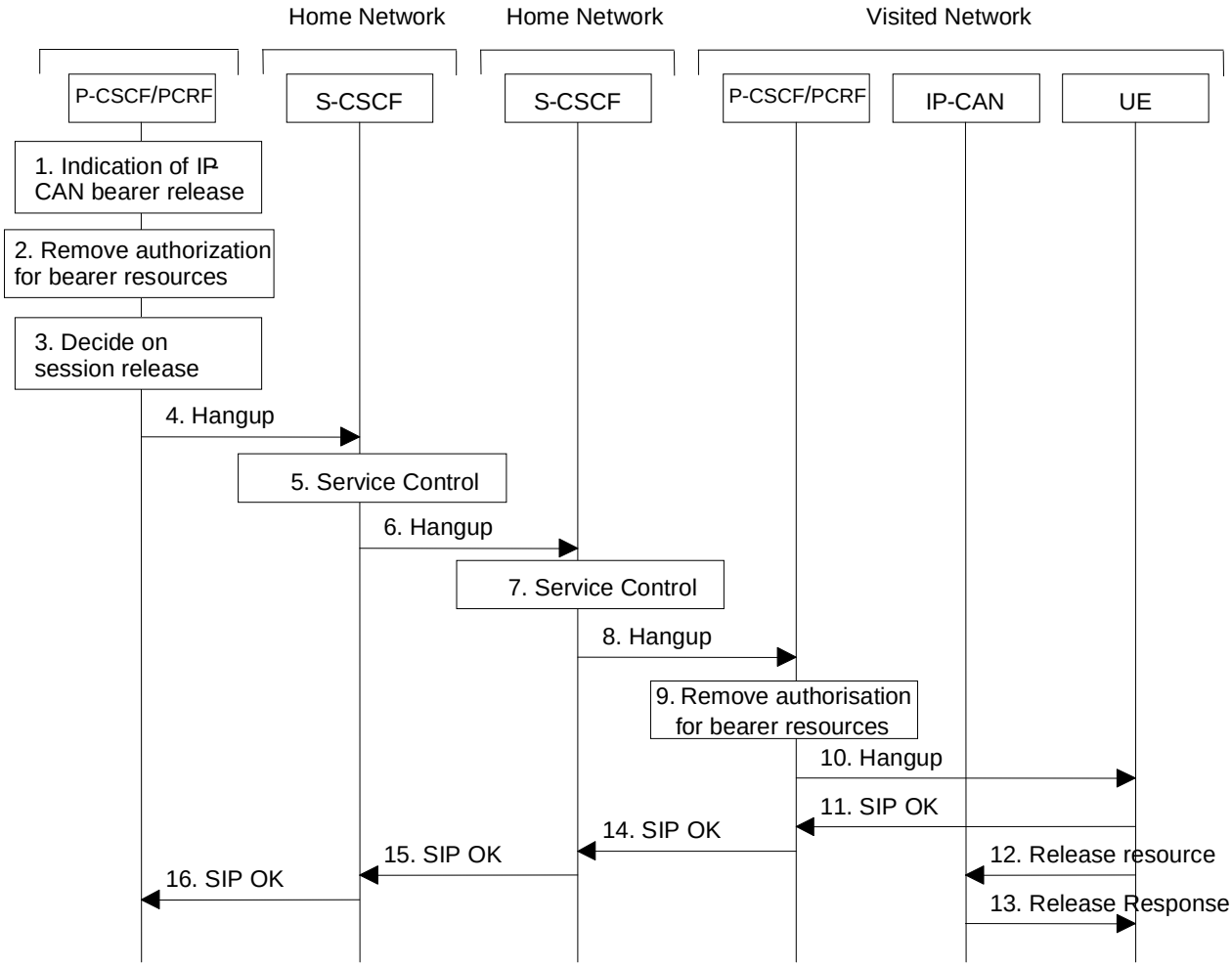


Figure 5.26: Network initiated session release - P-CSCF initiated – after removal of IP-CAN bearer

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

2. The P-CSCF instructs PCRF/PCF to remove the authorization for resources related to the released bearer that had previously been issued for this endpoint for this session (see TS 23.203 [54] and TS 23.503 [95]). It is optional for the P-CSCF to instruct PCRF/PCF to deactivate additional IP-CAN bearers (e.g. an IP-CAN bearer for chat could still be allowed).

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. In the event of the notification that the signalling transport to the UE is no longer possible, the P-CSCF shall terminate any ongoing session with that specific UE.

   If the P-CSCF decides to terminate the session, then the P-CSCF instructs the PCRF/PCF to remove the authorization for resources that has previously been issued for this endpoint for this session (see TS 23.203 [54] and TS 23.503 [95]).

The following steps are only performed if the P-CSCF has decided to terminate the session.

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

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

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

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

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

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

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

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

12-13. Steps 12 and 13 may be done in parallel with step 11. The IP network resources that had been reserved for the UE for this session are released, taking into account the bearer establishment mode used for the IP-CAN session. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would be invoked here.

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

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

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

5.10.3.1.2 Void

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 Policy and Charging Control is in use.

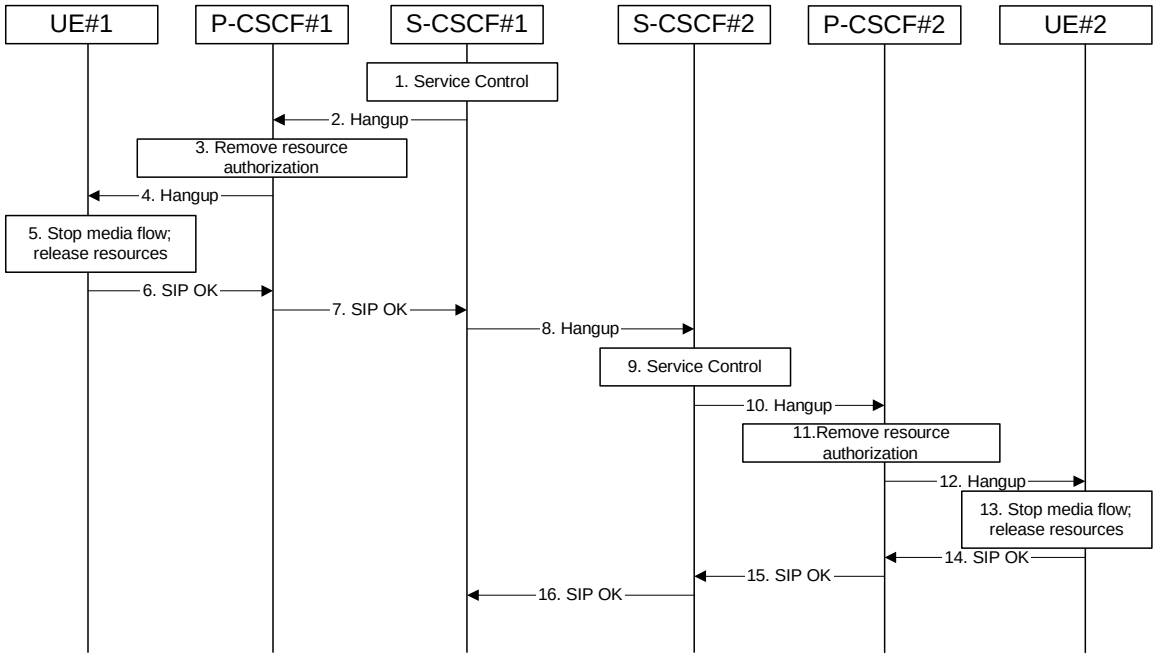


Figure 5.27: Network initiated session release - S-CSCF initiated

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 authorization for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the session have been deleted for UE#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 the resources used for the session are released taking into account the bearer establishment mode used for the IP-CAN 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 authorization for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the session have been deleted for UE#2.
12. P-CSCF#2 forwards the Hangup message to UE#2.
13. UE#2 stops sending the media stream to the remote end point, and the resources used for the session are released taking into account the bearer establishment mode used for the IP-CAN 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

5.11.1.0 General

This clause gives information flows for the procedures for placing sessions on hold that were previously established by the mechanisms of clauses 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 clause.

5.11.1.1 Mobile-to-Mobile Session Hold and Resume Procedures

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

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

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

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

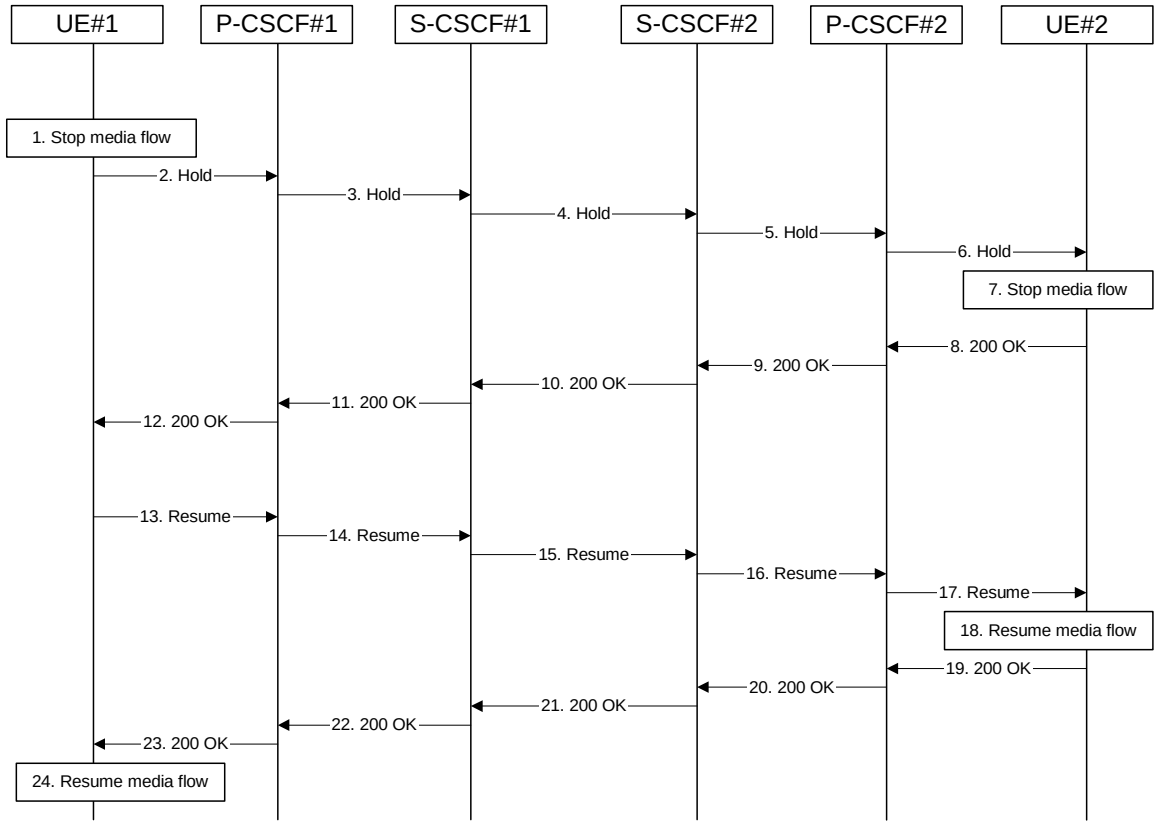


Figure 5.28: Mobile to Mobile session hold and resume

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, an S-CSCF assigned in its home network, and a BGCF that chooses the MGCF. The procedures are independent of whether the P-CSCF is located in the subscriber's home or visited network. Therefore there is no distinction in this clause 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:

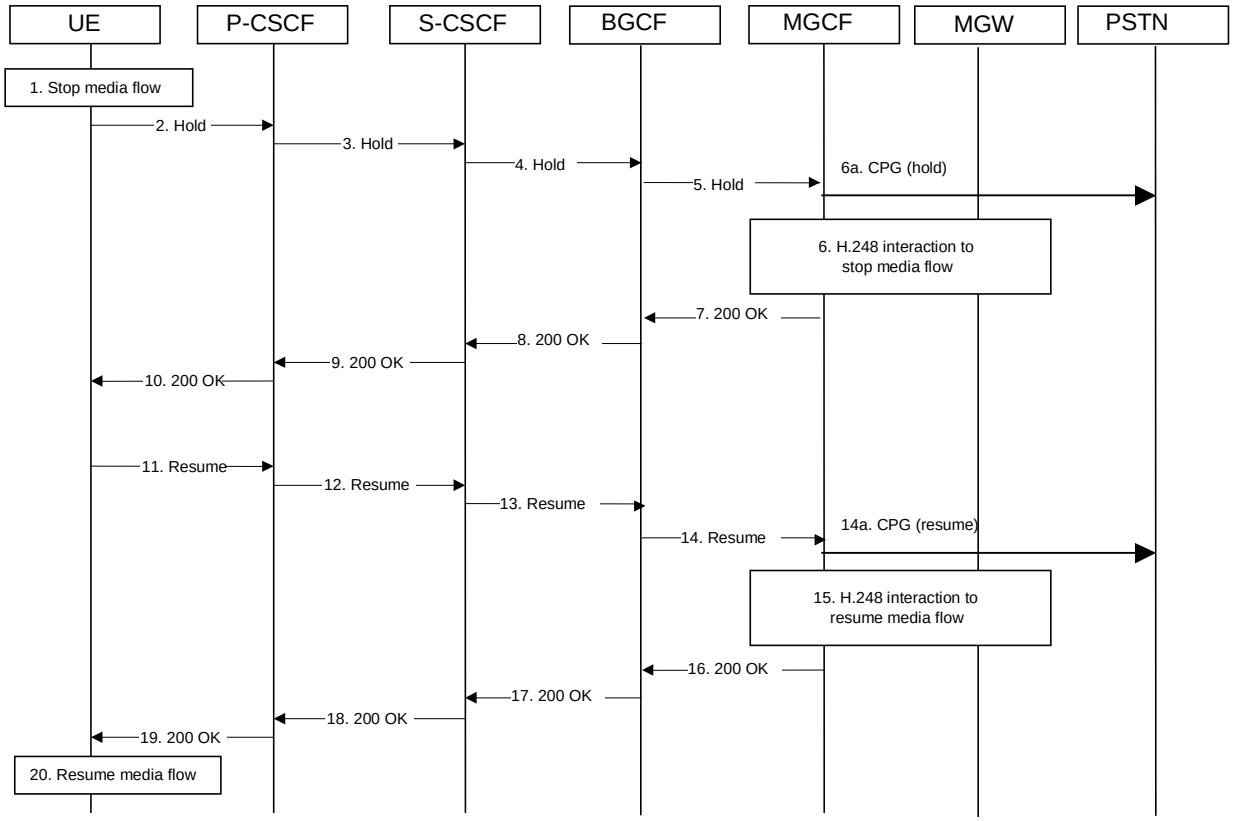


Figure 5.29: Mobile-initiated Hold and Resume of a Mobile-PSTN Session

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.

5a MGCF sends a CPG(hold) in order to express that the call has been placed on hold.

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.

14a. MGCF sends a CPG(resume) in order to resume the call.

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.

5.11.1.3 PSTN-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, an S-CSCF assigned in its home network, and a BGCF that chooses the MGCF. The procedures are independent of whether the P-CSCF is located in the subscriber's home or visited network. Therefore there is no distinction in this clause 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 following information flow shows the procedures, where the session is set on hold from the PSTN side:

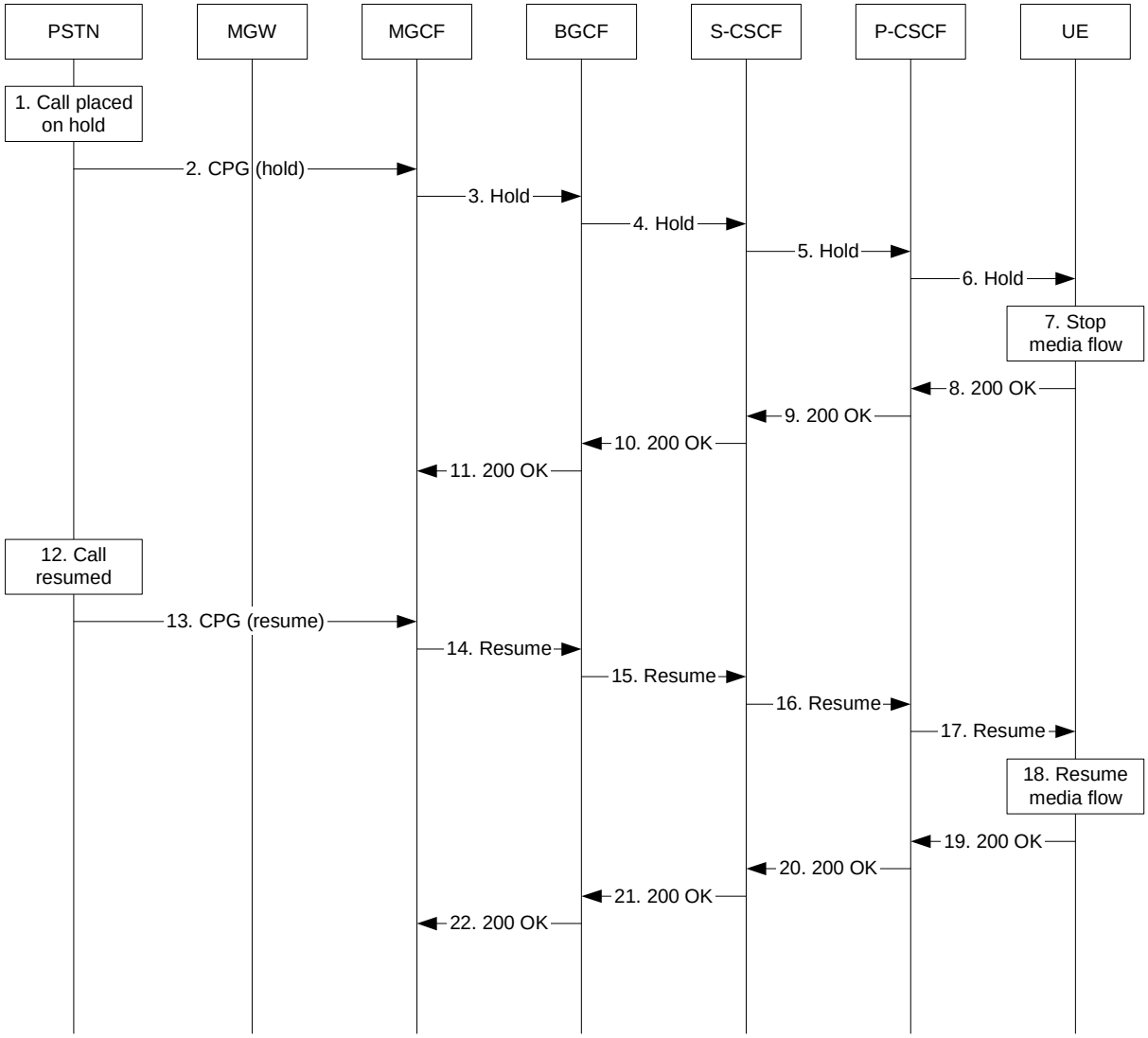


Figure 5.29a: PSTN-initiated Hold and Resume of a Mobile-PSTN Session

Information flow procedures are as follows:

1. The call is placed on hold in the PSTN.
2. The MGCF receives a CPG (hold) from the PSTN, which indicates that the call has been placed on hold.
3. MGCF sends a Hold message to BGCF.
4. BGCF forwards the Hold message to S-CSCF.
5. S-CSCF forwards the Hold message to P-CSCF.
6. P-CSCF forwards the Hold message to the UE.
7. UE stops sending the media stream to the remote endpoint, but keeps the resources for the session reserved.
8. The UE acknowledges receipt of the Hold message with a 200-OK final response, send to P-CSCF.
9. P-CSCF forwards the 200-OK final response to S-CSCF.
10. S-CSCF forwards the 200 OK final response to BGCF.
11. BGCF forwards the 200 OK final response to MGCF.
12. The call is resumed in the PSTN.

13. MGCF receives a CPG (resume) request from the PSTN, which indicates that the call is resumed.
14. MGCF sends a resume message to BGCF.
15. BGCF forwards the Resume message to S-CSCF.
16. S-CSCF forwards the Resume message to P-CSCF.
17. P-CSCF forwards the Resume message to UE.
18. UE resumes sending the media stream to the remote endpoint.
19. UE acknowledges receipt of the Resume message with a 200-OK final response, sent to P-CSCF.
20. P-CSCF forwards the 200 OK final response to the S-CSCF.
21. S-CSCF forwards the 200 OK final response to BGCF.
22. BGCF forwards the 200 OK final response to MGCF.

5.11.2 Procedures for anonymous session establishment

5.11.2.0 General

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

The purpose of the mechanism is to give an IMS user the possibility to withhold certain identity information as specified in IETF RFC 3323 [39] and IETF RFC 3325 [40].

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

IMS entities shall determine whether they are communicating with an element of the same Trust Domain for Asserted Identity or not as described in IETF RFC 3325 [40].

5.11.2.1 Signalling requirements for anonymous session establishment

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

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

5.11.2.2 Bearer path requirements for anonymous session establishment

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

5.11.3 Procedures for codec and media characteristics flow negotiations

5.11.3.0 General

This clause gives information flows for:

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

5.11.3.1 Codec and media characteristics flow negotiation during initial session establishment

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

The session initiator includes an SDP in the SIP INVITE message that lists every media characteristics (including codecs) that the originator is willing to support for this session. When the message arrives at the destination endpoint, it responds with the media characteristics (e.g. common subset of codecs) that it is also willing to support for the session. Media authorization 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 clause 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 clause 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 Policy and Charging Control is in use.

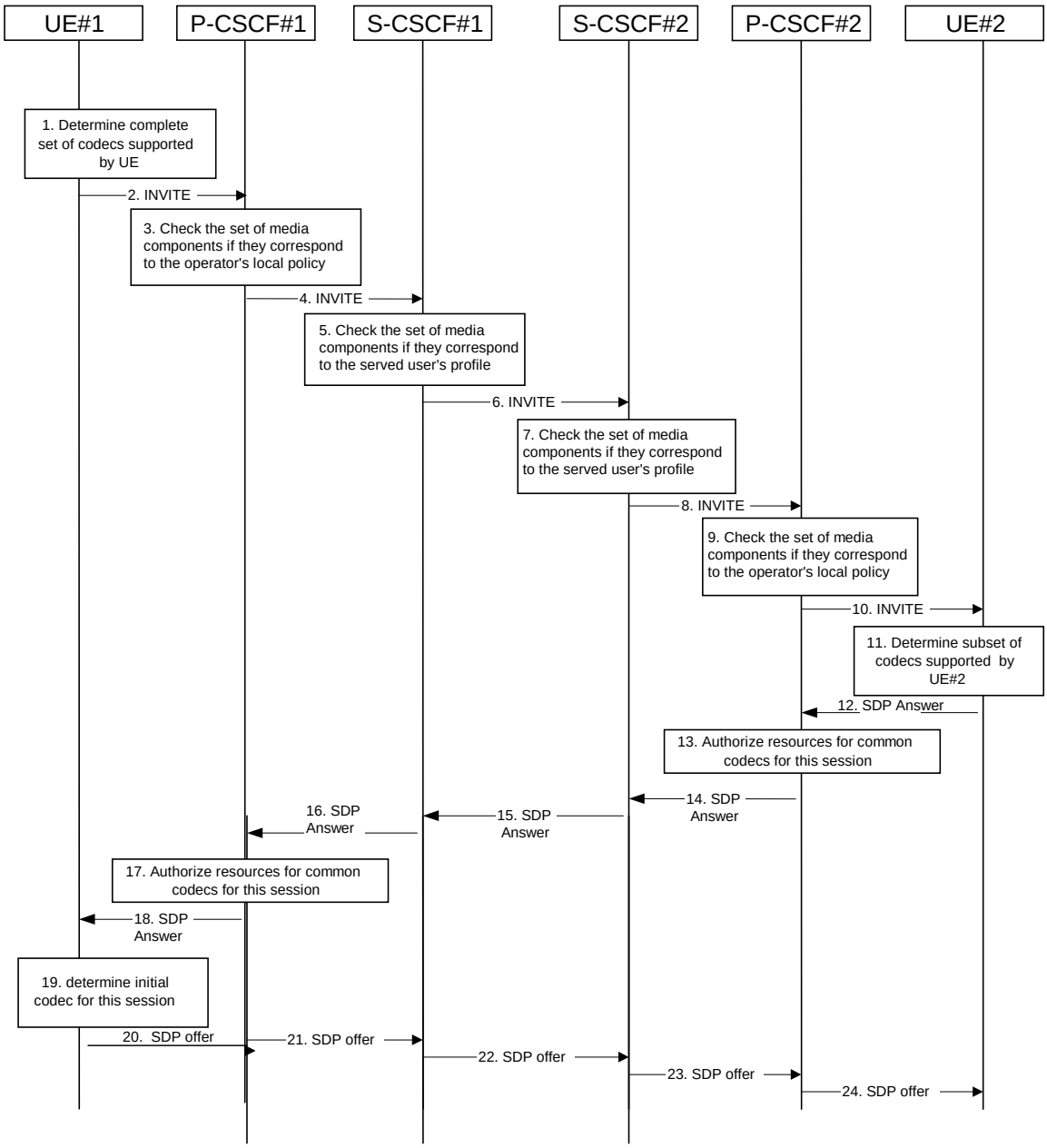


Figure 5.30: Codec negotiation during initial session establishment

The detailed procedure is as follows:

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

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

3. P-CSCF#1 examines the media parameters. If P-CSCF#1 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies, or if available bandwidth authorization limitation information coming from the PCRF/PCF), 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 IETF RFC 3261 [12].
   In this flow described in Figure 5.30 above the P-CSCF#1 allows the initial session initiation attempt to continue.

NOTE 1: Whether the P-CSCF should interact with PCRF/PCF in this step is based on operator policy.

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 IETF 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 IETF RFC 3261 [12].
   In this flow described in Figure 5.30 above the S-CSCF#2 allows the initial session initiation attempt to continue.

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

9. P-CSCF#2 examines the media parameters. If P-CSCF#2 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies, or if available bandwidth authorization limitation information coming from the PCRF/PCF), 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 IETF RFC 3261 [12].
   In this flow described in Figure 5.30 above the P-CSCF#2 allows the initial session initiation attempt to continue.

NOTE 2: Whether the P-CSCF should interact with PCRF/PCF in this step is based on operator policy.

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

13. P-CSCF#2 authorizes 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 authorizes the QoS resources 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 need to renegotiate the codecs by sending another offer to reduce codec to one with the UE#2.

20-24. UE#1 sends the "Offered SDP" message to UE#2, along the signalling path established by the INVITE request

The remainder of the multi-media session completes identically to a single media/single codec session, if the negotiation results in a single codec per media.

5.11.3.2 Codec or media characteristics flow change within the existing reservation

After the multi-media session is established, it is possible for either endpoint to change the set of media flows or media characteristics (e.g. codecs) for media flows. If the change is within the resources already reserved, then it is only necessary to synchronise the change with the other endpoint. Note that an admission control decision will not fail if the new resource request is within the existing reservation.

The flow presented here assumes that Policy and Charging Control is in use.

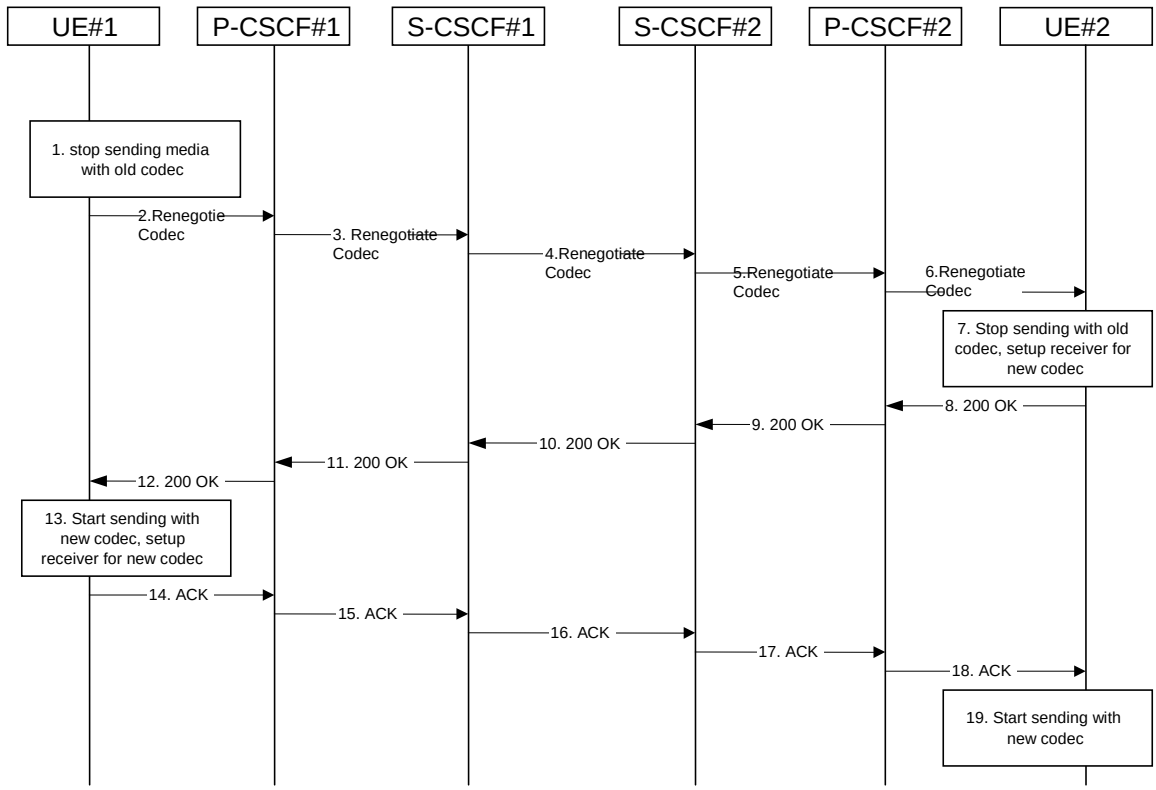


Figure 5.31: Codec or media flow change - same reservation

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 authorized, 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 authorization

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 Policy and Charging Control is in use.

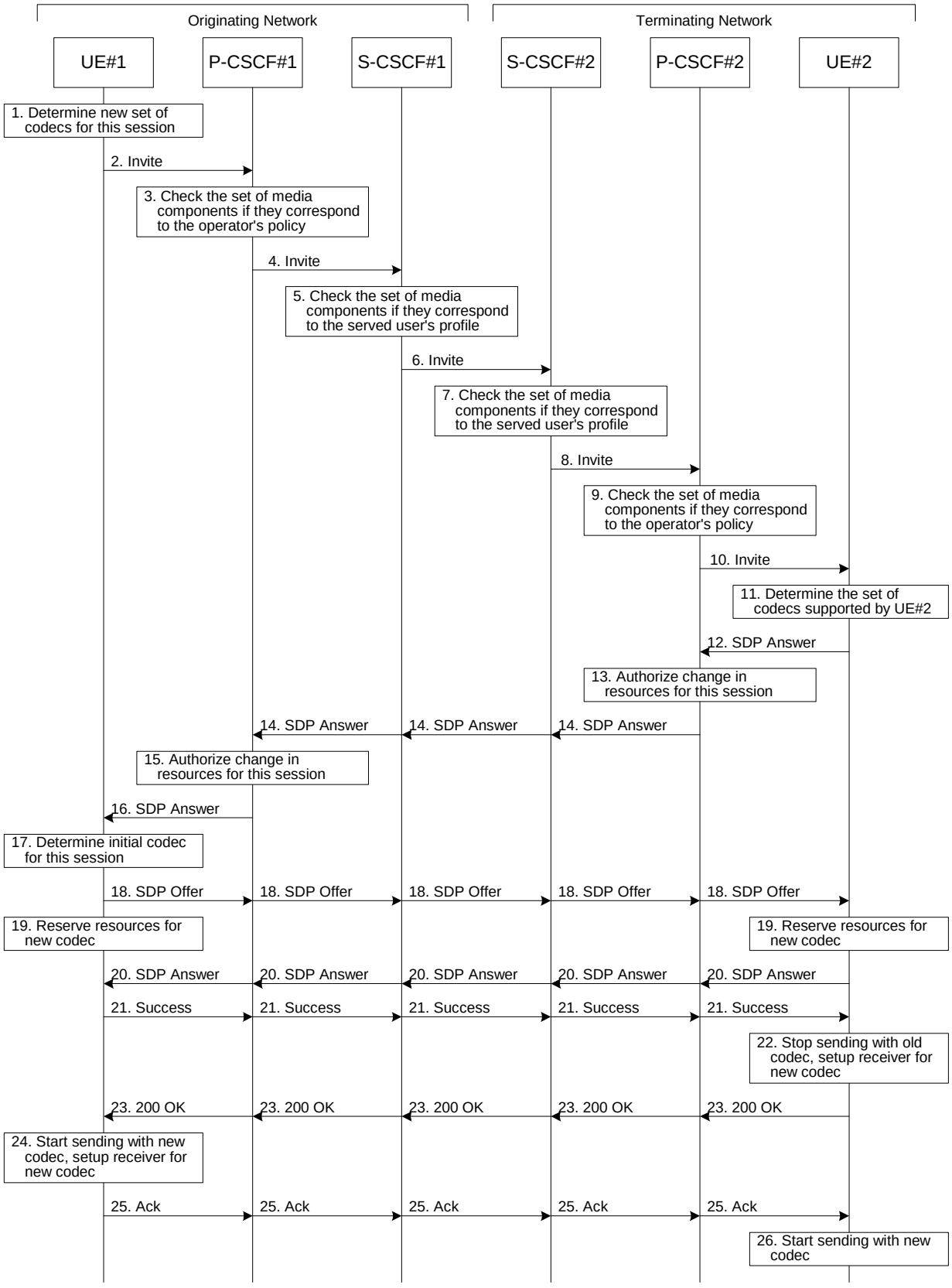


Figure 5.32: Codec or media flow change - new reservation

The detailed procedure is as follows:

1. UE#1 inserts the revised set of codecs to a SDP payload. The inserted codec(s) shall reflect the UE#1's terminal capabilities and user preferences for the session. It builds a SDP containing bandwidth requirements and

characteristics of each, and assigns local port numbers for each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.

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

3. P-CSCF#1 examines the media parameters. If P-CSCF#1 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies, or if available bandwidth authorization limitation information coming from the PCRF/PCF), 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 IETF RFC 3261 [12].
In this flow described in Figure 5.32 above the P-CSCF#1 allows the initial session modification attempt to continue.

NOTE 1: Whether the P-CSCF interacts with PCRF/PCF in this step is based on operator policy.

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 IETF 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 IETF RFC 3261 [12].
In this flow described in Figure 5.32 above the S-CSCF#2 allows the initial session modification attempt to continue.

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

9. P-CSCF#2 examines the media parameters. If P-CSCF#2 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies, or if available bandwidth authorization limitation information coming from the PCRF/PCF), 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 IETF RFC 3261 [12].
In this flow described in Figure 5.32 above the P-CSCF#2 allows the initial session modification attempt to continue.

NOTE 2: If session modification request indicates no requirements for resource reservation or that the required resources are already available on the originating side, the P-CSCF#2 can send updated session information to PCRF/PCF whenever SDP offer is contained in the session establishment request, as in such cases no SDP answer is received before the PCRF/PCF is requested to authorize the required QoS resources. Otherwise, whether the P-CSCF interacts with PCRF/PCF in this step is based on operator policy.

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 authorization for the QoS resources, if needed, for the remaining media flows and codec choices.

NOTE 3: P-CSCF can additionally authorize the resources in step 9.

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

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

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

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

18. UE#1 sends the offered SDP message to UE#2, including the SDP from step #17 if needed.

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

20. If UE#1 has sent an updated offer of SDP in step 18, then UE#2 responds to the offer and P-CSCF#1 authorizes the offered SDP sent by UE#2.

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

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

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

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

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

26. 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 Policy and Charging Control is in use.

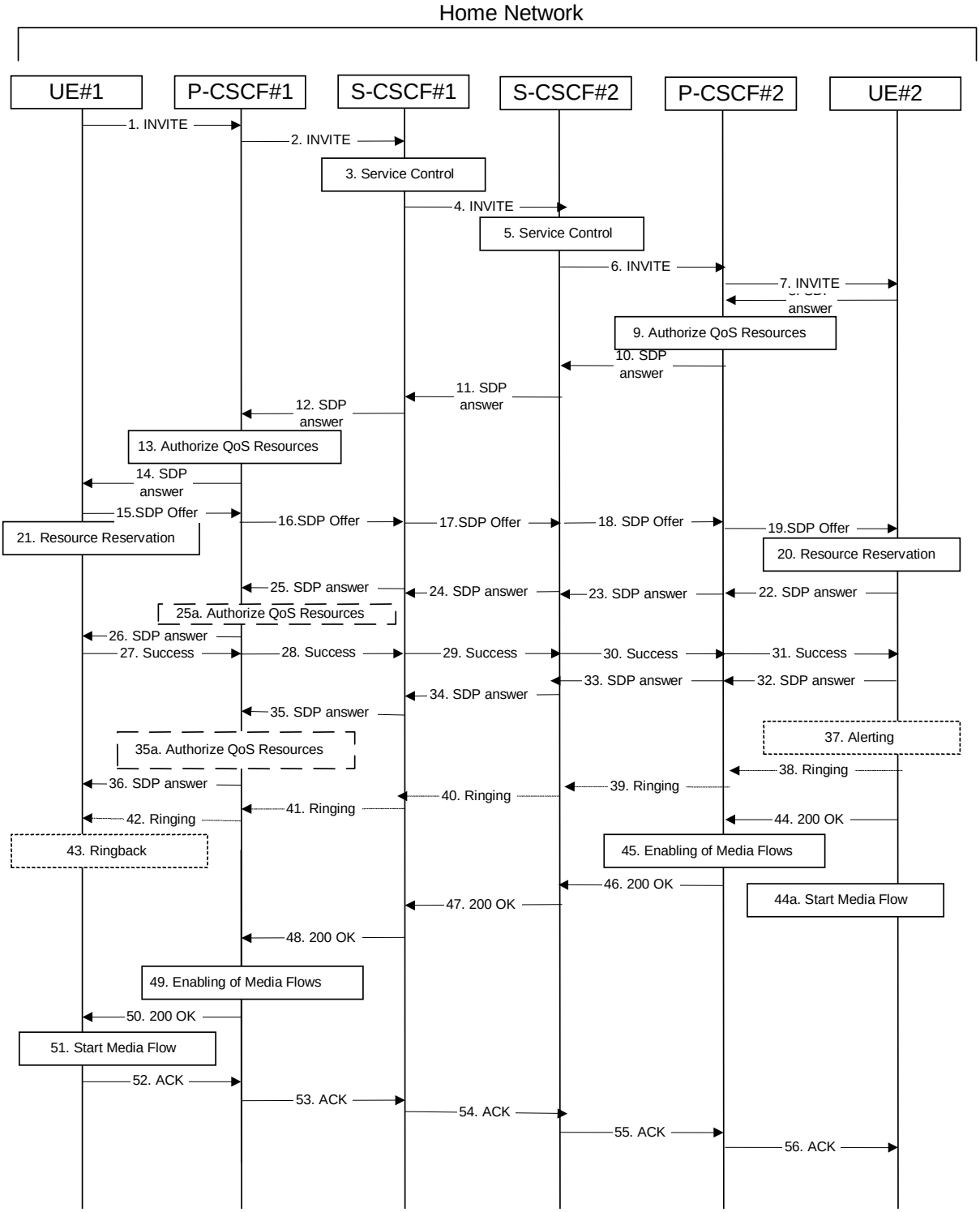


Figure 5.33: Multimedia session flow - addition of another media

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.

NOTE 1: If session modification request indicates no requirements for resource reservation or that the required resources are already available on the originating side, the P-CSCF#2 can send updated session information to PCRF/PCF whenever SDP offer is contained in the session establishment request, as in such cases no SDP answer is received before the PCRF/PCF is requested to authorize the required QoS resources. Otherwise, whether the P-CSCF interacts with PCRF/PCF in this step is based on operator policy.

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 authorizes the QoS resources required for this additional media.

NOTE 2: P-CSCF can additionally authorize the resources in step 7.

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 authorizes 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. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. UE#2 initiates the resource reservation procedures for the resources necessary for this additional media as shown in figure 5.33. Otherwise, the IP-CAN initiates the reservation of required resources after step 9.

21. Depending on the bearer establishment mode selected for the IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. After determining the offered set of media streams for this additional media, in step #15 above, UE#1 initiates the reservation procedures for the additional resources needed for this new media as shown in figure 5.33. Otherwise, the IP-CAN#1 initiates the reservation of required resources after step 13.

22-25. When the terminating side has successfully reserved the needed resources, it sends the "reservation successful" message to UE#1 along the signalling path established by the INVITE message. The message is sent first to P-CSCF#1.

25a. P-CSCF#1 authorizes 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 authorizes 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.S-CSCF#2 invokes whatever service logic is appropriate for this ringing flow.

40. S-CSCF#2 forwards the message to S-CSCF#1.

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 enables the media flows authorized for this additional media.

46. P-CSCF#2 forwards the final response to S-CSCF#2.

47. S-CSCF#2 forwards the final response to S-CSCF#1.

48. S-CSCF#1 forwards the final response to P-CSCF#1.

49. P-CSCF#1 enables the media flows authorized for this additional media.

50. P-CSCF#1 forwards the final response to UE#1.

51. UE#1 starts the media flow(s) for this additional media.

52. UE#1 responds to the final response with a SIP ACK message, which is passed to the destination via the signalling path. The message is sent first to P-CSCF#1.

53. P-CSCF#1 forwards the ACK to S-CSCF#1

54. S-CSCF#1 forwards the ACK to S-CSCF#2.

55. S-CSCF#2 forwards the ACK to P-CSCF#2.

56. P-CSCF#2 forwards the ACK to UE#2.

5.11.4 Procedures for providing or blocking identity

5.11.4.0 General

Identity is composed of a Public User Identity and an optional display name:

- The Public User Identity is used by any user for requesting communications to other users (see clause 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 clause gives information flows for the procedures for providing the authenticated Public User Identity and the optional display Name information of the originating party to the terminating party. It also describes the mechanisms for blocking the display of Public User Identity and optional display name if requested by the originating party.

5.11.4.1 Procedures for providing the authenticated identity of the originating party

Authentication of the subscriber is performed during the registration procedures, as described in clause 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. As part of this procedure, the display name associated with each Public User Identity, if provided by the

HSS, is also returned via the S-CSCF and stored in the 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, the UE shall include one of the Public User Identities the UE received during the SIP registration in the INVITE request. The P-CSCF#1 ensures that the INVITE request includes an authenticated Public User Identity, including the associated display name if provided by the S-CSCF during the registration procedures, before forwarding the INVITE request to the S-CSCF#1.

In the following call flow, it is assumed that no privacy has been required by UE#1.If the Public User Identity supplied by UE#1 in the INVITE request is incorrect, or if the UE did not provide a public identify, then the P-CSCF may reject the request, or may overwrite with the correct URI, including the associated display name if provided by the S-CSCF during the registration procedures.

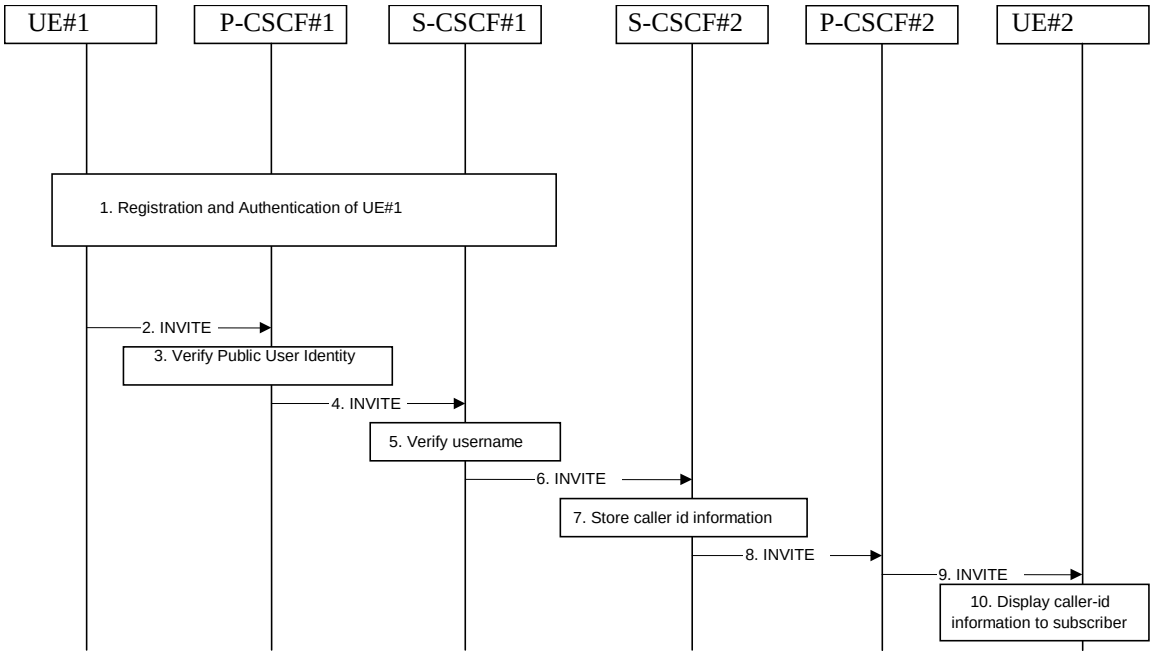


Figure 5.34: Providing the authenticated Identity of the originating party

The detailed procedure is as follows:

1. Registration and authentication of UE#1 is performed. One or more authenticated identities for UE#1, including display names if provided, are stored in the P-CSCF#1 and the UE.

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. If provided during registration procedures via the S-CSCF, the P-CSCF#1 ensures that the display name associated with the verified Public User Identity is present before forwarding the INVITE request.

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

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

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

7. S-CSCF#2 stores the Public User Identity and associated information.

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

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

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

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).

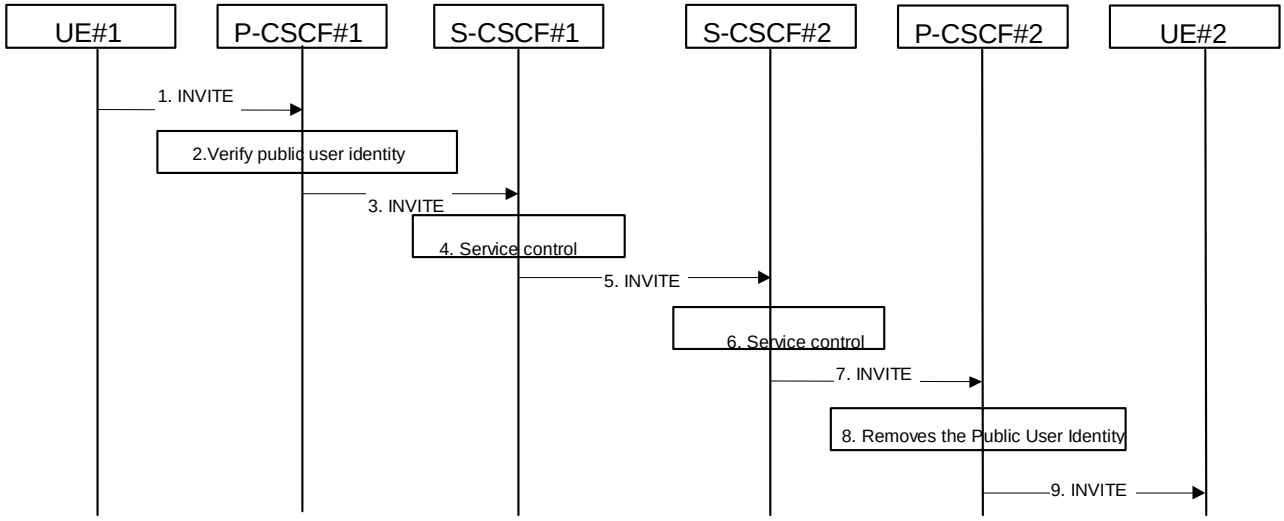


Figure 5.35: Blocking the identity of the originating party

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. If provided during registration procedures, the P-CSCF#1 ensures that the display name associated with the Public User Identity is present before forwarding the INVITE request.

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

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

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

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

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

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

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

5.11.4.3 Procedures for providing the authenticated identity of the originating party (PSTN origination)

For calls originating from the PSTN, the MGCF extracts information received from the PSTN and inserts an asserted identity into the SIP message. If the incoming information includes the calling name, or the MGCF can obtain the calling name, the MGCF may insert the information into the display name portion of the asserted identity.

The MGCF must propagate the privacy indicators received from the PSTN in the SIP message.

5.11.4.4 Procedures for providing the authenticated identity of the originating party (PSTN termination)

For calls terminating to the PSTN, the MGCF extracts information received in the SIP message and inserts the information into the PSTN signalling. This information must include the privacy setting and may include the display name.

5.11.5 Session Redirection Procedures

5.11.5.0 General

This clause 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:

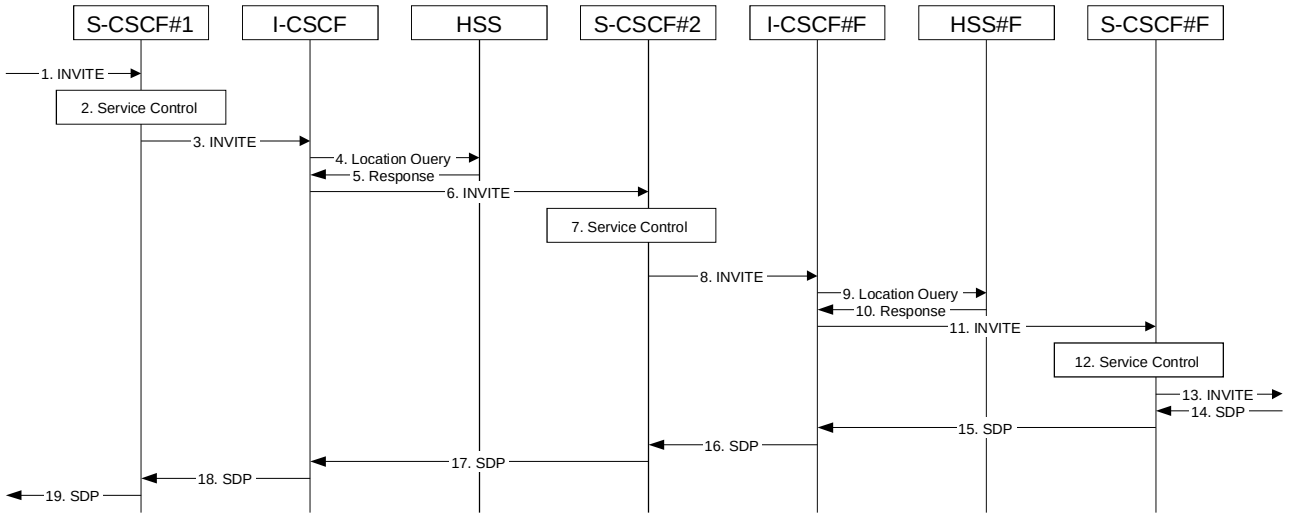


Figure 5.36: Session redirection initiated by S-CSCF to IMS

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.
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 URI within the IP Multimedia Subsystem. Based on operator policy and the user profile, S-CSCF#2 may restrict the media streams allowed in the redirected session.
8. S-CSCF#2 sends a SIP INVITE request to an I-CSCF (I-CSCF#F) for the network operator to whom the forwarded destination subscribes.
9. I-CSCF#F queries the HSS (HSS#F) for current location information of the destination user.
10. HSS#F responds with the address of the current Serving CSCF (S-CSCF#F) for the terminating user.
11. I-CSCF forwards the INVITE request to S-CSCF#F, who will handle the session termination.
12. S-CSCF#F invokes whatever service logic is appropriate for this session setup attempt
13. S-CSCF#F forwards the INVITE toward the destination UE, according to the procedures of the terminating flow.

14-19. The destination UE responds with the SDP message, and the session establishment proceeds normally.

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

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

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

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

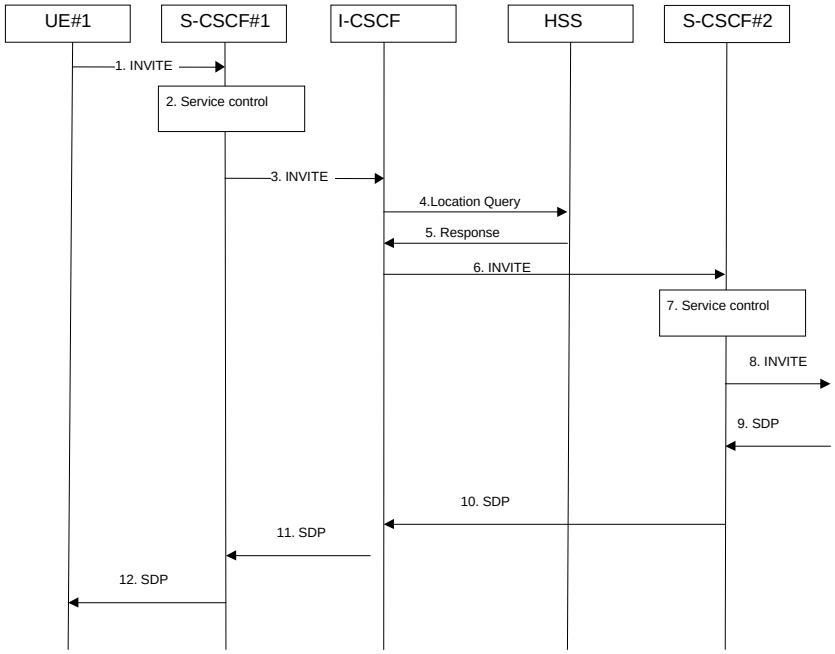


Figure 5.37: Session redirection to PSTN Termination (S-CSCF #2 forwards INVITE)

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE #1 to S-CSCF#1 by the procedures of the originating flow.
2. S-CSCF#1 performs whatever service control logic is appropriate for this session setup attempt.
3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. The INVITE message is sent to an I-CSCF for that operator.
4. I-CSCF queries the HSS for current location information of the destination user.
5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.
6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.
7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a PSTN termination. S-CSCF#2 determines that it wishes to remain in the path of the SIP signalling.
8. S-CSCF#2 forwards the INVITE using the Serving to Serving procedures S-S#3 or S-S#4. The PSTN terminating flows are then followed.

9-12. The destination responds with the SDP message, and the session establishment proceeds normally.

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

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

5.37a, or it may be any other type of originating entity as defined in clause 5.4a. The endpoint to which the session is redirected may be the PSTN as shown in figure 5.37a, or it may be any other type of terminating entity as defined in clause 5.4a. The originator may alternately receive a redirect from a non-IMS network SIP client. Only the scenario in which a call from a UE is redirected by S-CSCF service logic to a PSTN endpoint is shown.

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

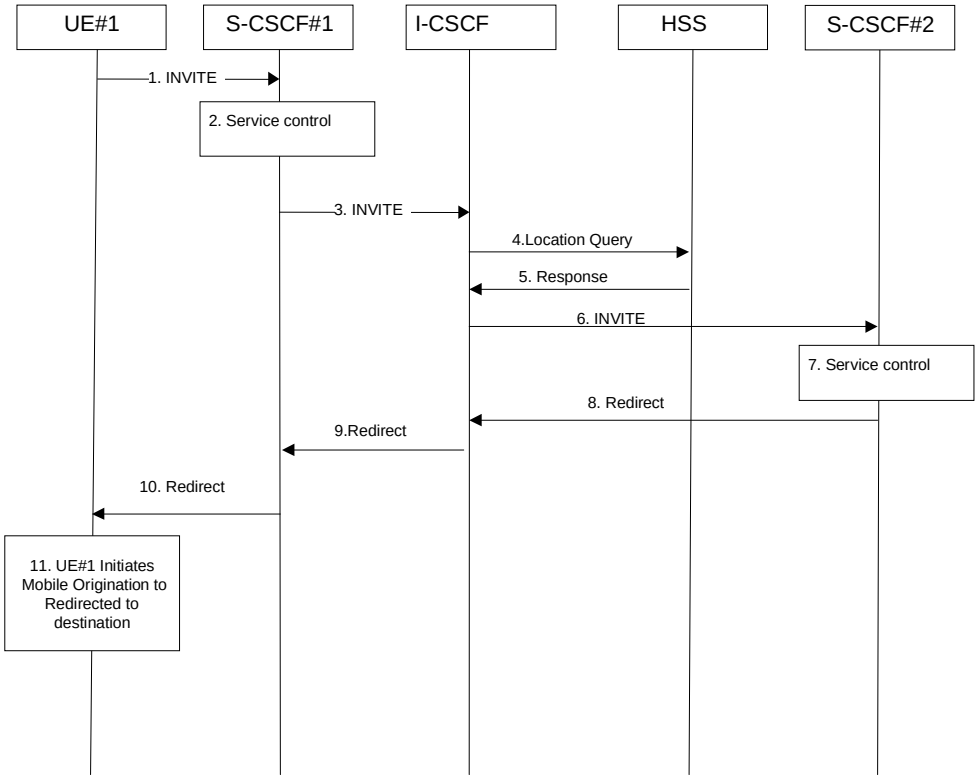


Figure 5.37a: Session redirection to PSTN Termination (REDIRECT to originating UE#1)

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE#1 to S-CSCF#1 by the procedures of the originating flow.
2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt.
3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. The INVITE message is sent to an I-CSCF for that operator.
4. I-CSCF queries the HSS for current location information of the destination user.
5. HSS responds with the address of the current Serving CSCF (S-CSCF#2) for the terminating user.
6. I-CSCF forwards the INVITE request to S-CSCF#2, who will handle the session termination.
7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt. As a result of this service control logic, S-CSCF#2 determines that the session should be redirected to a PSTN termination.
   S-CSCF#2 determines that it wishes to use the SIP REDIRECT method to pass the redirection destination information (the 'redirected-to PSTN Termination' information) to the originator (UE#1).
8. S-CSCF#2 sends a SIP Redirect response to I-CSCF with the redirection destination.
9. I-CSCF sends a Redirect response to S-CSCF#1, containing the redirection destination.
10. S-CSCF#2 forwards the Redirect response to UE#1, containing the redirection destination

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

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 URI being other than a sip: URI or tel: URL.

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

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

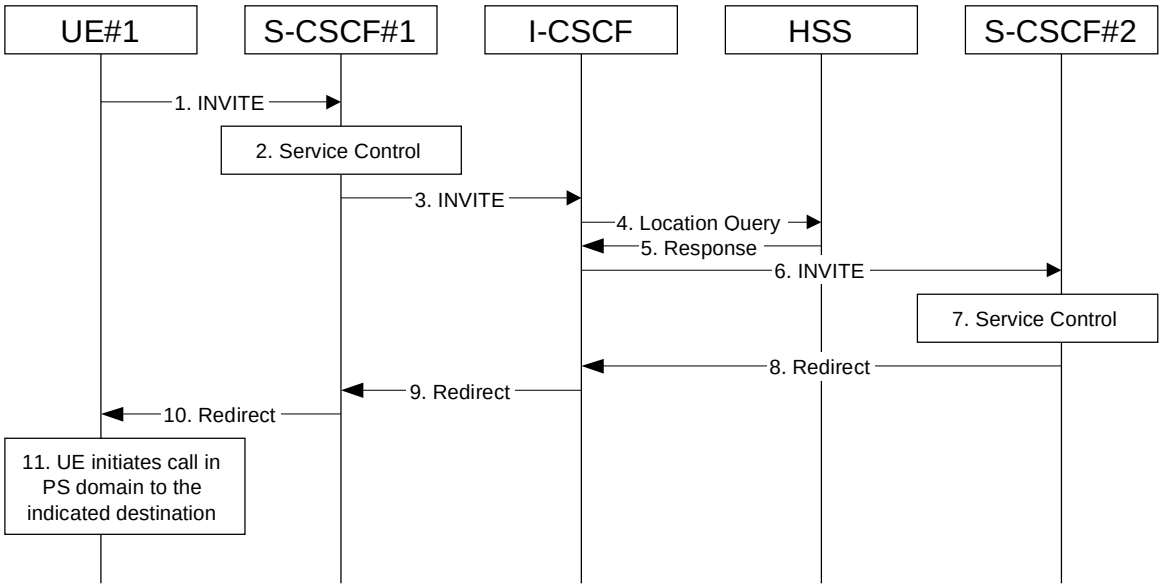


Figure 5.38: Session redirection initiated by S-CSCF to general endpoint

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.
2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt.
3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. The INVITE message is sent to an I-CSCF for that operator.
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 URI outside the IMS and outside the CS domain, i.e. other than a sip: URI or tel: URL.
8. S-CSCF#2 sends a SIP Redirect response back to I-CSCF, with redirection destination being the general URI.

9. I-CSCF sends a Redirect response back to S-CSCF#1, containing the redirection destination.
10. S-CSCF#1 forwards the Redirect response back to UE#1.
11. UE#1 initiates the session to the indicated destination.

5.11.5.4 Session Redirection initiated by P-CSCF

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

In cases when the destination user is not currently reachable in the IM CN subsystem (due to such factors as roaming outside the service area or loss of battery, but the registration has not yet expired), the P-CSCF may initiate a redirection of the session. The P-CSCF informs the S-CSCF of this redirection, without specifying the new location; S-CSCF determines the new destination and performs according to clauses 5.11.5.1, 5.11.5.2, or 5.11.5.3 above, based on the type of destination.

This is shown in the following information flow:

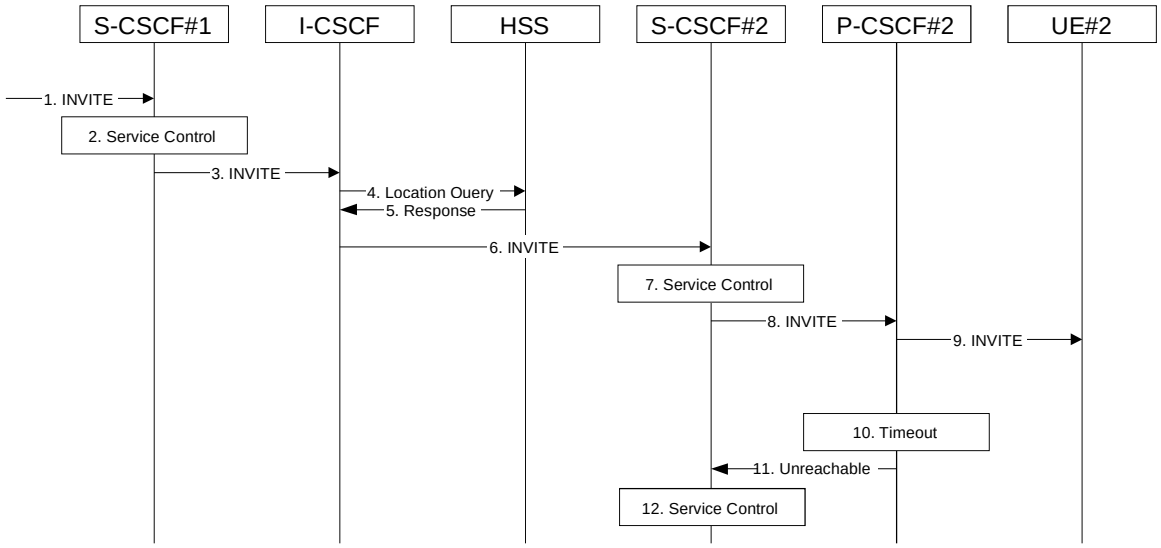


Figure 5.39: Session redirection initiated by P-CSCF

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.
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 URI, which may be a phone number, an email address, a web page, or anything else that can be expressed as a URI. Processing continues according to clauses 5.11.5.1, 5.11.5.2, or 5.11.5.3 above, based on the type of destination URI.

5.11.5.5 Session Redirection initiated by UE

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

The service implemented by this information flow is typically "Session Forward Busy", "Session Forward Variable" or "Selective Session Forwarding".

This is shown in the following information flow:

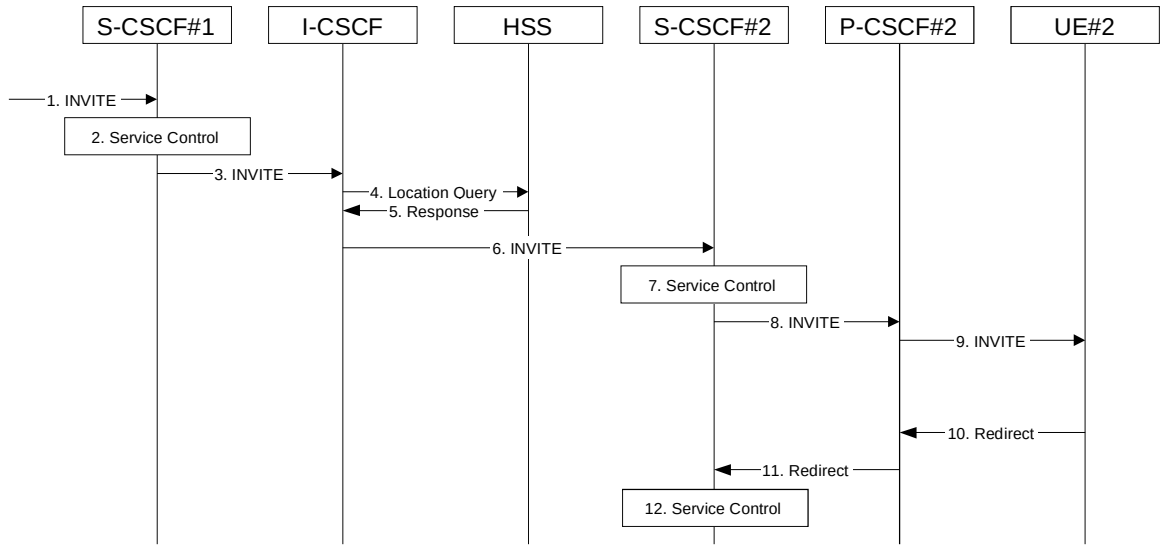


Figure 5.40: Session redirection initiated by UE

Step-by-step processing is as follows:

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

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

3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. The INVITE message is sent to an I-CSCF for that operator.

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 URI. This new destination URI may be a phone number, an email address, a web page, or anything else that can be expressed as a URI. The Redirect response is sent to P-CSCF#2

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

12. S-CSCF#2 invokes whatever service logic is appropriate for this session redirection. If UE#2 does not subscribe to session redirection service, or did not supply a new destination URI, S-CSCF#2 may supply one or may terminate the session setup attempt with a failure response. The new destination URI may be a phone number, an email address, a web page, or anything else that can be expressed as a URI. The procedures of clause 5.11.5.1, 5.11.5.2, or 5.11.5.3 given above are followed, based on the type of URI.

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

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

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

The originating end point may be a UE as shown in the example flow in figure 5.41 or it may be any other type of originating entity as defined in clause 5.4a. Redirect to another IMS endpoint (e.g. a sip: URI) is shown in the figure. The redirecting endpoint may be a UE as shown or an Application Server or a non-IMS network SIP client. Further, the endpoint to which the session is redirected may be a UE as shown in figure 5.41, or it may be any other type of terminating entity as defined in clause 5.4a. Only the scenario in which a call from the first UE is redirected by a second UE to a third UE is shown.

The flow presented here assumes that Policy and Charging Control is in use.

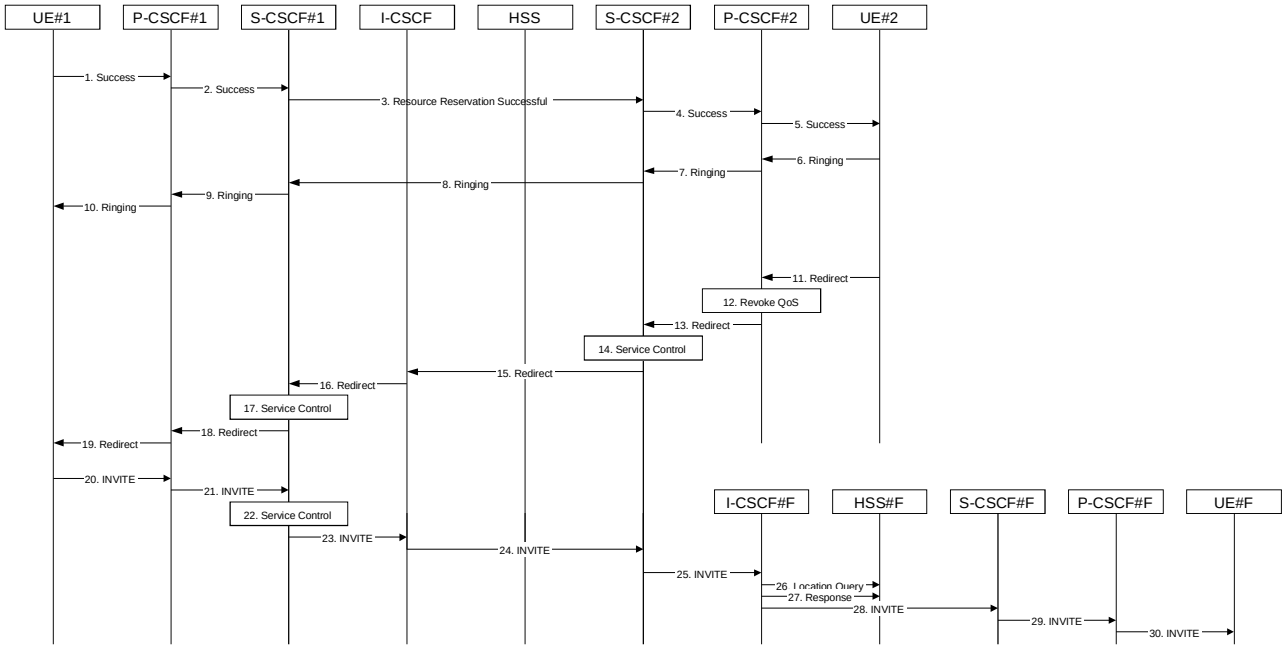


Figure 5.41: Session redirection after bearer establishment

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 URI. This new destination URI may be a phone number, an email address, a web page, or anything else that can be expressed as a URI. The Redirect response is sent to P-CSCF#2.

12. P-CSCF#2 shall revoke any authorization 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 URI, S-CSCF#2 service logic may supply one or may terminate the session setup attempt with a failure response. The new destination URI may be a phone number, an email address, a web page, or anything else that can be expressed as a URI. If S-CSCF#2 service logic requires that it remain on the path for the redirected request, the service logic generates a private URI, addressed to itself, as the new destination.

15. S-CSCF#2 sends a SIP Redirect response back to I-CSCF, containing the new destination URI.

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

17. S-CSCF#1 service logic may check the number of redirections that have occurred for this session setup attempt, and if excessive, abort the session. If S-CSCF#1 service logic requires that UE#1 not know the new destination URI, the service logic stores the new destination information, generates a private URI addressed to itself pointing to the stored information, and generates a modified Redirect response with the private URI.

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

19. P-CSCF#1 revokes any authorization 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 invokes whatever service logic is appropriate for this new session setup attempt. The service logic may retrieve destination information if saved in step #17.

23. S-CSCF#1 determines the network operator of the new destination address. If the service logic in step #14 did not provide its private URI as a new destination, the procedure continues with step #26, bypassing steps #24 and #25. If the service logic in step #14 did provide a private URI as a new destination, 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 URI, determines the network operator of the new destination, and sends the INVITE request to the I-CSCF for that network operator.

26-30. The remainder of this session completes as normal.

5.11.6 Session Transfer Procedures

5.11.6.0 General

This clause 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". The end point receiving a referral may be UE#1 as shown in the example flow in figure 5.42 or it may be any other type of originating entity as defined in clause 5.4a. The referring endpoint may be either UE#2 as shown, an Application Server or a non-IMS network SIP client. The referred-to destination may be UE#F as shown in figure 5.42 or it may be any other type of terminating entity as defined in clause 5.4a. Only the scenario in which a call from the first UE is referred by a second UE to a third UE is shown.

An information flow illustrating this is as follows:

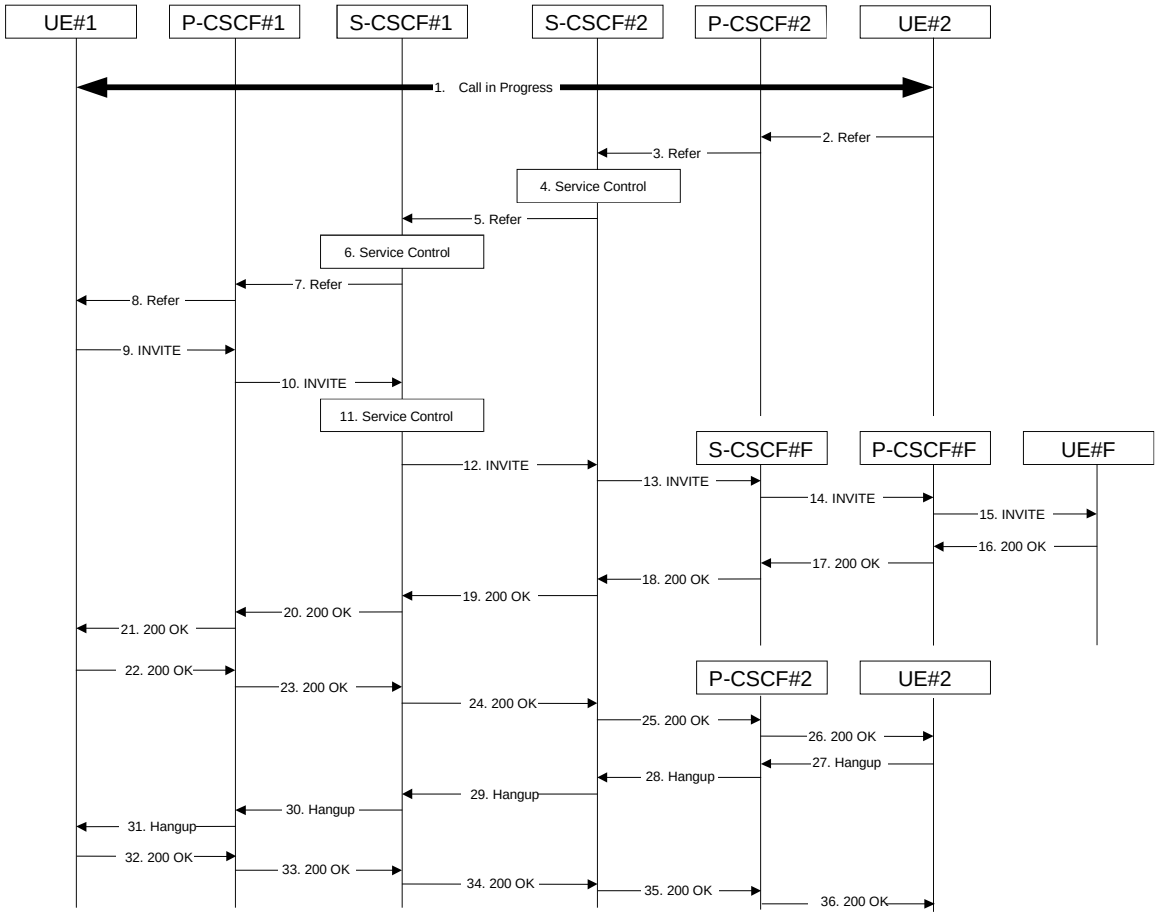


Figure 5.42: Refer operation

Step-by-step description of the information flow:

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

2. UE#2 sends the Refer command to P-CSCF#2, containing "Refer-To" UE#F and "Referred-By" UE#2. If UE#2 knows the GRUU of UE#F and desires to reach a particular instance of UE#F, the "Refer-To" contains the GRUU of UE#F otherwise the "Refer-To" contains the Public User Identity of UE#F.

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, service logic may reject the request. If S-CSCF#2 service logic requires that it remain on the path for the subsequent request, the service logic generates a private URI, addressed to itself, the "Refer-To" value in the request with the private URI.

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

6. S-CSCF#1 invokes whatever service logic is appropriate for this request. To hide the identities of UE#2 and UE#F, S-CSCF#1 service logic stores the "Refer-To" and "Referred-By" information and replaces them with private URIs.

7. S-CSCF#1 forwards the 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 may either be a URI for UE#F, a private URI pointing to S-CSCF#2, or a private URI pointing to S-CSCF#1.

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

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

12. S-CSCF#1 determines the network operator addressed by the destination URI, and forwards the INVITE to either S-CSCF#F or S-CSCF#2 (actually I-CSCF#F or I-CSCF#2, the public entry points for S-CSCF#F and S-CSCF#2, respectively). If S-CSCF#1 forwards the INVITE to S-CSCF#F, the procedure continues with step #14, bypassing step #13.

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

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

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

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

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

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

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

NOTE: The last BYE message to clear the original session can be issued either by UE#1 or by UE#2.

5.11.6.2 Application to Session Transfer Services

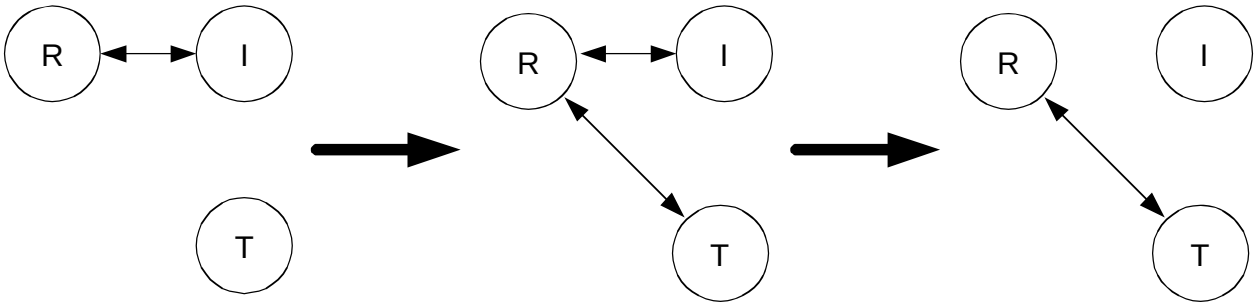
5.11.6.2.0 General

This clause 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.

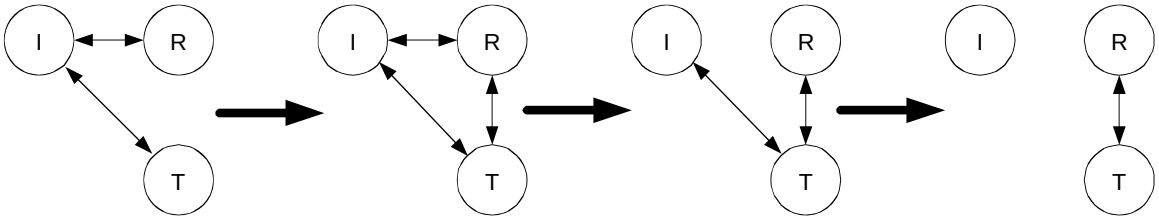


An Assured Transfer is identical to the above, except that I waits until the Refer successfully completes before issuing the BYE message to terminate its connection with R. If the new session from R to T were to fail, R would still have a session with I.

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.

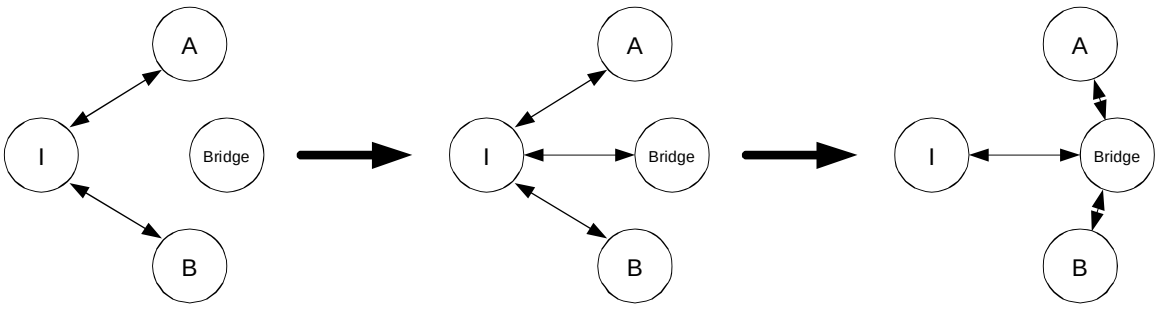
From the starting configuration, as shown in the leftmost diagram in the previous clause, I places the session with R on hold and establishes a new session with T. This is shown in the leftmost diagram below. I then sends a Refer message to T, causing T to establish a session with R. This is shown in 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 centre 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 clause 5.11, or may utilize the procedures of clause 5.11.6.2.1 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

5.12.0 General

This clause 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 clause 4.3.3.4, where the Public User Identities 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:

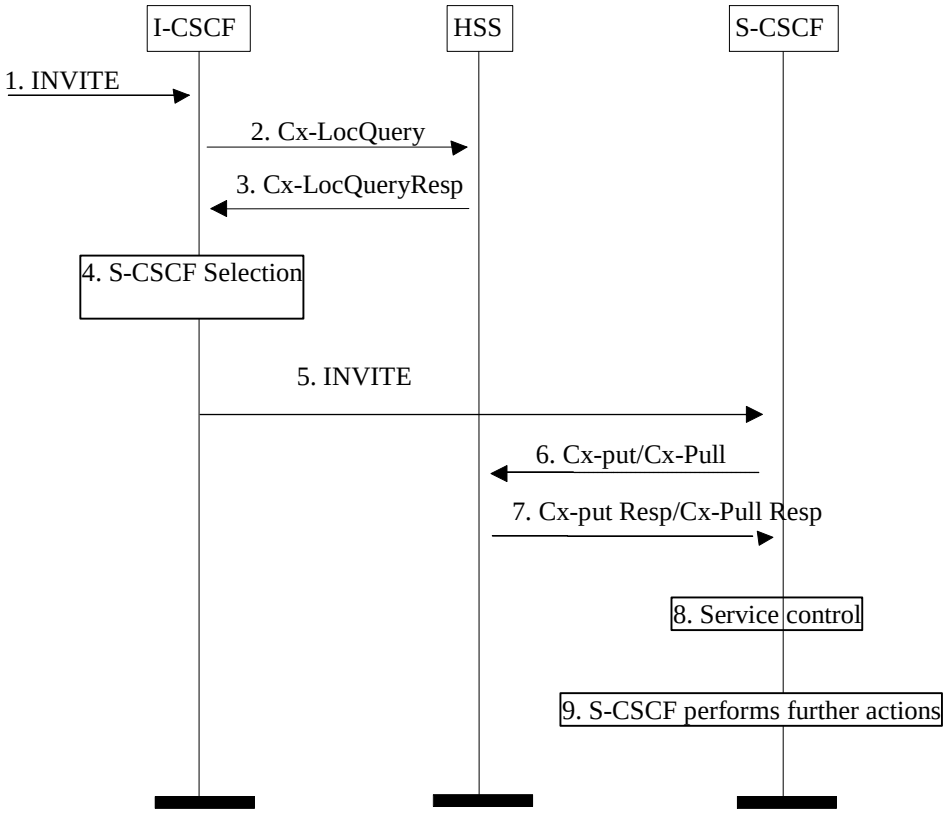


Figure 5.43: Mobile Terminating call procedures to unregistered IMS Public User Identity that has services related to unregistered state

1. I-CSCF receives an INVITE message.
2. I-CSCF queries the HSS for current location information.
3. HSS either responds with the required S-CSCF capabilities which I-CSCF should use as an input to select a S-CSCF for the unregistered Public User Identity of the user or provides the I-CSCF with the previously allocated S-CSCF name for that user.
4. If the I-CSCF has not been provided with the location of the S-CSCF, the I-CSCF selects an S-CSCF for the unregistered Public User Identity of the user.
5. I-CSCF forwards the INVITE request to the S-CSCF.
6. The S-CSCF sends Cx-Put/Cx-Pull (Public User Identity, S-CSCF name) to the HSS. When multiple and separately addressable HSSs have been deployed by the network operator, then the S-CSCF needs to query the SLF to resolve the HSS. The HSS stores the S-CSCF name for unregistered Public User Identities of that user. This will result in all terminating traffic for unregistered Public User Identities of that user being routed to this particular S-CSCF until the registration period expires or the user attaches the Public User Identity to the network. Note: Optionally the S-CSCF can omit the Cx-Put/Cx-Pull request if it has the relevant information from the user profile.
7. The HSS shall stores the S-CSCF name for that user and return the information flow Cx-Put Resp/Cx-Pull Resp (user information) to the S-CSCF. The S-CSCF shall store it for that indicated Public User Identity.
8. S-CSCF invokes whatever service logic is appropriate for this call attempt.
9. 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 (clause 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 Identity that has no services related to unregistered state

In the example information flow the Public User Identity of the user is unregistered and the Public User Identity has no services related to unregistered state.

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

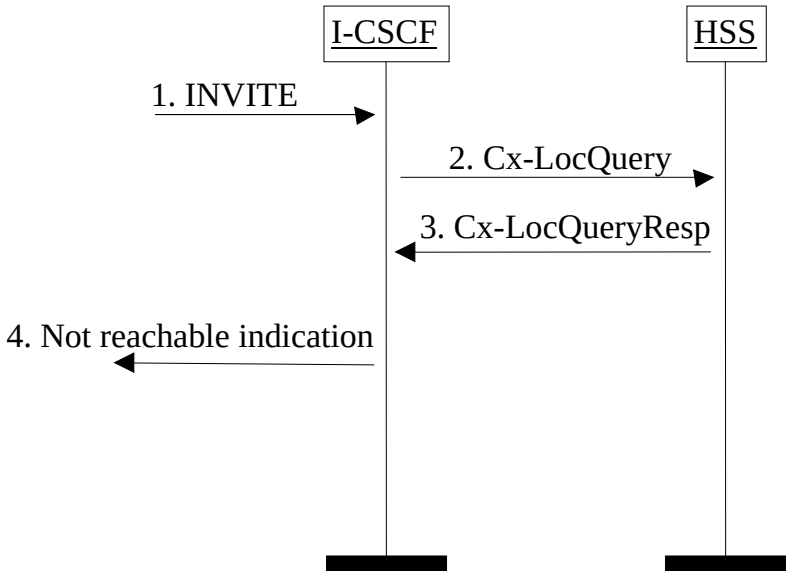


Figure 5.44: Mobile Terminating call procedures to unregistered Public User Identity that has no services related to unregistered state

1. I-CSCF receives an INVITE message.
2. I-CSCF queries the HSS for current location information.
3. HSS responds with an indication that the Public User Identity is unregistered, but no services are related to unregistered state.
4. I-CSCF responds to the origin of the request that the user is not reachable at the moment.

5.13 IMS Emergency Sessions

Emergency sessions via IMS are specified in TS 23.167 [58].

5.14 Interactions involving the MRFC/MRFP

5.14.0 General

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

5.14.1 Interactions between the UE and the MRFC

In some cases an operator may wish to make an MRFC available directly to a UE, for example to support ad-hoc multi-party sessions to be initiated by the UE. In this case, the operator advertises the name of one or more MRFCs and a UE

will invite an MRFC to a session. The session invitation would need to contain additional information indicating the specific capabilities (e.g., multi-party) desired. A conference ID would be assigned by the MRFC and returned to the UE. This would then be used by the UE in subsequent interactions with the MRFC and other UEs participating in the session.

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

5.14.2 Service control based interactions between the MRFC and the AS

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

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 invoke announcement and transcoding services. That is, the AS will send an INVITE to the MRFC with an indication of the capability being requested and with additional information related to the specific service such as identification of the announcement to be played or identification of the specific transcoding requirements.

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

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

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

5.14.4 Transcoding services involving the MRFC/MRFP

Network services involving MRFC and MRFP are not limited to conferencing and announcements, but also involve transcoding support for interworking between IMSs or inter-domain sessions, and intra-domain sessions between access technologies supported in an IMS (e.g. wireline wireless interworking, or interworking with non-3GPP wireless technologies).

The MRFC and MRFP act as transcoding entity in an IMS solving media encoding mismatches due to codec selection between operator networks, as well as to deal with encoding formats in a converged service environment. Service requests sent to the MRFC shall contain sufficient information to associate the systems that require media transcoding, and also for reservation of resources required at the MRFP. The MRFC shall always grant the requests from the control plane, unless there is a lack of resources. Media transcoding support based on MRFC/MRFP shall support the offer/answer procedure as defined in IETF RFC 3264 [72].

Additional description of transcoding support involving the MRFC/MRFP is provided in Annex P.

5.15 Mobile Terminating session procedure for unknown user

5.15.0 General

This clause 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.

In the case where the destination Public User Identity is an E.164 number in the SIP URI with user=phone parameter format, the I-CSCF shall first translate it into the Tel: URI format per IETF RFC 3966 [15] prior to sending to the HSS a Cx_LocQuery (or to the SLF a DX_SLF_QUERY). If a failure occurs under these circumstances, the Mobile Terminating user is not an IMS user of this network. In this case, the I-CSCF may invoke the portion of transit functionality that translates the E.164 address contained in the Request-URI of the Tel: URI format to a routable SIP URI, or BGCF for further routing as described in clause 5.19.

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 clause 5.15.2. The flows of figure 5.45 could include SLF determination of the HSS, however these are not shown for clarity.

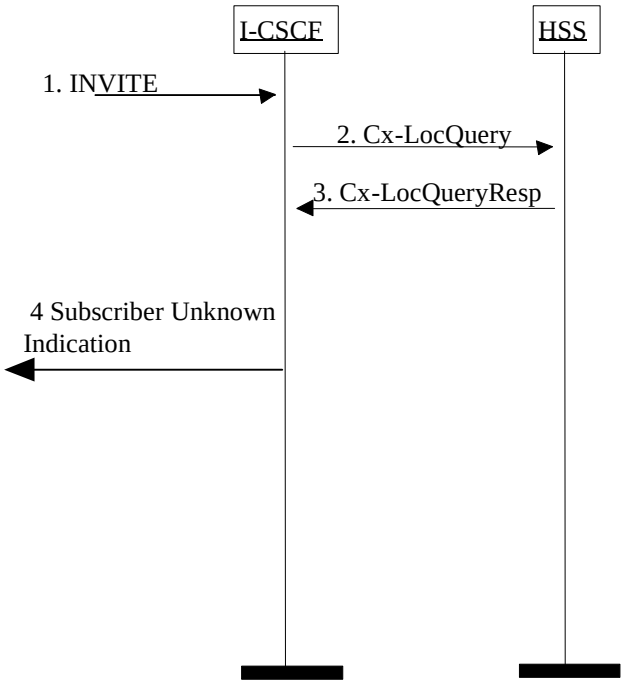


Figure 5.45: HSS determination of unknown user

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

5.15.2 Unknown user determined in the SLF

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

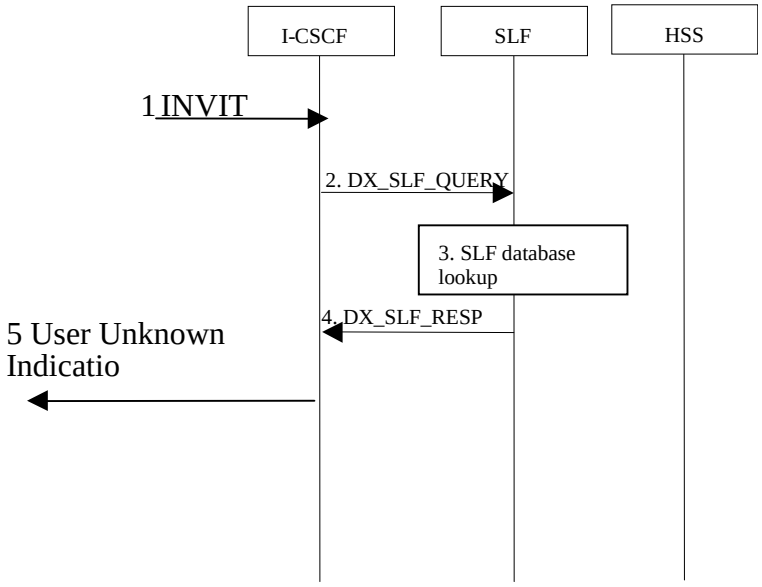


Figure 5.46: SLF determination of unknown user

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

5.16 IMS messaging concepts and procedures

5.16.0 General

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

Any ISIM or, for UEs supporting only non-3GPP accesses and containing IMC, any IMC related architectural requirements would be studied as part of overall IMS Messaging.

5.16.1 Immediate Messaging

5.16.1.0 General

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

5.16.1.1 Procedures to enable Immediate Messaging

5.16.1.1.0 General

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

- Pictures, video clips, sound clips with a format defined in the respective access specific annex.

If the message size exceeds the size limit for MESSAGE requests, the UE shall use alternative means to deliver the content of the Immediate Message. Session based messaging specified in clause 5.16.2 provides such means.
IETF RFC 3428 [43] presents guidelines for the selection of transport mechanism for an Immediate Message. The message size limitations described above are meant to be applicable for Immediate Messages sent over end-to-end congestion safe transport, i.e. are not necessarily equal to the limitations specified for MESSAGE over congestion-unsafe transport by IETF RFC 3428 [43].

NOTE: The actual size limit is part of stage-3 design.

If the size limit for a terminating MESSAGE request is exceeded, the network may refuse the request or respond to the sender with an indication that the size of the message is too large.

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

5.16.1.1.1 Immediate messaging procedure to registered Public User Identity

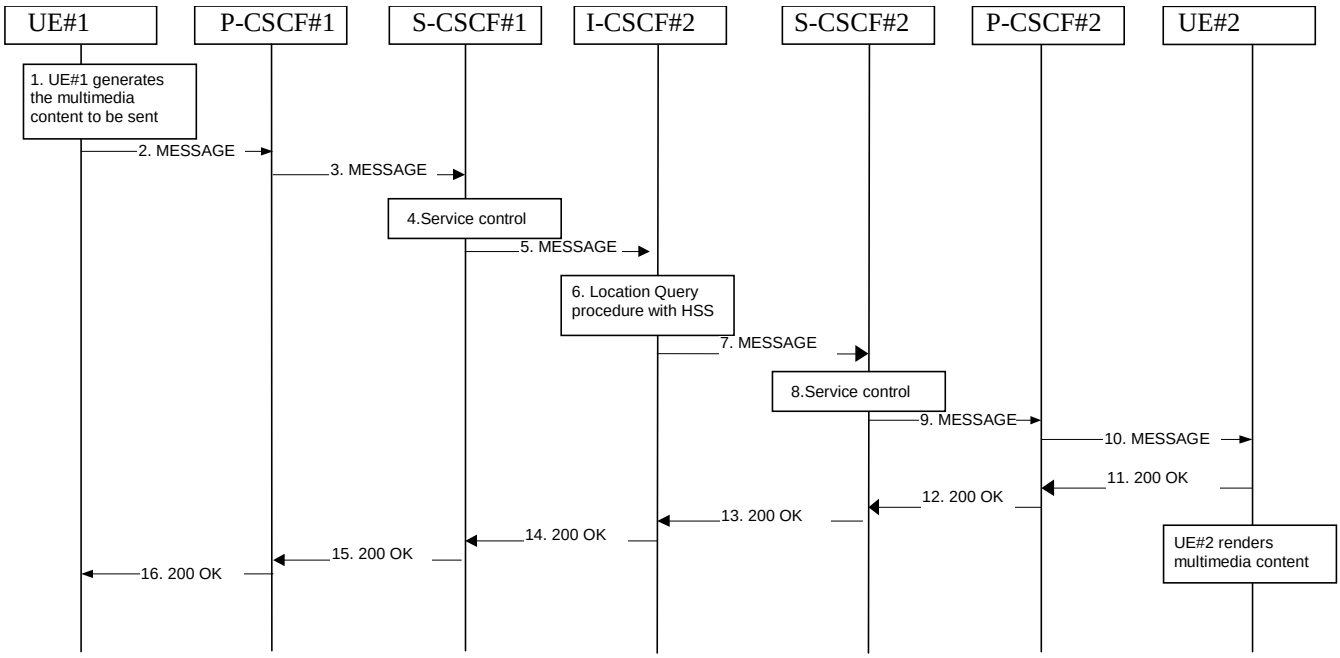


Figure 5.47: Immediate Messaging procedure to registered Public User Identity

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

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

7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.

8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF#2 invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an Application Server, which processes the request further on.
For example, the UE#2 may have a service activated that blocks the delivery of incoming messages that fulfil criteria set by the user. The AS may then respond to the MESSAGE request with an appropriate error response.

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

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

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

5.16.1.1.2 Immediate messaging procedure to unregistered Public User Identity

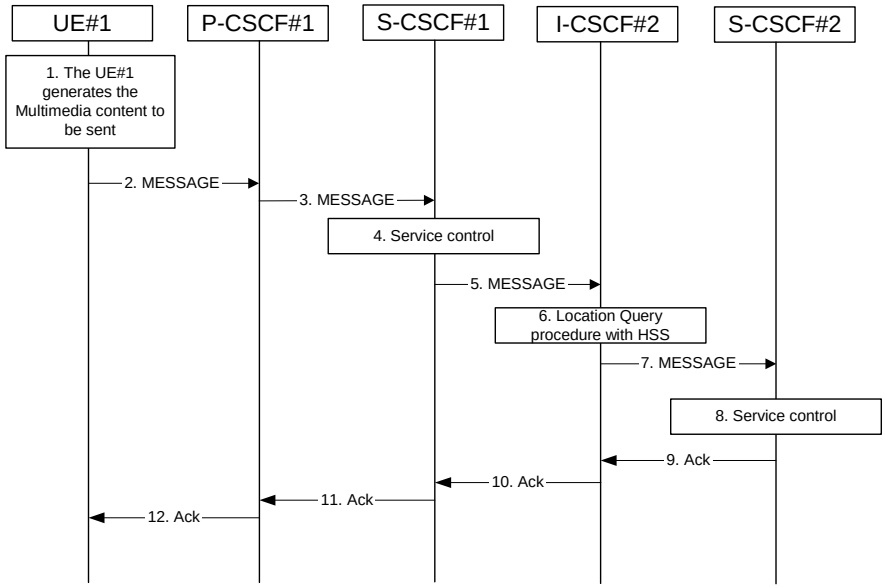


Figure 5.48: Immediate messaging to unregistered Public User Identity, service control invoked

1-5. The same actions apply as for when the Public User Identity is registered, see step 1-5 in clause 5.16.1.1.1.

6. I-CSCF#2 interacts with the HSS as per the terminating procedures defined for unregistered Public User Identities in clause 5.12.1. If the Public User Identity has no services related to unregistered state activated the interaction with HSS would be as per the procedure defined in clause 5.12.2.

7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.

8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable or the UE#2 does not have a service activated that temporarily hold the MESSAGE request in the network.

S-CSCF#2 invokes whatever service control logic appropriate for this MESSAGE request. This may include routing the MESSAGE request to an Application Server, which processes the request further on.

For example, the UE#2 may have a service activated that allows delivery of any pending MESSAGE request. The AS may then hold the MESSAGE request and deliver the MESSAGE request when the UE#2 becomes reachable. In this case, depending on user settings UE#2 controls the delivery of the pending MESSAGEs.

9-12. The MESSAGE request is acknowledged with an appropriate acknowledgement response. The acknowledgement response traverses the transaction path back to UE#1.

5.16.1.2 Immediate messages with multiple recipients

IMS users shall be able to send a single immediate message to multiple recipients, as specified in TS 22.340 [29a]. The following means are supported to achieve this:

- A PSI identifying a new group is created in the appropriate Application Server, and members are added to this group (e.g. by the user via the Ut interface or by the operator via O&M mechanisms). Immediate messages addressed to this PSI will be routed to the AS hosting the PSI, and this AS shall create and send immediate messages addressed to a group member of the group identified by the PSI.

- The user can send an immediate message by indicating the individual addresses (Public User Identities for IMS recipients) of the intended recipients as part of the immediate message. The AS of the user shall then create and send immediate messages addressed to each one of the intended recipients.

5.16.2 Session-based Messaging

5.16.2.0 General

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

5.16.2.1 Architectural principles

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

As the messaging media component usually does not require QoS beyond best-effort, use of the preconditions mechanism as defined in IETF RFC 3312 [41] is not required for session based messaging establishment that only includes a messaging media component.

NOTE: Pre-conditions mechanism may still be required for session establishment with additional media components that require the establishment of additional IP-CAN bearers.

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

The invited UE shall host the message session (accept a connection for the message session from the other endpoint). In order to host the message session the UE needs an appropriate IP-CAN bearer, on which it can accept the connection for the message media component. This IP-CAN bearer may be e.g. a general purpose bearer available prior to starting the session initiation or a dedicated bearer that is established during session establishment. Messages within a message session should be transported over a connection-oriented reliable transport protocol. Message sessions may be either established end to end between two UEs or may involve one or more intermediate nodes (e.g. a chat server for multi party chat or an Application Server to perform per message charging).

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

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

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

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

- Operator-controlled policy to be set on the size and content of the messages.
- Support for indication of maximum message content size that a UA will accept to be received.
- Support for a messaging media component as part of a session where other media components are also included.
- Support for messaging-only sessions.

If charging mechanisms like charging based on the message content, message type or number of sent and/or received messages (see TS 22.340 [29a]) are required, then an intermediate node (messaging AS) shall be involved, which is able to inspect the SIP signalling as well as the exchanged messages and their content. Such an intermediate node may also provide support for time- and/or volume based charging.

5.16.2.2 Procedures to enable Session based Messaging

5.16.2.2.0 General

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

- Pictures, video clips, sound clips with a format defined in the respective access specific documents.

5.16.2.2.1 Session based messaging procedure to registered Public User Identity

The following procedure shows the establishment of a message session between two registered UEs where the UEs are able to exchange messages end-to-end. The signalling flow is based on the general flow shown in chapter 5.7a of this specification.

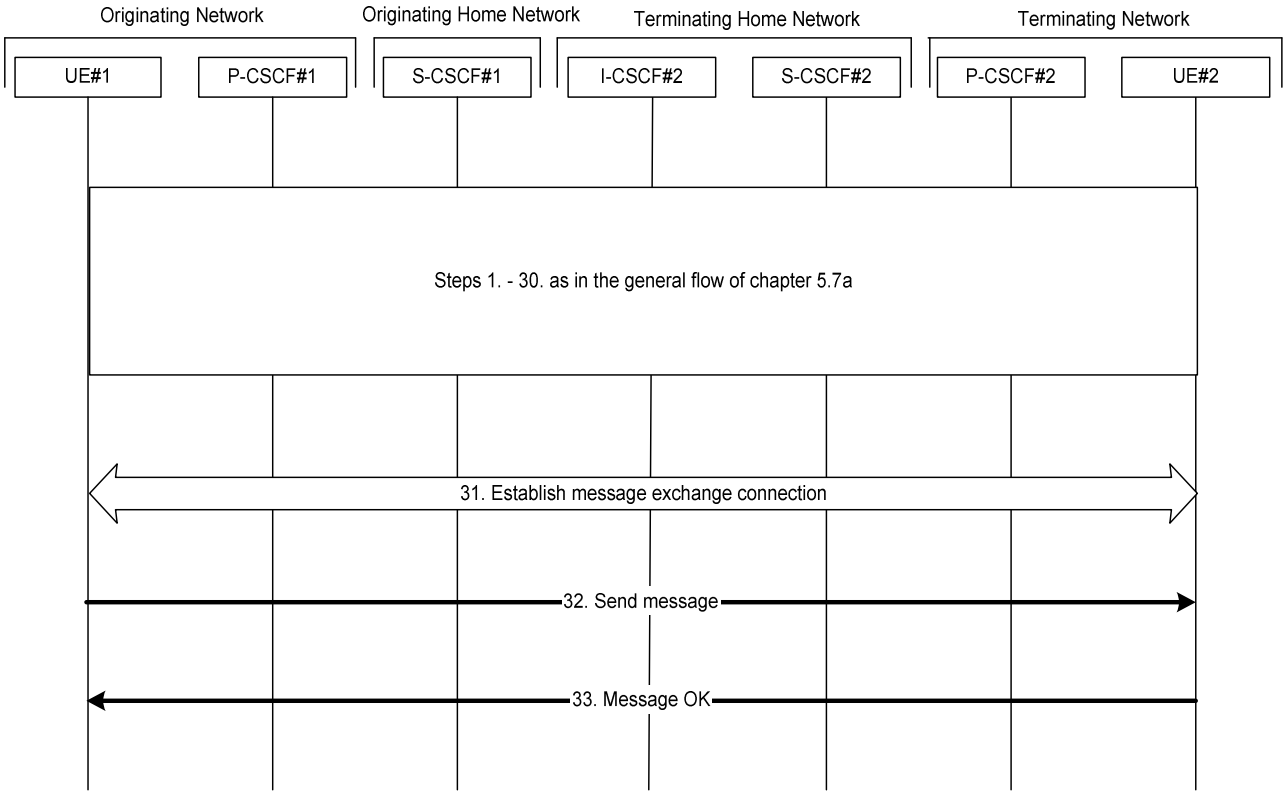


Figure 5.48a: Message session establishment

1-30. These steps are identical to the steps 1 to 30 in the flow of chapter 5.7a. After that the message session is established. For session based messaging the SDP offer in the first INVITE request may indicate the maximum message size UE#1 accepts to receive and the 200 OK (Offer response) to the INVITE request may indicate the maximum message size UE#2 accepts to receive.

31. UE#1 establishes a reliable end-to-end connection with UE#2 to exchange the message media.

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

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

Further messages may be exchanged in either direction between UE#1 and UE#2 using the established connection. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and UE#2 respectively.

5.16.2.2.2 Session based messaging procedure using multiple UEs

Session based messaging between more than two UEs require the establishment of a session based messaging conference.

Within session based messaging conferences including multiple UEs (e.g. multiparty chat conferences) an MRFC/MRFP or an IMS AS shall be used to control the media resources.

When MRFC/MRFP are used, then conferencing principles are used to provide the chat service:

- MRFP must be able to establish message connections with all involved parties.

- MRFC/MRFP must be able to receive messages from conference participants and to distribute messages to all or some of the participants.

- In order to enable the UE managing information related to the session based messaging conference the MRFC may be co-located with an IMS AS.

- MRFC/MRFP roles and interactions with an AS are described in more detail in chapters 4.7 and 5.14.1 and 5.14.2.

- The interface for session based messaging between MRFC and MRFP is not standardised in this release. When an AS is used, then the IMS service control architecture is used to provide the chat service. Both signalling and user plane are then supported by the AS. For more details, see clause 4.2.

The following flow shows the originating session based messaging set up using an intermediate server for a chat service. In this case the intermediate chat server is addressed by the UE#1 using a PSI. It is assumed that UE#1 is the first UE entering the chat session.

NOTE: Interactions between MRFC and MRFP are not shown in the flows below since these interactions are not standardized. An optional ringing response from MRFC/AS to the UE is not shown in the following procedure.

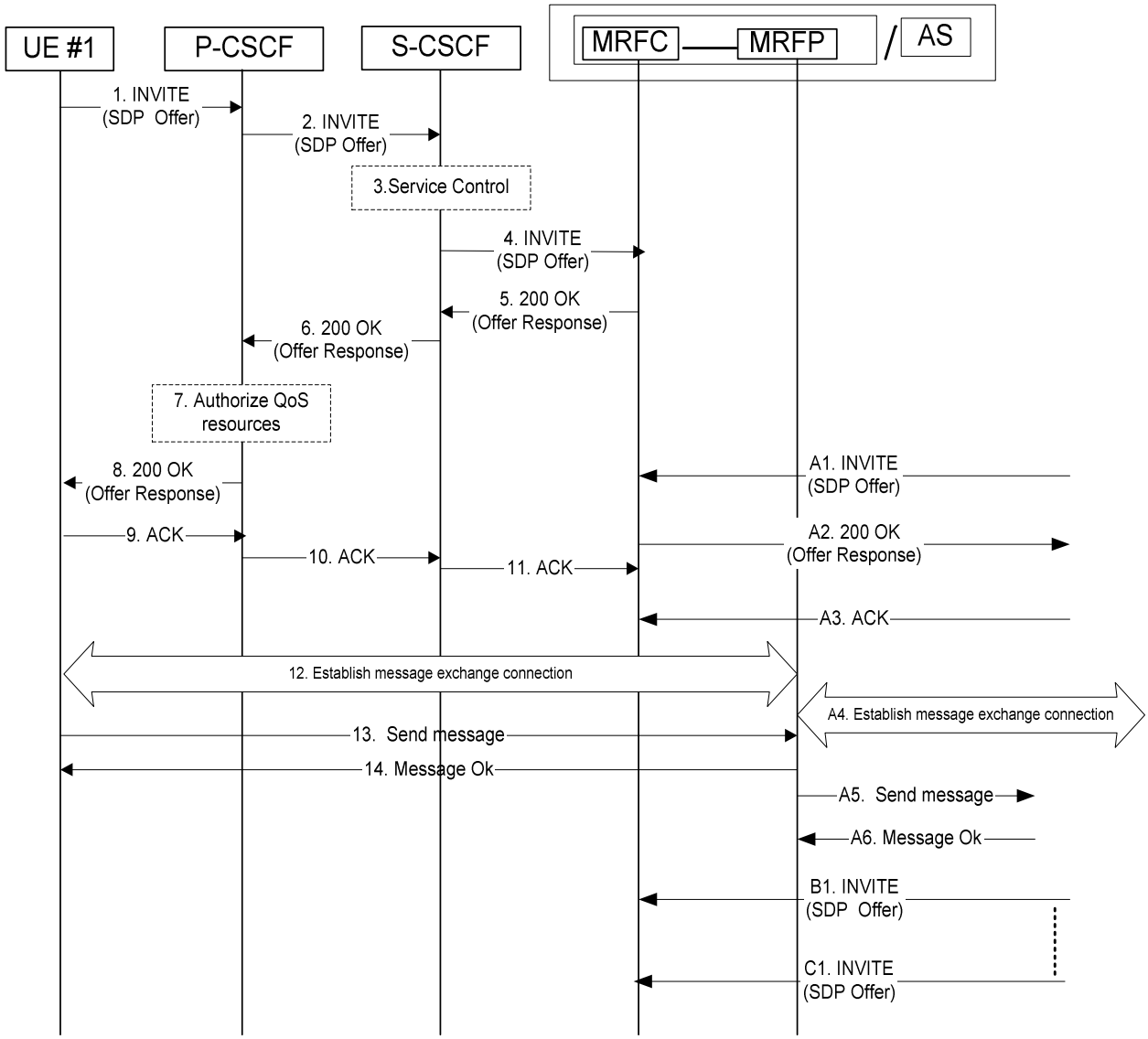


Figure 5.48b: Session based messaging using a chat server

1. UE #1 sends the SIP INVITE request addressed to a conferencing or chat PSI to the P-CSCF. The SDP offer indicates that UE#1 wants to establish a message session and contains all necessary information to do that. The SDP offer may indicate the maximum message size UE#1 accepts to receive.

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

3. S-CSCF may invoke service control logic for UE#1.

4. S-CSCF forwards the INVITE request to the MRFC/AS.

5., 6. and 8. MRFC/AS acknowledges the INVITE with a 200 OK, which traverses back to UE#1. The 200 OK (Offer response) may indicate the maximum message size the host of the PSI accepts to receive.

7. Based on operator policy P-CSCF may instruct PCRF/PCF to authorize the resources necessary for this session.

9.-11. UE#1 acknowledges the establishment of the messaging session with an ACK towards MRFC/AS.

12. UE#1 establishes a reliable end-to-end connection with MRFP/AS to exchange the message media.

13. UE#1 sends a message towards MRFP/AS.

14. MRFP/AS acknowledges the message.

A1. Another UE (UE#2) sends an INVITE request addressed to the same conferencing or chat PSI. The initial SDP indicates that the UE wants to establish a message session and contains all necessary information to do that.

A2. MRFC/AS acknowledges the INVITE request with a 200 OK.

A3. UE#2 acknowledges the 200 OK with an ACK.

A4. UE#2 establishes a reliable end-to-end connection with MRFP/AS to exchange the message media.

A5. MRFP/AS forwards the message to all recipients, e.g. all participants in the chat room.

A6. The recipients acknowledge the message towards MRFP/AS.

B1. and C1. Further INVITE requests from new possible participants may arrive at any time.

Further messages may be exchanged in either direction between the participating UEs using the established connection via the MRFC/MRFP or AS. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and the host of the PSI respectively.

5.16.2.2.3 Session based messaging procedure with an intermediate node

The following procedure shows the originating session based messaging involving an intermediate node. An optional ringing response from AS to the UE or vice versa is not shown in the following procedure.

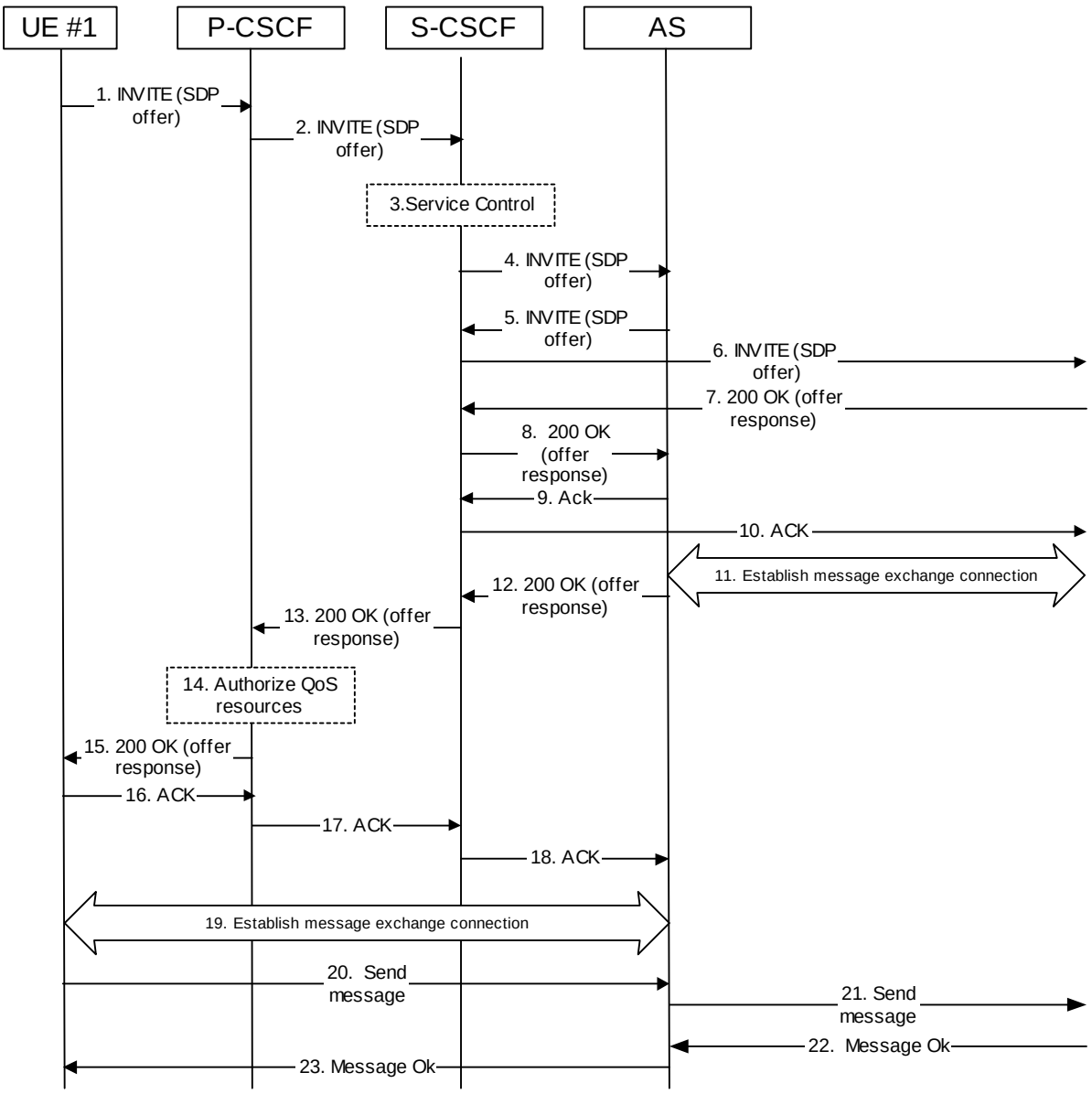


Figure 5.48c: Session based messaging with an intermediate node

1. UE#1 sends the SIP INVITE request addressed to UE#2, containing an initial SDP, to the P-CSCF. The SDP offer may indicate the maximum message size UE#1 accepts to receive.

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

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

4. The S-CSCF forwards the INVITE request to the AS. The AS may modify the content of the SDP (such as IP address/port numbers). Based on operator policy the AS may either reject the session set-up or decrease the maximum message size indication.

5. The AS sends the INVITE request to the S-CSCF.

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

7–8. UE#2 or AS in the terminating network accepts the INVITE request with a 200 OK response. The 200 OK response is forwarded by the S-CSCF to the AS. The 200 OK (Offer response) may indicate the maximum message size UE#2 accepts to receive, possibly decreased by the AS.

9-10. The AS acknowledges the 200 OK response from the terminating network with an ACK, which traverses back to UE#2 or AS in the terminating network via the S-CSCF.

11. The AS initiates the establishment of a reliable end-to-end connection with UE#2 or the AS in the terminating network to exchange the message media. This step can take place in parallel with step 12.

12, 13 and 15. The AS accepts the message session with a 200 OK response. The 200 OK response traverses back to UE#1.

14. Based on operator policy P-CSCF may instruct PCRF/PCF to authorize the resources necessary for this session.

16-18. UE#1 acknowledges the 200 OK with an ACK, which traverses back to the AS.

19. UE#1 establishes a reliable end-to-end connection with the AS to exchange the message media.

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

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

22. UE#2 or AS in the terminating network acknowledges the message with a response that indicates the reception of the message. The response traverses back to the AS.

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

Further messages may be exchanged in either direction between UE#1 and the terminating network using the established message connection via the AS. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and UE#2 respectively, possibly decreased by the AS.

5.16.2.2.4 Session based messaging release procedure

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

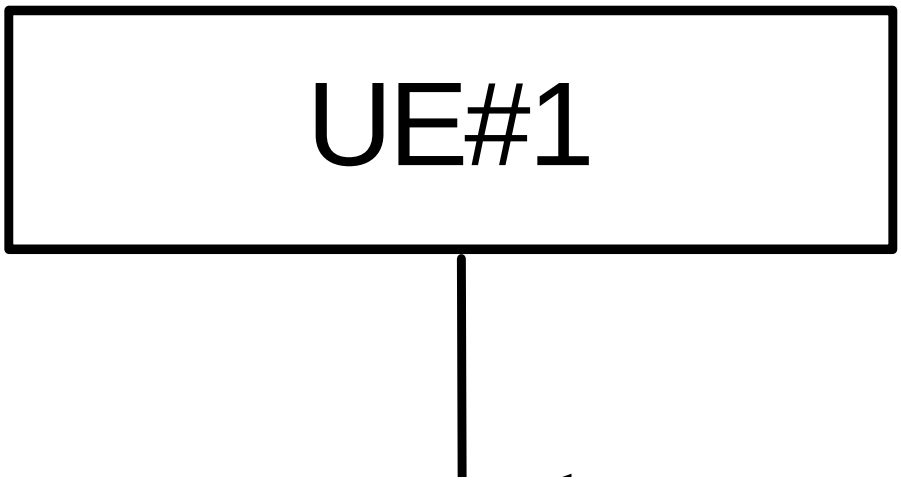


Figure 5.48d: Message session release procedure

1–6. UE#1 indicates its intent to terminate the message session by sending a BYE request to UE#2. UE#1 stops sending messages and tears down the message connection on the transport level and destroy local state for the message session. The UE#1 may use the IP-CAN bearer for some other services; hence it keeps the bearer activated.

7-8. UE#2 agrees to end the session and tear down the message connection on the transport level and destroy local state for the message session. The UE#2 may use the IP-CAN bearer for some other services; hence it keeps the bearer activated.

9-13. UE#2 acknowledges the BYE request by sending a 200 OK to UE#1, which traverses back the signalling path.

5.16.2.2.5 Session based messaging release procedure with an intermediate node

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

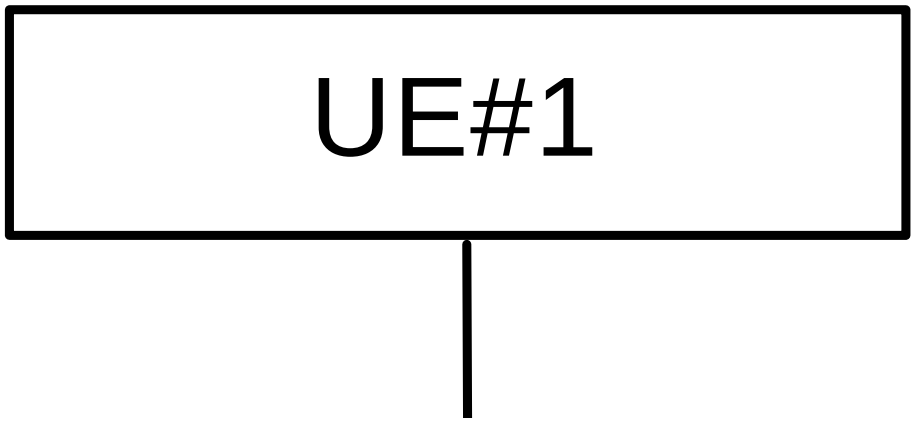


Figure 5.48e: Message session release procedure with intermediate node

1–4. UE#1 indicates its intent to terminate the message session by sending a BYE request to UE#2, via the AS. UE#1 stops sending messages and tears down the message connection on the transport level and destroy local state for the message session. The UE#1 may use the IP-CAN bearer for some other services; hence it keeps the bearer activated.

5. The AS forwards the BYE request to the UE#2.

6-9. The AS tears down the message connection on the transport level and destroys local state for the message session. The AS acknowledges the BYE request by sending a 200 OK to UE#1, which traverses back the signalling path

10. The AS receives the acknowledgement from UE#2 to end the session.

5.17 Refreshing sessions

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

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

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

5.18 Void

5.19 Support for Transit scenarios in IMS

5.19.1 General

This clause presents some high level flows to describe the procedures for supporting IMS transit network scenarios.

The IMS Transit Functions perform an analysis of the destination address, and determine where to route the session. The session may be routed directly to an MGCF, BGCF, or to another IMS entity in the same network, to another IMS network, or to a CS domain or PSTN. The address analysis may use public (e.g. DNS, ENUM) and/or private database lookups, and/or locally configured data. As described in clause 4.15 there are various transit configurations possible that may be supported.

For the case where an operator is providing transit functions for other operators and/or enterprise networks, the configuration is as shown in Figure 5.49. The configuration in Figure 5.49 is also intended to cover scenarios where an operator routes traffic from other IMS- or SIP-networks to CS domain or PSTN customers through the IMS transit network. In this case the terminating network as shown in the figure indicates the operator's CS domain or PSTN.

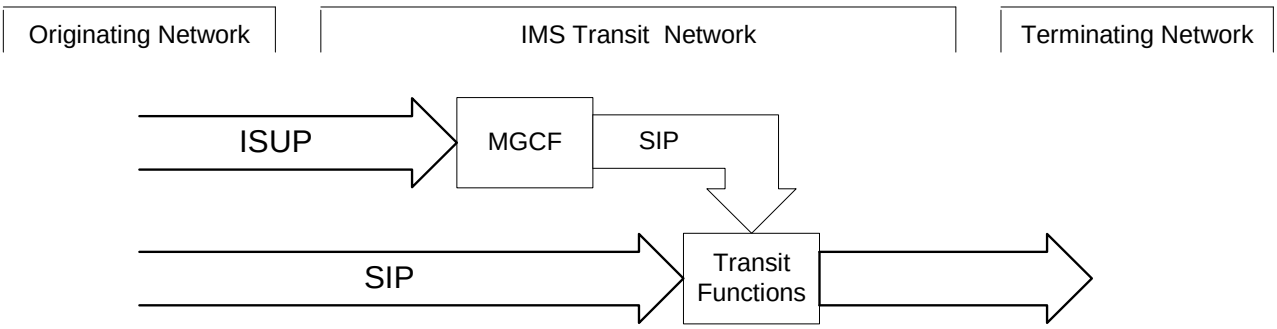


Figure 5.49: IMS transit network

For the transit operator in Figure 5.49, ISUP messages that arrive at a configured MGCF, are translated into SIP, and are passed to the IMS Transit Functions. SIP messages may arrive directly at the configured entity supporting the transit functions or first pass through an IBCF before arriving at the IMS Transit Functions. The IMS Transit Functions determine whether to route directly to an MGCF, BGCF, or to another IP entity on the path (e.g. an IBCF). In this transit operator configuration, the IMS Transit Functions might reside in a stand-alone entity or might be combined with the functionality of an MGCF, a BGCF, an I-CSCF, an S-CSCF or an IBCF. When residing in a stand-alone entity the IMS Transit Functions shall be able to generate CDRs.

For the case where the operator is the terminating network operator handling a terminating service for its own customers, the configuration and operation may be more complex as shown in figure 5.50.

NOTE 1: In the case of Fixed Broadband Access to IMS the term "CS domain" in the following text and in figure 5.50 may be replaced by the term "PSTN".

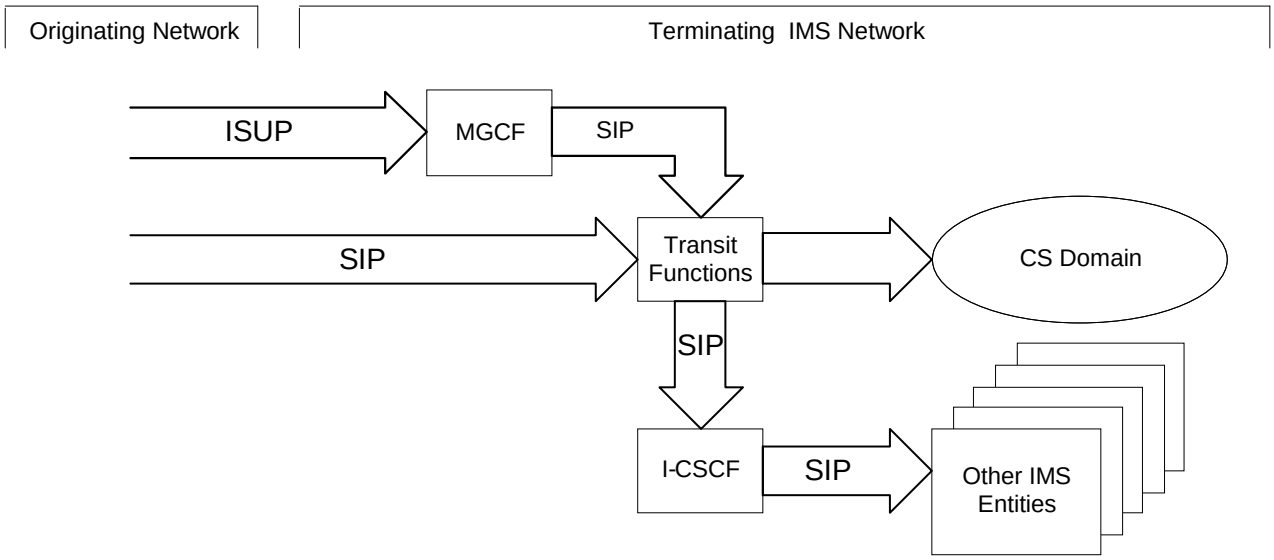


Figure 5.50: Terminating IMS network with transit support, Transit Functions first

For the operator in figure 5.50, ISUP messages arriving at an MGCF may be destined for an IMS or a CS domain customer (see clause 4.15). The ISUP messages are translated into SIP.

The operator can choose whether to route all traffic through the IMS Transit Functions, which subsequently route to the I-CSCF for IMS terminating call scenarios or to an MGCF for the case of CS domain subscribers as described above. This is depicted in figure 5.50. In this case, there may be an additional delay for terminating sessions destined for IMS subscribers.

NOTE 2: In this case, the IMS Transit Functions perform selection of the appropriate domain to terminate the call to, followed by routing to the CS domain (for CS domain destined traffic).

As an alternative, the operator may choose to route all traffic to the I-CSCF directly and then identify those sessions that are not destined to IMS subscribers based on an HSS query. Based on the response from the HSS, sessions are either routed to an S-CSCF or to the CS domain (optionally via Transit Functions). In this case there may be an additional delay for terminating sessions destined for the CS domain subscribers.

NOTE 3: If in this case, the I-CSCF becomes aware that the call is not destined to an IMS subscriber and forwards it to the Transit Function for further routing, then the Transit Functions only perform routing to the CS domain.

It is the operator's choice to determine which way to route the SIP messages, first through IMS Transit Functions or first to an I-CSCF. This may depend on whether the majority of the sessions that enter the IMS network, are destined to IMS or CS domain subscribers.

NOTE 4: In either configuration of the terminating network scenario, once it is determined that the call is not destined for an IMS subscriber, it is necessary to verify that the call is destined for a CS domain subscriber rather than to a ported number or to a wrong number. At which stage of the session establishment this decision is made is FFS.

In the terminating network configuration shown in figure 5.50, the IMS Transit Functions might reside in a stand-alone entity or might be combined with the functionality of an MGCF, a BGCF, an I-CSCF, an S-CSCF, or an IBCF. When residing in a stand-alone entity the IMS Transit Functions shall be able to generate CDRs.

For the case where an IMS network serves as a transit network and as a terminating network (depending on the destination of the session), the configuration and operation resembles that of the previous case as shown in figure 5.50a and figure 5.50b.

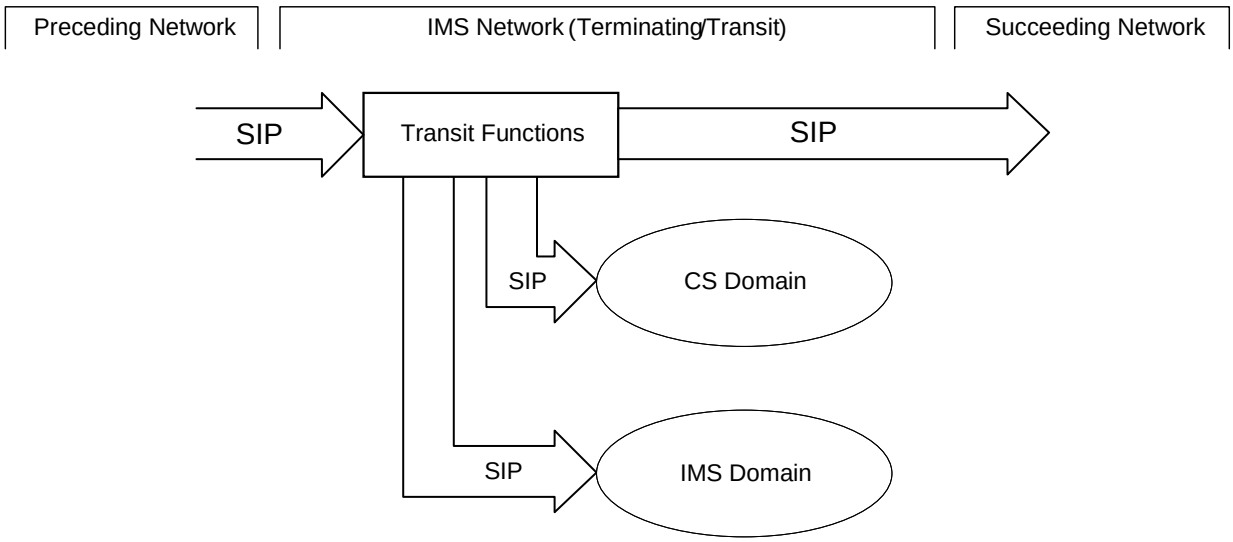


Figure 5.50a: Terminating/Transit IMS network, Transit Functions first

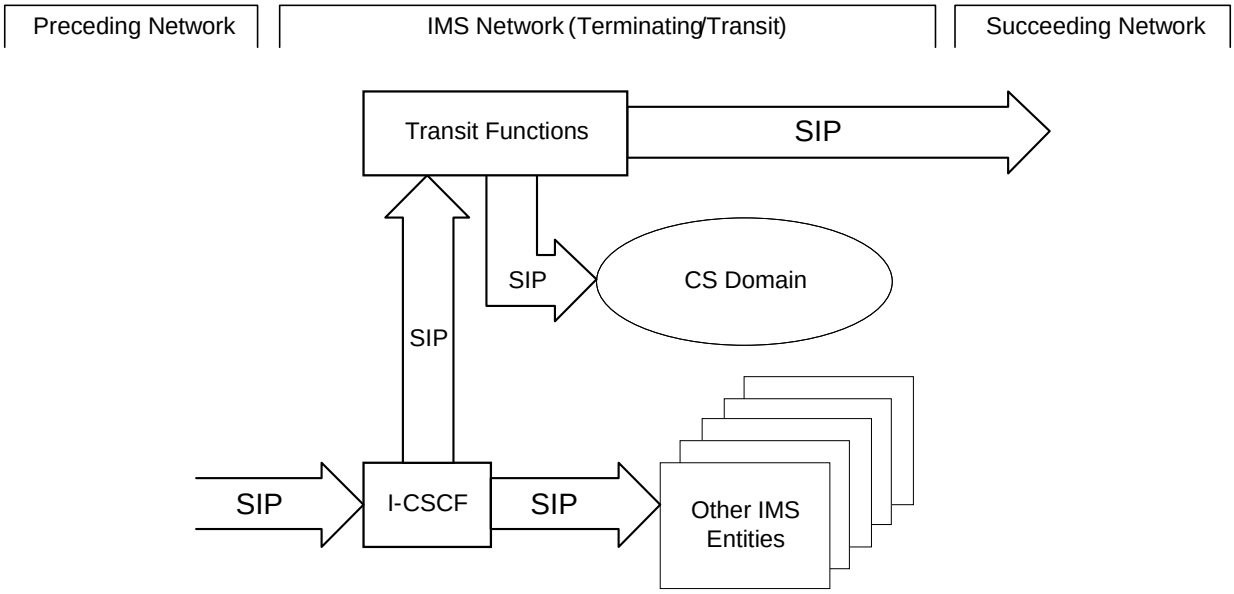


Figure 5.50b: Terminating/Transit IMS network, I-CSCF first

For the operator in figure 5.50a and figure 5.50b, ISUP messages arriving at an MGCF may be destined for the own IMS network of for a succeeding network. The ISUP messages are translated into SIP. This is not depicted in figure 5.50a and figure 5.50b.

The operator can choose whether to route all traffic through the IMS Transit Functions, which subsequently route to the I-CSCF for sessions destined for subcribers of the own IMS network, to the own CS domain for sessions destined to subscribers of the own CS domain, or to a succeeding network for sessions not destined for subscribers of the own IMS network or the own CS domain. This is depicted in figure 5.50a. In this case there may be an additional delay for sessions destined to subscribers of the own network.

NOTE 5: In this case, the Transit Functions perform selection of the appropriate domain to terminate the call to, for subscribers of the own network, followed by routing to another network (if the session is not destined to the own network).

As an alternative, the operator may choose to route all traffic to the I-CSCF directly and then identify those sessions that are not destined to IMS subscribers of the own IMS network based on an HSS query. Based on the response from the HSS, sessions are either routed to an S-CSCF of the own IMS network or to Transit Functions. The Transit Functions subsequently route the session to either the CS domain of the own network or to a succeeding network. This is depicted in figure 5.50b. In this case there may be an additional delay for sessions not destined to subscribers of the own IMS network.

It is the operator's choice to determine which way to route the SIP messages, first through IMS Transit Functions or first to an I-CSCF. This may depend on whether the majority of the sessions that enter the IMS network, are destined to subscribers of the own IMS network or not. This operator's choice may be implemented as a functionality of an entry functions such as an IBCF.

In the terminating/transit network configuration shown in figure 5.50a and figure 5.50b, the IMS Transit Functions might reside in a stand-alone entity or might be combined with the functionality of an MGCF, a BGCF, an I-CSCF, an S-CSCF, or an IBCF. When residing in a stand-alone entity the IMS Transit Functions shall be able to generate CDRs.

5.19.2 Providing IMS application services in transit network scenarios

This clause provides an overview of how IMS application services in transit network scenarios are provided.

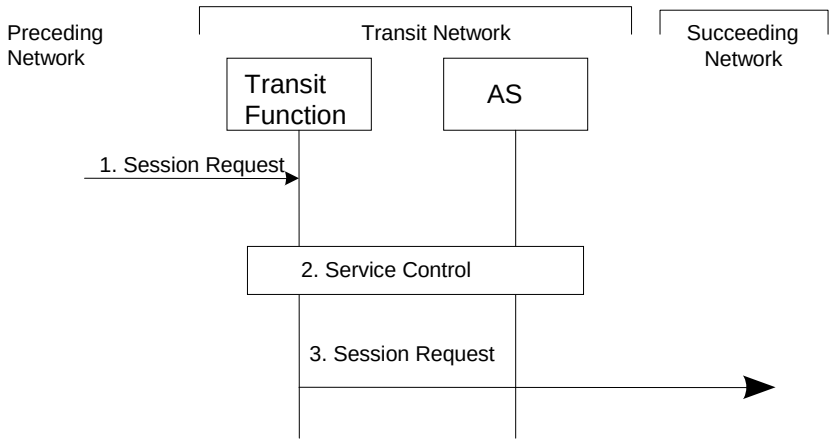


Figure 5.50c: IMS application services in transit network

The procedure for IMS application services in transit network is as follows:

1. The Transit function receives an incoming request from a preceding network.
2. Based on local configured Transit invocation criteria, the Transit function determines whether one or more services are to be performed.

   If the preceding network is the served network, for which special services are invoked, the invocation criteria will trigger and invoke the related services based on the origination of the request.

   If the succeeding network is the served network, for which special services are invoked, the invocation criteria will trigger and invoke the related services based on the termination point of the request.

   The related service(s) are invoked.
3. The Transit function performs the transit routing according to clause 5.19.1 and forwards the Session Request towards the succeeding network.

NOTE: An AS that acts as a B2BUA can decide to not route back the call to the transit function. In this case, it will use the terminating UA mode of operation for request from the Transit function. It can apply originating UA procedures according to TS 23.218 [71].

5.20 Procedures for Assigning, Using, and Processing GRUUs

5.20.1 UE

5.20.1.1 Obtaining a GRUU during registration

A UE shall indicate its support for the GRUU mechanism in the registration request and retain the GRUU set (P-GRUU and T-GRUU) in the registration response. The UE may retain some or all of the previous T-GRUUs obtained during the initial registration or previous re-registrations along with the new T-GRUU or the UE may replace some or all of the

previous T-GRUUs with the new T-GRUU. The UE shall generate an instance identifier that is a unique identifier for that UE. The UE shall include an instance identifier in all registration requests. Instance identifiers shall conform to the mandatory requirements for instance identifiers specified in RFC 5627 [49] and RFC 5626 [48].

If the registered Public User Identity is part of an implicit registration set, the UE shall obtain and retain the GRUU sets for each implicitly registered SIP URI sent by the S-CSCF in accordance to RFC 5628 [50].

5.20.1.2 Using a GRUU

When sending SIP requests from an explicitly or implicitly registered Public User Identity for which a UE obtained P-GRUU and at least one T-GRUU, the UE should use the corresponding retained P-GRUU or a T-GRUU as a Contact address.

When responding to SIP requests where the identification of the called party is a registered Public User Identity for which a UE obtained a GRUU, the UE shall use the corresponding retained P-GRUU or T-GRUU as the Contact address when addressing that UE.

If the UE has obtained GRUUs for its Public User Identity being used in a request or response and the user does not require privacy the UE should use the P-GRUU as the Contact address.

A UE may learn a GRUU of another UE using mechanisms that are outside the scope of this specification, (e.g. a UE may learn a GRUU from the contact header of a request, from presence information, or by other mechanisms).

If a UE that receives a notification from the S-CSCF indicating that an implicit registration has occurred for a contact the UE has registered, then the UE shall retain the GRUUs included in the notification for future use.

5.20.1.3 Using a GRUU while requesting Privacy

When a UE sends a request or response containing a GRUU, and it wishes to block the delivery of its Public User Identity to an untrusted destination, the UE shall use a T-GRUU as the Contact address.

5.20.2 Serving-CSCF

5.20.2.1 Allocating a GRUU during registration

The S-CSCF, when receiving a registration request from a UE that includes an instance id, shall allocate a GRUU set. If the UE indicates support of GRUU in the REGISTER request, then the S-CSCF shall return the GRUU set in the registration response and associate that GRUU set with the registered contact information for that UE.

NOTE: As long as the instance id provided in the register request is the same, the resulting P-GRUU in the GRUU set will always be the same for a given Public User Identity. The T-GRUU will be different from those returned during previous re-registrations. All T-GRUUs that are allocated continue to remain valid until that UE Instance ID and Public User Identity pair are deregistered.

If there are implicitly registered Public User Identities, the S-CSCF shall generate a GRUU set for each implicitly registered Public User Identity and include the corresponding GRUU set with the notification of each implicitly registered Public User Identity

5.20.2.2 Using a GRUU

The filter criteria in the service profile may check for the presence of a GRUU in the Request URI or related parameters of a request.

For originations, the S-CSCF shall validate the GRUU conveyed in the contact header of the SIP request and pass the SIP request with the validated GRUU to Application Servers based on the filter criteria.

For terminations, the S-CSCF may validate the GRUU conveyed in the Request URI header of the SIP request and pass the SIP request with the validated GRUU to Application Servers based on filter criteria.

Application servers may then apply services to the GRUU.

If the SIP message is destined to a GRUU, then the S-CSCF shall associate the request with the corresponding Public User Identity. The S-CSCF will not fork this request, but will direct the call to the identified instance.

S-CSCF shall provide an indication to UE that the SIP request was targeted to a GRUU.

5.20.3 Interrogating-CSCF

When routing requests addressed to a GRUU to the terminating S-CSCF, the I-CSCF uses the contents of the Request URI when querying the HSS. Requests routed to the terminating S-CSCF are addressed to the GRUU.

5.20.3a HSS

The HSS shall remove the P-GRUU as part of the canonicalization process of SIP URIs, to obtain the Public User Identity for identity look-up as it is defined in TS 29.228 [30].

5.20.4 Elements other than UE acting as a UA

5.20.4.1 Using a GRUU

It shall be possible for other IMS elements other than UEs, that act as UAs (e.g. MGCF, Application Server) to use a GRUU referring to itself when inserting a contact address in a SIP message. The MGCF and MRF are not required to store GRUUs beyond a session. If the incoming contact address that is being replaced by the B2BUA functionality contains a GRUU, then the replacement URI in the outgoing SIP message should also contain a GRUU.

If an element so uses a GRUU, it shall handle requests received outside of the session in which the contact was provided.

Routing procedures amongst IMS elements other than UEs that act as UAs are unchanged when GRUUs are in use.

5.20.4.2 Assigning a GRUU

The GRUUs shall either be provisioned by the operator or obtained by any other mechanism. The GRUU shall remain valid for the time period in which features addressed to this URI remains meaningful.

5.21 IMS Multimedia Priority Services Procedures

The IMS Multimedia Priority Service provides Service Users access to IMS services in a prioritised manner.

The P-CSCF shall control the priority of IMS based MPS sessions, using PCC procedures. The P-CSCF shall permit any authorised UE to originate an IMS based MPS session. The detection of MPS sessions is handled by the P-CSCF at the originating network.

PCC shall always be enabled in a network supporting IMS Multimedia Priority Services.

HSS shall store IMS Priority Indication and Priority Level as part of the subscription information.

The P-CSCF at the originating end shall determine whether the INVITE message requires priority handling based on user profile stored during the registration procedure and/or MPS code/identifier provided by the INVITE message. If the session is determined to require priority handling, then P-CSCF inserts/replaces the MPS priority indication in the INVITE and, if the Service User's priority level is known, may include it and forward the INVITE to the S-CSCF. If the Service User's priority level is not known, the P-CSCF includes the priority indication without the Service User's priority level. The S-CSCF routes (using initial Filter Criteria set for the MPS code/identifier) the INVITE to the AS for authentication/authorization for MPS (if needed), and the AS adds the Service User's priority level if it is not in the INVITE already. The AS then forwards the INVITE (with MPS priority indication and the Service User's priority level) to the next entity in the network via the S-CSCF as part of the normal IMS routing. All subsequent SIP messages carry both MPS priority indication and the Service User's priority level.

When the P-CSCF at the originating end determines that priority handling is required, the P-CSCF shall derive session information and interact with the PCRF/PCF providing the session information. The derived session information shall

indicate the priority of the MPS session which depends if the Service User's priority level is known at this stage. The PCC interaction between the P-CSCF and the PCRF/PCF is described in TS 23.203 [54] and TS 23.503 [95].

The P-CSCF at the terminating end shall determine whether the INVITE message requires priority handling based on MPS priority indication and the originating Service User's priority level received from the originating network. If priority handling is required, P-CSCF shall derive the session information based on the Service User's priority level to indicate the priority of the MPS session and interact with the PCRF/PCF providing the session information,

When the terminating user is a Service User, while the session request is from a normal user, the IMS signalling bearer may be given priority treatment when operator policy and MPS (IMS) priority subscription indicates so. For a Service User originating a non-priority session, the IMS signalling bearer may be given priority treatment when operator policy and MPS (IMS) priority subscription indicates so. For IMS media, priority treatment is not required in these cases.

If so configured by the operator, a P-CSCF or an IBCF shall prohibit the negotiation of ECN during SDP offer/answer exchanges and shall not invoke ECN (as described in clause 4.22) for IMS based MPS sessions.

NOTE: Disabling ECN in an IBCF does not prevent a P-CSCF (IMS ALG), subject to roaming agreement, from applying ECN over the access network between a UE and the P-CSCF (IMS ALG) / IMS AGW.

For E-UTRAN access, priority support for EPS bearer is described in TS 23.401 [70].

For 5GS, support Multimedia Priority Service is described in TS 23.501 [93].

5.22 Support of Overload Control

5.22.1 Next-hop monitoring of overload

The following figure depicts an example information flow for the overload control mechanism based on feedback.

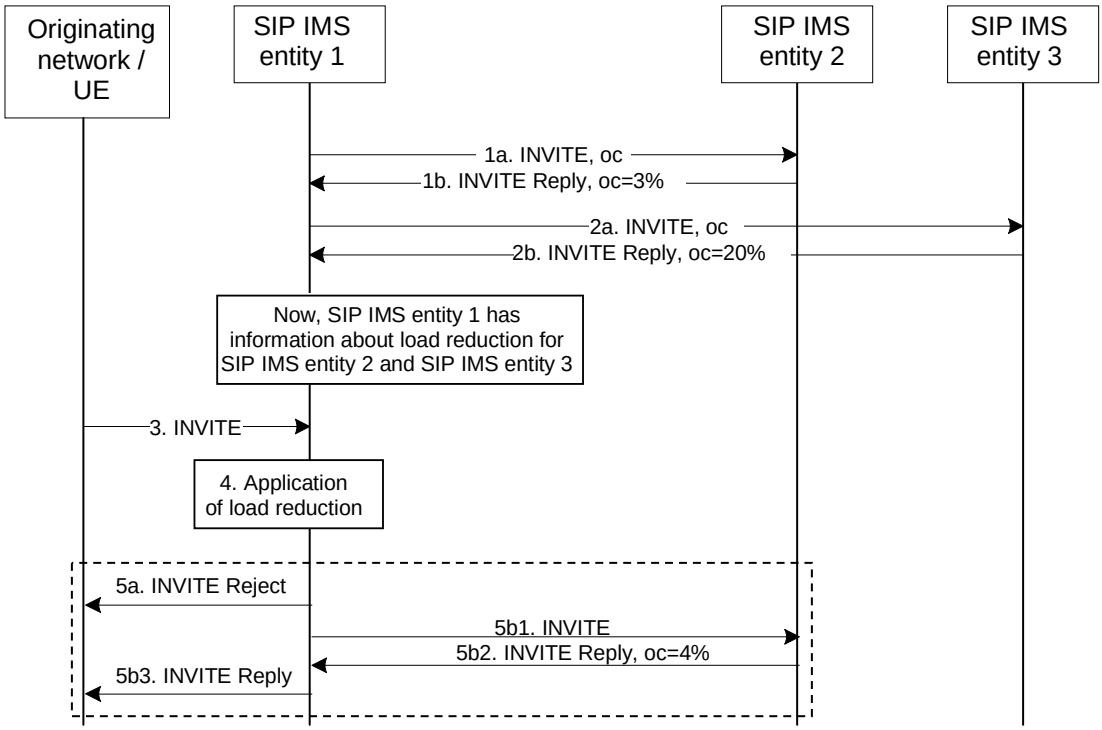


Figure 5.22.1-1: Information flow for Overload Control with next-hop monitoring

1. During a past INVITE, the SIP IMS entity 1 obtained a percentage by which the load forwarded to SIP IMS entity 2 should be reduced.

2. During a past INVITE, the SIP IMS entity 1 obtained a percentage by which the load forwarded to SIP IMS entity 3 should be reduced.

3. Incoming INVITE from Originating side (network or UE). The SIP IMS entity 1 determines that the INVITE has to be forwarded via SIP IMS entity 2.

4. With the information obtained in step 1, the SIP IMS entity 1 either:

   5a. refuses the INVITE request because of overload situation, or

   5b. forwards the INVITE to SIP IMS entity 2 (5b1). The Reply to the INVITE (5b2) can contain updated overload control information.

5.22.2 Filter based Overload Control

The following figure depicts an example information flow for the filter based overload control mechanism.

NOTE: The applicability of the filter based overload control mechanism is not restricted to the IMS entities mentioned on this figure.

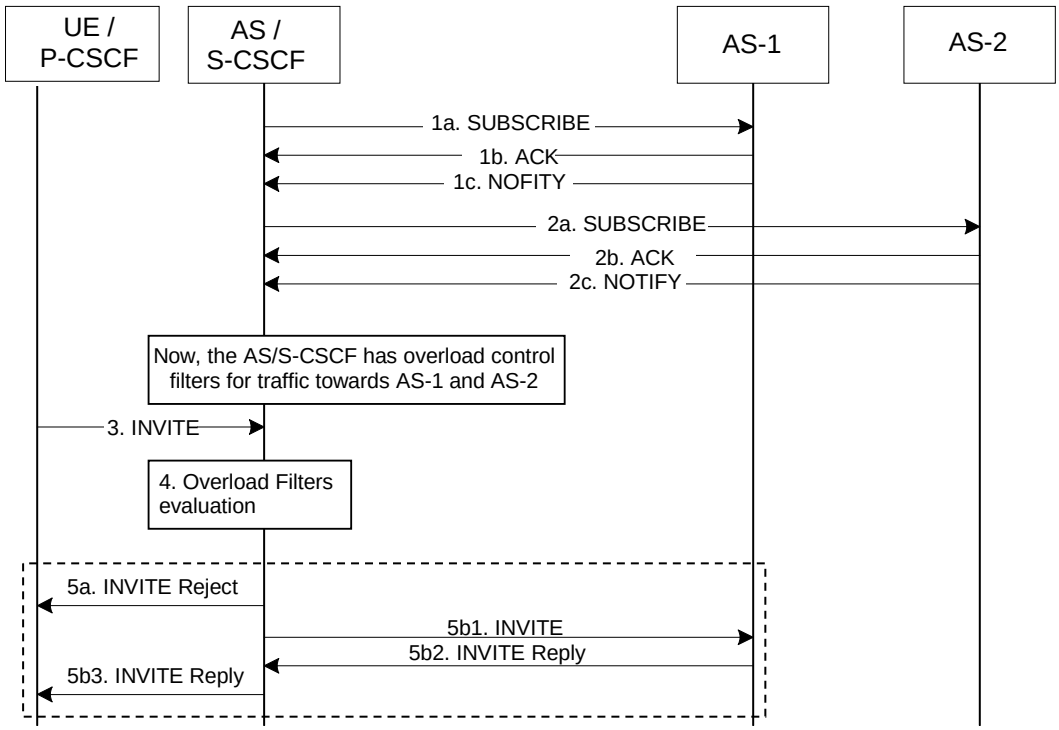


Figure 5.22.2-1 Information flow for AS Overload Control using a filter based mechanism

1. Upon initialization or restart, AS/S-CSCF subscribes to overload event notification of AS-1 and receives overload control filters (1c).

2. Upon initialization or restart AS/S-CSCF subscribes to overload event notification of AS-2 and receives overload control filters (2c)

3. An INVITE comes to AS/S-CSCF.

4-5. The AS/S-CSCF determines where to forward the message (AS-1 in this example), then evaluates whether the contents of the INVITE matches the filters received from AS-1:

   - If the request does not match any filter, the AS/S-CSCF forwards it to AS-1 (5b1);

   - Otherwise, depending on the throttling algorithm, the AS/S-CSCF either:

      - refuses the INVITE request because of the overload situation (5a), or

      - forwards the INVITE to AS-1 (5b1).

Annex A (informative): Information flow template

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

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

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

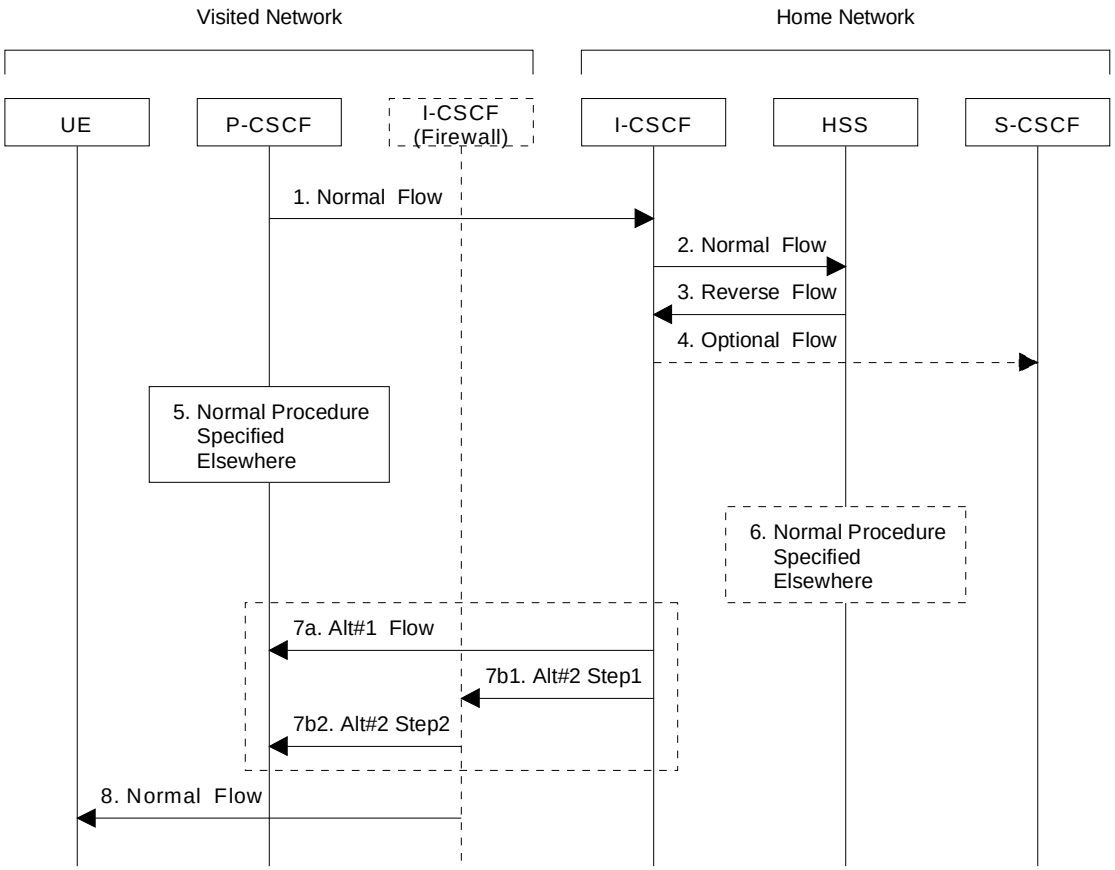


Figure A.1: Information Flow Template

This clause 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 clause. This clause 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):
Void

Annex D (informative):
Void

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

E.0 General

This clause describes the main IP-Connectivity Access Network specific concepts that are used for the provisioning of IMS services over GPRS and EPS system using GERAN and/or UTRAN radio access and/or E-UTRAN (using EPC only).

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

When using EPS the SGSN is responsible for mapping PDP Context(s) to EPS bearers, i.e. the UE (using GERAN/UTRAN) is using PDP Context(s) whereas EPS bearers are used from the SGSN towards the S-GW/P-GW. However, throughout this annex PDP context(s) are used when referring to an IP-CAN bearer for GPRS networks and when a UE is connected to EPS via GERAN/UTRAN access.

When GGSN/P-GW is shown, it represents either a GGSN or a P-GW for a specific UE connection towards a PDN.

E.1 Mobility related concepts

E.1.0 General

The Mobility related procedures for GPRS and EPS are described in TS 23.060 [23] and TS 23.401 [70] respectively and the IP address management principles are described in TS 23.221 [7]. As specified by the GPRS/EPS procedures, the UE shall acquire the necessary IP address(es) as part of the PDP Context activation procedures for GERAN/UTRAN access and Attach (or PDN connectivity)/EPS bearer activation procedure(s) for E-UTRAN.

If the UE changes its IP address due to changes triggered by the GPRS/EPS procedures or according to TS 23.221 [7], then the UE shall re- register in the IMS.

If the UE acquires an additional IP address, then the UE may perform an IMS registration using this additional IP address as the contact address. If IMS registration is performed, this IMS registration may co-exist with the previous IMS registration from this UE and the UE shall be notified that this IMS registration results in multiple simultaneous registrations.

NOTE: The UE can acquire an additional IP address that can be used for registration to the IMS only outside of the EPS.

When a routeing area update or tracking area update is not performed due to the Idle mode Signalling Reduction feature being active (see TS 23.401 [70] for more information), then the UE shall also not perform an IMS re registration because of such routeing area and tracking area change.

Similarly, the UE shall not perform an IMS re registration because the UE has moved between GERAN and UTRAN cells that share the same RAI.

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

In Dual Connectivity with EPC case, the UE shall use the access network information based on the primary cell of the Master RAN node that is serving the UE for network location information when the UE interacts with IMS, regardless whether the IMS traffic is routed via the Master RAN node or the Secondary RAN node or both.

E.1.1 Procedures for P-CSCF discovery

E.1.1.0 General

This clause describes the P-CSCF discovery procedures applicable for GERAN/UTRAN access. All the procedures described in clause 5.1.1 apply with the following additions:

P-CSCF discovery shall take place after GPRS/EPS attach and after or as part of a successful activation of a PDP context (in the case of GERAN/UTRAN access) and EPS bearer (in the case of E-UTRAN access) for IMS signalling using the following mechanisms:

a. For GERAN/UTRAN access: Transfer a Proxy-CSCF address within the PDP Context Activation signalling to the UE, as described in clause E.1.1.1. The UE shall request the P-CSCF address(es) when activating the PDP context. The GGSN/P-GW 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/S-GW for GERAN/UTRAN.

b. For E-UTRAN access: Transfer a P-CSCF address within the EPS Attach or PDN Connectivity Procedures to the UE, as described in clause E.1.1.1. The UE shall request the P-CSCF address(es) in the EPS Attach or PDN Connectivity request. The P-GW shall send the P-CSCF address(es) to the UE when accepting the EPS Default bearer activation. Both the P-CSCF address(es) request and the P-CSCF address(es) shall be sent transparently through the intermediate network entities (e.g. MME/S-GW).

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

E.1.1.1 GPRS/EPS procedure for P-CSCF discovery

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

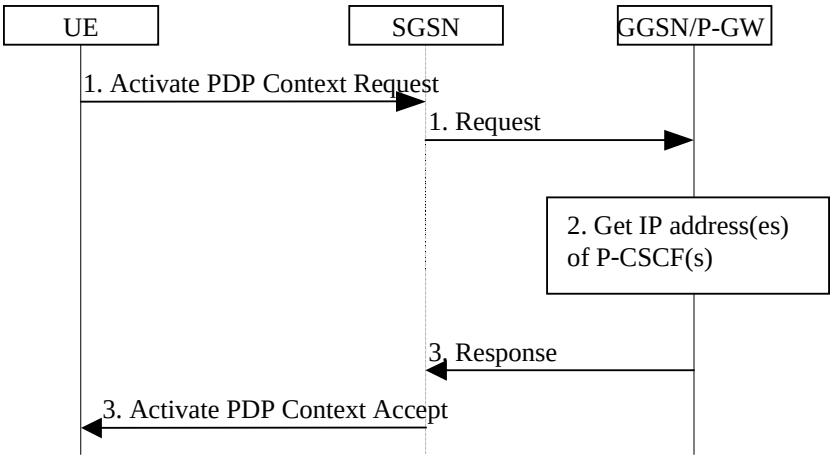


Figure E.1: P-CSCF discovery using PDP Context Activation signalling

1. The UE requests establishment of a PDP context according to clause 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 in the Create PDP Context Request or to the S-GW/P-GW in the Create Default Bearer Request.

2. The GGSN/P-GW 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/P-GW includes the IP address(es) of the P-CSCF(s) in the Create PDP Context Response or in the Create Default bearer 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 CN Subsystem.

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

E-UTRAN access only:

The procedure for E-UTRAN access applies to both Initial E-UTRAN Attach and PDN Connectivity Request.

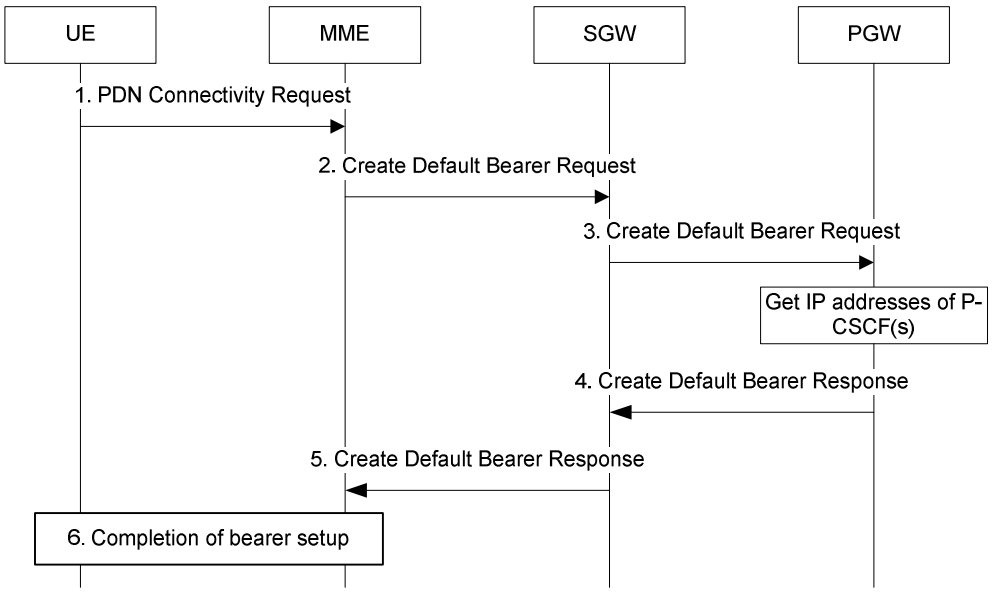


Figure E.2: P-CSCF discovery using EPS bearer activation signalling

1. During Initial Attach/PDN Connection Request, the UE indicates that it requests a P-CSCF IP address(es).
2. The MME sends a Create Default Bearer Request to the S-GW.
3. The S-GW forwards the request to the P-GW and the P-GW 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.
4. If requested by the UE, the P-GW includes the IP address(es) of the P-CSCF(s) in the Create Default Bearer Response.
5. The S-GW forwards the response to the MME
6. Completion of procedures, as described in TS 23.401 [70].

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

E.1.2 Support for Enhanced Coverage for data centric UEs

Support for Enhanced Coverage (CE) for data centric UE is specified in TS 23.401 [70].

If the UE's usage setting is set to "data centric" as defined in TS 23.221 [7] and it is operating in CE mode B then IMS PS voice/video services are not to be used in this IP-CAN.

If the UE's usage setting is set to "data centric" and it is operating in CE mode B, then the UE shall reject any SIP invite for IMS PS voice/video services as per the exisiting IMS procedures. In addition, the UE may deregister from IMS PS voice/video services.

When the UE determines that the radio conditions are suitable for IMS PS voice/video services (e.g. UE is in normal coverage or in CE mode A) then UE may (re-)register for IMS PS voice/video services.

NOTE: How UE determines that the radio conditions are suitable for voice/video services is left upto the UE implementation.

E.2 QoS related concepts

E.2.1 Application Level Signalling for IMS

E.2.1.0 General

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

When the UE uses E-UTRAN access for IMS services, it shall be able to request establishment of a default or dedicated EPS bearer for IM CN Subsystem related signalling.

E.2.1.1 QoS Requirements for Application Level Signalling

It shall be possible to request prioritised handling over the GERAN/UTRAN radio for IM CN Subsystem related signalling by including the Signalling Indication in the QoS IE of the PDP Context to be used for this traffic as described in clause E.2.1a.1.

It shall be possible to request prioritised handling over the E-UTRAN radio for IM CN Subsystem related signalling by including the appropriate QCI value for signalling traffic as specified in TS 23.203 [54], clause 6.1.7, Standardized QCI Characteristics, Table 6.1.7.

E.2.1.2 Requirements for IM CN subsystem signalling flag

The IM CN Subsystem Signalling flag is used to indicate the dedicated signalling PDP context for IMS signalling. If the network operator does not support a dedicated signalling PDP context or the UE does not include the IM CN Subsystem Signalling flag, the network will consider the PDP context as a general purpose PDP context.

The IM CN Subsystem Signalling flag is used to indicate EPS bearer dedicated for IMS signalling. If the network operator does not support a dedicated signalling EPS bearer or the UE does not include the IM CN Subsystem Signalling flag, the network will consider the EPS bearer as a default or dedicated bearer according to TS 23.401 [70].

A PDP context/EPS bearer dedicated for IM CN Subsystem signalling provides dedicated IP-Connectivity Access Network bearers for IM CN subsystem signalling 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/P-GW by the operator of the GGSN/P-GW.

If the PDP context request/EPS bearer is initiated by the IP-CAN, then the GGSN/P-GW may provide a set of UL filters for the PDP context/EPS bearer used for IM CN Subsystem Signalling. The UL filters provide the UE with the rules and restrictions applied by the GGSN/P-GW for the dedicated IM CN Subsystem signalling IP-CAN bearer. The GGSN/P-GW may in addition provide the IM CN subsystem signalling flag to explicitly indicate to the UE the intention of using the PDP context/EPS bearer for IM CN Subsystem related signalling.

Policy and Charging Control functionality can be used to provide additional charging capabilities for dedicated signalling PDP context/EPS bearer dedicated to be used for IMS signalling (as well as for a general-purpose PDP context) as described in clause 4.2.6.

Whether the network is configured to support IM CN signalling flag or Policy and Charging Control functionality or both, is dependent on the operator configuration policy.

The requirements described above also apply in the case of E-UTRAN access and for GERAN/UTRAN access using EPS supporting dedicated bearer for IM CN Subsystem Signalling traffic and where appropriate filters are configured in the P-GW and PCRF as applicable.

E.2.1.3 Application Level Signalling support for IMS services

In order to receive different level of support for application level signalling in a PDP context/EPS bearer, the UE may choose one of the following options:

- Include both the IM CN Subsystem Signalling Flag in the PCO IE and the Signalling Indication in the QoS. This indicates to the network (radio & core) the requirement of using the PDP context/EPS bearer for application level signalling after it has been negotiated with the networks, to provide prioritised handling over the radio interface (as described in sub clause E.2.1.1), with rules and restrictions applied in the network (as described in sub clause E.2.1.2).

  - For GERAN/UTRAN access the UE includes the IM CN Subsystem Signalling Flag in the PCO IE and the Signalling Indication in the QoS IE in the PDP context activation or the Secondary PDP context activation procedure.

  - For E-UTRAN access the UE includes both the IM CN Signalling Flag in the PCO IE and the appropriate QCI value for signalling traffic in the UE Requested Bearer resource Modification procedure.

  NOTE 1: When the UE Requested Bearer Resource Modification procedure is used the IM CN Subsystem Signalling Flag in the PCO IE should be sufficient to trigger the network to provide UL packet filters to the UE, i.e. the UE is not required to provide any meaningful filter information related to the IMS signalling.

- Include the IM CN Subsystem Signalling Flag in the PCO IE in the PDP context activation or the Secondary PDP context activation procedure for GERAN/UTRAN access and for E-UTRAN access in the Attach, PDN Connectivity request or the UE requested bearer resource modification procedure. This indicates to the GPRS/EPS network the requirement of using PDP context/EPS bearer for application level signalling with restricted handling as described in sub clause E.2.1.2, after it has been negotiated with the networks.

  NOTE 2: If the PDN connection is not limited to IMS based services only and the Default EPS bearer is used to support application level signalling for IMS, the UE request for establishment of a general purpose EPS bearer (i.e. a Dedicated non-GBR EPS bearer with a filter set appropriately for a general purpose EPS bearer) might be rejected by the network.

- Utilize a general purpose PDP Context/default EPS bearer with a negotiated QoS profile (this includes the possibility of having the Signalling Indication in the QoS IE for GERAN/UTRAN and the QCI for E-UTRAN.

In the case of E-UTRAN access, when referring to the appropriate QCI for the signalling traffic, the functions described above are fulfilled as specified in TS 23.203 [54] using EPS bearers.

The IM CN Subsystem signalling flag is used to reference rules and restrictions on the PDP context/EPS bearer used for application level signalling, as described in clause E.2.2.

The Signalling Indication in the QoS IE or the appropriate QCI for signalling traffic provides prioritised handling over the radio interface. The Signalling Indication in the QoS IE is detailed in TS 23.107 [55] and clause E.2.1a.1 and the appropriate QCI for signalling traffic is detailed in TS 23.203 [54].

Depending on the operator's policy, one or more of the above combinations may be allowed in the GPRS/EPS network.

E.2.1a PDP context/EPS Bearer procedures for IMS

E.2.1a.1 Establishing PDP Context/EPS bearer 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/EPS bearer for IM Subsystem related signalling. For this purpose it uses the mechanism described in this clause and Application Level Signalling in sub clauses E.2.1.1, E.2.1.2 & E.2.1.3.

When the bearer establishment is controlled or a bearer establishment is requested (in the case of EPS) by the UE, in order to establish a PDP context/EPS bearer for IM CN Subsystem related signalling, the UE shall be able to include the IM CN subsystem signalling flag in the PDP context activation/UE Requested Bearer Resource Modification procedure.

This indicates to the network the intention of using the PDP context/EPS bearer for IM CN Subsystem related signalling.

For GERAN/UTRAN access:

To establish a PDP context for IM CN Subsystem related signalling with prioritised handling over the radio interface, the UE shall be able to set the Signalling Indication in the QoS IE in the PDP context activation procedure and the Secondary PDP context activation procedure. The Signalling indication in the QoS IE indicates to the radio and core networks the requirement for enhanced handling over the radio interface, once it has been negotiated with the networks.

A request for a general purpose PDP context having the "signalling indication" within the QoS IE may be accepted or downgraded according to operator policy configured at the GGSN using the usual QoS negotiation mechanisms described in TS 23.060 [23]. It shall not be possible to modify a general purpose PDP context into a dedicated PDP context for IM CN Subsystem related signalling and vice versa.

For E-UTRAN access:

The (default or dedicated) EPS bearer for IMS signalling may be established from network side at Attach/UE Requested PDN connectivity Request time, in which case the appropriate QCI for signalling traffic and the packet filters will provide the necessary QoS and any restrictions applicable on packets sent over this EPS bearer.

A request for an EPS bearer having the appropriate QCI for signalling traffic according to TS 23.203 [54], may be either accepted or rejected according to operator policy configured at the P-GW i.e. there is no QoS negotiation mechanism used in EPS.

In order to establish a Dedicated EPS bearer for IM CN Subsystem related signalling, the UE shall be able to request the appropriate QCI for signalling traffic as specified in TS 23.203 [54] in the UE Requested Bearer Resource Modification procedure. This indicates to the radio and core network the requirement for enhanced handling over the radio interface, once it has been accepted by the network. It shall not be possible to modify an existing EPS bearer in order to convert it to be dedicated for IM CN Subsystem related signalling and vice versa.

For all 3GPP accesses:

The IM CN Signalling Flag in the PCO IE is used to reference rules and restrictions on the PDP context/EPS bearer used for application level signalling, as described in clause 4.2.6. Based on operator policy the "Signalling Indication" in the QoS IE or the appropriate QCI for signalling traffic may be allowed only if the "IM CN Subsystem Signalling" flag is present in the PCO IE.

The IM CN subsystem signalling flag and the Signalling Indication in the QoS IE or the appropriate QCI for signalling traffic may be used independently of each other.

E.2.1a.2 Deletion of PDP Context/EPS bearer used to transport IMS SIP signalling

If the GPRS subsystem deletes the PDP Context used to transport IMS SIP signalling, then according to clause 5.10.3.0 the UE or GGSN shall initiate a procedure to re-establish (or modify where possible) a PDP Context for IMS signalling transport. If there are any IMS related PDP contexts active, the re-establishment of the PDP context to transport IMS signalling shall be performed by using the Secondary PDP Context Activation Procedure (or the Network Requested Secondary PDP Context Activation Procedure if initiated by the GGSN) as defined in TS 23.060 [23].

If the EPC system deletes the Dedicated EPS bearer used to transport IMS SIP signalling, then according to clause 5.10.3.0 the UE or PDN Gateway shall initiate a procedure to re-establish (or modify where possible) an EPS bearer for IMS signalling transport. If there are any IMS related EPS bearers active, the re-establishment of the EPS bearer to transport IMS signalling shall be performed by the UE using the UE Requested Bearer Resource Modification procedure or the PDN Gateway using the Dedicated bearer activation procedure as defined in TS 23.401 [70].

The failure in re-establishing the ability to communicate towards the UE results also in the P-CSCF/PCRF being informed that the IMS SIP signalling transport to the UE is no longer possible which shall lead to a network initiated session release (initiated by the P-CSCF) as described in clause 5.10.3.1 if any IMS related session is still ongoing for that UE. Additionally, the P-CSCF shall reject subsequent incoming session requests towards the remote endpoint indicating that the user is not reachable, until either:

- the registration timer expires in P-CSCF and the user is de-registered from IMS;
- a new Register message from the UE is received providing an indication to the P-CSCF that the PDP Context/EPS bearer used for IMS SIP Signalling transport for that user has become available again and session requests can be handled again.

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

E.2.2.0 General

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

- the general requirements described in clause 4.2.5.

  for E-UTRAN access, the QoS handling is described in TS 23.401 [70], TS 23.203 [54].

- for GERAN/UTRAN access, the requirements described in this clause so as to guarantee the QoS requirement associated with an IM CN subsystem session 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 (received from the GGSN in the case of IP-CAN Bearer Control) to the RAN, the CN, and the IP BS manager, where appropriate QoS negotiation and resource allocation are activated accordingly. When UMTS QoS negotiation mechanisms are used to negotiate end-to-end QoS, the translation function in the GGSN shall co-ordinate resource allocation between UMTS BS Manager and the IP BS Manager.

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

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

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

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

All associated media 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/EPS bearer.

E.2.3 Interaction between GPRS/EPS QoS and session signalling

E.2.3.0 General

The generic mechanisms for interaction between QoS and session signalling are described in clause 5.4.7, the mechanisms described there are applicable to GERAN/UTRAN/E-UTRAN-accesses as well.

This clause describes the GERAN/UTRAN/E-UTRAN-access-specific concepts.

At PDP context/EPS bearer setup the user shall have access to either GPRS/EPS without Policy and Charging Control, or GPRS/EPS with Policy and Charging Control. The GGSN/P-GW shall determine the need for Policy and Charging Control, possibly based on provisioning and/or based on the APN of the PDN connection.

For the GPRS/EPS without Policy and Charging Control 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/EPS roaming agreements.

For the GPRS/EPS with Policy and Charging Control case, policy decisions (e.g., authorization and control) are also applied to the bearer.

The GGSN/P-GW contains a Policy and Charging Enforcement Function (PCEF).

E.2.3.1 Resource Reservation with Policy and Charging Control

Depending on the Bearer Control Mode, as defined in TS 23.060 [23], selected for the GPRS IP-CAN session, resource reservation shall be initiated either by the UE or by the IP-CAN itself. IMS media which require resource reservation is always mapped to a dedicated bearer, i.e. a dedicated EPS bearer or a PDP context activated using the Secondary PDP Context Activation Procedure. For IP-CAN initiated resource reservation, the PCRF has the responsibility to ensure that a dedicated bearer is used for media which require resource reservation.

For GERAN/UTRAN the UE initiates the activation or the modification of an existing PDP Context for the media parameters negotiated over SDP using the procedures for Secondary PDP-Context Activation and MS-Initiated PDP Context Modification respectively as defined in TS 23.060 [23] subject to policy control.

Otherwise, the GGSN/P-GW within the GPRS IP-CAN initiates the activation or the modification of an existing PDP Context for the media parameters negotiated over SDP using the procedures for Network Requested Secondary PDP Context Activation and GGSN/P-GW-Initiated PDP Context Modification respectively as defined in TS 23.060 [23].

For E-UTRAN, the UE initiates the resource reservation request for the media parameters negotiated over SDP using procedure UE Requested Bearer Resource Modification procedure as defined in TS 23.401 [70] subject to policy control.

Otherwise, the P-GW within the EPS IP-CAN initiates the activation or the modification of an existing Dedicated EPS bearer for the media parameters negotiated over SDP using the procedures for Dedicated bearer activation and PDN GW initiated bearer modification with or without bearer QoS update as specified in TS 23.401 [70].

The request for GPRS/EPS QoS resources may be signalled independently from the request for IP QoS resources by the UE. At the GPRS/EPS BS Level, the PDP Context activation / UE Requested Bearer Resource Modification shall be used by the UE for QoS signalling. At the IP BS Level, RSVP may be used for QoS signalling.

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

E.2.4.0 General

In the event of loss of coverage for GERAN/UTRAN access, TS 23.060 [23] defines the Iu or RAB Release procedures. In the case of PDP context/EPS bearer with streaming or conversational class the maximum bitrate of the GTP tunnel between SGSN and GGSN or between SGSN and S-GW/P-GW is modified to 0 kbit/s in up- and downlink direction. This is indicated to the P-CSCF/PCRF by performing an IP-CAN session modification procedure (see TS 23.203 [54]) as shown in Figure E.3. This procedure also applies to PDP Contexts/EPS bearer used for IMS SIP Signalling transport. For loss of coverage in the case of other PDP contexts/EPS bearer (background or interactive traffic class), the PDP context/EPS bearer is preserved with no modifications and therefore no indication to the P-CSCF/PCRF.

In the event of loss of coverage for E-UTRAN access, TS 23.401 [70] defines the S1 release Procedure. This procedure releases the EPS bearers. This is indicated to the P-CSCF/PCRF by performing an IP-CAN session modification procedure (see TS 23.203 [54]) as shown in figure E.3. The UE will become aware of the release of the GBR bearer the next time it accesses the E-UTRAN network via the procedures as described in the clauses 5.3.3 and 5.3.4 of TS 23.401 [70].

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

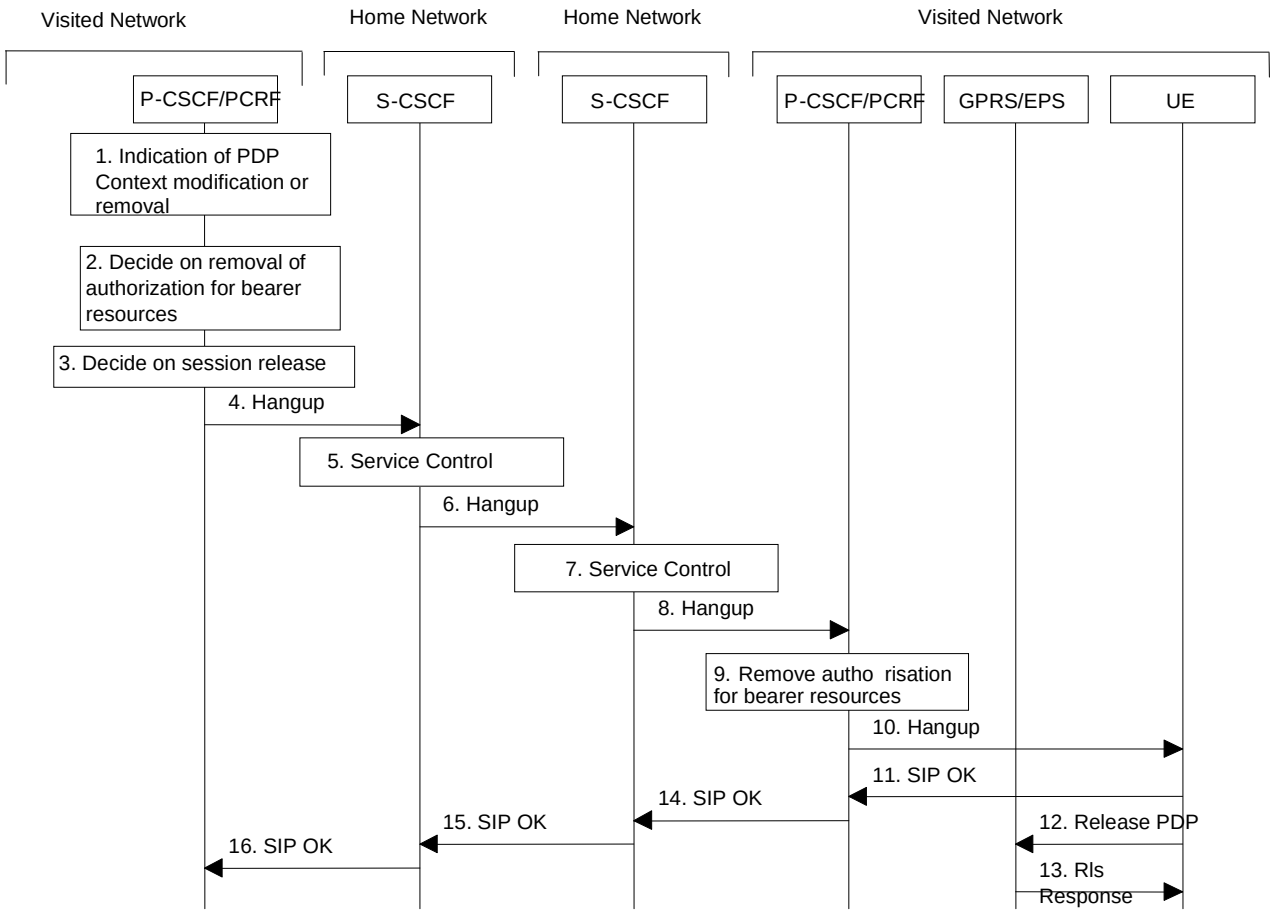


Figure E.3: Network initiated session release - P-CSCF initiated after loss of radio coverage

1. In the case of GERAN/UTRAN access, 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 and between SGSN and S-GW /P-GW is modified to 0 kbit/s in up- and downlink direction. The P-CSCF/PCRF receives an indication of PDP context/EPS bearer modification or EPS bearer removal. This also applies to PDP Contexts/EPS bearer used for IMS SIP Signalling transport.

In the case of E-UTRAN access, loss of radio coverage causes the GBR bearers to be released in the network and P-CSCF/PCRF is notified appropriately.

2. It is optional for the P-CSCF/PCRF to deactivate the affected bearer and additional IP bearers (e.g. an IP bearer for chat could still be allowed). If the P-CSCF decides to terminate the session then the P-CSCF/PCRF removes the authorization for resources that had previously been issued for this endpoint for this session (see TS 23.203 [54]).

3. The P-CSCF decides on the termination of the session. In the event of the notification that the signalling transport to the UE is no longer possible, the P-CSCF shall terminate any ongoing session with that specific UE. If the P-CSCF decides to terminate the session then the P-CSCF/PCRF removes the authorization for resources that had previously been issued for this endpoint for this session. (see TS 23.203 [54]).

The following steps are only performed if the P-CSCF/PCRF has decided to terminate the session.

When receiving an indication that bearer resources are not available for a voice media negotiated in a multimedia session that is in pre-alerting phase e.g. due to weak E-UTRAN coverage, the P-CSCF performs the procedures according to clause 6.2.1.3a or clause 6.2.2.3a in TS 23.237 [67].

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

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

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

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

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

9. The P-CSCF/PCRF removes the authorization for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the GPRS/EPS system 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. The IP network resources that had been reserved for the message receive path to the UE for this session are now released. Depending on the Bearer Control Mode selected for the IP-CAN session, the release of previously reserved resources shall be initiated either by the UE or by the IP-CAN itself. The UE initiates the release of the IP-CAN bearer resources as shown in figure E.3. Steps 12 and 13 may be done in parallel with step 11. Otherwise, the GGSN/P-GW within the GPRS/EPS IP-CAN initiates the release of the bearer PDP context/EPS bearer deactivation after step 9 instead.

13. The GPRS/EPS system releases the PDP context/EPS bearer. The IP network resources that had been reserved for the message receive path to the UE for this session are now released. This is initiated from the GGSN/P-GW. 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.

E.3 Address and identity management concepts

E.3.1 Deriving IMS identifiers from the USIM

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

The Private User Identity shall be derived from the USIM's IMSI, which allows for uniquely identifying the user within the 3GPP operator's network. The format of the Private User Identity derived from the IMSI is specified in TS 23.003 [24].

- A Temporary Public User Identity shall be derived from the USIM's IMSI, and shall be used in SIP registration procedures. The format of the Temporary Public User Identity is specified in TS 23.003 [24].

It is strongly recommended that the Temporary Public User Identity is set to barred for SIP 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 SIP initial registration, re-registration and mobile initiated de-registration procedures.
- The implicitly registered Public User Identities shall be used for session handling, in non-registration SIP messages and may be used at subsequent SIP registration procedures.
- A Temporary Public User Identity shall only be available to the CSCF and HSS nodes.

NOTE: If a Temporary Public User Identity is used, the user can not initiate any sessions until the implicitly registered public identities are available in the UE.

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

When a Temporary Public User 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.

E.4 Void

E.5 IP version interworking in IMS

A PDP context & its associated additional PDP contexts (i.e. PDP contexts associated to the same IP address/prefix) support either PDP type IPv4 or IPv6 or IPv4v6. For communication with the IMS, the UE establishes an IPv4 PDN connection or an IPv6 PDN connection or an IPv4IPv6 PDN connection via PDP contexts/EPS bearers. Termination of this PDP context/EPS bearer will normally trigger de-registration of IMS application first. Hence, the PDP context/EPS bearer that has been established for IMS communication must be retained for the UE to establish a SIP session via the IMS with an IPv4 SIP client.

As such, any interworking on IP version on the application level (i.e. IMS & SIP) need to work with the architecture requirement from GPRS/EPS of maintaining the IP connectivity over GPRS/EPS by maintaining the PDP contexts/EPS bearers.

For IMS perspective, a user may be connected either to a home GGSN/P-GW or a visited GGSN/P-GW depending on the configuration as specified in TS 23.221 [7].

E.6 Usage of NAT in GPRS/EPS

There should be no NAT (or its existence should be kept transparent towards the UE) located between the GGSN/P-GW and the P-CSCF, which is possible as they are either located within the same private network and share same address space, or both the UE and the P-CSCF are assigned globally unique IP addresses (see Annex M).

NOTE: If the UE discover a NAT between the UE and the P-CSCF, the UE might send frequent keep-alive messages and that may drain the UE battery.

E.7 Retrieval of Network Provided Location Information in GPRS/EPS

Information related to the location of the user provided by the access network may be required in IMS in order to comply with regulatory requirements (e.g. data retention, lawful interception) and/or in order to enable certain types of added value services based on the user's location.

Depending on usage scenario, the following mechanisms are defined and can be used to retrieve the user location and/or UE Time Zone information from the access network when using GPRS and/or EPS to access IMS:

- The P-CSCF can retrieve the user location and/or UE Time Zone information using PCC mechanisms as specified in TS 23.203 [54] and in TS 29.214 [11]. Operator policy determines whether to provide the the user location and/or UE Time Zone information from the access network in the INVITE request or within a subsequent message of the dialog.

- When the user location and/or UE Time Zone information is required from the access network but not already available (e.g. when required in an INVITE request, when it is needed prior to session delivery, or when call is broken out to a MGCF), an IMS AS can trigger the retrieval of the user location and/or UE Time Zone information from the SGSN/MME via the HSS as specified in TS 29.328 [79] and as described in clause 4.2.4a.

Operator policies at P-CSCF and IMS AS need to be coordinated in order to ensure that the appropriate method to retrieve the user location and/or UE Time Zone information is used for specific scenarios according to operator's preferences. The IMS entity that retrieves the user location and/or UE Time Zone information shall have the capability to further distribute the information to other IMS entities once it has been retrieved. User location and/or UE Time Zone information provided in the signaling by the network shall be possible to distinguish from user location information provided by the UE. The transfer of the user location and/or UE Time Zone information within IMS signalling shall not affect the transfer of any UE provided user location information. Information flows on how user location and/or UE Time Zone information can be further distributed within IMS depending on the alternative mechanism used can be found in Annex R.

The level of granularity of user location information may be changed at network/trust boundaries. Thus, the level of user location information granularity that can be retrieved by an IMS AS via the HSS-based procedures in roaming scenarios depends on inter-operator agreement, and needs to be aligned with policies in the P-CSCF.

E.8 Geographical Identifier

The Geographical Identifier identifies a geographical area within a country or territory. It may be described in a geospatial manner (e.g. geodetic coordinates) within a country or territory or as civic user location information (e.g. a postcode, area code, etc.), or use an operator-specific format. It is assumed that a given cell cannot belong to more that one area identified by a Geographical Identifier.

A network which requires the Geographical Identifier to be generated in the IMS may implement a mapping table between an (E)CGI (received as part of Access Network Information) and a Geographical Identifier. The P-CSCF or an IMS AS may then, based on operator policy, use this mapping table to convert the user location into a Geographical Identifier, and insert the Geographical Identifier in the SIP signalling, thus enabling routing decision in downstream IMS entities or interconnected network.

E.9 Support for Paging policy differentiation for IMS services

As a network configuration option, where P-CSCF and P-GW are located in the same PLMN, it shall be possible for the P-CSCF for terminating signalling to identify conversational voice as defined in IMS multimedia telephony service, TS 22.173 [53].

NOTE 1: This feature may be extended for other IMS services if so desired as long as the same principles are reused.

P-CSCF may support Paging Policy Differentiation (as defined in TS 23.401 [70]) for a specific IMS service by marking packet(s) to be send towards the UE related to that IMS service. For such an IMS service, a specific DSCP (IPv4) value and/or a specific Traffic Class (IPv6) value are assigned by local configuration in the P-CSCF.

When Paging Policy Differentiation is deployed in a PLMN, all P-CSCF entities of that PLMN shall homogeneously support it and shall be configured with the same policy for setting the specific DSCP (IPv4) and/or Traffic Class (IPv6) values used by P-CSCF for that feature.

NOTE 2: It is assumed that the DSCP / Traffic Class header is not rewritten by intermediate routers between the P-CSCF and the P-GW.

E.10 Support of RAN Assisted Codec Adaptation

RAN assisted codec adaptation is a functionality that assists codec rate adaptation for Multimedia Telephony based on access network bitrate recommendation (ANBR) messages that the UE receives in the access stratum of the 3GPP access network (E-UTRA RAT). The functionality is defined in TS 26.114 [76] and affects the following system entities: UE, RAN, P-CSCF and PCRF/PCF.

During SIP registration or emergency registration if the network supports ANBR as specified in TS 26.114 [76] and RAN-assisted codec adaptation as specified in TS 36.300 [99] and TS 36.321 [100], the P-CSCF indicates'anbr' support to the UE.

NOTE: When IMS services are provided in deployments with home routed traffic a supporting P-CSCF does not indicate its capability to handle the 'anbr' SDP attribute unless it is configured to know that the roaming partner supports RAN assisted codec adaptation with access network bitrate recommendation.

As specified in TS 26.114 [76]:

- support for RAN assisted codec adaptation can be used only if it is supported end-to-end.
- support for RAN assisted codec adaptation is assumed to be homogeneous in a PLMN i.e. all affected system entities in a PLMN including equivalent PLMNs need to support it. RAN support is required on E-UTRA.
- the UE includes the 'anbr' attribute in the SDP offer only if the P-CSCF has indicated its ability to handle it.
- the P-CSCF forwards the 'anbr' attribute if it has received it in the SDP offer from the UE.
- when the 'anbr' attribute is successfully negotiated end-to-end, the PCRF/PCF uses MBR>GBR setting for the corresponding IP-CAN bearer relying on RAN assisted codec adaptation.

A UE supporting Multimedia Telephony and RAN assisted codec adaptation shall support the procedures described in TS 26.114 [76].

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

This annex provides some background information related to clause 5.4.5.3.

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

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

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

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

- If a UE registered to the S-CSCF uses a Globally Routable User Agent URI (GRUU) assigned by the S-CSCF as a contact address when establishing a dialog, then the S-CSCF needs to remain in the signalling path in order to translate mid-dialog requests addressed to that contact address.

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

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

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

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

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

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

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

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

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

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

Annex G (normative): Reference Architecture and procedures when the NAT is invoked between the UE and the IMS domain

G.1 General

This clause specifies concepts of IMS service provisioning for the following scenarios:

1. When a device or devices that perform address and/or port translation are located between the UE and the P-CSCF performing translation both of signalling and media packets.

2. When IP address and/or port translation is needed between the IP-CAN and the IMS domain (e.g. different IP versions) on the media path only. This scenario covers the case when a device or devices that perform address and/or port translation are located on the media path only.

The IP address and/or port translation device can be a NAT or a NAPT as defined in IETF RFC 2663 [34]. Another type of translation is NA(P)T-PT as specified in IETF RFC 2766 [33]. In the rest of this clause NAT will be used for all of the devices that perform one or more of NA(P)T and NA(P)T-PT functions.

Note that the procedures of this Annex shall only be applied when they are necessary. If the terminal and/or the access network provide a transparent way of NAT traversal or no IP address translation is needed between the IP-CAN and the IMS domain on the media path then the function as defined in this Annex shall not be invoked.

It is expected the NAT traversal methods of this Annex will co-exist. UE may support one or more of these methods. It shall be possible for an operator to use one or more of NAT traversal methods in its IMS domain. The selection of the method for a particular case shall depend on the UE's capabilities, the capabilities of the network and policies of the operator.

Where possible, usage of these procedures shall not adversely impact usage of power saving modes in the UEs, i.e. when the NAT is integrated with the IMS Access Gate way which is under operator control, the reserved temporary addresses and port (binding) should be retained without requiring keep-alive messages from the UE. If the access type to IMS is GPRS, then the UE is not required to initiate any keep-alive messages, see clause E.6 for more information.

NOTE: A solution to allow power saving modes when non-operator controlled NATs are used is not defined in this version of the specification.

G.1.1 General requirements

The following list contains requirements that a NAT Traversal solution should satisfy:

- Support multiple UEs (on one or more devices) behind a single NAT;
- Support both inbound and outbound requests to and from UEs through one or more NAT device(s);
- Support the traversal of NATs between the UE and the IMS CN;
- Support uni-directional and bi-directional media flows;
- Minimize additional session setup delay.

G.2 Reference models

This clause describes various reference models which can be used for NAT traversal.

G.2.1 IMS-ALG and IMS Access Gateway model

Figure G.1 presents the general reference model for IMS access when both the signalling and media traverses NAT devices. Figure G.2 presents the general reference model when IP address translation is needed between the IP-CAN and the IMS domain. The IMS network architecture is the same for both cases. The NAT integrated with the IMS Access Gateway is under operator control in this reference model.

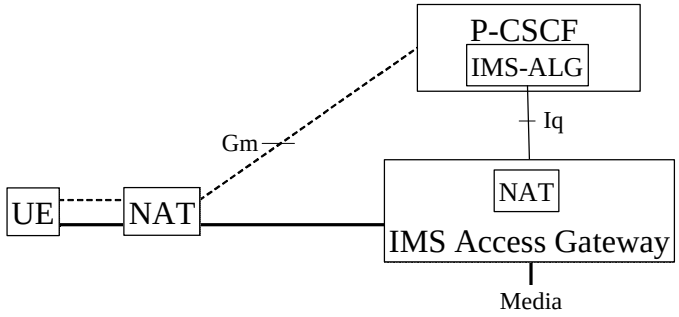


Figure G.1: Reference model for IMS access when both the signalling and media traverses NAT

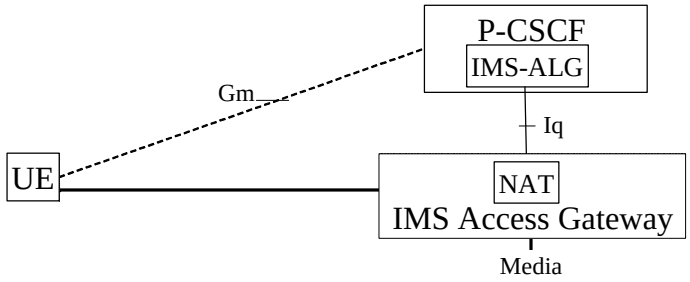


Figure G.2: Reference model for IMS access when NAT is needed between the IP-CAN and the IMS domain

G.2.2 ICE and Outbound reference model

Figure G.2a presents the general reference model for IMS access when both the signalling and media traverses NAT devices. Functional elements with dashed lines represent optional functionality. The transport of the Gm signalling is also subject to the policy enforcement.

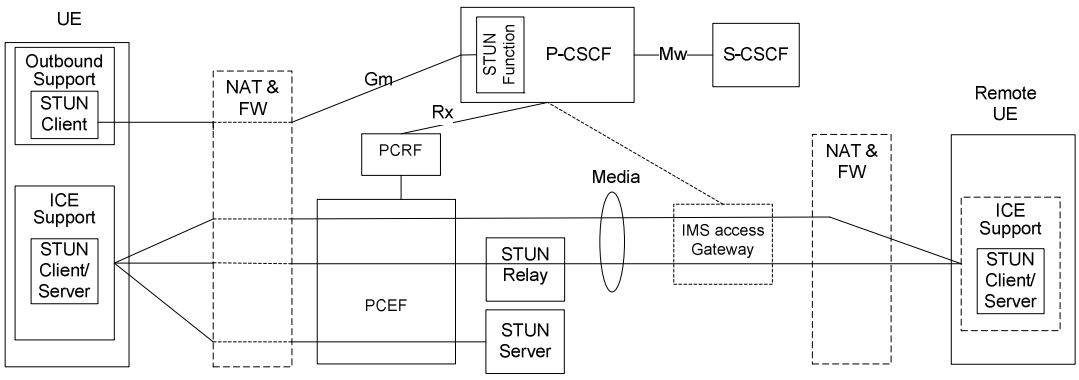


Figure G.2a: Reference model for ICE and Outbound Methodology

The STUN Function shown within the P-CSCF is a limited STUN Server for supporting STUN keep-alive messages as described in clause G.5.3.2.

For deployments where the IMS Access gateway (or other media manipulating functional entities, such as a MRFP, are used (see clause G.2.1), such functional entities shall be placed on the network side of the STUN server and STUN relay server (i.e. not between the UE and the STUN server or STUN relay server) as shown in figure G.2a. Otherwise they will prevent STUN messages from reaching the STUN Relay/Server outside of a session.

G.3 Network elements for employing the IMS-ALG and IMS Access Gateway

G.3.1 Required functions of the P-CSCF

When supporting IMS communication for a UE residing behind a NAT or when IP address translation is needed between the IP-CAN and the IMS domain on the media path only, the P-CSCF may include the IMS-ALG function that is defined in Annex I of this specification. The following functions shall be performed in the P-CSCF:

1) The P-CSCF shall be able to recognize that the UE is behind a NAT device or IP address translation is needed between the IP-CAN and the IMS domain on the media path only.

2) The IMS-ALG function in the P-CSCF shall control the IMS Access Gateway, e.g. request transport addresses (IP addresses and port numbers) from the IMS Access Gateway, and shall perform the necessary changes of the SDP parameters.

3) The IMS-ALG function in the P-CSCF shall perform the necessary changes of headers in SIP messages.

4) The IMS-ALG function in the P-CSCF shall be able to support scenarios where IMS CN domain and IP-CAN use the same IP version and where they use different IP versions.

5) The IMS-ALG function in the P-CSCF shall be able to request opening and closing of gates on the IMS Access Gateway.

6) The IMS-ALG function in the P-CSCF may configure the IMS Access Gateway to police the remote source address/port of the associated media flow(s).

7) The IMS-ALG function in the P-CSCF may configure the IMS Access Gateway to police the bandwidth/data rate of the associated media flow(s) (see TS 23.333 [73]).

8) The IMS-ALG may configure the IMS Access Gateway to set the differentiated service code point for egress packets to an explicit value or alternately to allow the differentiated service code point of the ingress packet to be copied into the corresponding egress packet. An IMS Access Gateway can also support differentiated service code point marking based on local configuration.

9) The IMS-ALG may request an IMS Access Gateway to detect and report inactive media flows.

G.3.2 Required functions of the IMS Access Gateway

The required functions of the IMS Access Gateway for NAT translation are the following:

1) It allocates and releases transport addresses according to the requests coming from the IMS-ALG function of the P-CSCF.

2) It ensures proper forwarding of media packets coming from or going to the UE.

3) It shall support the scenarios where IMS CN domain and IP-CAN use the same IP version and where they use different IP versions.

4) It shall support opening and closing of gates, under control of the IMS-ALG.

5) It shall support policing of the remote source address/port and bandwidth/data rate of media flows, as configured by the IMS-ALG.

6) It shall support the setting of the differentiated service code point for egress packets as configured by the IMS-ALG or else based on local configuration.

7) It may support detection and reporting of inactive media flows.

8) It shall support remote NAT traversal.

G.3.3 Iq reference point

The Iq reference point is between the P-CSCF and the IMS Access Gateway. It conveys the information necessary for the IMS-ALG to activate the procedures defined in clause G.3.2. Those procedures are further detailed in TS 23.334 [74].

G.4 Procedures for employing the IMS-ALG and IMS Access Gateway

G.4.1 General

The procedures described in this clause are applied in addition to the procedures of the P-CSCF described in the other clauses of this specification.

G.4.2 NAT detection in P-CSCF

When supporting the IMS-ALG function, the P-CSCF, based on information received in a SIP request message (e.g. a REGISTER request), shall detect if there is NAT between the UE and itself and shall make a decision if IMS-ALG function shall be invoked for the session of subscriber. In addition to when a NAT is detected between the UE and the P-CSCF, the IMS-ALG function may be invoked for other reasons (e.g. UEs using IP address from a Private IP address range).

G.4.3 Session establishment procedure

This procedure is applied when P-CSCF invokes the IMS-ALG function for a session. This can happen at terminating side if the called party is behind a NAT or at the originating side if the session initiator is behind a NAT. Both cases are handled in the P-CSCF and the IMS Access Gateway as described in this clause.

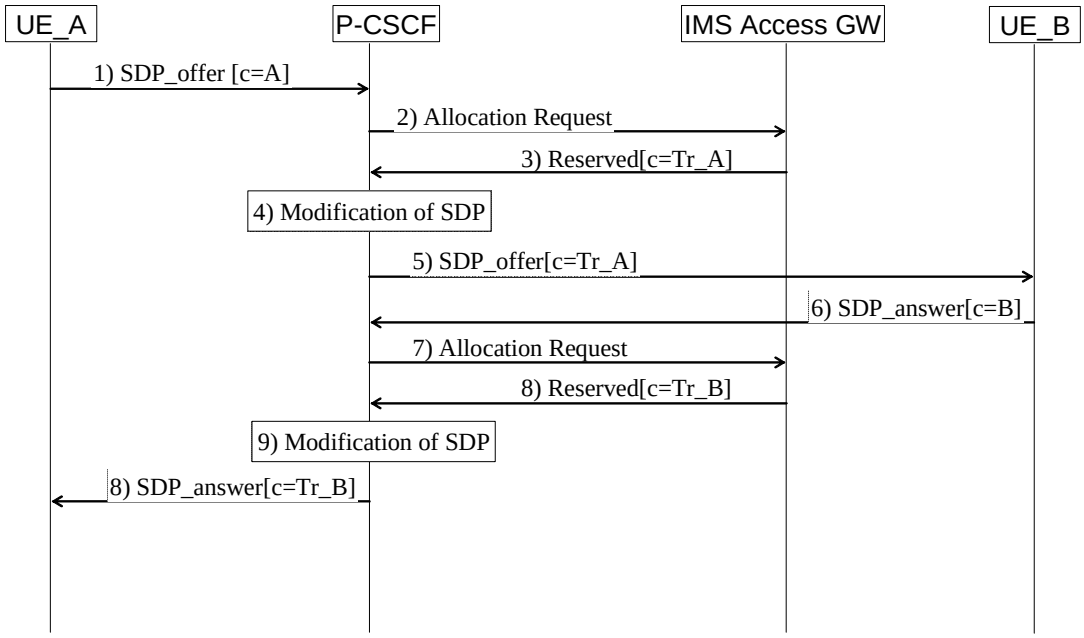


Figure G.3: Session establishment procedure with NAT traversal

NOTE 1: In figure G.3 if UE_A belongs to the P-CSCF (originating case) then there will be IMS elements, i.e., CSCFs, between the P-CSCF and UE_B. If UE_B belongs to the P-CSCF (terminating case) then there will be IMS elements, i.e., CSCFs, between the P-CSCF and UE_A.

NOTE 2: The Transport address refers to both the IP address and Ports (see definition in clause 3.1).

1) The P-CSCF receives a SIP message with an SDP offer from UE_A and decides to invoke the IMS-ALG function for this session. The session can either an originating or a terminating session. The SDP offer contains the transport address(es) of UE_A where the media flow(s) should be sent.

2) The P-CSCF requests a transport address for each media flow from the IMS Access Gateway. Each request contains sufficient information to determine the side of the IMS access gateway that the transport request is being requested for. (e.g. local or remote side with respect to UE_A).

3) The IMS Access Gateway reserves one of its transport addresses for the given side of the media flow and this transport address is sent back to the P-CSCF. The IMS Access Gateway shall keep the reserved temporary transport address (binding) until the session is released.

4) The P-CSCF changes the original transport address(es) of the SDP offer to the transport address(es) received from the IMS Access Gateway.

5) The P-CSCF forwards the SIP message with the modified SDP offer according to the normal routing procedures.

6) UE_B sends back a SIP message with an SDP answer, which is forwarded to the P-CSCF according to the normal SIP message routing procedures.

7) The P-CSCF requests a transport address for each media flow in the routing domain of its own IMS network from the IMS Access Gateway. The request contains sufficient information to correlate to the transport address request performed in step 2.

NOTE: If some of the offered media flows are rejected in the answer, then the P-CSCF shall indicate this to the IMS Access Gateway. The IMS Access Gateway can release the resources (e.g., the transport address) reserved for that media flow. The P-CSCF may indicate directly to release the resources.

8) The IMS Access Gateway reserves one of its transport addresses for the given side of the media flow and this transport address is sent back to the P-CSCF.

9) The P-CSCF changes the original transport address(es) of the SDP answer to the transport address(es) received from the IMS Access Gateway.

10) The P-CSCF forwards the SIP message with the modified SDP answer according to the normal SIP message routing procedures.

G.4.4 Session release procedure

This procedure is applied when a session has to be released, for which the IMS-ALG function is invoked.

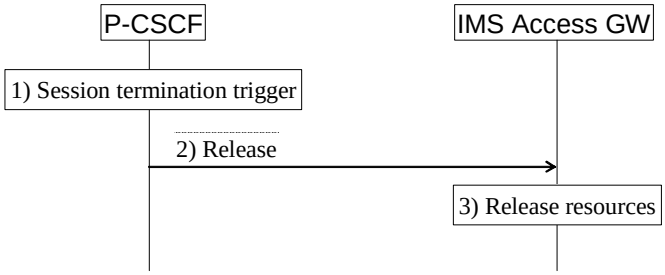


Figure G.4: Session release procedure with NAT traversal

1) The P-CSCF receives a trigger to release a session, for which the IMS-ALG function is invoked.
2) The P-CSCF sends an indication to the IMS Access Gateway for each media flow of the session that the resources allocated during the session establishment procedures are to be released.
3) The IMS Access Gateway releases its resources allocated for the given media flows.

G.4.5 Session modification

A session modification can cause the creation, and/or modification, and/or release of media flows.

When a new media flow is created the procedure used during session establishment shall be applied.

When an existing media flow is released the procedure for session termination shall be applied for the particular media flow.

When an existing media flow is modified, this may lead to a modification of the media flow directly, or to the establishment of a new media flow and release of the existing one.

G.4.6 Media forwarding in the IMS Access Gateway

This clause presents the media forwarding performed by the IMS Access Gateway. The behaviour presented in this clause is valid in both directions.

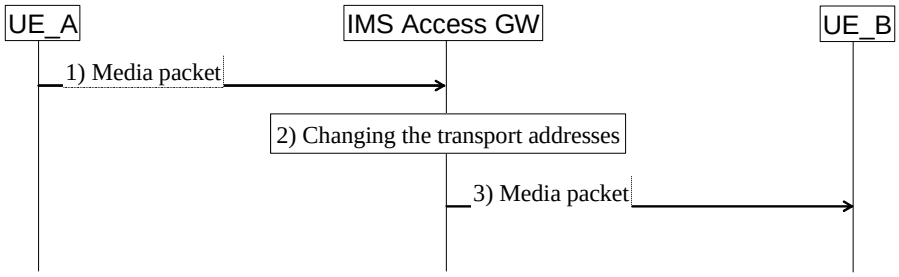


Figure G.5: Packet forwarding in the IMS Access Gateway

1) UE_A sends a media packet to the transport address of the IMS Access Gateway that was received during the session establishment/modification.

2) After receiving the media packet the IMS Access Gateway recognizes the media flow based on the transport address where the packet arrived at. The IMS Access Gateway changes the source transport address to its own transport address that was given to the UE_B as the destination transport address during session establishment/modification and the destination transport address to the transport address of UE_B.

   The IMS Access Gateway can learn the transport addresses where the inbound (i.e. towards the UE) media packets shall be forwarded to in two ways, depending on whether there is a NAT device in the path or not. In absence of a NAT device in the path, it is the P-CSCF that signals the destination transport address for the inbound media flows. In presence of NAT device in the path, it is the IMS Access Gateway that may, upon being informed that there is a NAT in the network, determine the destination transport address of the inbound media flow based on previously received media packets in the opposite direction.

   Beyond the changes of transport addresses the IMS Access Gateway shall perform the other necessary changes in the IP header as it is specified in the NAT related IETF specifications, IETF RFC 2766 [33] and IETF RFC 2663 [34].

NOTE 1: If the IMS Access Gateway does not know the transport address where a packet shall be forwarded, i.e. no packet of the other direction of the media flow has been received, then it can store or drop the packet.

NOTE 2: If this is not the first packet then the IMS Access Gateway can check the source transport address. If it is not the same as the transport address previously used for this media flow in this direction then the media packet may be a fraud one and should be dropped.

NOTE 3: This solution (i.e. when the IMS Access Gateway determine the destination transport address on its own) assumes that the UE supports "symmetric media" i.e. it supports receiving media packets at the same address and port as it uses for sending.

3) The IMS Access Gateway routes the media packet towards UE_B.

G.5 Network elements for employing NAT Traversal for ICE and Outbound

G.5.1 General requirements

In addition to the general requirements outline in clause G.1.1, the following NAT traversal solution also addresses the following additional requirements:

- Does not require the network to be aware of the presence of a NAT;
- Avoid unnecessarily long media paths due to media pinning;
- It shall be possible to establish communication towards a remote UE that does not support of the functionality listed in G.5;
- Minimize the impacts on Policy and Charging Control functionality.

G.5.2 ICE

G.5.2.1 Overview

The Interactive Connectivity Establishment (ICE) described in IETF RFC 5245 [45] defines a methodology for media traversal of NAT devices.

However, ICE is not a complete solution in of itself as ICE only addresses address advertisement and NAT binding maintenance. ICE does not address RTP and RTCP port symmetry requirements or non-sequential RTP and RTCP port assignment. A complete UE managed NAT traversal solution shall take into account each of these issues.

G.5.2.2 Required functions of the UE

When supporting ICE, the UE is responsible for managing the overall NAT traversal process and for invoking the various protocol mechanisms to implement the NAT traversal approach. As such, the following functions shall be performed by the UE:

- STUN relay server and STUN server discovery;

NOTE: A configuration mechanism can be used to provision STUN server and STUN relay server addresses in the UE.

- Transmission of media packets from the same port on which it expects to receive media packets;
- RTCP port advertisement.
- ICE functionality which includes:
  - Maintaining of NAT bindings to insure inbound media packets are allowed to traverse the NAT device.
- Address advertisement, which consists of the following operations:
  - Gathering candidate addresses for media communications;
  - Advertising the candidate addresses in a special SDP attribute (a=candidate) along with the active transport address in the m/c lines of the SDP.
- Perform connectivity checks on the candidate addresses in order to select a suitable address for communications.

Depending on the results of the connectivity checks, one of the candidate addresses may be promoted to become the active transport address.

Depending on the active transport address, provide additional information in the session description to insure that correct policy and charging functionality can be applied on relayed media packets.

Given the desire to minimize session establishment delays during connectivity checks, the UE shall advertise its active address in the SDP offer or answer in the following order based on their availability:

1. STUN relay server assigned address;
2. STUN derived address;
3. Locally assigned address.

G.5.2.3 Required functions of the STUN relay server

The STUN relay server and associated signalling requirements are documented in IETF RFC 5766 [46] and its use is detailed in IETF RFC 5245 [45]. No additional requirements are placed on this server.

NOTE: While it is not required that a STUN relay server be deployed in the network, a STUN Relay server would allow for media exchange in the presence of all NAT types.

G.5.2.4 Required functions of the STUN server

The STUN server and associated signalling requirements are documented in RFC 5389 [47] and its use is detailed in IETF RFC 5245 [45]. No additional requirements are placed on this server.

NOTE: While it is not required that STUN servers be deployed in the network, a STUN server would allow for UEs to discover the WAN facing transport address of the NAT. Such discovery may minimize the need for STUN Relay server resources by allowing UEs to directly exchange media in the presence of the majority of NAT types.

G.5.3 Outbound

G.5.3.1 Overview

RFC 5626 [48] "Managing Client-Initiated Connections in the Session Initiation Protocol" (Outbound) defines a methodology for signalling traversal of NAT devices. This methodology involves the establishment of flows to allow for the routing of inbound dialog initiating requests and the maintenance of the flow through keep-alive messages. Outbound does not however address inbound response routing or inbound mid-dialog requests. A complete UE managed NAT traversal solution shall take into account each of these issues.

This clause is restricted to the use of Outbound in the context of SIP NAT traversal and not to the usage of Outbound for multiple registration support.

NOTE: ICE and Outbound are not dependent on each other, and can be deployed separately or together. The STUN keep-alive function, for SIP signalling, can also be implemented as a standalone function, without ICE or Outbound.

G.5.3.2 Required functions of the P-CSCF

When supporting Outbound, the P-CSCF's primary role in NAT traversal is to ensure that requests and responses occur across a flow for which there is an existing NAT binding. The P-CSCF shall ensure that inbound dialog initiating requests can be forwarded to the UE on a flow for which there is an existing NAT binding.

The P-CSCF shall ensure that all responses to the UE including those from mid-dialog requests are sent to the same source IP address and port which the request was received from.

The P-CSCF shall also implement a limited STUN server functionality to support the STUN keep-alive usage as defined in RFC 5389 [47] which is used by the UE to maintain the NAT bindings.

NOTE: The STUN server implementation on the P-CSCF need only support the STUN functionality required for the STUN binding request operation.

Additionally the P-CSCF shall transmit signalling packets from the same port on which it expects to receive signalling packets.

G.5.3.3 Required functions of the S-CSCF

When supporting Outbound, the S-CSCF should be responsible for indicating to the UE that Outbound procedures are supported.

G.5.3.4 Required functions of the UE

When supporting Outbound, the UE is responsible for managing the overall NAT traversal process and for invoking the various protocol mechanisms to implement the NAT traversal approach. As such, the following functions shall be performed by the UE:

- Maintaining of NAT bindings between the UE and the P-CSCF through the use of a keep-alive mechanism to insure inbound signalling packets are allowed to traverse the NAT device.

NOTE: Solutions to determine the frequency of the keep-alive are not defined in this version of the specification. A configuration mechanism can be used in place of a dynamic discovery process.

- Transmission of signalling packets from the same port on which it expects to receive signalling packets;

- Establishment of signalling flows to its assigned P-CSCF(s) during registration.

NOTE 1: The UE can determine that STUN based keep-alive can be used towards the P-CSCF based on the presence of the STUN keep-alive parameter from the P-CSCF SIP URI received during P-CSCF discovery.

NOTE 2: If a UE supports only STUN keep-alives, but not Outbound, it does not need to determine Outbound support, and it does not need to register flows as defined by Outbound. It only sends STUN requests to the P-CSCF to keep NAT bindings open.

G.6 Procedures for employing ICE and Outbound

The procedures described in the following clauses are applied in addition to the procedures of the UE and P-CSCF described in other clauses of this specification.

G.6.1 Flow establishment procedures

This procedure is initiated by the UE at network registration time, and allows for the establishment of a flow between a UE and its assigned P-CSCF. This flow can then be used by the P-CSCF to allow an initial inbound request to traverse the NAT.

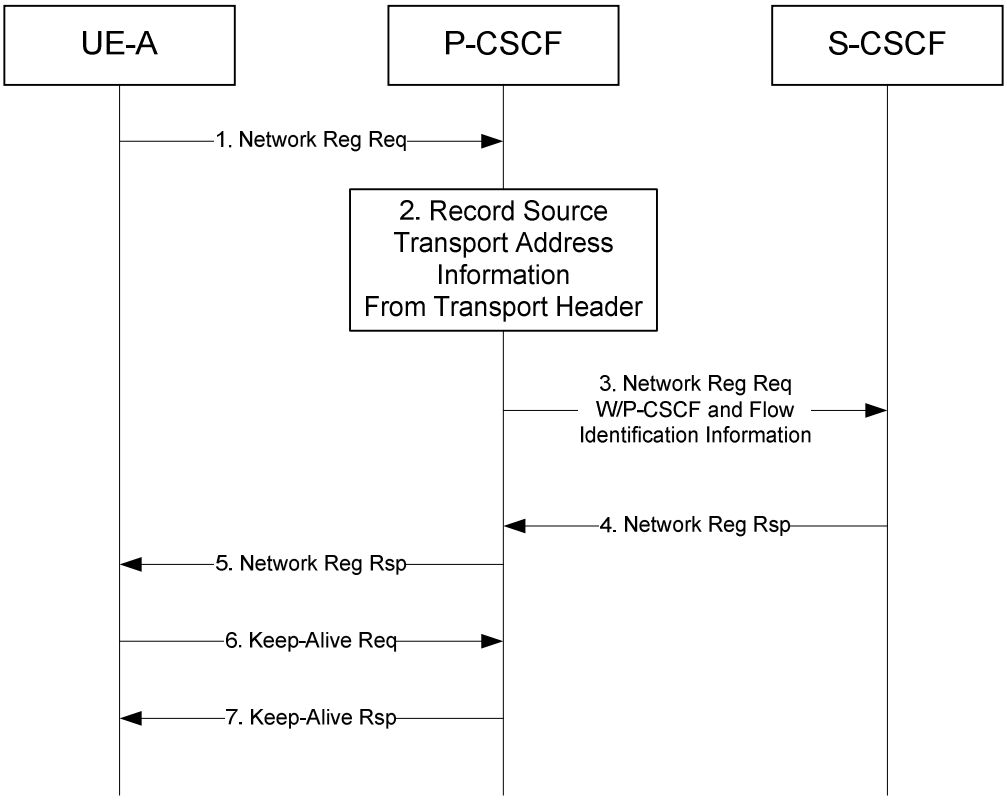


Figure G.7: Flow Establishment Procedures for Outbound

1. UE-A initiates network registration by sending a registration request to its assigned P-CSCF.
2. Upon receipt of a registration request, the P-CSCF stores received transport header. This includes information to identify the flow between P-CSCF and UE.
3. The P-CSCF then sends the registration request to the assigned S-CSCF after adding information identifying the serving P-CSCF to the registration request.
4. The S-CSCF stores the information identifying the serving P-CSCF and returns a registration response.
5. Upon receipt of the registration responses from the S-CSCF, the P-CSCF forwards the registration response to UE-A using the stored transport address information from the registration request.
6. UE-A sends a Keep-Alive request to its assigned P-CSCF using the same transport address information (source and destination) which was used for the registration request. This Keep-Alive ensures that a NAT binding exists between UE-A and the P-CSCF allowing for inbound session requests from the P-CSCF to UE-A.

7. The P-CSCF responds with a Keep-Alive response which also reflects the received source transport address information. Inclusion of such information allows UE-A to determine if the NAT has rebooted and assigned a new binding and take appropriate action.

G.6.2 Session establishment procedures

The following procedure illustrates the session establishment procedures when both UEs support the ICE methodology. These procedures apply to both the terminating and originating side of the session regardless of whether the UE is behind a NAT.

In the following figure the STUN element represents both a STUN server and STUN Relay server as a single logical element. It would be equally valid if these functions we represented in separate logical elements. The procedures are unaffected by the grouping. Further, this call flow represents a simplified view to illustrate the NAT traversal procedures only. Other network elements not show may be involved in the session establishment process.

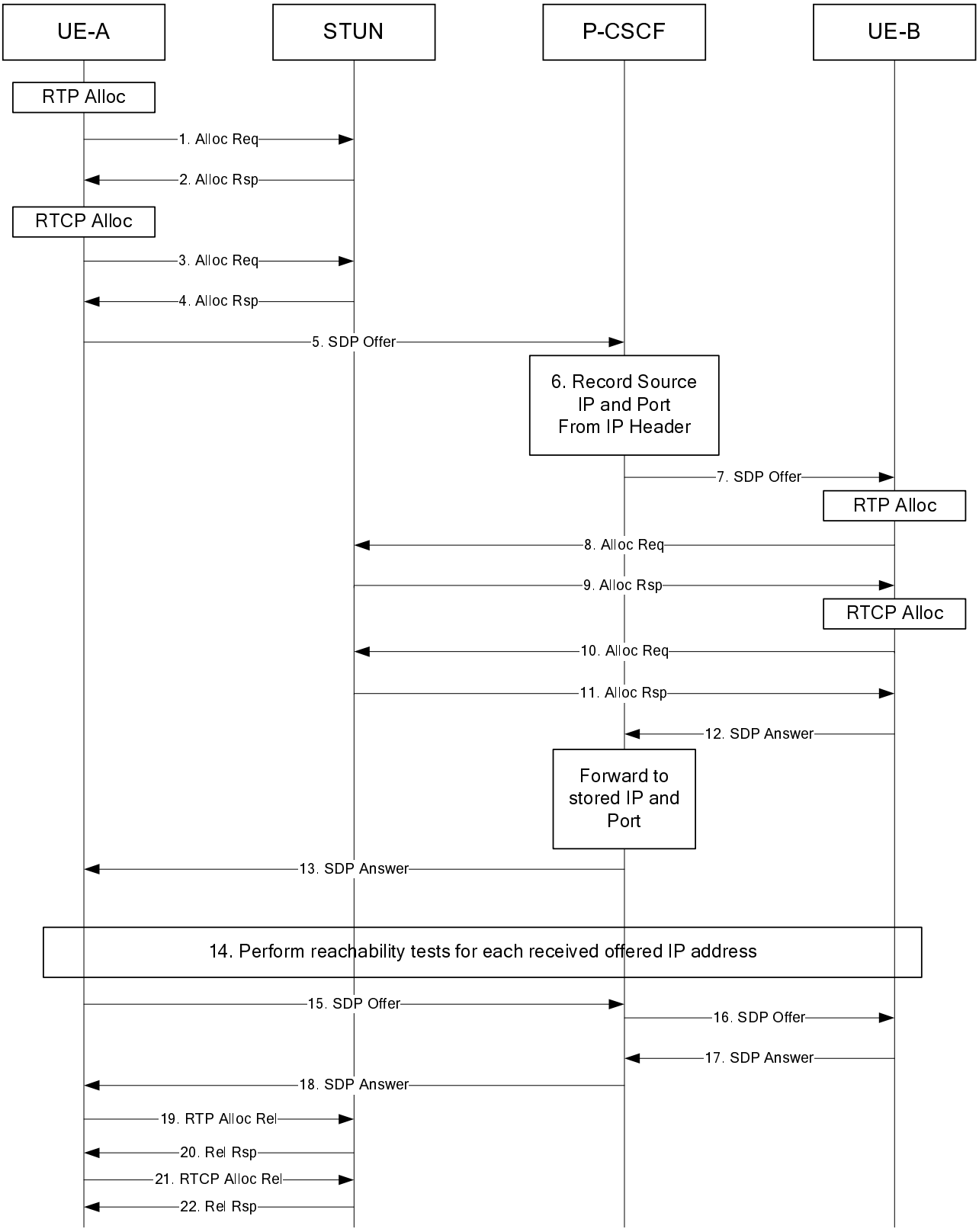


Figure G.8: Session Establishment procedure for NAT Traversal using ICE and Outbound

1. UE-A begins candidate transport address collection by performing a request for a transport address for each media flow from the STUN server.

2. The STUN server reserves one of its transport addresses for each media flow and sends the reserved transport address information back to the UE. The STUN server also reflects the source transport address of the original request for a transport address

If the UE fails to identify STUN servers it concludes that ICE and Outbound procedures are not supported by the network and defaults to operation using the procedures described in clause G.4.

3-4. UE-A repeats the procedures for requesting a transport address for each RTCP flow. These steps may be executed in parallel with steps 1. – 2. or in series.

5. With its three candidates (locally assigned, server reflected and relay) UE-A forms an offer and forwards to its assigned P-CSCF. The UE includes the SP cand-type, SP rel-addr and SP rel-port in the candidate attribute as defined in IETF RFC 5245 [45].

6. To ensure subsequent responses to the offer are allowed through the NAT, the P-CSCF stores the transport address information received in the transport header of the offer.

7. The P-CSCF forwards the Offer to UE-B using one of the previously established flows.

8-11. UE-B performs the candidate gathering procedures as outlined in steps 1. – 4. above.

12. With its three candidates (locally assigned, server reflected and relay) UE-B forms an answer and forwards to its assigned P-CSCF

13. The P-CSCF for UE-A forwards the Answer to UE-A based on the previously stored transport address information. Media can being to flow at this point using the default transport addresses (recommended to be the STUN Relay provided address)

14. Both UE-A and UE-B perform connectivity tests on each received transport address to determine which of the received transport addresses are actually reachable.

15. After the connectivity tests are concluded UE-A sends an updated SDP Offer indicating the agreed to transport address

16. The P-CSCF forwards the Offer according to normal routing procedures.

17. UE-B sends an Answer indicating the agreed to transport address.

18. The P-CSCF forwards the Answer according to normal routing procedures. Media can begin flowing using the newly identified addresses.

19-21. STUN Relay allocated transport addresses are released by the UE once a more efficient address has been identified and the session updated.

G.6.3 Session release procedures

This procedure is applied to by the UE if the IMS-ALG function is not supported by the network, but the network does support ICE and Outbound procedures. Normal session release procedures are followed with the following exception. If a STUN Relay allocated transport address was used for the session, it shall be released by the UE for which the transport address was allocated.

In the following figure the STUN element represents both a STUN server and STUN Relay server as a single logical element. It would be equally valid if these functions we represented in separate logical elements. The procedures are unaffected by the grouping.

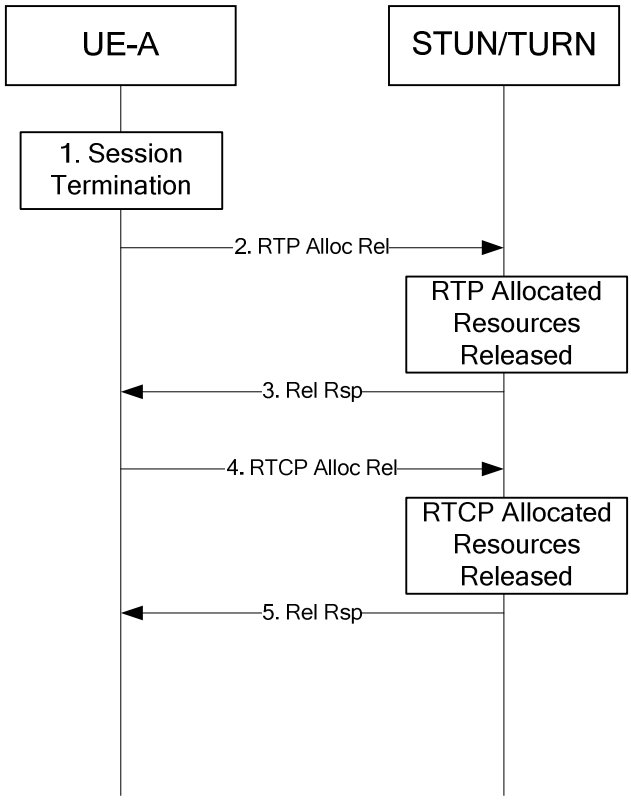


Figure G.9: Session Release Procedure with STUN Relay Resources

1. UE-A receives a trigger to release the session for which STUN Relay resources were allocated.
2. UE-A sends an indication to the STUN Relay server to release resources allowed for RTP.
3. The STUN Relay server releases the allocated resources and returns a response.
4. UE-A sends an indication to the STUN Relay server to release resources allowed for RTCP.
5. The STUN Relay server releases the allocated resources and returns a response.

G.6.4 Session modification procedures

A session modification can cause the creation, and/or modification, and/or release of media flows.

This procedure is applied to by the UE if the IMS-ALG function is not supported by the network, but the network does support ICE and Outbound procedures. When a new media flow is created the procedure used during session establishment for updating the transport addresses (steps 15-17. of the session establishment procedures) shall be applied.

When an existing media flow is released the procedure for session termination shall be applied for the particular media flow.

When an existing media flow is modified, this may lead to a modification of the media flow directly, or to the establishment of a new media flow and release of the existing one.

G.6.5 Policy and Charging Control procedures

When PCC is to be employed for a session, the P-CSCF is responsible for providing the PCRF/PCF with IMS media flow information related to the service. If the UE has indicated that the active transport address corresponds to a relayed address, the P-CSCF shall be responsible for using the additional information provided by the UE to convert the media flows derived from the SDP into flow descriptions which will traverse the Policy and Charging Enforcement Point.

The deployment of STUN relay servers requires that the UE be able to communicate with such servers prior to session establishment. The PCC for the IP-CAN must be set up to allow communication with the STUN relay server prior to IMS session establishment. This may impact gating control in some IP-CANs which do not support a default or best effort flow which can be used to communicate with the STUN relay server prior to session establishment.

NOTE 1: Predefined PCC rules can be created to allow the UE to communicate with the STUN relay much in the same way the UE is allowed to communicate with the IMS network for session management.

NOTE 2: Given that a STUN relay is a forwarding server under the direction of the UE, necessary precaution needs to be taken by the operator in how it chooses to craft these rules. It is recommended that such predefined rules only guarantee the minimal amount of bandwidth necessary to accomplish the necessary UE to STUN relay communication. Such an approach helps reduce the resources required to support NAT traversal mechanisms. Finally, such an approach allows the preconfigured rule to be over-ridden by dynamic rules which allow for the necessary bandwidth needed by the session.

NOTE 3: The dynamic PCC rule will need to differentiate between different media traffic between UE and STUN relay (e.g. voice vs. video), which can be identified by the different ports assigned by the residential NAT. Session bindings need to take into account that the relevant Terminal IP address may be contained within the ICE candidates contained in the session description, rather than in the normal media description.

G.6.6 Detection of NAT Traversal support

The UE shall be able to determine whether the IMS CN supports the Outbound procedures by the capabilities indicated in the registration response to the UE. If the indication of the capability is present, the UE knows that the IMS CN supports Outbound and the associated procedures.

NOTE: A configuration mechanism can be used to provision STUN server and STUN relay server addresses in the UE.

G.6.7 Procedures at other IMS entities processing SDP

IMS entities processing SDP, such as the P-CSCF, IBCF or MRFs, may or may not be updated to understand the "candidate alternative addresses" that are part of the ICE procedures, IETF RFC 5245 [45]. IMS entities processing SDP that do not understand the ICE procedures will, in accordance with there compatibility procedures, ignore the "alternative addresses", and media entities, such as the IMS Access Gateway, PCEF, MRFP and TrGW, controlled by the IMS entities processing SDP will not pass connectivity check requests and media on those addresses. IMS entities processing SDP which behave as B2BUAs may or may not pass on the alternative address in accordance with their own compatibility procedures.

Annex H (informative): Example HSS deployment

This clause describes possible deployment scenarios for the HSS when it operates as an IMS only database.

The following depicts the HSS functionality as described in TS 23.002 [1] repeated here for clarity; note that the functional description in TS 23.002 [1] shall always be considered as the most updated version, if it is different than the version shown here. 3GPP HSS contains functions also known as HLR and AuC, which are needed for 3GPP GPRS and CS domain access authentication and authorization and overall subscription handling as well as service data management.

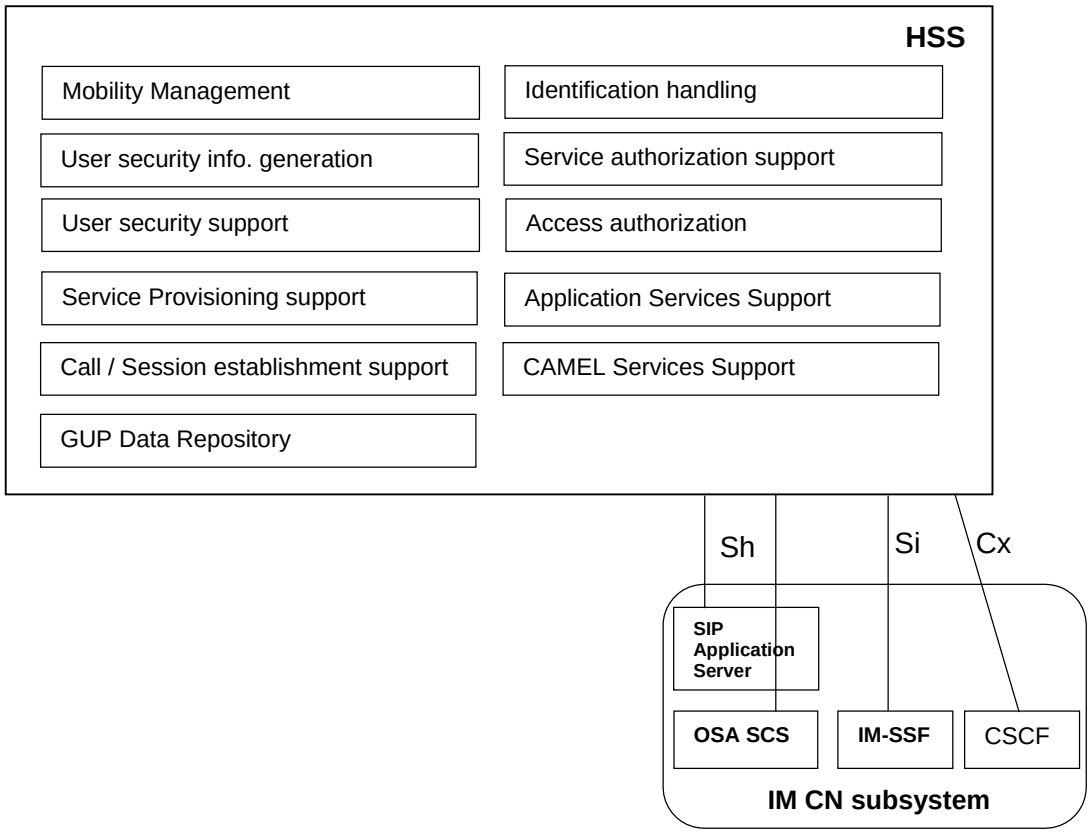


Figure H.1: HSS functional decomposition

In cases where the HSS would operate as an IMS only entity, the functions and interfaces specific to IMS operations would be applicable. These include support of functionalities such as identification handling, service provisioning support, call/session establishment support, application services support, IMS access authentication and authorization provided by the interfaces Cx, Sh and Si (if applicable to interwork with CAMEL) and any additional subscription and configuration handling for IMS users. This type of configuration of the HSS would be used for access to the IMS as defined by, for example, TISPAN NGN.

Annex I (normative): Border Control Functions

I.1 General

This annex describes a collection of functions that can be performed on interconnection boundaries between two IM CN subsystem networks or between an IM CN subsystem network and other SIP based multimedia network, based on operator configuration.

I.2 Overall architecture

Figure I.1 presents a high-level architecture diagram showing how Border Control Functions fit into the IMS architecture.

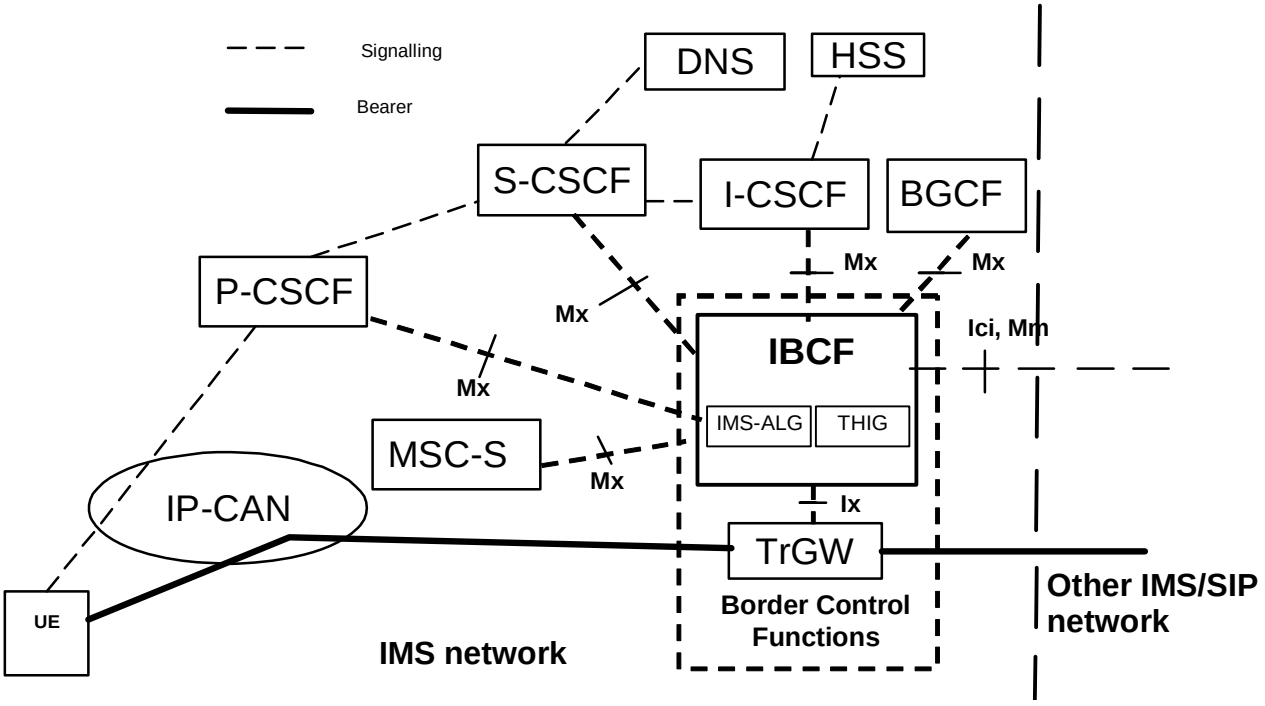


Figure I.1: Border Control Functions

The Mx reference point allows S-CSCF/I-CSCF/P-CSCF/MSC Server enhanced for ICS or MSC Server enhanced for SRVCC to communicate with an IBCF in order to provide border control functions. The functionality of the reference point is specified in TS 24.229 [10a].

The Mm reference point allows IBCF to be the entry / exit point towards other IM Core Network Subsystems and provide border control functions. The Ici reference point allows IBCF to be the entry / exit point towards other SIP networks and provide border control functions. The functionality of the reference points are specified in TS 24.229 [10a].

The Ix reference point allows the IBCF to control the TrGW. The functionality of Ix is defined in TS 29.162 [75].

I.3 Border Control Functions

I.3.1 IP version interworking

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

The IMS ALG provides the necessary application function for SIP/SDP protocol stack in order to establish communication between IPv6 and IPv4 SIP applications.

The IMS ALG receives an incoming SIP message from CSCF nodes or from an external IPv4 SIP network. It then changes the appropriate SIP/SDP parameters, translating the IPv6 addresses to IPv4 addresses and vice versa. The IMS ALG needs to modify the SIP message bodies and headers that have IP address association indicated. The IMS ALG will request NA(P)T-PT to provide the bindings data between the different IP addresses (IPv6 to IPv4 and vice versa) upon session initiation, and will release the bindings at session release.

I.3.1.1 Originating Session Flows towards IPv4 SIP network

The following example session flow shows a scenario where the S-CSCF is responsible for inserting the IMS-ALG in the session path. No I-CSCF node shown in this scenario, if configuration requires presence of an I-CSCF then it would have been collocated with the IMS-ALG.

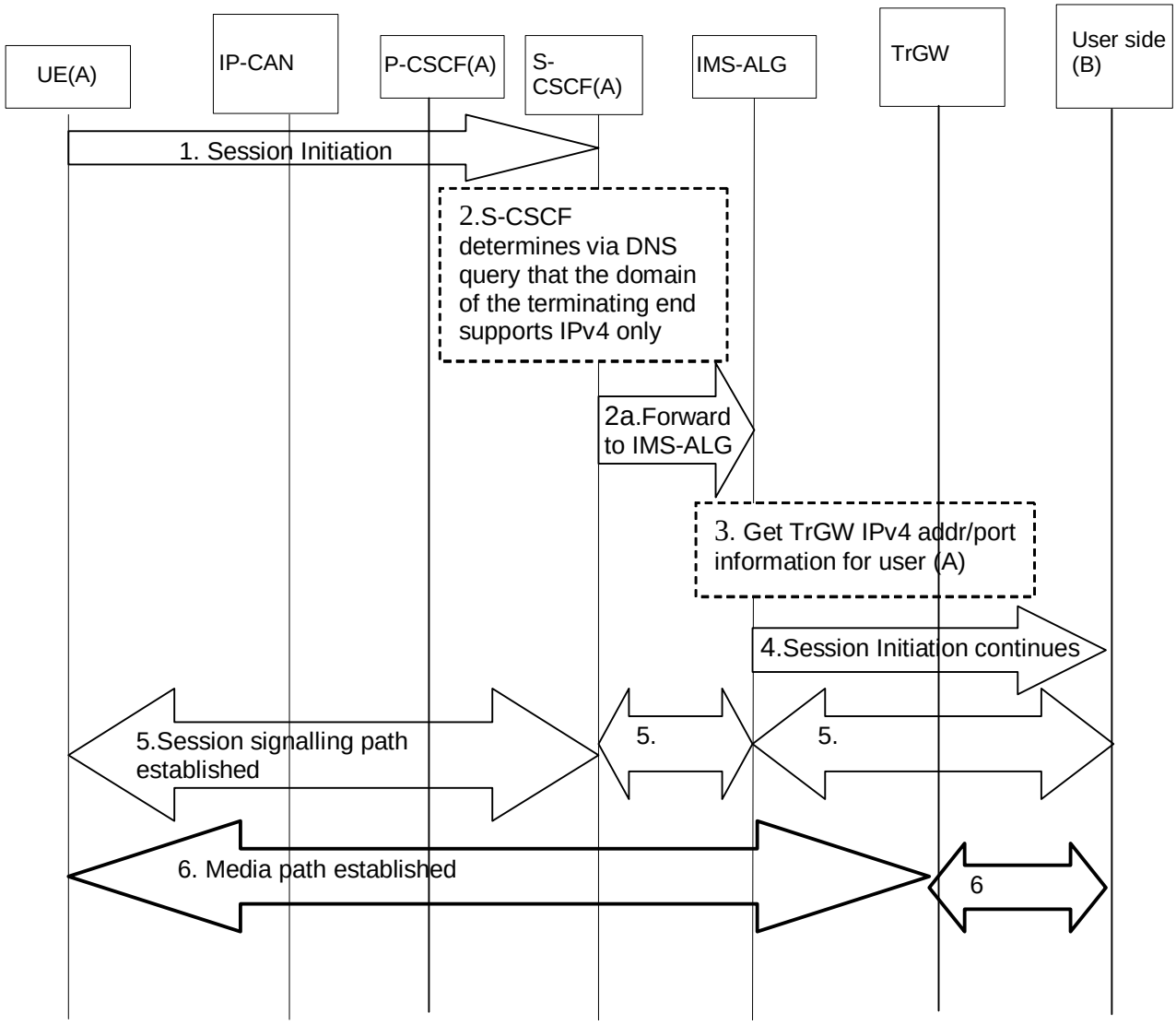


Figure I.2: Originating IMS session towards an IPv4 end point

1. UE (A) initiates an IMS session towards User B, via the session path for IMS and the session is analysed at the S-CSCF of UE (A).

2. S-CSCF for user A determines via DNS (or other mechanism) that the User B's domain cannot be communicated via IPv6 but can be via IPv4.

2a. S-CSCF forwards the request to IMS-ALG.

3. The IMS-ALG then acquires the necessary resources from the TrGW such as the IPv4 address and ports on behalf of user A so that User A can communicate with user B transparently.

4. The IMS-ALG continues IMS signalling towards User B network where User A's IPv6 address/port information is replaced by IPv4 information.

5. When User (B) responds to the session initiation requests, the IMS-ALG will replace the IPv4 address/port information of User (B) with its own IPv6 information for signalling and with TrGW IPv6 information for the media path as the contact information of User (B) and forward the request to S-CSCF of UE (A). Session signalling path is then established between the UE and the S-CSCF, the S-CSCF and the IMS-ALG, the IMS-ALG and the external network for User B.

6. The media path is established between the UE (A) and the TrGW, via the IP-CAN, and then between the TrGW and user B.

At session release, the IP address/Port information will be released for reuse by other sessions.

I.3.1.2 Terminating Session Flows from IPv4 SIP network

The following session flow shows an example of a terminating session from an IPv4 SIP client towards an IPv6 IMS client. In order for the IPv6 IMS client to be reachable by the IPv4 network, it is assumed that the IPv4 network discovers (via mechanism such as DNS query) the IMS-ALG as the entry point to the IPv6 IMS network.

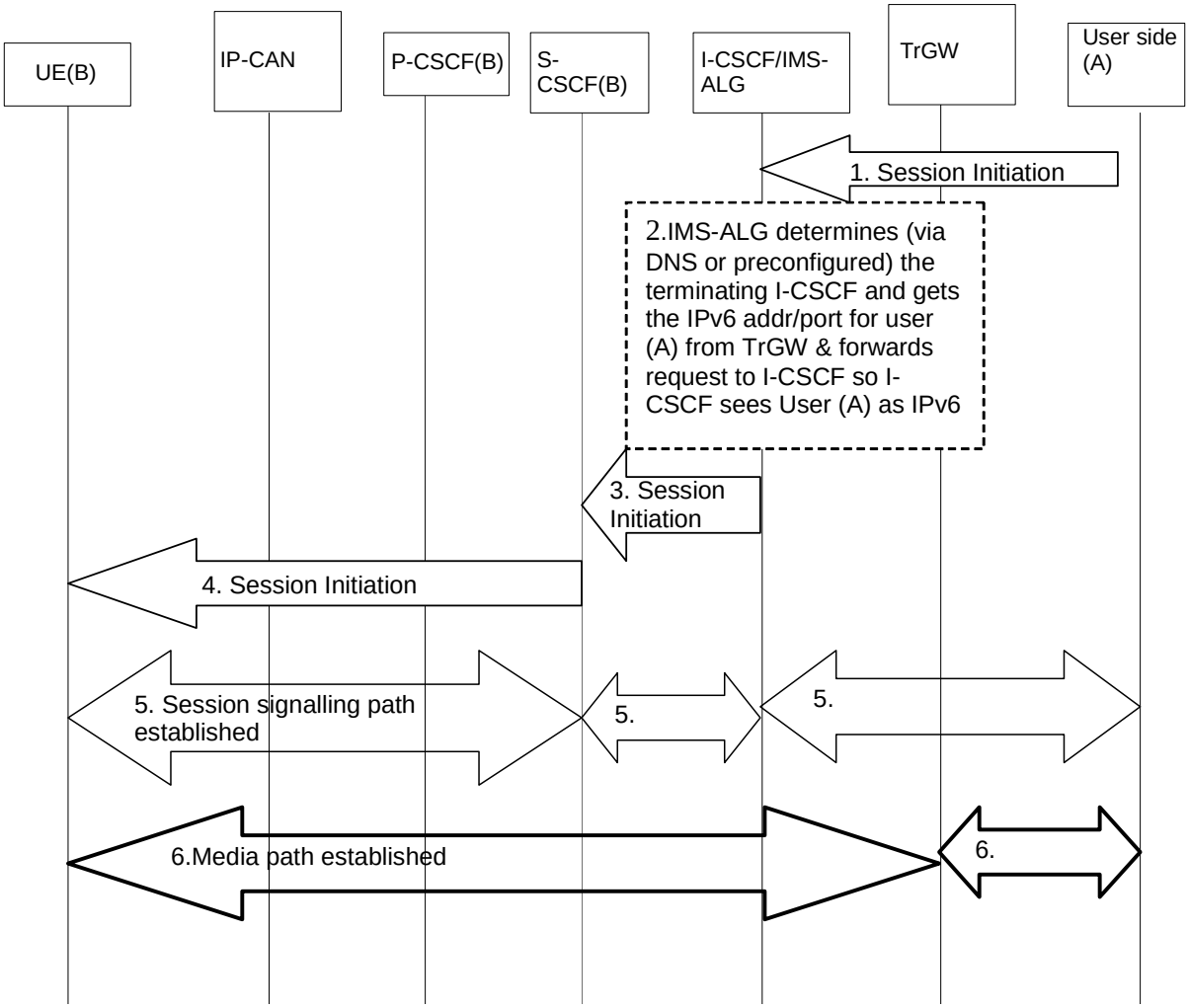


Figure I.3: Terminating IPv4 SIP session towards an IPv6 IMS user

1. In the IMS-ALG, a terminating session is received. IMS-ALG determines either via DNS query or via preconfiguration the appropriate I-CSCF for the user (B) in the IMS network.

2. IMS-ALG also communicates with TrGW to get the mapping of IPv6 address and ports on behalf of user (A) and replaces the User (A) information in the incoming SIP message and forwards the message towards S-CSCF. From S-CSCF point of view, it continues setting up the IMS session like any other IMS sessions.

3. The incoming session arrives in the S-CSCF for the user (B).

4. Session set up continues as usual in the IMS domain towards user (B).

5. When UE (B) responds to the session initiation requests, the IMS-ALG will replace the IPv6 address/port information of User (B) with its own IPv4 information for signalling and with TrGW IPv4 information for the media path as contact information of UE (B) and forward the request towards the network of User (A). Session signalling path is established between User (B) and S-CSCF, S-CSCF and I-CSCF/IMS-ALG and IMS-ALG and the external User (A)'s network.

6. Media path is established between UE (B) and the TrGW, via the IP-CAN, and then between the TrGW and User (A).

At session release, the IP address/Port information will be released for reuse by other sessions.

I.3.2 Configuration independence between operator networks

The 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: addresses of operator network entities.

NOTE: The THIG functionality was not intended to be invoked in IMS roaming scenarios when the P-CSCF and IBCF are both located in the visited network as information available in certain SIP headers may be used by the home network for further processing of signalling messages.

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.

Competitively 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.

NOTE: The encryption mechanism for implementing network configuration hiding is specified in TS 33.203 [19].

I.3.3 Transcoding Support for Interworking

I.3.3.1 General

The IBCF/TrGw provides the necessary function for codec transcoding, when required by interworking agreement and session information, in order to establish communication between end points belonging to different IMS domains. These transcoding procedures are applicable to both the originating and the terminating side of the session or (in inter-network scenarios) in a transit network

Transcoding shall only be performed in the case where a common codec cannot be negotiated between the two UEs.

Media transcoding services can be triggered proactively (before the session request is sent to the called UE) or reactively (after the session request has been sent to, and rejected by, the called UE).

The IBCF may allocate a TrGW before sending the SDP Offer to the terminating UE or it may allocate the TrGW upon receiving the SDP answer. The protocol solutions should ensure that the called party is not alerted until resources for transcoding are seized and user plane connection towards the calling party is established to avoid ghost ringing or voice clipping.

NOTE: The proactive transcoding example flows illustrates only the allocation of the TrGW before sending the SDP offer.

If the IBCF is configured per local policy to use proactive transcoding, the IBCF shall add codecs to the offer. When inserting additional codec(s), the network should be able to indicate the preferred codec order.

If the IBCF is configured per local policy to use reactive transcoding, the IBCF shall first determine the codecs supported by the calling and called UEs so that insertion of the TrGW is performed when necessary, if not required for any other interconnect function. This means that the IBCF shall trigger a new offer/answer to the terminating UE, based on the initial offer from the originating UE but including additional codecs supported by the TrGW in the same manner as for the proactive support.

I.3.3.2 Session Flows

I.3.3.2.1 Proactive transcoding support

The following example session flow shows a proactive transcoding support scenario where an IBCF acting as an exit point allocates a TrGW prior to signalling towards the entry point of the other operator's network. The IBCF inserts additional codecs in the SIP signalling. The calling UE capabilities are contained in the SDP offer. Based on the interworking agreement between IM CN subsystems, terminating IBCFs acting as the network entry points may also insert additional codecs in the SIP signalling.

The IBCF and TrGW in Figure I.4 below may be located in the originating network (the IBCF acts as an exit point), or in the terminating network (the IBCF acts as an entry point). There can also be additional IBCF's and TrGW's (not shown) in the case of scenarios involving transit networks.

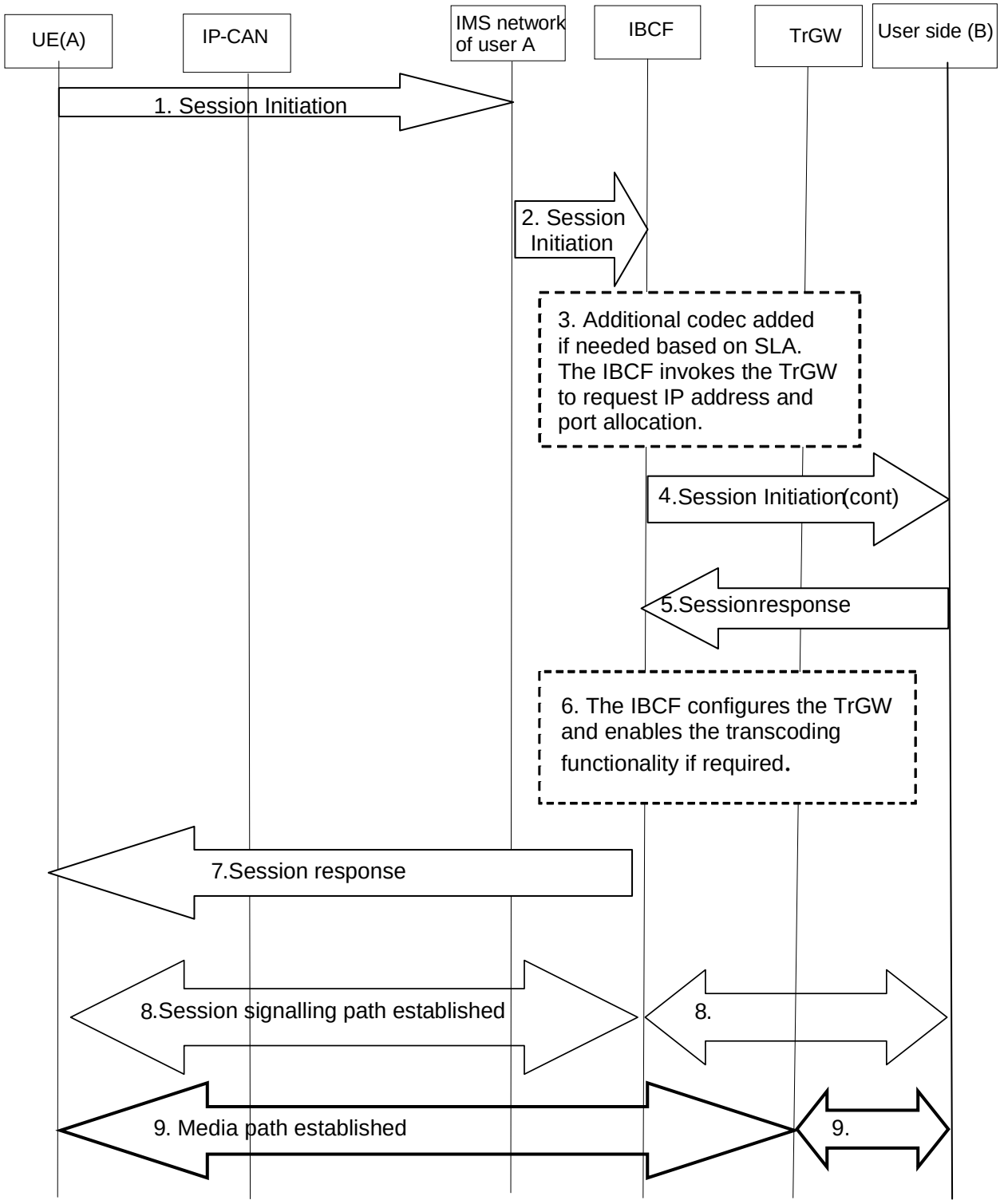


Figure I.4: Proactive transcoding invocation

1. UE (A) initiates an IMS session towards User B, via the session path for IMS and the session is analysed at the IMS network of UE (A).

2. The IMS network of UE (A) determines that the User B's domain need be communicated via IBCF and forwards the request to the IBCF.

3. The IBCF checks the SIP message and decides whether additional codec(s) need be inserted into SIP message based on the session information (such as ICSI , SDP) and interworking agreement. When inserting additional codec(s), the network should be able to indicate the preferred codec order. A TrGW is allocated.

4. The IBCF generates a new SIP message towards User B network based on the received SIP message where additional codec(s) have been added and where the transport address and port information has been altered to indicate the addresses associated by the TrGW.

5. User (B) selects a codec from the offer modified by IBCF, and responds with an SDP answer.

6. When receiving the SDP answer, if the IBCF invoked the TrGW in step 3, it now configures the TrGW with address and port towards UE (B). The IBCF checks if the agreed codec belongs to the original offer it received in step 3 or it is one of the codecs that was added by IBCF. If the agreed codec was added by the IBCF, the IBCF configures the TrGW to enable the transcoding functionality. Otherwise, the IBCF will not invoke the transcoding function.

NOTE 1: If the IBCF forwards an SDP offer without allocating a TrGW and changing the connection information, and the subsequent SDP answer indicates selection of a transcoding option associated with the TrGW, then the IBCF needs to allocate a TrGW and initiate another SDP offer/answer transaction to forward the TrGW connection information. If the IBCF forwards an SDP offer with connection information for its TrGW, and the subsequent SDP answer indicates the use of an original codec (transcoding is not needed), then the IBCF can initiate another SDP offer/answer transaction to forward the original connection information, and de-allocate the TrGW. The details are not shown.

7. The IBCF generates a new response message back to UE (A) based on the received response message where the codec received from peer side has been replaced with the selected codec.

NOTE 2: On the new response message the selected codec will based on the SDP offer received by IBCF on step 3.

8. Session signalling path is established between User (A) and IBCF, IBCF and User (B).

9. The media path is established between the UE (A) and the TrGW, and then between the TrGW and user B.

At session release, the codec transcoding resource will be released.

I.3.3.2.2 Reactive transcoding support

The following example session flow shows a reactive transcoding scenario where IBCF located at the network exit point first determines if a session can be established without addition of transcoding options and, will insert additional codecs in the SIP signalling only after failure to establish a session due to lack of a common codec. Based on the interworking agreement between IM CN subsystems the terminating IBCF may also perform this function.

NOTE 1: In the event a session is being forked in the terminating network, the reactive transcoding will only be performed if all UEs receiving the forked request initially reject the session for any reason, e.g. due to lack of support for the offered codecs.

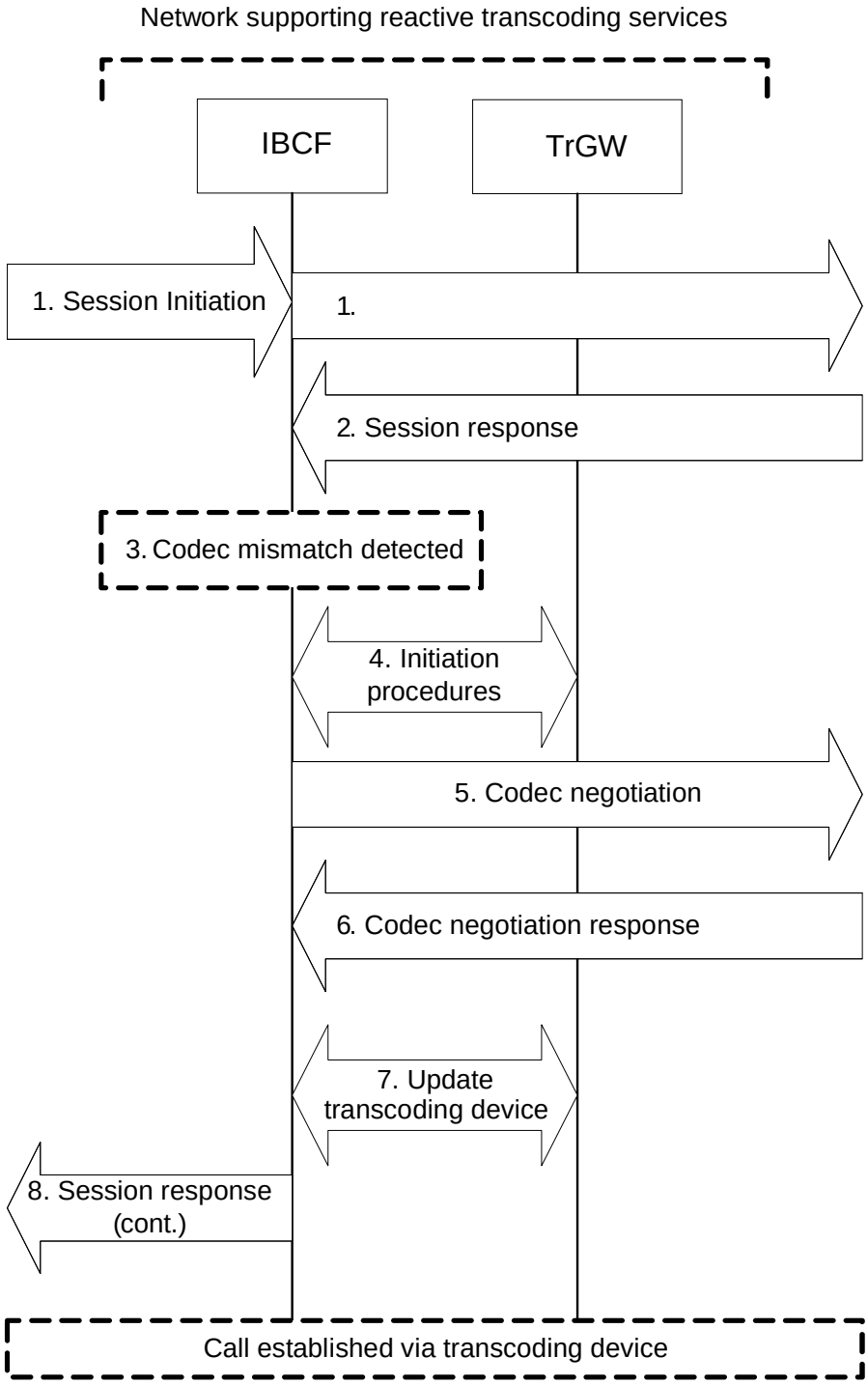


Figure I.5: Reactive transcoding invocation

1. UE (A) initiates an IMS session towards User B, and the session is analysed at the IBCF. The SDP offer is forwarded toward User B without the proactive addition of transcoding options.

2. A subsequent entity in the signalling path determines that it does not support any codec in the SDP offer and answers with an appropriate error response. This response may include a list of supported codecs.

NOTE 2: The subsequent entity in the signalling path can be a network entity in a transit network, in the terminating network, or UE (B).

3. Based on the response, the IBCF detects the need for reactive transcoding invocation.

4. The IBCF instructs the TrGW to allocate media processing resources for the session, allocate appropriate transcoding resources for the session and bridge the media flows between the calling and called party endpoints.

5. Based on the response from the TrGW, the IBCF creates a new SDP offer that contains the codec and transport address information received from the TrGW. If no information about supported codecs was available from the error response, the IBCF may offer all codecs supported by the transcoding device. The IBCF sends this SDP offer towards UE (B).

6. UE (B) selects a codec and acknowledges the SDP offer with an SDP answer.

7. Upon receipt of the SDP answer, the IBCF updates the TrGW with the information from the SDP answer.

8. The IBCF prepares an SDP answer to the SDP offer in step 1, including the selected codec and transport address information for the originating side of the TrGW. The session between the end-points is now established with the media flow traversing the transcoding device.

At session release, the codec transcoding resource will be released.

Annex J (informative): Dynamic User Allocation to the Application Servers

J.1 General

The complexity of operating a network increases with the number of supported subscribers, and one contributor will be the management of allocating subscribers to the application servers for the same set of services, where there is a requirement for a user to be assigned to an application servers longer than the duration of one session. This would occur when there is data which is to be retained together with the processing resources longer than a single session.

Possible solutions described below do not require impacts on the stage 3 specifications.

J.2 Representative AS

J.2.1 Concept of Representative AS

The Representative AS is the application server which allocates the user to the application servers and keeps the user allocation information and relevant data for the service during the duration of a session or longer than that. The incoming call for the service is received and forwarded to the allocated application server by the Representative AS.

The following points are considered as requirements for the dynamic user allocation procedures using the representative AS.

- The representative AS for each service is the initial contact point for all signalling. This can include ISC; and for example, Ut; and others signalling that may or may not be defined in 3GPP.
- For the ISC, the representative AS is included in every message which opens a new dialogue. It is not included after the initial transaction.
- For example, when the AS is to be invoked by evaluating the iFC at the S-CSCF, the address in the iFC is the address of the Representative AS.

The following figure shows an example service deployment for three different services using the representative AS.

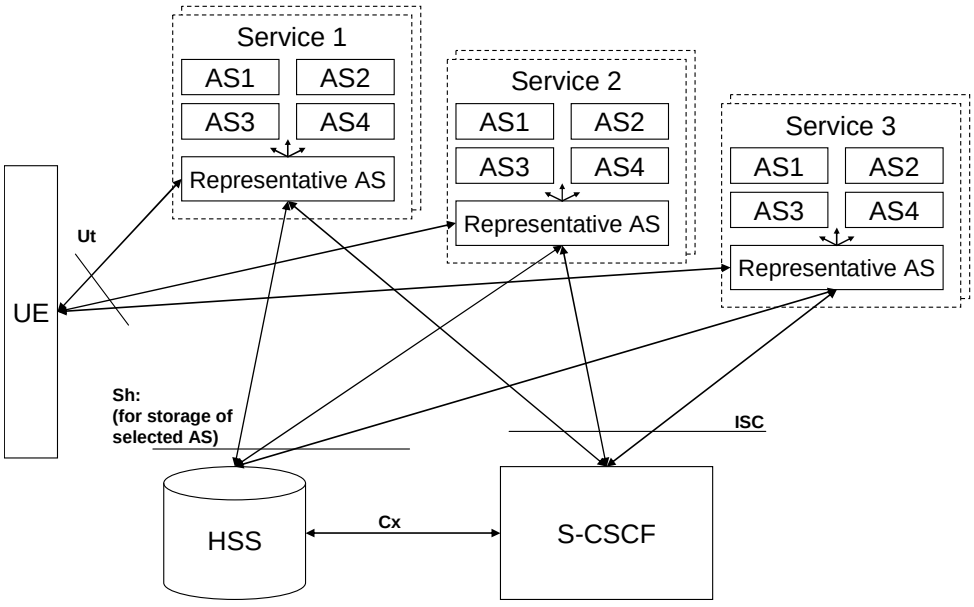


Figure J.2.1: Dynamic User Allocation using Representative AS

J.2.2 Procedures related to Representative AS

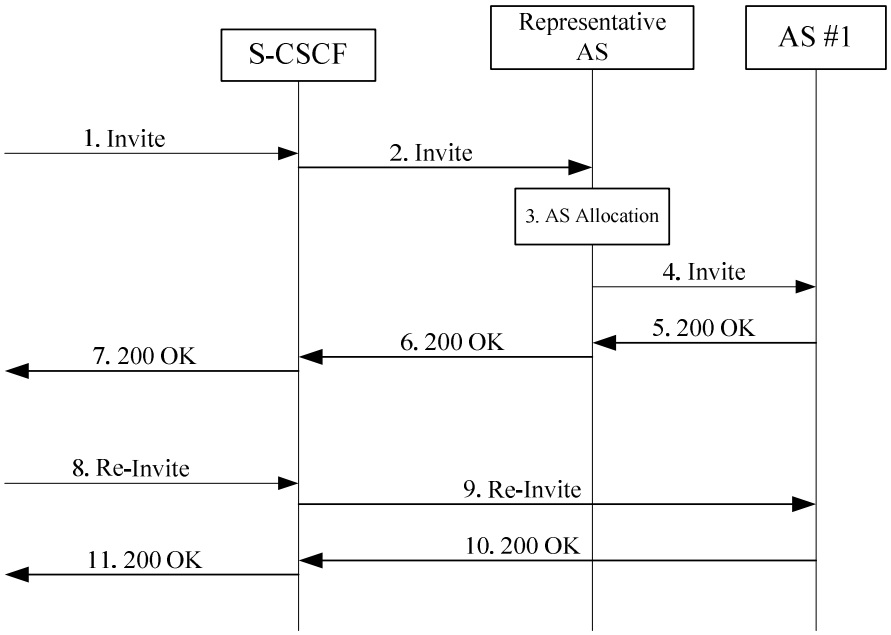


Figure J.2.2: Bypassing Representative AS procedure

Procedure is as follows:

1. The initial SIP INVITE request is sent to S-CSCF to create a new dialogue.
2. The SIP INVITE request is forwarded to the Representative AS according to the service logic, e.g., iFC evaluation at the S-CSCF.
3. The Representative AS retrieves the user allocation information and forwards the SIP INVITE request to the AS#1 according to the allocation information. If there is no allocated AS for the user, the Representative AS allocates one.
4. The SIP INVITE request is forwarded to the AS#1. Note that the Representative AS does not record-route itself.

5-7. The SIP INVITE request is processed and results in the 200 OK response.

8. The subsequent SIP INVITE request in the same dialog is sent to the S-CSCF.
9. The SIP INVITE request is forwarded directly to the AS#1 according to the Route information in the request message.

10-11. The SIP INVITE request is processed and results in the 200 OK response.

J.3 Dynamic assignment of AS by S-CSCF caching

J.3.1 Concept of Dynamic assignment of AS by S-CSCF caching

The proposed solution "Dynamic assignment of AS by S-CSCF caching" is based on standard SIP session control combined with a new S-CSCF caching functionality. This solution is re-using the DNS (IETF RFC 1035) mechanism, and supports only the ISC interface.

J.3.2 Procedures related to Dynamic assignment of AS by S-CSCF caching

Figure J.3.2.1 shows the procedure for allocating an AS by the first request of a service to an IMS registered user:

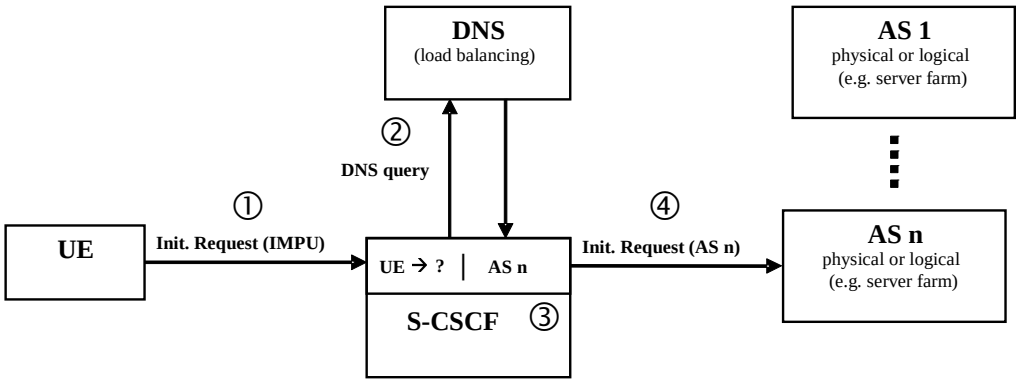


Figure J.3.2.1: Assignment of AS via DNS query during first service request

1. After IMS registration a user sends an initial request to the S-CSCF for requesting a service (served by an AS).
2. The S-CSCF performs the DNS query on the server name and resolves one (or a prioritised list) of the IP address(es), which represents a physical or logical AS.
3. The S-CSCF caches the IP address of the assigned AS and stores it during the IMS registration period of the user.
4. The S-CSCF routes the request to the assigned AS. (Depending on the service the AS could read/write/store user data, e.g., using Sh interface).

Figure J.3.2.2 shows how subsequent service requests are routed directly to the assigned AS during the registration period of the IMS user:

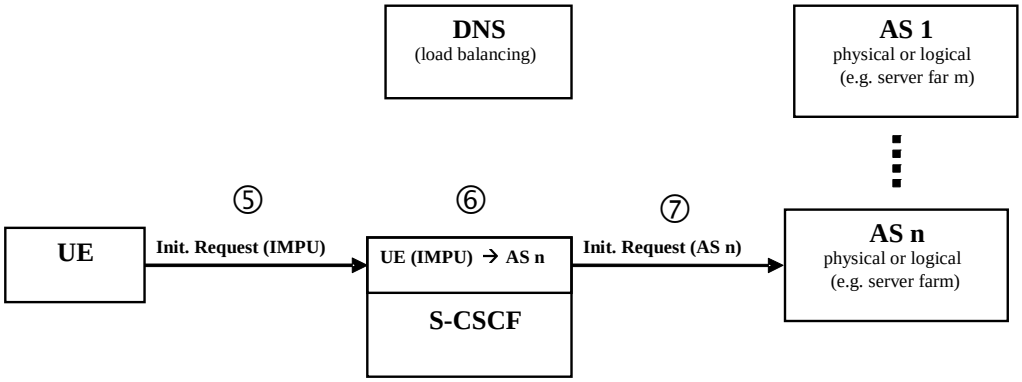


Figure J.3.2.2: S-CSCF has stored assigned AS for following service requests

5. The IMS user requests the service again and sends an initial request to the S-CSCF.
6. The S-CSCF has stored the IP Address (or a prioritised list) of the assigned AS. There is no longer need to perform a DNS query.
7. The S-CSCF routes the request to the assigned AS. (Depending on the service the AS can reuse prior stored user data).

The AS pre-assignment and storage could be also done after downloading the service profile during the user registration procedure.

Annex K (normative): Inter-IMS Network to Network Interface between two IM CN subsystem networks

K.1 General

This annex describes the Inter-IMS Network to Network Interface which is used to interconnect two IM CN subsystem networks.

K.2 Overall architecture

Figure K.1 illustrates an high-level architecture diagram showing the Inter-IMS Network to Network Interface (II-NNI) between two IM CN subsystem networks.

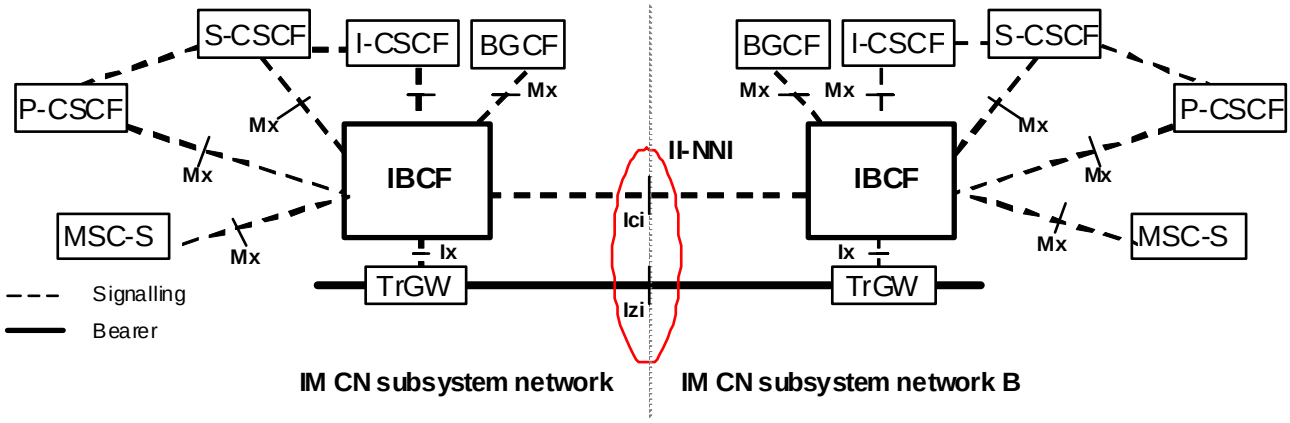


Figure K.1: Inter-IMS Network to Network Interface between two IM CN subsystem networks

The protocols over the two reference points Ici and Izi make up the Inter-IMS Network to Network Interface.

The Ici reference point allows IBCFs to communicate with each other in order to provide the communication and forwarding of SIP signalling messaging between IM CN subsystem networks. The Izi reference point allows TrGWs to forward media streams between IM CN subsystem networks.

NOTE: Whenever the Inter-IMS Network to Network Interface is used to interconnect two IM CN subsystem networks belonging to different security domains security procedures applies as described in TS 33.210 [20].

Annex L (normative): Aspects for use of Common IMS in 3GPP2 systems

L.1 General

This clause describes the main concepts that are used when providing IMS services using 3GPP2 IP-CAN as defined in 3GPP2 X.S0011 [60] or using 3GPP2 radio access with CDMA 1X as defined in 3GPP2 C.S0001-D [61] and/or HRPD as defined in 3GPP2 C.S0024-A [62] and/or UMB as defined in 3GPP2 C.S0084-000 [63] radio access.

L.2 Definitions

L.2.1 HSS

For 3GPP2 systems, the term "HSS" is used to represent the Home AAA entity plus the Databases to which it interfaces. The HSS in 3GPP2 systems does not include the HLR functionality. Figure x shows the HSS in 3GPP2 systems.

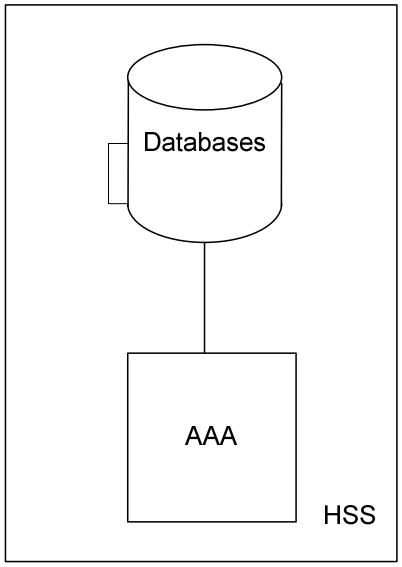


Figure L.1: HSS in 3GPP2

L.3 Mobility related concepts when using 3GPP2 Packet Data Subsystem

L.3.1 General

The Mobility related procedures for 3GPP2 systems are described in 3GPP2 X.S0011 [60] and the IP address management principles are described in 3GPP2 X.S0011 [60]. As specified by these procedures, the UE acquires the necessary IP address(es) to access IM CN system.

The restriction on using a single IP address for IMS Local Breakout functionality as defined in clause 5.1.0 does not apply to 3GPP2 based systems.

L.3.2 Procedures for P-CSCF discovery

This clause describes the P-CSCF discovery procedures applicable for 3GPP2 systems. These procedures follow the generic mechanisms described in clause 5.1.1 with the following exception:

- Discovery of P-CSCF as part of establishment of connectivity towards the 3GPP2 IP-CAN is not supported.

L.4 QoS related concepts when using 3GPP2 Packet Data Subsystem

The QoS procedures follow the generic requirements described in clause 4.2.5 with the following modification to bullet 6.e in clause 4.2.5:

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

L.5 IP version support in IMS when using 3GPP2 Packet Data Subsystem

The UE shall support IPv4 only or both IPv4 and IPv6.

L.6 Address and identity management concepts

L.6.1 Deriving IMS identifiers

ISIM is the primary source for IMS identity information. If an ISIM is not present, the UE shall use the IMS credentials stored in the IMC to access IMS.

If no IMS credentials are stored in the IMC, then temporary credentials shall be derived as follows:

- a Temporary Private User Identity shall be derived from the Mobile Station ID (IMSI, MIN or IRM), which allows for uniquely identifying the user within the operator's network;

- a Temporary Public User Identity shall be derived from the MSID, and shall be used in SIP registration procedures. The Temporary Public User Identity shall take the form of a SIP URI (as defined in RFC 3261 [12] and RFC 3986 [13]).

It is strongly recommended that the Temporary Public User Identity is set to barred for SIP 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 SIP initial registration, re-registration and mobile initiated de-registration procedures.

- The implicitly registered Public User Identities shall be used for session handling, in non-registration SIP messages and may be used at subsequent SIP registration procedures.

- A Temporary Public User Identity shall only be available to the CSCF and HSS nodes.

NOTE: If a Temporary Public Identity is used, the user can not initiate any sessions until the implicitly registered public identities are available in the UE.

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.

L.7 Relationship to 3GPP Generic User Profile (GUP)

3GPP GUP is not applicable to 3GPP2 systems.

Annex M (informative): IMS Local Breakout

M.1 P-CSCF located in visited network

M.1.1 Description

M.1.1.0 General

The architectures and flows in this clause are only showing EPS and 5GS. The principles shown are also applicable for GPRS Core Network.

For 5GS, there is no support for roaming interface between vPCF and hPCF in this Release of the specification.

M.1.1.1 Architecture

The architecture for this scenario is shown in figure M.1.1.1.

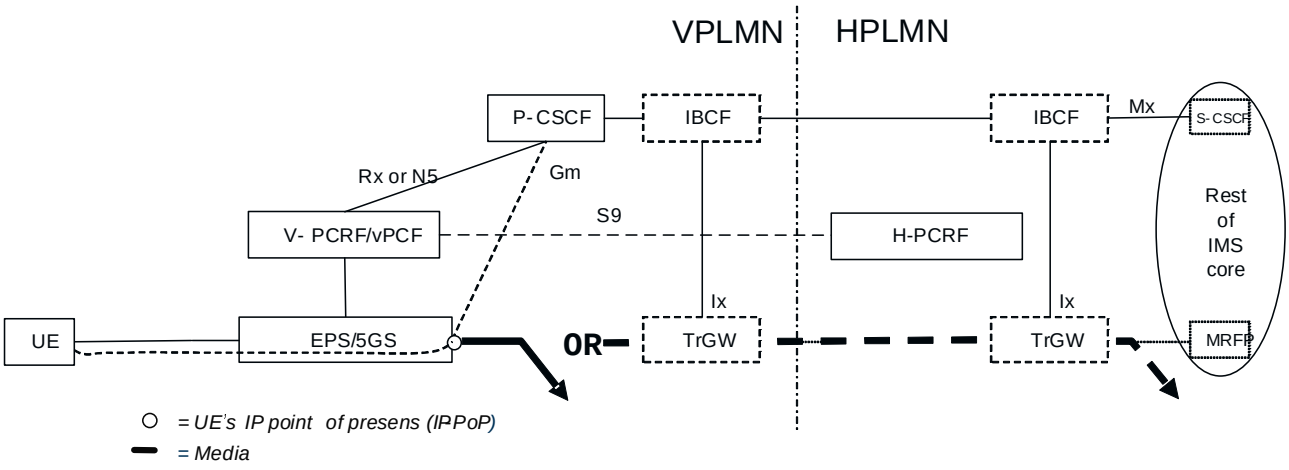


Figure M.1.1.1: EPS/5GS architecture for IMS Local Breakout with P-CSCF located in visited network

Optionally IBCF and TrGW may be present in the HPLMN and VPLMN according to II-NNI reference architecture (see Annex K), and thus there will be an Ici reference point between the IBCFs and an Izi reference point between the TrGWs.

M.1.1.2 Flow for originating session

The information flows for originating session for this scenario is illustrated in figure M.1.1.2.

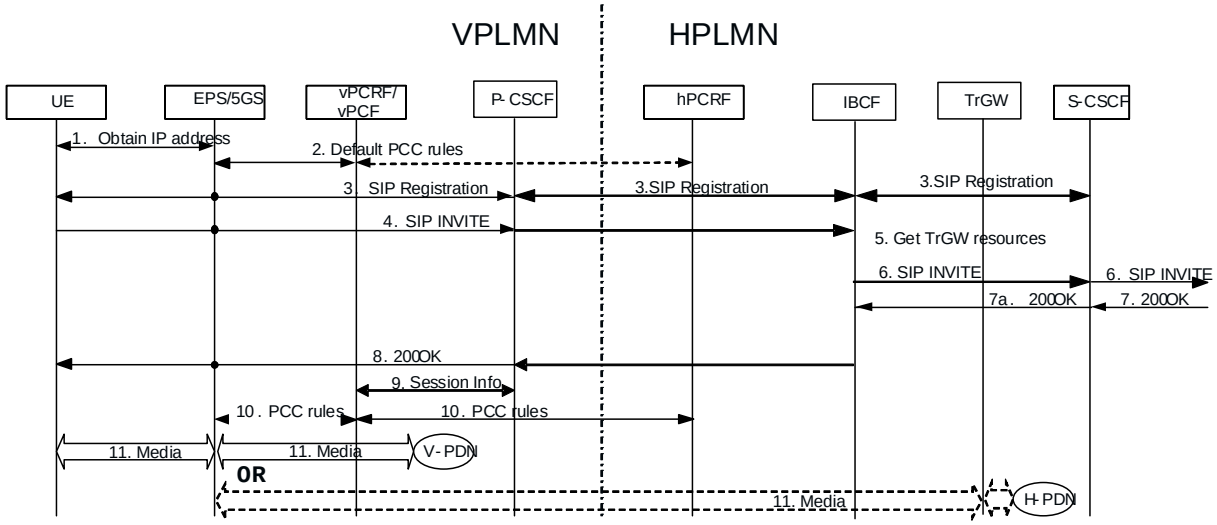


Figure M.1.1.2: Example scenario with P-CSCF located in visited network and IBCF and TrGW in home network

1. The UE obtains an IP address from the EPS/5GS in the visited network according to the procedures specified by TS 23.401 [70] / TS 23.502 [94].

2. The EPS/5GS obtains default PCC rules and associates it with this IP-CAN. The V-PCRF/vPCF and H-PCRF (in the case of S9 in EPS) provides these rules according to TS 23.203 [54] / TS 23.503 [95].

3. Using the IP address obtained in step 1, the UE performs IMS registration. This SIP message is routed by the EPS/5GS in the visited network through the P-CSCF in the visited network, which was discovered according to the procedures in Annex E/Annex Y, to the S-CSCF in the home network, via IBCFs also in the visited and home network if deployed.

4. Using the IP address obtained in step 1 in the SDP, the UE initiates a SIP session. The INVITE request is routed by the EPS/5GS in the visited network through the P-CSCF to the IBCF in the home network.

5. If the IBCF decides to route media to home based on operator policy, it then allocates resources in TrGW and alters the offered SDP accordingly.

NOTE 1: Per operator policy, the IBCF may have other reasons than only address translation to route media home.

6. IBCF sends the INVITE further to the S-CSCF, and S-CSCF continues the session towards the far-end.

7 The 200 OK received from the far-end is sent by the S-CSCF to the IBCF. If a TrGW was allocated in step 5, then IBCF changes the SDP answer accordingly.

NOTE 2: Step 7a) If the IBCF decides to anchor the call when it has received SDP answer (e.g. because the MRFP needs to be involved in the user plane or because of other reasons), then step 5 in the procedure starts again, and it re-INVITEs the far-end.

8. The 200 OK is sent further on to the P-CSCF and via EPS/5GS in the visited network towards the UE.

9. The P-CSCF in the visited network also provides the session information to the V-PCRF/vPCF in the visited network.

10. The H-PCRF in the home network provides PCC rules to the V-PCRF in the visited network when S9 is supported. The V-PCRF/vPCF in the visited network provisions PCC rules in the EPS/5GS in the visited network

11. Media exchanged between the UE and the far end is now routed either between the 5GS in the visited network and the far end, thus achieving local breakout mode of operation; or between the EPS/5GS in the visited network via the TrGW in the home network if IBCF was deployed.

NOTE 3: Per operator policy, the IBCF can route media home due to other reasons than stated in this specification, thus also giving the possibility to get home routed mode of operation.

M.2 P-CSCF located in home network

M.2.1 Description

M.2.1.0 General

The architectures and flows in this clause are only showing EPS and 5GS. The principles shown are also applicable for GPRS Core Network.

This scenario assumes that both IMS signalling and IMS media traffic are anchored in EPS/5GS in the Visited network. UE performs a P-CSCF discovery according to clause 5.1.1.0.

M.2.1.1 Architecture

The Local Breakout architecture for P-CSCF at home is shown in figure M.2.1.1.

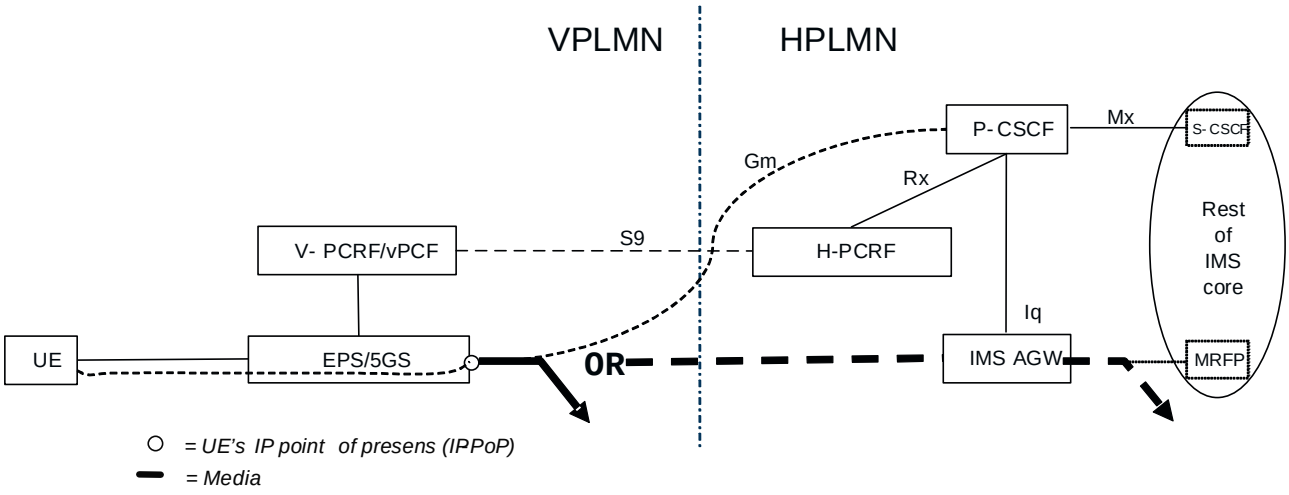


Figure M.2.1.1-1: EPS/5GS architecture for IMS Local breakout with P-CSCF located in home network

M.2.1.2 Flow for originating session

The information flows for originating session for this scenario is illustrated in figure M.2.1.2.

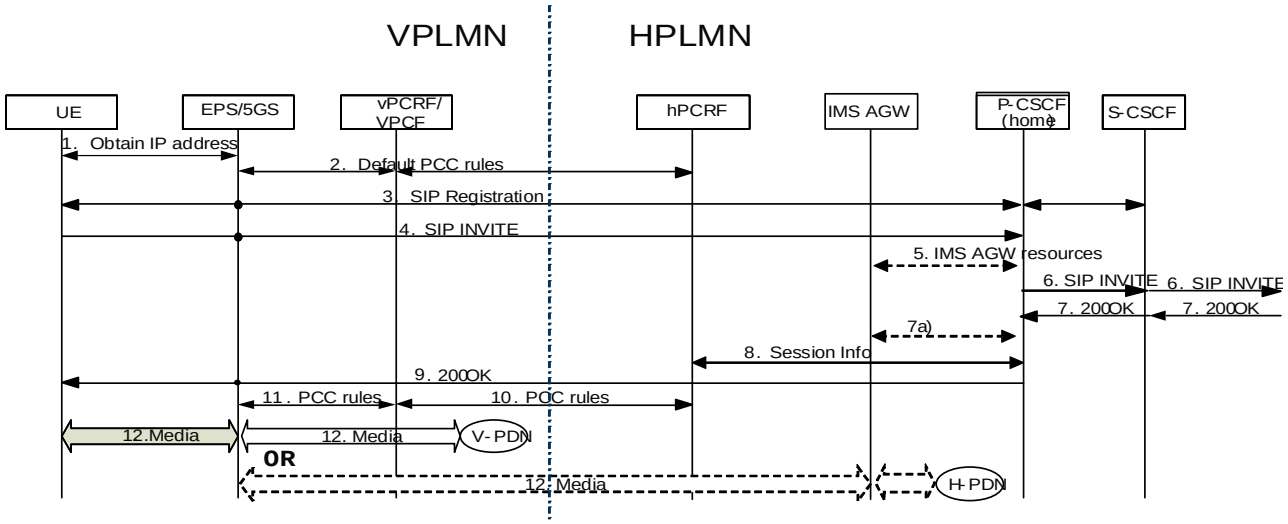


Figure M.2.1.2: Example scenario with P-CSCF located in home network

1 The UE obtains an IP address from the EPS/5GS in the visited network, according to the IP Connectivity Access Network procedures specified by TS 23.401 [70] /TS 23.502 [94].

2 The serving EPS/5GS (in visited network) obtains default PCC rules, and associates it with this IP-CAN. The V-PCRF/vPCF and H-PCRF (in the case S9 in EPS is available) provides these rules according to TS 23.203 [54] / TS 23.503 [95].

3 Using the IP address obtained in step 1, the UE performs IMS registration. This SIP message is IP-routed by the EPS/5GS, in the visited network, to the P-CSCF in the home network, which was discovered according to the procedures in clause 5.1.1. When P-CSCF receives the REGISTER message, it optionally interacts with H-PCRF/vPCF to subscribe to signalling bearer state changes.

4 Using the IP address obtained in step 1 in the SDP, the UE initiates a SIP session. The INVITE request is routed from the EPS/5GS in the visited network, via the visited PDN to the P-CSCF in the home network.

5 If the P-CSCF decides to route media to home e.g. due to the need for address translation or due to other reasons, it then allocates resources in IMS AGW and alters the offered SDP accordingly.

NOTE 1: Per operator policy, the P-CSCF may have other reasons to route media to the home PLMN.

6. INVITE proceeds from P-CSCF to S-CSCF and onwards.

7. 200 OK is received from the far end by the P-CSCF. If an IMS-AGW was allocated in step 5, the P-CSCF changes the SDP answer accordingly.

NOTE 2: In step 7a) if the P-CSCF decides to route media home when it receives the SDP answer, then step 5 in the procedures starts again, and it re-INVITEs the far end.

8. The P-CSCF provides the session information to the H-PCRF/hPCRF in the home network.

9. The 200 OK received from the far-end is sent by the P-CSCF through the EPS/5GS in the visited network towards the UE.

10-11. Based on the IP address included in the session information, the H-PCRF in the home network provides the PCC rules to the V-PCRF in the visited network when S9 is available. The V-PCRF/vPCF in the visited network provisions PCC rules in the EPS/5GS in the visited network.

12. Media exchanged between the UE and the far end is now routed either between the EPS/5GS in the visited network and the far end, thus achieving local breakout mode of operation; or between the EPS/5GS in the visited network via the IMS AGW in the home network if step 5 or step 7a happened.

NOTE 3: Per operator policy, the P-CSCF may route media home due to other reasons than stated in this specification, thus also giving the possibility to get home routed mode of operation.

M.2.2 Address assignment

Home domain and visiting domains can not be managed to share the same private IPv4 address space, and furthermore Rx and N5 do not support globally unique addresses (realm information is not supported) which would be needed to handle overlapping private IPv4 address spaces. Therefore, both the address assigned to the UE and the address of the P-CSCF must be globally unique IP addresses.

If the visited operator cannot assign a globally routable IPv4 address to an individual UE, then an IPv6 address will be assigned, if the UE supports IPv6.

M.2.3 IPv4 - IPv6 interworking

In a dual-stack IMS environment, an SDP offer to an UE with a single IP address may offer a media bearer over the IP version not supported by the UE. For such a call to succeed, a NAPT-PT capable media relay is needed to be inserted in the media path. The alternatives for this are: to deploy either IMS-AGWs either in home or visited network; or TURN servers in visited network.

To use IMS-AGWs in the home network is the way the home operator is able to control whether the IMS user plane traffic shall be routed home or not in this scenario. Thus, it is possible to do NAPT-PT, but it will be done in the home network, which means all traffic that needs interworking will be home routed.

To use TURN servers requires all IPv6 terminals to support TURN IPv4 - IPv6 interworking, and that the visited network supports TURN IPv4 - IPv6 interworking.

NOTE 1: Since IPv4 - IPv6 interworking must be done on IPv6 side, IPv6 originating sessions to IPv4 UEs may need an extra INVITE because first INVITE may fail.

NOTE 2: An IP type PDU session for a 5GS UE will have either an IPv4 or an IPv6 address, see Annex Y.

M.2.4 NAT traversal

Although this scenario assumes globally routable IP addresses, there is still a possibility that end users may use residential NAT/firewalls before connecting to EPS.

Annex G describes two methods how NAT/FW may be supported, if the UE accesses IMS using an IP address of a local private network.

M.3 P-CSCF located in visited network and with VPLMN loopback possibility

M.3.1 Description

M.3.1.1 General

The architecture and flows in this clause are assuming local breakout with P-CSCF in VPLMN, for further info about local breakout see clause M.1.

M.3.1.2 Architecture

The architecture for this scenario is shown in figure M.3.1.2. The Transit and Roaming Function and the related requirements are defined in clause 4.15a.

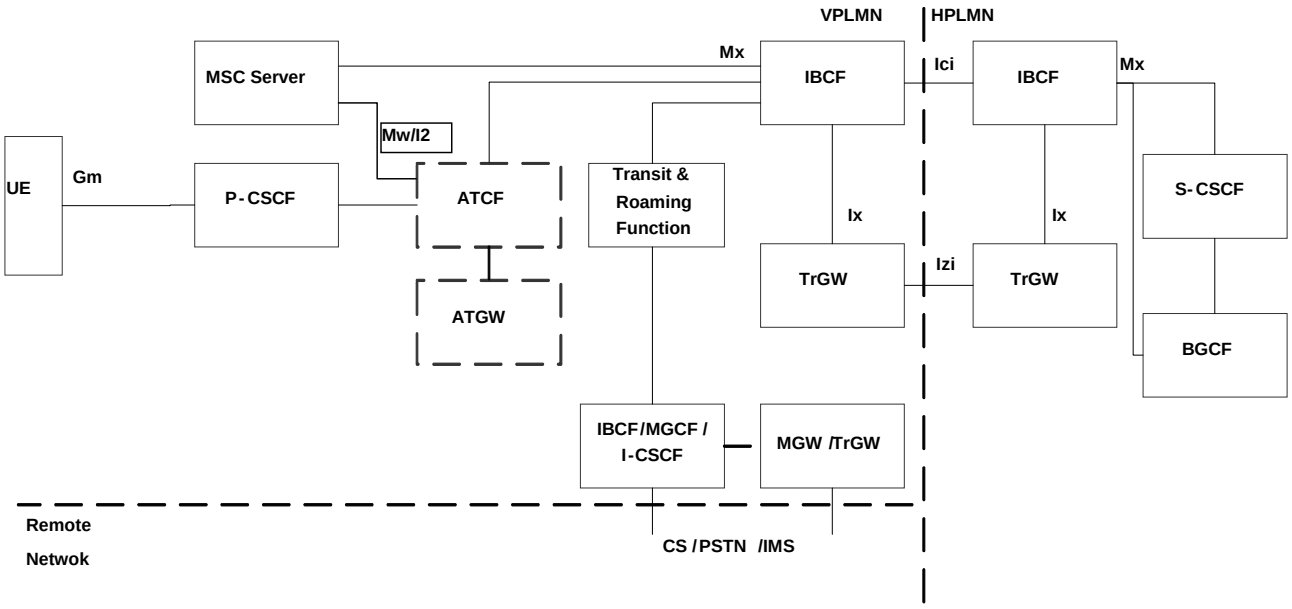


Figure M.3.1.2: Overall architecture for IMS Local Breakout with P-CSCF located in visited network and with VPLMN loopback possibility

M.3.1.3 Flow for originating session with VPLMN routing

The information flows for originating session with VPLMN routing for this scenario is illustrated in figure M.3.1.3.

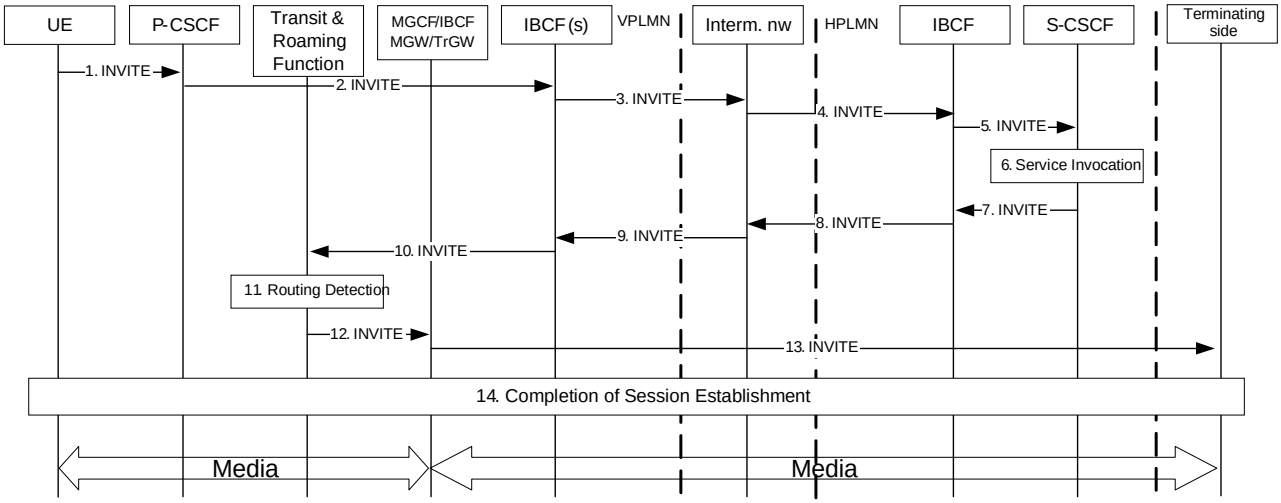


Figure M.3.1.3: Example scenario with P-CSCF located in visited network and with VPLMN routing

1. The roaming UE sends an INVITE request to the P-CSCF.

2. P-CSCF forwards the INVITE request to the visited IBCF. Based on operator policy, the P-CSCF adds a reference to the preferred Transit and Roaming Function.

3. This first IBCF in the VPLMN allocates a TrGW for the media and follows standard OMR procedures when forwarding the INVITE request to allow this TrGW to be bypassed if the INVITE request later returns to the VPLMN and no other intermediate nodes anchor the media before the request returns.

4-5. The intermediate network and the first IBCF in the HPLMN forward the INVITE request to the S-CSCF. Nodes in the intermediate network and the first IBCF in the HPLMN support OMR and allow their TrGWs to be bypassed.

6. The S-CSCF performs service invocation.

7. The S-CSCF performs routing decision, and based on local policy and on the facts that the UE is roaming, a roaming agreement for VPLNM call routing is in place, and home routing is not required, the S-CSCF decides to route back to the VPLMN for call routing. A loopback indicator is included in the INVITE request to inform the VPLMN that this request is being routed back to the VPLMN for call routing. The S-CSCF can also forward UE location information to the VPLMN. If a reference to the preferred Transit and Roaming Function is available in the request, the S-CSCF uses this information to route the session back to the VPLMN. If a reference to the preferred Transit and Roaming Function is not available, the S-CSCF uses a default derived address to the Transit and Roaming Function to route the session back to the VPLMN.

   If local policy requires access to BGCF routing data to make the loopback decision for a particular SIP request, then the loopback decision can be performed in the BGCF.

8-9. The IBCF in the HPLMN and the intermediate network forward the SIP request towards the indicated Transit and Roaming Function in the VPLMN. Functions in the intermediate network support OMR and allow their TrGWs (if any) to be bypassed.

10. The IBCF in the VPLMN receives the SIP request, notes that the SDP includes an alternative media address within the VPLMN that allows bypass of allocated TrGWs, applies OMR to remove any TrGWs allocated between the VPLMN and HPLMN, and forwards the request to the indicated Transit and Roaming Function.

11. Based on the loopback indicator, the Transit and Roaming Function detects that this is a loopback request. The Transit and Roaming Function routes the request toward the destination network based on available SIP URI, ENUM lookup, or BGCF routing. The Transit and Roaming Function can use information such as originating UE location to select a nearby egress point for media anchoring.

12. If the called party is determined to be available in IMS, the call is routed towards the remote end through an IBCF. If the called party is determined to be available in CS, the call is broken out to CS through an MGCF. If the called party is determined to be available in VPLMN, the call is routed to the I-CSCF. The called party information is included in the Request URI when forwarding the request to the next hop.

    When forwarding to an IBCF, the Transit and Roaming Function ensures by means of signalling that media is anchored in the VPLMN.

NOTE 1: If the called user is an IMS user of the VPLMN then the call will be routed directly to the terminating side, (i.e. I-CSCF of the VPLMN) without traversing an MGCF/IBCF.

13. The MGCF/IBCF performs normal call routing procedures to route towards the remote network/end.

NOTE 2: The call will be anchored in the VPLMN (outgoing IBCF), and OMR is not provided towards the terminating side.

14. The session establishment is completed.

NOTE 3: During subsequent session establishment signalling, OMR information passed back through the IBCFs and intermediate networks between the VPLMN and HPLMN cause them to release any allocated TrGWs.

M.3.1.4 Flow for originating session with Home routing

The information flows for originating session with the possibility for VPLMN routing, but where the HPLMN decides to perform home routing is illustrated in figure M.3.1.4.

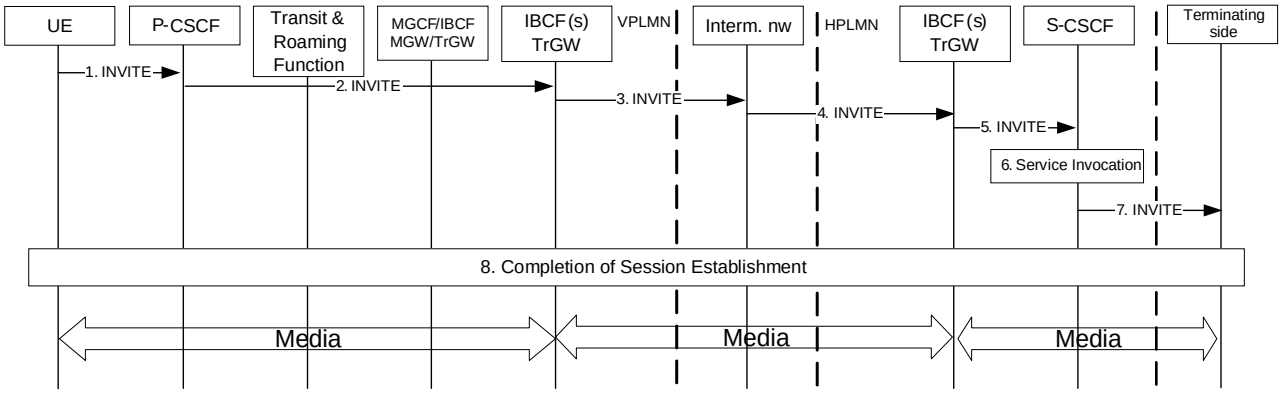


Figure M.3.1.4: Example scenario with P-CSCF located in visited network and with home routing

1-6. These steps are done according to clause M.3.1.3.

7. The S-CSCF performs routing decision, and based on the facts that the UE is roaming, and home routing is required, the S-CSCF decides to route the INVITE request directly from the home network towards the terminating side. If local policy requires access to BGCF routing data to make the routing decision for a particular SIP request, then the routing decision can be performed in the BGCF. When forwarding, the S-CSCF/BGCF ensures by means of signalling that media is anchored in the HPLMN.

NOTE: The S-CSCF decides whether to perform home routing based on local policy or based on knowledge that the VPLMN does not support the loopback procedure.

8. The session establishment is completed.

M.3.2 Interaction with SRVCC and ICS

The IMS roaming with local breakout and possibility for loopback also applies for ICS and SRVCC as follows:

- For an originating session for PS to CS SRVCC or vSRVCC that uses ATCF enhancements, the ATCF is in the signalling path between the P-CSCF and IBCF in the VPLMN (i.e. at step 2 in clause M.3.1.3).

- For an originating sessions that uses CS media with MSC Server enhanced for ICS, the UE initiates a CS call setup towards the MSC Server enhanced for ICS, and the MSC Server enhanced for ICS will initiate the call setup towards IMS analogous to the INVITE request from P-CSCF (i.e. at step 2 in clause M.3.1.3). As for the P-CSCF, the MSC Server enhanced for ICS may provide a reference to the preferred Transit and Roaming Function:

Annex N (normative): Aspects for use of Common IMS in Fixed xDSL, Fiber and Ethernet based systems

N.1 Origination procedures

N.1.1 (FO#1) Fixed xDSL origination, home

This origination procedure applies to users located in their home service area. As in clause 5.6.2, the UE is located in the home network, but is using an xDSL IP-CAN to access the IM CN Subsystem.

NOTE: The below flows are example flows. The detailed stage 2 description of the RACS information flows can be found in ETSI ES 282 003 [78].

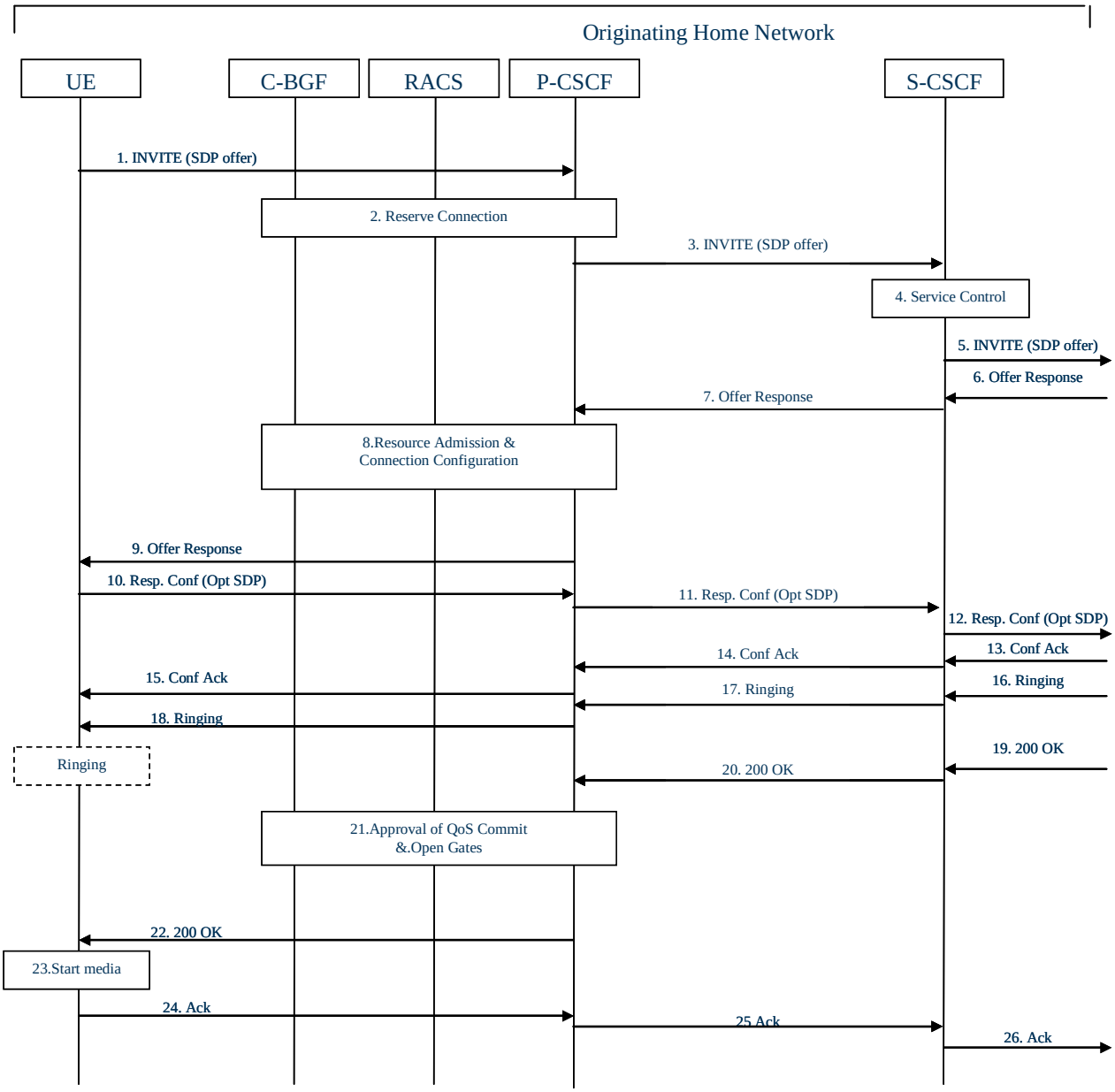


Figure N.1.1: Fixed xDSL originating - home (example flow)

Procedure F0#1 is as follows:

1. UE sends the SIP INVITE request, containing an initial SDP, to the P-CSCF address determined with P-CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session.

2. A connection is reserved in the C-BGF with optional NAT binding list retrieval.

3. 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.

4. S-CSCF validates the service profile, and invokes any origination service logic required for this user. This includes authorization of the requested SDP based on the user's subscription for multi-media services.

5. S-CSCF forwards the request, as specified by the S-S procedures. In addition, subject to operator policy, the S-CSCF may insert in the request a reference location of the user, when network-provided location information is not already present. The reference location (e.g. line identification) is determined by the operator as part of the user profile and may be received from the HSS at registration.

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

7-9. S-CSCF forwards the Offer Response message to the P-CSCF which triggers RACS. RACS performs admission control based on the Offer and Answer parameters.
RACS configures the connections in the C-BGF based on the SDP answer and optionally requests a NAT binding list.

10. 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 9 or a subset. If new media are defined by this SDP, a new connection configuration shall be performed following step 2. The originating UE is free to continue to offer new media in this request or in subsequent requests using the Update method. Each offer/answer exchange will cause the P-CSCF to repeat the RACS interactions again.

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. 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 admission control and configure connection flows are repeated.

14-15. S-CSCF and P-CSCF forward the answered media towards the UE.

16-18. 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. UE indicates to the originating user that the destination is ringing.

19-20. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating endpoint, as specified by the termination procedures and the S-S procedures.

21. P-CSCF performs the approval of QoS Commit procedure which triggers the Open Gates procedures if required.

22. P-CSCF passes the 200-OK response back to UE.

23. UE starts the media flow(s) for this session.

24-26. 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 endpoint.

N.2 Termination procedures

N.2.1 (FT#1) Fixed xDSL termination, home

NOTE: The below flows are example flows. The detailed stage 2 description of the RACS information flows can be found in ETSI ES 282 003 [78].

This termination procedure applies to users located in their home service area. As in clause 5.7.2, the UE is located in the home network, but has registered to the IM CN Subsystem via an xDSL IP-CAN.

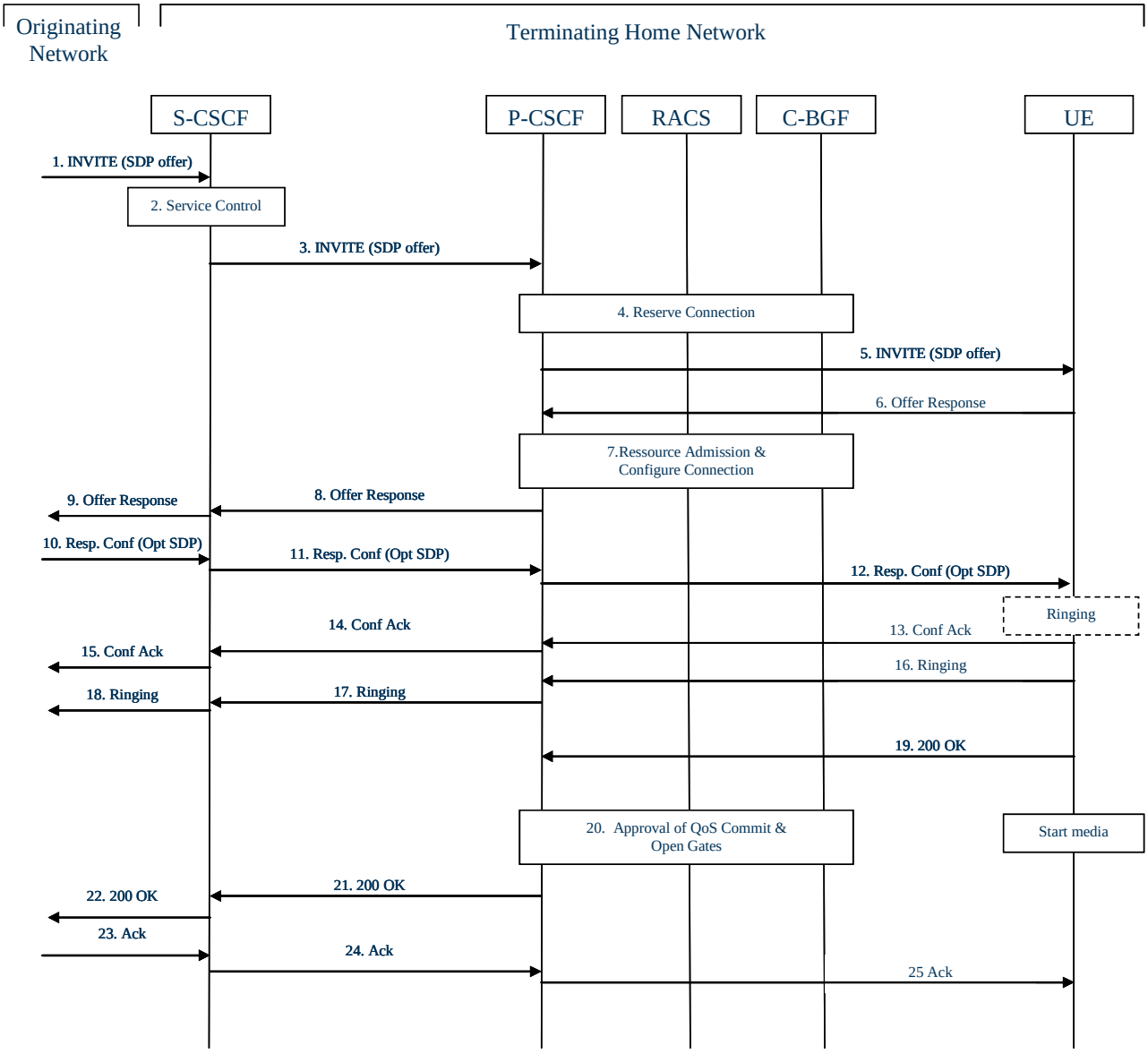


Figure N.2.1: Fixed xDSL terminating - home (example flow)

Procedure FT#1 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, via one of the origination procedures and the S-S procedures, to the S-CSCF for the terminating UE.

2. S-CSCF validates the service profile, and invokes any termination service logic required. This includes authorization of the requested SDP based on the user's subscription for multi-media services.

3. S-CSCF remembers (from the registration procedure) the P-CSCF address for this UE. The S-CSCF forwards the INVITE to the P-CSCF, which in this case is located in the home network.

4. The P-CSCF triggers RACS which reserves a connection in C-BGF with optional NAT binding retrieval.

5. P-CSCF remembers (from the registration procedure) the UE address, and forwards the INVITE to the UE.

6. UE determines the subset of the media flows proposed by the originating endpoint that it is capable and willing to support, 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 the P-CSCF.

7. P-CSCF triggers RACS to perform admission control based on Offer and Answer parameters.
RACS configures the connection in the C-BGF based on SDP answer with optional NAT binding retrieval.

8. P-CSCF forwards the Offer Response message to S-CSCF.

9. S-CSCF forwards the Offer Response message to the originator, per the S-S procedure.

10-15. The originating endpoint sends a Response Confirmation via the S-S procedure, to the terminating S-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in step 19 or a subset. If new media are defined by this SDP, a new interaction with the RACS (as in steps 4-8) will be done by the P-CSCF. The originating UE is free to continue to offer new media in this request or in a subsequent request using the Update method. Each offer/answer exchange will cause the P-CSCF to repeat the RACS interactions (steps 4-8) again.

16-18. 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 endpoint.

19. When the destination party answers, UE sends a SIP 200 OK final response to P-CSCF.

20. P-CSCF indicates that the resources reserved for this session should now be committed.

21-22. P-CSCF forwards the 200 OK to S-CSCF, following the signalling path.

23-25. 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.

N.3 Geographical Identifier

For fixed xDSL, Fiber or Ethernet access, Geographical Identifier may be used within the IMS as described in clause E.8.

Annex P (informative): Transcoding Support involving the MRFC/MRFP

P.1 General

P.1.1 Scope

This clause describes media transcoding services involving the MRFC/MRCP applicable in the following cases:

- between two IMSs;
- between an IMS and other SIP based multimedia network; and
- internal to an IMS servicing media endpoints with different media encoding requirements. This can arise due to support of different access technologies (e.g. wireline-wireless interworking, or support of non-3GPP wireless technologies), or from divergence in supported or allowed media encoding formats (e.g. configuration of devices to only allow certain codecs).

The MRFC and MRFP act as transcoding entity in an IMS solving media encoding mismatches due to codec selection between operator networks, as well as to deal with encoding formats in a converged service environment.

P.1.2 Description

Application Servers can invoke the MRFC for the purpose of media transcoding between UEs that have no supported codec in common. The MRFC controls functionality in the MRFP to perform media plane transcoding.

The decision to perform media transcoding requires knowledge of the codecs supported by the calling and called UEs. Media transcoding services can be triggered proactively (before the session request is sent to the called UE) or reactively (after the session request has been sent to, and rejected by, the called UE). Proactive transcoding invocation requires prior knowledge of the codecs supported by the UE at which the called party is registered. In the case of reactive transcoding the list of codecs supported by the called UE is carried in the SIP response message.

NOTE: Calling and called UEs can be in an IMS or in a CS network. SIP requests are sent by either the called UE or a network entity acting on behalf of the calling UE. SIP requests are answered by either the called UE or a network entity acting on behalf of the called UE.

P.1.3 Session flows

P.1.3.1 General

The following use cases illustrate session procedures involving the MRFC required to support transcoding between UEs due to error cases or incompatible terminal equipment. In addition, transcoding procedures are applicable to both the originating and the terminating side of the session or even (in inter-network scenarios) in a transit network, and are subject to bilateral agreements and operator configuration. A media transcoding session refers to a SIP session between an entity in the IMS control plane (hereafter referred to as the "invoking function") and the MRFC/MRFP as actual transcoding device, setup for the purpose to mediate between calling and called UEs. The SIP session between the invoking function and the MRFC is used to reserve resources at the transcoding unit, in this case the MRFP, and to exchange transport address and port information. The session flows described here have been simplified by abbreviating the message exchange, e.g., by eliminating 100 trying messages. Similar session flows are available in Annex B of TS 23.218 [71].

P.1.3.2 Proactive transcoding invocation

As noted above, proactive transcoding invocation requires prior knowledge of the codecs supported by the UE at which the called party is registered. At session initiation the calling UE capabilities are contained in the SDP offer, while

called UE capabilities can be either preconfigured or known by other means in the network (e.g. if the control plane entity responsible for detecting the need of transcoding previously learned the codecs supported by the UE that is now called by monitoring session requests initiated by it).

The following session flow illustrates proactive media transcoding:

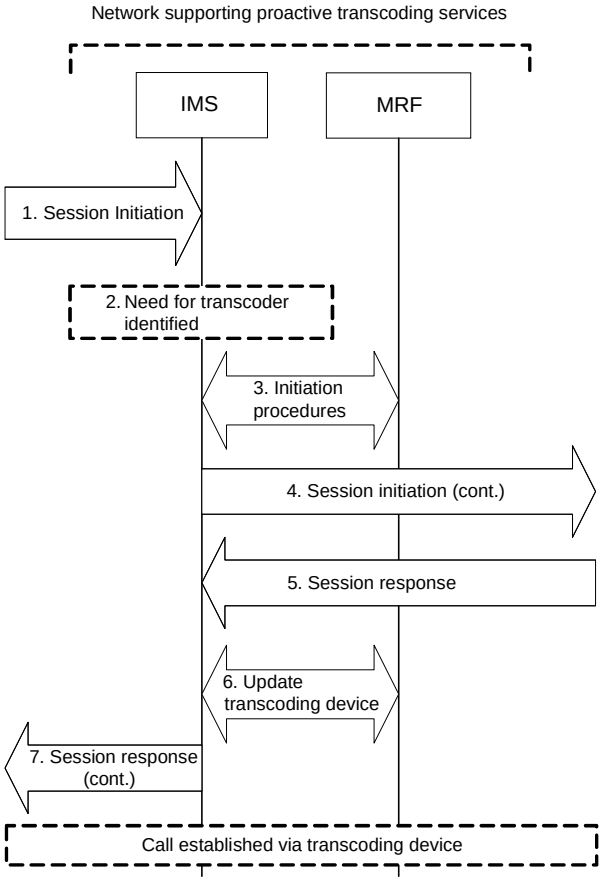


Figure P.1.3.2-1: Proactive transcoding triggering logic

1. Calling UE sends a SIP request targeted at an address registered at the called UE, including an SDP offer containing codec(s) and the IP address and TCP or UDP port number at which the calling UE wishes to receive media.

2. The SIP request is received by an IMS control plane entity responsible for detecting the need of proactive transcoding invocation. If the SDP offer does not include any codec supported by the called UE, then the invoking function is triggered to set up a SIP session with the MRFC, providing codecs and transport parameters to initiate a transcoding session.

NOTE 1: If the codec(s) supported by the called UE are not known, or the SDP includes one of the codec(s) supported by the called UE, the SIP request is forwarded to the called UE without manipulation. This step is not illustrated in the figure.

3. The invoking function instructs the MRFC to:

   - allocate media processing resources from an MRFP entity under the MRFC's control, configured with the address and port at which the calling UE wishes to receive media, using a codec (say, codec-A) previously included by the calling UE in the SDP offer and hence known to be supported;

   - allocate media processing resources from the same MRFP entity to the called UE, using a codec (say, codec-B) known to be supported by the called UE; and

   - cause the MRFP entity to bridge those two media flows, such that media received on one will be converted to the format of and transmitted on the other.

The MRFC accepts the transcoding request and contacts an MRFP to allocate the requested resources. The MRFP responds with the IP address and port number associated with each requested codec. The MRFC returns this information to the invoking function.

4. The invoking function updates the SIP request received in step 1 by appending codec-B to the list of codecs in the SDP offer (after all codecs that were previously in the offer), and altering the transport address and port information to indicate the addresses associated by the MRFP with its resources of type codec-B.

5. Called UE acknowledges the SDP offer and makes a codec selection (codec-B), providing also its actual IP address/port number information in the SDP answer.

6. Upon receipt of the answer from the called UE, the invoking function updates the session with the MRFC (providing the codec selected and the address /port information from the SDP answer). The MRFC processes the received information to configure the transcoding unit with the codec, the destination address and port towards the called UE.

7. The invoking function modifies the SDP answer to reference codec-A, and the transport address and port information to indicate the addresses associated by the MRFP with its resources of type codec-A. The invoking function forwards the SIP message containing the SDP answer to the calling UE.

NOTE 2: If the invoking function determines that the called UE has selected a codec from the original SDP offer, it will inform the MRFC to release the transcoding resources allocated in step 3, send a new SIP request to the called UE to change the transport address and port information to those of the calling UE, and forward the unmodified SDP answer to the calling UE. These steps are not illustrated in the figure.

P.1.3.3 Reactive transcoding invocation

Reactive invocation of media transcoding is useful in the case that the calling and called UE support no common codec, and for whatever reason transcoding is not proactively invoked. In this case the SDP offer received by the called UE contains no codecs that the called UE supports. The called UE will answer with an appropriate SIP error response, which can include information about actually supported codecs. Transcoding invoked in response to receipt of such an error response is termed Reactive.

The following example session flow describes reactive invocation of media transcoding:

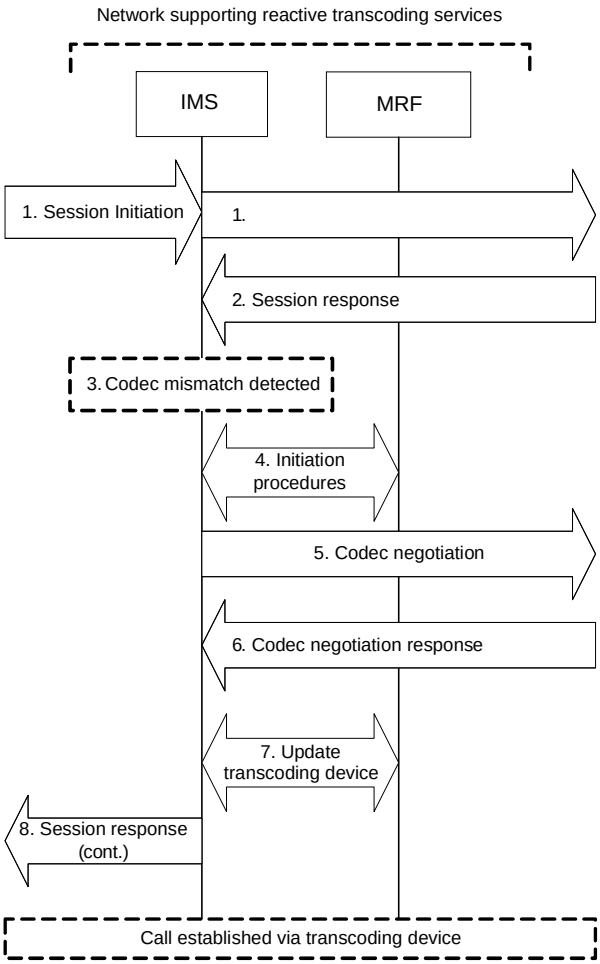


Figure P.1.3.3-1: Reactive transcoding triggering logic

1. Calling UE sends a SIP request, including an SDP offer containing codec(s) and the IP address and TCP or UDP port number at which calling UE wishes to receive media. For some reason, e.g. because proactive invocation of media transcoding is not supported in the terminating network, transcoding is not proactively invoked.

2. The called UE or a terminating network entity (such as MGCF) determines that it does not support any codec in the SDP offer and answers with an appropriate error response. This response can include a list of codecs that the called UE can support.

3. Based on the response from called UE indicating that it does not support the offered codecs, an IMS control plane entity responsible for detecting the need of reactive transcoding invocation triggers the invoking function to set up a SIP session with the MRFC, providing codecs and transport parameters to initiate a transcoding session.

4. The invoking function instructs the MRFC to:

   - allocate media processing resources from an MRFP entity under the MRFC's control, configured with the address and port at which the calling UE wishes to receive media, using a codec (say, codec-A) previously included by calling UE in the SDP offer hence known to be supported by calling UE;

   - allocate media processing resources from the same MRFP entity to called UE, using a codec (say, codec-B) known to be supported by called UE; and

   - cause the MRFP entity to bridge those two media flows, such that media received on one will be converted to the format of and transmitted on the other.

   The MRFC accepts the transcoding request and contacts an MRFP to allocate the requested resources. The MRFP responds with the IP address and port number associated with each requested codec. The MRFC returns this information to the invoking function.

5. Based on the information received from the MRFC, the invoking function creates a new SDP offer that contains the information provided by the MRFC (codec and transport addresses). If no information about supported codecs was available from the error response, the invoking function offers all codecs supported by the transcoding device. It sends this offer to the called UE.

6. Called UE acknowledges the SDP offer and makes a codec selection, providing in the SDP answer the IP address and TCP or UDP port at which it wants to receive media.

7. Upon receipt of the answer from the called UE, the invoking function updates the session with the MRFC (providing the codec selected and the address /port information from the SDP answer). The MRFC processes the received information to configure the transcoding unit with the codec, the destination address and port towards the called UE.

8. The invoking function modifies the SDP answer received from the called UE such that it refers to codec-A and the MRFP address and port number associated with it in step 4, and sends this message to the calling UE. The session between the end points is now established with the media flow traversing the transcoding device.

Annex Q (normative): Optimal media routing

Q.1 General

The purpose of optimal media routing (OMR) is to identify and remove unnecessary media functions from the media path for each media stream associated with a session.

The IP Multimedia Subsystem has the option to deploy media functions such as TrGWs on the media path associated with each media stream associated with a session. These media functions can perform only transport level functions such as firewall or NAT, or can also perform application level functions such as transcoding or conferencing. These media functions are typically allocated proactively during SDP offer/answer signalling within a session since it is unknown which of the functions are actually needed for a media stream until the SDP offer/answer signalling completes. For example, a transcoder can be allocated during session establishment but whether transcoding is needed is determined once the SDP offer reaches the far endpoint. In another example, the IBCFs at the boundary of a network allocate TrGWs to protect media functions within the network or to provide address translation to the private address space used within the network, however it might be determined later during session establishment that no media resources are needed within the network, thus making the TrGWs unnecessary.

Any SIP signalling entity within the IMS network that allocates, to a session flow, a media function that might later be determined to be unnecessary may implement the procedures in this Annex to assist in the removal of unnecessary media functions. In particular, any entity with an IMS-ALG may implement the OMR algorithm. This includes the IBCF (see Annex I) and P-CSCF (see Annex G). Any AS performing as a B2BUA controlling media resources may also implement the OMR procedures. Annex Q shows every controlling OMR entity as an IMS-ALG and every controlled media resources as a TrGW, but other options are possible. An MGCF or AS performing as UA may also implement OMR procedures to assist in the removal of unnecessary media functions in some cases. MGCF and AS procedures can be derived from the procedures in this annex by collocating an IMS-ALG with the MGCF or AS.

The OMR procedures identify and name the IP address realm used for each media path segment among UAs and TrGWs. The terms IP realm and realm are equivalent to the term IP address realm in this annex. An IP realm name is associated with each set of IP endpoints that are mutually reachable via IP routing and without address translation. Endpoints in different IP realms usually require allocation of a TrGW between those IP realms for connectivity and possibly for NAT.

When endpoints in different IP realms are mutually reachable without allocation of a TrGW, then OMR procedures may use provisioned information about such connected IP realms to determine possible optimal media paths through these connected realms.

NOTE: Connected IP realms are particularly useful when there are bilateral IP transport connections between operator networks, e.g., using IP tunnels via IP transport networks. In this case, each operator network can manage its own IP realm for inter-operator interconnection and provision the names of connected IP realms. Without the concept of connected IP realms, each bilateral connection (e.g. IP tunnel) in this example would need to be defined as its own IP realm.

IMS-ALGs implementing OMR shall include information in forwarded SDP regarding IP realm, codec and IP connectivity information for TrGWs on the media path to assist in bypassing unnecessary TrGWs. A TrGW can be bypassed when it is not required to transcode, when it is unnecessary to protect a network resource, and when a successive TrGW on the path is reachable by a previous TrGW on the path via a common IP realm.

The OMR procedures have the following additional characteristics:

- They build on the ALG NAT traversal model that is an alternative to the ICE NAT traversal model.
- They usually complete within a single end-to-end SDP offer/answer transaction. Some transcoding scenarios require additional signalling to complete optimisation.
- They apply independently to each media stream established by an SDP offer/answer transaction.
- They apply to media streams established between any types of endpoints (e.g., UEs, media servers, media gateways).

- They apply to media streams established using SIP 3pcc procedures. OMR applies to the endpoints of an SDP offer/answer transaction and not necessarily to the endpoints of a SIP dialog.
- They apply separately to each dialog when forking occurs. An IMS-ALG shall delay the release of a TrGW for OMR until it is clear that no forked dialog needs the TrGW.
- For early media negotiated with the same SDP as normal media, the OMR procedures have no direct impact on early media handling since path modifications are in place as soon as the SDP offer/answer transaction completes. An IMS-ALG can anchor in place any TrGW needed for blocking of unauthorized early media by removing OMR SDP extension attributes as necessary. For separate early-session disposition SDP the OMR algorithm shall not be applied.
- They do not require endpoints to support new procedures, although some additional optimisations are possible in some special cases.

Q.2 Procedures and flows

Q.2.1 SDP extension

Each OMR-capable entity on the signalling path of an SDP offer/answer transaction shall be able to manipulate an SDP offer to describe the following information about the IP realm associated with each known media path segment for each media line:

- a unique name for the IP realm on the subsequent media path segment,
- the position of the IP realm instance in the media path,
- connection/port data for the corresponding media resource in the IP realm on the subsequent media path segment,
- sufficient information to reconstruct the codec list for the previous media path segment if the codec list has changed (e.g. to offer transcoding options).

Each instance of such information is called an IP realm instance. Each IP realm instance associated with a media line in an SDP offer is a visited realm instance. If a signalling entity on the path controls a media resource with connection to an alternate IP realm not already associated with a media line, the SDP may also include the same information about the alternate IP realm, called a secondary realm instance.

An OMR-capable entity that forwards an SDP offer with OMR specific attributes for a media line shall ensure that the forwarded SDP offer includes a visited realm instance that matches the connection information for the media line in the forwarded SDP offer. This SDP offer shall also include information that makes it possible for a subsequent OMR-capable entity to detect if an intermediate entity has changed any codec information for the media line without also changing the connection and port information for the media line.

To bypass one or more previous TrGWs for a media line, an IMS-ALG shall include an IP realm instance with valid connection information for the earliest acceptable IP realm in the forwarded SDP answer. It shall be possible to identify the visited or secondary realm instance from the SDP offer that corresponds to the IP realm instance in the SDP answer.

Globally reachable IPv6 addresses shall be associated with a reserved realm name to assure that networks are not artificially isolated. Globally reachable IPv4 addresses shall be associated with another reserved realm name. Networks with private or restricted reachability shall have unique realm names.

Q.2.2 General IMS-ALG procedures

IMS-ALGs supporting OMR shall be able to support the call flows in clauses Q.2.4 and Q.2.5 according to local policy. These call flows describe the simplest scenarios and should be treated as examples. It shall be possible to support the addition of IMS-ALGs and TrGWs in any flow between any of the entities shown whenever such additions are reasonable. It shall be possible to support any interconnection of these flows whenever it is reasonable to do so. Additional information can be present in the forwarded SDP messages to support these more complex scenarios.

The following high level procedures apply to all of the scenarios.

Upon receiving an initial SDP offer, the IMS-ALG in the signalling path shall perform the following for each media line:

- If the SDP offer includes realm instance information for the media line, and the latest visited realm instance is not for the connection information in the incoming SDP offer, then the IMS-ALG shall remove all OMR specific SDP attributes from the SDP offer.

NOTE: A non-OMR-capable IMS-ALG might have inserted a TrGW without removing unrecognized OMR specific SDP attributes.

- If the SDP offer includes realm instance information that corresponds to the connection information in the incoming SDP offer, then the IMS-ALG shall attempt to verify that no intermediate entity has changed the codec information in the SDP offer since it was generated by the previous OMR-capable entity. If the IMS-ALG cannot verify that the codec information is unchanged, it shall remove all OMR specific SDP attributes from the SDP offer.

- Determine according to local policy if a TrGW is required in the user plane path for a purpose unrelated to transcoding or NAT, e.g., lawful intercept. Visited realm and secondary realm instances for previous user plane segments shall be removed to prevent subsequent signalling entities from bypassing the media resource.

- Based on the outgoing IP realm, IP realm accessibility from controlled TrGWs, and information from visited realm and secondary realm instances in the received SDP offer, the IMS-ALG shall determine whether to allocate a TrGW and whether one or more previous TrGWs can be bypassed. If transcoding is also supported, the IMS-ALG may also consider whether to modify the codec set, move the transcoding point, and which transcoding procedure to apply, if any.

- Allocate a TrGW and transcoder as necessary. If the IMS-ALG allocates a transcoder, it shall include information about the transcoding options in the visited realm instance for the outgoing realm.

- Optionally allocate one or more secondary TrGWs according to local policy.

- Forward the SDP offer after modifying the connection, port, codec, visited realm instances, and secondary realm instances as appropriate. If the IMS-ALG added a TrGW it shall:

  - Add a visited realm instance with the connection/port and IP realm on the the previous media path segment if no visited realm instances have been received and local policy allows potential bypass of the TrGW by subsequent entities.

  - Add a visited realm instance with the connection/port and IP realm on the the subsequent media path segment.

Upon receiving an initial SDP answer, the IMS-ALG in the signalling path shall perform the following for each media line:

- Based on the selected codec, connection information and IP realm instances in the SDP answer, and information from the received SDP offer, the IMS-ALG shall determine whether to deallocate any TrGW(s) and whether a second SDP offer/answer transaction is needed to send updated connection information towards the SDP answerer.

- Initiate and complete the second SDP offer/answer transaction if required.

- Determine how to modify the forwarded SDP answer to signal the bypass of previous TrGWs/transcoders, if any.

- Deallocate any unused TrGW/transcoder as necessary.

- Forward the modified SDP answer to signal other TrGW bypass decisions.

The end-to-end user plane path selected via the OMR procedures during the initial SDP offer-answer exchange should not be modified by subsequent SDP offer-answer exchanges, unless the new SDP offer-answer exchanges requires a new media path (e.g. transcoding, adding media, playing announcements).

NOTE: If the media path is changed, there is a risk of speech gaps and/or media drops during the media path switch.

Q.2.3 Common flows

Q.2.3.1 IMS-ALG allocates a TrGW

When an IMS-ALG allocates a TrGW during forwarding of an SDP offer without performing any media optimisations and is not bypassed during subsequent processing of the SDP answer, OMR has no impact on the standard call flow except for the addition of some SDP extension information to the SDP messages.

If an IMS-ALG does not support OMR then it will treat all OMR extension attributes as unrecognized SDP information.

If an IMS-ALG that does not support OMR inserts a TrGW in the media path and removes unrecognized OMR attributes from the SDP before forwarding, then the IMS-ALG will remove any OMR extension attributes from the forwarded SDP, thus effectively anchoring its TrGW in the media path and preventing further optimisation of the user plane segment prior to this point.

If an IMS-ALG that does not support OMR inserts a TrGW in the path without removing unrecognized OMR attributes, then the subsequent OMR-capable entity in the signalling path shall remove OMR extension attributes from the SDP offer before handling.

Q.2.3.2 IMS-ALG does not allocate a TrGW

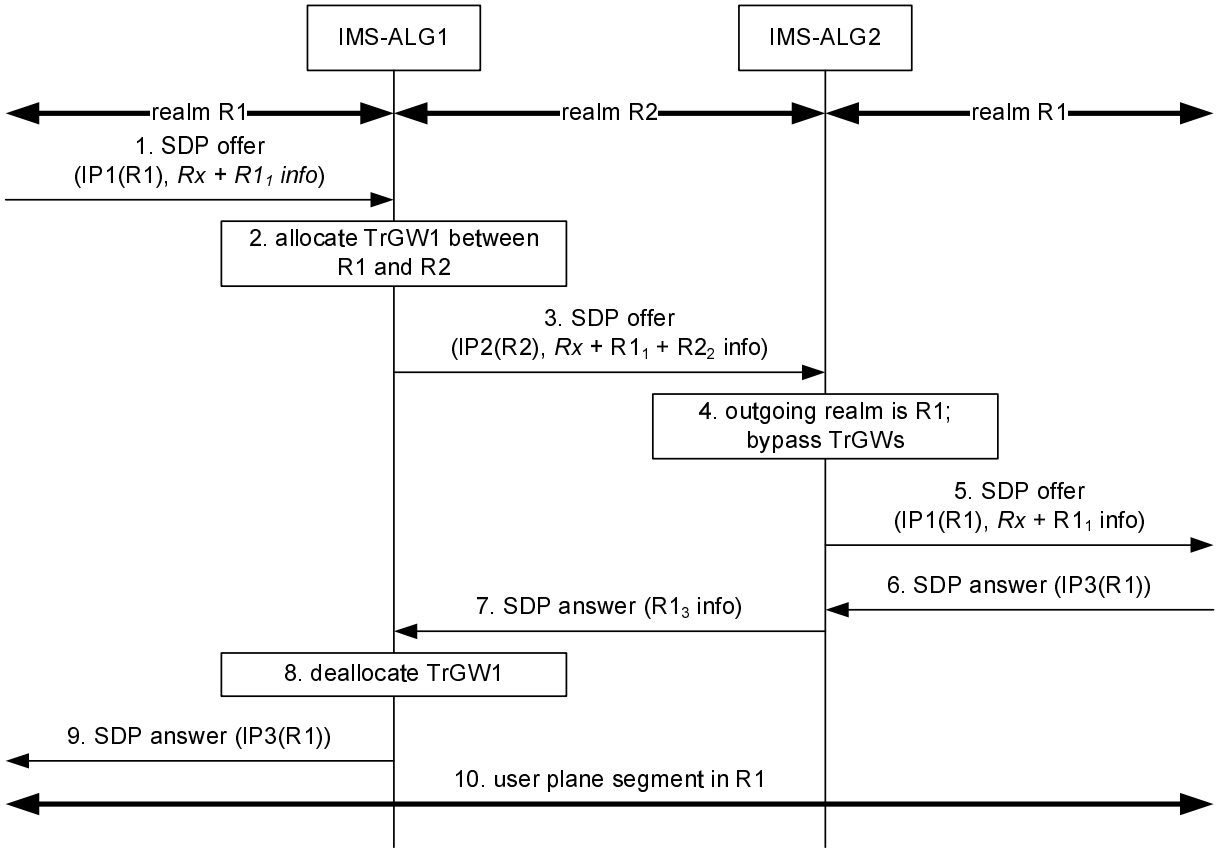
When an IMS-ALG does not allocate a TrGW during forwarding of an SDP offer and does not perform any media optimisations during processing of either the SDP offer or SDP answer, it transparently passes any SDP extensions for OMR in forwarded SDP messages. OMR has no impact on the standard call flow except for the addition of some SDP extension information to the SDP messages.

If an IMS-ALG that does not support OMR and does not allocate a TrGW upon receipt of an SDP offer transparently forwards the SDP offer, including unrecognized SDP attributes related to OMR, then it is possible for other OMR-compliant IMS-ALGs to perform user plane optimisations.

If an IMS-ALG that does not support OMR and does not allocate a TrGW upon receipt of an SDP offer removes unrecognized SDP attributes from the forwarded SDP offer, then further optimisation of the user plane segment prior to this point is not possible.

Q.2.3.3 IMS-ALG bypasses its TrGW and one or more prior TrGWs

Figure Q.1 applies when an IMS-ALG (IMS-ALG2) recognizes that it can avoid allocating a TrGW because an address for the outgoing IP realm is already available from a previous user plane segment. Thus it can bypass its own TrGW and one or more prior TrGWs. A common application of this scenario is when realm R1 is the internet and realm R2 is a private network isolated by the two IMS-ALGs. If no media resources are required within the network of realm R2 then there is no need to allocate TrGWs. IMS-ALG1 must initially allocate a TrGW since it does not know the ultimate destination of the SDP offer.



NOTE: Realm instances shown in *italics* in this and subsequent figures indicate their optionality. For example, an SDP offer from a UE will contain no realm instances.

Figure Q.1: IMS-ALG bypasses its TrGW and one or more prior TrGWs

1. IMS-ALG1 receives an SDP offer from realm R1. The SDP offer can include IP realm instances Rx associated with prior user plane segments and can include a visited realm instance for incoming realm R1. If realm instances are included in the received SDP offer, the IMS-ALG1 (and subsequent IMS-ALGs) verify that intermediate signalling entities have not modified the SDP.

2. IMS-ALG1 allocates TrGW1 to provide a NAT between R1 and R2.

3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with prior IP realm instance information Rx and visited realm instances for both the incoming and outgoing realms. IMS-ALG1 creates a new visited realm instance for the incoming realm if it was not present in the received SDP offer.

4. Since an IP address already exists within a visited realm instance for the outgoing realm R1, the IMS-ALG2 can avoid allocating a TrGW and can bypass a previous TrGW1.

5. IMS-ALG2 forwards connection information from the SDP offer in step 1 (IP1), which is valid in the outgoing realm R1. The forwarded SDP offer retains those IP realm instances that remain connected to the media path.

6. IMS-ALG2 receives an SDP answer with valid connection information (IP3) in realm R1.

7. IMS-ALG2 forwards the SDP answer to IMS-ALG1 after including an IP realm instance for the connection information from the SDP answer in step 6. The IP realm instance in the SDP answer identifies a corresponding realm instance from the SDP offer associated with the same IP realm, thus uniquely identifying the TrGWs to be bypassed. The connection information in the forwarded SDP answer cannot be used by the receiving IMS-ALG to establish this segment of the media path.

8. IMS-ALG1 de-allocates TrGW1 since there is no valid connection information available in the SDP answer for realm R2.

9. IMS-ALG1 forwards the SDP answer after modifying the connection information to correspond to the IP realm instance received in step 7.

10. A user plane connection is now established in realm R1 without the need to allocate any additional TrGWs.

Q.2.3.4 IMS-ALG bypasses its TrGW using secondary realm from prior IMS-ALG

Figure Q.2 applies when an IMS-ALG (IMS-ALG2) recognizes that it can avoid allocating a TrGW by using a secondary realm instance from a prior IMS-ALG.

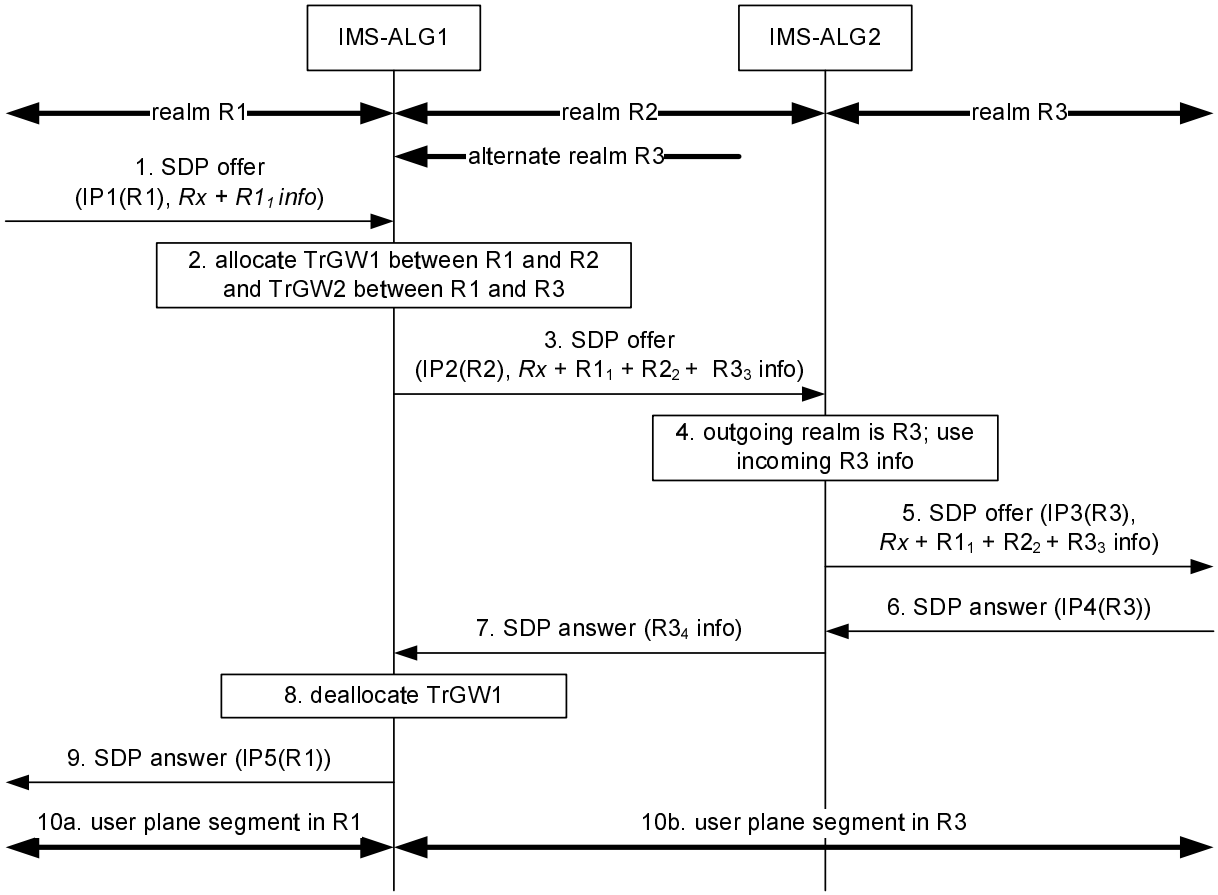


Figure Q.2: IMS-ALG bypasses its TrGW using secondary realm from prior IMS-ALG

1. IMS-ALG1 receives an SDP offer from realm R1. The SDP offer can include IP realm instances Rx associated with prior user plane segments and can include a visited realm instance for incoming realm R1.

2. IMS-ALG1 allocates TrGW1 to provide a NAT between R1 and R2. IMS-ALG1 also allocates TrGW2 to provide a NAT between R1 and alternate realm R3.

3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with prior IP realm instance information Rx, visited realm instances for both the incoming and outgoing realms R1 and R2, and a secondary realm instance for realm R3.

4. Since an IP address already exists within a secondary realm instance for the outgoing realm R3, the IMS-ALG2 can avoid allocating a TrGW.

5. IMS-ALG2 forwards the SDP offer with connection information from the secondary realm instance received in step 3 (IP3), which is valid in the outgoing realm R3. The forwarded SDP offer retains those IP realm instances that remain connected to the media path.

6. IMS-ALG2 receives an SDP answer with valid connection information (IP4) in realm R3.

7. IMS-ALG2 forwards the SDP answer to IMS-ALG1 after including an IP realm instance for the connection information from the SDP answer in step 6. The connection information in the forwarded SDP answer cannot be used by the receiving IMS-ALG to establish this segment of the media path.

8. IMS-ALG1 de-allocates TrGW1 since there is no valid connection information available in the SDP answer for realm R2. IMS-ALG1 retains TrGW2 to maintain the user plane connection via R3.

9. IMS-ALG1 forwards the SDP answer after modifying the connection information to correspond to the IP address of the TrGW2 in realm R1.

10. A user plane connection is now established with one segment in realm R1 and a second segment in realm R3, mediated by TrGW2.

Q.2.3.5 IMS-ALG bypasses one or more prior TrGWs using a secondary realm

Figure Q.3 applies when an IMS-ALG (IMS-ALG2) determines that it must allocate a TrGW under its control but can bypass previously allocated TrGWs by allocating a TrGW with access to an alternate realm (not the incoming one) associated with an earlier user plane segment.

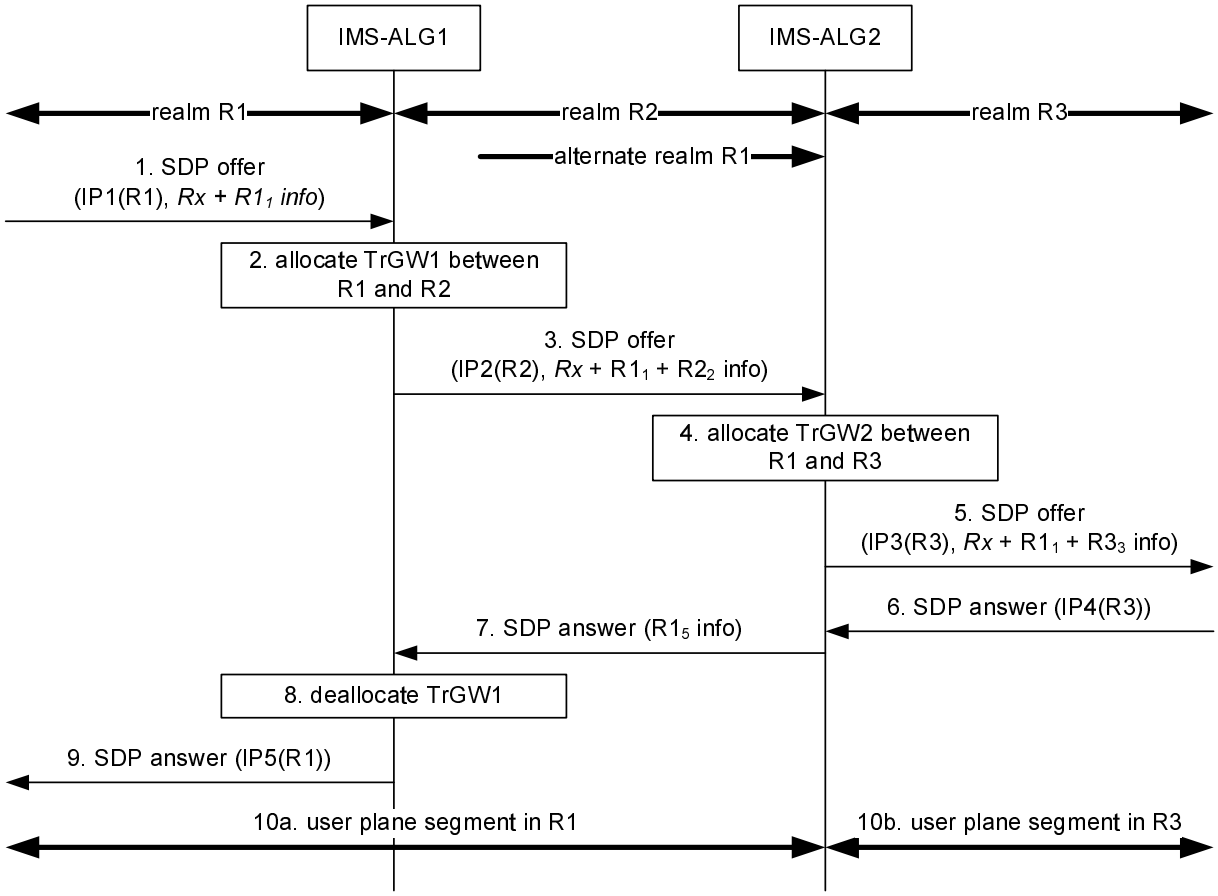


Figure Q.3: IMS-ALG bypasses one or more prior TrGWs using a secondary realm

1. IMS-ALG1 receives an SDP offer from realm R1. The SDP offer can include IP realm instances Rx associated with prior user plane segments and can include a visited realm instance for incoming realm R1.

2. IMS-ALG1 allocates TrGW1 to provide a NAT between R1 and R2.

3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with prior IP realm instance information Rx and visited realm instances for both the incoming and outgoing realms.

4. If IMS-ALG2 controls a TrGW (TrGW2) with access to realm R1, then IMS-ALG2 can use the visited realm instance for R1 to establish the incoming user plane segment, rather than using the connection information for TrGW1 from the received SDP offer in step 3. IMS-ALG2 allocates TrGW2 to provide a NAT between alternate realm R1 and realm R3.

5. IMS-ALG2 forwards the SDP offer with connection information for TrGW2 in realm R3 along with IP realm instances Rx and the visited realm instances for R1 and R3.
6. IMS-ALG2 receives an SDP answer with valid connection information (IP4) in realm R3.
7. IMS-ALG2 forwards the SDP answer to IMS-ALG1 after including an IP realm instance for the TrGW2 address in realm R1. The connection information in the forwarded SDP answer cannot be used by the receiving IMS-ALG to establish this segment of the media path.
8. IMS-ALG1 de-allocates TrGW1 since there is no valid connection information available in the SDP answer for realm R2.
9. IMS-ALG1 forwards the SDP answer after modifying the connection information to correspond to the IP address of the TrGW2 in realm R1.
10. A user plane connection is now established with one segment in realm R1 and a second segment in realm R3, mediated by TrGW2.

Q.2.3.6 IMS-ALG bypasses TrGWs performing NAT traversal

Figure Q.4 applies when an IMS-ALG (IMS-ALG2) that is performing NAT traversal for a terminating UA recognizes that the offering UA is in the same private realm behind a NAT, so that all TrGWs can be bypassed and a direct user plane connection established between the endpoints.

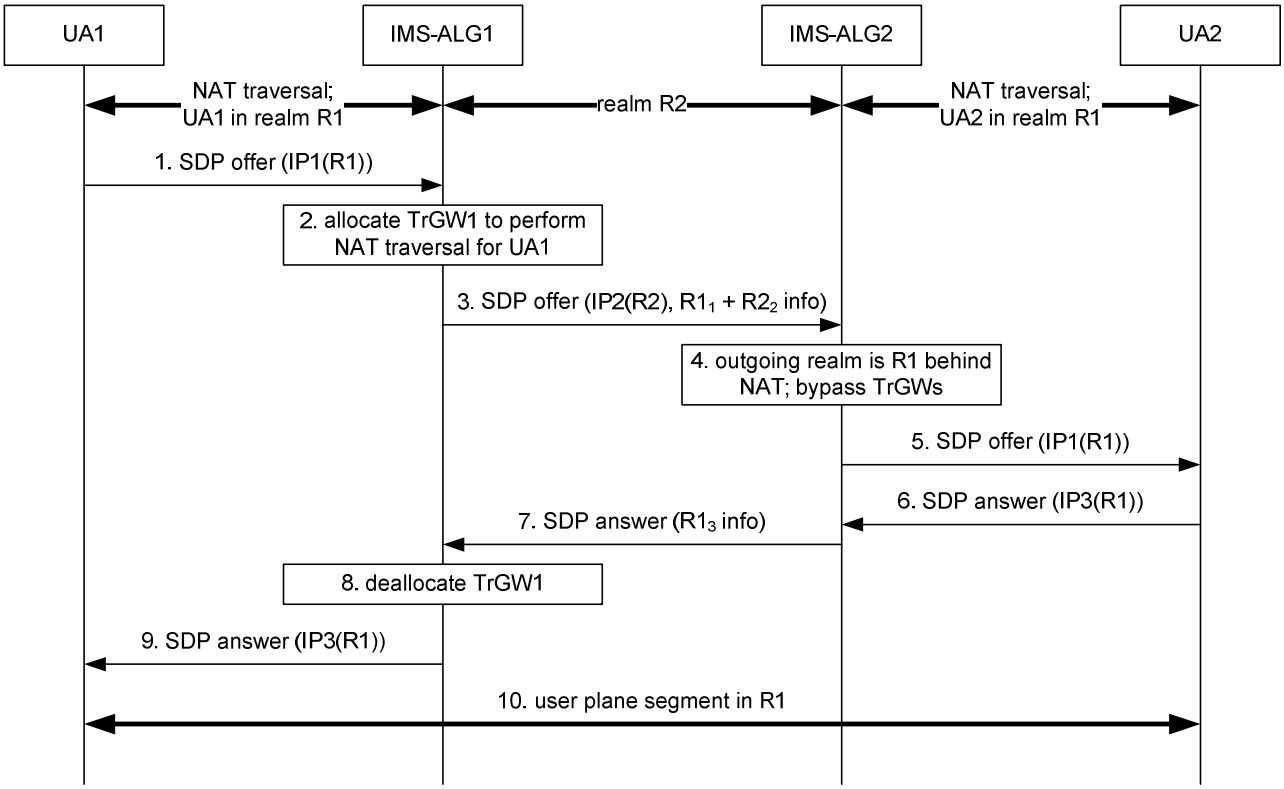


Figure Q.4: IMS-ALG bypasses TrGWs performing NAT traversal

1. IMS-ALG1 receives an SDP offer from UA1 in private realm R1 behind a NAT.
2. IMS-ALG1 allocates TrGW1 to provide NAT traversal between private realm R1 and realm R2. TrGW1 can only be bypassed if the answering UA2 is in the same private realm R1.
3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with visited realm instances for the private realm R1 for UA1, and the outgoing realm R2.
4. Since an IP address already exists within the visited realm instance for the private realm R1 for UA2, the IMS-ALG2 can avoid allocating a TrGW and can bypass a previous TrGW1.

5. IMS-ALG2 forwards connection information from the SDP offer in step 1 (IP1), which is valid in the outgoing private realm R1 behind the NAT.
6. IMS-ALG2 receives an SDP answer with valid connection information (IP3) in realm R1.
7. IMS-ALG2 forwards the SDP answer to IMS-ALG1 after including an IP realm instance for the connection information from the SDP answer in step 6. The connection information in the forwarded SDP answer cannot be used by the receiving IMS-ALG to establish this segment of the media path.
8. IMS-ALG1 de-allocates TrGW1 since there is no valid connection information available in the SDP answer for realm R2.
9. IMS-ALG1 forwards the SDP answer after modifying the connection information to correspond to the IP realm instance received in step 7.
10. A user plane connection is now established in realm R1 without the need to allocate any TrGWs.

Q.2.5 Flows with transcoding

Q.2.5.1 Proactive transcoding where transcoding is required

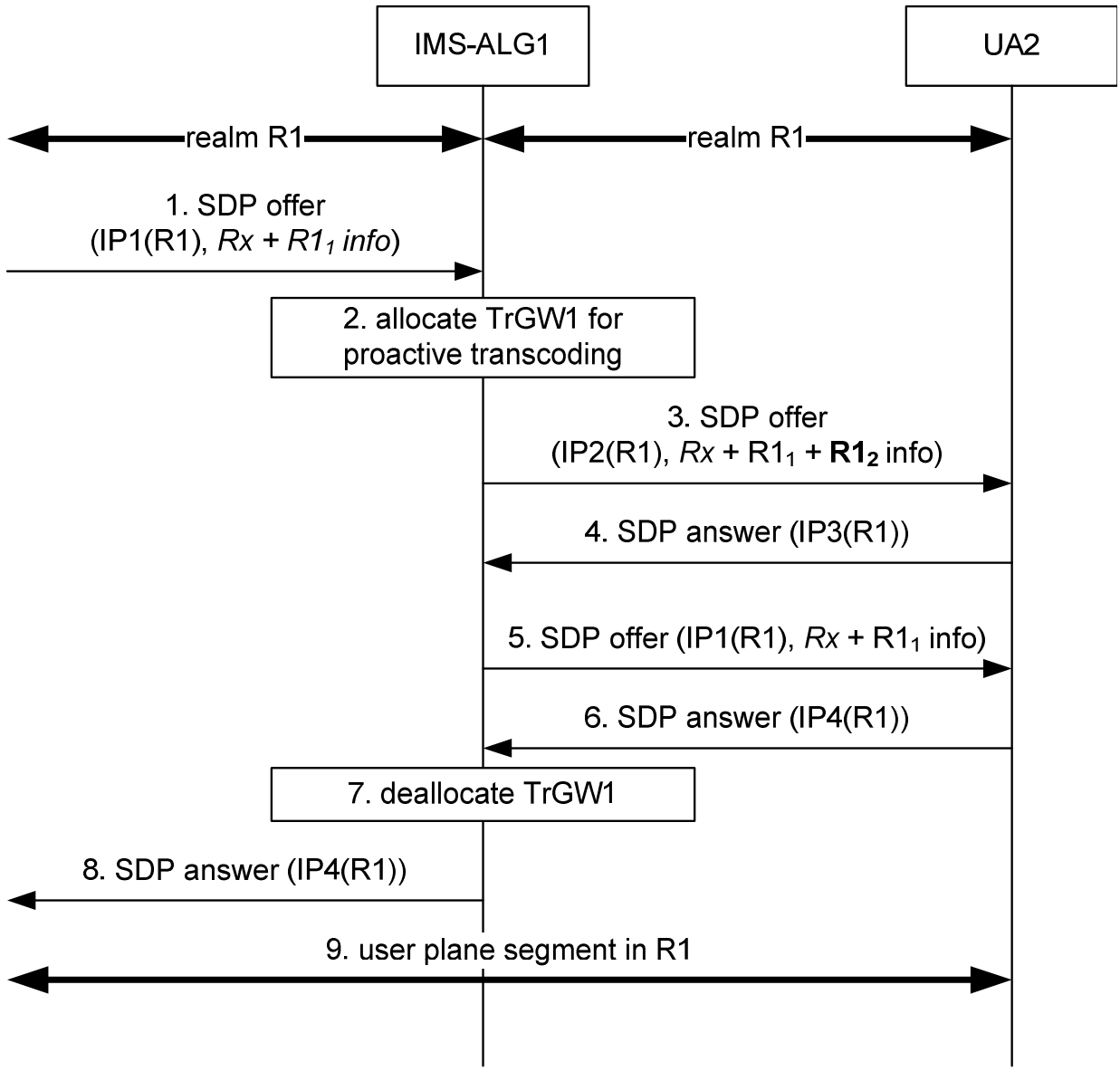
When an IMS-ALG supporting OMR allocates a TrGW during forwarding of the SDP offer for proactive transcoding with resource reservation, if subsequent IMS-ALGs do not replace the transcoder and the answering side signals in the SDP answer that transcoding is required, then the IMS-ALG retains the TrGW for transcoding and anchors it in the user plane path. The call flow is the same as the usual call flow for TrGW insertion except for the addition of some SDP extension information to the SDP messages.

Q.2.5.2 Proactive transcoding where transcoding not required

Figure Q.5 applies when IMS-ALG1 allocates a TrGW during forwarding of the SDP offer for proactive transcoding with resource reservation, IMS-ALG1 is the last signalling entity on the path before UA2, and UA2 signals in the SDP answer that transcoding is not required. UA2 ignores unrecognized OMR extension attributes.

A second SDP offer/answer transaction is required to remove the transcoder from the path.

As an alternative to the procedure shown, the IMS-ALG1 may forward connection information for a prior user plane segment without transcoding options while including an IP realm instance for the transcoding TrGW. This alternative avoids a second SDP offer/answer transaction if transcoding is not required, but does include a second SDP offer/answer transaction if transcoding is required.



NOTE: Realm instances shown in **bold** in this and subsequent figures include codec change information.

Figure Q.5: Proactive transcoding where transcoding not required

1. IMS-ALG1 receives an SDP offer from realm R1. The SDP offer can include IP realm instances Rx associated with prior user plane segments and can include a visited realm instance for incoming realm R1. The realm instances in this and other messages in the figure are shown in italics to indicate their optionality. For example, an SDP offer from a UE will contain no realm instances. If realm instances are included in the received SDP offer, the IMS-ALG1 (and subsequent IMS-ALGs) verify that intermediate signalling entities have not modified the SDP.

2. IMS-ALG1 allocates TrGW1 to offer transcoding options to UA2.

3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with prior IP realm instance information Rx and visited realm instances for both its incoming and outgoing user plane segments. IMS-ALG1 creates a new visited realm instance for the incoming realm if it was not present in the received SDP offer. The visited realm instance for the outgoing side includes information about the codec changes associated with TrGW1.

4. UA2 selects one of the original codecs, i.e., transcoding is not needed. In response to the SDP offer, UA2 sends an SDP answer to IMS-ALG1 with connection information for its address in realm R1.

5. IMS-ALG1 determines that the transcoder is not needed and forwards a second SDP offer to UA2 with connection information from a prior realm. This SDP offer includes those IP realm instances that remain options without transcoding.
6. UA2 updates its remote connection information and responds with a new SDP answer.
7. IMS-ALG1 de-allocates TrGW1.
8. IMS-ALG1 forwards the SDP answer with connection information for UA2 in realm R1.
9. A user plane connection is now established in realm R1 without use of any TrGWs.

Q.2.5.3 IMS-ALG bypasses prior unrequired proactive transcoder

Figure Q.6 applies when IMS-ALG1 allocates a TrGW during forwarding of the SDP offer for proactive transcoding with resource reservation, another IMS-ALG (IMS-ALG2) is the last signalling entity on the path before UA2, IMS-ALG2 must allocate a TrGW to provide NAT, and UA2 signals in the SDP answer that transcoding is not required. There may be additional IMS-ALGs between IMS-ALG1 and IMS-ALG2.

This scenario avoids the need for a second SDP offer/answer transaction as required in clause Q.2.5.3 and clause Q.2.5.5. IMS-ALG2 signals to IMS-ALG1 in the SDP answer to bypass the transcoder.

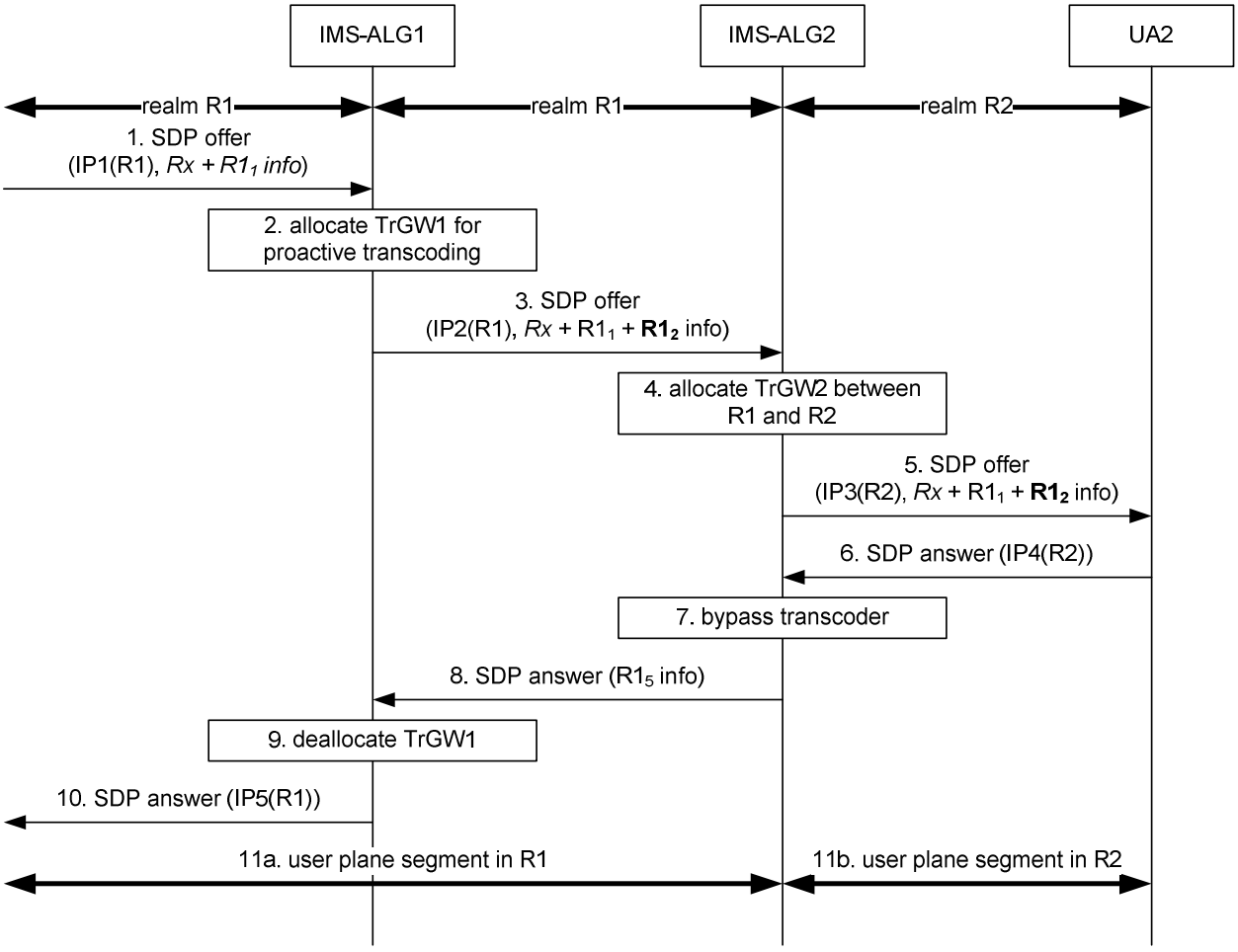


Figure Q.6: IMS-ALG bypasses prior unrequired proactive transcoder

1. IMS-ALG1 receives an SDP offer from realm R1. The SDP offer can include IP realm instances Rx associated with prior user plane segments and can include a visited realm instance for incoming realm R1.
2. IMS-ALG1 allocates TrGW1 to offer transcoding options to UA2.

3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with prior IP realm instance information Rx and visited realm instances for both its incoming and outgoing user plane segments. The visited realm instance for the outgoing side includes information about the codec changes associated with TrGW1.

4. IMS-ALG2 allocates TrGW2 to provide a NAT between R1 and R2.

5. IMS-ALG2 forwards the SDP offer with connection information for TrGW2 in realm R2 along with IP realm instances for prior user plane segments.

6. UA2 selects one of the original codecs, i.e., transcoding is not needed. In response to the SDP offer, UA2 sends an SDP answer to IMS-ALG2 with connection information for its address in realm R2.

7. IMS-ALG2 determines that transcoding is not necessary.

8. IMS-ALG2 forwards the SDP answer to IMS-ALG1 after including an IP realm instance for the TrGW2 address in realm R1. The connection information in the forwarded SDP answer cannot be used by the receiving IMS-ALG to establish this segment of the media path.

9. IMS-ALG1 de-allocates transcoder TrGW1 since there is no valid connection information available in the SDP answer.

10. IMS-ALG1 forwards the SDP answer after modifying the connection information to correspond to the IP address of the TrGW2 in realm R1.

11. A user plane connection is now established with one segment in realm R1 and a second segment in realm R2, mediated by TrGW2.

Q.2.5.4 IMS-ALG bypasses its TrGW and prior unrequired proactive transcoder

Figure Q.7 applies when IMS-ALG1 allocates a TrGW during forwarding of the SDP offer for proactive transcoding with resource reservation, another IMS-ALG (IMS-ALG2) is the last signalling entity on the path before UA2, IMS-ALG2 does not need to allocate a TrGW to provide NAT, and UA2 signals in the SDP answer that transcoding is not required. There may be additional IMS-ALGs between IMS-ALG1 and IMS-ALG2.

A second SDP offer/answer transaction is required to remove the transcoder from the path. The scenario allows IMS-ALG2 to initiate the second SDP offer/answer transaction rather than requiring IMS-ALG1 to do this, thus saving some messaging.

As an alternative to the procedure shown, the IMS-ALG1 may forward connection information for a prior user plane segment without transcoding options while including an IP realm instance for the transcoding TrGW. This alternative avoids a second SDP offer/answer transaction if transcoding is not required, but does include a second SDP offer/answer transaction if transcoding is required.

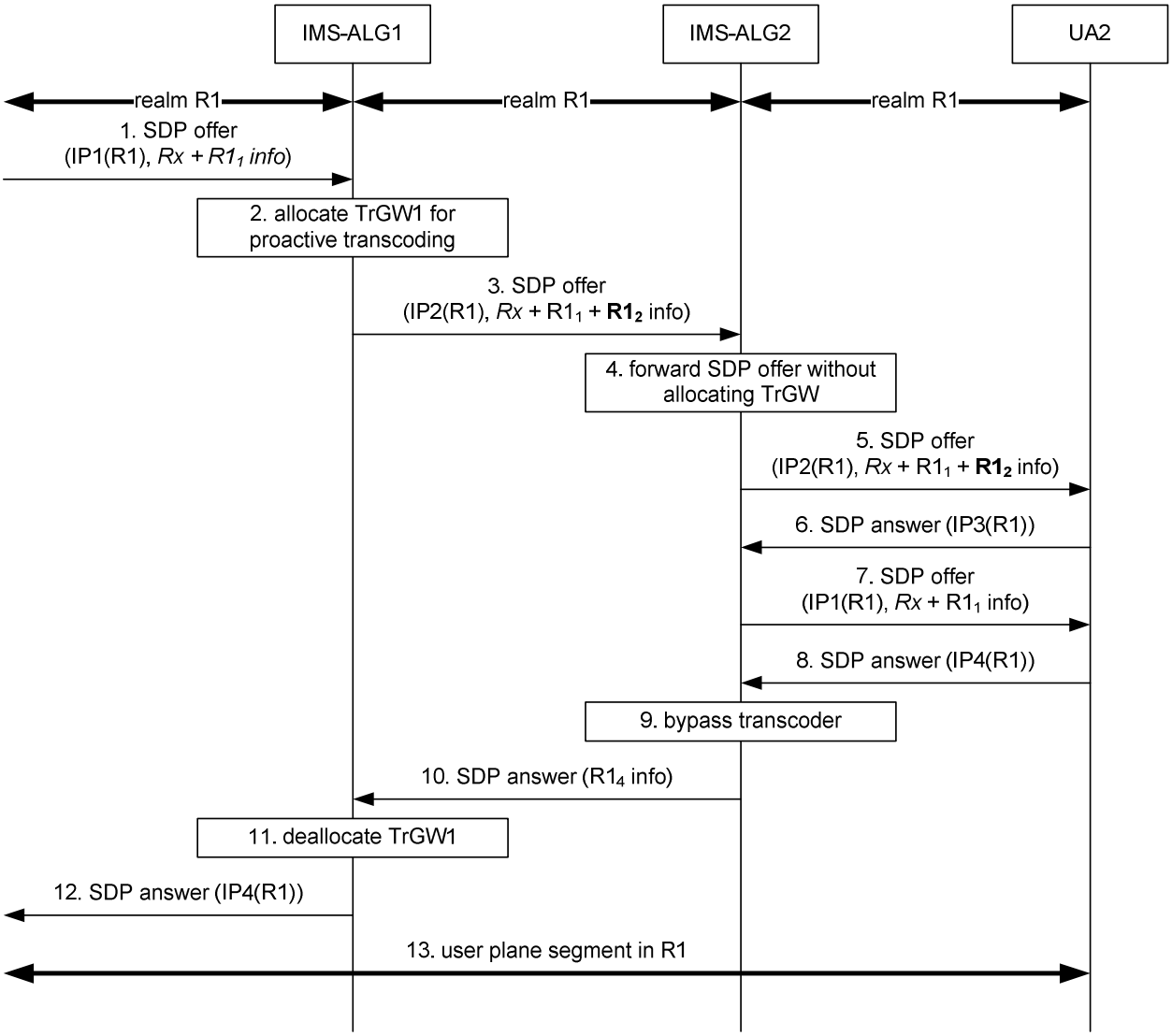


Figure Q.7: IMS-ALG bypasses its TrGW and prior unrequired proactive transcoder

1. IMS-ALG1 receives an SDP offer from realm R1. The SDP offer can include IP realm instances Rx associated with prior user plane segments and can include a visited realm instance for incoming realm R1.
2. IMS-ALG1 allocates TrGW1 to offer transcoding options to UA2.
3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with prior IP realm instance information Rx and visited realm instances for both its incoming and outgoing user plane segments. The visited realm instance for the outgoing side includes information about the codec changes associated with TrGW1.
4. IMS-ALG2 does not allocate a TrGW since its incoming and outgoing realms are compatible.
5. IMS-ALG2 forwards the SDP offer with no changes.
6. UA2 selects one of the original codecs, i.e., transcoding is not needed. In response to the SDP offer, UA2 sends an SDP answer to IMS-ALG2 with connection information for its address in realm R1.
7. IMS-ALG2 determines that transcoding is not necessary and sends a second SDP offer with the connection information from the visited realm instance for a prior user plane segment. This SDP offer includes those IP realm instances that remain options without transcoding.
8. UA2 updates its remote connection information and responds with a new SDP answer.
9. IMS-ALG2 determines that the prior transcoder is to be bypassed.

10. IMS-ALG2 forwards the SDP answer to IMS-ALG1 after including an IP realm instance for the UA2 address in realm R1. The connection information in the forwarded SDP answer cannot be used by the receiving IMS-ALG to establish this segment of the media path.

11. IMS-ALG1 de-allocates transcoder TrGW1 since there is no valid connection information available in the SDP answer.

12. IMS-ALG1 forwards the SDP answer after modifying the connection information to correspond to the IP address of UA2 in realm R1.

13. A user plane connection is now established in realm R1.

Q.2.5.5 IMS-ALG replaces prior proactive transcoder

Figure Q.8 applies when IMS-ALG1 allocates a TrGW during forwarding of the SDP offer for proactive transcoding with resource reservation, and a later IMS-ALG (IMS-ALG2) chooses to bypass the transcoding offered by IMS-ALG1 and optionally offer its own transcoding options. There may be additional IMS-ALGs between IMS-ALG1 and IMS-ALG2.

The flow assumes that TrGW2 must remain to providing transcoding or NAT. The call flow variant if TrGW2 is not needed can be derived by combining this flow with one of the other transcoding flows.

An IMS-ALG may remove codec options, or re-instate codec options removed by a previous IMS-ALG by bypassing that IMS-ALG's TrGW if allocated. The call flow continues to apply except that TrGW allocation is optional.

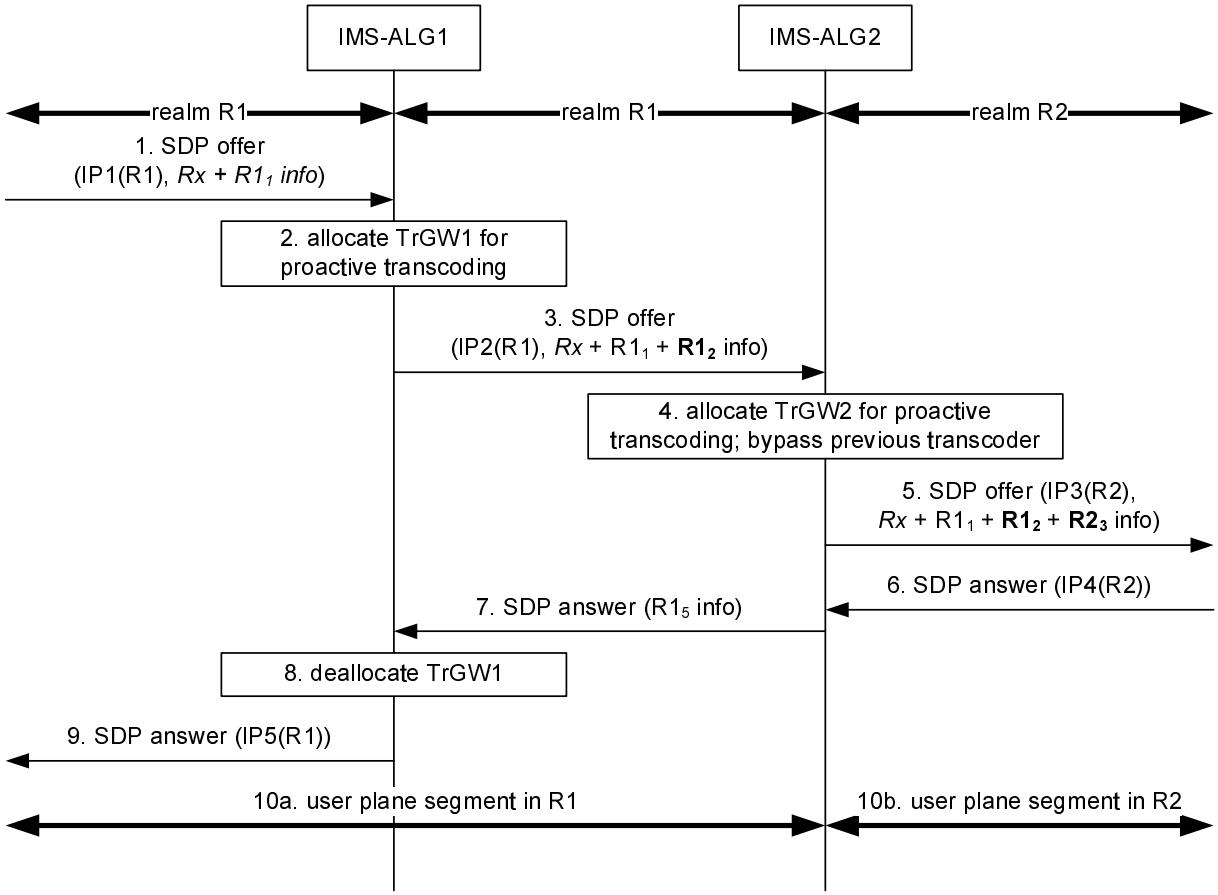


Figure Q.8: IMS-ALG replaces prior proactive transcoder

1. IMS-ALG1 receives an SDP offer from realm R1. The SDP offer can include IP realm instances Rx associated with prior user plane segments and can include a visited realm instance for incoming realm R1.

2. IMS-ALG1 allocates TrGW1 to offer transcoding options to UA2.

3. IMS-ALG1 forwards connection information for TrGW1 in the SDP offer along with prior IP realm instance information Rx and visited realm instances for both its incoming and outgoing user plane segments. The visited realm instance for the outgoing side includes information about the codec changes associated with TrGW1.
4. IMS-ALG2 bypasses the prior transcoder and allocates TrGW2 to provide alternate transcoding options to UA2.
5. IMS-ALG2 forwards the SDP offer with connection information for TrGW2 in realm R2 along with IP realm instances associated with all user plane segments. The forwarded SDP offer includes information about all potential transcoders so that a subsequent entity has the option to choose the earlier one if appropriate.
6. IMS-ALG2 receives an SDP answer with connection information for a valid address in realm R2.
7. IMS-ALG2 forwards the SDP answer to IMS-ALG1 after including an IP realm instance for the TrGW2 address in realm R1. The connection information in the forwarded SDP answer cannot be used by the receiving IMS-ALG to establish this segment of the media path.
8. IMS-ALG1 de-allocates transcoder TrGW1 since there is no valid connection information available in the SDP answer.
9. IMS-ALG1 forwards the SDP answer after modifying the connection information to correspond to the IP address of the TrGW2 in realm R1.
10. A user plane connection is now established with one segment in realm R1 and a second segment in realm R2, mediated by TrGW2.

Q.2.5.6 Proactive transcoding without resource reservation

An IMS-ALG performing proactive transcoding without resource reservation provides an indication in the forwarded SDP that an address is unavailable if transcoding is selected. Subsequent IMS-ALGs can replace this transcoder when forwarding the SDP offer according to the procedure in clause Q.2.5.6, but cannot insert a transcoding TrGW on behalf of the IMS-ALG performing proactive transcoding if needed. Thus the procedures in clause Q.2.5.4 and clause Q.2.5.5 do not apply. If transcoding is required, the IMS-ALG performs a procedure very similar to clause Q.2.5.3 to allocate the transcoding TrGW and signal its address to the answering side.

Q.2.5.7 Reactive transcoding

An IMS-ALG performing reactive transcoding follows all OMR procedures when forwarding the initial SDP offer but does not allocate a transcoder. If the initial SDP offer is rejected due to lack of support for an offered codec, the IMS-ALG performing reactive transcoding will restart the OMR procedure with the answering side after allocating and anchoring a TrGW with transcoding. The IMS-ALG removes all prior visited realm and secondary realm instances from the SDP offer before forwarding.

Q.3 Charging

Charging records shall include sufficient information to capture the allocation and/or bypass of TrGWs in the media path of an IMS session. If required by local configuration, charging records shall indicate whether the resulting user plane connection on either the incoming or outgoing leg of the IMS session traverses an IP realm different from its default IP realm (the IP realm traversed without OMR). If required by local configuration, charging records shall indicate whether a transcoder is inserted by the IMS-ALG.

Annex R (informative): Distribution of Network Provided Location Information within IMS

R.1 General

This annex describes how the user location and/or UE Time Zone information can be further distributed to IMS entities once it has been retrieved by either P-CSCF or an IMS AS. The exact mechanism for how the user location and/or UE Time Zone information are obtained is not described in this annex.

Information related to the location of the user provided by the access network may be required in IMS in order to comply with regulatory requirements (e.g. data retention, lawful interception) and/or in order to enable certain types of added value services based on the user's location.

To simplify the infomation flows, the IMS AS shown in the figures can represent several AS's. The CSCF represents the I-CSCF and/or the S-CSCF.

For the P-CSCF case in the originating side, the P-CSCF can, depending on operator policy, retrieve the user location and/or UE Time Zone information either before sending the INVITE towards the terminating side or upon reception of the SDP answer from the terminating side.

The transfer of the user location and/or UE Time Zone information within IMS signalling does not affect the transfer of any UE provided user location information. User location and/or UE Time Zone information provided in the signaling by the network will be distinguished from user location information provided by the UE.

R.2 Session Establishment/Modification at Mobile Origination - Location Info in Request

This information flow shows the procedure when operator policy requires the the user location and/or UE Time Zone information to be included within IMS session establishment/modification signalling before sending the INVITE towards the terminating side.

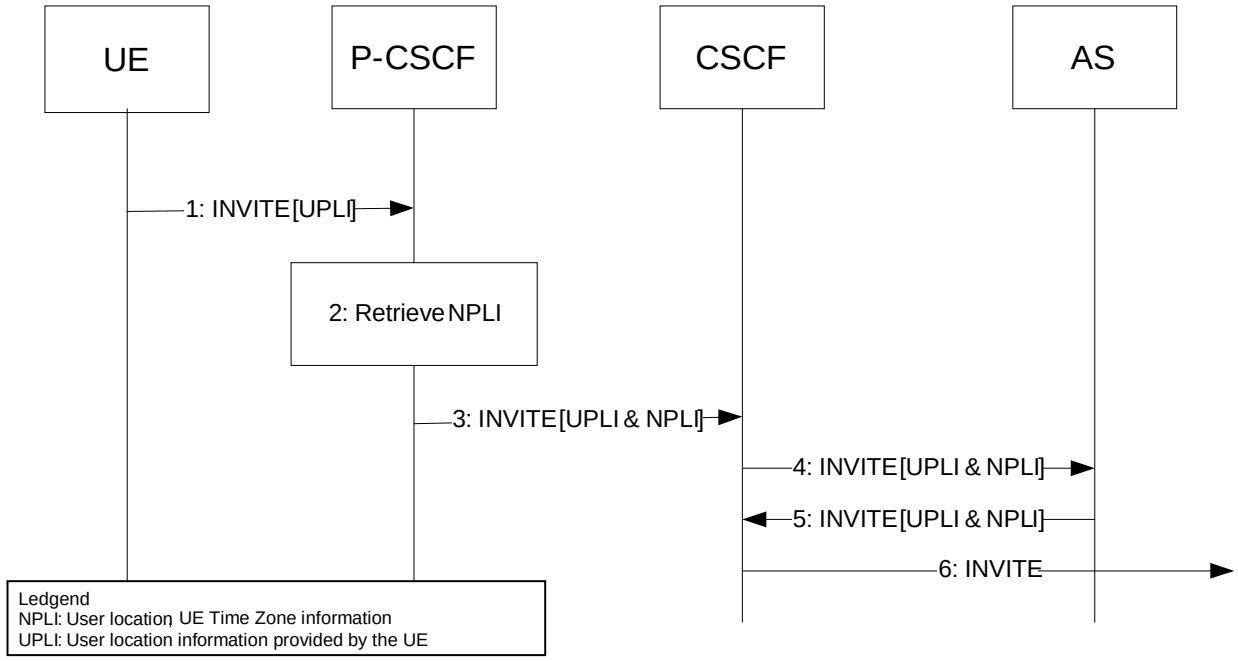


Figure R.2 -1: Mobile origination (user location and/or UE Time Zone information included within INVITE)

1. The UE sends a SIP INVITE request. It can contain user location information provided by the UE.
2. The P-CSCF obtains the user location and/or UE Time Zone information from the access network.
3. The P-CSCF includes the user location and/or UE Time Zone information obtained from the access network and sends the INVITE towards the next hop together with the user location information provided by the UE.
4. If an AS is to be invoked for this session, the S-CSCF (or I-CSCF) sends the INVITE towards the AS, including the user location and/or UE Time Zone information (assuming the AS is in the same trust domain).
5. The AS sends the INVITE towards the S-CSCF, still containing the user location and/or UE Time Zone information.
6. The S-CSCF routes the INVITE towards the terminating side. The user location and/or UE Time Zone information may be removed or modified (e.g. to change location granularity to just indicate the serving PLMN) before routing outside the trust domain.

R.3 Session Establishment/Modification at Mobile Origination - Location Info in Response

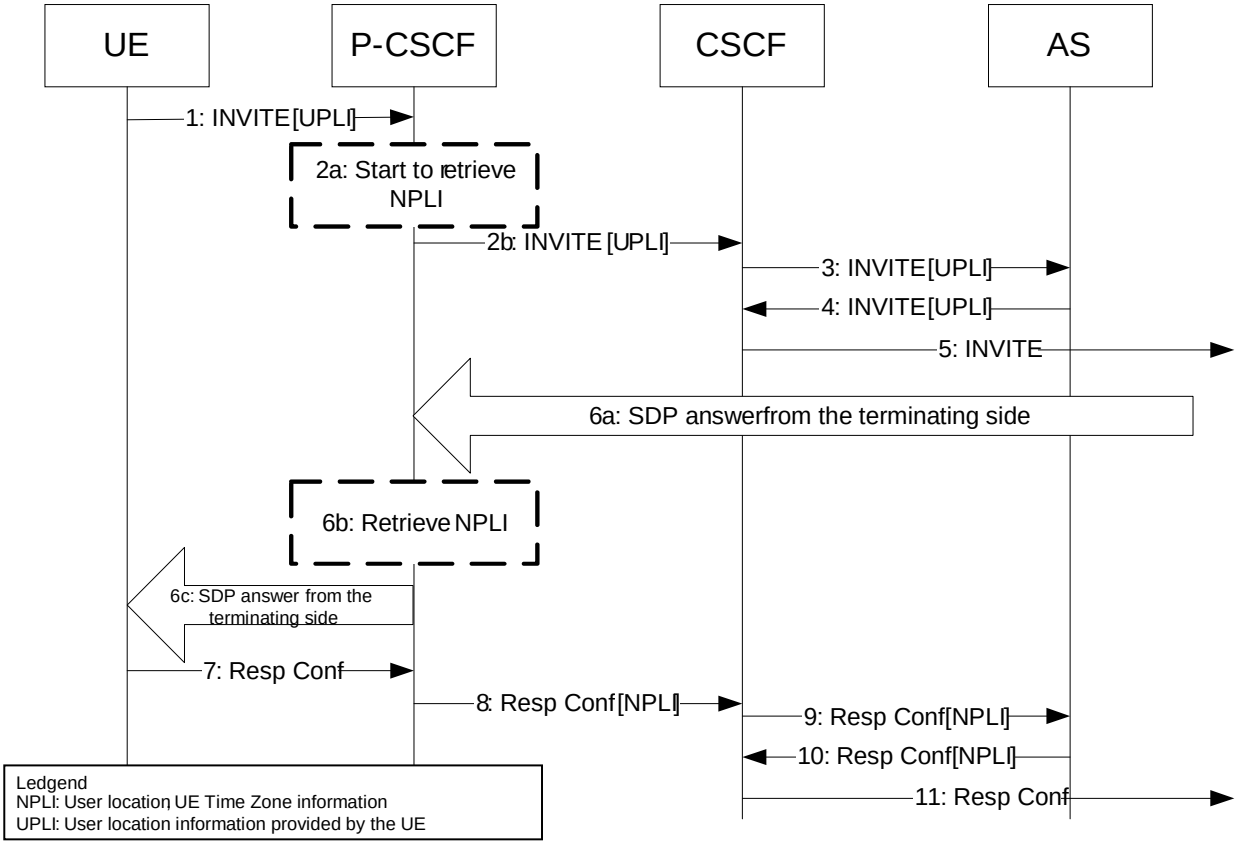


Figure R.3-1: Mobile origination (user location and/or UE Time Zone information included within Response Confirmation)

1. The UE sends a SIP INVITE request. It can contain user location information provided by the UE.

2a. Optionally, the P-CSCF may start procedures to obtain the user location and/or UE Time Zone information from the access network at reception of SDP Offer in parallel with steps 2b to 7.

2b. The P-CSCF sends the INVITE towards the next hop.

3. If an AS is to be invoked for this session the S-CSCF (or I-CSCF) sends the INVITE towards the AS.

4. The AS sends the INVITE towards the S-CSCF.

5. The S-CSCF routes the INVITE towards the terminating side.

6a. The P-CSCF receives an SDP answer sent by the terminating side.

6b. If the P-CSCF did not initiate procedures to obtain the user location and/or UE Time Zone information from the access network at step 2a, it will initiate them. This step will be executed together with Authorization of QoS resources.

6c. The P-CSCF forwards the SDP answer to the UE.

7. The UE provides a response confirmation towards the P-CSCF.

8. The P-CSCF inserts the user location and/or UE Time Zone information provided by the access network in the response confirmation, and this is routed towards the terminating side in steps 9 - 11. The user location and/or

UE Time Zone information may be removed or modified (e.g. to change location granularity to just indicate the serving PLMN) before routing outside the trust domain.

R.4 Session Establishment/Modification at Mobile Termination

This information flow shows the procedure when operator policy requires the user location and/or UE Time Zone information from the access network to be included within IMS session establishment/modification signalling before sending the response towards the originating side.

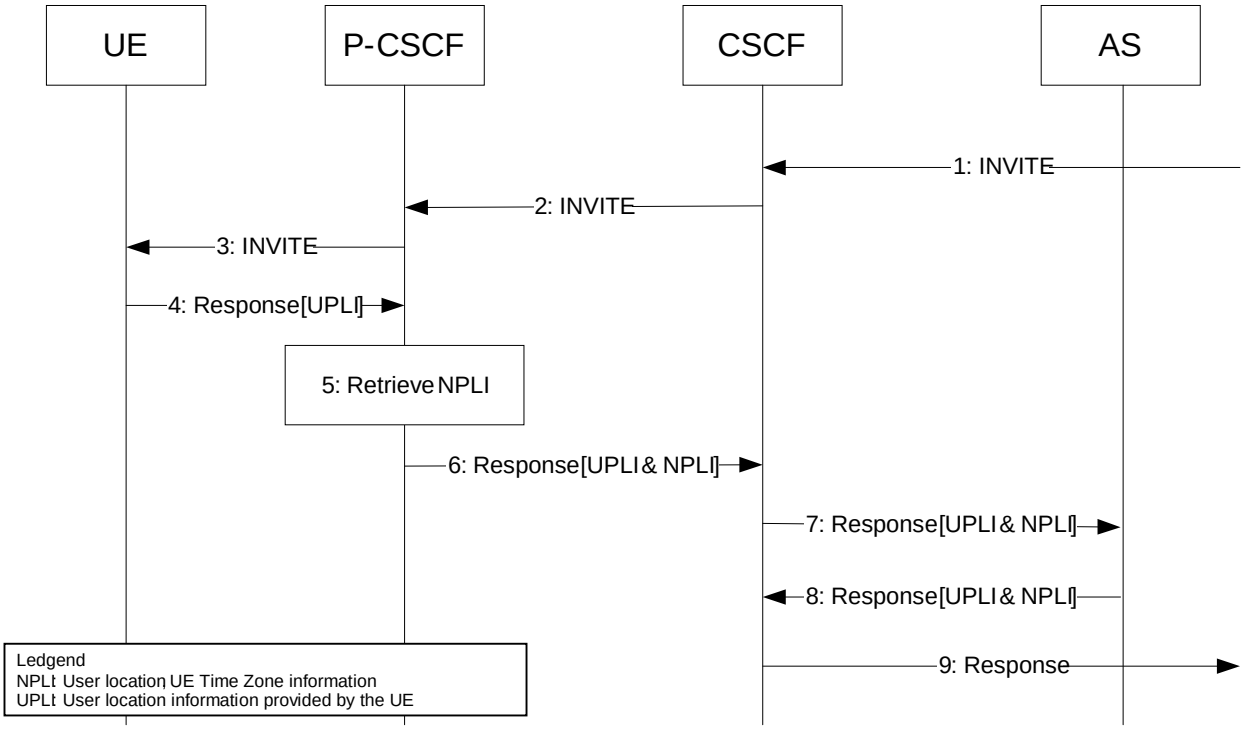


Figure R.4-1: Mobile termination

1. The CSCF receives an incoming INVITE.
2. The CSCF send the INVITE to the P-CSCF.
3. The P-CSCF sends the INVITE to the UE.
4. The UE sends a response to the INVITE (the response can be either a provisional or final response). This can contain user location information provided by the UE.
5. The P-CSCF invokes procedures to obtain user location and/or UE Time Zone information from the access network. This step will be executed together with Authorization of QoS resources. In some scenarios, it might be possible to obtain or at least initiate the fetching of user location and/or UE Time Zone information already at step 3.
6. The P-CSCF adds the user location and/or UE Time Zone information obtained from the access network and sends the response towards the next CSCF, together with the user location information provided by the UE (if available).

7-9. The response is routed towards the originating party. The user location and/or UE Time Zone information may be removed or modified (e.g. to change location granularity to just indicate the serving PLMN) before routing outside the trust domain.

R.5 Session Establishment/Modification - Location Information Distributed by IMS AS

The call flow in this clause describes the procedures to distribute user location and/or UE Time Zone information provided by the network within IMS session establishment/modification signalling when the retrieval of user location and/or UE Time Zone information is performed by an IMS AS.

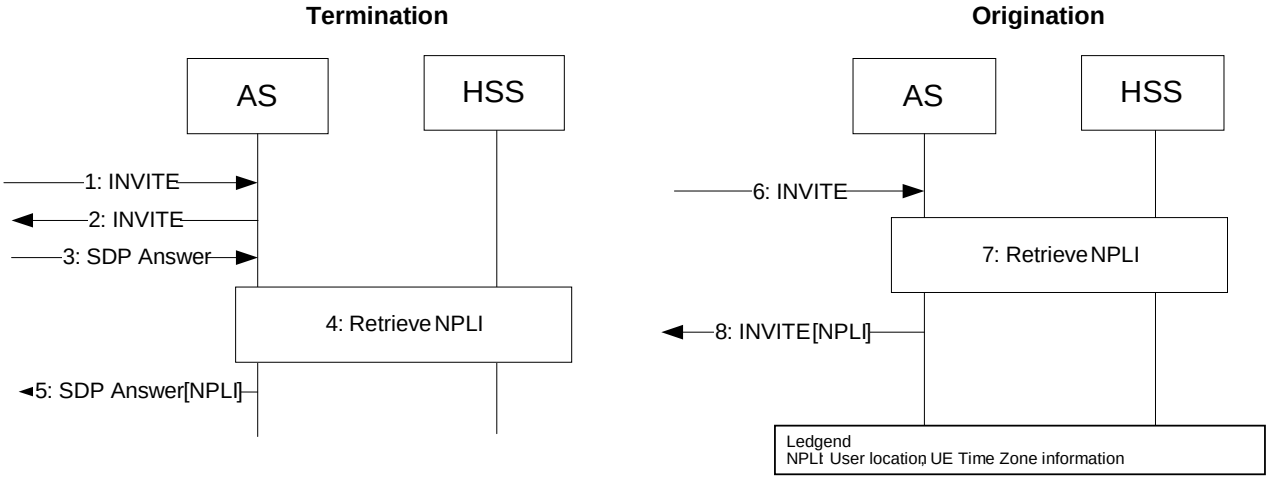


Figure R.5-1: User location and/or UE Time Zone information Distribution by an IMS AS

Terminating Side:

1. A SIP INVITE request is received bv an AS.
2. The INVITE is processed by the AS and returned to the S-CSCF.

NOTE 1: If the AS requires user location and/or UE Time Zone information for the service execution as such, the user location and/or UE Time Zone information can be fetched prior sending the INVITE to the next hop.

3. The SDP Answer is received by the AS.
4. The AS retrieves user location and/or UE Time Zone information from the access network via the HSS.

   The HSS retrieves the requested information from the Access Network

   The HSS/UDM may not be aware whether the UE is currently camping on 3GPP or Non 3GPP access and may need to request Location Information from the AMF, the MME, the SGSN and from the TWAN (via the AAA server in this last case).

   The HSS provides the AS with the requested information. When the HSS has received multiple user location (from multiple access: 3GPP and non 3GPP), the HSS provides the AS with the most recent user location.

5. The AS includes the user location and/or UE Time Zone information obtained from the access network via the HSS and sends the SDP answer towards the S-CSCF.

NOTE 2: The S-CSCF may further distribute user location and/or UE Time Zone information to other ASs within the trust domain.

Originating Side:

6. A SIP INVITE request is received by an AS.
7. The AS retrieves user location and/or UE Time Zone information from the access network via the HSS. The same procedures as described in steps 4a and 4b above apply.

8. The AS includes the user location and/or UE Time Zone information obtained from the access network via the HSS and sends the INVITE towards the S-CSCF.

NOTE 3: The S-CSCF can further distribute user location and/or UE Time Zone information to other ASs within the trust domain. The S-CSCF does not distribute the user location and/or UE Time Zone information to the P-CSCF.

R.6 Session Release

The call flows in this clause present the mobile or network initiated IMS session release for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side valid when either P-CSCF or an IMS AS retrieve user location and/or UE Time Zone information from the access network.

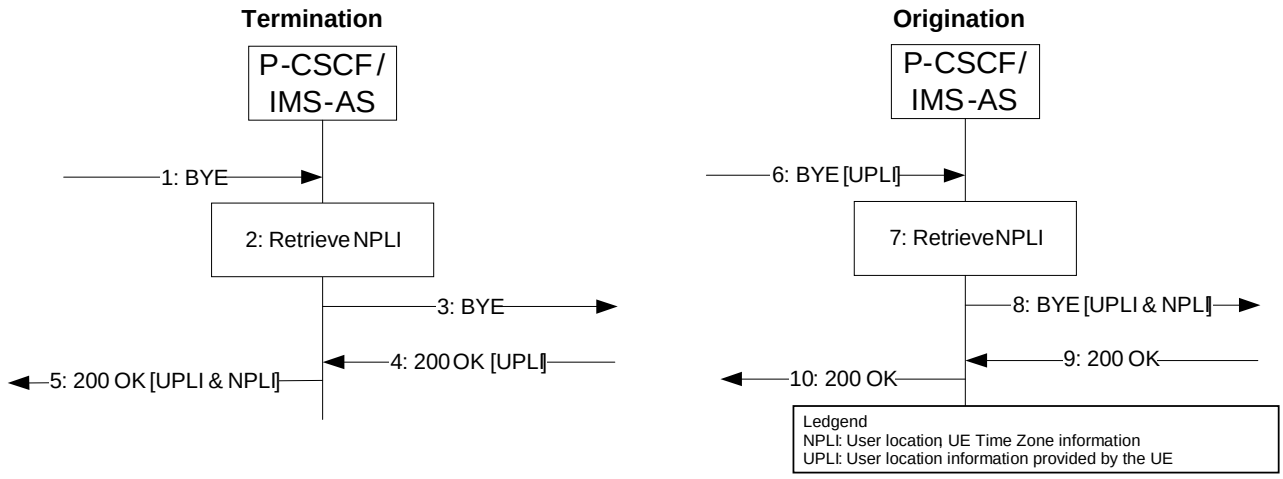


Figure R.6-1: IMS Session Release

Terminating Side:

1. A session release message which terminates the dialog, e.g., BYE, is received by the P-CSCF/IMS AS.
2. The P-CSCF/IMS AS invokes procedures to obtain the user location and/or UE Time Zone information from the access network. In the P-CSCF, this step will be executed together with the procedure to release corresponding QoS resources in the IP-CAN.
3. The P-CSCF/IMS AS forwards the BYE message to the UE or the S-CSCF respectively.
4. The UE/S-CSCF provides a response to the P-CSCF/IMS AS.
5. The P-CSCF/IMS AS inserts the user location and/or UE Time Zone information in the response confirmation, and this is routed towards IMS Core.

Originating Side:

6. A session release message which terminates the dialog, e.g. BYE, is received by the P-CSCF/IMS AS.
7. The P-CSCF/IMS AS invokes procedures to obtain the user location and/or UE Time Zone information from the access network. In the P-CSCF, this step will be executed together with the procedure to release corresponding QoS resources in the IP-CAN.
8. The P-CSCF/IMS AS forwards the BYE message within IMS Core containing the user location and/or UE Time Zone information together with the user location information provided by the UE. The user location and/or UE Time Zone information may be removed or modified (e.g. to change location granularity to just indicate the serving PLMN) if routing outside the trust domain is needed.

9-10. The Session Release procedure is completed.

Annex S (normative): Business Trunking

S.1 General

This annex describes the IMS architecture and procedures for support of IP-PBX business trunking.

Two different modes of operation are supported

- Registration mode, or
- Static mode.

In both modes, the IP-PBX can be provisioned as a subscriber in the HSS.

In registration mode, the IP-PBX registers to and receives service from the IMS network as specified in TS 24.525 [81].

The architecture and procedures for an IP- PBX using static mode is described in clause S.2.

S.2 IP-PBXs using static mode Business Trunking

S.2.1 High level architecture

The support for business trunking in static mode is provided by either an IBCF or a P-CSCF.

The architecture for support of IP-PBX in static mode of operation is shown in Figure S.2-1.

NOTE: The IP-PBX can not register when using the static mode.

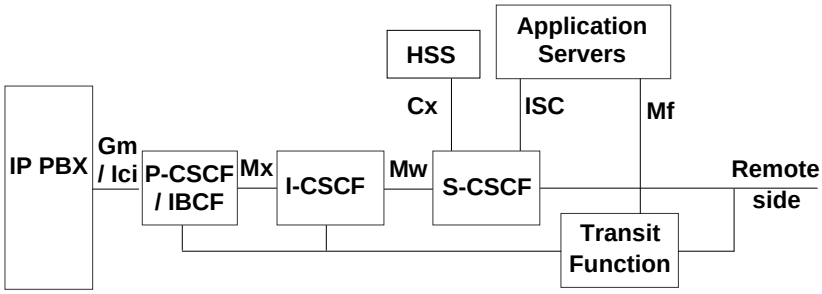


Figure S.2-1: High level Static mode business trunking Architecture

The IP-PBX identity assertion and the routing of terminating sessions are performed by Application Server(s), which may or may not also host a business trunking application. The architecture for support of IP-PBX in static mode of operation shown in Figure S.2-1 allows for two different deployment alternatives.

- The Application Server(s) hosting these functionalities are invoked by the S-CSCF based on Initial Filter Criteria contained in the unregister part of the IP-PBX's subscriber profile, retrieved from the HSS.
- As according to clause 4.15 and TS 24.525 [81], this deployment relies on the Transit function with Application Server(s) hosting these functionalities are invoked by the Transit Function based on transit invocation criteria, which need to be provisioned in the Transit Function.

In both cases, the AS performing the routing of terminating sessions needs to be the last AS invoked for terminating sessions.

Both deployment options can simultaneously be used in in an IMS Network, although it requires that the enterprise user identities allocated in the different deployments are not overlapping.

S.2.2 High level Flows

S.2.2.1 General

Before any originating or terminating procedures can take place between the IP-PBX and the P-CSCF or between the IP-PBX and the IBCF of the IMS network, security and authentication between the IP-PBX and IMS is done using the TLS procedures according to TS 33.310 [5], using certificates. The certificates are provided by a trusted root. The P-CSCF or the IBCF is provisioned with its own certificate, and will receive the IP-PBX certificate during the TLS handshake.

In configurations where there is a NAT between the IP-PBX and the IMS, the TLS connection needs to be initiated and maintained by the IP-PBX.

If the network between the PBX and the IBCF complies with the peering based interconnect procedures according to TS 24.525 [81], the IBCF may deploy the Gq' interface. The Gq' interface and its interactions are not depicted in these flows.

S.2.2.2 Originating procedures

S.2.2.2.1 Originating procedures using the S-CSCF

This clause depicts originating procedures for IP-PBXs using static mode business trunking when the IP-PBX is provisioned as a subscriber in HSS and served via the S-CSCF.

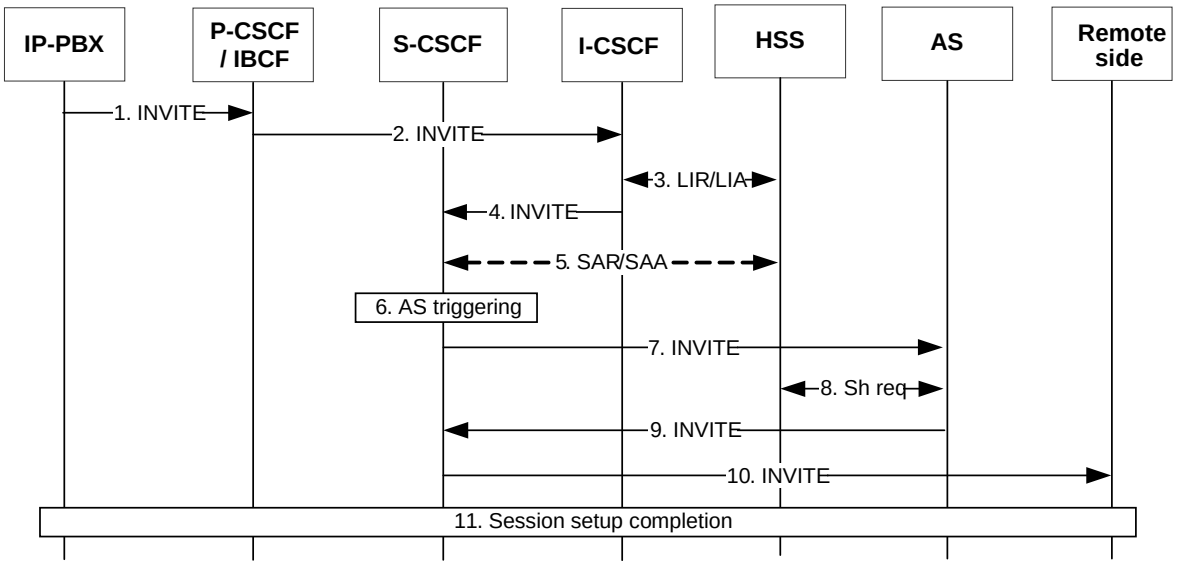


Figure S.2-1: Originating procedures for IP-PBXs using static mode business trunking and served by the S-CSCF

The following steps are performed:

1. An enterprise user within the IP-PBX tries to establish a call. The IP-PBX sends an INVITE towards IMS via the P-CSCF or via the IBCF (contact point for the IP-PBX). If no security association exists between the P-CSCF/IBCF and the IP-PBX, TLS will be initiated as a result of trying to send the INVITE. Once the TLS session is setup (using the certificates), the INVITE will be sent over the secure connection. The INVITE is assumed to include a calling party identity.

2. The P-CSCF/IBCF may apply general screening rules to the request and adds a P-Served-User-Identity to the INVITE with the identity of the PBX (SIP URI identifying the domain of the PBX retrieved from the certificate). Additionally, the P-CSCF/IBCF adds the orig parameter to the INVITE to indicate that this is an origination request. The P-CSCF/IBCF forwards the INVITE to the I-CSCF.

3. The I-CSCF performs the normal (originating request) user location request towards HSS to find an S-CSCF to serve the IP-PBX. If there is no subscription in the HSS, the I-CSCF forwards the request to a Transit Function (and routing may continue as described in step 4 of clause S.2.2.2.2); otherwise, the following steps are performed.

4. The I-CSCF forwards the request to the S-CSCF.

5. When the S-CSCF does not have the IP-PBX's subscriber profile, the S-CSCF contacts HSS to download the subscriber information for the unregistered IP-PBX.

NOTE: The load on the Cx interface due to the downloading of unregistered IP-PBXs subscriber profiles is dependent on the timer in the S-CSCF defining the duration the profile is kept for unregistered users. By increasing this timer, this load can be lowered.

6. The S-CSCF performs normal (unregistered) originating service invocation for the incoming request.

7. The S-CSCF forwards the request to the AS hosting the IP-PBX identity assertion. Based on the P-Served-User-Identity, this AS identifies the IP-PBX and inserts a P-Asserted-Identity identifying the enterprise user. Other Application Servers may be triggered based on iFC and may, based on the P-Asserted-Identity, perform any enterprise specific actions if required.

8. Each of the triggered ASes may optionally query HSS for any subscriber information if required using the Sh interface.

9. The INVITE is forwarded to S-CSCF for further onward routing towards the remote side.

10. The S-CSCF performs onward routing towards the remote side.

11. The session setup is completed.

S.2.2.2.2 Originating procedures using the Transit Function

This clause depicts the originating procedures for IP-PBXs using static mode business trunking as described in TS 24.525 [81] when the IP-PBX is not provisioned as a subscriber in HSS and served via the Transit Function.

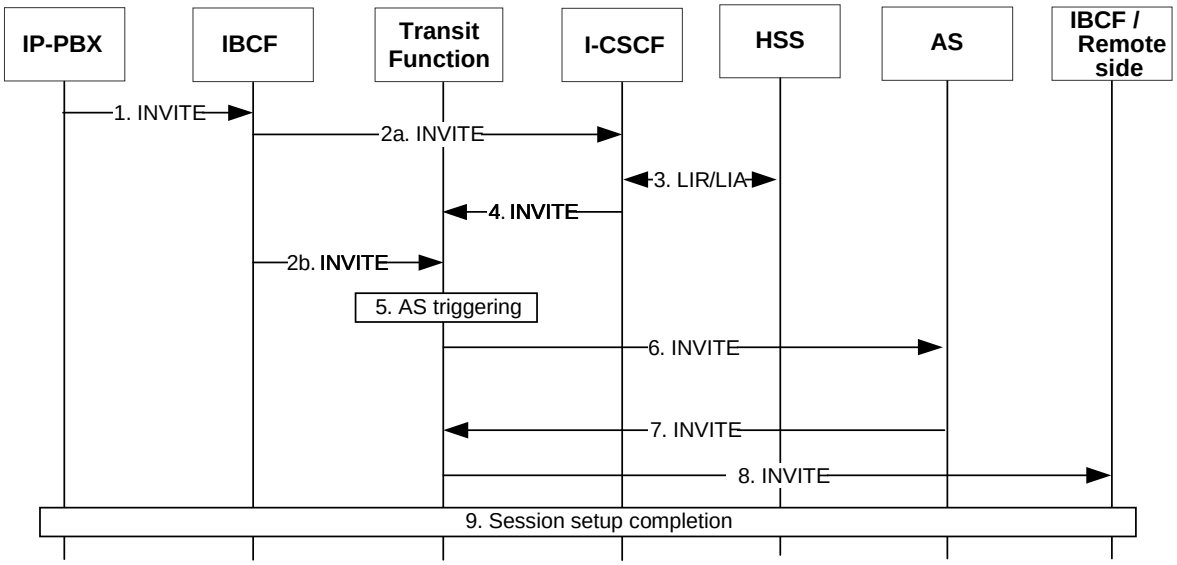


Figure S.2-2: Originating procedures for IP-PBXs using static mode business trunking and served by the Transit Function

The following steps are performed:

1. An enterprise user within the IP-PBX tries to establish a call. The IP-PBX sends an INVITE towards IMS via the IBCF (contact point for the IP-PBX). If no security association exists between the IBCF and IP-PBX, TLS will be initiated as a result of trying to send the INVITE. Once the TLS session is setup (using the certificates), the INVITE will be sent over the secure connection. The INVITE is assumed to include a calling party identity.

2a. The IBCF may apply general screening rules to the request, and adds a P-Served-User-Identity to the INVITE with the identity of the IP-PBX (SIP URI identifying the domain of the IP-PBX retrieved from the certificate). Additionally, the IBCF adds the orig parameter to the INVITE to indicate that this is an origination request. The IBCF sends the INVITE to the I-CSCF).

2b. The IBCF performs the same actions as in step 2a. but sends the INVITE directly to the the Transit Function instead of the I-CSCF. (The next step is step 5).

3. The I-CSCF performs the normal (originating request) user location request towards HSS to find the served user, but as it is not provisioned in HSS, "user not found" is returned.

4. Ths I-CSCF sends the INVITE to the Transit Function.

5. The Transit Function is configured with a set of Transit invocation criteria that are triggered to find a correct AS to route to. As this is an origination case (as indicated by the orig parameter), the P-Served-User-Identity is used to identify the IP-PBX.

6. The Transit Function forwards the request to the AS hosting the IP-PBX identity assertion. Based on the P-Served-User-Identity, this AS identifies the IP-PBX, verifies that this IP-PBX is a valid user and inserts a P-Asserted-Identity identifying the enterprise user. Other ASes may be triggered based on iFC and may, based on the P-Asserted-Identity, apply any enterprise specific actions if required.

7. The INVITE is forwarded for further onward routing towards the remote side.

8. Transit Function performs onward routing towards the remote side.

9. The session setup is completed.

S.2.2.3 Terminating Procedures

S.2.2.3.1 Terminating procedures using the S-CSCF

This clause depicts terminating procedures for IP-PBXs using static mode business trunking when the IP-PBX is provisioned as a subscriber in HSS and served via the S-CSCF.

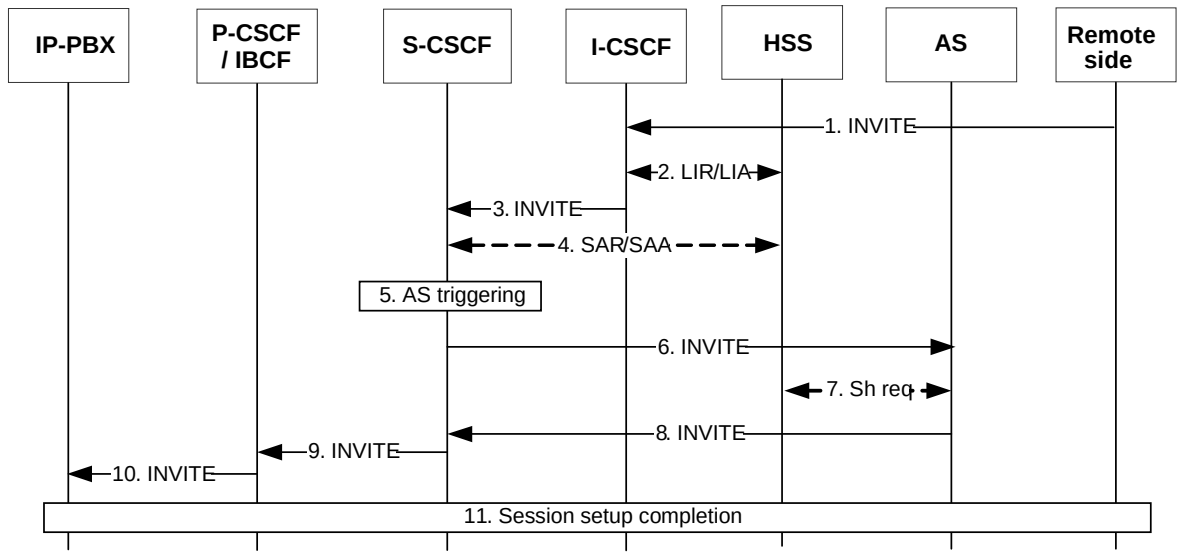


Figure S.2-3: Terminating procedures for IP-PBXs using static mode business trunking and served by the S-CSCF

The following steps are performed:

1. An INVITE is sent from the remote side towards the I-CSCF with a Request-URI which belongs to a particular enterprise user of a served IP-PBX.

2. The I-CSCF performs the normal user location request towards HSS to find an S-CSCF to serve the IP-PBX.

3. The I-CSCF forwards the request to the S-CSCF.

4. When the S-CSCF does not have the IP-PBX's subscriber profile, the S-CSCF contacts HSS to download the subscriber information for the unregistered IP-PBX.

NOTE 1: The load on the Cx interface due to the downloading of unregistered IP-PBXs subscriber profiles is dependent on the timer in the S-CSCF defining the duration the profile is kept for unregistered users. By increasing this timer, this load can be lowered.

5. The S-CSCF performs normal (unregistered) terminating service invocation for the incoming request.

6. The S-CSCF forwards the request to the ASes to be triggered per iFC. Each of these ASes may identify the IP-PBX the enterprise user belongs to and perform any enterprise specific actions if required.

7. Each of the triggered ASes may optionally query HSS for any subscriber information if required using the Sh interface.

8. The IP-PBX routing functionality (hosted by the last AS in the iFC chain) identifies the particular IP-PBX the enterprise user belongs to, and also the P-CSCF(s) or the IBCF(s) serving the IP-PBX, and forwards the INVITE toward the IP-PBX (by creating a route to the IP-PBX, adding the S-CSCF, the P-CSCF/IBCF, and the IP-PBX in the Route header fields).

NOTE 2: Inserting the route to the IP-PBX in Route header fields will not allow to trigger any AS after the IP-PBX routing functionality. Similar to the T-ADS functionality, the IP-PBX routing functionality has to be last in the chain of iFCs.

9. The INVITE is forwarded using the route information to the P-CSCF or the IBCF.

10. The P-CSCF/IBCF will forward the INVITE to the IP-PBX using the route information provided by the IP-PBX routing functionality. If no security association exist between the P-CSCF/IBCF and the IP-PBX (and TLS is used), TLS will be initiated as a result of trying to send the INVITE. Once the TLS session is setup (using the certificates) the INVITE will be sent over the secure connection.

11. The session setup is completed.

S.2.2.3.2 Terminating procedures using the Transit Function

This clause depicts the terminating procedures for IP-PBXs using static mode business trunking as described in TS 24.525 [81] when the IP-PBX is not provisioned as a subscriber in HSS and served via the Transit Function.

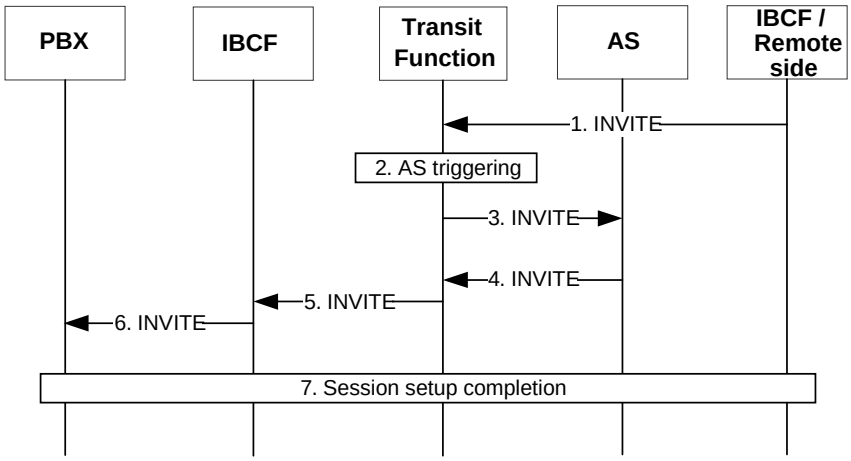


Figure S.2-4: Terminating procedures for IP-PBXs using static mode business trunking and served by the Transit Function

The following steps are performed:

1. An INVITE is sent from the remote side via an incoming IBCF towards the Transit Function with a Request-URI targeting an enterprise user allocated to a particular IP-PBX.

NOTE: The INVITE from the IBCF can be sent via an I-CSCF before it ends up in the Transit Function. In such case, the I-CSCF will detect that this is not a provisioned user, and therefore decide to route to the Transit Function.

2. The Transit Function will based on the Request-URI determine that the served user is belonging to an IP-PBX and corresponding transit invocation criteria that are used to identify the ASes to be triggered, including the AS hosting the IP-PBX routing functionality, which is the last AS to be triggered.

3. The Transit Function forwards the request to the required ASes. Each of these ASes may identify the IP-PBX the enterprise user belongs to and perform any enterprise specific actions if required.

4. The IP-PBX routing functionality (hosted by the last AS in the chain) identifies the particular IP-PBX the enterprise user belongs to, and optionally also the IBCF(s) serving the IP-PBX, and forwards the INVITE toward the IP-PBX by creating a route to the IP-PBX, adding the Transit Function, the IBCF, and the IP-PBX in the Route header fields.

5. The INVITE is forwarded using the route information to the IBCF.

6. The IBCF will forward the INVITE to the IP-PBX using the route information provided by the AS. If no security association exist between the IBCF and the IP-PBX (and TLS is used), TLS will be initiated as a result of trying to send the INVITE. Once the TLS session is setup (using the certificates) the INVITE will be sent over the secure connection.

7. The session setup is completed.

Annex T (normative): IP-Connectivity Access Network specific concepts when using Trusted WLAN (TWAN) to access IMS

T.0 General

This clause describes the main IP-Connectivity Access Network specific concepts that are used for the provisioning of IMS services over a Trusted WLAN (TWAN) access to EPC.

As IMS is accessed over EPC, most of the features defined in clause E for the case of EPC (and PDN connections/EPS bearers) apply in the case of a TWAN access, e.g. a P-GW is used as an IP anchor point and IP-Connectivity Access Network bearers are provided by PDN connections and bearers.

Following specific considerations apply to the case of a TWAN access:

- The Mobility related procedures for EPS and TWAN access are described in TS 23.402 [82]
    - TWAG/TWAP (refer to clause 16 of TS 23.402 [82]) are used to interface the access network and to control relevant PDN connectivity (over S2a) towards a P-GW.
- For a TWAN access, the way the notification of the loss of IP-CAN session for an UE is triggered within a TWAN is out of scope of 3GPP specifications.

T.1 Retrieval of Network Provided Location Information in TWAN access

For a TWAN access, Access Network Information may be reported to the IMS as described in clause E.7 for the case of a GPRS/EPS access, with following exceptions:

- The Access Network Information being reported to the P-CSCF is defined in clause 16 of TS 23.402 [82].

A Geographical Identifier may be generated by the P-CSCF or an IMS AS based on the retrieved Access Network Information, as specified in clause E.8.

Annex U (normative): WebRTC access to IMS - network-based architecture

U.1 Overview

U.1.0 General

Web Real-Time Communication (WebRTC) is specified in IETF Draft, draft-ietf-rtcweb-overview [84] and WebRTC 1.0 [85]. This Annex specifies a network-based architecture for the support of WebRTC client's access to IMS. Any requirements for specific audio and video codecs from draft-ietf-rtcweb-overview (directly and indirectly referenced) do not apply for WebRTC access to IMS; the codecs that shall be supported for WebRTC access to IMS are described in TS 26.114 [76].

NOTE: The UE can also perform WebRTC access to IMS by implementation specific means in the UE in which it exposes a standard Gm interface towards IMS.

U.1.1 Assumptions

- This Release specifies an option to use a signalling interface from the UE to the network based on SIP over WebSocket (RFC 7118 [89]), which is used as the information model which may be used by other options. Options other than SIP over WebSocket, such as XMPP or other application protocols over WebSocket, a RESTful based interface, etc. are allowed but not described. Alternative message body formats such as JSON and alternative transport protocols are also not precluded. Any enhancements required to accommodate an unspecified signalling interface are considered compliant to the Release as long as other defined interfaces in the architecture are not impacted.

- SDP offer/answer exchange is the mechanism used for media plane feature negotiation.

- The architecture does not support media multiplexing that is defined for WebRTC clients. A WebRTC IMS Client (WIC) accessing IMS services should not allow usage of media multiplexing in the browser.

- If an SDP offer with media multiplexing is sent to the network the part of the SDP offer associated with media multiplexing shall be removed at the entry of the IMS network.

- WebRTC specific media plane extensions will be handled at the access edge and will not be propagated to other IMS functions.

- For network based interworking between WebRTC and IMS, in the case of 3GPP and EPC access from a WebRTC client:

  - Use of available techniques to select preferred access technologies and APNs/DNNs, and to provide IP address continuity, are allowed but not described.

  - When the WebRTC client is served by an IP-CAN that supports PCC, it is possible to request QoS within the IP-CAN for WebRTC media.

NOTE: To ensure full end to end QoS support, proper IP forwarding policies can be set in the path between the P-GW and the Functions supporting media interworking to the IMS.

- QoS can be provided in configurations where the IMS can identify the transport (TCP-UDP/IP) addresses handled by the PCEF and where based on this information PCC functions can identify the UE media flows to prioritize.

- The eP-CSCF is located in the Home IMS domain of the IMS Public User Identity being registered via the eP-CSCF.

- The WIC may have no way to access the content of an ISIM/USIM on the UE

U.1.2 Architecture and reference model

Figure U.1.2-1 shows the WebRTC IMS architecture. The WWSF (WebRTC Web Server Function) is located either within the operator network or within a third party network and is the web server contacted by the user agent (generally after clicking on a link or entering a URL into the browser). The P-CSCF enhanced for WebRTC (eP-CSCF) is the endpoint for the signalling connection from the client and is located in the operator network.

NOTE 1: The presence of dashed elements in the figure depends on the configuration.
PCC functional elements are present only for EPC access with QoS.
The corresponding PCC elements for fixed access are also optionally supported but not shown.
The NAT in figure U.1.2-1 is meant for non-cellular access to IMS.

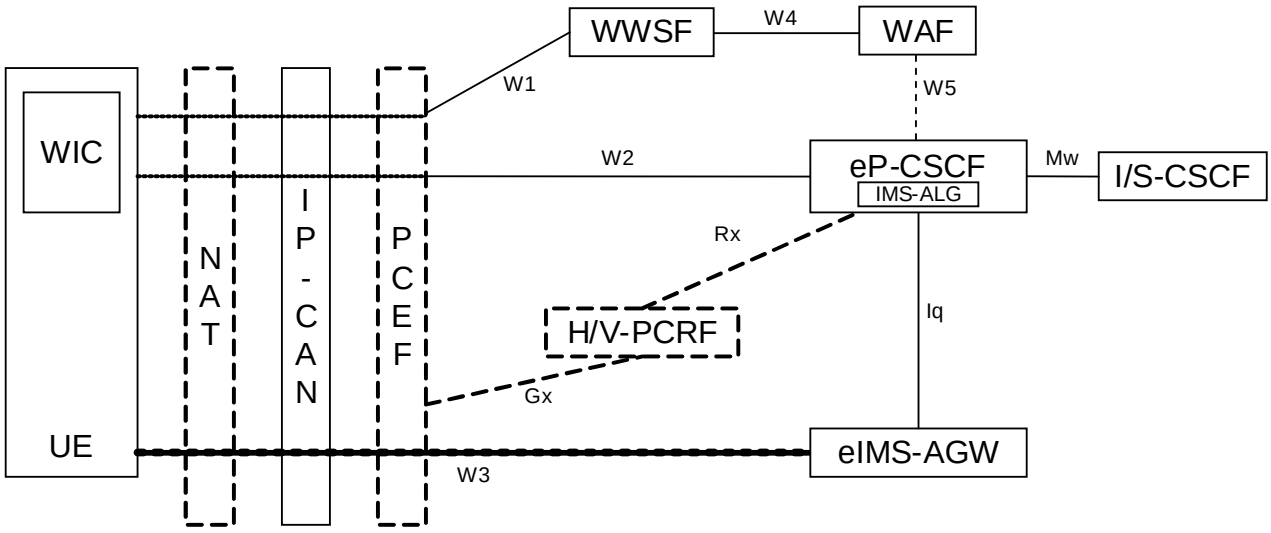


Figure U.1.2-1: WebRTC IMS architecture and reference model

NOTE 2: W3 corresponds to the output of the IETF RTCWEB discussions.

NOTE 3: The enhanced network entities, such as the eP-CSCF, might be decomposed into multiple network elements (e.g. P-CSCF and WebRTC Signalling Function) in future Releases to address additional use cases and configurations.

NOTE 4: The W5 reference point is an optional signalling interface between the WAF and the eP-CSCF. The W5 reference point is not specified and is implementation specific.

U.1.3 Functional entities

U.1.3.1 WIC (WebRTC IMS Client)

A WebRTC IMS Client (WIC) is an application using the WebRTC extensions specified in WebRTC 1.0 [85] except for those extensions specifically exempted by 3GPP specifications (e.g. TS 26.114 [76]) and providing access to IMS by interoperating with the WebRTC IMS access architecture defined in this Annex.

Any IP access network with access to the internet may be used by a WIC; nevertheless WebRTC traffic is subject to the QoS and reachability limitations of this access network.

U.1.3.2 WWSF (WebRTC Web Server Function)

The WebRTC Web Server Function (WWSF) is the initial point of contact in the Web that controls access to the IMS communications services for the user. The WWSF has the following characteristics and functions:

- The WWSF is located either in the operator network or a third party network
- The WWSF provides the Web page presenting the user interface to the user for IMS access.

- The WWSF provides the JS WIC application for downloading to the browser on the UE.

- The WWSF manages the allocation of authorized IMS identities to WICs. The JS application downloaded from the WWSF controls which authentication method applies.

NOTE 1: The WWSF represents a collection of functions that might be further split across servers or networks, so long as they behave in the aggregate as described in this Annex U.

NOTE 2: The WWSF can include WAF functionality in the case WWSF and WAF are in the same domain.

U.1.3.3 eP-CSCF (P-CSCF enhanced for WebRTC)

The P-CSCF enhanced for WebRTC (eP-CSCF) is a P-CSCF including the IMS-ALG functionality and with the following additional functions:

- The eP-CSCF shall support at least one WebRTC IMS client-to-network signalling protocol, e.g. SIP over WebSocket, REST/HTTP based interface, XMPP over WebSocket, etc.

NOTE 1: Other application protocols, alternative message body formats such as JSON and alternatives to WebSocket transport are also not precluded.

- The eP-CSCF provides interworking between W2 and Mw.

- The eP-CSCF verifies that the UE is executing a WIC from an authorized WWSF.

- In the case of WIC registration of individual Public User Identity using IMS Authentication, the eP-CSCF shall relay the IMS authentication and registration information between W2 and Mw.

- Otherwise, i.e. for users authorized by the WWSF or WAF:

  - The eP-CSCF shall verify any UE authorization information received from the WIC;

  - The eP-CSCF shall verify that the WWSF is authorized to allocate IMS identities;

NOTE 2: For this purpose the eP-CSCF can identify an existing trust relationship between the eP-CSCF and the WWSF or WAF.

  - The eP-CSCF shall perform Trusted Node Authentication (TNA) in IMS, as defined in TS 33.203 [19].

- The eP-CSCF shall control the media plane interworking functions provided by the eIMS-AGW, including those additional media plane functions specific to WebRTC.

- The eP-CSCF shall ensure via signalling that RTP streams are not multiplexed ("bundled") onto the same port.

- The eP-CSCF shall negotiate via signalling whether RTP and RTCP flows of an RTP stream are multiplexed onto the same port and shall configure the eIMS-AGW to (de)multiplex such flows if entities anchoring the session media path in the IMS domain do not support that capability.

- The eP-CSCF is located in the domain of the operator that provides the WWSF or with which the WWSF has a service level agreement.

U.1.3.4 eIMS-AGW (IMS Access GateWay enhanced for WebRTC)

The IMS-AGW enhanced for WebRTC (eIMS-AGW) is a standard IMS-AGW with the following additional mandatory characteristics and functions:

- The eIMS-AGW shall support the media plane interworking extensions as needed for WICs.

- The eIMS-AGW shall reside in the same network as the eP-CSCF.

- The eIMS-AGW shall support media security of type "e2ae" (as specified in TS 33.328 [83]) for media protocols specific to WebRTC, including media consent, and DTLS-SRTP as key exchange mechanism for media components using SRTP.

- The eIMS-AGW shall provide NAT traversal support including ICE

- The eIMS-AGW may be used to perform any transcoding needed for audio and video codecs supported by the browser.

- When GTT service is required, the eIMS-AGW shall perform transport level interworking between T.140 [87] over Data Channels and other T.140 transport options supported by IMS.

- When MSRP is transported over the data channel, the eIMS-AGW shall act as an MSRP B2BUA between MSRP over Data Channels and the other MSRP transport options supported by IMS.

NOTE: If CEMA extensions for transport-level interworking for MSRP are supported in IMS, the eIMS-AGW will also support this option.

- When BFCP service is required for conference floor control and BFCP is transported over Data Channels, the eIMS-AGW shall perform transport level interworking between BFCP over Data Channels and other BFCP transport options supported by IMS.

- The eIMS-AGW shall support the media plane optimization for WICs.

- The eIMS-AGW shall support that RTP and RTCP flows of an RTP stream between WIC and eIMS-AGW are multiplexed onto the same port, and shall support de-multiplexing such RTP and RTCP flows toward the core network.

U.1.3.5 WAF (WebRTC Authorisation Function)

The WebRTC Authorisation Function (WAF) has the following characteristics and functions:

- The WAF shall issue the authorisation token to WWSF.

- The WAF may either authenticate the user itself as part of the token issuance process, or it trusts the user identity provided by the WWSF.

- The WAF may either reside in the operator domain or the third party domain.

The WAF is not used in the case of IMS registration scenario using IMS Authentication, described in clause U.2.1.1.

NOTE: The WWSF can include WAF functionality in the case WWSF and WAF are in the same domain.

U.1.4 Reference points

U.1.4.1 W1 (UE to WWSF)

The W1 reference point is between the UE and the WWSF. The HTTPS protocol is normally used to access the web page providing the User Interface for the WIC and to download the WIC JS application to the browser.

U.1.4.2 W2 (UE to eP-CSCF)

The W2 reference point is the signalling interface between the UE and the eP-CSCF. SIP over secure WebSocket is a non-mandatory option for W2 in Release 12, where the SIP/SDP procedures are based on Gm with enhancements to support extensions defined for WIC, and secure WebSocket is the supported transport protocol. Other protocols are allowed on W2 for WebRTC access but are not described in this document.

U.1.4.3 Iq (eP-CSCF to eIMS-AGW)

The Iq reference point is between the eP-CSCF and eIMS-AGW and is enhanced to control the additional bearer plane functions specific to WIC.

U.1.4.4 W3 (UE to eIMS-AGW)

The W3 reference point is between the UE and eIMS-AGW. W3 carries the user plane between the UE and the network (see clause U.1.5).

U.1.4.5 W4 (WWSF to WAF)

The W4 reference point is the signalling interface between the WWSF and the WAF. The WWSF obtains an authorisation token from the WAF from which the user's identities, identities of WWSF and WAF, and a lifetime may be derived in the case of IMS registration scenarios based on web authentication and assignment from a pool of user identities.

U.1.5 Media plane protocol architecture

U.1.5.0 General

The IMS AGW enhanced for WebRTC (eIMS-AGW) is the media plane interworking element with the functions described in clause U.1.3.4.

NOTE: In this clause, the figures describe the end to end scenario where "the peer" corresponds to a remote IMS terminal. In this case, when e2ae security is needed, TS 33.328 [83] shall govern the interaction between "the peer" and the IMS-AGW that serves it. Other scenarios with other kind of peers (e.g. the peer is another webRTC terminal) are possible but not represented.

U.1.5.1 Protocol architecture for MSRP

Figure U.1.5.1-1 shows the protocol architecture for support of MSRP, when transported over the data channel, from a WebRTC IMS client (WIC).

When MSRP is transported over the data channel, the eIMS-AGW shall provide either a transport relay function from Data Channel to TCP or an MSRP B2BUA to allow interoperation with existing MSRP peer endpoints.

UDP transport of DTLS shall be supported and TCP transport of DTLS may be supported to enable traversal of UDP-blocking NATs/firewalls.

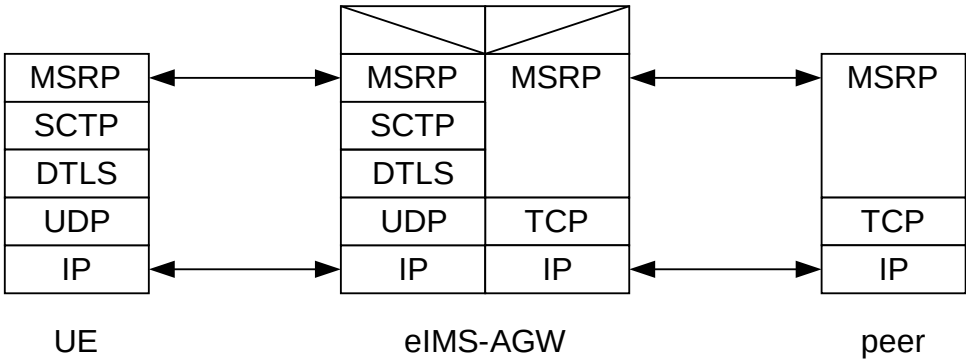


Figure U.1.5.1-1: Protocol architecture for MSRP

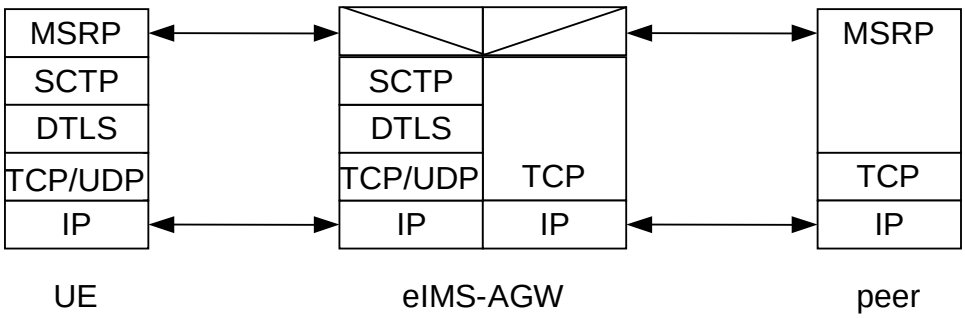


Figure U.1.5.1-2: Protocol architecture for MSRP acting as transport relay function

U.1.5.2 Protocol architecture for BFCP

Figure U.1.5.2-1 shows the protocol architecture for support of BFCP, when transported over the data channel for conference floor control, from a WebRTC IMS client (WIC).

When BFCP service is required for conference floor control and BFCP is transported over Data Channels, the eIMS-AGW shall provide a transport relay function from Data Channel to TCP to allow interoperation with existing BFCP peer endpoints.

UDP transport of DTLS shall be supported and TCP transport of DTLS may be supported to enable traversal of UDP-blocking NATs/firewalls.

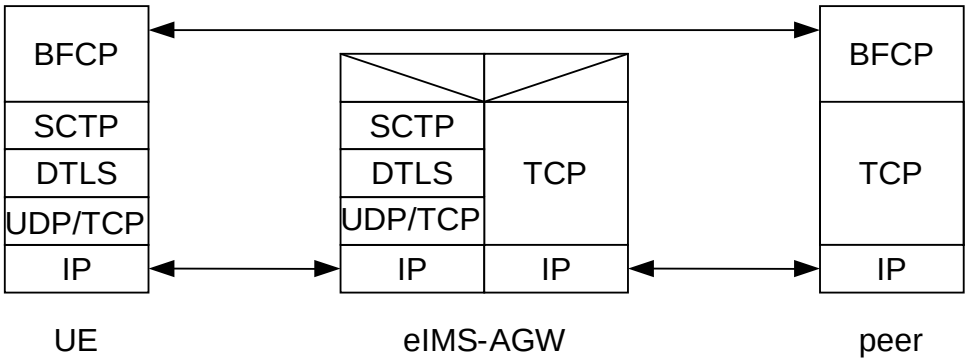


Figure U.1.5.2-1: Protocol architecture for BFCP

U.1.5.3 Protocol architecture for T.140

Figure U.1.5.3-1 shows the protocol architecture for support of T.140 from a WebRTC IMS client (WIC).

The eIMS-AGW shall provide a transport relay function from Data Channel to RTP to allow interoperation with existing T.140 peer endpoints.

UDP transport of DTLS shall be supported and TCP transport of DTLS may be supported to enable traversal of UDP-blocking NATs/firewalls.

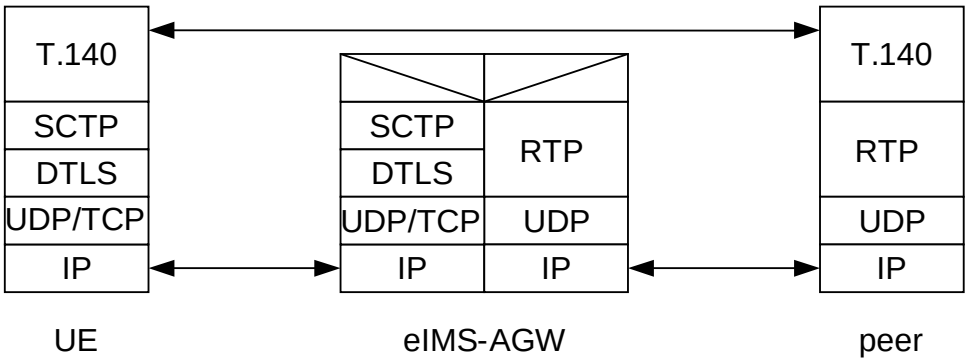


Figure U.1.5.3-1: Protocol architecture for T.140

U.1.5.4 Protocol architecture for Voice and Video

Figure U.1.5.4-1 shows the protocol architecture for support of Voice and Video from a WebRTC IMS client (WIC). Transcoding (i.e. allowing codec1 to be different from codec2) is optional. SRTP between the UE and the eIMS-AGW relies on keying material negotiated via DTLS.

NOTE 1: Transcoding at the eIMS-AGW may apply to none, one or both of the voice and video components

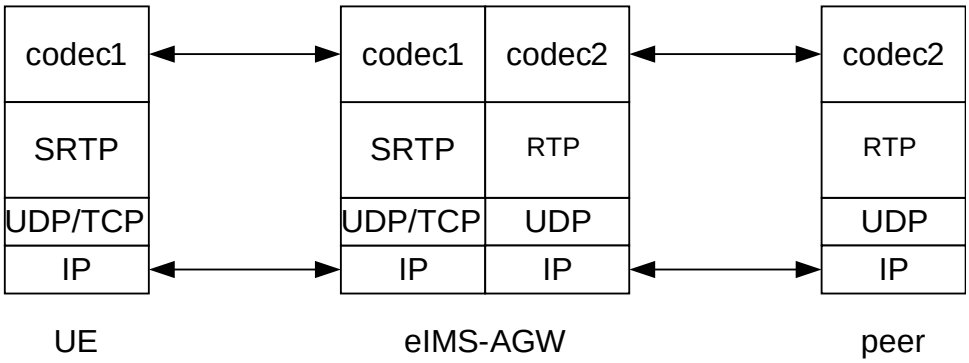


Figure U.1.5.4-1: Protocol architecture for Voice and Video

NOTE 2: RFC 4571 [90] framing is used for RTP streams transferred over TCP. RTP over TCP may be used when NATs/Firewalls perform UDP blocking.

U.2 Procedures

U.2.0 WWSF discovery

The URI to a WWSF for WebRTC access to IMS may be configured in the UICC.

Prior to performing registration, a UE may use the following mechanism to determine the URI of the WWSF:

- If the UICC contains a URI to a WWSF for WebRTC access to IMS, then the UE uses this URI for registration.
- Otherwise, the UE derives the URI to WWSF from the home domain name as specified in TS 23.003 [24].

Alternatively, the URI to a WWSF may be obtained by means outside the 3GPP scope.

U.2.1 Registration

U.2.1.1 Introduction

The WebRTC IMS architecture supports the following different IMS registration scenarios that may differ in the authentication method, and ownership of the WWSF (i.e. operator network or third party):

- "WIC registration of individual Public User Identity using IMS authentication": The user has a subscription with an individual Public User Identity and an IMS authentication mechanism as specified in TS 33.203 [19] is used to authenticate with IMS. Clause U.2.1.2 provides detailed procedures for this scenario.
- "WIC registration of individual Public User Identity based on web authentication": The user has an IMS subscription. The WWSF or WAF authenticates the user using a web identity and authentication scheme. The WWSF determines IMS identities for the user (e.g. based on the user's web identity via database lookup or other translation means). An individual registration is handled by the S-CSCF per WIC registration. Clause U.2.1.3 provides detailed procedures for this scenario.
- "WIC registration of individual Public User Identity from a pool of Public User Identities": The WWSF is typically located in a third party network and has a business arrangement with the IMS operator. The WWSF or WAF authenticates the user using a web identity and authentication scheme, or authorizes the WIC without authenticating the user. The WWSF assigns IMS identities to the user from within a pool allocated by the operator. An individual registration is handled by the S-CSCF per WIC registration. Clause U.2.1.4 provides detailed procedures for this scenario.

U.2.1.2 WIC registration of individual Public User Identity using IMS authentication

The WIC obtains information needed for IMS registration (e.g. Private User Identity and Public User Identity) via unspecified means. For example, some of this information might be stored in cookies or local browser storage after visiting a secure web site provided by the IMS operator.

Figure U.2.1.2-1 shows a registration call flow where IMS authentication is used to register the WIC.

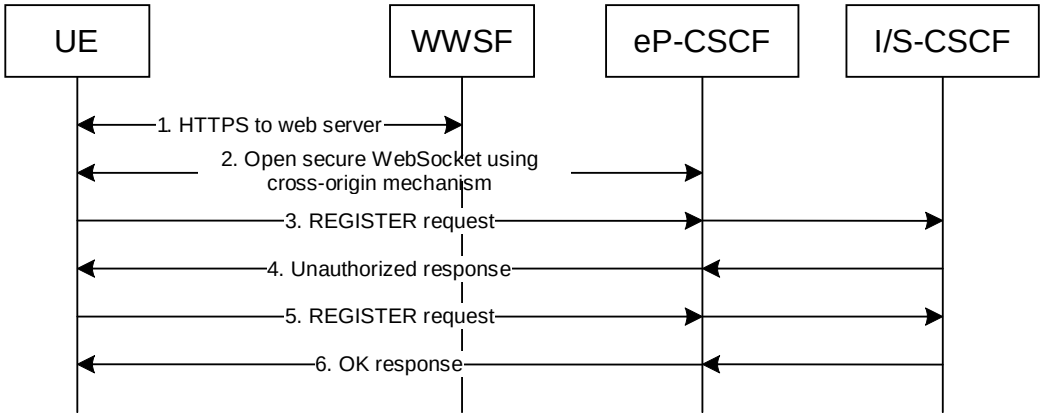


Figure U.2.1.2-1: WIC registration of individual Public User Identity using IMS authentication

1. The WIC initiates an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WIC from the WWSF.

2. The WIC opens a WSS (secure WebSocket) connection using cross-origin mechanism to the eP-CSCF. Standard cross-origin resource sharing procedures are used to ensure that the WIC originated from a WWSF authorized to access this eP-CSCF.

3-6. The WIC initiates a registration transaction with IMS via the eP-CSCF by sending a REGISTER request to the eP-CSCF via the WSS (secure Web Socket) connection. The REGISTER request includes IMS Authentication parameters, Private User Identity, Public User Identity and other information as needed for proper IMS registration. This request is translated into an IMS registration process by the eP-CSCF. This process leverages user credentials in HSS.

U.2.1.3 WIC registration of individual Public User Identity based on web authentication

Figure U.2.1.3-1 shows a registration call flow where the WIC registers with IMS based on web authentication with the WWSF.

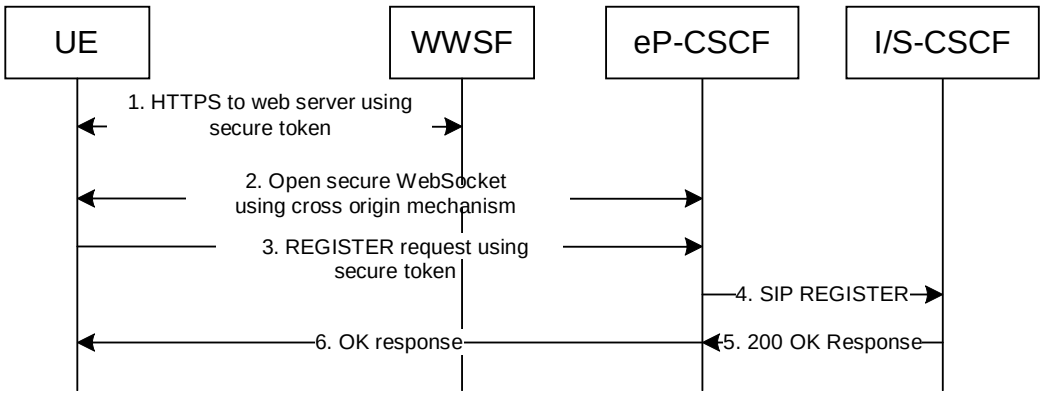


Figure U.2.1.3-1: WIC registration of individual Public User Identity based on web authentication

1. The WIC initiates an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WIC from the WWSF. The WWSF or WAF authenticates the user using a common web authentication procedure. The WWSF determines the Private User Identity and Public User Identity for the WIC and returns the security token which is issued by the WAF to the WIC. The IMS identities may be provided to the WIC in addition to the security token.

2. The WIC opens a WSS (secure WebSocket) connection using cross-origin mechanism to the eP-CSCF. Standard cross-origin resource sharing procedures are used to ensure that the WIC originated from a WWSF authorized to access this eP-CSCF.

3. The WIC sends a REGISTER request to the eP-CSCF via the WSS (secure Web Socket) connection. The request includes the security token received from the WWSF. If the WIC received the IMS identities in step 1, the request shall include the IMS identities.

4. The eP-CSCF validates the contents of the security token and obtains the IMS identities being registered. The eP-CSCF then forwards the authorized REGISTER request to IMS to initiate authentication-less IMS registration using TNA (see TS 33.203 [19], Annex U) procedures, with an indication that the authentication has already been carried out.

5. The S-CSCF responds with a 200 OK message are accepted.

6. The eP-CSCF sends the OK response back to the WIC.

As the security token may be associated with a lifetime, the WIC may need to periodically refresh its registration. This registration refresh process entails all steps above with following exceptions:

- For Step 1, the opening of the TLS connection, the downloading of the WIC and the web authentication of the user using the WIC may not be needed.

- Step 2 may not be needed.

U.2.1.4 WIC registration of individual Public User Identity from a pool of Public User Identities

The WWSF is provided with a pool of IMS subscriptions, each associated to a single Private User Identity and one or more Public User Identities as specified in clause 4.3.3.4. The WWSF can assign individual Public and Private User Identities from this pool. The WWSF may be located in a third party network and have a business arrangement with the IMS operator.

For pool management, the IMS operator may also provide the WWSF with an unbounded number of Private User Identities/Public User Identities associations to be allocated to WIC users, where each user may use multiple WICs sharing the same Public User Identity and each WIC being assigned a different Private User Identity.

NOTE: How the HSS handles and manages the unbounded users is implementation specific.

The registration call flow for a WIC being assigned an individual Public User Identity from a pool of Public User Identities assigned to the WWSF is the same registration call flow defined in Figure U.2.1.3-1 with following differences:

- In step 1, the WWSF or WAF may decide not to authenticate the user. Unauthenticated users are anonymous to the third party but may still be authorized for IMS service.

- The lifetime of the security should be coordinated between the IMS provider and the WWSF provider; otherwise, the WWSF cannot know when a Public User Identity Private User Identity association from its pool can be re-assigned to another user.

- Alternatively, as an implementation specific option, eP-CSCF may indicate to the WWSF when a certain Public User Identity can be re-assigned.

U.2.2 Session management related procedures

Origination and termination and Session release procedures for WebRTC IMS clients follow standard IMS procedures in the core network (see clauses 5.6 and 5.7 and 5.10) with the exception that routing of all messages between the WIC

and S-CSCF traverse the eP-CSCF (rather than P-CSCF) and that parameters of Iq procedures take into account the WebRTC-specific extensions used by the WIC to send and receive media.

U.2.3 De-Registration procedures

De-registration procedure for WebRTC IMS clients follows standard IMS procedures in the core network (see clause 5.3) with the exception that routing of all messages between the WIC and S-CSCF traverse the eP-CSCF (rather than P-CSCF).

U.2.4 Media plane Optimization

The IMS operator is able to convey the audio and chat session without bearer level protocol conversion when session is between WebRTC clients.

When both ends are WebRTC client, the eIMS-AGWs remain allocated but media plane interworking is disabled, except when LI is needed. When media plane optimization is enabled, the eIMS-AGW forwards all protocol layers either including DTLS, or on top of DTLS transparently (see clause U.1.5).

NOTE: Terminating the DTLS protocol layer for all calls can improve the transparency of LI.

When LI is performed, media plane interworking is performed according to TS 33.328 [83].

Figure U.2.4-1 shows a call flow diagram establishing the e2ae communication between WebRTC clients through the IMS network. I/S-CSCFs are not shown for brevity.

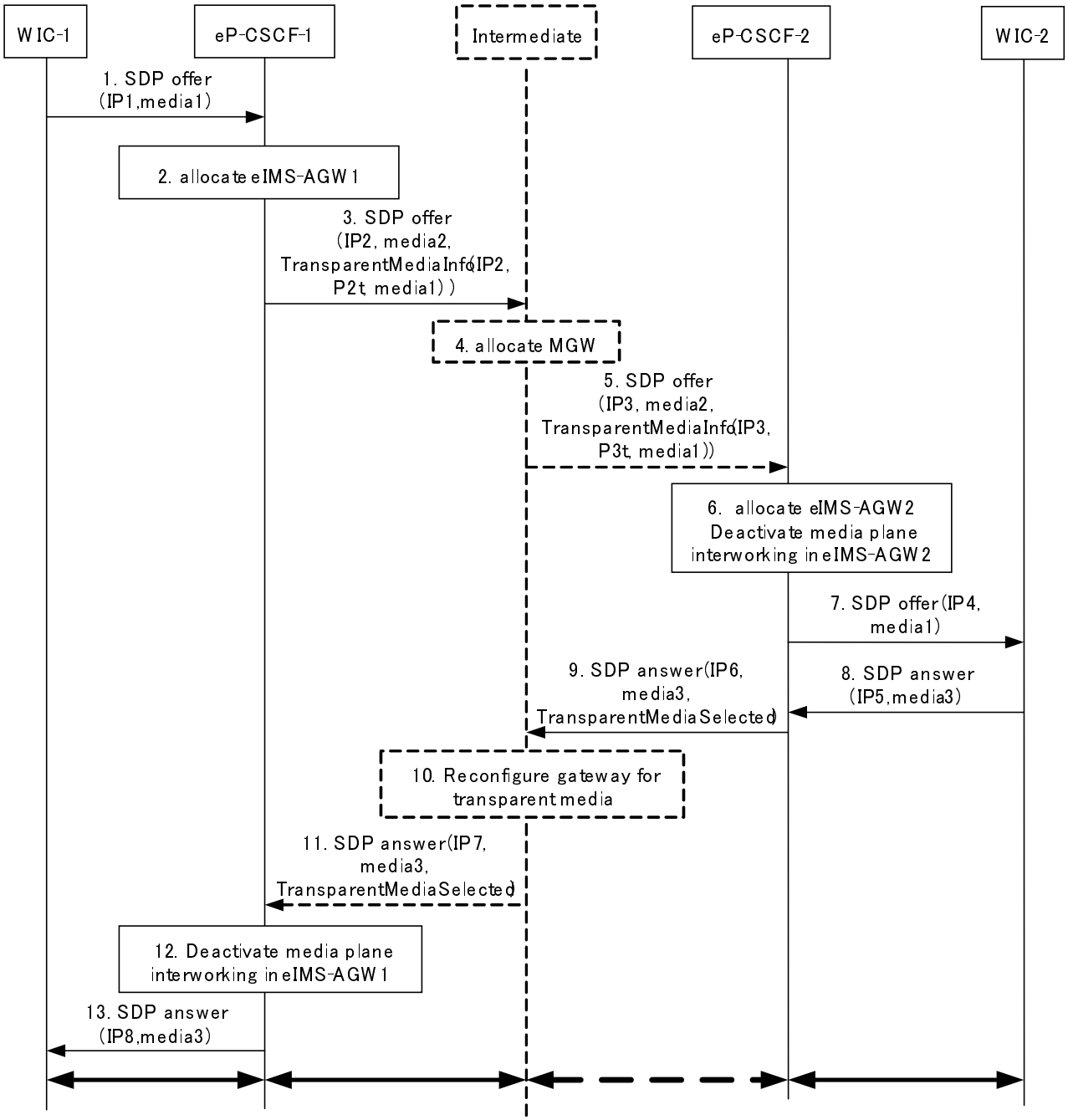


Figure U.2.4-1: Media plane Optimization

1. WebRTC client (WIC-1) initiates a call, creating a Session Description Protocol (SDP) offer and sends it to the originating side eP-CSCF. The SDP offer may contain SRTP, ICE and Data Channel information. The WIC-1 IP address is IP1.

2. The eP-CSCF-1 receives the SDP offer from WIC-1. The eP-CSCF-1 allocates eIMS-AGW1 and configures it to terminate ICE procedures and provide interworking (e.g. transcoding, or transport interworking between a Data Channel and transport outside a Data Channel). eIMS-AGW1 allocates address IP2. It also requests the media gateway to provide a transport port suitable for a transparent forwarding of the media. IMS-AGW1 allocates port P2t for that purpose. Depending on configuration, it either configures the IMS-AGW1to terminate or to transparently forward the DTLS layer for transparent media. The eP-CSCF-1 shall not apply OMR procedures according to Annex Q.

3. The eP-CSCF-1 describes the new media2 that result from the interworking and inserts the address IP2 at the eIMS-AGW1 in the SDP offer connection line it sends. Within the SDP offer, the eP-CSCF-1 also indicates that the media1 targeted for transparent forwarding (those media are called "transparent media" in what follows) can be selected instead and also encapsulates in SDP attribute(s) information about those transparent media (SDP

attributes, SDP media line including transport protocol and port P2t, Data Channel related information, but no ICE related information. A DTLS fingerprint is included, and depending on configuration, it either contains the fingerprint received from the WIC-1 or a fingerprint allocated by eIMS-AGW1). To enable the check in step 6 wether intermediates which do not support switching to the encapsulated media are inserted into the media path, the eP-CSCF-1 also encapsulates the address IP2.

4. A possible intermediate (e.g. IBCF with attached TrGW or MTFC with attached MRFP) may also insert a media gateway into the user plane. Such an intermediate may optionally also support switching to the transparent media; this is required to allow the transparent media to be selected when its media gateway is present in the media path. Intermediates which do not support switching to the transparent media will be detected and will cause media 2 to be selected in step 6.

   The possible intermediate can also apply OMR procedures according to Annex Q to offer that its media gateway is bypassed by an optimised media path.

5 The intermediate replaces the transport address within the connection line in the SDP offer with the address IP3 allocated at its media gateway. If the intermediate supports switching to the transparent media, it also modifies the transparent media information encapsulated in SDP attribute(s) by replacing the encapsulated transport address with IP3 and the port information with P3t.

6. eP-CSCF-2 allocates eIMS-AGW2. It compares the transport address in the SDP connection line with the transport address in the transparent media information encapsulated in SDP attribute(s). Because both addresses match, the eP-CSCF-2 takes the transparent media information into consideration. Otherwise it shall ignore the transparent media information. The eP-CSCF-2 shall not apply OMR procedures according to Annex Q and shall discard any received OMR related information. Because eP-CSCF2 knows that the served WIC-2 is a WIC, it decides that the transparent media information is appropriate and configures the eIMS-AGW2 to transparently forward those media; depending on configuration, eP-CSCF2 either configures the eIMS-AGW2 either transparently forward the DTLS layer or to terminate it, and it either forwards the fingerprint received as part of the transparent media information or a fingerprint allocated by eIMS-AGW2.

7. The eP-CSCF-2 forwards SDP offer with the transparent media1 and the transport address IP4 allocated at eIMS-AGW2 to WIC-2.

8. WIC2 selects media3 from the offered media1 and sends the selected media3 in the SDP answer to the eP-CSCF-2.

9. The eP-CSCF-2 forwards the SDP answer including connection information for eIMS-AGW2 and the unmodified media3, and includes an indication that the transparent media have been selected. Depending on configuration, it either forwards the fingerprint received from WIC2 or a fingerprint allocated by eIMS-AGW2.

10. The possible intermediate reconfigures its MGW to transparently pass media3.

11. The intermediate forwards the SDP answer with unmodified media3 and indication that the transparent media have been selected and includes address information IP7 of the controlled MGW.

12. According to received SDP answer, the eP-CSCF-1 knows that there is no bearer level protocol conversion. So eP-CSCF-1 deactivates media plane interworking in eIMS-AGW1.

13. The eP-CSCF-1 forwards the SDP answer to WIC-1. Depending on configuration, it either forwards the fingerprint received in step 12 or a fingerprint allocated by eIMS-AGW1.

Annex V (normative): IP-Connectivity Access Network specific concepts when using Untrusted WLAN to access IMS

V.1 General

This clause describes the main IP-Connectivity Access Network specific concepts that are used for the provisioning of IMS services over untrusted WLAN access to EPC.

Following specific considerations apply to the case of untrusted WLAN access:

- The Mobility related procedures for untrusted WLAN access to EPC are described in TS 23.402 [82].
  - For untrusted WLAN access, ePDG is used to interface the access network and to control relevant PDN connectivity (over S2b) towards a P-GW.
- For untrusted WLAN access, the way the notification of the loss of IP-CAN session for a UE is triggered within an untrusted WLAN is out of scope of 3GPP specifications.
- For untrusted WLAN access, the Reporting of User location information (i.e. UE local IP address and Network Provided WLAN Location Information) in the EPS is defined in clauses 4.5.7.2.8, 7.4.3.1, 7.9.2, 7.10 and 7.11.14 of TS 23.402 [82] and the related PCC Access Network Information reporting procedure is defined in clause H.4 of TS 23.203 [54]. Information flows on how user location information can be further distributed within IMS can be found in Annex R.
- In order to fulfil regulatory requirements, IMS requires in addition to the UE local IP address, the identity of the ePDG to which the UE is connected, and the UE source port (TCP port or UDP port) used by the UE to establish the IKEv2 tunnel with the ePDG.

NOTE 1: The identity of the ePDG is the IP address used in IKEv2 tunnel.

NOTE 2: The P-CSCF has to subscribe to the IP-CAN type changes with PCRF to be notified when IP-CAN type changes to non 3GPP and the ePDG IP address (and other information) is than provided to the P-CSCF.

V.2 UE Provided Access Information in Untrusted WLAN access

A UE accessing IMS via untrusted WLAN shall support the following:

- If available, provide the identity of the WLAN AP the UE is currently associated with, and used for IMS signalling at IMS registration, IMS emergency registration, IMS session initiation, and in any procedure defined in TS 24.229 [10a], where access network information is provided.
- If available, provide geographical location coordinates during IMS emergency session setup.
- Provide the cell information (cell-ID) for the most recent seen cell at IMS registration, IMS emergency registration, IMS emergency session initiation, and in any procedure defined in TS 24.229 [10a] where access network information is provided. The cell-ID access information shall include additional information describing when the information about the cell-ID was collected and that can be used to calculate the "age" of the information. The information about the cell-ID shall be included in an appropriate field of the SIP request that is distinguished from the information about the access network currently used to transport SIP signalling (i.e. Untrusted WLAN).

NOTE: Operator specific local control policies may be applied and which can result in a registration being accepted, rejected, and/or may also result in additional implementation specific actions. Any node that participates in the registration process (e.g. P-CSCF, HSS) may apply these local control policies.

Annex W (normative): Support of IMS Services for roaming users in deployments without IMS-level roaming interfaces

W.1 General

This clause describes the functions that are used to support IMS services for roaming users in deployments without IMS-level roaming interfaces. This annex is applicable to UTRAN and E-UTRAN using EPC access and to 5GC. In this roaming model the PGW is located in the home PLMN and therefore UE IMS signalling and user plane are routed to home PLMN.

W.2 Architecture

The architecture to support IMS services for roaming users, including Voice over IMS, in deployments without IMS-level roaming interfaces is shown in figure W.2-1

The following architecture requirements apply:

- P-CSCF (at HPLMN) identifies the serving network (VPLMN) where the UE is located using the procedure defined in clause W.3.

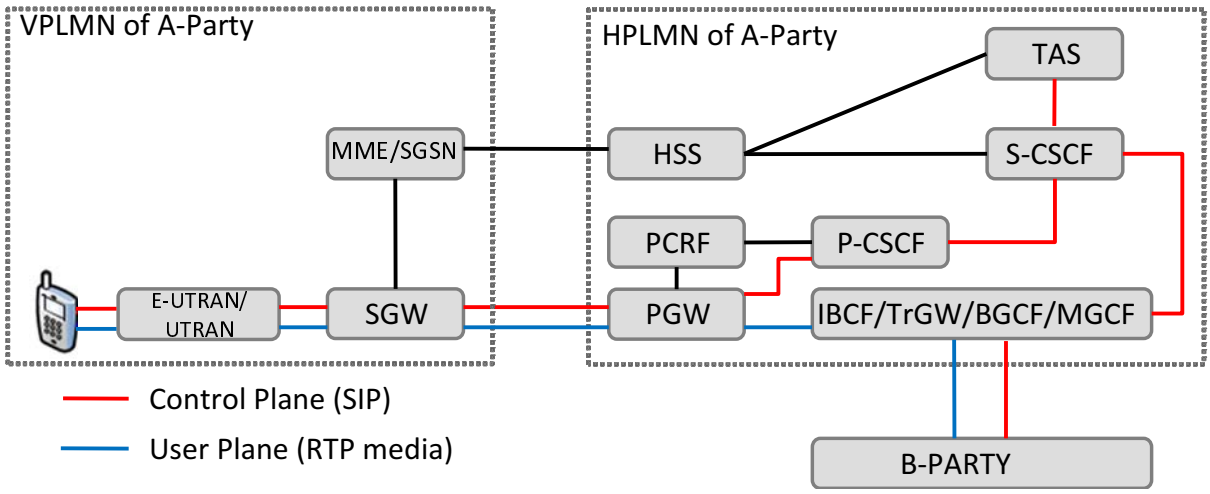


Figure W.2-1: IMS traffic home routed

The corresponding architecture for 5GS is defined in clause Y.9.2.

W.3 Subscription to changes in PLMN ID at IMS Initial Registration

In LBO roaming model where P-CSCF is located in VPLMN (see Annex M.1), the home network determines the serving PLMN of the UE from the location of the P-CSCF during initial IMS Registration, using the P-CSCF network identifier.

In deployments without IMS-level roaming interfaces, the home network determines the serving PLMN of the UE using procedure defined in TS 23.203 [54] or TS 23.503 [95], where P-CSCF requests the PCRF/PCF to report the PLMN identifier where the UE is currently located. The received PLMN ID information is then forwarded in the SIP REGISTER request.

This procedure shall be applied by the P-CSCF at initial UE IMS registration.

The corresponding architecture for 5GS is defined in Annex Y. In this case the P-CSCF interfaces with a PCF instead of interfacing with a PCRF.

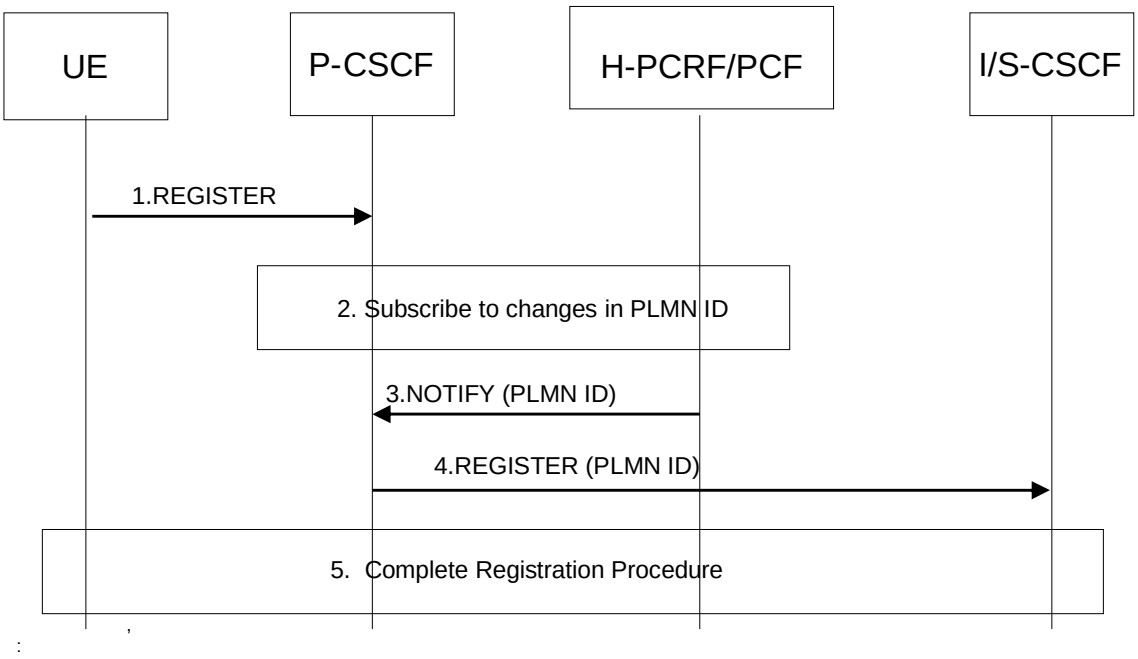


Figure W.3-1: Subscription by P-CSCF to changes in PLMN ID during initial IMS Registration

1. The UE sends a SIP REGISTER request to the P-CSCF.
2. If this is initial IMS registration then the P-CSCF subscribes to the PCRF/PCF to be notified of the PLMN ID where the UE is currently attached.
3. The PCRF/PCF forwards the PLMN ID to the P-CSCF. The P-CSCF stores the PLMN ID.
4. The P-CSCF includes the received PLMN ID in the SIP REGISTER request before forwarding the request to the I-CSCF.
5. Normal IMS registration procedure is then completed.

Annex X (normative): IMS 3GPP PS Data Off Service Accessibility

X.1 General

3GPP PS Data Off is an optional feature. When activated by the user and when the network supports the feature, this feature allows control of the IMS services and more broadly SIP based services using the IMS framework that the user is allowed to access, for both originating and terminating sessions.

The list of 3GPP PS Data Off Exempted Services is configured by the HPLMN in the UE and in the network for enforcement. The list of SIP based service can include any one or any combination of the following services:

- MMTel Voice;
- SMS over IMS;
- MMTel Video;
- USSI;
- Particular IMS Services not defined by 3GPP, where each such IMS service is identified by an IMS communication service identifier.

X.2 UE Behaviour

X.2.1 UE 3GPP PS Data Off Status Reporting

The UE shall include an indication that depicts the 3GPP PS Data Off status (active/inactive) at initial IMS registration, and subsequent to that, any time the end user changes the 3GPP PS Data Off status in a (re-)REGISTER request. In all these registration requests the UE shall register the SIP based services that are configured in the UE.

NOTE: When the 3GPP PS Data Off status is reported, the configured SIP based services in UE are registered as defined in clause B.3.1.0 of TS 24.229 [10a].

The UE and the network shall ensure that the proper services are enforced in accordance with the 3GPP PS Data Off status.

X.2.2 UE Provisioning

The UE may be provisoned by HPLMN with up to two enumerated lists of SIP-based services that are 3GPP PS Data Off exempted either via Device Management or in the UICC, one list is valid for the UEs camping in the home PLMN and the other list is valid for any VPLMN the UE is roaming in. When the UE is configured only with a single list, without an indication to which PLMNs the list is applicable, then this list is valid for the home PLMN and any PLMN the UE is roaming in.

A UE provisioned with an updated list shall enforce the updated list immediately.

X.2.3 UE Enforcement of 3GPP SIP-Based 3GPP PS Data Off Exempt Services

When the UE changes its 3GPP PS Data Off status from inactive to active, the UE shall ensure that only the 3GPP PS Data Off Exempted Services in the provisioned list are allowed to be transported, and the corresponding IP uplink packets shall be sent accordingly as follows:

- The UE shall prevent sending of UE-originating SIP requests which are for services other than the 3GPP PS Data Off Exempted Services configured in the UE via device management or in the UICC.
- The UE shall prevent sending of SDP offers and SDP answers with media streams for the media types other than those related to the 3GPP PS Data Off Exempted Services configured via device management or in the UICC.
- A UE shall immediately stop sending any media packets and shall terminate all ongoing sessions for all SIP-based services that are not 3GPP PS Data Off Exempt.
- A UE provisioned with an updated list shall enforce the updated list immediately. To that effect, the UE shall immediately stop sending any media packets and terminate all ongoing SIP-based sessions handling the 3GPP PS Data Off Exempt Service(s) removed from the list.

X.3 Network Behaviour

X.3.1 Network Update to 3GPP PS Data Off Exempted Services

The HPLMN network shall provision in the UE either via Device Management or in the UICC the lists of 3GPP PS Data Off Exempt Services. Up to two lists are provisioned in the UE for that purpose: one list is used when the UE is at home, while the second list is used when the UE is roaming in any visited PLMN.

The information shall be provisioned in the UE prior to enabling the 3GPP PS Data Off Service. Any change to either one or both lists shall immediately be sent to the UE for enforcement.

X.3.2 Network Enforcement of SIP-Based 3GPP PS Data Off Exempted Services

Application Servers implementing the SIP-based services shall enforce the SIP based 3GPP PS Data Off Exempted services for all UEs.

Each Application Server shall be configured with up to two lists of 3GPP PS Data Off Exempt Services, one list for non-roaming users, and the other list for users roaming in the various VPLMNs with whom roaming agreements exist.

The AS shall become aware of the UE 3GPP Data Off status (active/inactive) at IMS (re-)Registration through third party registration. If the UE has changed its 3GPP PS Data Off status from inactive to active, the AS shall ensure that only SIP-based services which are part of the SIP-based 3GPP PS Data Off Exempt Services are permitted.

If the UE has changed its 3GPP PS Data Off status from active to inactive, the AS shall also let through the terminating requests to the UE for services that were not Data Off exempt.

NOTE 1: The AS could be implemented in an existing AS e.g. SCC AS or distributed across other AS's.

NOTE 2: The operator needs to ensure coordinated lists of 3GPP Data Off Exempt services provisioned in the UE and configured the network.

Annex Y (normative): IP-Connectivity Access Network specific concepts when using 5GS to access IMS

Y.0 General

This clause describes the main IP-Connectivity Access Network specific concepts that are used for the provisioning of IMS services over 5GS.

HSS is used to store IMS related subscription and context as shown in the Figure 4.0 "Reference Architecture" specified in clause 4.0. For 5GS, HSS functionality for IMS shall continue to be as standalone regardless if it is co-located or implemented as part of the UDM. When the HSS and UDM are deployed as separate network functions, their interaction is defined by TS 23.632 [97] and TS 29.563 [98], or it may be implementation specific. A single IMS subscription profile is used regardless of UE accessing IMS via different IP-CANs.

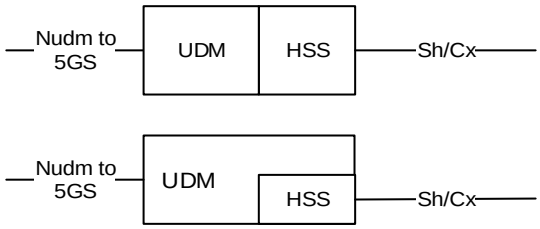


Figure Y.0-1: UDM and HSS collocated or HSS as part of UDM

NOTE: The HSS shown in Figure Y.0-1 is only considering the functionality required for IMS.

From IMS perspective, either the N5 interface as specified in TS 23.503 [95] or the Rx interface as specified in TS 23.203 [54] are used between the P-CSCF and the Policy Control Function (PCF).

NOTE: In PLMNs where both Rx and N5 are used it is implementation specific how the P-CSCF determins the applicable interface/protocol used for a particular interaction with the PCF/PCRF - e.g. Separate P-CSCF's used for Rx and N5, local routing configuration in the P-CSCF.

In 5G System the Gm reference point defined in clause 4.0 and clause 4.4 is supported for the communication between UE and IMS, e.g. related to registration and session control. Therefore, the same interface is used, i.e. Gm, from P-CSCF perspective towards the UE, when UE is in 5G System or any other IP-CAN.

Y.1 Mobility related concepts

Y.1.0 General

To support IMS, the UE shall establish a PDU session with PDU session type set to IP for the corresponding DNN (see TS 23.501 [93], clause 5.6.1), and acquire an IP address according to TS 23.501 [93], clause 5.8.1.1. If IMS Multimedia Telephony Service as specified in TS 22.173 [53] is to be used within the PDU session, SSC mode 1 shall be set for the PDU session. In this release of the specification, it is assumed that single PDU session with multiple PDU session anchors defined in TS 23.501 [93] clause 5.6.4 is not applicable for PDU sessions dedicated to IMS.

NOTE 1: In the case of Dual Registration as defined in TS 23.501 [93], the UE will register (and if needed re-register) in IMS with the IP address of the IMS PDU session when the IMS PDU session is transferred between 5GS and EPS.

If the UE changes its IP address due to changes triggered by the 5GS procedures or due to, for example, PLMN change, then the UE shall re- register in the IMS.

If the UE acquires an additional IP address, then the UE may perform an IMS registration using this additional IP address as the contact address. If IMS registration is performed, this IMS registration may co-exist with the previous IMS registration from this UE and the UE shall be notified that this IMS registration results in multiple simultaneous registrations.

NOTE 2: In this Release of the specification, the UE can acquire an additional IP address that can be used for registration to the IMS only outside of the 5G System.

In Dual Connectivity with 5GC case, the UE shall use the access network information based on the primary cell of the Master RAN node that is serving the UE for network location information when the UE interacts with IMS, regardless whether the IMS traffic is routed via the Master RAN node or the Secondary RAN node or both.

Y.1.1 Procedures for P-CSCF discovery

All the procedures described in clause 5.1.1 apply with the following additions:

- For the option where P-CSCF discovery is part of the IP-CAN connectivity establishment the following applies:
  - P-CSCF discovery shall take place during the PDU session establishment procedure see TS 23.502 [94], clause 4.3.2.

In addition to the procedures in clause 5.1.1, the SMF may determine the P-CSCF using service-based discovery methods (using the NRF), as described in TS 23.501 [93] clause 5.16.3.

Y.2 QoS related concepts

Y.2.1 Application Level Signalling for IMS

Y.2.1.0 General

When the UE uses 5GS-access for IMS services, it shall be possible to establish at least one QoS flow identified by a QFI for IMS signalling.

Y.2.1.1 QoS Requirements for Application Level Signalling

It shall be possible to request prioritised handling over the 5GS system for IMS signalling by applying the appropriate 5QI for the established QoS flow for the IMS signalling, see TS 23.501 [93], clause 5.7.

Y.2.1.2 Void

Y.2.2 The QoS requirements for an IMS session

Y.2.2.0 General

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

- The general requirements described in clause 4.2.5.
- The QoS handling is described in TS 23.501 [93], TS 23.502 [94] and TS 23.203 [54] and TS 23.503 [95].

Y.2.2.1 Relation of IMS media components and 5GS QoS flows carrying IMS media

All associated media 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 5GS QoS flow.

Y.2.3 Interaction between 5GS QoS and session signalling

Y.2.3.0 General

The generic mechanisms for interaction between QoS and session signalling are described in clause 5.4.7. The mechanisms described there and the related procedures througout the present specification are applicable to 5GS-accesses as well with the following clarifications:

- An IP-CAN bearer in this specification shall be interpreted as a 5GS QoS flow.
- An IP-CAN session in this specification shall be interpreted as a 5GS PDU session of type IP.
- The negotiation of the bearer establishment mode does not apply for the 5GS.
- The PCEF corresponds to the combination of SMF and UPF.

Y.2.3.1 Resource Reservation with PCF

The UE or 5GC can initiate the resource reservation request for the media parameters negotiated over SDP using PDU session modification procedure, see TS 23.502 [94], clause 4.3.3. However, for IMS. the network shall initiate the establishment, modification and termination of 5GS QoS flows triggered by negotiated SDP.

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

Y.2.4.0 General

In the event of loss of coverage for 5GS radio access, TS 23.502 [94], clause 4.2.6, defines the N2 release procedure. This procedure releases the QoS flows. This is indicated to the P-CSCF as shown in figure Y.3.

Y.2.4.1 Network initiated session release - P-CSCF initiated

Covers radio coverage loss and that GFBR cannot be maintained by the radio access.

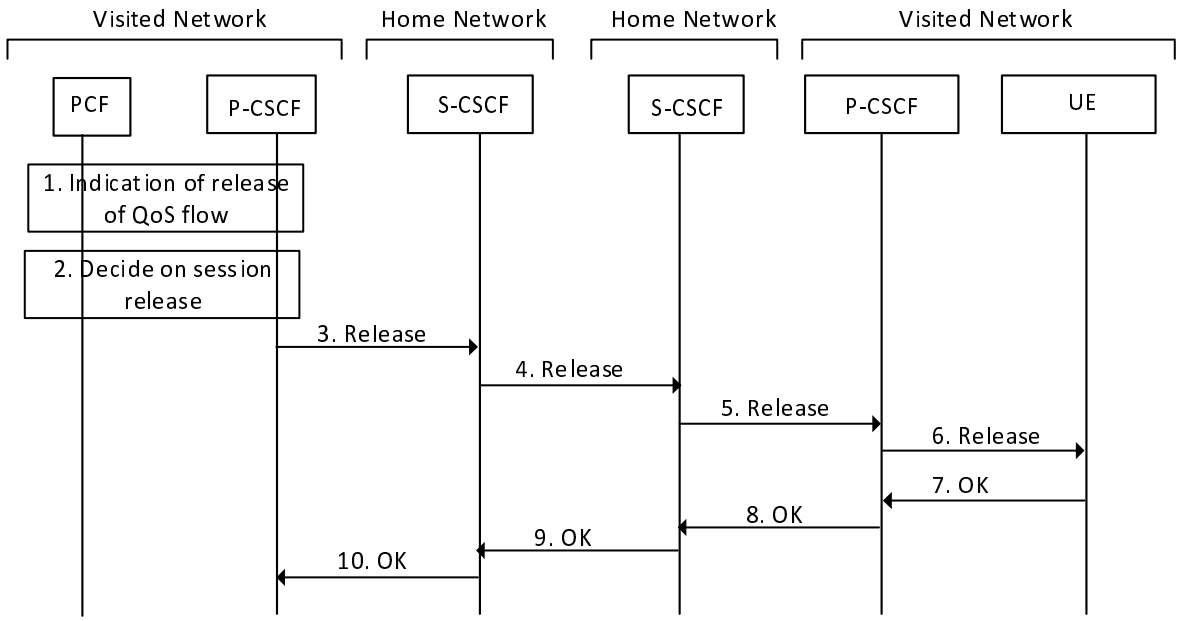


Figure Y.3: Network initiated session release - P-CSCF initiated after loss of radio coverage

1. In the case of loss of radio coverage or that GFBR cannot be retained in NG-RAN, the 5GC may release the related GBR QoS flow and PCF and P-CSCF are notified appropriately.

2. The P-CSCF decides on the termination of the IMS session. In the event of the notification that the signalling transport to the UE is no longer possible, the P-CSCF shall terminate any ongoing IMS session with that specific UE. If the P-CSCF decides to terminate the IMS session, it indicates this to PCF, which removes the authorization for resources that had previously been issued for this endpoint for this session. (see TS 23.503 [95]).

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

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

4. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session. The S-CSCF of the releasing party forwards the Release to the S-CSCF of the other party.

5. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session. The S-CSCF of the other party forwards the Release on to the P-CSCF.

6. The P-CSCF of the other party removes the authorization for resources if they have previously been issued for this endpoint for this session. The P-CSCF forwards the Release to the UE.

7. The UE of the other party responds with a SIP OK to the P-CSCF

8. Depending on the Bearer Control Mode selected for the IP-CAN session, the release of previously reserved resources shall be initiated either by the UE or by the IP-CAN itself. The SIP OK message is sent to the S-CSCF of the other party.

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

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

Y.3 Address and identity management concepts

Y.3.1 Deriving IMS identifiers from the USIM

If the UICC does not contain an ISIM application, and the permanent user identity is IMSI then clause E.3.1 applies.

Y.4 IP version interworking in IMS

A PDU session is associated with either an IPv4 or an IPv6 address. For communication with the IMS, the UE shall acquire an IP address according to TS 23.501 [93], clause 5.8.1.1 for the PDU session. The IP address will be either an IPv4 address or and IPv6 address. Hence, a UE will register to the IMS with either an IPv4 or an IPv6 address. Here the P-CSCF and IMS-AGW may support both IP versions and/or may do interworking depending IP version used within the IMS. If the P-CSCF and IMS-AGW do not support both versions, then network design is expected to ensure that IP address incompatibility does not occur.

Y.5 Usage of NAT in 5GS

There should be no NAT (or its existence should be kept transparent towards the UE) located between the UPF and the P-CSCF, which is possible as they are either located within the same private network and share same address space, or both the UE and the P-CSCF are assigned globally unique IP addresses (see Annex M).

NOTE: If the UE discover a NAT between the UE and the P-CSCF, the UE might send frequent keep-alive messages and that may drain the UE battery.

Y.6 Retrieval of Network Provided Location Information in 5GS

Information related to the location of the user provided by the access network may be required in IMS in order to comply with regulatory requirements (e.g. data retention, lawful interception) and/or in order to enable certain types of added value services based on the user's location.

Depending on usage scenario, the following mechanisms are defined and can be used to retrieve the user location and/or UE Time Zone information from the access network when using 5GS to access IMS:

- The P-CSCF can retrieve the user location and/or UE Time Zone information using PCC mechanisms as specified in TS 23.203 [54] / TS 23.503 [95] and in TS 29.214 [11]. Operator policy determines whether to provide the user location and/or UE Time Zone information from the access network in the INVITE request or within a subsequent message of the dialog.

- When the user location and/or UE Time Zone information is required from the access network but not already available (e.g. when required in an INVITE request, when it is needed prior to session delivery, or when call is broken out to a MGCF), an IMS AS can trigger the retrieval of the user location and/or UE Time Zone information from the AMF via the HSS/UDM as specified in TS 29.328 [79] and as described in clause 4.2.4a.

Information flows on how user location and/or UE Time Zone information can be further distributed within IMS depending on the alternative mechanism used can be found in, Annex R, where the terms HSS and HSS/UDM shall be understood as in clause Y.0.

The level of granularity of user location information may be changed at network/trust boundaries. Thus, the level of user location information granularity that can be retrieved by an IMS AS via the HSS/UDM-based procedures in roaming scenarios depends on inter-operator agreement, and needs to be aligned with policies in the P-CSCF.

Y.7 Geographical Identifier

A network which requires the Geographical Identifier to be generated in the IMS may implement a mapping table between a NG-RAN cell identifier received as part of Access Network Information and a Geographical Identifier. The P-CSCF or an IMS AS may then, based on operator policy, use this mapping table to convert the user location into a Geographical Identifier, and insert the Geographical Identifier in the SIP signalling, thus enabling routing decision in downstream IMS entities or interconnected network.

Y.8 Support for Paging policy differentiation for IMS services

P-CSCF may support Paging Policy Differentiation (as defined in TS 23.501 [93]) for a specific IMS service by marking packet(s) to be send towards the UE related to that IMS service. For such an IMS service, a specific DSCP (IPv4) value and/or a specific Traffic Class (IPv6) value are assigned by local configuration in the P-CSCF.

When Paging Policy Differentiation is deployed in a PLMN, all P-CSCF entities of that PLMN shall homogeneously support it and shall be configured with the same policy for setting the specific DSCP (IPv4) and/or Traffic Class (IPv6) values used by P-CSCF for that feature.

NOTE: It is assumed that the DSCP / Traffic Class header is not rewritten by intermediate routers between the P-CSCF and the UPF.

Y.9 Support of IMS Services for roaming users

Y.9.1 General

This clause describes support for IMS services for roaming users using IMS level roaming interfaces or without IMS level roaming interfaces.

Y.9.2 Architecture without IMS-level roaming interfaces

This clause describes the functions that are used to support IMS services for roaming users in deployments without IMS-level roaming interfaces. In this roaming model the UPF holding the UE's IP point of presence is located in the home PLMN and therefore UE IMS signalling and user plane are routed to home PLMN.

The architecture to support IMS services for roaming users, including Voice over IMS in deployments without IMS-level roaming interfaces is shown in figure Y.9.2-1.

The following architecture requirements apply:

- P-CSCF (in HPLMN) identifies the serving network (VPLMN) where the UE is located using the procedure defined in clause Y.9.3.

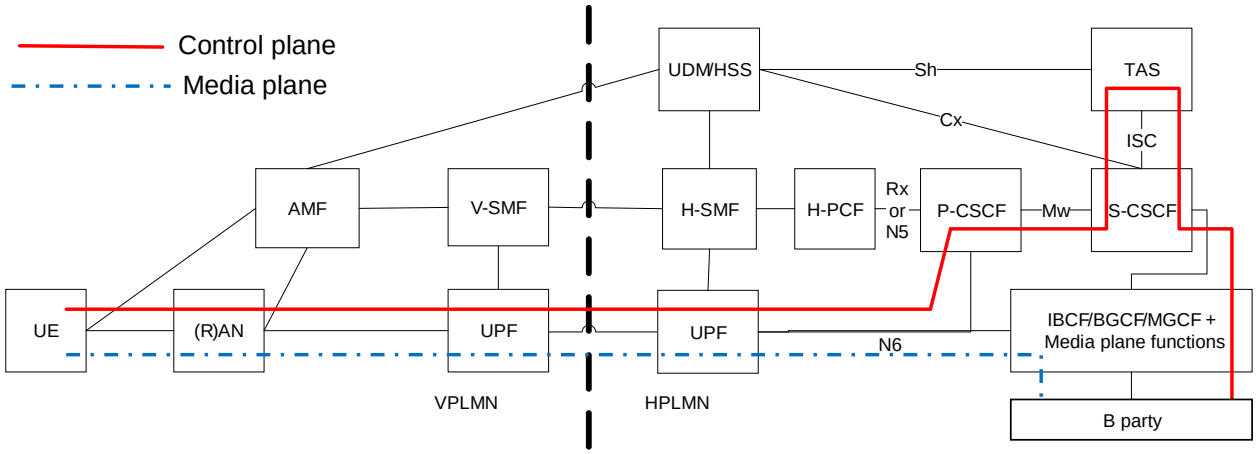


Figure Y.9.2-1: IMS traffic home routed

Y.9.3 Architecture with IMS-level roaming interfaces

For IMS services with roaming level interfaces the P-CSCF and UPF are located in VPLMN (local breakout), see clauses 4.2.3 and M.1. For roaming architecture for voice over IMS with local breakout see clause 4.15a. For information on how to apply the loopback possibility in clause 4.15a, see clause M.3.

Y.9.4 Subscription to changes in PLMN ID at IMS Initial Registration

In IMS local breakout where P-CSCF is located in VPLMN (see Annex M.1 and Annex M.3), the home network determines the serving PLMN of the UE from the location of the P-CSCF during initial IMS Registration, using the P-CSCF network identifier.

In deployments without IMS-level roaming interfaces, the home network determines the serving PLMN of the UE using procedure defined in TS 23.503 [95], where P-CSCF requests the PCF to report the PLMN identifier where the UE is currently located. The received PLMN ID information is then forwarded in the SIP REGISTER request.

This procedure shall be applied by the P-CSCF at initial UE IMS registration.

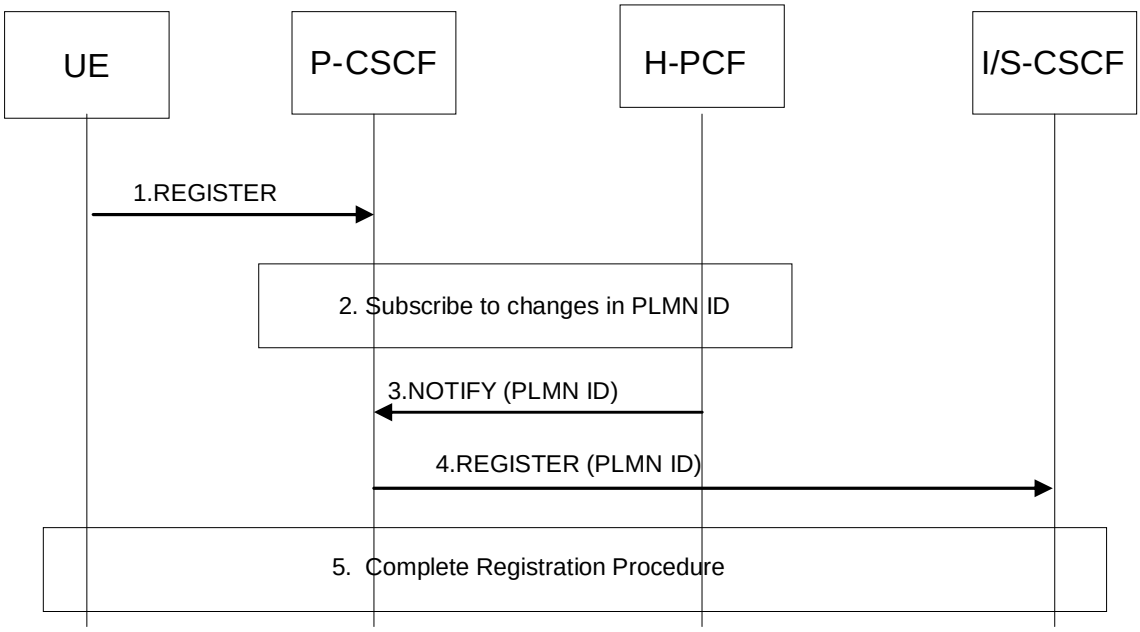


Figure Y.9.4-1: Subscription by P-CSCF to changes in PLMN ID during initial IMS Registration

1. The UE sends a SIP REGISTER request to the P-CSCF.
2. If this is initial IMS registration then the P-CSCF subscribes to the PCF to be notified of the PLMN ID where the UE is currently attached.

3. The PCF forwards the PLMN ID to the P-CSCF. The P-CSCF stores the PLMN ID.

4. The P-CSCF includes the received PLMN ID in the SIP REGISTER request before forwarding the request to the I-CSCF.
5. Normal IMS registration procedure is then completed.

Y.10 Support of RAN Assisted Codec Adaptation

RAN assisted codec adaptation is supported as described in clause E.10 with the addition that RAN assisted codec adaptation needs to be supported on NR RAT as specified in TS 38.300 [101] and TS 38.321 [102], in addition to E-UTRA RAT.

Y.11 Void

Y.12 P-CSCF Registration in NRF

In order to support service based SMF discovery of the P-CSCF using the NRF (as described in TS 23.501 [93] clause 5.16.3) the P-CSCF's in a network will need to register with an applicable NRF. When a network uses other P-CSCF discovery methods (as described in clause 5.1.1) the P-CSCF does not need to register with the NRF. Local configuration of the P-CSCF is used to determine if the P-CSCF shall perform registration with the NRF.

When the P-CSCF is configured to support SMF discovery of the P-CSCF, P-CSCF shall register in NRF their capabilities using the Nnrf_NFManagement_NFRegister Request message. The NF profile of the P-CSCF registered in NRF shall include the IP address and may include an FQDN if available. The same applies to the Nnrf_NFManagement_NFUpdate Request.

Based on the same configuration, a P-CSCF taken out of service will deregister itself using the Nnrf_NFManagement_NFDeregister Request.

Y.13 Subscription to EPS Fallback Event

Based on local configuration in the case of an originating or a terminating session, the P-CSCF may subscribe to the PCF for notification for the EPS Fallback event using existing procedures defined in TS 23.503 [95].

If the PCF reports that an EPS fallback occurred, based on local configuration, the P-CSCF may include this information in outgoing SIP messages towards other IMS nodes.

Annex Z (normative): Support of IMS-based Restricted Local Operator Services (RLOS)

Z.1 General

This clause describes the required functions to support IMS-based restricted local operator services (RLOS). RLOS services are operator owned services that are offered to the following categories of subscribers:

- Roaming users who are subscribers of other operators with whom the local operator has no roaming agreement, or the local operator cannot communicate with their network.
- Roaming users who are subscribers of other operators with whom the local operator has roaming agreements for IMS services and for Restricted Operator Local Services.
- Operator own subscribers who roamed in cells with restricted services. These subscribers may or may not have been successfully authenticated prior to roaming in cells with restricted services.

NOTE: Operator restricted services can also be offered to the local operator own subscribers roaming in unrestricted areas, however this is out of scope.

RLOS is used only for originating services.

In this version of the specification, RLOS is only defined for users connected to IMS over EPS (see TS 23.401 [70]);

Z.2 Architecture

Support for RLOS requires additional functionalities in the P-CSCF, I- CSCF, and S-CSCF as will be depicted below. The additional functionality can be built on the existing functionality to support RLOS and non-RLOS IMS services. Optionally, dedicated IMS nodes (P/I/S-CSCFs) supporting only RLOS can be deployed.

NOTE: Architecture for roaming scenarios without IMS-level roaming agreement (as defined in Annex W) does not apply to RLOS users accessing IMS.

Z.3 IMS Registration to access RLOS

Z.3.1 RLOS IMS Registration for Roaming users (no roaming Agreements with home network)

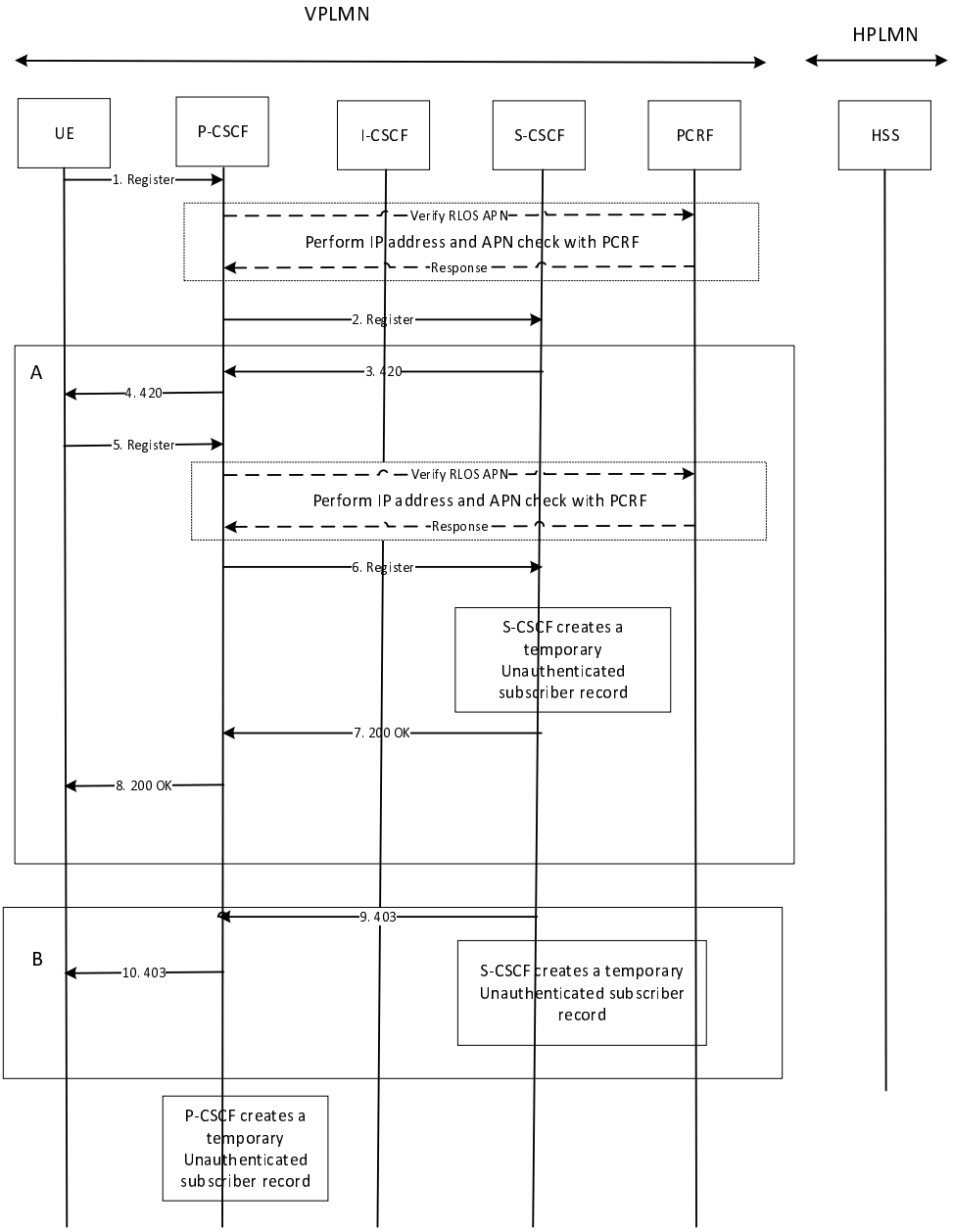


Figure Z.3.1-1: RLOS IMS Registration procedures for roaming users without roaming agreements with their home network

1. After the UE has obtained IP connectivity (as defined in TS 23.401 [70] for RLOS users), it performs regular IMS registration and includes an indication that this is an RLOS related IMS registration in the Register information.

2. The P-CSCF is a P-CSCF that supports RLOS, and upon receipt of the Register information, optionally, and based on operator policy performs the security checks in clause Z.3.3. Based on the subscriber being a roaming user without roaming agreement with his home network, and the RLOS indication in the Register information, the P-CSCF shall send the Register information to the S-CSCF configured in the P-CSCF to handle RLOS users.

NOTE: The P-CSCF ID for handling RLOS would have been sent to the UE during the Attach procedure which included an explicit indication to access RLOS.

Steps 3-8 apply if the S-CSCF has responded with 420 response.

3. Upon receipt of the Register information, the S-CSCF, based on the RLOS indication and the subscriber being a roaming user without roaming agreement with his home network and depending on the network configuration, and if the network supports GIBA, sends back a 420 response with sec-agree value listed in the unsupported header field.

4. The P-CSCF forwards the 420 response to the UE.

5. The UE initiates a new Register request and does not include the Authorization header field.

6. The P-CSCF optionally performs the RLOS APN verification in clause Z.3.3, then sends the Register information to the S-CSCF allocated to the UE.

7. Upon receipt of the Register information, the S-CSCF shall accept the Registration, creates a temporary record for the unauthenticated UE with a default service profile and responds with a 200 OK.

8. The P-CSCF sends the 200 OK to the UE.

Steps 9-10 apply if the S-CSCF has responded with 403 response.

9. Upon receipt of the Register information, the S-CSCF, based on the RLOS indication and the subscriber being a roaming user without roaming agreement with his home network and depending on the network configuration as well as operator configuration (no support for GIBA), responds with a 403 response. The S-CSCF creates a temporary registration record for the unauthenticated UEs with a default service profile.

10. The P-CSCF sends the 403 response to the UE. The P-CSCF creates a temporary registration record for the unauthenticated UE given that the subscriber is a roaming user without roaming agreement with his home network. The UE is allowed to initiate an IMS session.

Z.3.2 RLOS IMS Registration for Operator own subscribers and Roaming users with roaming agreements with their home network

Operator own subscribers, and/or roaming users with IMS services and Restricted Local Operator Services roaming agreement with their home network, shall perform a new IMS registration, as specified below, to access IMS-based Restricted Local Operator Services upon roaming in cells with restricted services. The UE shall also delete any valid IMS registration performed by the UE prior to roaming in cells with restricted services.

Z.3.2.1 Unsuccessful IMS Registration

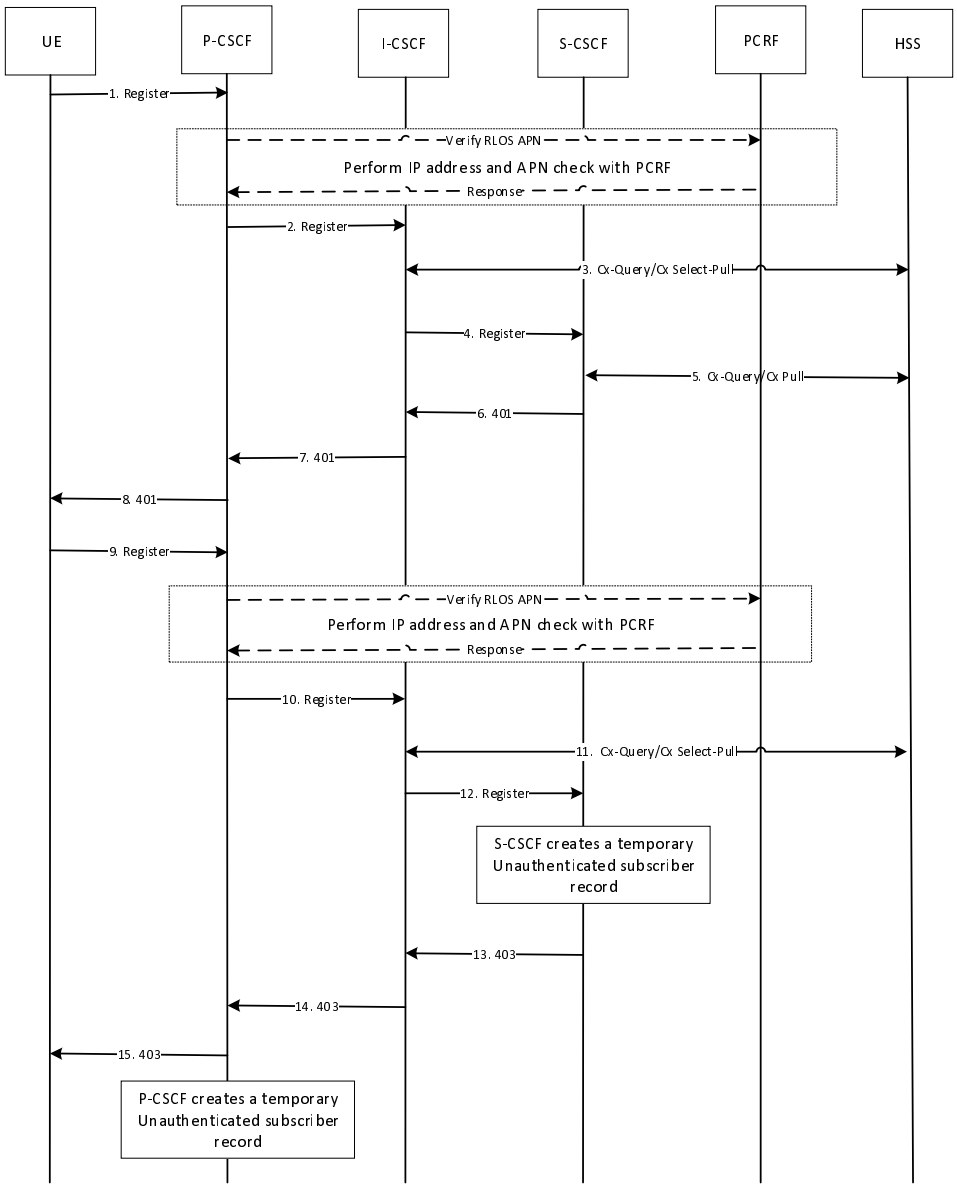


Figure Z.3.2.1-1: Unsuccessful RLOS IMS Registration procedure

1. After the UE has obtained IP connectivity (as defined in TS 23.401 [70] for RLOS users), it performs regular IMS registration and includes an indication that this is an RLOS IMS related registration in the Register information.

2. The P-CSCF is a P-CSCF that supports RLOS, and upon receipt of the Register information optionally, and based on operator policy, performs the RLOS APN verification in clause Z.3.3. The P-CSCF based on the RLOS indication and the subscriber being its own subscriber sends the Register information to the I-CSCF.

NOTE 1: The P-CSCF ID for handling RLOS would have been sent to the UE during the Attach procedure which included an explicit indication to access RLOS.

3. The I-CSCF queries HSS for the subscriber S-CSCF. If the I-CSCF determines based on configuration that the received S-CSCF does not support RLOS and since this is an RLOS related registration, the I-CSCF queries HSS again for required S-CSCF capabilities in the user profile. The I-CSCF shall use the returned S-CSCF capability information and in addition configured information about S-CSCF support for RLOS to select a S-CSCF.

NOTE 2: The S-CSCF allocated to a subscriber may be from an old registration that did not expire and is not deleted, or for an RLOS related registration. The S-CSCF support of RLOS is preconfigured in the I-CSCF rather than a capability stored in the user profile within the HSS as otherwise RLOS support would be a requirement for the S-CSCF selection even if the registration is not for RLOS.

4. The I-CSCF sends the Register information to the selected S-CSCF.
5. The S-CSCF fetches the authentication information from HSS.
6. The S-CSCF challenges the UE by sending a 401 response.
7. The I-CSCF forwards the 401 response to the P-CSCF.
8. The P-CSCF forwards the 401 response to the UE.
9. The UE sends a new Register request to the P-CSCF including the authentication information.
10. The P-CSCF optionally and based on operator policy, performs the RLOS APN verification in clause Z.3.3, then sends the Register information to the I-CSCF.
11. The I-CSCF queries HSS for the subscriber S-CSCF and receives the S-CSCF name allocated to the UE. If the I-CSCF determines based on configuration that the received S-CSCF does not support RLOS and since this is an RLOS related registration, the I-CSCF queries HSS again for required S-CSCF capabilities in the user profile. The I-CSCF shall use the returned S-CSCF capability information and in addition configured information about S-CSCF support for RLOS to select a S-CFCF.
12. The I-CSCF sends the Register information to the selected S-CSCF.
13. The S-CSCF validates the UE received authentication information but failed to successfully authenticate the UE. Since this is an RLOS related IMS registration, the S-CSCF creates a temporary "unauthenticated subscriber" registration record for the UE with a default service profile and responds with a 403 response.
14. The I-CSCF sends the 403 response to the P-CSCF.
15. The P-CSCF sends the 403 response to the UE, and creates a temporary "unauthenticated subscriber" registration record for the UE.

Z.3.2.2 Successful IMS Registration

A successful IMS registration is identical to the failed one with following exceptions:

- The S-CSCF successfully authenticates the UE in step 12.
- The S-CSCF tags the UE registration record as being successfully RLOS registered.
- The S-CSCF updates HSS with the S-CSCF name being allocated to the UE, downloads the UE profile from HSS, and stores it. This step is not performed in the previous case.
- The P-CSCF tags the UE registration record as being successfully RLOS registered.

Z.3.3 RLOS APN Verification

The P-CSCF may be configured with a range of IP addresses dedicated to UEs requesting access to RLOS. These addresses, if configured, shall be checked against the contact information received by the P-CSCF Register information at IMS registration.

Furthermore, the P-CSCF shall validate that an incoming IMS registration did indeed use the APN dedicated to RLOS by the access network. To that effect, the P-CSCF shall indicate to the PCRF that the UE requests access to RLOS. The PCRF shall then validate whether the UE uses the APN dedicated to RLOS and otherwise reject the related Rx session with the indication that the UE is not using the APN dedicated to RLOS. Upon reception of such an indication from the PCRF, the P-CSCF shall reject the IMS registration.

Z.4 IMS-based RLOS Session Initiation

Clause 5.6.2 applies with the following additional requirements:

- The UE shall include an RLOS indication in all originating sessions. The P-CSCF shall reject an originating session without such an indication.
- The S-CSCF shall include the RLOS indication in its charging data related to an IMS session.
- The S-CSCF shall forward the session initiation request to the Telephony Application Server. The Telephony Application Server shall bypass originating services for all successfully authenticated UEs. The Telephony Application Server, based on operator policy, may be configured with different policies (e.g. set of destinations) for all of the above registration cases. The Telephony Application Server shall enforce these policies.
- The S-CSCF shall include the RLOS indication in its charging data related to an IMS session.
- The registered identity shall be used as the asserted identity.

Annex AA (normative): Support of SBA in IMS

AA.1 General

AA.1.0 Overview

This Annex AA describes support for SBA for IMS nodes. This Annex is intended to be used in conjunction with 5GC.

AA.1.1 Architectural Support

Figure AA.1.1-1 shows the architecture to support SBA interactions between IMS entities.

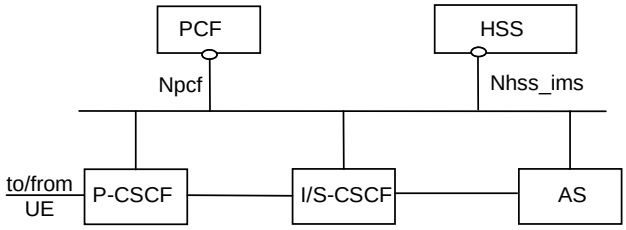


Figure AA.1.1-1: System Architecture to support SBA in IMS

Figure AA.1.1-2 shows the architecture using the reference point representation.

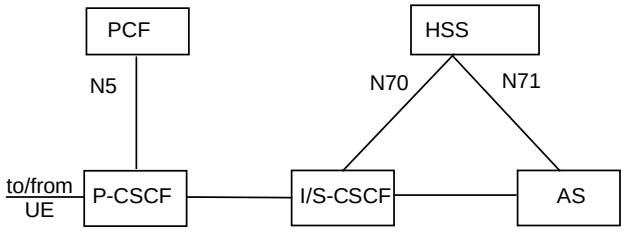


Figure AA.1.1-2: System Architecture to support SBA in IMS in reference point representation

AA.1.2 Reference point to support SBA in IMS

Following reference points are realized by service-based interfaces in IMS:

N5: Reference point between the PCF and an AF.

NOTE: P-CSCF acts as an AF from PCF point of view. N5 Reference point is defined in TS 23.501 [93].

N70: Reference point between an SBI capable I/S-CSCF and an SBI capable HSS.

N71: Reference point between an SBI capable IMS AS and an SBI capable HSS.

AA.1.3 Service based interface to support SBA in IMS

Npcf: Service-based interface exhibited by PCF.

Nhss: Service-based interface exhibited by an SBI capable HSS.

These SBI services provide equivalent functionality to the Diameter Rx and Cx/Sh reference points.

To support co-existence of IMS nodes supporting SBA services and IMS nodes not supporting SBA services SBI enabled IMS nodes may support both SBI and non-SBI interfaces.

AA.2 IMS SBA Services

AA.2.1 HSS Services

AA.2.1.1 General

The following table shows the services exposed by an SBI capable HSS.

Table AA.2.1.1-1: IMS Services provided by an SBI capable HSS

Service	Service Operations	Operation Semantics	Example Consumer(s)
imsSubscriber Data Management (_ImsSDM)	Get	Request/Response	S-CSCF, I-CSCF, AS
	Subscribe	Subscribe/Notify	AS
	Unsubscribe	Subscribe/Notify	S-CSCF, AS
	Notification	Subscribe/Notify	S-CSCF, AS
	Update	Request/Response	AS
imsUE Context Management (_ImsUECM)	Registration	Request/Response	S-CSCF
	DeregistrationNotification	Subscribe/Notify	S-CSCF
	Deregistration	Request/Response	S-CSCF
	Authorize	Request/Response	I-CSCF
	Update	Request/Response	S-CSCF
	RestorationInfoGet	Request/Response	S-CSCF
	RestorationInfoUpdate	Request/Response	S-CSCF
ImsUE Authentication	Get	Request/Response	S-CSCF

AA.2.1.2 Nhss_ImsUEContextManagement (ImsUECM) service

AA.2.1.2.1 Nhss_ImsUECM_Registration service operation

Service operation name: Nhss_ImsUECM_Registration

Description: This service operation registers the serving S-CSCF assigned to an IMS User. If authentication is not to be performed, this operation also sets the registration state. The S-CSCF is implicitly subscribed to be notified when it is deregistered in HSS. This notification is done by means of Nhss_ImsUECM_DeregistrationNotification operation.

Inputs, Required: Public Identity, S-CSCF name, Registration Type (e.g. Initial Registration, Unregistered).

Inputs, Optional: Private Identity.

Outputs, Required: Result indication.

Outputs, Optional: List of registered Private Identities sharing the same Public Identity which is being registered, S-CSCF Restoration indication.

AA.2.1.2.2 Nhss_ImsUECM_Deregistration service operation

Service operation name: Nhss_ImsUECM_Deregistration

Description: This service operation deregisters the S-CSCF allocated to a public identity.

Inputs, Required: S-CSCF name, Deregistration Type.

Inputs, Optional: User Identity (Private Identity and/or Public Identity), P-CSCF Restoration indication, Session Priority.

Outputs, Required: Result indication.

Outputs, Optional: None.

AA.2.1.2.3 Nhss_ImsUECM_DeregistrationNotification service operation

Service operation name: Nhss_ImsUECM_DeregistrationNotification

Description: This service operation enables HSS to inform a S-CSCF which has previously registered in HSS of a Public Identity deregistration. This notification corresponds to an implicit subscription.

Inputs, Required: Private Identity, Reason for Deregistration.

Inputs, Optional: Public Identity, Associated Private Identities.

Outputs, Required: Result indication.

Outputs, Optional: Associated Private Identities, Identities with Emergency Registration.

AA.2.1.2.4 Nhss_ImsUECM_Authorize service operation

Service operation name: Nhss_ImsUECM_Authorize

Description: This service operation is used by the I-CSCF to request authorization from HSS for:

- The registration of a Public Identity by a UE in a P-CSCF network identifier according to the IMS User's subscription and operator limitations/restrictions.
- The reception of a terminating request based on the user state and IMS user's subscription (e.g. IMS User's barring status).

If the IMS User is authorized, the HSS may provide the address of the S-CSCF assigned to the Public Identity if any.

Additionally, this service operation is used to authorize in HSS a S-CSCF reselection (e.g. after I-CSCF detection if a S-CSCF failure).

Inputs, Required: Public Identity, Authorization Type.

Inputs, Optional: Private User Identity, P-CSCF network identifier.

Outputs, Required: Result indication.

Outputs, Optional: S-CSCF name.

AA.2.1.2.5 Nhss_ImsUECM_Update service operation

Service operation name: Nhss_ImsUECM_Update

Description: This service operation updates the registration state of a Public Identity or Private Identity in HSS i.e. to update the registration state from Not Registered or Unregistered to Registered state.

NOTE: This operation is used by S-CSCF after successful authentication to set the registration state (if not already set).

Inputs, Required: Public Identity, S-CSCF name.

Inputs, Optional: Private Identity.

Outputs, Required: Result indication.

Outputs, Optional: None.

AA.2.1.2.6 Nhss_ImsUECM_RestorationInfoGet service operation

Service operation name: Nhss_ImsUECM_RestorationInfoGet

Description: This service operation is used between the S-CSCF and the HSS to retrieve information from HSS to support the S-CSCF procedures.

Inputs, Required: Public Identity.

Inputs, Optional: Private Identity.

Outputs, Required: Result Indication.

Outputs, Optional: Restoration data.

AA.2.1.2.7 Nhss_ImsUECM_RestorationInfoUpdate service operation

Service operation name: Nhss_ImsUECM_RestorationInfoUpdate

Description: This service operation is used between the S-CSCF and the HSS to update information in HSS to support the S-CSCF Restoration procedures.

Inputs, Required: Private Identity, Public Identity, Restoration data.

Inputs, Optional: None.

Outputs, Required: Result indication.

Outputs, Optional: None.

AA.2.1.3 Nhss_ImsSubscriberDataManagement (ImsSDM) service

AA.2.1.3.1 General

IMS Subscriber data types used in the Nhss_ImsSDM Service are defined in Table AA.2.1.3.1-1 below.

NOTE: IMS Subscriber data is terminology only used in Annex AA. It includes IMS subscription data and other data related to the subscriber, e.g. network functionality entity address, location information or T-ADS information.

Table AA.2.1.3.1-1: IMS Subscriber data types

IMS Subscriber data	Description
Service Profile Data	This may include e.g. service parameters, the S-CSCF allocated to a public identity or the list of S-CSCFs and their capabilities, Application Server address, triggers, information on subscribed media, profile parameters (e.g. barring indicator, etc.) as defined in TS 29.228 [30]. **Service Profile Data is consumed by CSCF.**
Repository Data	Data that is understood syntactically but not semantically by the HSS (unstructured Data). It is data that an AS may store in the HSS to support its service logic. One example is data that an AS stores in the HSS, using it as a repository. Service Indication identifies the set of service related transparent data associated to a Public Identity. **Repository Data is consumed by IMS-AS.**
Non-Transparent Data	Data that is understood both syntactically and semantically by the HSS e.g. location information. Non-Transparent Data is structured using data references as defined in TS 29.328 [79]. **Non-Transparent Data is consumed by IMS-AS.**

At least a mandatory key is required for each IMS Subscriber Data Type to identify the corresponding data as defined in Table AA.2.1.3.1-2 below.

Table AA.2.1.3.1-2: IMS Subscriber data types keys

IMS Subscriber Data Types	Data Key	Data Sub Key
Service Profile Data	Public Identity	
Repository Data	Public Identity	Service Indication
Non-Transparent Data	See NOTE 1	
NOTE 1: TS 29.328 [79] defines the data keys/subkeys required by each data reference.		

AA.2.1.3.2 Nhss_ImsSDM_Get service operation

Service operation name: Nhss_ImsSDM_Get

Description: This service operation enables the NF consumer to fetch the service profile data, repository data, and non-transparent data references for an IMS User.

The HSS shall check that the requested NF consumer is authorized to fetch the requested data. In the case that the requested data is Repository data, the HSS may also authorize based on service indication.

Inputs, Required: NF Type, IMS Subscriber data type(s), Key for each IMS Subscriber data type(s).

Inputs, Optional: Application Service Identity.

Outputs, Required: Result indication.

Outputs, Optional: Requested Data.

AA.2.1.3.3 Nhss_ImsSDM_Subscribe service operation

Service operation name: Nhss_ImsSDM_Subscribe

Description: The NF consumer subscribes for updates to requested data. HSS shall check that the requested NF consumer is authorized to subscribe to requested updates.

Inputs, Required: NF Type, IMS Subscriber data type(s), Key for each IMS Subscriber data type(s).

Inputs, Optional: Application Server Identity.

Outputs, Required: When the subscription is accepted: Subscription Correlation ID.

Outputs, Optional: None.

AA.2.1.3.4 Nhss_ImsSDM_Unsubscribe service operation

Service operation name: Nhss_ImsSDM_Unsubscribe

Description: The NF consumer unsubscribes for updates to Requested data.

Inputs, Required: Subscription Correlation ID.

Inputs, Optional: None.

Outputs, Required: Result.

Outputs, Optional: None.

AA.2.1.3.5 Nhss_ImsSDM_Notification service operation

Service operation name: Nhss_ImsSDM_Notification

Description: This service operation enables HSS to notify a NF of any changes to what the NF subscribed to.

Inputs, Required: IMS Subscriber data type(s), Key for each IMS Subscriber data type(s).

Inputs, Optional: None.

Outputs, Required: Result indication.

Outputs, Optional: None.

AA.2.1.3.6 Nhss_ImsSDM_Update service operation

Service operation name: Nhss_ImsSDM_Update

Description: The NF consumer updates HSS subscription data if authorized to do so.

Inputs, Required: NF Type, IMS Subscriber data type(s), Key for each IMS Subscriber data type(s).

Inputs, Optional: Application Service Identity.

Outputs, Required: Result.

Outputs, Optional: None.

AA.2.1.4 Nhss_ImsUEAuthentication service

AA.2.1.4.1 Nhss_ImsUEAuthenticate_Get service operation

Service operation name: Nhss_ImsUEAuthenticate_Get

Description: This service operation is used between the S-CSCF and the HSS to exchange information to support the authentication between the end user and the home IMS network.

Inputs, Required: Private User Identity, Public User Identity, Authentication Data (Authentication Scheme).

Inputs, Optional: Authentication Data (Authentication Context, Authorization Information).

Outputs, Required: Result Indication.

Outputs, Optional: User Identity, Authentication Data (e.g. AV).

AA.2.2 Mapping of Cx and Sh operations and terminology to HSS SBI services

AA.2.2.1 General

This clause gives mappings from Cx and Sh operations to HSS SBI services and service operations.

AA.2.2.2 Mapping of Cx messages to HSS SBI services

The following table defines the mapping between stage 2 Cx messages and HSS SBI services and service operations:

Table AA.2.2.2-1: Cx messages to HSS SBI services and service operations mapping

Cx message	Source	Destination	HSS SBI service operation name
Cx-Query	I-CSCF	HSS	Nhss_ImsUECM_Authorize
Cx-Select-Pull	I-CSCF	HSS	Nhss_ImsSDM_Get (see NOTE 1)
Cx-Put	S-CSCF	HSS	Nhss_ImsUECM_Registration (see NOTE 2) Nhss_ImsUECM_Deregistration (see NOTE 3) Nhss_ImsUECM_Update (see NOTE 4) Nhss_ImsUECM_RestorationInfoUpdate (see NOTE 5)
Cx-Pull	S-CSCF	HSS	Nhss_ImsSDM_Get (see NOTE 6) Nhss_ImsSDM_Subscribe (see NOTE 6) Nhss_ImsSDM_Unsubscribe Nhss_ImsUECM_RestorationInfoGet (see NOTE 7)
Cx-Location-Query	I-CSCF	HSS	Nhss_ImsUECM_Authorize Nhss_ImsSDM_Get (see NOTE 8)
Cx-AuthDataReq	S-CSCF	HSS	Nhss_ImsUECM_Registration (see NOTE 9) Nhss_ImsUEAuthenticate_Get
Cx-Deregister	HSS	S-CSCF	Nhss_ImsUECM_DeregistrationNotification
Cx-Update_Subscr_Data	HSS	S-CSCF	Nhss_ImsSDM_Notification

NOTE 1: Corresponds to Cx-Select-Pull for the requests of S-CSCF capabilities from I-CSCF to the HSS.
NOTE 2: Corresponds to Cx-Put for Registration of S-CSCF in HSS during Registration/Re-registration and Unregistered cases.
NOTE 3: Corresponds to Cx-Put for de-registration of S-CSCF in HSS.
NOTE 4: Corresponds to Cx-Put message for updating the registration state of Public Identity in HSS.
NOTE 5: Corresponds to Cx-Put message for storing S-CSCF Restoration data during IMS registration procedures.
NOTE 6: Corresponds to Cx-Pull when S-CSCF needs to fetch and subscribe to notification of changes in IMS User's Service Profile Data.
NOTE 7: Corresponds to Cx-Pull for retrieval of S-CSCF Restoration data from HSS.
NOTE 8: Corresponds to Cx-Location-Query for the requests of S-CSCF capabilities from I-CSCF to the HSS.
NOTE 9: Corresponds to Cx-Put for the assignment of a S-CSCF during execution of the authentication of the IMS User.

AA.2.2.3 Mapping of Sh messages to HSS SBI services

The following table defines the mapping between stage 2 Sh messages and HSS SBI services and service operations:

Table AA.2.2.3-1: Sh messages to HSS SBI services and service operations mapping

Sh message	Source	Destination	HSS SBI service operation name
Sh-Pull	AS	HSS	Nhss_ImsSDM_Get
Sh-Update	AS	HSS	Nhss_ImsSDM_Update
Sh-Subs-Notif	AS	HSS	Nhss_ImsSDM_Subscribe Nhss_ImsSDM_Unsubscribe Nhss_ImsSDM_Get
Sh-Notif	HSS	AS	Nhss_ImsSDM_Notification

AA.3 SBI Capable HSS Discovery and Selection

AA.3.1 General

An SBI capable IMS entity (e.g. I-CSCF, S-CSCF or IMS AS) performs HSS discovery to discover an HSS that manages the user subscriptions.

The SBI capable IMS entity shall utilize the NRF to discover the SBI capable HSS instance(s) unless the information about SBI capable HSS instances is available by other means, e.g. locally configured on the SBI capable IMS entity. The HSS selection function in SBI capable IMS entities selects an SBI capable HSS instance based on the available SBI capable HSS instances (obtained from the NRF or locally configured).

An SBI capable IMS entity always selects an HSS within its own PLMN. The HSS selection should consider one of the following factors when available to the SBI capable IMS entity:

1. HSS Group ID of the UE's IMS user identity (IMPI or IMPU).
2. IMPI; e.g. the SBI capable IMS entity selects an SBI capable HSS instance based on the IMPI range the UE's IMPI belongs to, configured locally or based on the results of a discovery procedure with NRF using the UE's IMPI as input for HSS discovery.
3. IMPU; e.g. the SBI capable IMS entity selects an SBI capable HSS instance based on the IMPU range the UE's IMPU belongs to, configured locally or based on the results of a discovery procedure with NRF using the UE's IMPU as input for HSS discovery.

Unless the information about the interface type to be used towards HSS is locally configured on the SBI capable IMS entity, an SBI capable IMS entity can also use the NRF to decide the type of interface (SBI vs diameter) to be used towards HSS.

The following clause describes the procedure for HSS registration in NRF, SBI capable HSS discovery and interface type selection via NRF.

AA.3.2 HSS Registration in NRF

An SBI capable HSS registers in the NRF using the Nnrf_NFManagement_NFRegister Request message as defined in TS 23.502 [94]. The NF profile of the HSS registered in NRF includes necessary information for an SBI capable IMS entity to send SBI service requests to the selected SBI capable HSS service instance.

Different SBI capable HSS instances managing different sets of IMPIs/IMPUs may be deployed in a given PLMN. In this case, the SBI capable HSS instances register in NRF using either different ranges of IMPIs/IMPUs and/or HSS Group IDs.

NOTE: In deployments where simple IMPU and IMPI ranges are not suitable to describe the IMPU/IMPI sets served by HSS instances, it is expected the HSS instances only register HSS Group IDs.

AA.3.3 HSS Discovery and Selection via NRF

AA.3.3.1 General

During the IMS procedure, an SBI capable IMS entity sends a Nnrf_NFDiscovery_Request to NRF as defined in TS 23.502 [94] to discover SBI capable HSS instances within a given PLMN. The SBI capable IMS entity may store all returned SBI capable HSS instances and their NF profiles for subsequent use, including, if applicable, supported IMPIs/IMPUs ranges, and/or HSS Group IDs. If no SBI capable HSS instance is available in the PLMN, then the NRF replies to the SBI capable IMS entity with no information. In this case, the SBI capable IMS may then attempt to communicate with the HSS using non-SBA protocols.

NOTE: The SBI enabled IMS entity can also perform HSS discovery prior to receiving an IMS request without any public identity information.

When an SBI capable IMS entity receives an NRF response that HSS supports SBI and stores the information received from the HSS, it shall make use of Nnrf_NFStatusSubscribe/Unsubscribe service operations with NRF as defined in TS 23.502 [94] to receive Nnrf_NFStatusNotify service operation for updates to the NF profiles of SBI capable HSS instances registered in NRF.

AA.3.3.2 HSS Discovery

The call flow in Figure AA.3.3.2-1 illustrates the steps to locate the HSS instance for an IMS public identity.

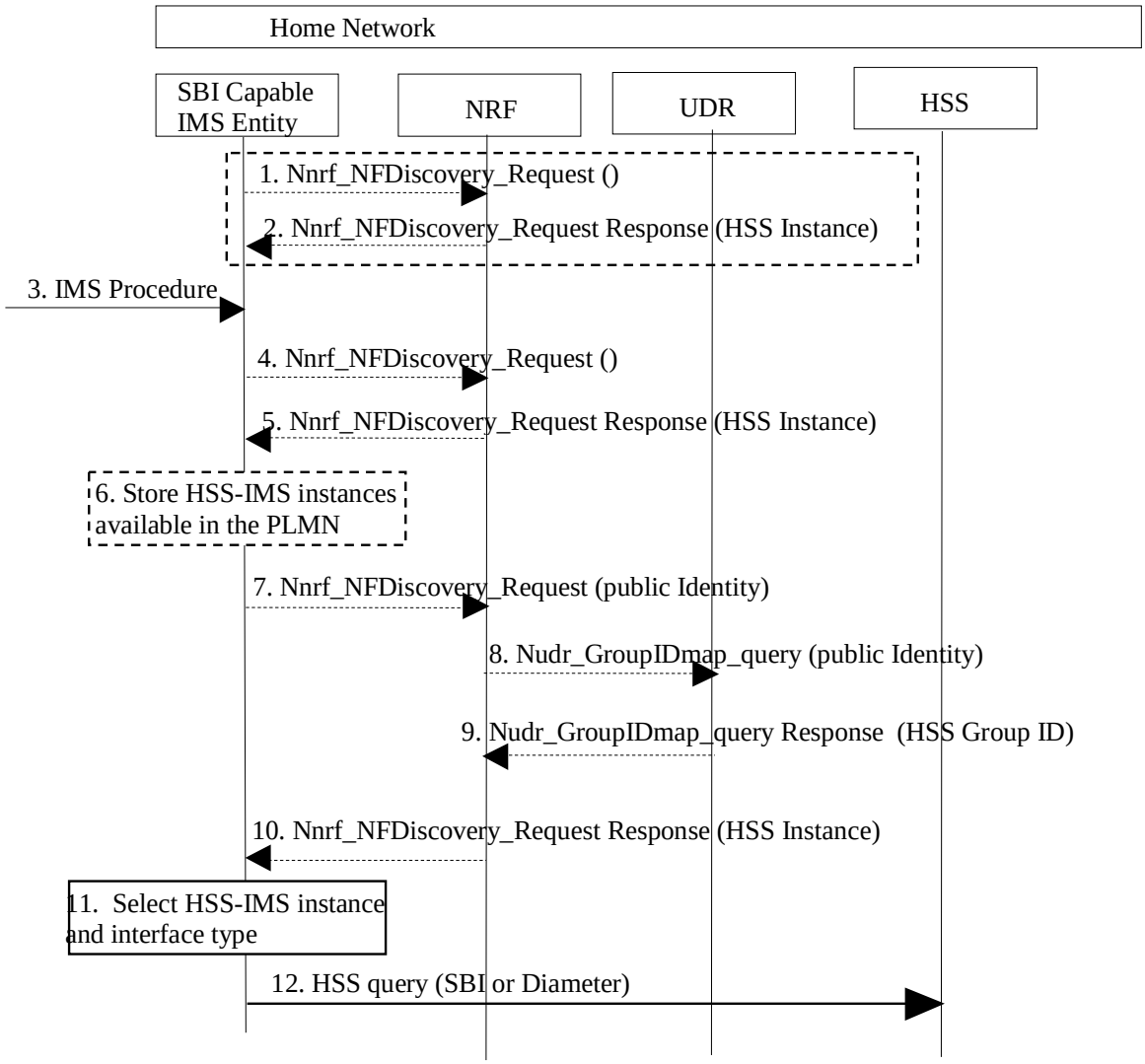


Figure AA.3.3.2-1: HSS discovery and selection

Steps 1 - 2 may be performed, any time after power up, e.g. in the scenario where only a single HSS instance or HSS group is deployed, and in the scenario where an operator has IMPI/IMPU ranges that are registered in NRF as described in clause AA.3.2. In this case there is no need for any IMPU to perform the 2 steps.

1. An SBI capable IMS entity may discover the SBI capable HSS instances available in the PLMN via Nnrf_NFDiscovery_Request.

2. The NRF provides the SBI capable IMS entity with the HSS instances and/or any HSS Group IDs registered in the PLMN. If no SBI capable HSS instance and/or any HSS Group ID is available in the PLMN, then the NRF will reply to the SBI capable IMS entity with no information about available SBI capable HSS instances.

3. The SBI capable IMS entity receives an IMS procedure related to a given IMS user (IMPI or IMPU depending on the procedure).

Steps 4 - 6 may be performed, e.g. if the SBI capable IMS entity did not retrieve and store information about HSS instances and/or HSS Group IDs registered in the PLMN at an earlier stage (performed steps 1-2).

4. An SBI capable IMS entity may discover the SBI capable HSS instances available in the PLMN via Nnrf_NFDiscovery_Request.

5. The NRF provides the SBI capable IMS entity with the HSS instances and/or any HSS Group IDs registered in the PLMN. If no SBI capable HSS instance and/or any HSS Group ID is available in the PLMN, then the NRF will reply to the SBI capable IMS entity with no information about available SBI capable HSS instances.

6. The SBI capable IMS entity stores the result of the NRF discovery, if any is received. The IMS capable entity may store the received response for future use, otherwise the IMS entity must perform the query in response to each IMS request it receives.

   If the SBI capable IMS entity received no results at all, the procedure is exited, and the SBI capable IMS entity may use Diameter interfaces to interact with an HSS.

NOTE 1: The SBI capable IMS entity can request the NRF to be notified of updates in the SBI capable HSS instances/ HSS Group IDs registered in NRF by using a Nnrf_NFManagement_NFStatusSubscribe service operation.

Steps 7 - 10 are performed only if the SBI capable IMS entity cannot locate an HSS instance corresponding to the IMS public identity based on stored information.

7. The SBI capable IMS entity sends to NRF an Nnrf_NFDiscovery_Request with the IMS public identity received in step 1.

8. NRF may query the UDR, via the Nudr_GroupIDmap service, for the HSS Group ID corresponding to the IMS public identity.

9. If requested the UDR returns the HSS-IMS Group ID to NRF.

10. NRF locates HSS instance(s) corresponding to the HSS Group ID and provides and them to the SBI capable IMS entity.

11. The SBI capable IMS entity selects the HSS instance.

12. The SBI capable IMS entity can then start interaction with the selected HSS instance.

Annex AB (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2014-09	SA#65	SP-140430	1073	3	B	Paging Policy Differentiation over LTE for IMS Voice	**13.0.0**
2014-09	SA#65	SP-140431	1084	2	B	Sharing Resources For Sessions on Hold	**13.0.0**
2014-12	SA#66	SP-140690	1092	1	B	Media components of a session put on hold	13.1.0
2014-12	SA#66	SP-140690	1093	2	B	P-CSCF Information Reporting Shared resources	13.1.0
2014-12	SA#66	SP-140686	1095	1	A	Interface between IM-SSF and HSS	13.1.0
2014-12	SA#66	SP-140676	1097	1	A	Support for flexible BFCP	13.1.0
2014-12	SA#66	SP-140688	1098	1	F	Configuration for paging policy differentiation	13.1.0
2014-12	SA#66	SP-140693	1099	-	B	Insertion of GI by an AS	13.1.0
2015-03	SA#67	SP-150109	1101	1	A	T-ADS for UEs supporting access to IMS via WLAN connected to EPC using S2b or S2a	13.2.0
2015-03	SA#67	SP-150022	1103	1	A	MSRP Clarification	13.2.0
2015-03	SA#67	SP-150022	1105	-	A	BFCP Clarification	13.2.0
2015-06	SA#68	SP-150223	1110	-	A	AS allowing non-international format Request-URI when RAVEL is used	13.3.0
2015-06	SA#68	SP-150225	1116	1	A	Codecs for WebRTC	13.3.0
2015-06	SA#68	SP-150222	1120	-	A	Removal of long expired reference to draft-kaplan-enum-sip-routing	13.3.0
2015-06	SA#68	SP-150222	1126	2	A	OMR handling of SDP offer-answer exchanges after media path has been selected	13.3.0
2015-06	SA#68	SP-150230	1129	2	A	Stage 2 cleanup regarding the WIC registration with a security token	13.3.0
2015-06	SA#68	SP-150232	1134	3	B	Supporting Class of Users	13.3.0
2015-09	SA#69	SP-150494	1135	1	D	Clarifying IMPU/IMPI relationship for WIC registration from a pool of Identities	13.4.0
2015-09	SA#69	SP-150503	1136	3	B	Support for providing and distinguishing multiple UE provided access information over untusted WLAN access	13.4.0
2015-09	SA#69	SP-150500	1139	2	F	Clarifications on indication of resource sharing	13.4.0
2015-09	SA#69	SP-150526	1138	2	B	Support Minimizing bearer level protocol conversion	13.4.0
2016-03	SA#71	SP-160155	1144	2	A	Replacing Incorrect Reference for business trunking Specification TS	13.5.0
2016-06	SA#72	SP-160298	1142	7	C	Priority sharing for concurrent sessions, IMS	13.6.0
2016-06	SA#72	SP-160297	1147	2	F	NPLI for untrusted WLAN access in IMS	13.6.0
2016-06	SA#72	SP-160304	1146	6	B	Support for Acquisition and subscription to changes in PLMN id by P-CSCF	**14.0.0**
2016-09	SA#73	SP-160660	1148	3	B	Support for P-CSCF sending a response to UE or IMS network when receiving Bearer Setup Request Rejection for QCI=1	14.1.0
2016-09	SA#73	SP-160664	1151	2	A	NPLI for untrusted WLAN access in IMS for LI purposes	14.1.0
2016-09	SA#73	SP-160651	1152	2	C	Handling of Local Number Translation for roaming users in deployments without IMS-level roaming interfaces	14.1.0
2016-09	SA#73	SP-160658	1153	3	B	TCP transport for data channels towards the WIC.	14.1.0
2016-09	SA#73	SP-160658	1154	3	B	WebRTC Media plane optimization with DTLS termination.	14.1.0
2016-09	SA#73	SP-160651	1155	1	F	Inter-PLMN Mobility support clarification for V8	14.1.0
2016-09	SA#73	SP-160658	1156	3	B	Support of RTP/RTCP multiplexing for WebRTC	14.1.0
2016-09	SA#73	SP-160651	1157	-	B	MCC Implementation correction for text in clause 4.15b	14.1.0
2016-09	SA#73	SP-160658	1159	1	F	Reference point clarification between IMS entities for IMS session and dialog	14.1.0
2016-09	SA#73	SP-160658	1160	3	B	Control parameter for predictable pre-emption of media flows	14.1.0
2016-12	SA#74	SP-160809	1163	1	A	Editorial change reflecting IMS being access agnostic	14.2.0
2016-12	SA#74	SP-160809	1164	1	A	Editorial changes and inclusion of Mp Reference Point and missing reference point P-CSCF - I-CSCF	14.2.0
2016-12	SA#74	SP-160826	1166	5	B	Support for 3GPP PS Data off for SIP-Based Service	14.2.0
2017-03	SA#75	SP-170051	1169	1	F	3GPP Data Off IMS Status Reporting Correction	14.3.0
2017-03	SA#75	SP-170052	1170	2	F	Alignment with CT WG3 for support for subscription to changes to IP-CAN by P-CSCF at IMS session setup.	14.3.0
2017-06	SA#76	SP-170372	1172	2	F	Adding SIP AS as the entity to determines when resource sharing is to be performed	14.4.0
2017-09	SA#77	SP-170716	1176	2	F	Support for Enhanced Coverage for data centric UEs	14.5.0
2017-09	SA#77	SP-170732	1173	1	B	WebRTC Web Server Function discovery	**15.0.0**
2017-09	SA#77	SP-170727	1174	4	B	new annex to 23.228 for 5GS support	**15.0.0**
2017-09	SA#77	SP-170727	1175	2	B	Adaptation to TS 23.228 due to 5GS	**15.0.0**
2017-09	SA#77	SP-170729	1177	2	C	IMS support to 3GPP PS Data Off Phase 2	**15.0.0**
2017-12	SA#78	SP-170919	1179	1	F	Improvements to TS 23.228 Annex M to reflect 5GS	15.1.0
2017-12	SA#78	SP-170919	1180	1	F	Improvements to TS 23.228 Annex Y	15.1.0
2017-12	SA#78	SP-170921	1183	-	C	Clarification on UE behavior when receiving single list of Exempt Services - TS 23.228	15.1.0
2017-12	SA#78	SP-170924	1184	2	B	Support for identity attestation and verification	15.1.0
2017-12	SA#78	SP-170915	1186	2	A	Modification on PS Data Off support in IMS Client - TS 23.228	15.1.0
2018-03	SA#79	SP-180094	1187	1	F	Clarification on additional IP address	15.2.0
2018-03	SA#79	SP-180090	1188	2	F	IMS registration procedures for UE in Dual Registration mode	15.2.0

2018-09	SA#81	SP-180712	1191	1	F	Clarification on access network information during IMS call in 5G dual connectivity scenario	15.3.0
2019-03	SA#83	SP-190156	1196	1	F	Clause W.2 on "Architecture without IMS-level roaming interfaces" to refer to clause Y.9.2 that defines it for the 5GS case.	15.4.0
2019-03	SA#83	SP-190163	1193	4	B	Support for RLOS in IMS	**16.0.0**
2019-03	SA#83	SP-190175	1194	1	B	Support for RAN Assisted Codec Adaptation	16.0.0
2019-06	SA#84	SP-190419	1199	1	B	eIMS P-CSCF use of NRF	16.1.0
2019-06	SA#84	SP-190419	1200	3	B	SBA HSS Services for IMS	16.1.0
2019-06	SA#84	SP-190419	1201	3	B	HSS Discovery and Interface Type Selection	16.1.0
2019-06	SA#84	SP-190419	1202	1	B	Allowing SMF to perform P-CSCF Discovery using NRF	16.1.0
2019-06	SA#84	SP-190419	1203	3	B	Allowing IMS to use N5 interface to interact with PCF	16.1.0
2019-06	SA#84	SP-190419	1204	-	B	Additional corrections for allowing IMS to use N5 interface to interact with PCF	16.1.0
2019-06	SA#84	SP-190419	1205	2	F	Bearer establishment mode negotiation not applicable in 5GC	16.1.0
2019-06	SA#84	SP-190426	1206	1	B	Introduction of UDICOM	16.1.0
2019-06	SA#84	SP-190406	1208	2	F	Correction to Support for RAN Assisted Codec Adaptation	16.1.0
2019-09	SA#85	SP-190611	1211	5	F	Update of SBA HSS Services for IMS	16.2.0
2019-09	SA#85	SP-190611	1212	3	F	Clarification for HSS Discovery and Interface Type Selection	16.2.0
2019-09	SA#85	SP-190611	1218	-	F	Resolve EN on networks with both Rx and N5 support	16.2.0
2019-09	SA#85	SP-190611	1219	2	F	Update P-CSCF Registration with NRF	16.2.0
2019-12	SA#86	SP-191087	1222	1	F	Fixing incorrectly implemented 23.228 CR1193	16.3.0
2019-12	SA#86	SP-191078	1223	1	F	HSS Service Name correction	16.3.0
2019-12	SA#86	SP-191078	1225	2	F	Correction on HSS service Nhss_imsSubscriberDataManagement	16.3.0
2019-12	SA#86	SP-191078	1226	-	F	UDR service for mapping IMS Public Identity to HSS Group ID for HSS selection	16.3.0
2019-12	SA#86	SP-191087	1228	-	F	Corrections to S-CSCF discovery during RLOS IMS registration	16.3.0
2020-03	SA#87E	SP-200080	1231	2	F	EPS Fallback event transporting within IMS	16.4.0

History

Document history		
V16.4.0	October 2020	Publication