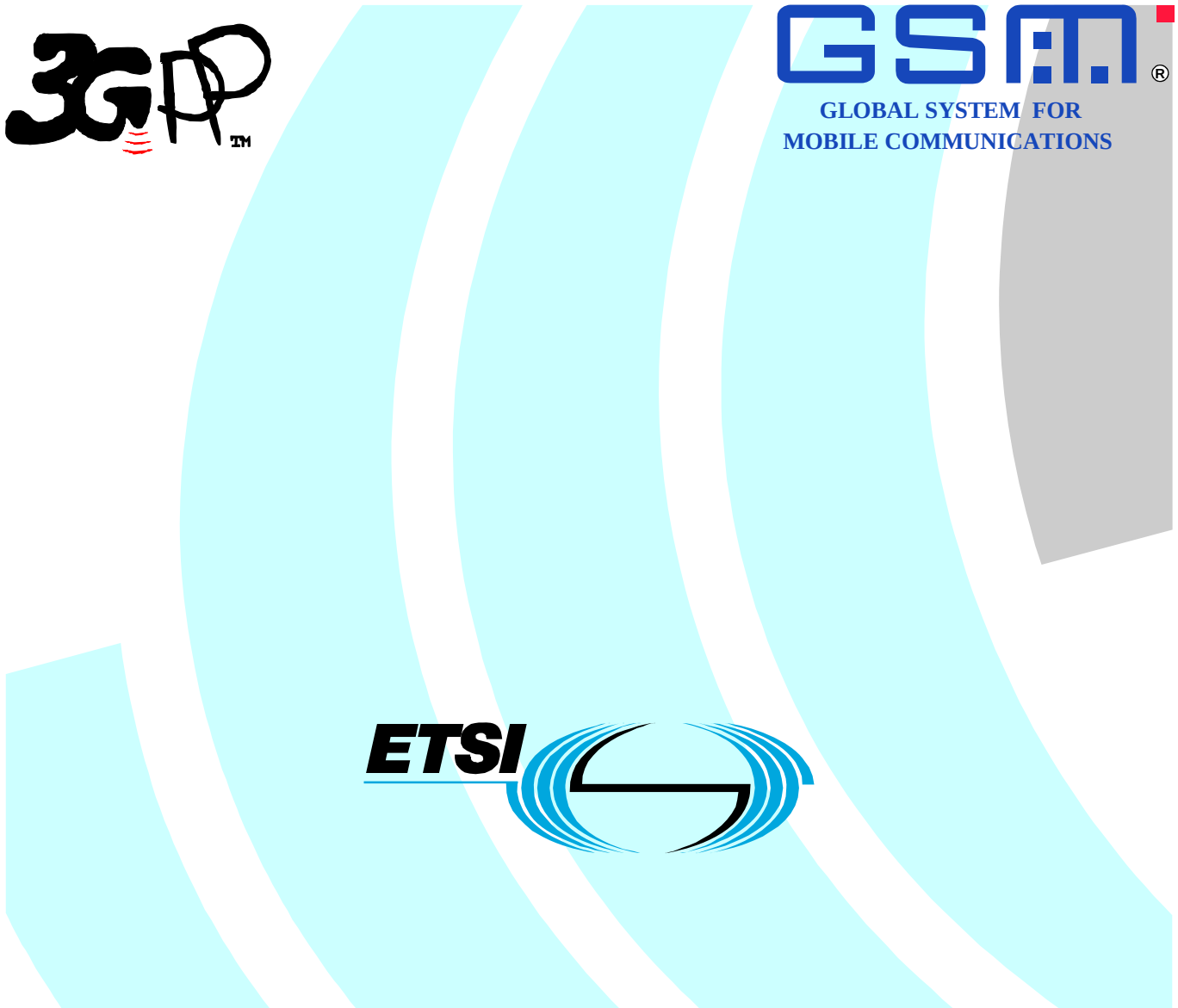
ETSI TS 123 228 V8.3.0 (2008-01)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
IP Multimedia Subsystem (IMS);
Stage 2
(3GPP TS 23.228 version 8.3.0 Release 8)



Reference
RTS/TSGS-0223228v830

Keywords
GSM, 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

IPRs essential or potentially essential to the present document 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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

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

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 11
1 Scope 12
2 References 12
3 Definitions, symbols and abbreviations 15
3.1 Definitions 15
3.2 Symbols 16
3.3 Abbreviations 17
4 IP multimedia subsystem concepts 18
4.0 General 18
4.1 Relationship to CS domain and the IP-Connectivity Access Network 19
4.2 IMS services concepts 20
4.2.1 Home-network based services 20
4.2.1.1 Support of CAMEL 20
4.2.1.2 Support of OSA 20
4.2.2 Support of numbers in non-international format in the IMS 20
4.2.3 Support of roaming users 21
4.2.4 IP multimedia Subsystem Service Control Interface (ISC) 22
4.2.4a HSS to service platform Interface 24
4.2.4b S-CSCF Service Control Model 25
4.2.5 The QoS requirements for an IM CN subsystem session 26
4.2.6 QoS Requirements for IM CN subsystem signalling 27
4.2.7 Support of SIP forking 28
4.2.7.1 SIP Forking 28
4.2.7.2 Forking within and outside the IM CN Subsystem 28
4.2.7.3 Support for forked requests 29
4.3 Naming and addressing concepts 29
4.3.1 Address management 29
4.3.2 Void 29
4.3.3 Identification of users 30
4.3.3.0 General 30
4.3.3.1 Private user identities 30
4.3.3.2 Public user identities 30
4.3.3.2a Globally Routable User Agent URI (GRUU) 31
4.3.3.2a.1 Architecture Requirements 31
4.3.3.2b Wildcarded public user identity 32
4.3.3.3 Routing of SIP signalling within the IP multimedia subsystem 33
4.3.3.3a Handling of dialled number formats 33
4.3.3.3b Termination of session with the TEL URI format public user identity 33
4.3.3.4 Relationship of Private and Public User Identities 33
4.3.3.5 Relationship of Public User Identities, GRUUs, and UEs 34
4.3.4 Identification of network nodes 35
4.3.5 E.164 address to SIP-URI resolution in an IM CN subsystem 35
4.3.6 Public Service Identities 36
4.4 Signalling concepts 36
4.5 Mobility related concepts 37
4.6 Roles of Session Control Functions 37
4.6.0 General 37
4.6.1 Proxy-CSCF 37
4.6.2 Interrogating-CSCF 38
4.6.2.0 General 38
4.6.2.1 Void 39
4.6.3 Serving-CSCF 39

4.6.4 Breakout Gateway Control Function 41
4.6.5 Void 41
4.7 Multimedia Resource Function 41
4.8 Security Concepts 43
4.9 Charging Concepts 43
4.10 IMS group management concepts 43
4.10.0 General 43
4.10.1 IMS group administration 43
4.10.2 Group identifiers 43
4.11 Relationship to 3GPP Generic User Profile (GUP) 43
4.12 Network Address Translation traversal in access network 43
4.13 Identification of IMS communication Services 44
4.13.1 General 44
4.13.2 Identification of IMS communication Services 44
4.13.3 Identification of IMS applications 46
4.14 Border Control concepts 46
4.15 IMS in transit network scenarios 47
4.15.1 General concepts 47
4.15.2 IMS transit network configurations 47
4.16 Support of multimedia telephony 48
4.16.1 Telephony Application Server 48
4.16.2 Identification of multimedia telephony 48
4.16.3 Session setup principles 48
4.17 Support of short message service 48
4.17.1 IP Short Message Gateway (IP-SM-GW) 48
4.18 Support of Number portability 48
4.18.1 Number portability 48
4.19 Support of Preferred Circuit Carrier Access and Per Call Circuit Carrier Selection 49
4.19.1 Preferred Circuit Carrier Access and Per Call Circuit Carrier Selection 49

5 IP multimedia subsystem procedures 49
5.0 General 49
5.0a Session-unrelated procedures 49
5.1 CSCF related procedures 50
5.1.0 Establishing IP-Connectivity Access Network bearer for IM CN Subsystem Related Signalling 50
5.1.1 Procedures related to local CSCF discovery 50
5.1.1.0 General 50
5.1.1.1 DHCP/DNS procedure for P-CSCF discovery 50
5.1.1.2 Void 51
5.1.2 Procedures related to Serving-CSCF assignment 51
5.1.2.1 Assigning a Serving-CSCF for a user 51
5.1.2.2 Cancelling the Serving-CSCF assignment 52
5.1.2.3 Void 52
5.1.3 Procedures related to Interrogating-CSCF 52
5.1.4 Procedures related to Proxy-CSCF 52
5.1.5 Subscription Updating Procedures 52
5.1.5.0 General 52
5.1.5.1 Subscription updating information flow 52
5.2 Application level registration procedures 53
5.2.0 General 53
5.2.1 Requirements considered for registration 53
5.2.1a Implicit Registration 54
5.2.1a.0 General 54
5.2.1a.1 Implicit Registration for UE without ISIM 55
5.2.2 Registration flows 55
5.2.2.1 Requirements to consider for registration 55
5.2.2.2 Assumptions 56
5.2.2.3 Registration information flow – User not registered 56
5.2.2.4 Re-Registration information flow – User currently registered 58
5.2.2.5 Stored information. 60
5.3 Application level de-registration procedures 60
5.3.1 Mobile initiated de-registration 60

5.3.2 Network initiated de-registration 62
5.3.2.0 General 62
5.3.2.1 Network Initiated Application (SIP) De-registration, Registration Timeout 62
5.3.2.2 Network Initiated Application (SIP) De-registration, Administrative 63
5.3.2.2.0 General 63
5.3.2.2.1 Network Initiated De-registration by HSS, administrative 64
5.3.2.2.2 Network Initiated De-registration by Service Platform 64
5.4 Procedures for IP multi-media sessions 66
5.4.0 General 66
5.4.1 Bearer interworking concepts 66
5.4.2 Interworking with Internet 66
5.4.2a IP version interworking 66
5.4.3 Interworking with PSTN 67
5.4.4 Requirements for IP multi-media session control 68
5.4.5 Session Path Information 68
5.4.5.1 Session Path Information during Registration and Session Initiation 68
5.4.5.2 P-CSCF in the Session Path 68
5.4.5.3 S-CSCF in the Session Path 69
5.4.6 End-user preferences and terminal capabilities 69
5.4.6.0 General 69
5.4.6.1 Objectives 69
5.4.6.2 End-user expectations 69
5.4.6.3 Mechanism for bearer establishment 70
5.4.6.4 Session progress indication to the originating UE 72
5.4.7 Interaction between QoS and session signalling 72
5.4.7.0 General 72
5.4.7.1 Authorize QoS Resources 73
5.4.7.1a Resource Reservation with Policy and Charging Control 73
5.4.7.2 Enabling of Media Flows 73
5.4.7.3 Disabling of Media Flows 74
5.4.7.4 Revoke Authorisation for IP-Connectivity Access Network and IP Resources 74
5.4.7.5 Indication of IP-Connectivity Access Network bearer release 74
5.4.7.6 Authorization of IP-Connectivity Access Network bearer modification 74
5.4.7.7 Indication of IP-Connectivity Access Network bearer modification 74
5.4.8 QoS-Assured Preconditions 74
5.4.9 Event and information distribution 75
5.4.9.0 General 75
5.4.9.1 Subscription to event notifications 76
5.4.10 Void 78
5.4.11 Signalling Transport Interworking 78
5.4.12 Configuration and Routing principles for Public Service Identities 78
5.4.12.0 General 78
5.4.12.1 PSIs on the originating side 78
5.4.12.2 PSIs on the terminating side 78
5.4.12.3 Subdomain based PSIs 79
5.4.12.4 PSI configuration in the HSS 79
5.4.12.5 Requests originated by the AS hosting the PSI 79
5.4a Overview of session flow procedures 80
5.4a.1 End-to-End session flow procedures 80
5.4a.2 Transit network session flow procedures 82
5.5 Serving-CSCF/MGCF to serving-CSCF/MGCF procedures 84
5.5.0 General 84
5.5.1 (S-S#1) Different network operators performing origination and termination 84
5.5.2 (S-S#2) Single network operator performing origination and termination 86
5.5.3 (S-S#3) Session origination with PSTN termination in the same network as the S-CSCF. 89
5.5.4 (S-S#4) Session origination with PSTN termination in a different network from the S-CSCF. 91
5.6 Origination procedures 93
5.6.0 General 93
5.6.1 (MO#1) Mobile origination, roaming 93
5.6.2 (MO#2) Mobile origination, home 96
5.6.3 (PSTN-O) PSTN origination 98
5.6.4 (NI-O) Non-IMS Origination procedure from an external SIP client 99

5.6.5 Application Server Origination Procedure 101
5.6.5.1 (AS-O) Origination at Application Server 101
5.6.5.2 Void 103
5.6.5.3 S-CSCF selection by I-CSCF for AS Originating call procedures 103
5.7 Termination procedures 105
5.7.0 General 105
5.7.1 (MT#1) Mobile termination, roaming 105
5.7.2 (MT#2) Mobile termination, home 107
5.7.2a (MT#3) Mobile termination, CS Domain roaming 110
5.7.3 (PSTN-T) PSTN termination 110
5.7.4 (NI-T) Non-IMS Termination to an external SIP client 112
5.7.5 (AS-T#1) PSI based Application Server termination – direct 114
5.7.6 (AS-T#2) PSI based Application Server termination – indirect 115
5.7.7 (AS-T#3) PSI based Application Server termination – DNS routing 116
5.7.8 (AST#4) Termination at Application Server based on service logic 117
5.7a Procedures for the establishment of sessions without preconditions 118
5.7a.1 General 118
5.7a.2 Procedures for the establishment of sessions without preconditions - no resource reservation required before session becomes active 120
5.7a.3 Void 122
5.8 Procedures related to routing information interrogation 122
5.8.0 General 122
5.8.1 User identity to HSS resolution 122
5.8.2 SLF on register 123
5.8.3 SLF on UE invite 124
5.8.4 SLF on AS access to HSS 125
5.9 Routing of mid-session signalling 125
5.10 Session release procedures 126
5.10.0 General 126
5.10.1 Terminal initiated session release 126
5.10.2 PSTN initiated session release 128
5.10.3 Network initiated session release 129
5.10.3.0 Removal of IP-CAN bearers used to transport IMS SIP signalling 129
5.10.3.1 Network initiated session release - P-CSCF initiated 129
5.10.3.1.0 General 129
5.10.3.1.1 Network initiated session release - P-CSCF initiated – after removal of IP-Connectivity Access Network bearer 130
5.10.3.1.2 Void 131
5.10.3.2 Network initiated session release - S-CSCF Initiated 131
5.11 Procedures to enable enhanced multimedia services 132
5.11.1 Session Hold and Resume Procedures 132
5.11.1.0 General 132
5.11.1.1 Mobile-to-Mobile Session Hold and Resume Procedures 132
5.11.1.2 Mobile-initiated Hold and Resume of a Mobile-PSTN Session 134
5.11.1.3 PSTN-initiated Hold and Resume of a Mobile-PSTN Session 136
5.11.2 Procedures for anonymous session establishment 138
5.11.2.0 General 138
5.11.2.1 Signalling requirements for anonymous session establishment 138
5.11.2.2 Bearer path requirements for anonymous session establishment 138
5.11.3 Procedures for codec and media characteristics flow negotiations 138
5.11.3.0 General 138
5.11.3.1 Codec and media characteristics flow negotiation during initial session establishment 139
5.11.3.2 Codec or media characteristics flow change within the existing reservation 142
5.11.3.3 Codec or media characteristics flow change requiring new resources and/or authorisation 143
5.11.3.4 Sample MM session flow - addition of another media 146
5.11.4 Procedures for providing or blocking identity 149
5.11.4.0 General 149
5.11.4.1 Procedures for providing the authenticated identity of the originating party 149
5.11.4.2 Procedures for blocking the identity of the originating party 150
5.11.4.3 Procedures for providing the authenticated identity of the originating party (PSTN origination) 151
5.11.4.4 Procedures for providing the authenticated identity of the originating party (PSTN termination) 152
5.11.5 Session Redirection Procedures 152

5.11.5.0 General 152
5.11.5.1 Session Redirection initiated by S-CSCF to IMS 152
5.11.5.2 Session Redirection to PSTN Termination (S-CSCF #2 forwards INVITE) 153
5.11.5.2a Session Redirection to PSTN Termination (REDIRECT to originating UE#1) 154
5.11.5.3 Session Redirection initiated by S-CSCF to general endpoint (REDIRECT to originating UE#1) 156
5.11.5.4 Session Redirection initiated by P-CSCF 157
5.11.5.5 Session Redirection initiated by UE 158
5.11.5.6 Session Redirection initiated by originating UE#1 after Bearer Establishment (REDIRECT to originating UE#1) 159
5.11.6 Session Transfer Procedures 160
5.11.6.0 General 160
5.11.6.1 Refer operation 160
5.11.6.2 Application to Session Transfer Services 162
5.11.6.2.0 General 162
5.11.6.2.1 Blind Transfer and Assured Transfer 162
5.11.6.2.2 Consultative Transfer 163
5.11.6.2.3 Three-way Session 163
5.12 Mobile Terminating call procedures to unregistered Public User Identities 164
5.12.0 General 164
5.12.1 Mobile Terminating call procedures to unregistered Public User Identity that has services related to unregistered state 164
5.12.2 Mobile Terminating call procedures to unregistered Public User Identity that has no services related to unregistered state 166
5.13 IMS Emergency Sessions 166
5.14 Interactions involving the MRFC/MRFP 166
5.14.0 General 166
5.14.1 Interactions between the UE and the MRFC 166
5.14.2 Service control based interactions between the MRFC and the AS 167
5.14.3 Interactions for services using both the Ut interface and MRFC capabilities 167
5.15 Mobile Terminating session procedure for unknown user 167
5.15.0 General 167
5.15.1 Unknown user determined in the HSS. 168
5.15.2 Unknown user determined in the SLF 168
5.16 IMS messaging concepts and procedures 169
5.16.0 General 169
5.16.1 Immediate Messaging 169
5.16.1.0 General 169
5.16.1.1 Procedures to enable Immediate Messaging 169
5.16.1.1.0 General 169
5.16.1.1.1 Immediate messaging procedure to registered Public User Identity 170
5.16.1.1.2 Immediate messaging procedure to unregistered Public User Identity 171
5.16.1.2 Immediate messages with multiple recipients 172
5.16.2 Session-based Messaging 172
5.16.2.0 General 172
5.16.2.1 Architectural principles 172
5.16.2.2 Procedures to enable Session based Messaging 173
5.16.2.2.0 General 173
5.16.2.2.1 Session based messaging procedure to registered Public User Identity 173
5.16.2.2.2 Session based messaging procedure using multiple UEs 174
5.16.2.2.3 Session based messaging procedure with an intermediate node 177
5.16.2.2.4 Session based messaging release procedure 178
5.16.2.2.5 Session based messaging release procedure with an intermediate node 179
5.17 Refreshing sessions 179
5.18 Void 180
5.19 Support for Transit scenarios in IMS 180
5.20 Procedures for Assigning, Using, and Processing GRUUs 181
5.20.1 UE 181
5.20.1.1 Obtaining a GRUU during registration 181
5.20.1.2 Using a GRUU 182
5.20.1.3 Using a GRUU while requesting Privacy 182
5.20.2 Serving-CSCF 182
5.20.2.1 Allocating a GRUU during registration 182

5.20.2.2 Using a GRUU 182
5.20.3 Interrogating-CSCF 183
5.20.3a HSS 183
5.20.4 Elements other than UE acting as a UA 183
5.20.4.1 Using a GRUU 183
5.20.4.2 Assigning a GRUU 183

Annex A (Informative): Information flow template 184

Annex B (Informative): Void 186

Annex C: Void 187

Annex D: Void 188

Annex E (normative): IP-Connectivity Access Network specific concepts when using GPRS to access IMS 189

E.0 General 189

E.1 Mobility related concepts 189
E.1.0 General 189
E.1.1 Procedures for P-CSCF discovery 189
E.1.1.0 General 189
E.1.1.1 GPRS procedure for P-CSCF discovery 190

E.2 QoS related concepts 190
E.2.1 Application Level Signalling for IMS 190
E.2.1.0 General 190
E.2.1.1 QoS Requirements for Application Level Signalling 190
E.2.1.2 Requirements for IM CN subsystem signalling flag 190
E.2.1.3 Application Level Signalling support for IMS services 191
E.2.1a PDP context procedures for IMS 191
E.2.1a.1 Establishing PDP Context for IM CN Subsystem Related Signalling 191
E.2.1a.2 Deletion of PDP Context used to transport IMS SIP signalling 192
E.2.2 The QoS requirements for an IM CN subsystem session 192
E.2.2.0 General 192
E.2.2.1 Relation of IMS media components and PDP contexts carrying IMS media 193
E.2.3 Interaction between GPRS QoS and session signaling 193
E.2.3.0 General 193
E.2.3.1 Resource Reservation with Policy and Charging Control 193
E.2.4 Network initiated session release - P-CSCF initiated 194
E.2.4.0 General 194
E.2.4.1 Network initiated session release - P-CSCF initiated after loss of radio coverage 194

E.3 Address and identity management concepts 195
E.3.1 Deriving IMS identifiers from the USIM 195

E.4 Void 196

E.5 IP version interworking in IMS 196

E.6 Usage of NAT in GPRS 196

Annex F (informative): Routing subsequent requests through the S-CSCF 197

Annex G (Normative): Reference Architecture and procedures when the NAT is invoked between the UE and the IMS domain 198

G.1 General 198
G.1.1 General requirements 198

G.2 Reference models 198
G.2.1 IMS-ALG and IMS Access Gateway model 199
G.2.2 ICE and Outbound reference model 199

G.3 Network elements for employing the IMS-ALG and IMS Access Gateway 200
G.3.1 Required functions of the P-CSCF 200
G.3.2 Required functions of the IMS Access Gateway 200
G.3.3 Iq reference point 201

G.4 Procedures for employing the IMS-ALG and IMS Access Gateway 201
G.4.1 General 201
G.4.2 NAT detection in P-CSCF 201
G.4.3 Session establishment procedure 201
G.4.4 Session release procedure 203
G.4.5 Session modification 203
G.4.6 Media forwarding in the IMS Access Gateway 203

G.5 Network elements for employing NAT Traversal for ICE and Outbound 204
G.5.1 General requirements 204
G.5.2 ICE 204
G.5.2.1 Overview 204
G.5.2.2 Required functions of the UE 205
G.5.2.3 Required functions of the STUN relay server 205
G.5.2.4 Required functions of the STUN server 205
G.5.3 Outbound 206
G.5.3.1 Overview 206
G.5.3.2 Required functions of the P-CSCF 206
G.5.3.3 Required functions of the S-CSCF 206
G.5.3.4 Required functions of the UE 206

G.6 Procedures for employing ICE and Outbound 207
G.6.1 Flow establishment procedures 207
G.6.2 Session establishment procedures 208
G.6.3 Session release procedures 210
G.6.4 Session modification procedures 211
G.6.5 Policy and Charging Control procedures 211
G.6.6 Detection of NAT Traversal support 212
G.6.7 Procedures at other IMS entities processing SDP 212

Annex H (Informative): Example HSS deployment 213

Annex I (normative): Border Control Functions 214

I.1 General 214

I.2 Overall architecture 214

I.3 Border Control Functions 215
I.3.1 IP version interworking 215
I.3.1.1 Originating Session Flows towards IPv4 SIP network 215
I.3.1.2 Terminating Session Flows from IPv4 SIP network 217
I.3.2 Configuration independence between operator networks 218

Annex J (Informative): Dynamic User Allocation to the Application Servers 219

J.1 General 219

J.2 Representative AS 219
J.2.1 Concept of Representative AS 219
J.2.2 Procedures related to Representative AS 220

J.3 Dynamic assignment of AS by S-CSCF caching 220
J.3.1 Concept of Dynamic assignment of AS by S-CSCF caching 220
J.3.2 Procedures related to Dynamic assignment of AS by S-CSCF caching 221

Annex K (normative): Inter-IMS Network to Network Interface between two IM CN subsystem networks 223

K.1 General 223

K.2 Overall architecture 223

Annex L (informative): Change history 224

History 229

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 Annex E.

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] Void.

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

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

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

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

[10] Void.

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

[11] Void.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[25] 3GPP TS 32.240: "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] 3GPP TS 26.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia System (IMS) Messaging and Presence; Media formats and codecs".

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

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

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

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

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

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

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

[45] IETF draft, draft-ietf-mmusic-ice-18: "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", September 13, 2007.

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

[46] IETF draft, draft-ietf-behave-turn-04: "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", July 8, 2007.

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

[47] IETF draft, draft-ietf-behave-rfc3489bis-10: "Session Traversal Utilities for (NAT) (STUN)", July 5, 2007.

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

[48] IETF draft, draft-ietf-sip-outbound-10: "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)", July 5, 2007.

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

[49] IETF draft, draft-ietf-sip-gruu-11: "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)", April 2007.

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

[50] IETF draft, draft-ietf-sipping-gruu-reg-event-08: "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUU)", April 2007.

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

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

[52] 3GPP TS 23.279: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services; Stage 2".

[53] 3GPP TS 22.173: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IMS Multimedia Telephony Service and supplementary services; Stage 1".

[54] 3GPP TS 23.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control architecture".

[55] 3GPP TS 23.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture".

[56] 3GPP TS 23.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access".

[57] IETF RFC 4769 (November 2006): "IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information".

[58] 3GPP TS 23.167: "Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions".

[59] 3GPP TS 29.333: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp Interface; Stage 3;"

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

IP-Connectivity Access Network: refers to the collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities**.** An example of an "IP-Connectivity Access Network" is GPRS.

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

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.

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 domain 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.

ALG: Application Level Gateway (ALG) is an application specific functional entity that allows 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 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. 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 IPv6 and IPv4 SIP applications.

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.

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).

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

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).

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 regarless 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).

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 draft-ietf-behave-rfc3489bis-04 [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 draft-ietf-behave-turn-01 [46] for further details.

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

Outbound: Managing Client Initiated Connections in the Session Initiation Protocol (Outbound) defines behaviors for User Agents, registrars and proxy servers that allow requests to be delivered on existing connections established by the User Agent. See draft-ietf-sip-outbound-04 [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.

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

Alias Public User Identities: A Public User Identity is an alias of another Public User Identity if both identities belong to the same implicit registration set, are linked to the same service profile and have the same service data configured for each and every service.

3.2 Symbols

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

Cx	Reference Point between a CSCF and an HSS.
Dx	Reference Point between an I-CSCF and an SLF.
Gi	Reference point between GPRS and an external packet data network.
Gm	Reference Point between a UE and a P-CSCF.
ISC	Reference Point between a CSCF and an Application Server.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
Ix	Reference Point between IBCF and TrGW.
Ici	Reference Point between an IBCF and another IBCF belonging to a different IM CN subsystem network.

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 to IPv6 network services.
Mg	Reference Point between an MGCF and a CSCF.
Mi	Reference Point between a CSCF and a BGCF.
Mj	Reference Point between a BGCF and an MGCF.
Mk	Reference Point between a BGCF/IMS ALG and another BGCF.
Mm	Reference Point between a CSCF/BGCF/IMS ALG and an IP multimedia network.
Mr	Reference Point between an CSCF and an MRFC.
Mw	Reference Point between a CSCF and another CSCF.
Mx	Reference Point between a CSCF/BGCF and IBCF.
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 following abbreviations apply. Additional applicable abbreviations can be found in GSM 01.04 [1].

AMR	Adaptive Multi-rate
API	Application Program Interface
AS	Application Server
BCSM	Basic Call State Model
BG	Border Gateway
BGCF	Breakout Gateway Control Function
BS	Bearer Service
CAMEL	Customised Application Mobile Enhanced Logic
CAP	Camel Application Part
CDR	Charging Data Record
CN	Core Network
CS	Circuit Switched
CSCF	Call Session Control Function
CSE	CAMEL Service Environment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENUM	E.164 Number
GGSN	Gateway GPRS Support Node
GLMS	Group and List Management Server
GMLC	Gateway Mobile Location Centre
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
IMS	IP Multimedia Core Network Subsystem
IMS ALG	IMS Application Level Gateway
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IP-CAN	IP-Connectivity Access Network
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
NAI	Network Access Identifier
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
SGW	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 bearer related network elements as defined in TS 23.002 [1]. IP multimedia services are based on an IETF defined session control capability which, along with multimedia bearers, utilises the IP-Connectivity Access Network (this may include an equivalent set of services to the relevant subset of CS Services).

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

The IP multimedia core network (IM CN) subsystem enables PLMN operators to offer their subscribers multimedia services based on and built upon Internet applications, services and protocols. There is no intention here to standardise such services within the IM CN subsystem, the intention is that such services will be developed by PLMN operators and other third party suppliers including those in the Internet space using the mechanisms provided by the Internet and the

IM CN subsystem. The IM CN subsystem should enable the convergence of, and access to, voice, video, messaging, data and web-based technologies for the wireless user, and combine the growth of the Internet with the growth in telecommunications.

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

Figure 4.0 below represents the IMS reference architecture including interfaces towards legacy networks and other IP based multimedia systems. Details of the roles of these nodes are described in sections 4.6 and 4.7.

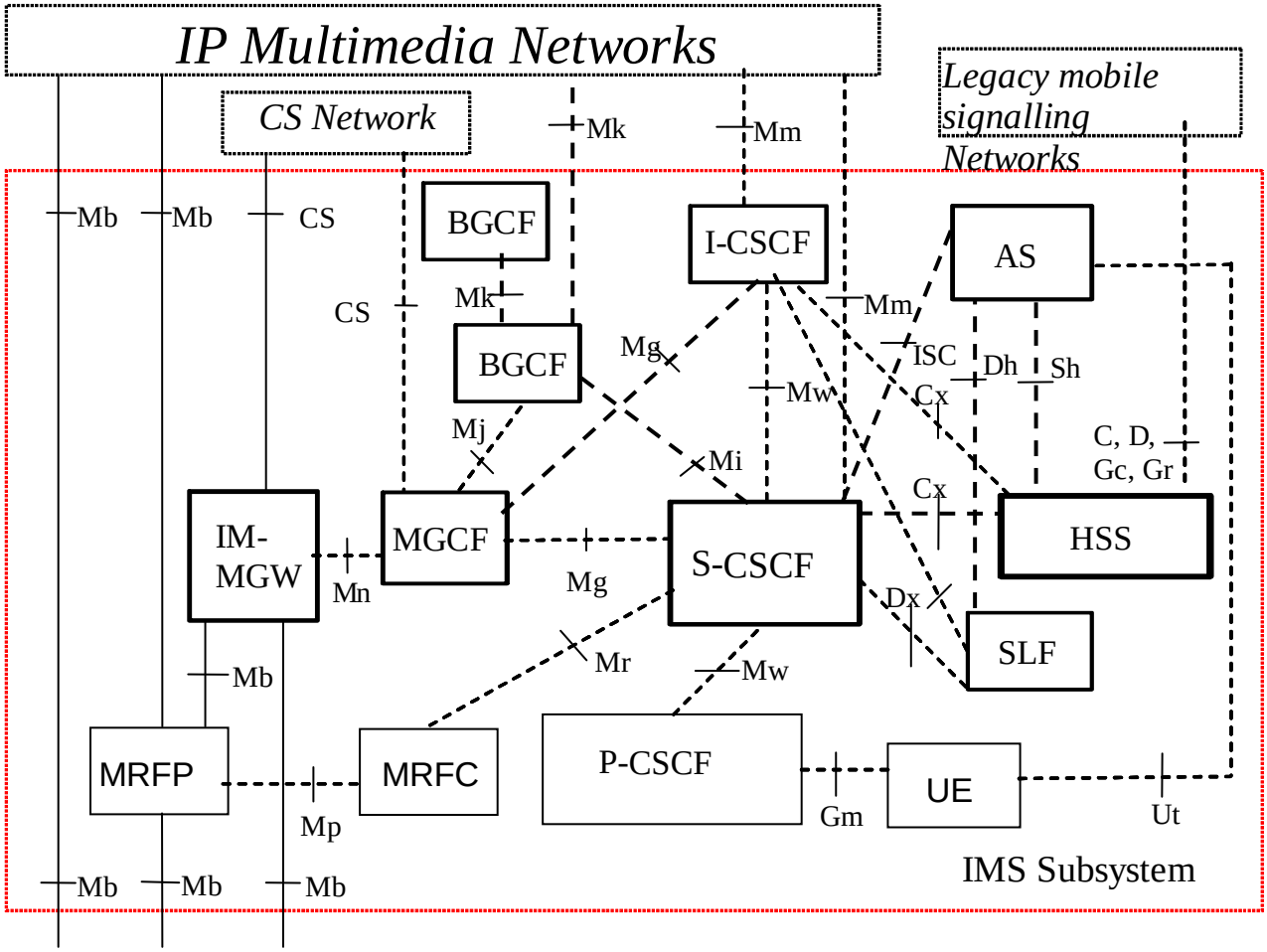


Figure 4.0: Reference Architecture of the IP Multimedia Core Network Subsystem

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. The IP-CAN maintains the service while the terminal moves and hides these moves from the IP multimedia subsystem.

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

4.2 IMS services concepts

4.2.1 Home-network based services

4.2.1.1 Support of CAMEL

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

For more information refer to section 4.2.4.

4.2.1.2 Support of OSA

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

For more information refer to section 4.2.4.

4.2.2 Support of 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 upto 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 case of GPRS access this is the VPLMN. In case of other access types this is most probably the IPCAN 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.

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. 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.

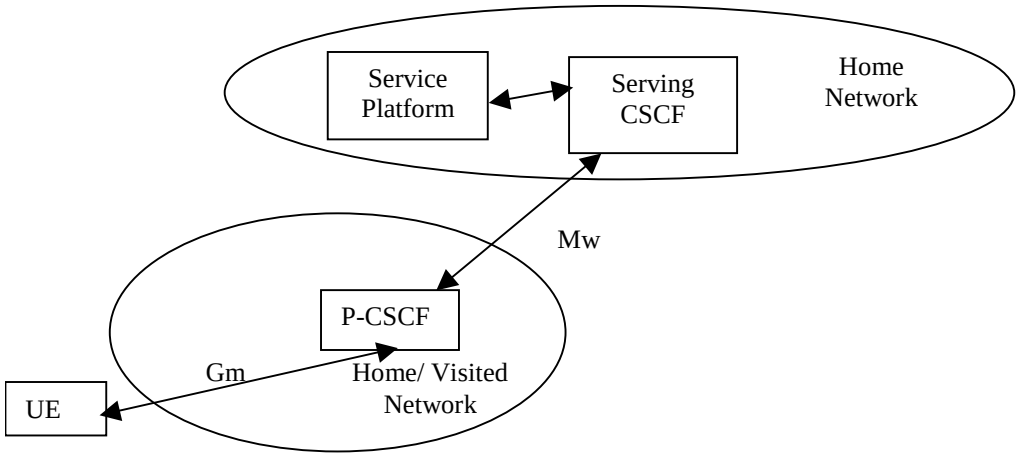


Figure 4.1: Service Platform in Home Network

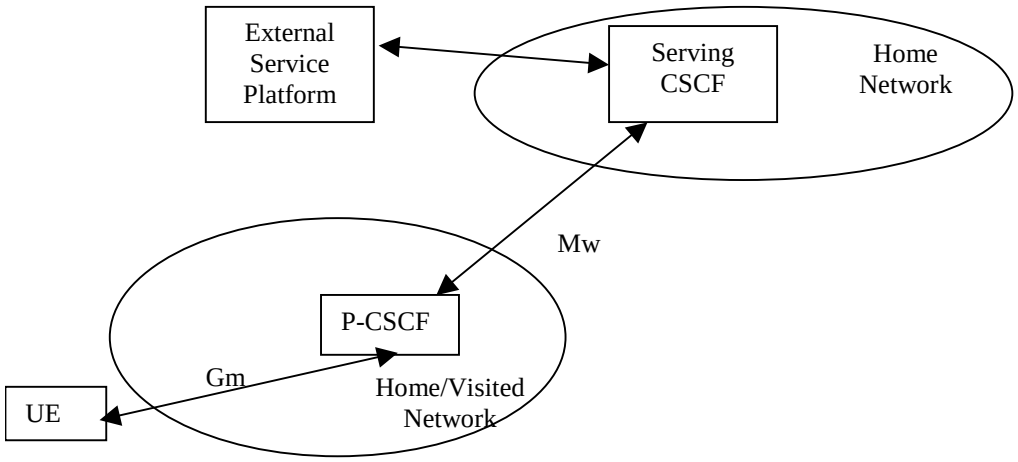


Figure 4.2: External Service Platform

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 section 4.2.4.

The roles that the CSCF plays are described below.

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

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

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

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

Network initiated Proxy-CSCF reassignment is not a requirement.

The use of additional elements to be included in the SIP signalling path is optional. Such additional elements may provide functions as described in Section 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 ISC interface shall be able support subscription to event notifications between the Application Server and S-CSCF to allow the Application Server to be notified of the implicit registered Public User Identities, registration state and UE capabilities and characteristics in terms of SIP User Agent capabilities and characteristics.

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

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

The S-CSCF does not handle service interaction issues.

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

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

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

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

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

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

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). On the ISC interface, extensions to SIP shall be avoided but are not expressly prohibited.

The notion of a "SIP leg" used throughout this specification is identical to the notion of a call leg which is the same as a SIP dialog defined by 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.

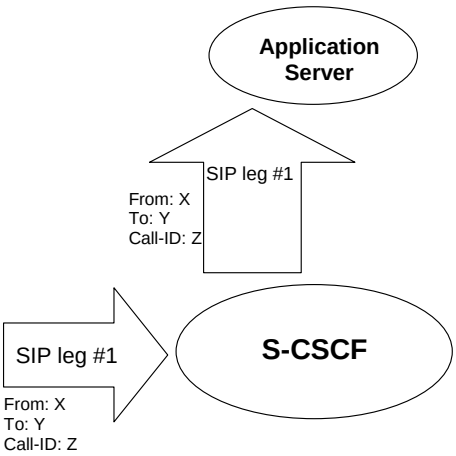


Figure 4.3a: Application Server acting as terminating UA, or redirect server

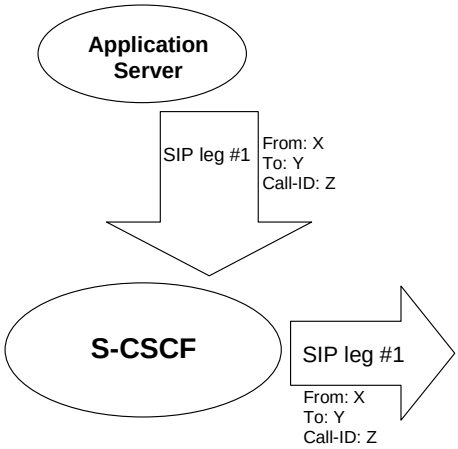


Figure 4.3b: Application Server acting as originating UA

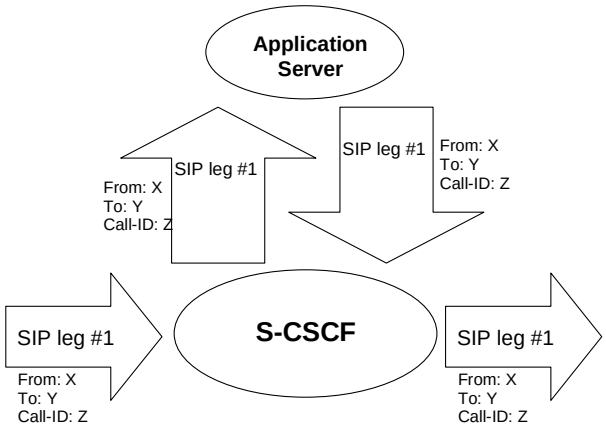


Figure 4.3c: Application Server acting as a SIP proxy

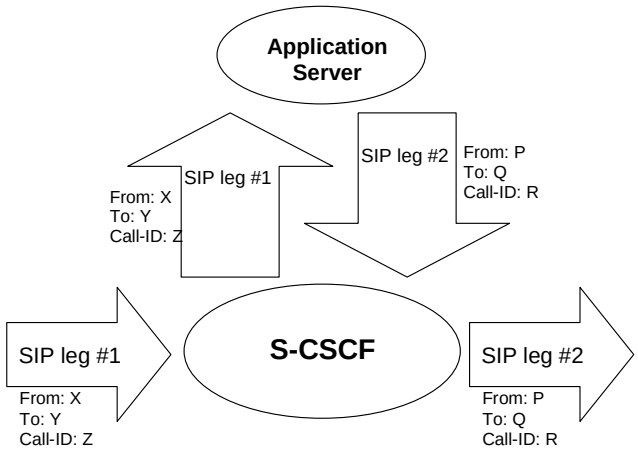


Figure 4.3d: Application Server performing 3rd party call control

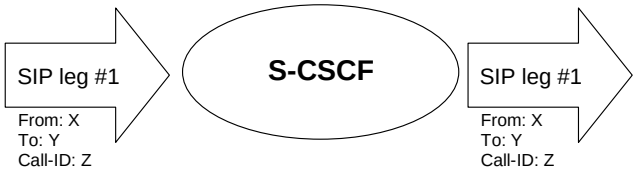


Figure 4.3e: A SIP leg is passed through the S-CSCF without Application Server involvement

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, …
   In this case, the term transparent implies that the exact representation of the information is not understood by the HSS or the protocol.

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

NOTE: before providing information relating to the location of the user to a SIP Application Server, detailed privacy checks frequently need to be performed in order to meet the requirements in 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.

4.2.4b S-CSCF Service Control Model

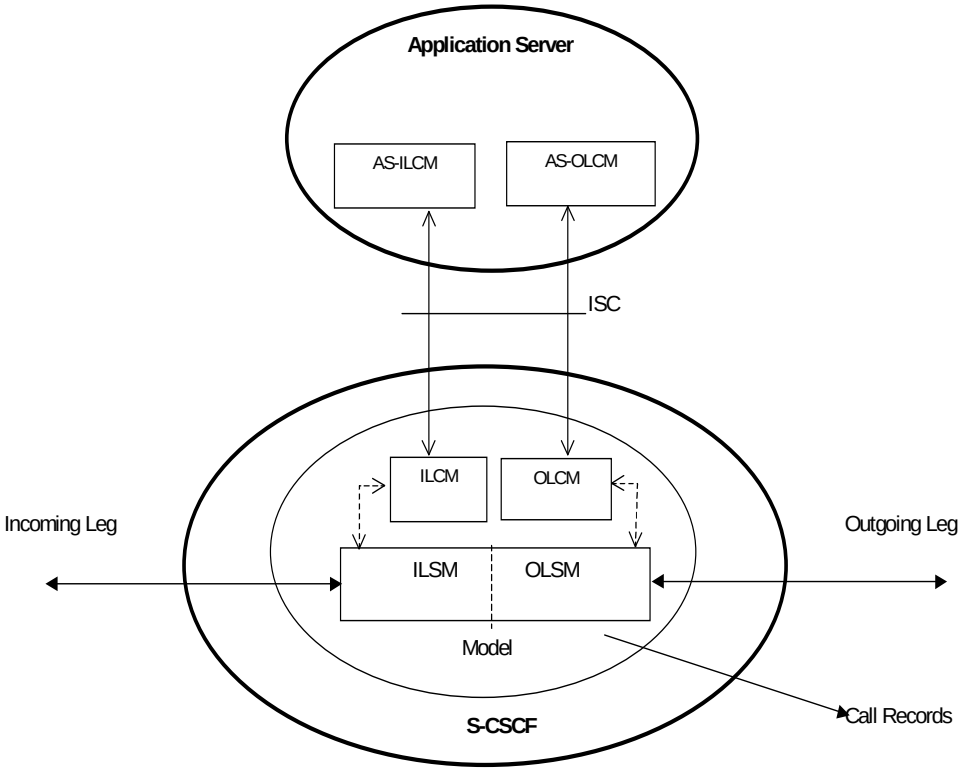


Figure 4.3f: Service Control Model with Incoming Leg Control and Outgoing Leg Control

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.

4.2.5 The QoS requirements for an IM CN subsystem session

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

1. Independence between QoS signalling and Session Control

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

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

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

3. Void.

4. Restricted Resource Access at the IP BS Level

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

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

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

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

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

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

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

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

   e. In establishing an IMS session, it shall be possible to use already allocated bearer resources, if these resources 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 bulletpoint below.

    2. If the UE has indicated preference information for contact addresses upon registration, then the S-CSCF shall use it to decide if parallel or sequential forking is used across the contact addresses that have matching callee capabilities, as described in 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 section.

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. In case the UE or MGCF receives a subsequent 200 OK, the UE or MGCF shall acknowledge the dialogue and immediately send a BYE to drop the dialog.

NOTE: Upon the reception of a first final 200 OK (for INVITE), the UE or MGCF may terminate the early dialogue, as specified in 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 3041 [16a], or similar means. When a UE is registered in the IM CN Subsystem with an IP address, any change to this IP address that is used to access the IM CN subsystem will result in dropping the active SIP dialogs, and shall trigger automatic registration. This automatic registration updates the UE's IP address and security association. To avoid disruption of ongoing IM CN subsystem services, the UE should not change the IP address that it uses to access the IM CN subsystem while engaged in active SIP dialogs (e.g. INVITE or SUBSCRIBE-NOTIFY dialogs).

4.3.2 Void

Figure 4.4: Void

4.3.3 Identification of users

4.3.3.0 General

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

4.3.3.1 Private user identities

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

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

4.3.3.2 Public user identities

Every IM CN subsystem user shall have one or more Public User Identities (see TS 22.228 [8]). The Public User Identity/identities are used by any user for requesting communications to other users. For example, this might be included on a business card.

- Both telecom numbering and Internet naming schemes can be used to address users depending on the Public User identities that the users have.
- The Public User Identity/identities shall take the form of a SIP URI (as defined in IETF RFC 3261 [12] and IETF RFC 2396 [13]) or the "tel:"-URI format IETF RFC 3966 [15].
- An ISIM application shall securely store at least one Public User Identity (it shall not be possible for the UE to modify the Public User Identity), but it is not required that all additional Public User Identities be stored on the ISIM application.
- A Public User Identity shall be registered either explicitly or implicitly before 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 section 5.6.5.
- 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 IMPUs 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.

NOTE: An implicit registration set may contain Public User Identities of more than one service profile.

- 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 draft-ietf-sip-gruu [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. A single instance ID should be assigned by the UE regardless of the number of IP-CANs interfacing with the UE.

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 generatation 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 draft-ietf-sip-gruu [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.

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.

When the value of a public user identifier 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 2396 [13]. Routing of SIP signalling within the IMS using AbsoluteURI (non SIP) shall only be supported for IMS signalling from IMS user to external networks. E.164 [2] format Public User Identities shall not be used for routing within the IMS, and session requests based upon E.164 format Public User Identities will require conversion into SIP URI format for internal IMS usage.

4.3.3.3a Handling of dialled number formats

When using a phone number as the dialled address, the UE can provide this number in the form of a SIP URI or a TEL 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.

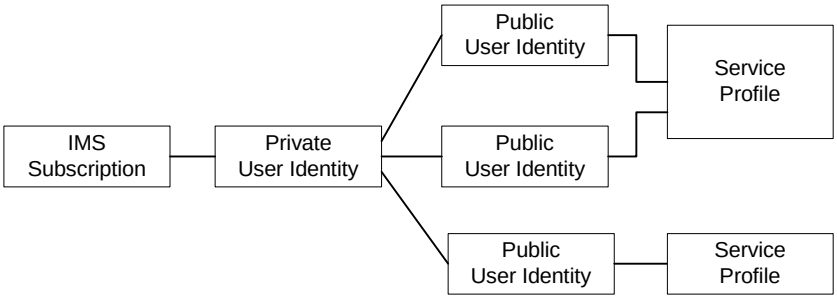


Figure 4.5: Relationship of the Private User Identity and Public User Identities

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. 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.

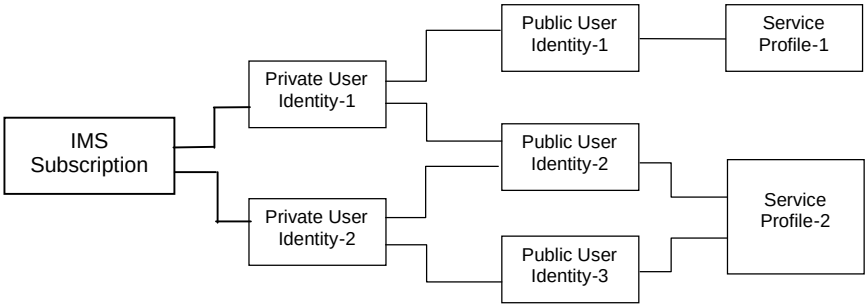


Figure 4.6: The relation of a shared Public User Identity (Public-ID-2) and Private User Identities

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.

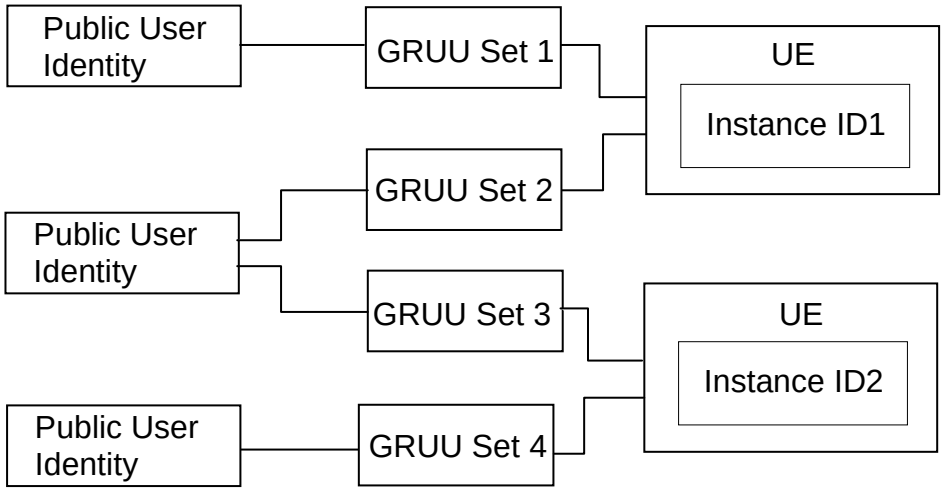


Figure 4.6a: The relationship of Public User Identities, GRUUs, and UEs

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

The S-CSCF shall support the ability to translate the E.164 address contained in a Request-URI in the non-SIP URI Tel: URI format IETF RFC 3966 [15] to a SIP routable SIP URI using an ENUM DNS translation mechanism with the format as specified in IETF RFC 3761 [16]. 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 routed to a BGCF for further routing as described in clause 5.19 or appropriate notification shall be sent to the originating session endpoint, depending on network operator configuration..

Per operator policy, the network may or may not attempt to address resolve and route a SIP URI with user=phone and a domain that does not own the target user. The need for address resolution may be triggered by the S-CSCF, and the I-CSCF or transit function, as determined by the operator directed network 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, operator policy shall dictate whether the procedure should be carried out for all the domains of the SIP URI, only if the domain belongs to the home network, or not at all. If operator policy indicates that the procedure is to be performed, then the S-CSCF shall attempt to translate the E.164 address in the SIP URI into a globally routable SIP URI using an ENUM/DNS translation mechanism as determined by operator policy. If this translation fails, the request MAY be forwarded to a BGCF to allow routing to the PSTN. If this translation succeeds, the S-CSCF shall update the Request URI and route the request based on the globally routed SIP URI that was obtained. (Note that these enhancements would make handling of this case equivalent to the handling of a Tel URI).

If the operator policy at the S-CSCF dictates that the procedure is not performed, then the S-CSCF handles and routes the request in the same manner as a SIP-URI.

Prior to an HSS Location Query, the I-CSCF shall translate an E.164 address contained in a Request-URI having the SIP URI with user=phone parameter format into the Tel: URI format of IETF RFC 3966 [15]. The Tel: URI format shall be used in this case for performing the HSS Location Query.

In the event of HSS Location Query response from the HSS that indicates that the user does not exist, and if configured by operator policy, 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.Note that the entire transit functionality is not required for this purpose. If this translation succeeds, then the session shall be routed according to the returned

SIP URI. If the translation fails, then the session may be routed to a BGCF for further routing as described in clause 5.19 or appropriate notification shall be sent to the originating session endpoint, depending upon network operator configuration.

The actual ENUM/DNS database(s) used to perform address translations are outside the scope of 3GPP andare therefore a matter for the IM 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], section 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.

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 Section 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;
- 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 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 sections describe these various roles.

4.6.1 Proxy-CSCF

The Proxy-CSCF (P-CSCF) is the first contact point within the IM CN subsystem. Its address is discovered by UEs using the mechanism described in section "Procedures related to Local CSCF Discovery". The P-CSCF behaves like a Proxy (as defined in 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: 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 founf in Section 4.14 and Annex I.

The interface between the Policy and Charging Rules Function (PCRF) and the P-CSCF is the Rx interface standardised in TS 23.203 [54].

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.
- Forward the SIP request or response to the UE.

  Detect and handle an emergency session establishment request as per error handling procedures defined by stage-3.
- Generation of CDRs.
- Maintain a Security Association between itself and each UE, as defined in TS 33.203 [19].
- Should perform SIP message compression/decompression.
- Authorisation of bearer resources and QoS management. For details see TS 23.203 [54].

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: In case border control concepts are applied, the contact point within an operator's network may be different, see Section 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 Section 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 section on Procedures related to Serving-CSCF assignment)

Session-related and session-unrelated flows

- Route a SIP request received from another network towards the S-CSCF.
- 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 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.

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 subclause 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 orginating user's subscription.

- 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].

- 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 an ENUM/DNS translation mechanism (either this is done only for domains in the SIP URI known by the S-CSCF to belong to the home network, or as for all domains depending on local policy). If this translation fails, the request may be forwarded to a BGCF to allow routing to the PSTN. If this translation succeeds, the Request URI is updated and the request is routed based on the globally routed SIP URI that was obtained.

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 founf in Section 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 and 5.19).

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 Section 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.

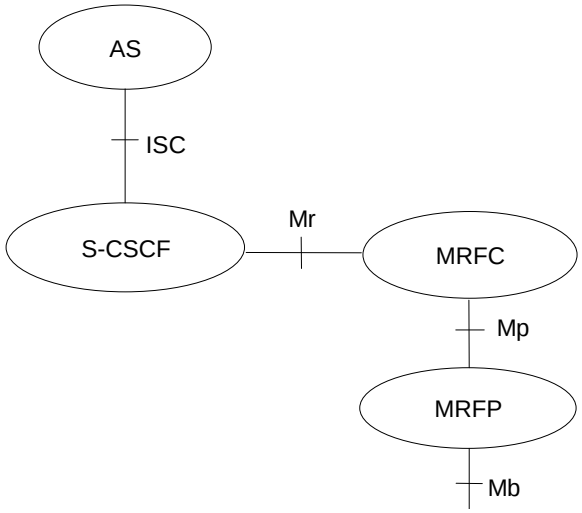


Figure 4.7: Architecture of MRF

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 reference point is SIP (as defined by IETF RFC 3261 [12], other relevant IETF RFCs, and additional enhancements introduced to support 3GPP´s needs).

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

The Mp reference point has the following properties:

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

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

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 section 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.

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 2: 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 authorise 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.

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

NOTE 3: 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.

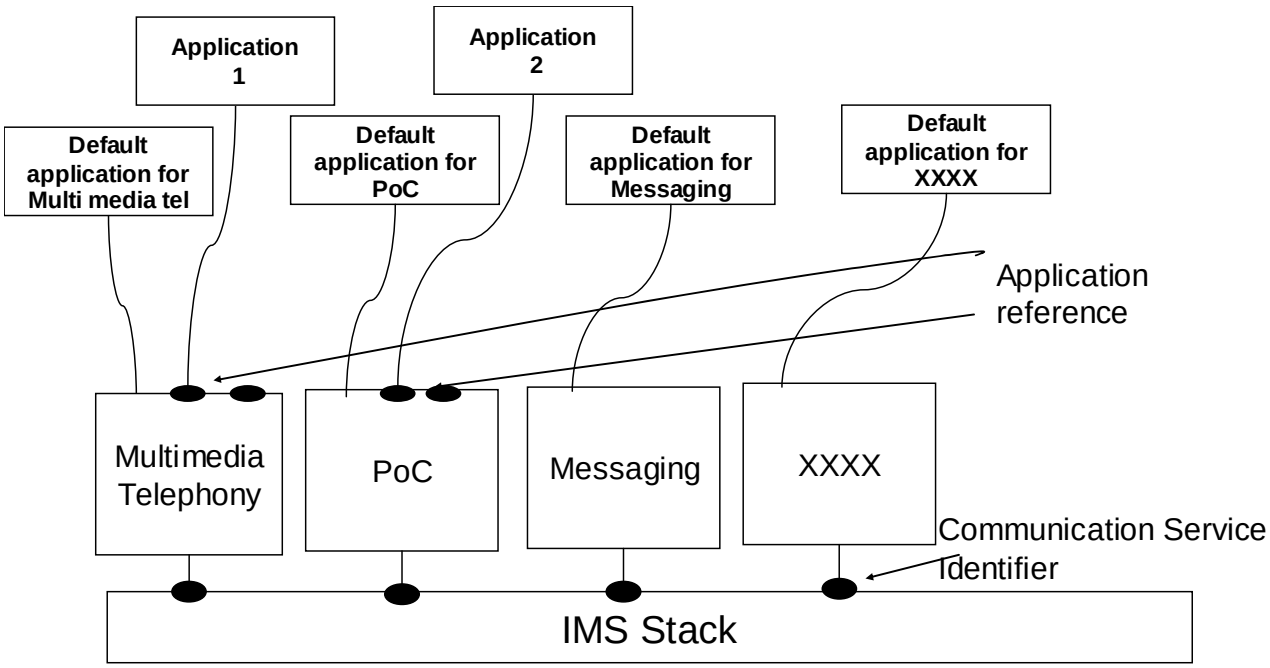


Figure 4.13-1: IMS applications on top of an IMS communication service

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; Mi, Mj, Mk, Mw; Mg; Mr; Ro, Rx, Rf.

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;

- 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.

In case 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.

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 the operator's I-CSCF (or IBCF) and PSTN traffic arrives at the operator's MGCF. This is the same as the normal Mobile Terminating cases for IMS. 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.

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 colocated.

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.

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 URI with user=phone parameters. NP is subject to regional requirements and is accomplished through the retrieval of ported data from those data bases. The specification of these data bases is out of 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, the S-CSCF as an example, needs to support, or not remove, NP protocol parameters retrieved as part of ENUM/DNS procedures contained in this specification. Subsequent network elements used to process the call to the PSTN do 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.

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.

5 IP multimedia subsystem procedures

5.0 General

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

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

5.0a Session-unrelated procedures

The IM CN Subsystem provides means to conduct session-unrelated interactions between users, e.g. OPTIONS query, outband REFER. These interactions are described in 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 sections and specifications.

5.1 CSCF related procedures

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

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

5.1.1 Procedures related to local CSCF discovery

5.1.1.0 General

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

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

- Alternatively, the P-CSCF discovery may be 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.

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.

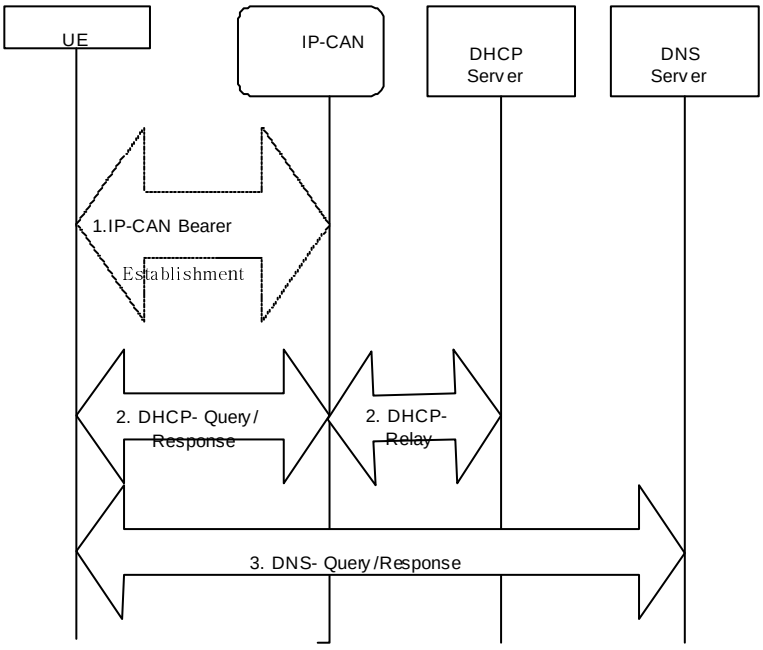


Figure 5.0a: P-CSCF discovery using DHCP and DNS

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 section provides the information flows for subscription data updating procedure.

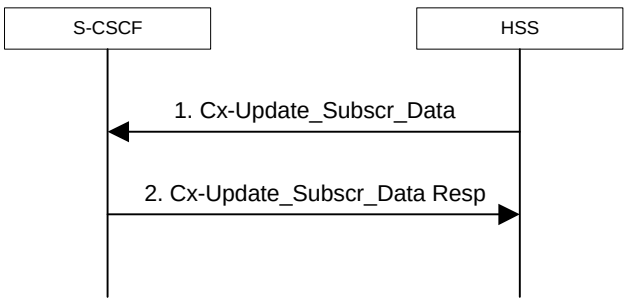


Figure 5.0b: Subscription data updating

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

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

5.2 Application level registration procedures

5.2.0 General

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

5.2.1 Requirements considered for registration

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

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

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

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

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

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

6. The Serving-CSCF is able to retrieve a service profile of the user who has IMS subscription. The S-CSCF shall check the registration request against the filter information and if necessary inform 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. In case the user/operator wants to prevent this Public User Identity from being used for IMS communications, it shall be possible to do so in the network without affecting the ISIM application directly.

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

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

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

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

12. When multiple UEs share the same public identity (es), each UE shall be able to register its contact address(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. If the relevant Service Point Trigger is configured, the S-CSCF shall use the UE capabilities provided during registration for initial filter criteria match processing.

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 draft-ietf-sip-gruu [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.

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.

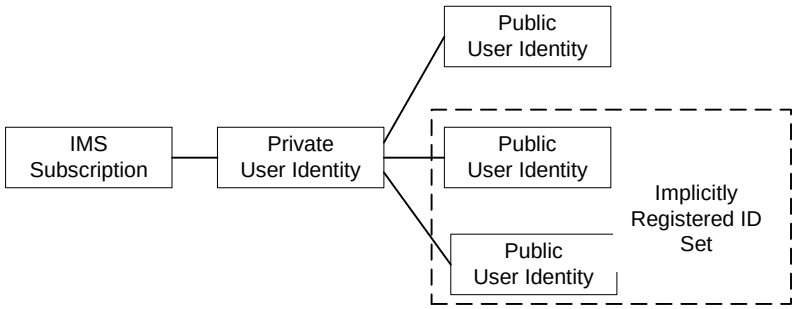


Figure 5.0c: Relationship of Public User Identities when implicitly registered

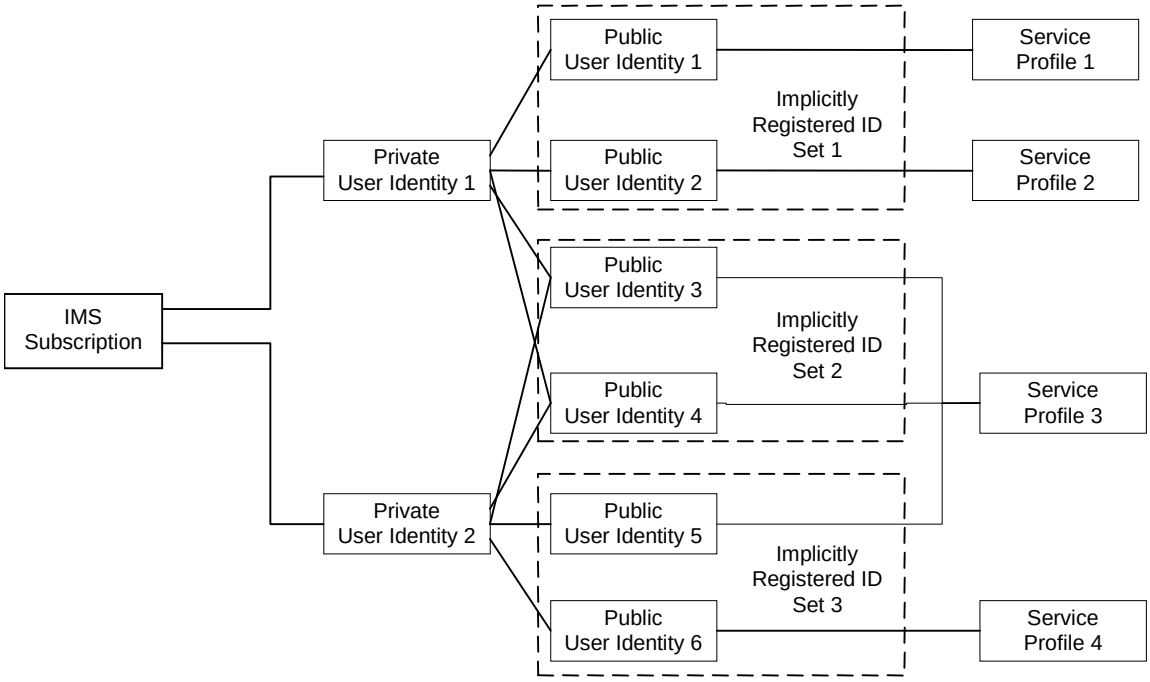


Figure 5.0d: The relation of two shared Public User Identities (Public-ID-3 and 4) and Private User Identities

5.2.1a.1 Implicit Registration for UE without ISIM

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

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

5.2.2 Registration flows

5.2.2.1 Requirements to consider for registration

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

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

5.2.2.2 Assumptions

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

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

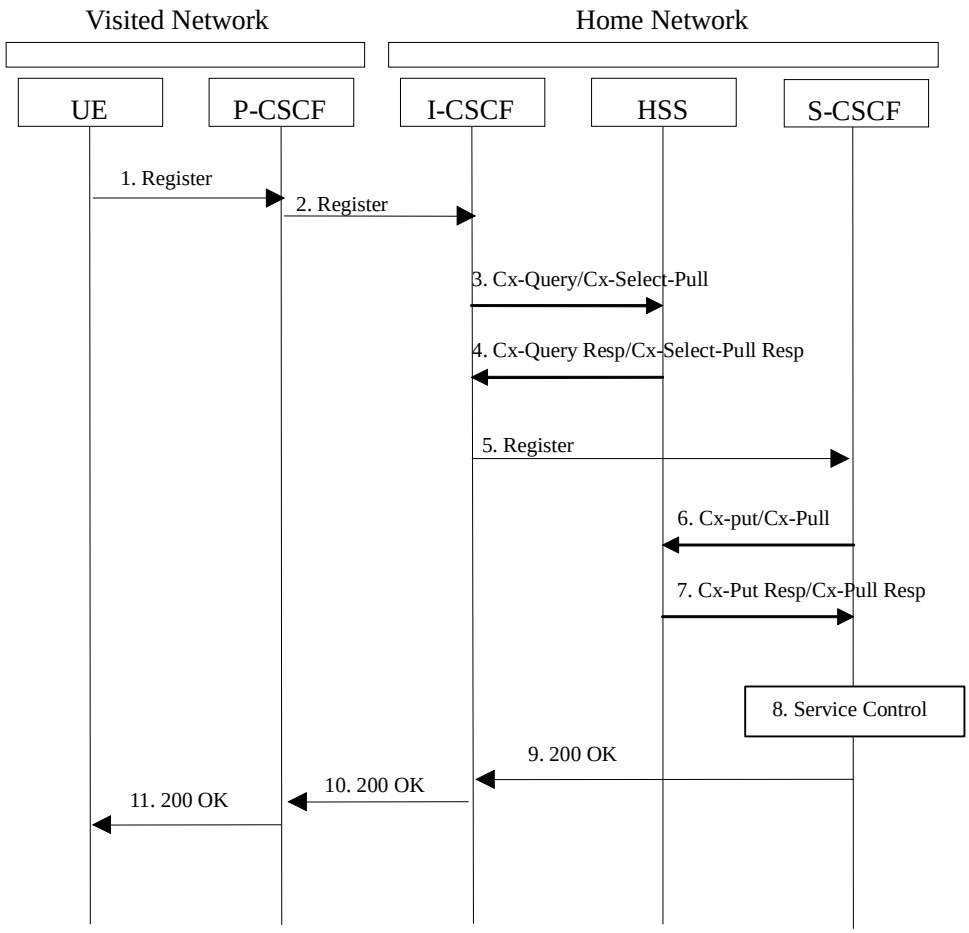


Figure 5.1: Registration – User not registered

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 perform the new S-CSCF selection function based on the capabilities returned.

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

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. The I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. 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. 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 subcribe at the PCRF to notifications of the status of the IMS Signalling connectivity (see TS 23.203 [54] for more details).

5.2.2.4 Re-Registration information flow – User currently registered

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

NOTE 1: if the UE does not re-register, any active sessions may be deactivated.

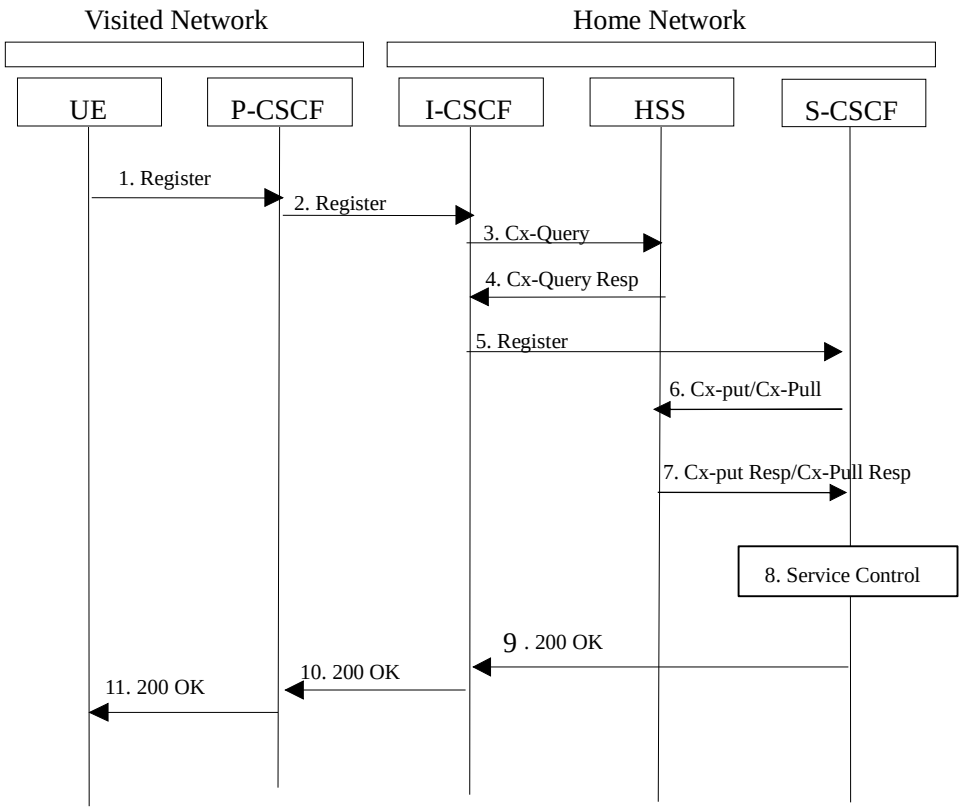


Figure 5.2: Re-registration - user currently registered

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).

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.

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.

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 subclause 5.2.2.3 "Registration Information Flow – User not registered".

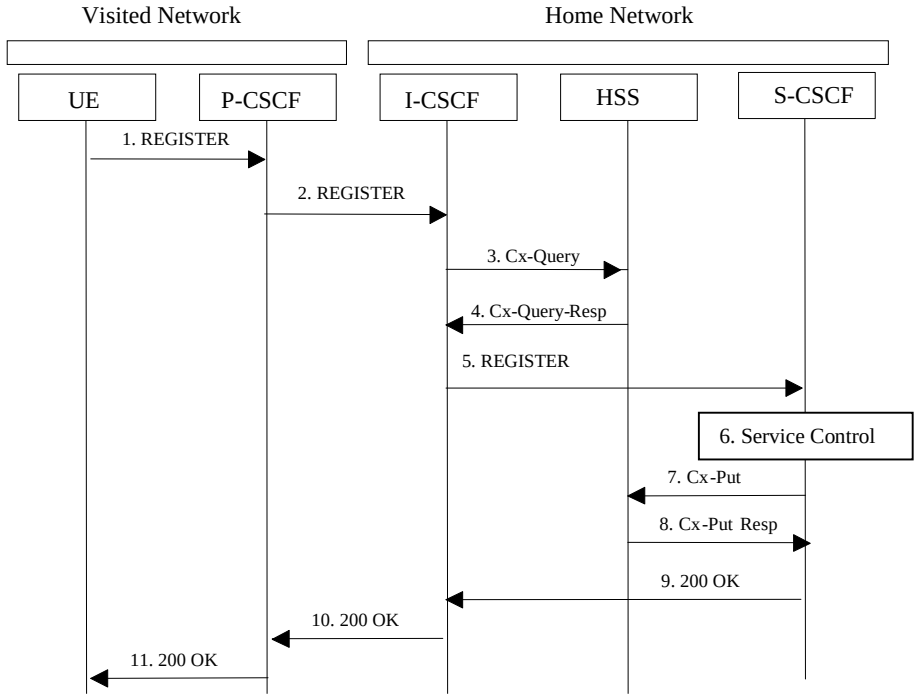


Figure 5.3: De-registration - user currently registered

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

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

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

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

   The HSS then either clears or keeps the S-CSCF name for that Public User Identity according to the Cx-Put request. 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] 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 case of data inconsistency at node failure, in case of UICC lost, etc. Cancelling the current contexts of the user spread among the IM CN Subsystem network nodes at registration, and imposing a new IM registration solves this condition.

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

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

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

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

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

- To deal with registrations expirations.

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

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

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

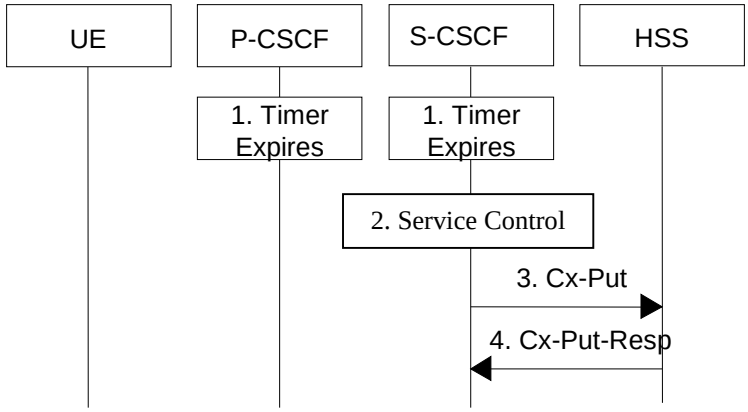


Figure 5.4: Network initiated application de-registration, registration timeout

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

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

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

   The HSS then either clears or keeps S-CSCF name for that Public User Identity according to 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 authorisation, etc. This scenario only addresses the specific action of clearing the SIP application registration that is currently in effect.

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

5.3.2.2.1 Network Initiated De-registration by HSS, administrative

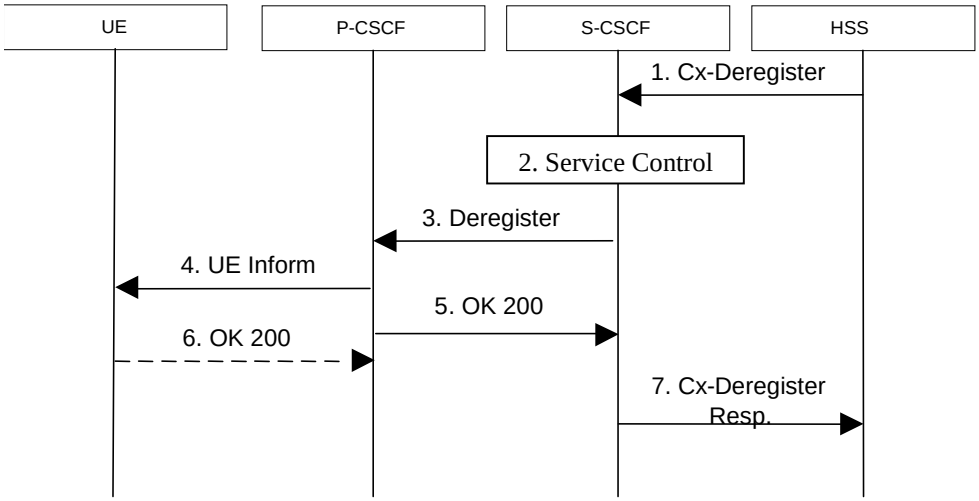


Figure 5.5: Network initiated application de-registration by HSS, administrative

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

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

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

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

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

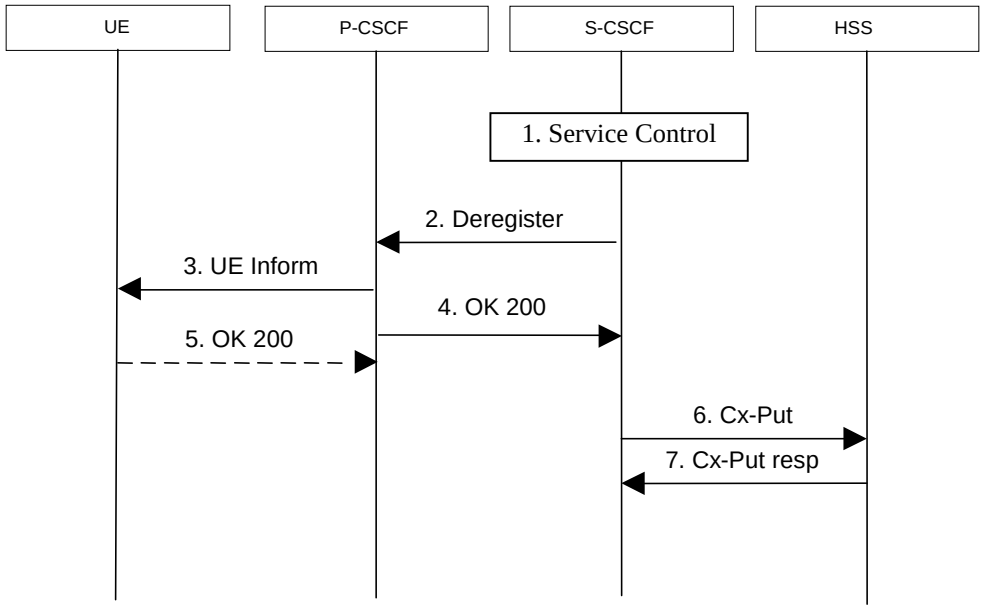


Figure 5.5a: Network initiated application de-registration, service platform

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

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

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 defined in TS 26.235 [21]. The use of default codecs within the UE enables the IM CN subsystem to interwork with other networks on an end to end basis or through transcoding.

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

In order to support existing network capabilities, it is required that 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. 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.

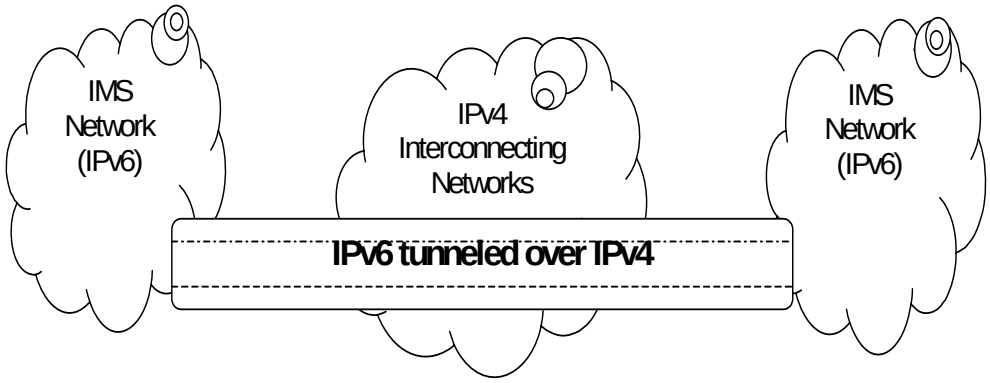


Figure 5.5b: Example tunneling of IPv6 traffic over IPv4 networks

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.

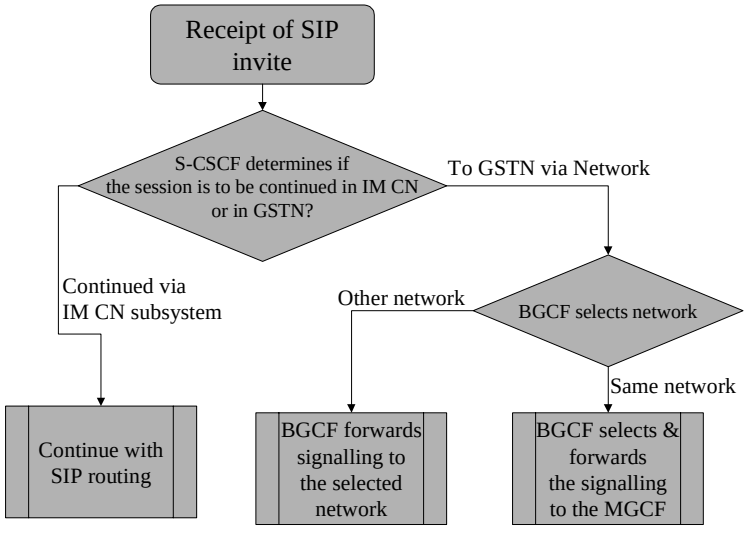


Figure 5.6: Network based PSTN interworking breakout process

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 suspend\ed 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 expressed in 23.221[7].

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

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

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

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

5.4.5.2 P-CSCF in the Session Path

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

5.4.5.3 S-CSCF in the Session Path

All initial requests to or from the UE traverse the S-CSCF assigned to the UE. The S-CSCF uses the "Record-Route" mechanism defined in 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.

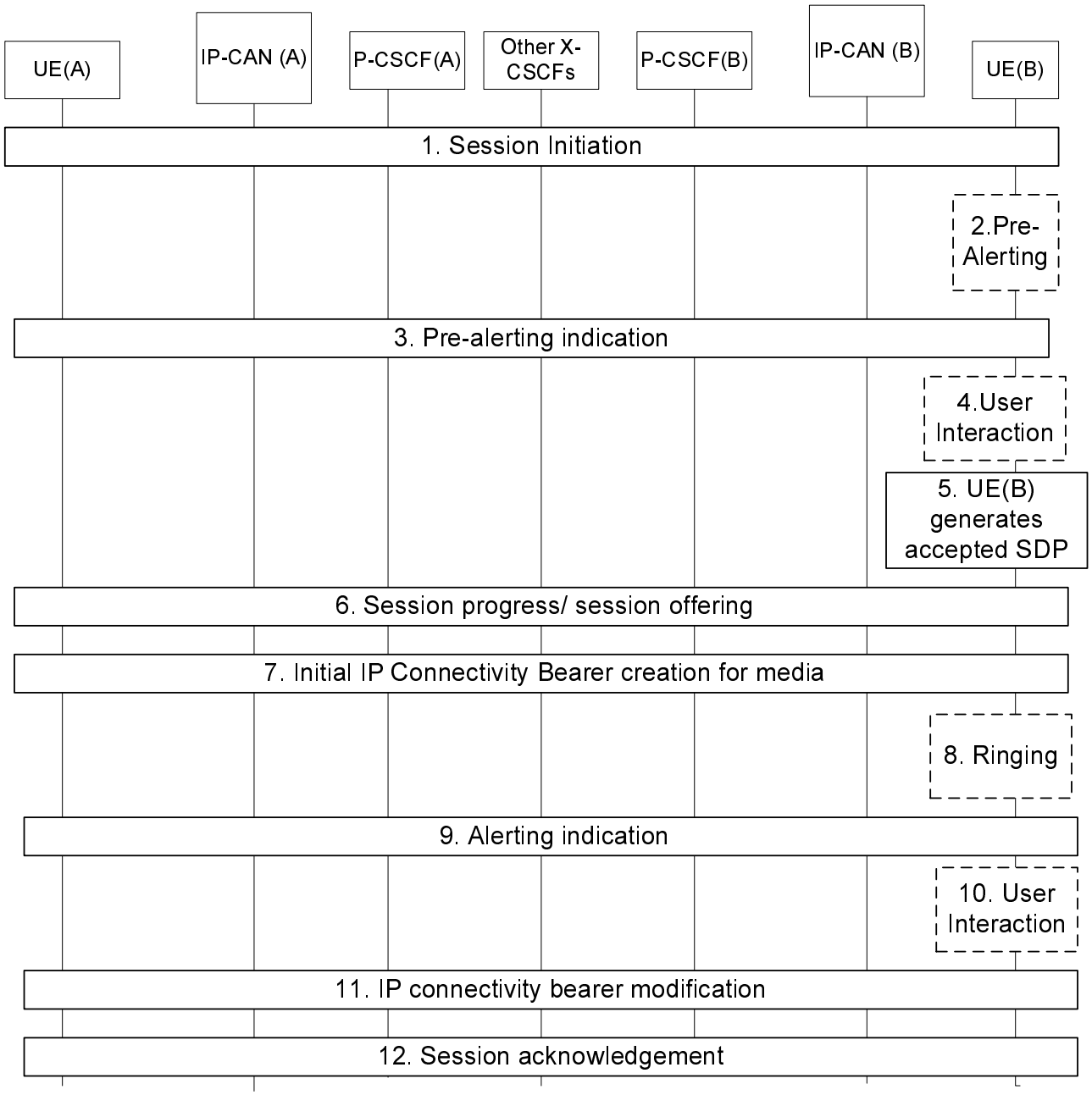


Figure 5.7: Bearer establishment showing optional pre-alerting

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, the bearer is established according to the user's subscription, local operator's IP bearer resource based policy, local operator's admission control function and roaming agreements.

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

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

The IP-Connectivity Access Network contains a Policy and Charging Enforcement Function (PCEF) that has the capability of policing packet flow into the IP network, and restricting the set of IP destinations that may be reached from/through an IP-CAN bearer according to a packet classifier. This 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 (the interface between the PCRF and the P-CSCF is the Rx interface standardised in TS 23.203 [54]).

There are eight interactions defined for Policy and Charging Control:

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

These requirements and functional description of these interactions are explained further in the following sections. The complete specification of the interface between the Policy and Charging Rules Function and the Policy and Charging Enforcement Function is contained in TS 23.203 [54].

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 signaling to derive the session information that is relevant for Policy and Charging Control and forwards it to the PCRF. The PCRF shall use the received information to calculate the proper authorisation. This enables the PCRF to authorize the required QoS resources.

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

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.

Authorisation 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 authorisation, possibly based on provisioning and/or based on requested parameters, which may be IP-CAN specific.

Resource Reservation is initated 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]:

- Resource reservation requests initiated from the UE shall contain the traffic mapping information which enables the IP-CAN to correctly match the reservation request to the corresponding authorisation. The authorisation is normally 'Pulled' from the PCRF 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 authorised 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 authorisation of QoS resources. The PCRF "Pushes" the authorisation 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.

5.4.7.2 Enabling of Media Flows

The PCRF 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 authorisations 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 may authorise the "logical OR" of the resources requested in the responses. When the session established indication has been received, if the PCRF earlier have authorised the "logical OR" of the resources then the PCRF will modify the authorisation 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, 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 authorised by the PCRF.

5.4.7.3 Disabling of Media Flows

The PCRF 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 authorisations. 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, e.g. by closing the gate and blocking the media flow.

5.4.7.4 Revoke Authorisation 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 provides indication to the PCEF within the IP-CAN when the resources previous authorised, 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 authorisation from the PCRF shall be reported to the PCRF 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.

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 case of a modification of a SIP session which results in an update of the authorization as described in subclause 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 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.

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.

5.4.8 QoS-Assured Preconditions

This section contains concepts for the relation between the resource reservation procedure and the procedure for end-to-end sessions.

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

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

The following cases exist in the context of using "QoS-Assured" preconditions for IMS:

a. The IMS session requires the reservation of additional bearer resources, and the UE requires confirmation from the other endpoint of the fulfilment of the pre-conditions related to this resource reservation. 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: The flows of sections 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 section 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.

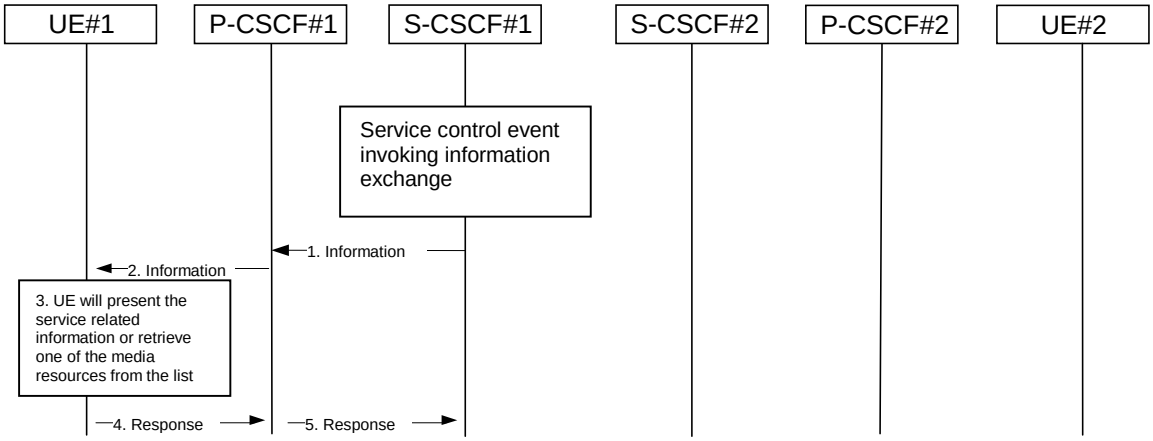


Figure 5.8: Providing service event related information to related endpoint

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 authorisation 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, in case the S-CSCF does not execute any functions for the subsequent requests and responses of the dialog. The

example, in figure 5.8a below, assumes that the S-CSCF does not want to execute any functions for the subsequent requests.

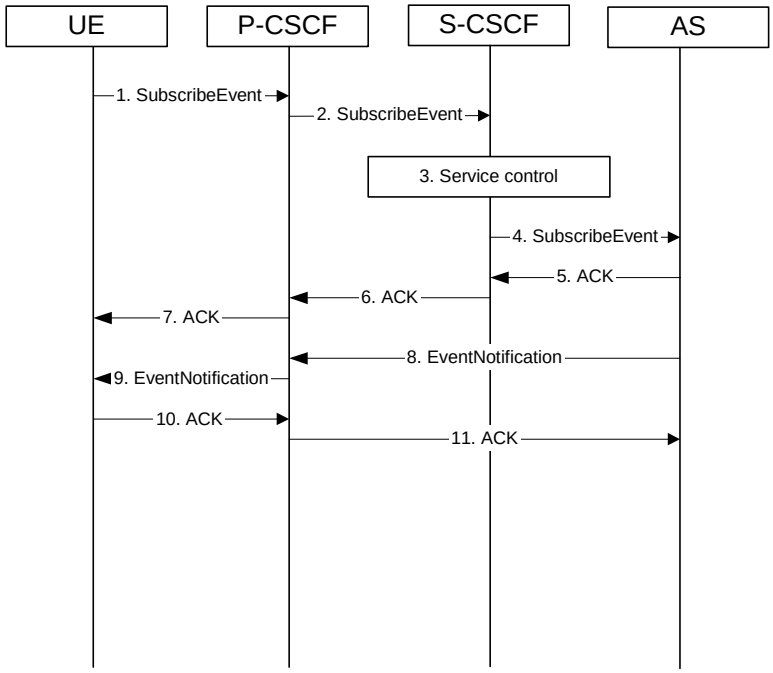


Figure 5.8a: Subscription to event in AS

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

5.4.10 Void

5.4.11 Signalling Transport Interworking

A Signalling gateway function (SGW) is used to interconnect different signalling networks i.e. SCTP/IP based signalling networks and SS7 signalling networks. The signalling gateway function may be implemented as a stand alone entity or inside another entity (see TS 23.002 [1]). The session flows in this specification do not show the SGW, but when interworking with PSTN/CS domain, it is assumed that there is a SGW for signalling transport conversion.

5.4.12 Configuration and Routing principles for Public Service Identities

5.4.12.0 General

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

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

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

5.4.12.1 PSIs on the originating side

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

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

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

5.4.12.2 PSIs on the terminating side

The Application Server hosting the PSI may be invoked as a terminating Application Server via information stored in the HSS. Such PSIs are globally routable and can be made available to users within and outside the operator domain, and can take the following form:

- Distinct PSIs 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 sub-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 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: URL, ENUM translation needs to be performed, and the request shall be routed based on the translation result.

Routing from the Originating AS hosting the PSI can be performed as follows:

a) 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 doesn't 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.

5.4a Overview of session flow procedures

5.4a.1 End-to-End session flow procedures

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

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

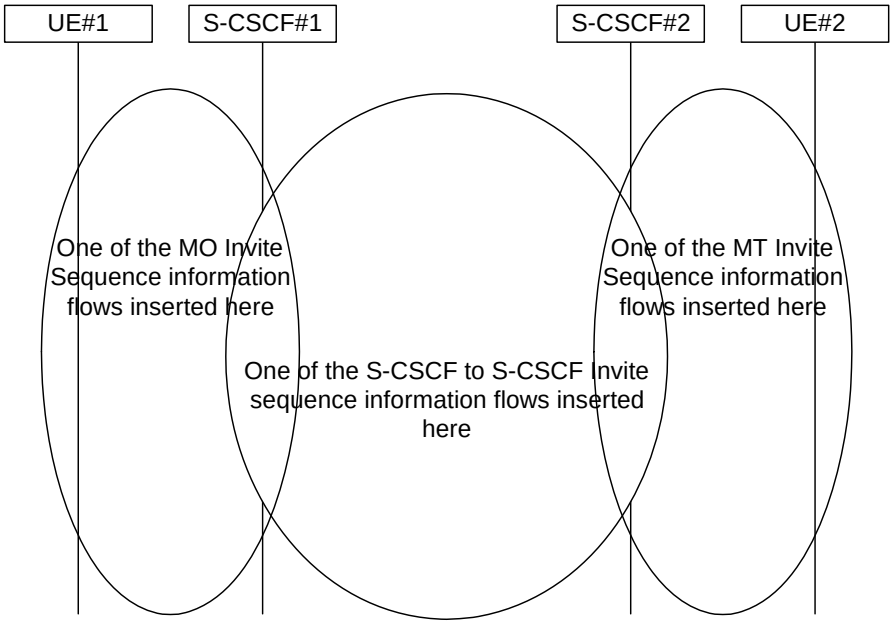


Figure 5.9: Overview of Session Flow Sections

The following procedures are defined:

For the origination sequences:

- (MO#1) Mobile origination, roaming , see subclause 5.6.1;
- (MO#2) Mobile origination, home, see subclause 5.6.2;
- (PSTN-O) PSTN origination, see subclause 5.6.3;
- (NI-O) Non-IMS network origination (external SIP client), see subclause 5.6.4;
- (AS-O) Application Server origination, see subclause 5.6.5.

For the termination sequences:

- (MT#1) Mobile termination, roaming, see subclause 5.7.1;
- (MT#2) Mobile termination, home, see subclause 5.7.2;
- (MT#3) Mobile termination, CS Domain roaming, see subclause 5.7.2a;
- (PSTN-T) PSTN termination, see subclause 5.7.3;
- (NI-T) Non-IMS network termination (external SIP client), see subclause 5.7.4;
- (AS-T#1) PSI based Application Server termination, direct, see subclause 5.7.5;
- (AS-T#2) PSI based Application Server termination, indirect, see subclause 5.7.6;
- (AS-T#3) PSI based Application Server termination, direct, using DNS, see subclause 5.7.7;
- (AS-T#4) PUI based Application Server termination, indirect, see subclause 5.7.8.

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

- (S-S#1) Session origination and termination are served by different network operators, see subclause 5.5.1;
- (S-S#2) Session origination and termination are served by the same operator, see subclause 5.5.2;
- (S-S#3) Session origination with PSTN termination in the same network as the S-CSCF, see subclause 5.5.3;
- (S-S#4) Session origination with PSTN termination in a different network to the S-CSCF, see subclause 5.5.4.

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

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

- (MO#2) Mobile origination, home,
- (S-S#2) Single network operator,
- (MT#2) Mobile termination, home.

There are a large number of end-to-end session flows defined by these procedures. They are built from combinations of origination, serving to serving, and termination procedures, as determined from the following table. For each row of the table, any one of the listed origination procedures can be combined with any one of the serving-serving procedures, which can be combined with any one of the termination procedures.

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 subclause 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.

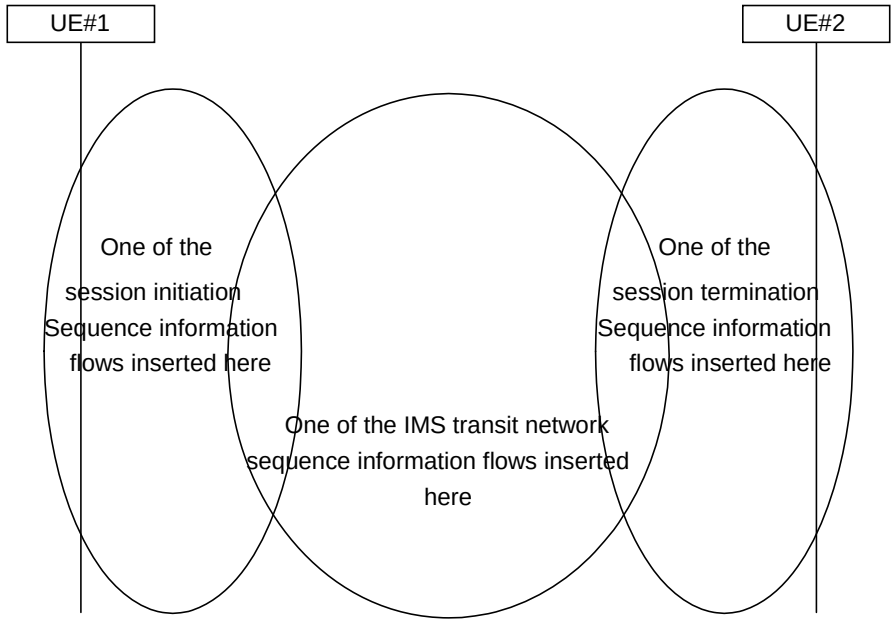


Figure 5.9a: Overview of Session Flow Sections for transit scenarios

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 subclause 5.6.1;
- (MO#2) Mobile origination, home, see subclause 5.6.2;
- (PSTN-O) PSTN origination, see subclause 5.6.3;
- (NI-O) Non-IMS network origination (external SIP client), see subclause 5.6.4;

For the termination sequences:

- (MT#1) Mobile termination, roaming, see subclause 5.7.1;
- (MT#2) Mobile termination, home, see subclause 5.7.2;
- (MT#3) Mobile termination, CS Domain roaming, see subclause 5.7.2a;
- (PSTN-T) PSTN termination, see subclause 5.7.3;
- (NI-T) Non-IMS network termination (external SIP client), see subclause 5.7.4;

For the IMS transit network aspects seeclause 5.19.

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

5.5.0 General

This section presents the detailed application level flows to define the procedures for Serving-CSCF/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 section contains four session flow procedures, showing variations on the signalling path between the Serving-CSCF that handles session origination, and the Serving-CSCF that handles session termination. This signalling path depends on:

- whether the originator and destination are served by the same network operator,
- whether the network operators have chosen to hide their internal configuration.

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

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

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

The Serving-CSCF handling session origination performs an analysis of the destination address, and determines that it belongs to a subscriber of a different operator. The request is therefore forwarded 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.

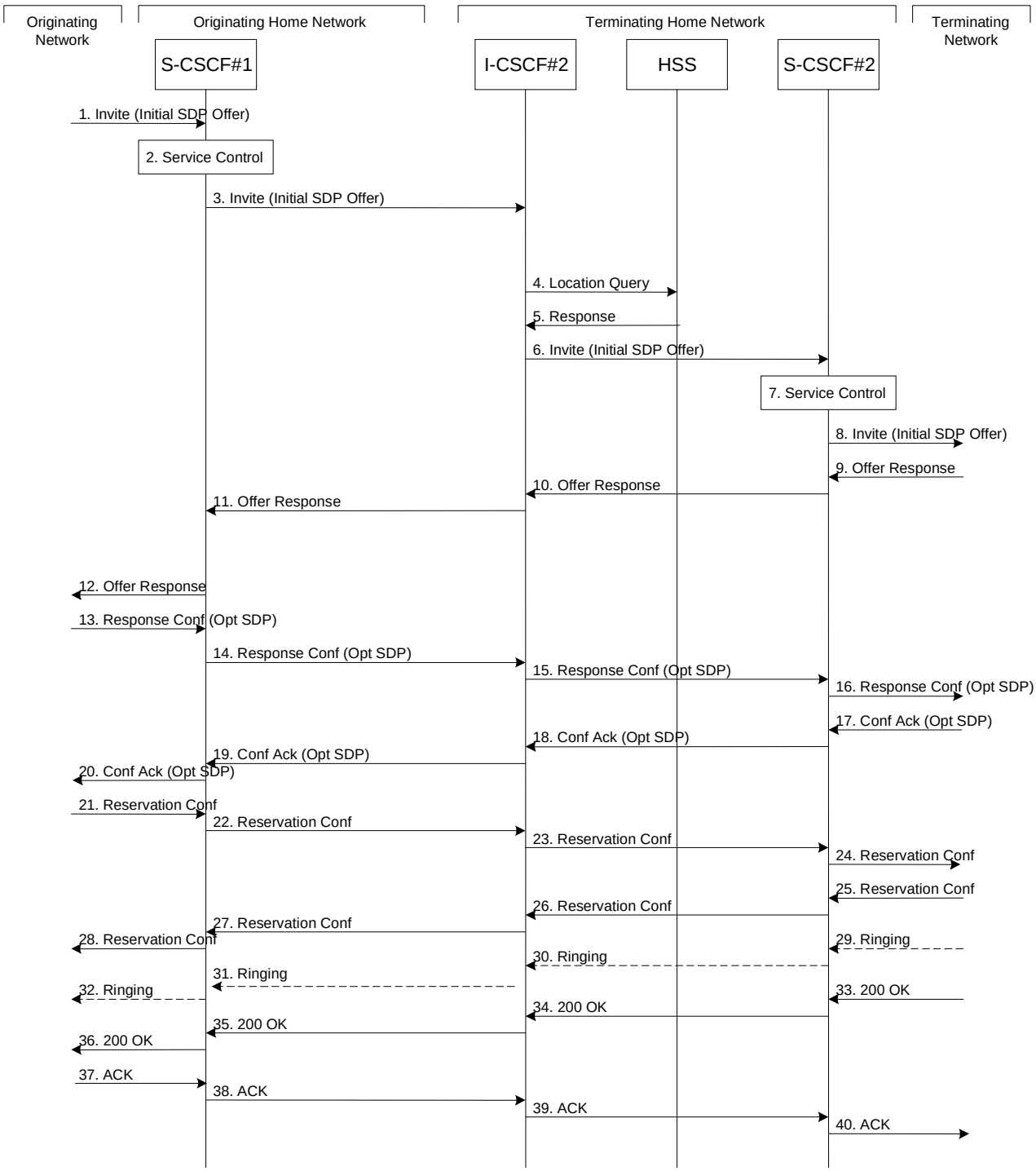


Figure 5.10: Serving to serving procedure - different operators

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 subclause 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 subclause 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.

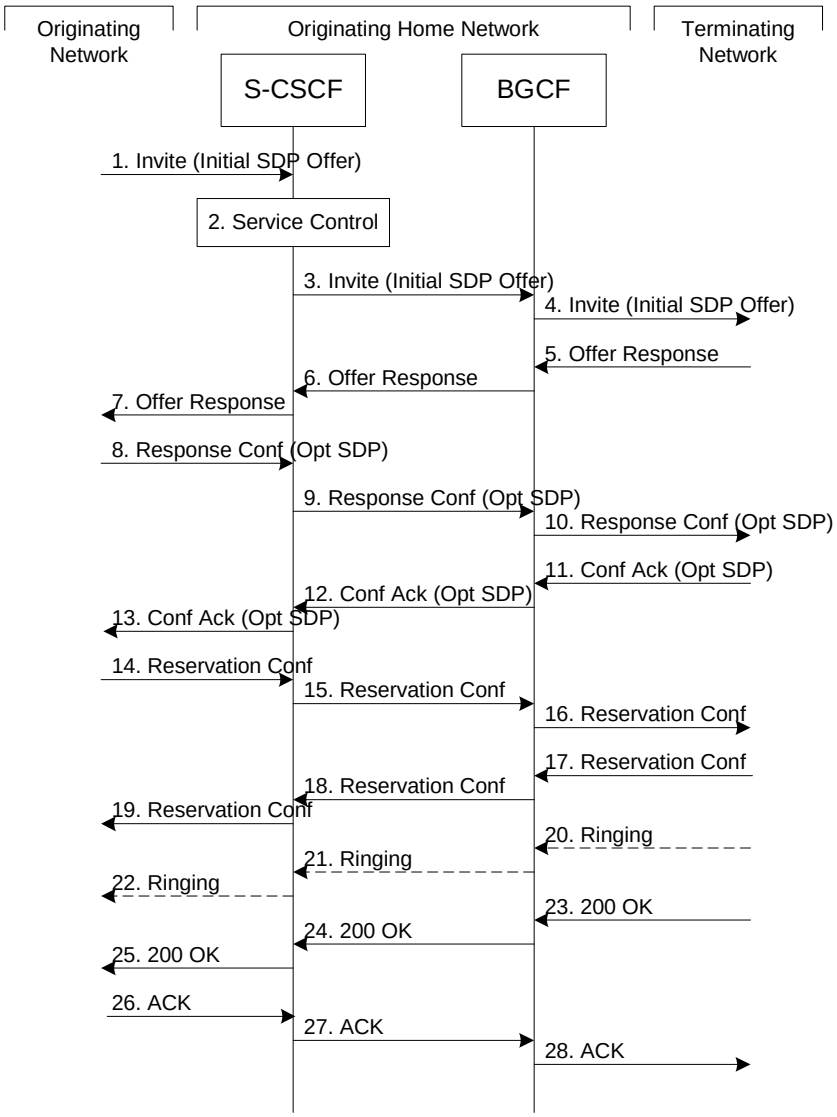


Figure 5.12: Serving to PSTN procedure - same operator

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 subclause 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.

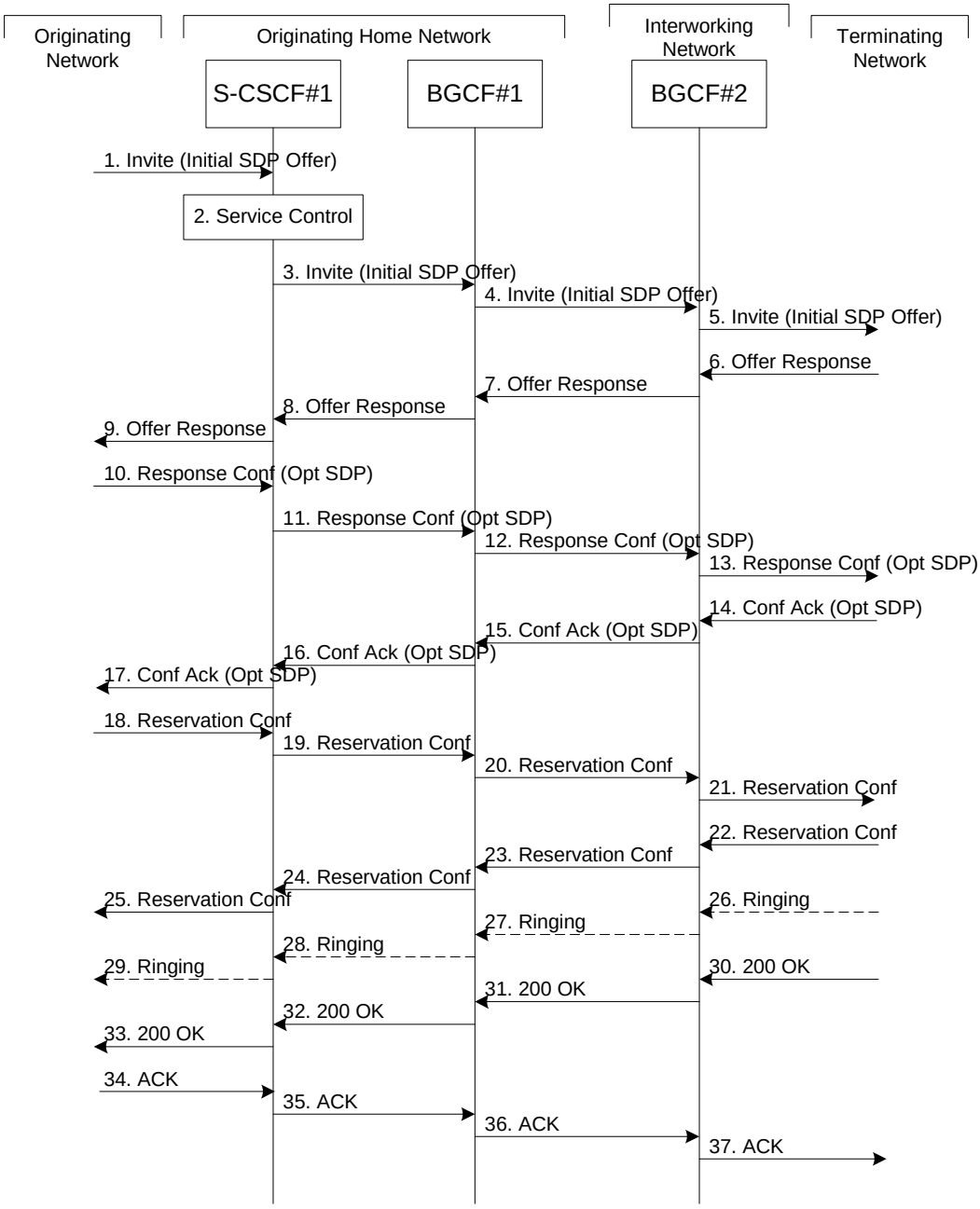


Figure 5.13: Serving to PSTN procedure - different operator

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

The flows presented in the section 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 authorisation, and may have additional functions in handling of emergency sessions. The P-CSCF is determined by the CSCF discovery process, described in Section 5.1.1 (Local CSCF Discovery).

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

Sessions originated in the PSTN to a 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 section 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.

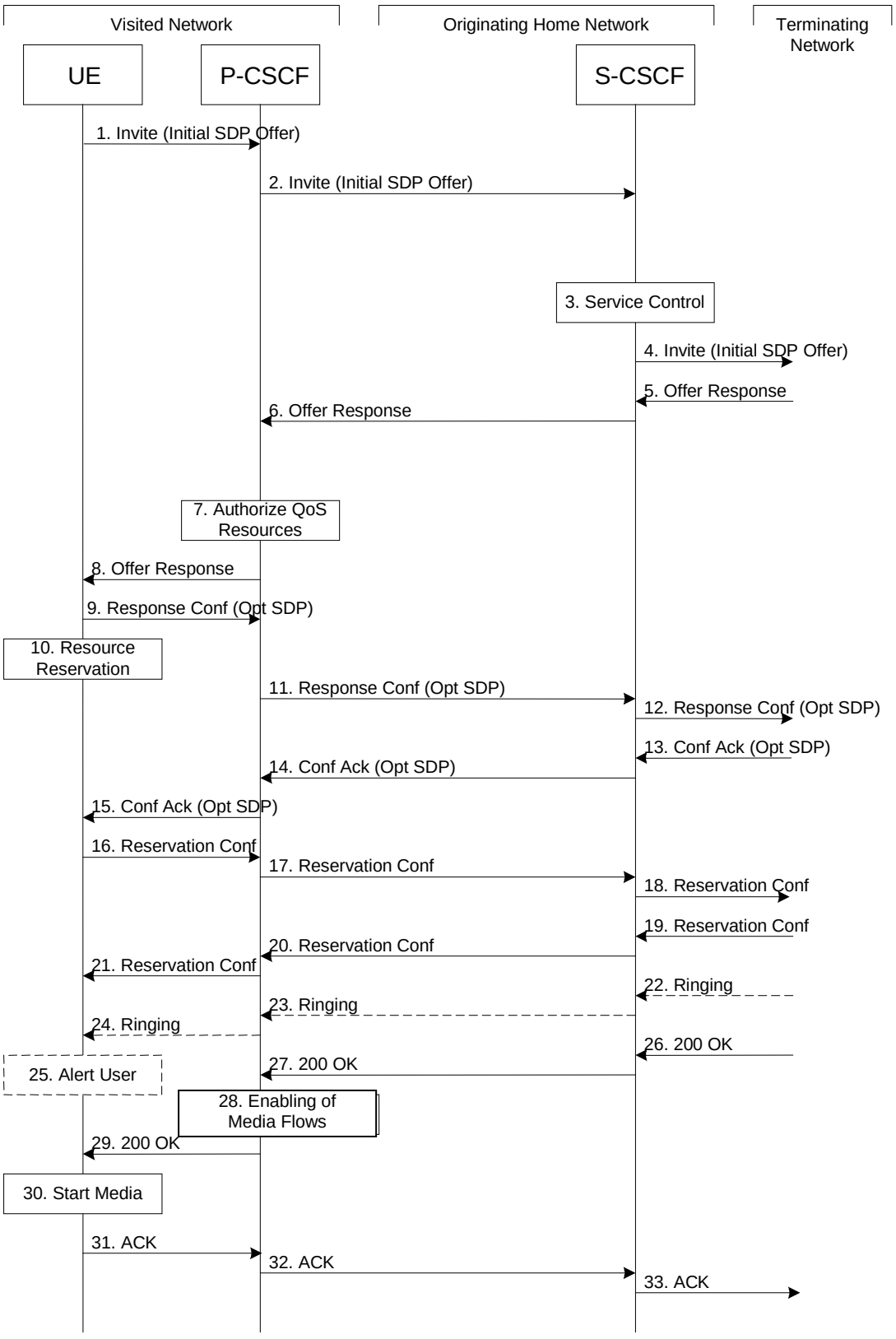


Figure 5.14: Mobile origination procedure - roaming

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.

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 authorisation 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 number and permitted by operator policy, the S-CSCF attempts translation of the E.164 address in the SIP URI to a globally routable SIP URI using an ENUM/DNS translation mechanism (this is either done only for domains in the SIP URI known by the S-CSCF to belong to the home network, or as for all domains depending on local policy).

4. S-CSCF forwards the request, as specified by the S-S procedures.

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

6. S-CSCF forwards the Offer Response message to P-CSCF.

7. P-CSCF authorises the resources necessary for this session.

8. 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 by the P-CSCF(PCRF) 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(PCRF) 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 section 5.1.1. During registration, the home network allocates an S-CSCF in the home network.

When registration is complete, P-CSCF knows the name/address of S-CSCF.

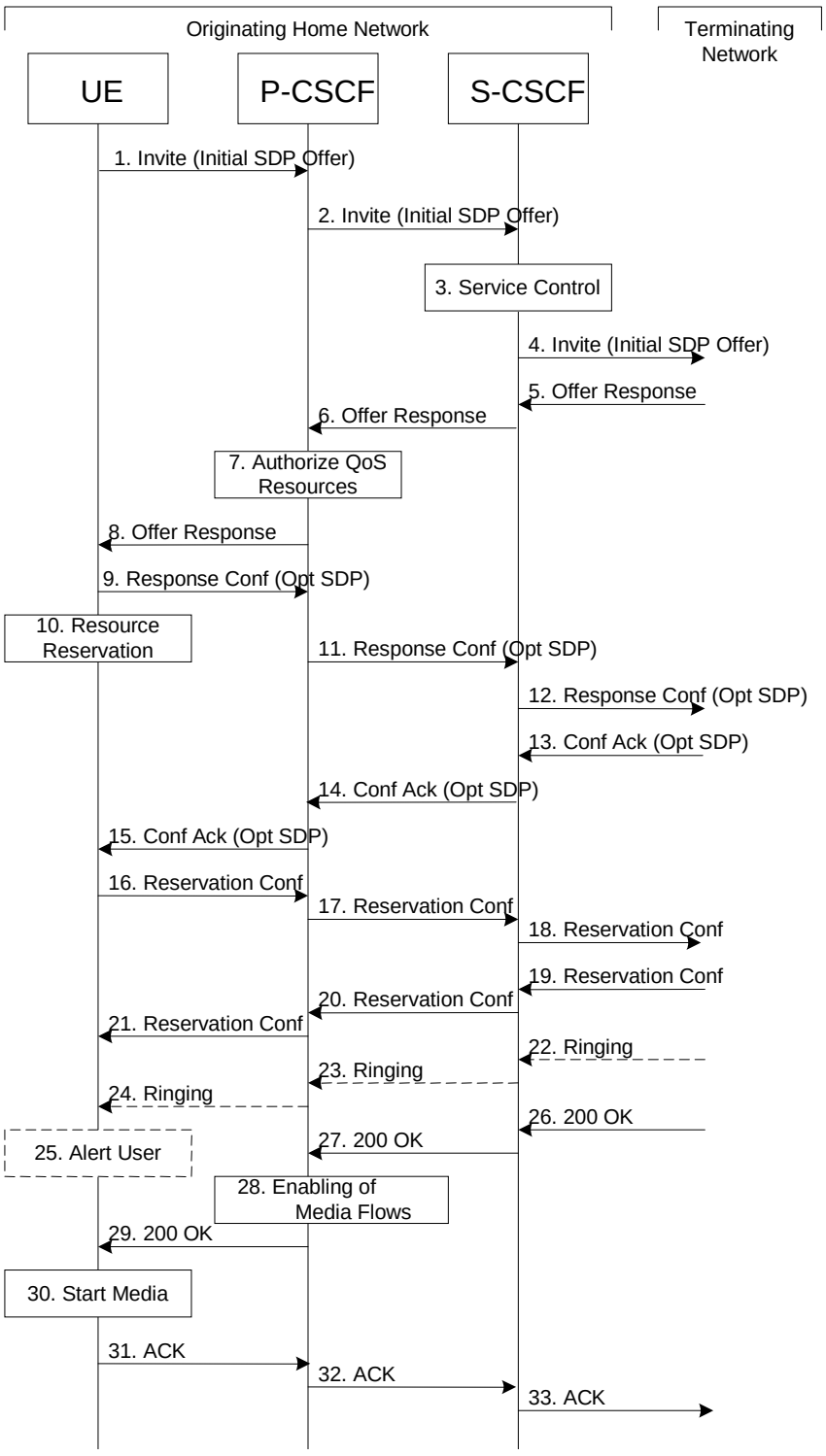


Figure 5.15: Mobile origination procedure - home

Procedure MO#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session.

2. P-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. In this case it forwards the INVITE to the S-CSCF in the home network.

3. S-CSCF validates the service profile, 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 authorisation 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 number and permitted by operator policy, the S-CSCF attempts translation of the E.164 address in the SIP URI to a globally routable SIP URI using an ENUM/DNS translation mechanism (this is either done only for domains in the SIP URI known by the S-CSCF to belong to the home network, or as for all domains depending on local policy).

4. S-CSCF forwards the request, as specified by the S-S procedures.

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

6. S-CSCF forwards the Offer Response message to P-CSCF

7. P-CSCF authorises the resources necessary for this session.

8. 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 by the P-CSCF(PCRF) 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(PCRF) 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 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 authorises the media.

15. PCSCF forwards the answered media towards the UE.

16-18. When the resource reservation is completed, UE sends the successful Resource Reservation message to the terminating endpoint, via the signalling path established by the INVITE message. The message is sent first to P-CSCF.

19-21. The terminating end point responds to the originating end when successful resource reservation has 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.

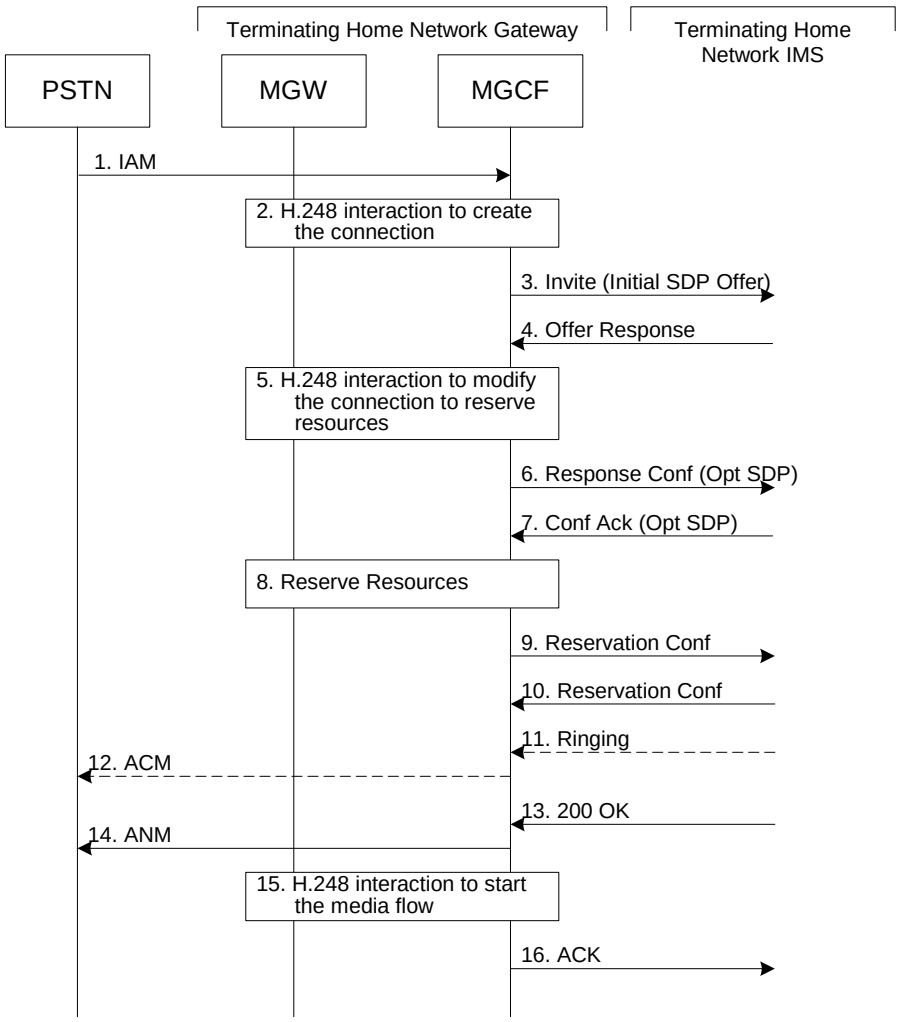


Figure 5.16: PSTN origination procedure

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.

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]. In case the external SIP client does not support the Precondition extension of SIP, the UE continues to setup the session without activating media transfer until the session has been accepted. 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.

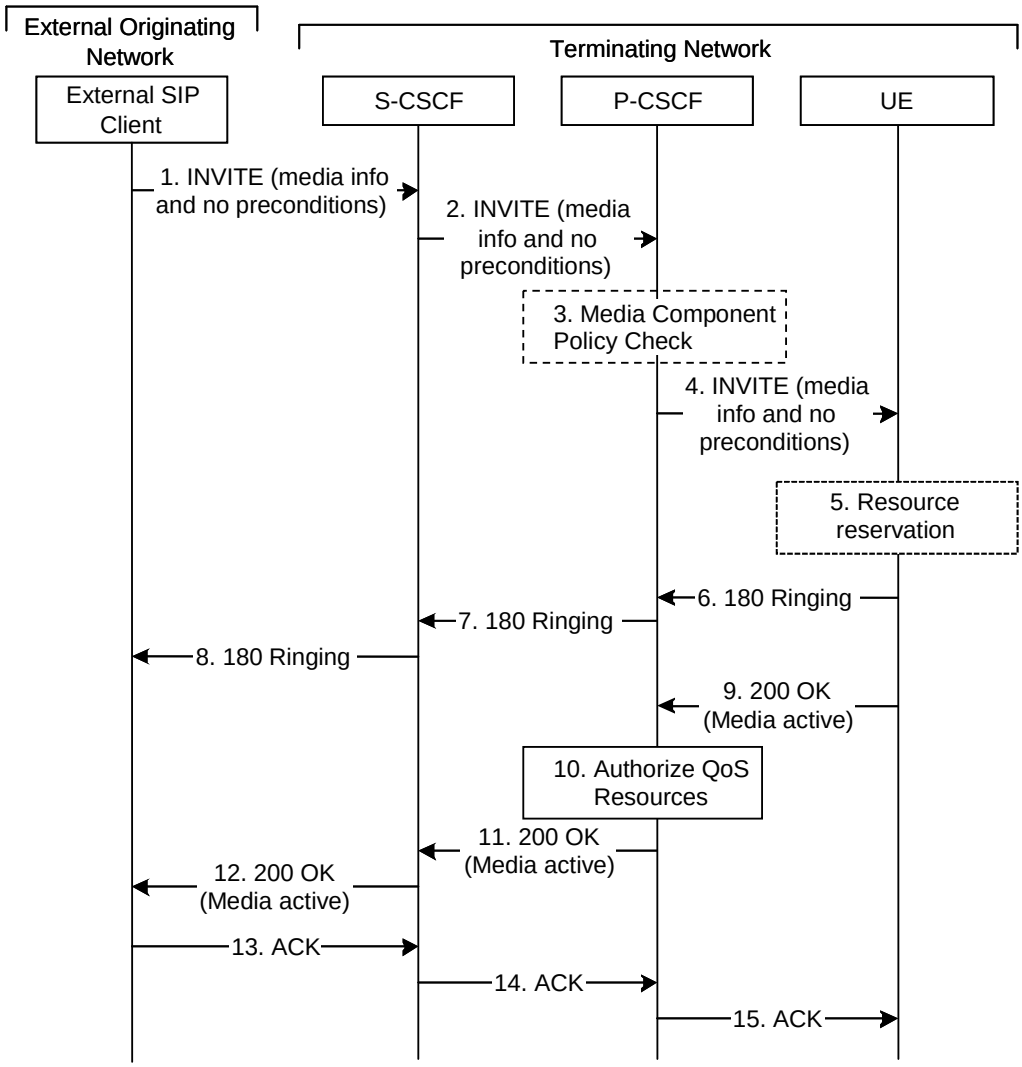


Figure 5.16a: Originating session from external SIP client

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 authorisation limitation information coming from the PCRF), it rejects the session initiation attempt.

NOTE 1: Whether the P-CSCF should interact with PCRF 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/PCRF may 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 (i.e. a Public User Identity) or a Public Service Identity. In case the AS initiates the session on behalf of a user, the user may be a user with no profile in the HSS (e.g. a PSTN user). It will be referred as a non-IMS user. In case the AS initiates the session on behalf of a user, the identity-related fields of the initial request are populated the same way as if the request was originated by the user himself.

In case of originating unregistered procedures, the handling of the S-CSCF in the HSS will follow the same principle as terminating unregistered user handling.

In case of originating unregistered procedures, the S-CSCF shall execute any unregistered origination service logic before forwarding requests from an AS on behalf of a user (i.e. 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 Identies 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.

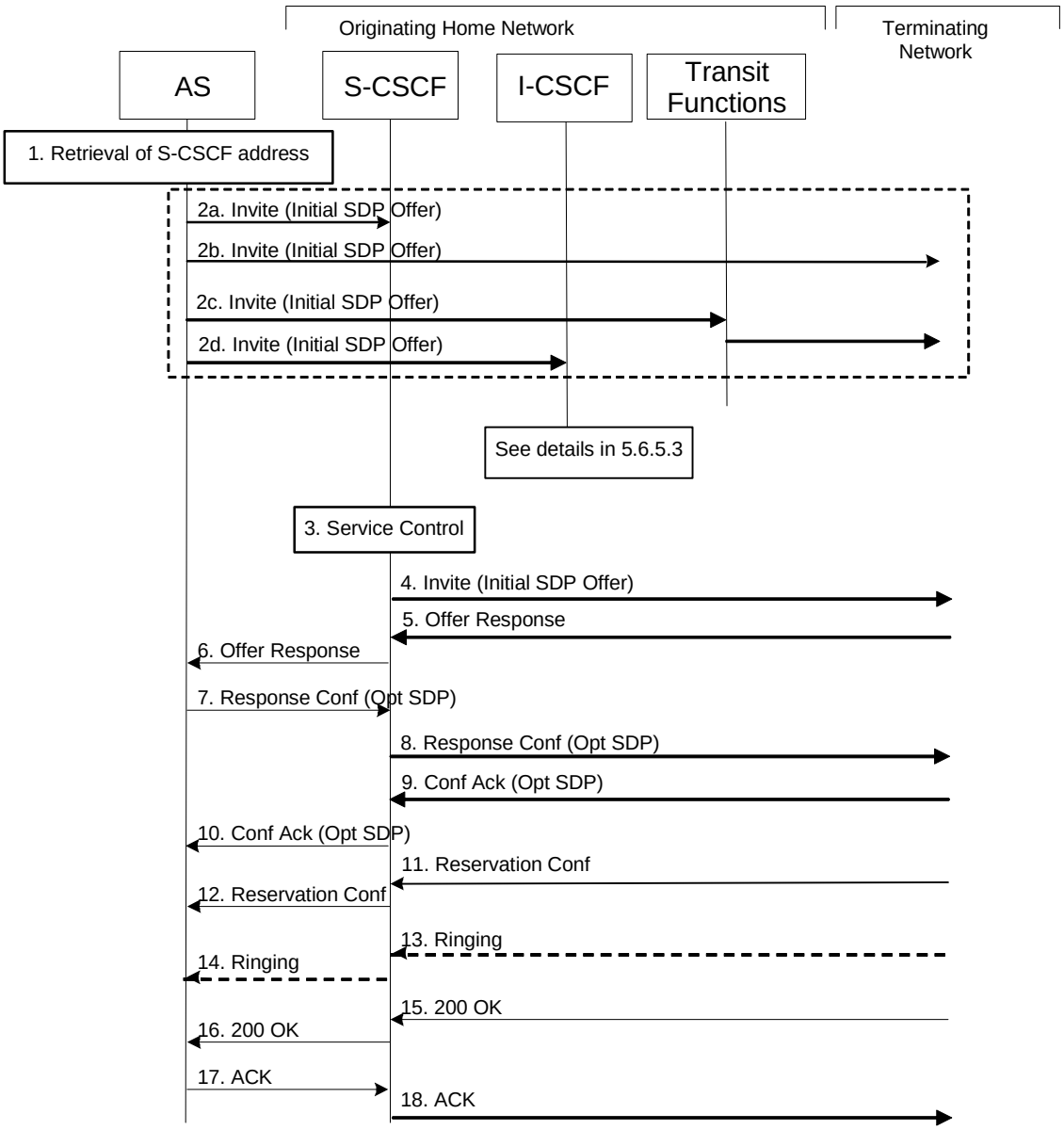


Figure 5.16b: Application Server origination procedure

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 an E.164 number and permitted by operator policy, the S-CSCF attempts translation of the E.164 address in the SIP URI to a globally routable SIP URI using an ENUM/DNS translation mechanism (this is either done only for domains in the SIP URI known by the S-CSCF to belong to the home network, or as for all domains depending on local policy).

4. S-CSCF forwards the request, as specified by the S-S procedures.

5-6. The media stream capabilities of the destination are returned along the signalling path.

7-8. The AS decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation along the signaling path towards the destination network. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response or a subset. The AS is free to continue to offer new media on this operation or on subsequent exchanges using the Update method.

9-10. The terminating end point responds to the originating end with an acknowledgement, which is forwarded along the session signaling path. If Optional SDP is contained in the Response Confirmation, the Confirmation Acknowledge will also contain an SDP response.

11-12. The terminating endpoint responds to the originating end when successful resource reservation has occurred.

13-14. The destination UE may optionally perform alerting. If so, it signals this to the originating party by a provisional response indicating Ringing. This message is sent to the AS along the signaling path.

15-16. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating end.

17-18. The AS responds to the 200 OK with an ACK message which is passed along the signalling path to the terminating end.

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: In case 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:

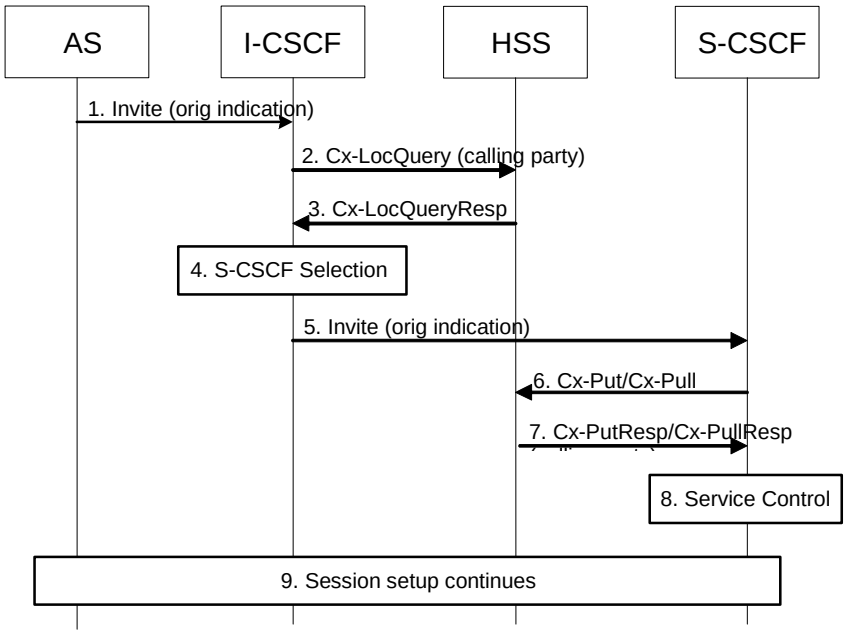


Figure 5.16c: S-CSCF selection by I-CSCF for AS Originating call procedure

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

The flows presented in the section 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 authorisation for the sessions to the UE. The P-CSCF is determined by the CSCF discovery process, described in Section 5.1.1 (Local CSCF Discovery).

As a result of the registration procedure, the P-CSCF knows the address of the UE. The assigned S-CSCF, knows the name/address of the P-CSCF (procedure MT#3, and MT#4, depending on the location of S-CSCF and P-CSCF).

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

5.7.1 (MT#1) Mobile termination, roaming

This termination procedure applies to roaming users.

The UE is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure described in section 5.1.1. The home network advertises 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.

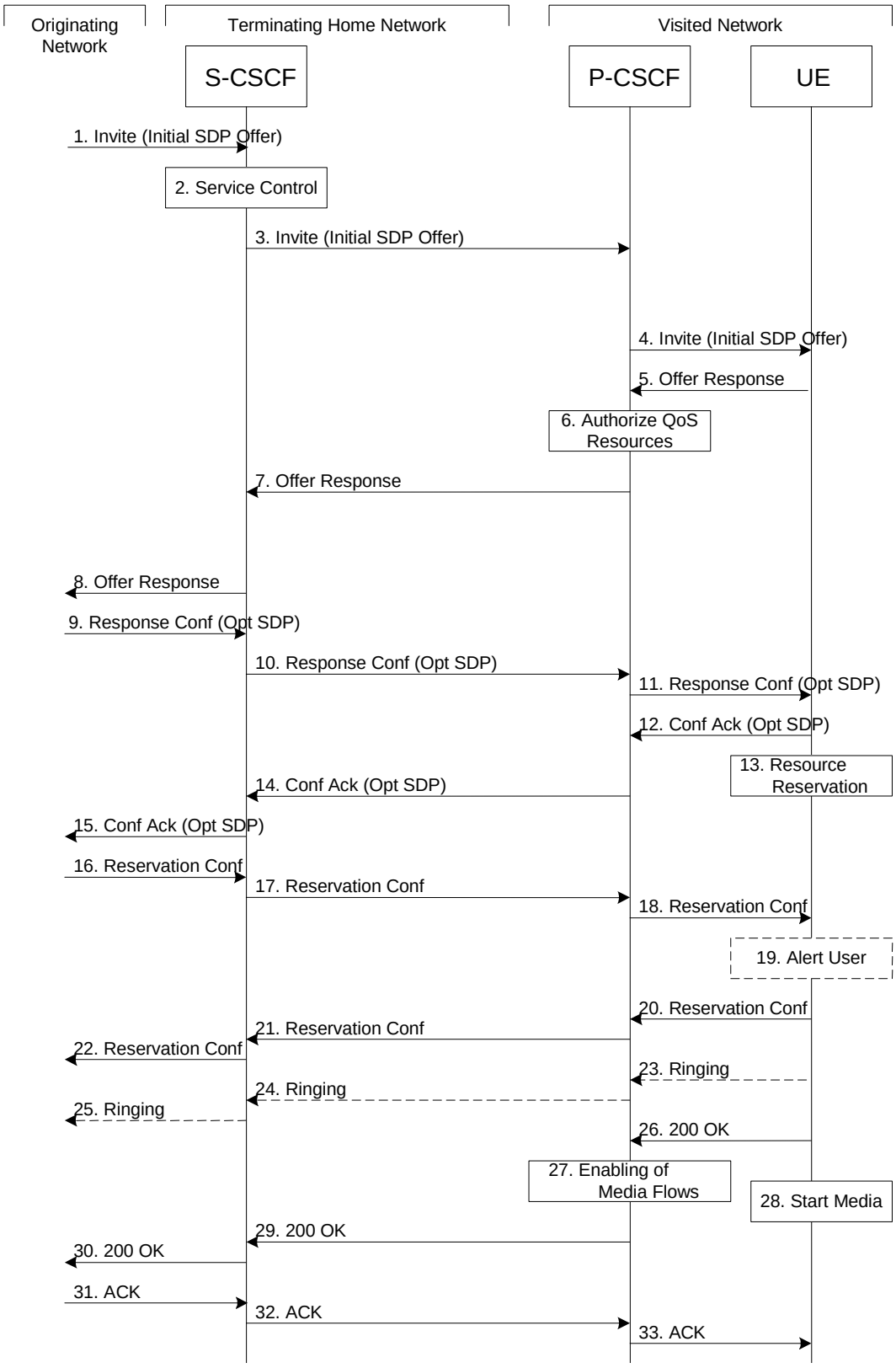


Figure 5.17: Mobile termination procedure - roaming

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 authorisation of the requested SDP based on the user's subscription for multi-media services.

3. S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF in the visited network.

4. P-CSCF remembers (from the registration procedure) the UE address, and forwards the INVITE to the UE.

5. UE determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. The SDP may represent one or more media for a multi-media session. This response is sent to P-CSCF.

6. P-CSCF authorises the resources necessary for this session.

7. P-CSCF forwards the Offer Response message to S-CSCF.

8. S-CSCF forwards the Offer Response message to the originator, per the S-S procedure.

9. The originating endpoint sends a Response Confirmation via the S-S procedure, to S-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in Step 8 or a subset. If new media are defined by this SDP, a new authorization (as in Step 6) will be done by the P-CSCF(PCRF) 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(PCRF) to repeat the Authorization step (Step 6) again.

10. S-CSCF forwards the Response Confirmation to P-CSCF. This may possibly be routed through the I-CSCF depending on operator configuration of the I-CSCF.

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 that the media flows authorized 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 section 5.1.1.

When registration is complete, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.

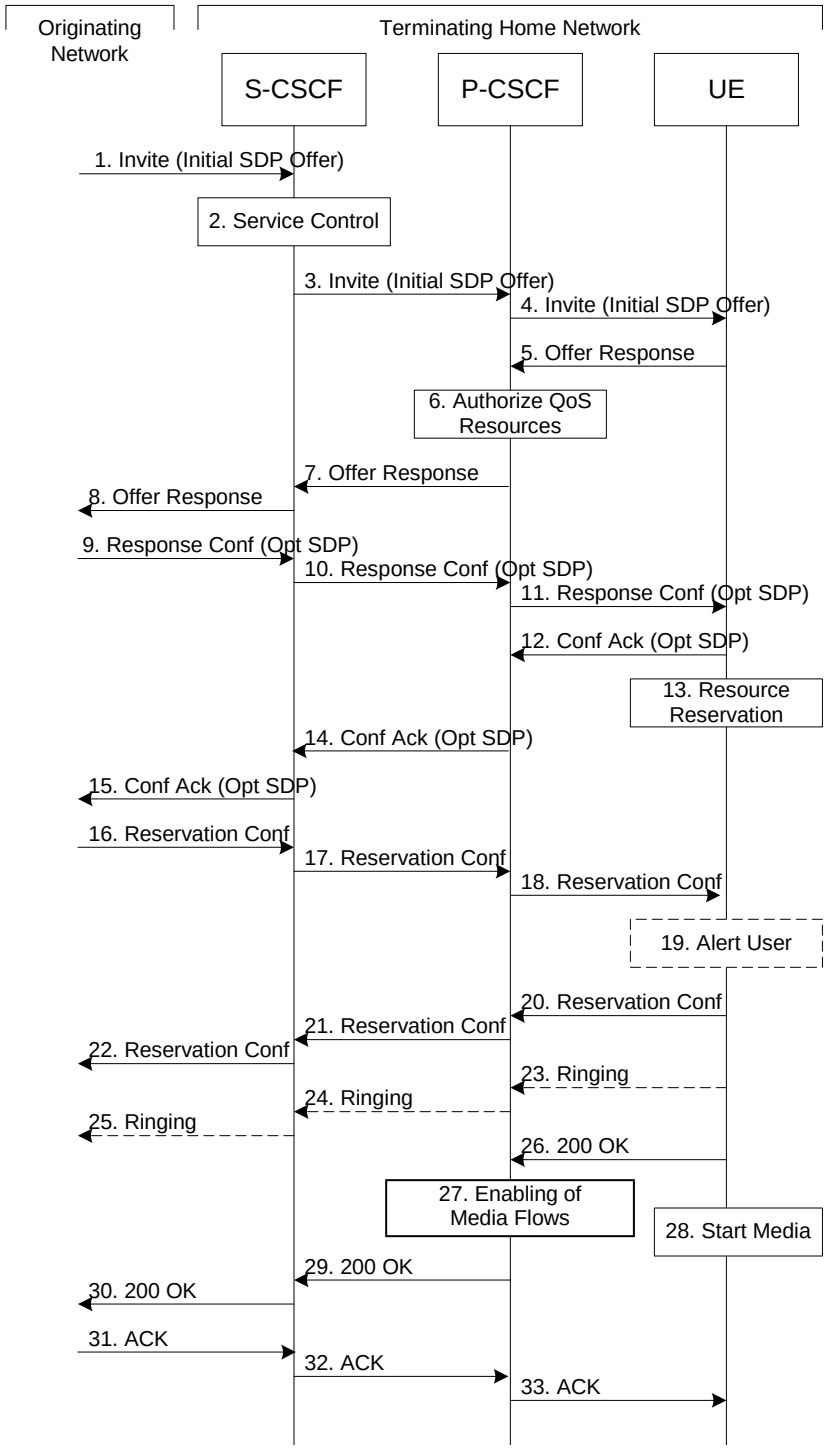


Figure 5.18: Mobile termination procedure - home

Procedure MT#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, via one of the origination procedures, and via one of the Serving to Serving-CSCF procedures, to the Serving-CSCF for the terminating user.

2. S-CSCF validates the service profile, and invokes any termination service logic required for this user. This includes authorisation of the requested SDP based on the user's subscription for multi-media services.

3. S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF in the home network.

4. P-CSCF remembers (from the registration procedure) the UE address, and forwards the INVITE to the UE.

5. UE determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. The SDP may represent one or more media for a multi-media session. This response is sent to P-CSCF.

6. P-CSCF authorises the resources necessary for this session.

7. P-CSCF forwards the Offer Response message to S-CSCF.

8. S-CSCF forwards the Offer Response message to the originator, per the S-S procedure.

9. The originating endpoint sends a Response Confirmation via the S-S procedure, to S-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response sent in Step 8 or a subset. If new media are defined by this SDP, a new authorization (as in Step 6) will be done by the P-CSCF(PCRF) 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(PCRF) to repeat the Authorization step (Step 6) again.

10. S-CSCF forwards the Response Confirmation to P-CSCF.

11. P-CSCF forwards the Response Confirmation to UE.

12. UE responds to the Response Confirmation with an acknowledgement. If Optional SDP is contained in the Response Confirmation, the Confirmation Ack will also contain an SDP response. If the SDP has changed, the P-CSCF authorizes that the resources are allowed to be used.

13. 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 signaling path.

31-33. The session originator responds to the 200-OK by sending the ACK message to S-CSCF via the S-S procedure and it is forwarded to the terminating end along the signalling path..

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

This termination procedure applies to a user registered for CS services, either in the home network or in a visited network. The user has both IMS and CS subscriptions but is unregistered for IMS services

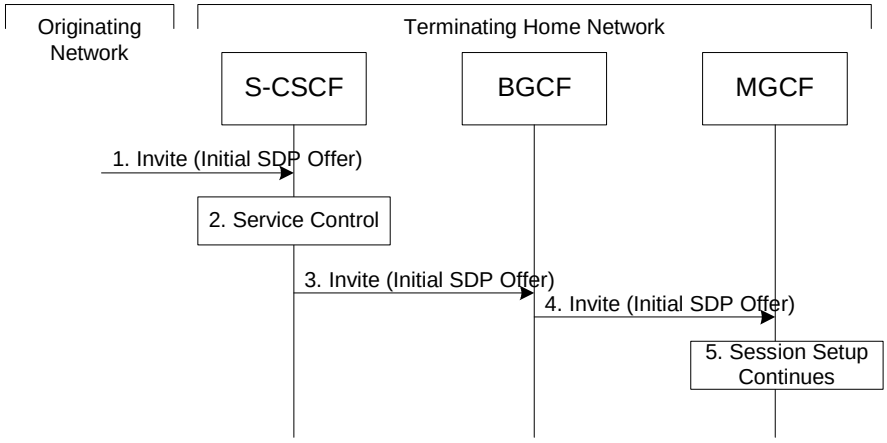


Figure 5.18a: Mobile Terminating procedures to a user that is unregistered for IMS services but is registered for CS services

1. In case the terminating user does not have an S-CSCF allocated, the session attempt is routed according to the section 5.12.1 (Mobile Terminating procedures to unregistered IMS user that has services related to unregistered state).

2. S-CSCF invokes service control appropriate for this session setup attempt, which may result in e.g. re-routing the session to a messaging service, or continued routing towards the user's CS domain termination address (e.g. E.164).

3. S-CSCF performs whatever further actions are appropriate for this session setup attempt. In case of routing towards the user's CS domain termination address, the S-CSCF performs an analysis of this address. From the analysis of the destination address, S-CSCF determines that this is for the CS domain, and passes the request to the BGCF.

4. The BGCF forwards the SIP INVITE message to the appropriate MGCF in the home network, or to a BGCF in another network. This depends on the PSTN interworking configuration of the IMS network. Eventually, the session initiation arrives to an MGCF.

5. Normal session setup continues according to PSTN-T flow as described in Section 5.7.3.

5.7.3 (PSTN-T) PSTN termination

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

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

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

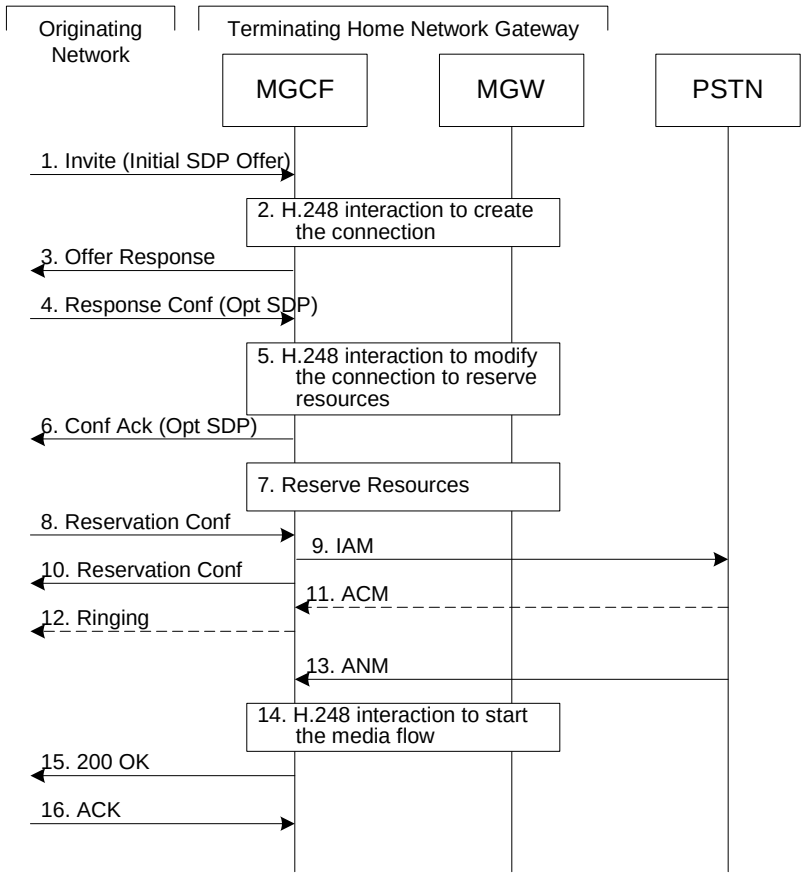


Figure 5.19: PSTN termination procedure

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 (a UE may originate an IMS session without requiring the support for precondition capabilities, see subclause 5.7a), the UE originates an IMS session requiring the support for precondition capabilities towards an external SIP entity that does not support those capabilities. Based on the response indicating no support, the UE re-initiates the session by resetting the requirements and announcing its own support only. The UE sets all the media components to inactive until the media information has been negotiated at a later stage of the session. When both parties have agreed to the session and media parameters and the UE has established resources for the media, the UE initiates session modification setting the status of the media components to active and is thus enabling the media transfer to start. Figures 5.19a , 5.19b and 5.19c together illustrate session flows for one possible originating session establishment towards a non-IMS client in an external network with QoS authorisation and Policy and Charging Control support. In this example the external SIP client does not support the Precondition extension of SIP.

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

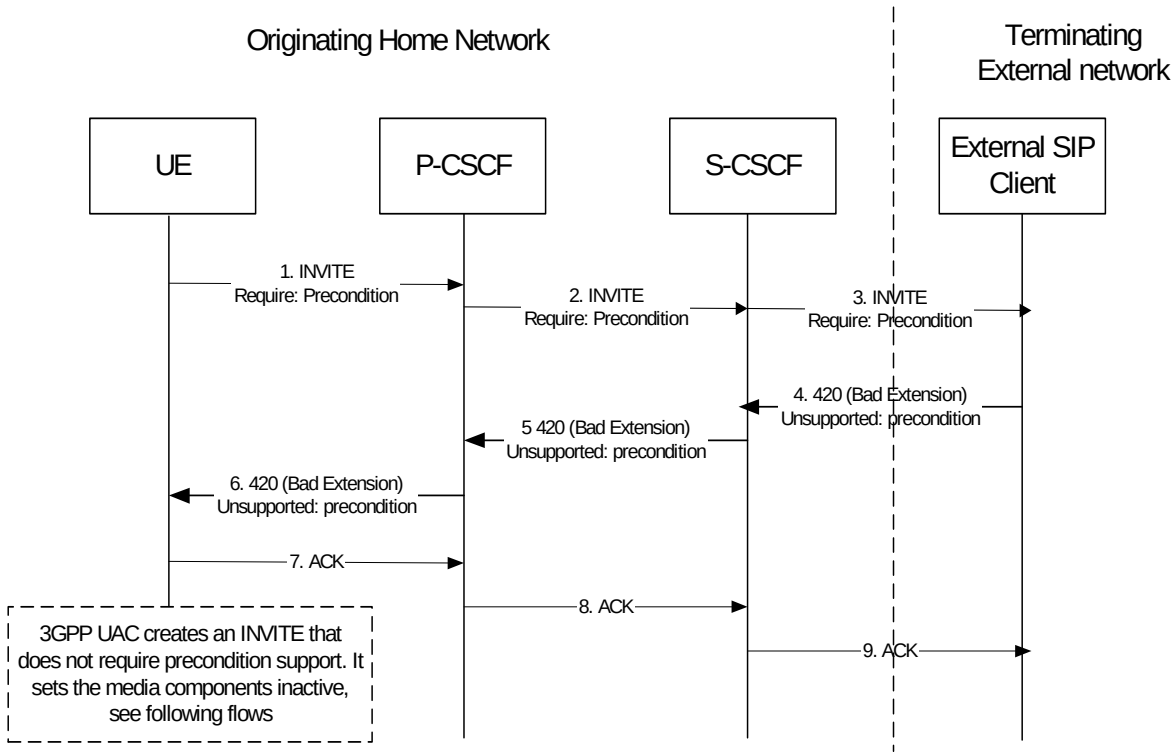


Figure 5.19a: Terminating session towards external SIP client, detection phase

The terminating IMS session detection phase is as follows:

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

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

7-9. Acknowledgement to the response is sent through the session path and the session setup procedure is terminated.

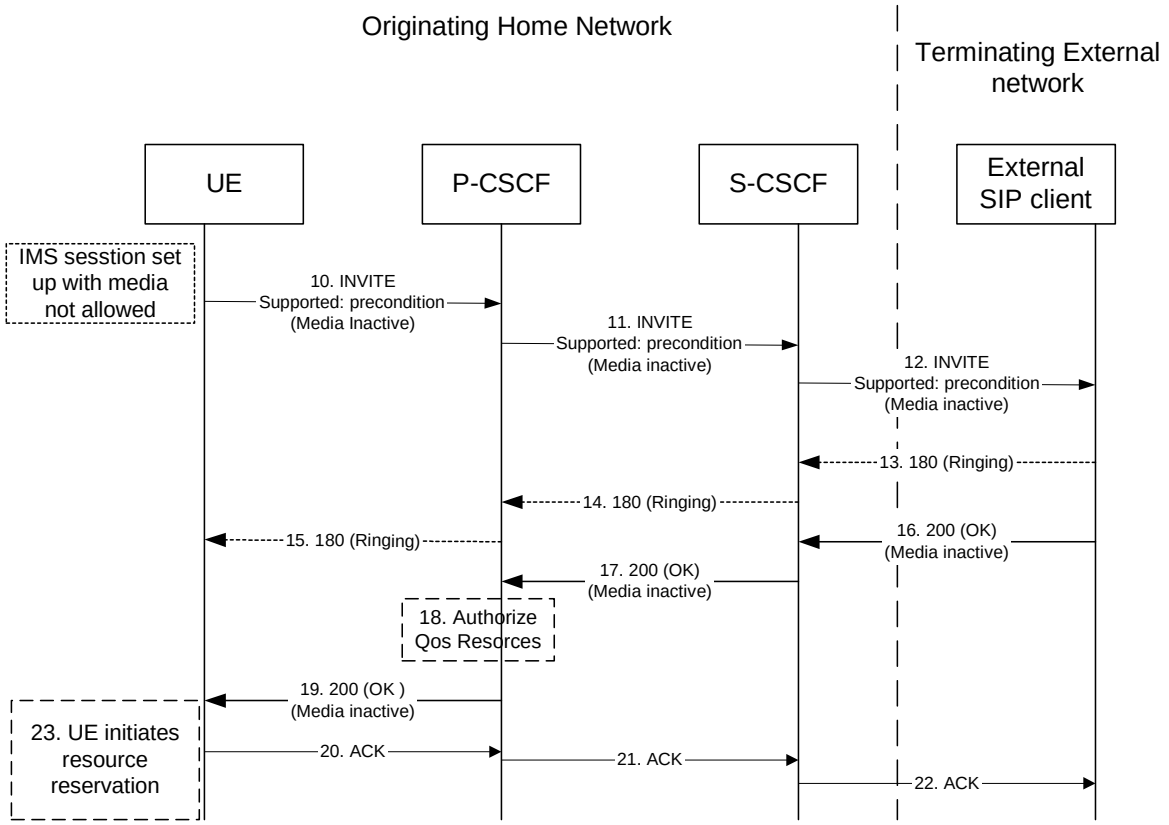


Figure 5.19b: Terminating session towards external SIP client, re-initiate session set up not requiring precondition capabilities and with inactive media

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

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

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

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

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

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

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

23. 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 18.

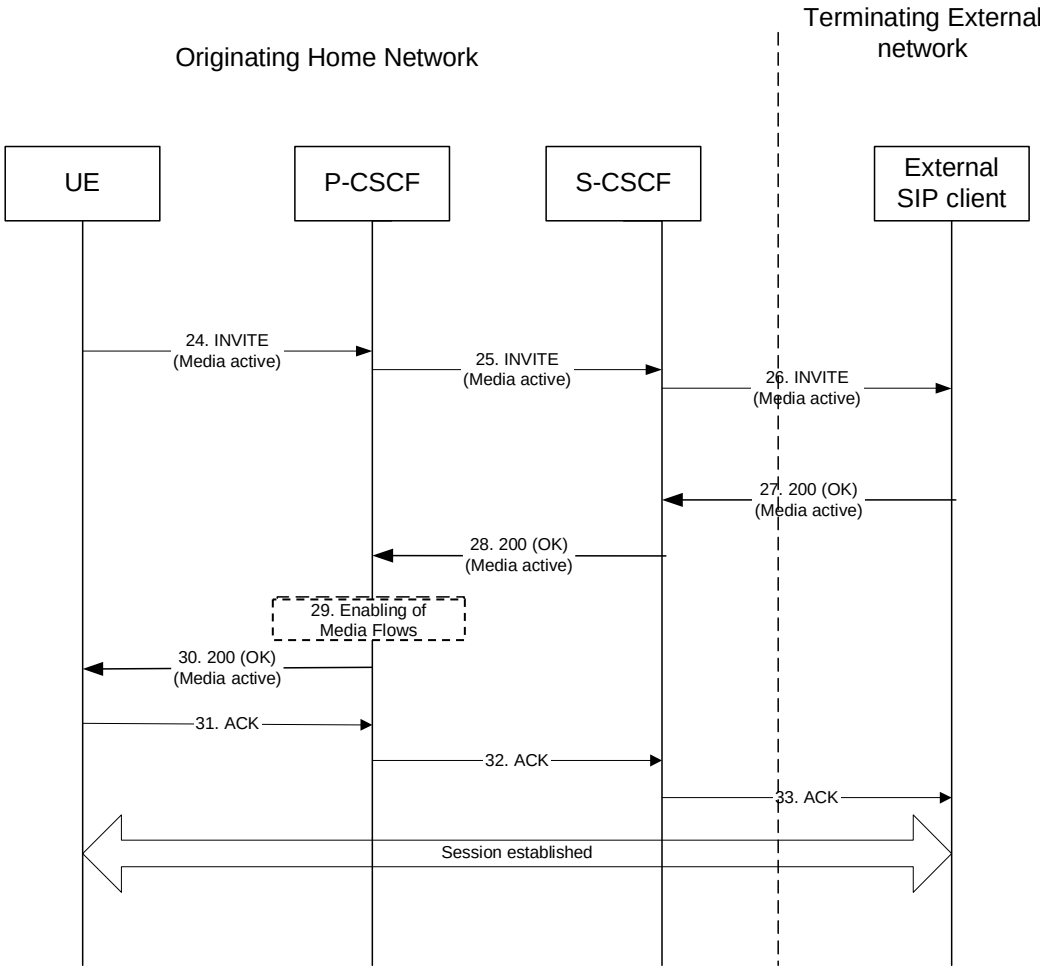


Figure 5.19c: Continuation of terminating session towards external SIP client, session set up with active media

Once the session parameters have been agreed and the UE has successfully reserved resources for the media components, the session set-up continues by setting the media components to active, as shown in session flow 5.19c.

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

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

29. The P-CSCF/PCRF receives the acceptance of media activation. At this point, the P-CSCF/PCRF may enable the media flows that have been authorised for the session.

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

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

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

5.7.5 (AS-T#1) PSI based Application Server termination – direct

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

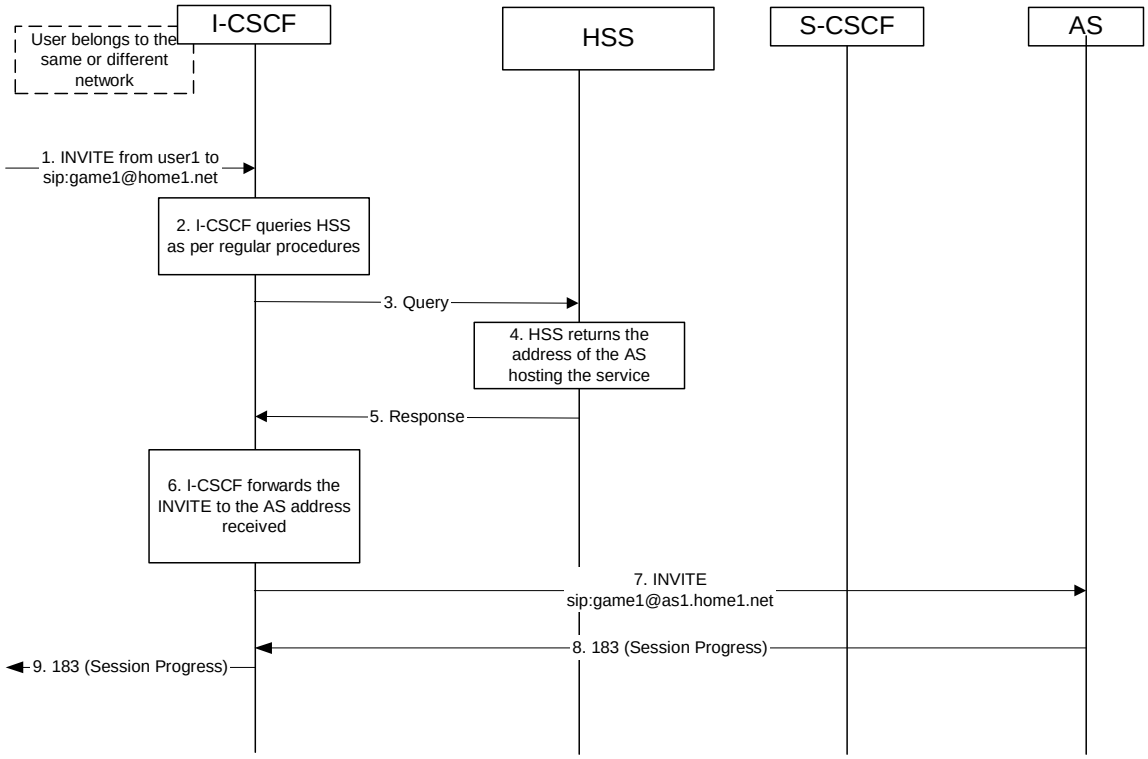


Figure 5.19d: Incoming session, direct route towards the AS

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

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

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

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

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

8-9. Session setup continues as per existing procedures.

5.7.6 (AS-T#2) PSI based Application Server termination – indirect

This section depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.

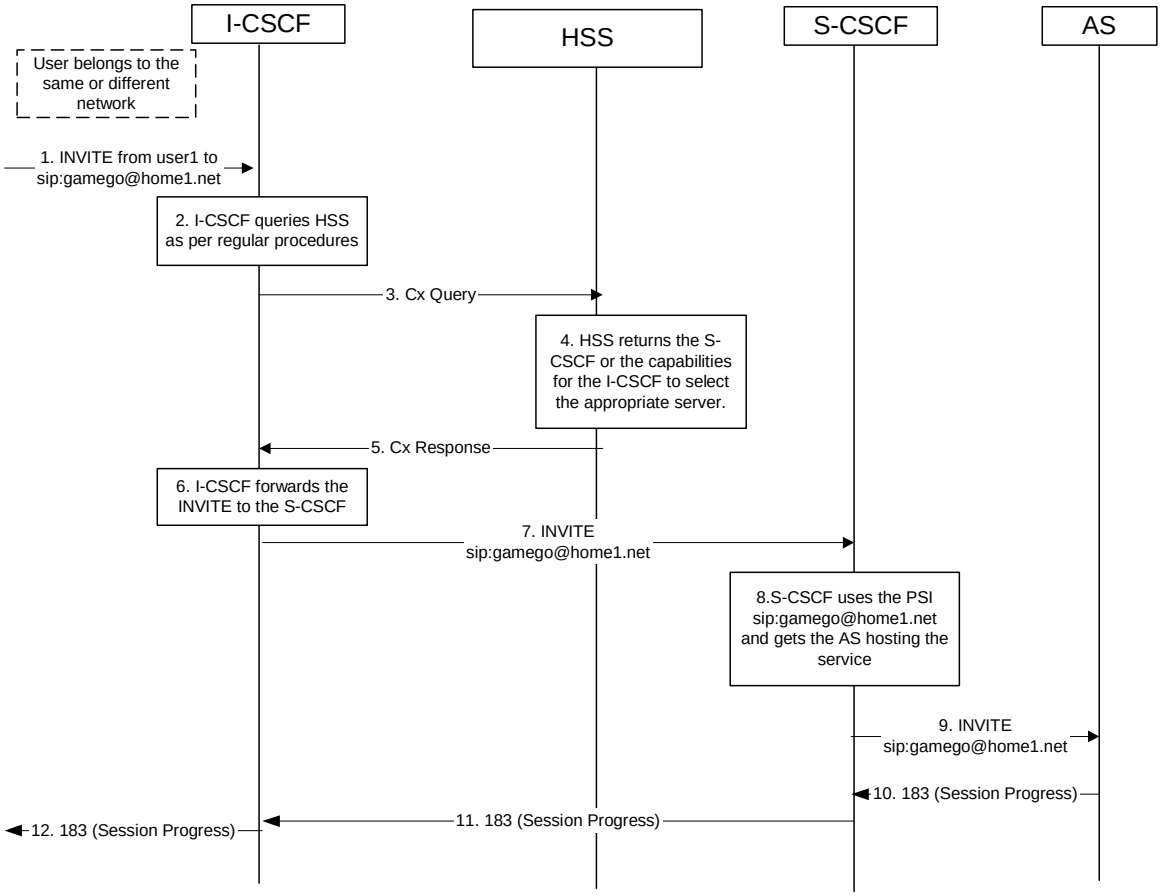


Figure 5.19e: Incoming session, indirect route to AS via S-CSCF

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

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

4. HSS determines the routing information, which is the S-CSCF defined for the "PSI user".

5. HSS returns the S-CSCF address/capabilities to the I-CSCF.

6-7. I-CSCF, as per existing procedures, forwards the request towards the entity (i.e., S-CSCF) received from the query, or the I-CSCF selects a new S-CSCF if required.

8. S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.

9. The request is then routed towards the AS identified by the filter criteria.

10-12. Session setup continues as per existing procedures.

5.7.7 (AS-T#3) PSI based Application Server termination – DNS routing

This section shows an example of DNS based routing of an incoming session from an external network. The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.

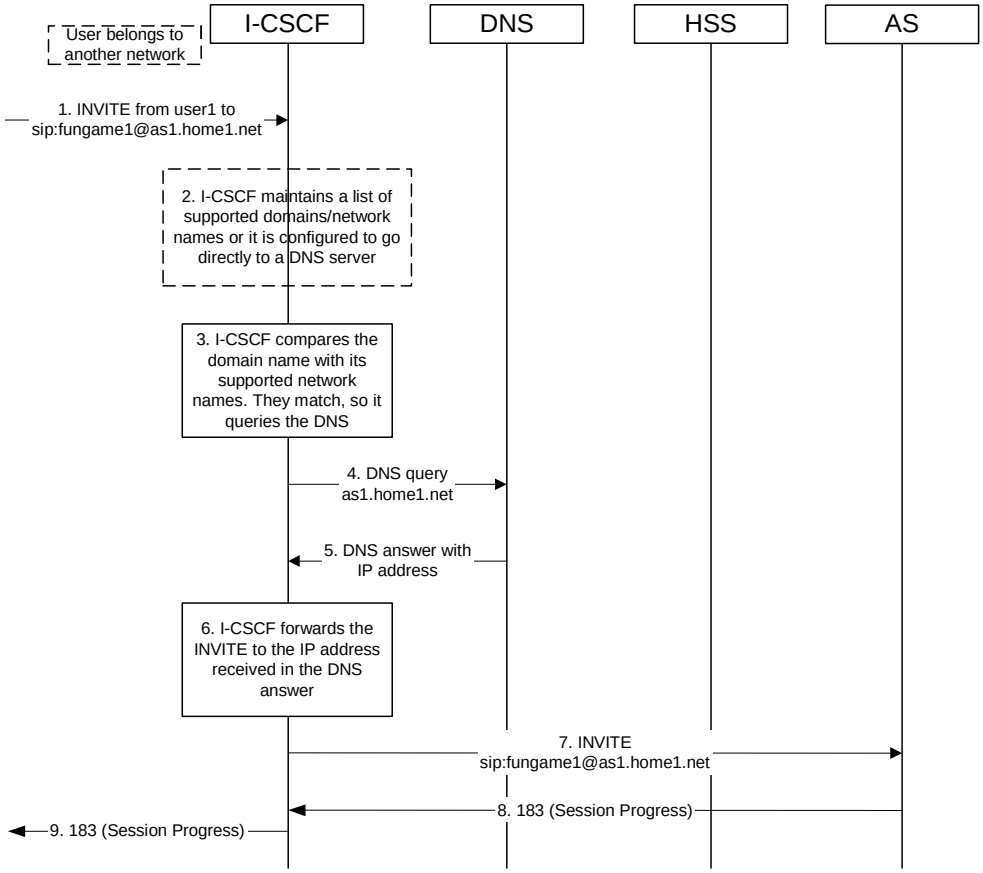


Figure 5.19f: Incoming session, direct route to AS using DNS

1. I-CSCF receives a request that is destined to the PSI.
2. I-CSCF has been configured with the list of supported domains/network names, or it may have been configured to directly query a local DNS server.
3. In this case the I-CSCF checks the list and finds a match.
4. I-CSCF sends DNS query to find the route.
5. DNS server returns the IP address of the AS hosting the PSI.

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

8-9. Session setup continues as per existing procedures.

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.

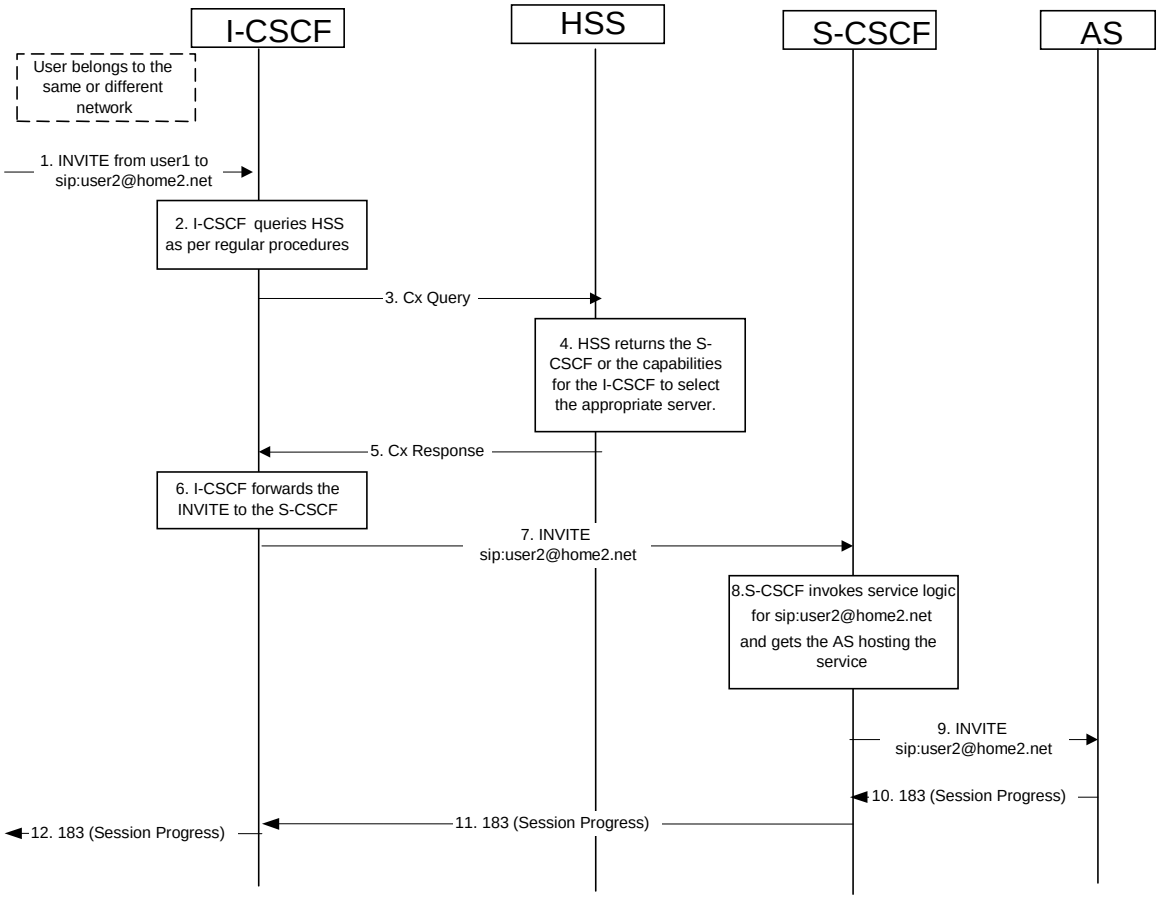


Figure 5.19g: Application Server termination

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 subclauses present the general end-to-end session flow procedures without preconditions. The flow in subclause 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 sections 5.6 and 5.7 apply for services with real-time QoS requirements before session becomes active.

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

5.7a.2 Procedures for the establishment of sessions without preconditions - no resource reservation required before session becomes active

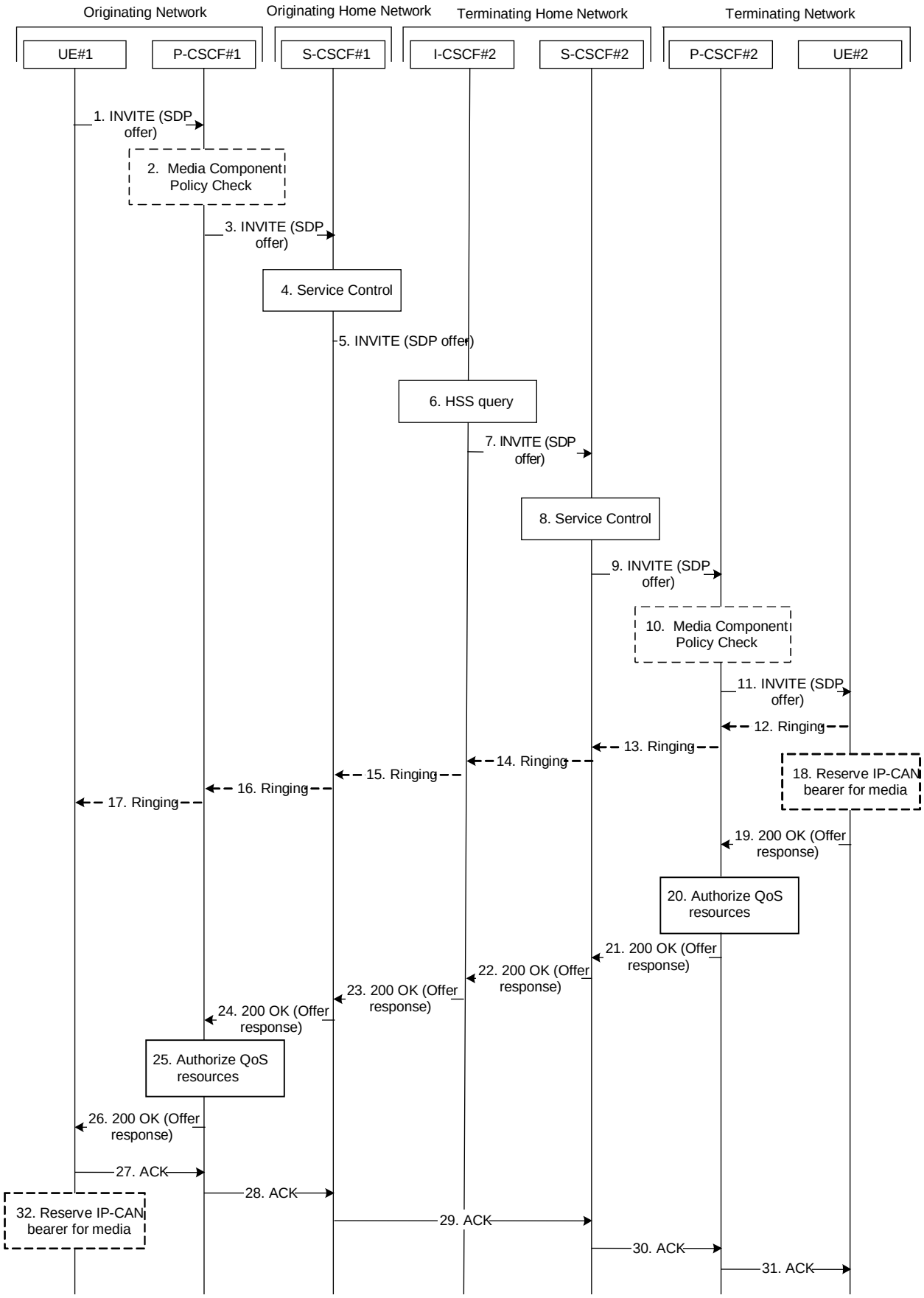


Figure 5.19h: End-to-end session flow procedure without preconditions - no resource reservation required before session becomes active

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 authorisation limitation information coming from the PCRF), it rejects the session initiation attempt.

NOTE 0a: Whether the P-CSCF should interact with PCRF 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 authorisation limitation information coming from the PCRF), it rejects the session initiation attempt.

NOTE 0b: Whether the P-CSCF should interact with PCRF 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/PCRF may 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/PCRF may 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 authorised to route sessions, the I-CSCF interrogates the HSS for routing information. The mobile terminated sessions for a user shall be routed to a S-CSCF.

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

5.8.1 User identity to HSS resolution

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

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

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

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

The Dx interface provides:

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

By sending the Dx-operation DX_SLF_QUERY the I-CSCF or the S-CSCF indicates a user identity of which it is looking for an HSS. By the Dx-operation DX_SLF_RESP the SLF responds with the HSS name. The I-CSCF or the S-CSCF, respectively, continues by querying the selected HSS. 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.

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

The Dh interface provides:

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

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

Subclause 5.8.4 presents the message flow on the Dh interface.

5.8.2 SLF on register

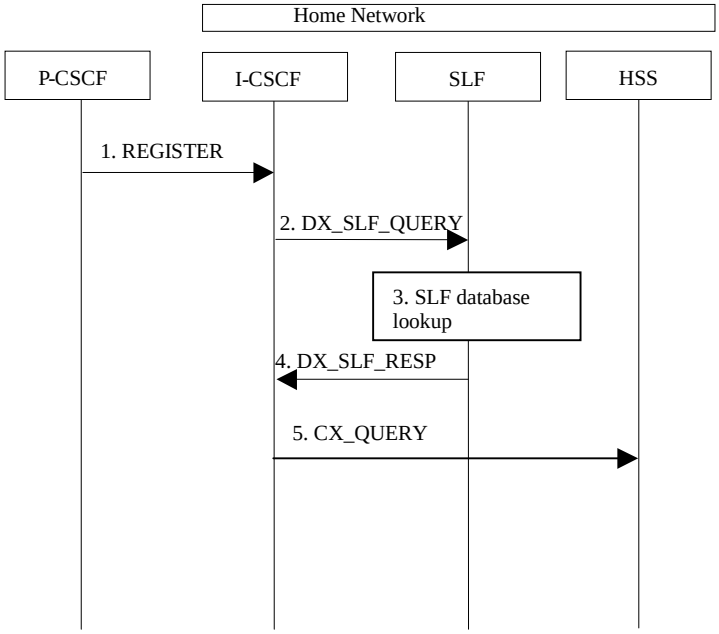


Figure 5.20: SLF on register (1st case)

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.

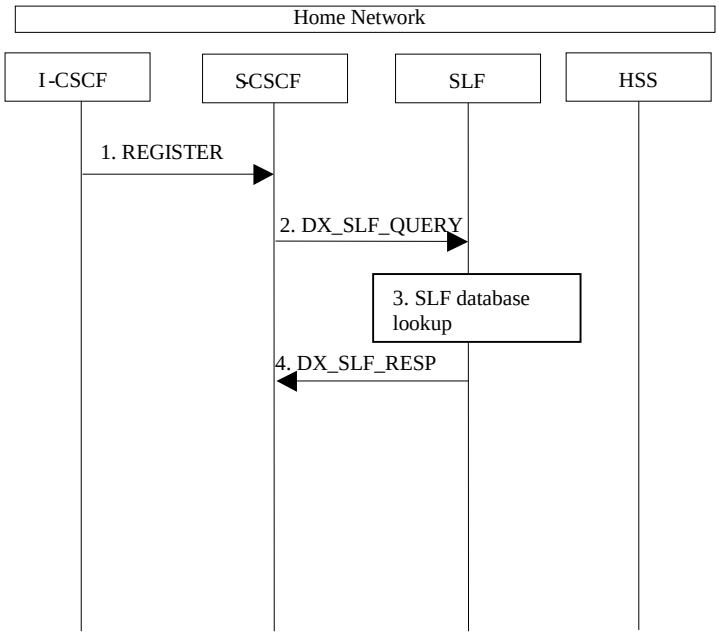


Figure 5.20a: SLF on register (2nd case)

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

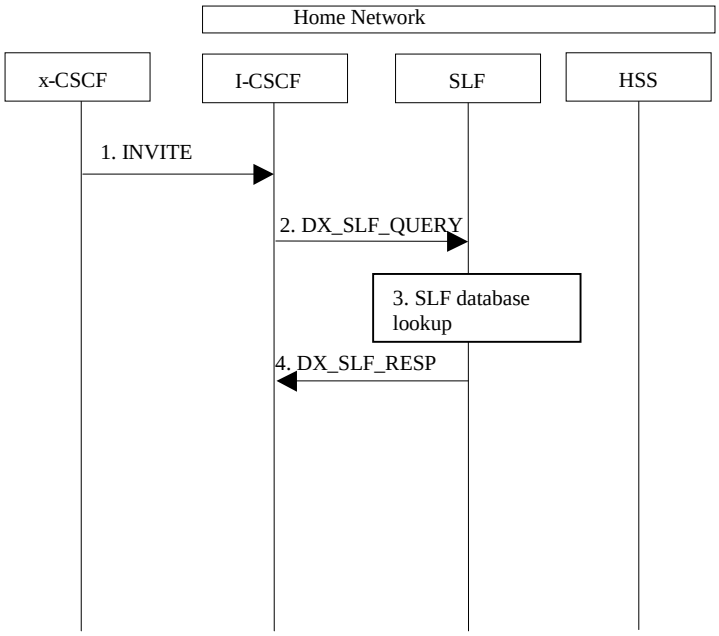


Figure 5.21: SLF on UE invite

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.

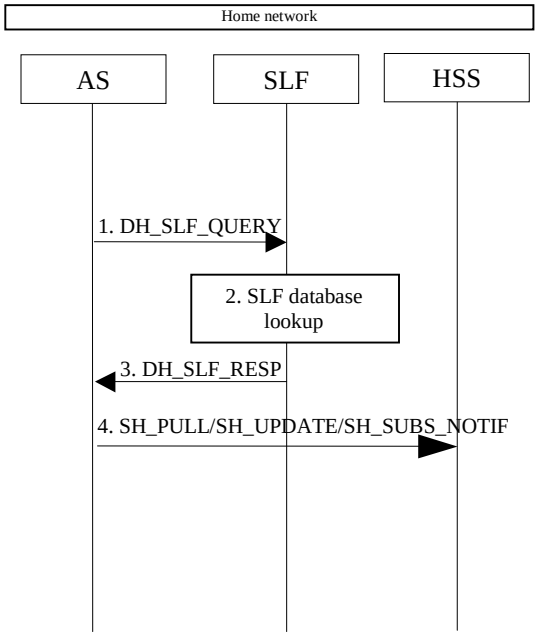


Figure 5.21a: SLF on AS access to HSS

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

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

- Normal session termination resulting from an end user requesting termination of the session using session control signalling or deletion of the IP bearers associated with a session,

- Session termination resulting from network operator intervention,

- Loss of the session control bearer or IP bearer for the transport of the IMS signalling, and

- Loss of one or more radio connections which are used to transport the IMS signalling

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

5.10.1 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.

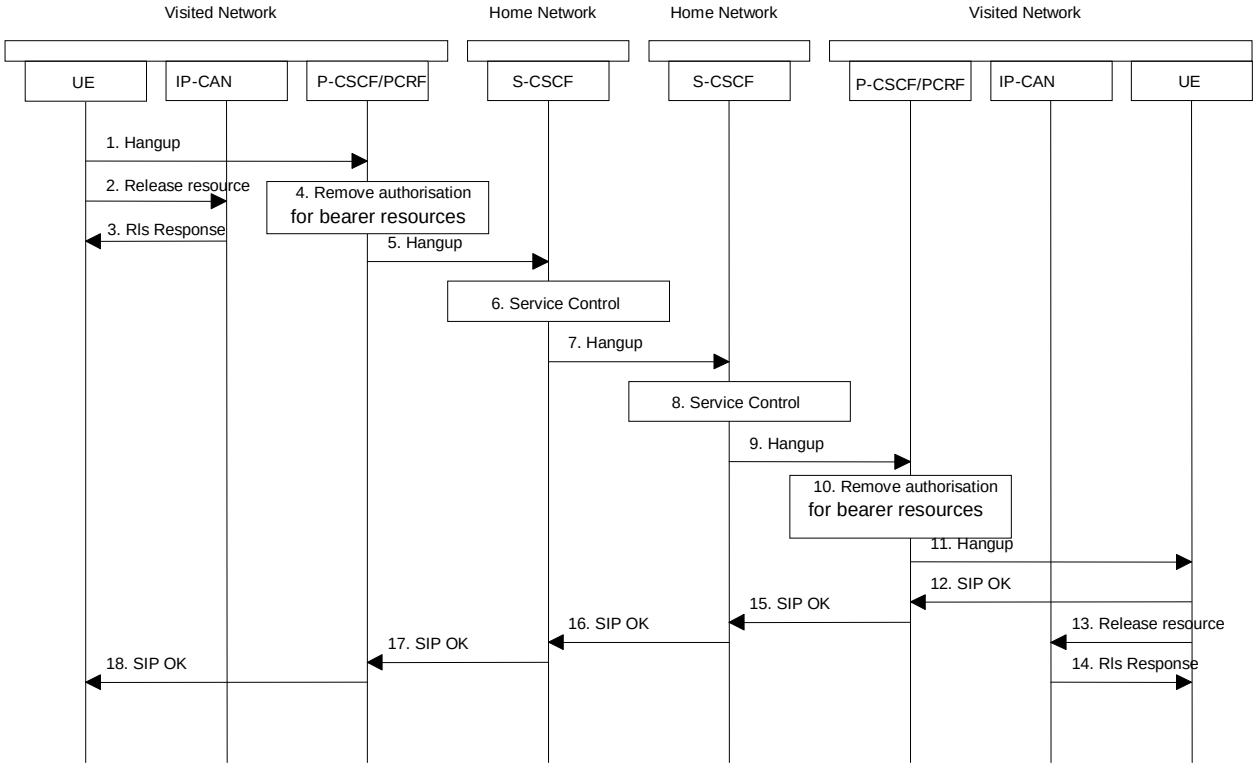


Figure 5.22: Terminal initiated session release

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

2-3. The IP network resources that had been reserved for the endpoint for this session are released, taking into account the bearer establishment mode used for the IP-CAN session. Steps 2 and 3 may take place before or after Step 1 and in parallel with Step 4.

   If RSVP was used to allocated resources, then the appropriate release messages for that protocol would be invoked here.

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

5. The P-CSCF sends a hangup to the S-CSCF of the releasing party.

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

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

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

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

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

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

12. The terminal responds with an acknowledgement, the SIP OK message (number 200), that is sent back to the P-CSCF.

13-14. The IP network resources that were reserved for the endpoint for this session are released, taking into account the bearer establishment mode used for the IP-CAN session. Steps 13 and 14 may be done in parallel with step 12. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would be invoked here.

15. The SIP OK message is sent to the S-CSCF.
16. The S-CSCF of the other party forwards the OK to the S-CSCF of the releasing.
17. The S-CSCF of the releasing party forwards the OK to the P-CSCF of the releasing.
18. The P-CSCF of the releasing party forwards the OK to the UE.

5.10.2 PSTN initiated session release

The following flow shows a PSTN terminal initiated IM CN subsystem application (SIP) session release. It is assumed that the session is active and that the bearer was established to the PSTN from the Home Network (the visited network could be the Home network in this case). Furthermore, this flow assumes that Policy and Charging Control is used.

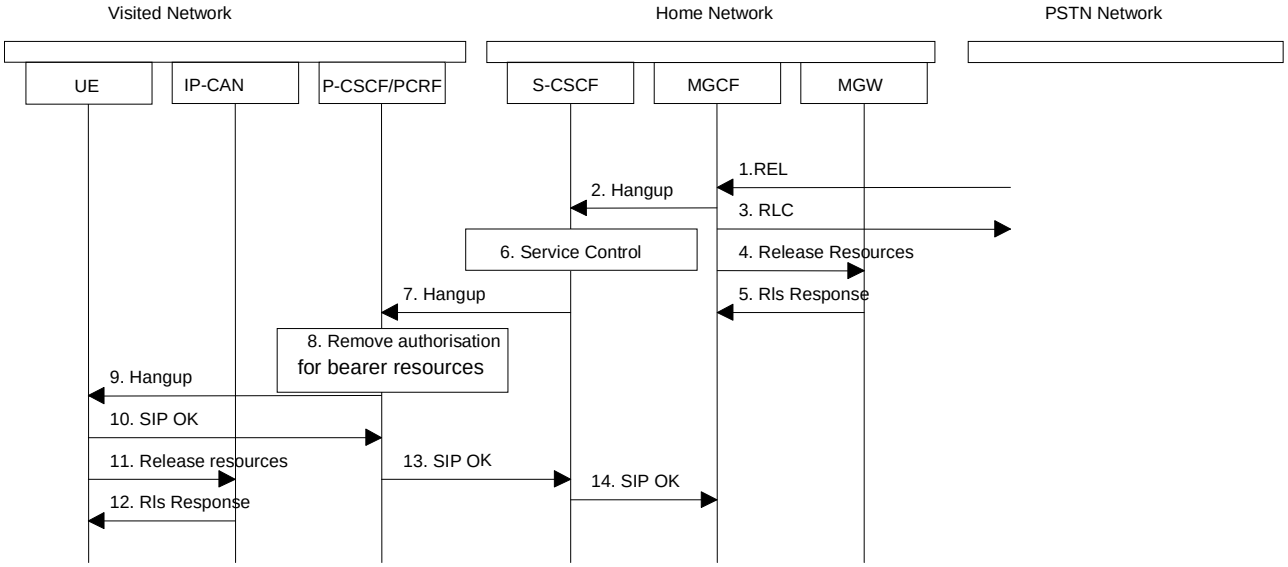


Figure 5.23: PSTN initiated session release

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

10. The 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 bearers 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/PCRF being informed of the bearer release which may, depending on policy, lead to a network initiated session release (initiated by the P-CSCF) as described in clause 5.10.3.1.

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 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 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 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]). 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

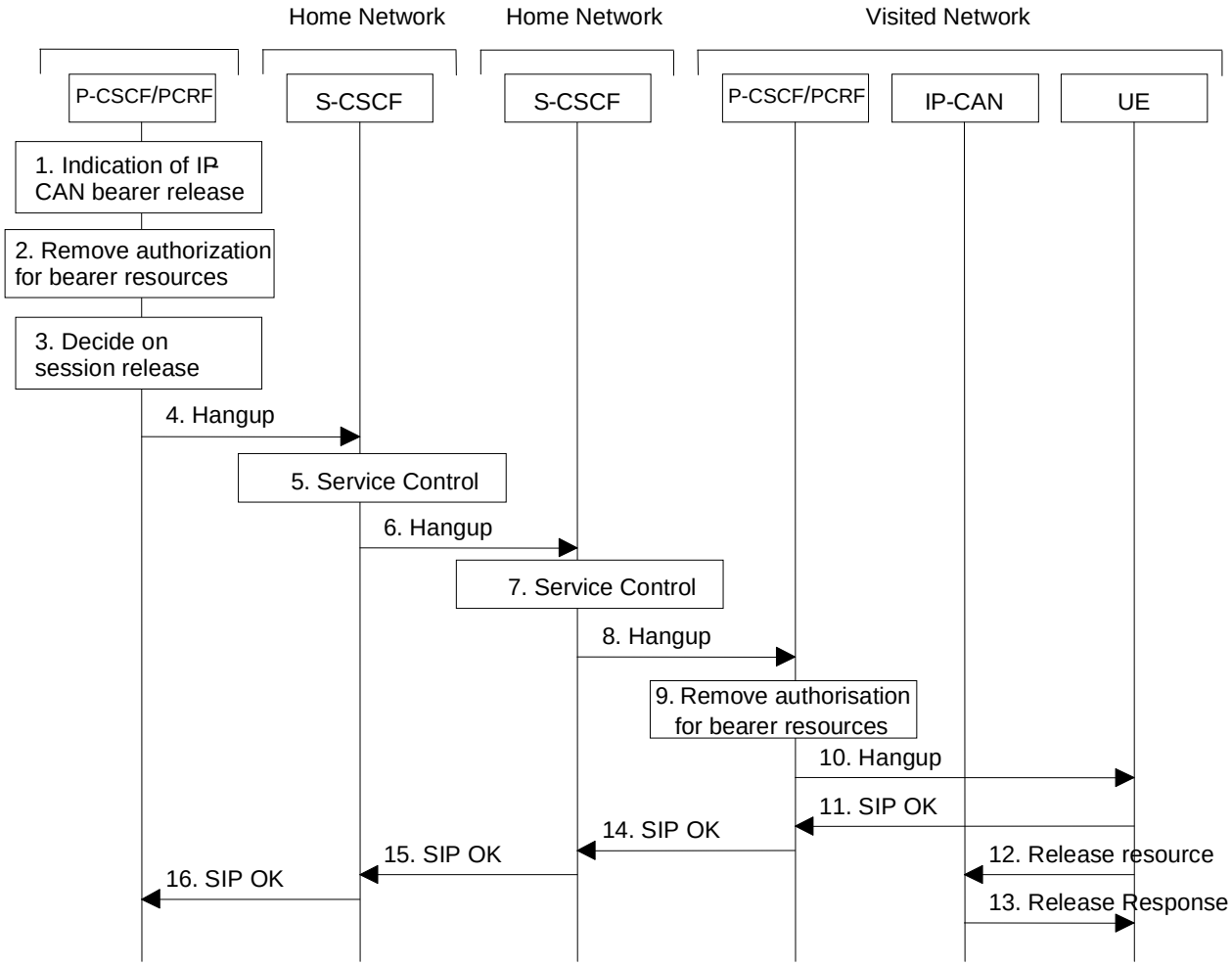


Figure 5.26: Network initiated session release - P-CSCF initiated – after removal of IP-CAN bearer

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

2. The P-CSCF/PCRF removes the authorisation for resources related to the released bearer that had previously been issued for this endpoint for this session (see TS 23.203 [54]). It is optional for the P-CSCF/PCRF 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/PCRF removes the authorisation for resources that has previously been issued for this endpoint for this session (see TS 23.203 [54]).

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

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

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

12-13. 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.

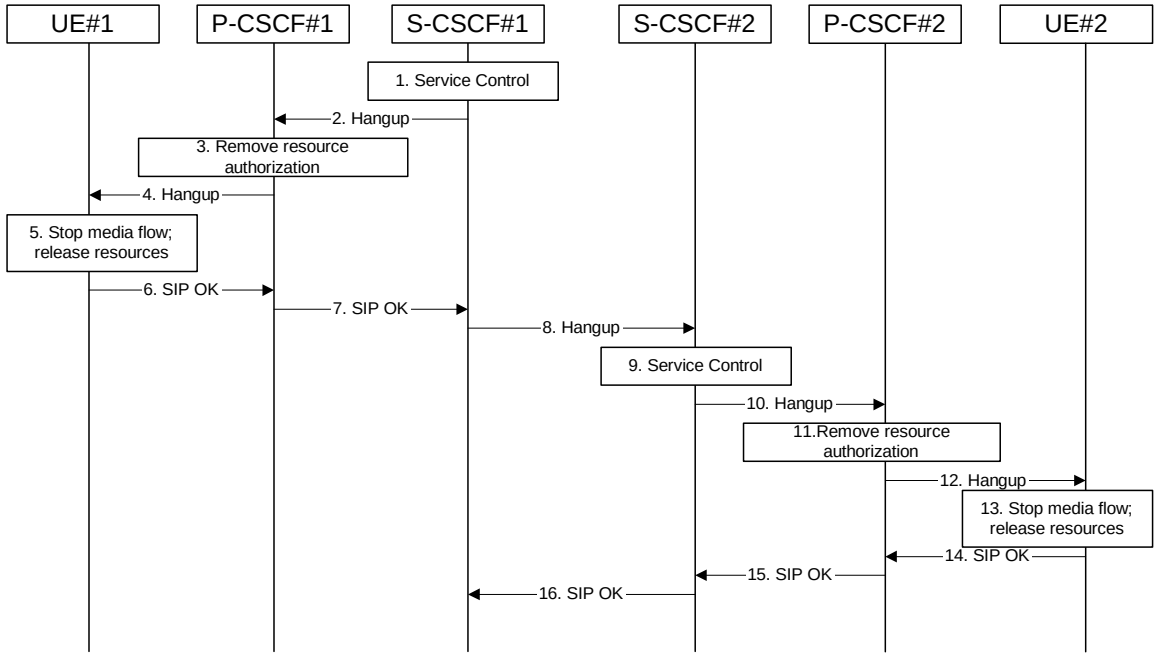


Figure 5.27: Network initiated session release - S-CSCF initiated

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 authorisation for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the session have been deleted for UE#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 authorisation for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the session have been deleted for UE#2.
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 section gives information flows for the procedures for placing sessions on hold that were previously established by the mechanisms of sections 5.4, 5.5, 5.6, and 5.7, and resuming the session afterwards. Two cases are presented: mobile-to-mobile (UE-UE), and a UE-initiated hold of a UE-PSTN session.

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

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

5.11.1.1 Mobile-to-Mobile Session Hold and Resume Procedures

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

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

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

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

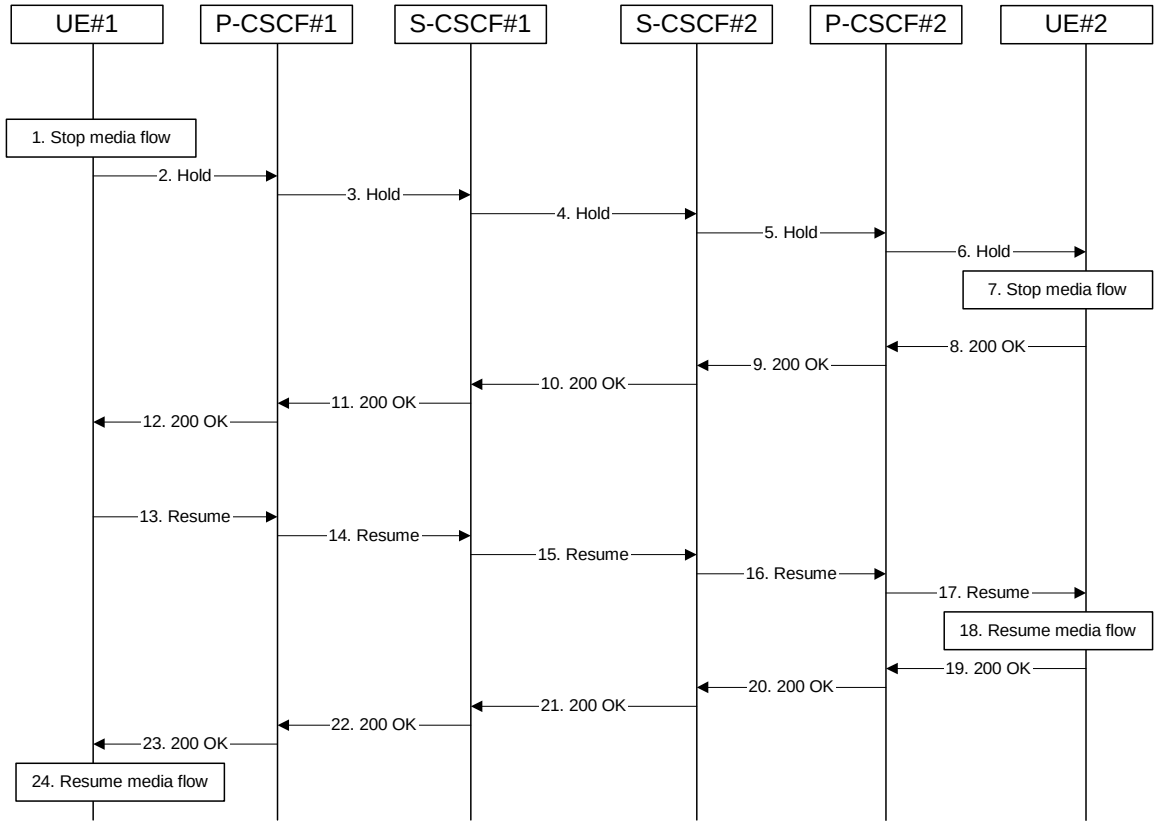


Figure 5.28: Mobile to Mobile session hold and resume

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 section of home network vs. visited network.

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

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

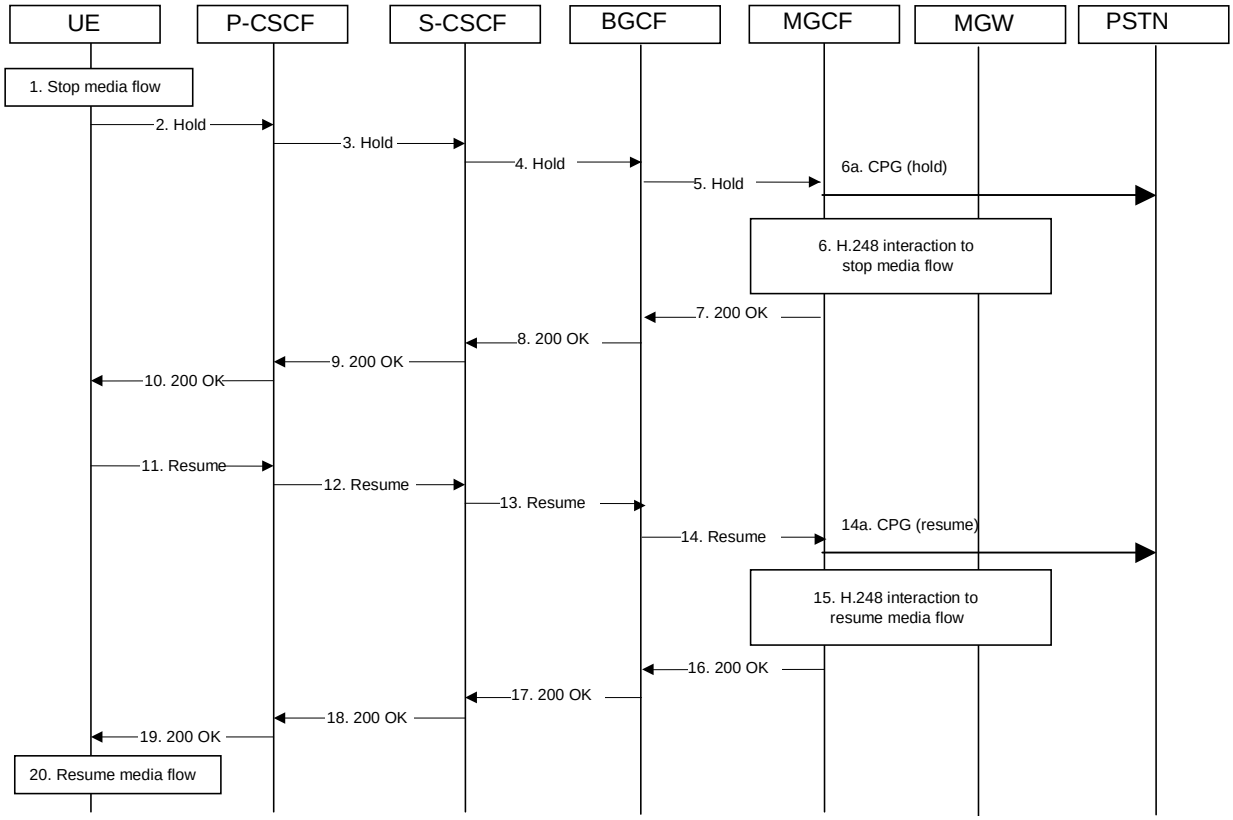


Figure 5.29: Mobile-initiated Hold and Resume of a Mobile-PSTN Session

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 section of home network vs. visited network.

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

The following information flow shows the procedures, where the session is set on hold from the PSTN side:

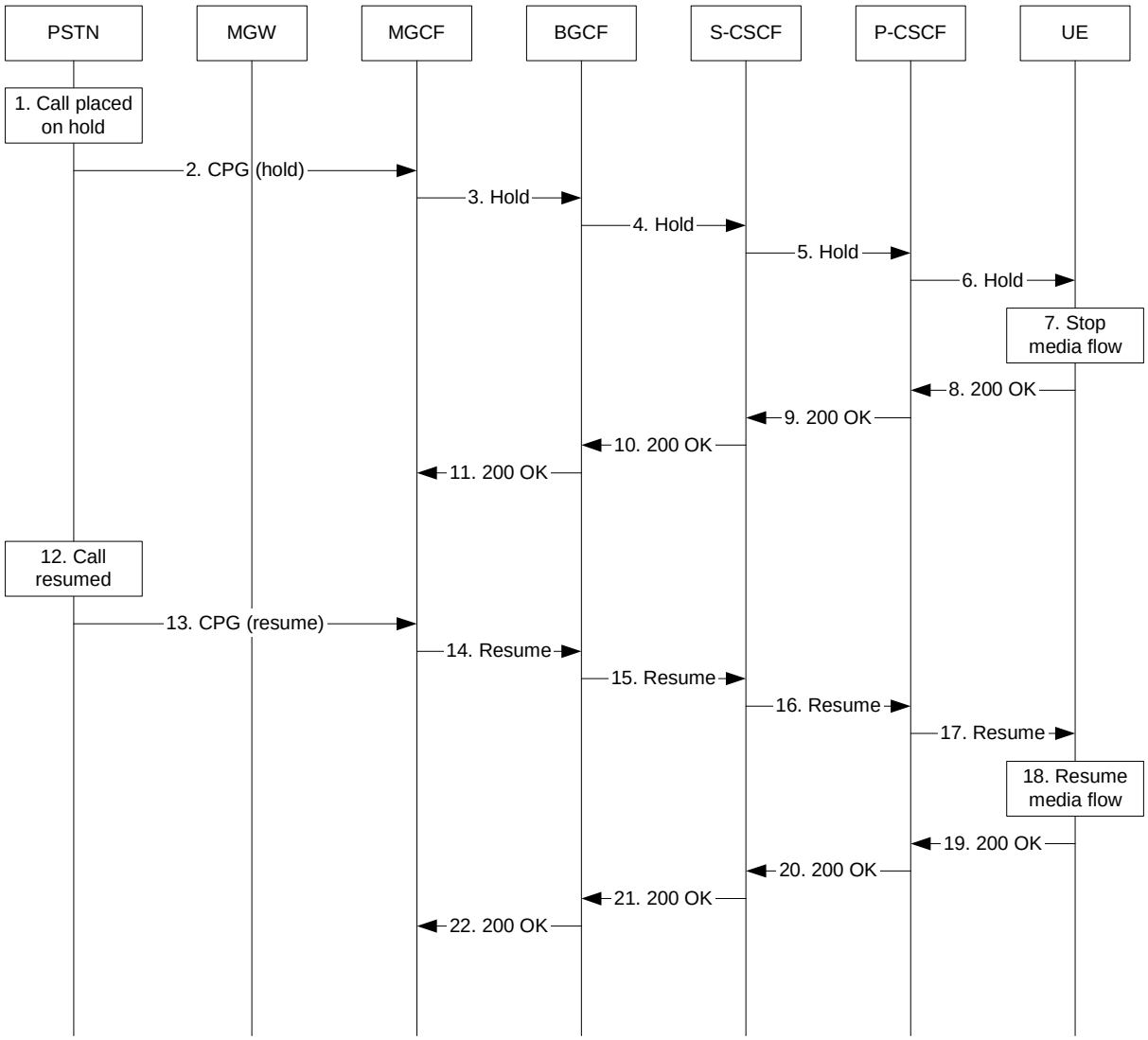


Figure 5.29a: PSTN-initiated Hold and Resume of a Mobile-PSTN Session

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

The purpose of the mechanism is to give an IMS user the possibility to withhold certain identity information as specified in 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 section gives information flows for:

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

5.11.3.1 Codec and media characteristics flow negotiation during initial session establishment

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

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

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

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

The flow presented here assumes that Policy and Charging Control is in use.

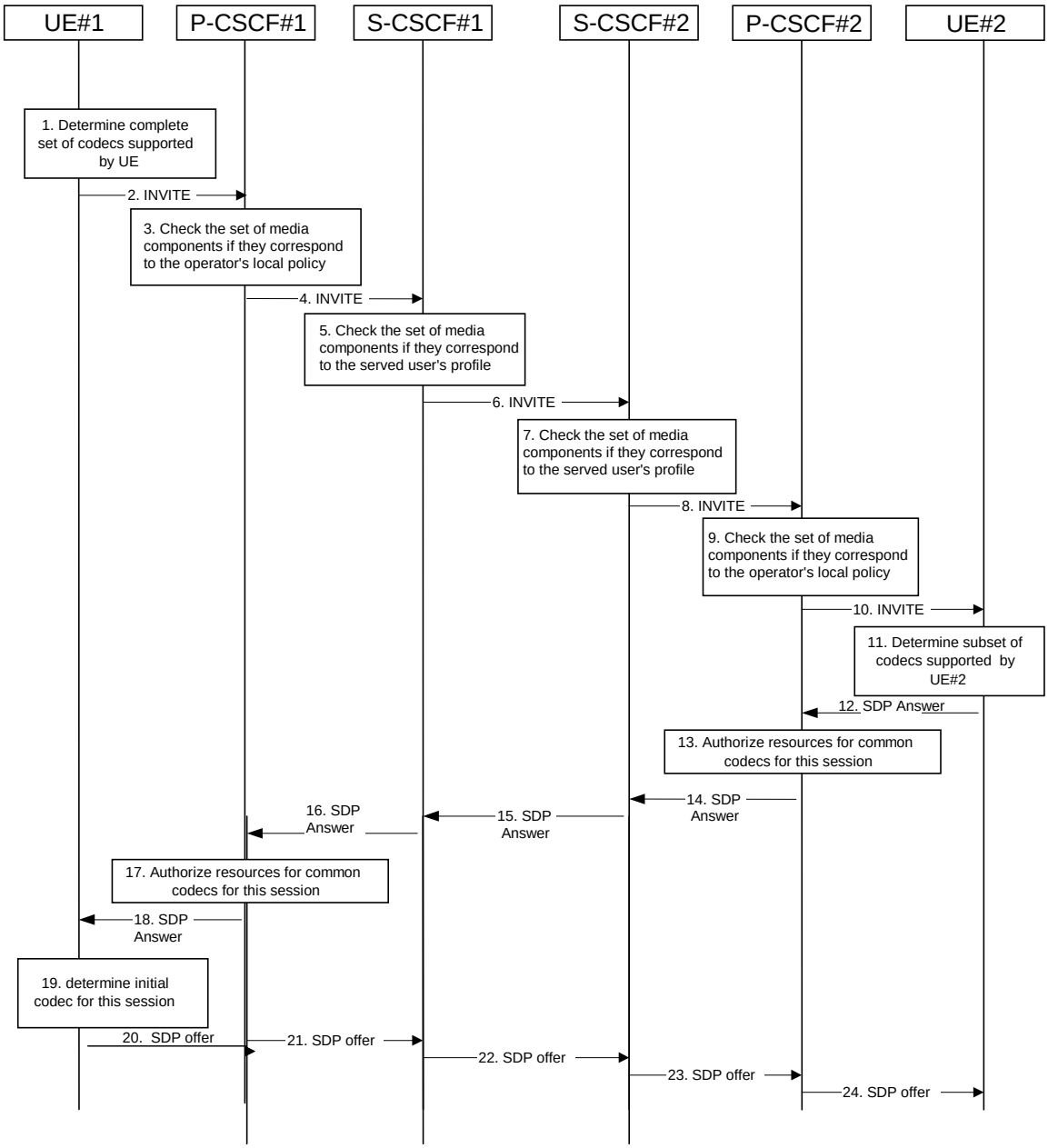


Figure 5.30: Codec negotiation during initial session establishment

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 authorisation limitation information coming from the PCRF), 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 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 authorisation limitation information coming from the PCRF), 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 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 authorises the QoS resources for the remaining media flows and codec choices.

14. P-CSCF#2 forwards the SDP response to S-CSCF#2.

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

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

17. P-CSCF#1 authorises the QoS resources for the remaining media flows and codec choices.

18. 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.

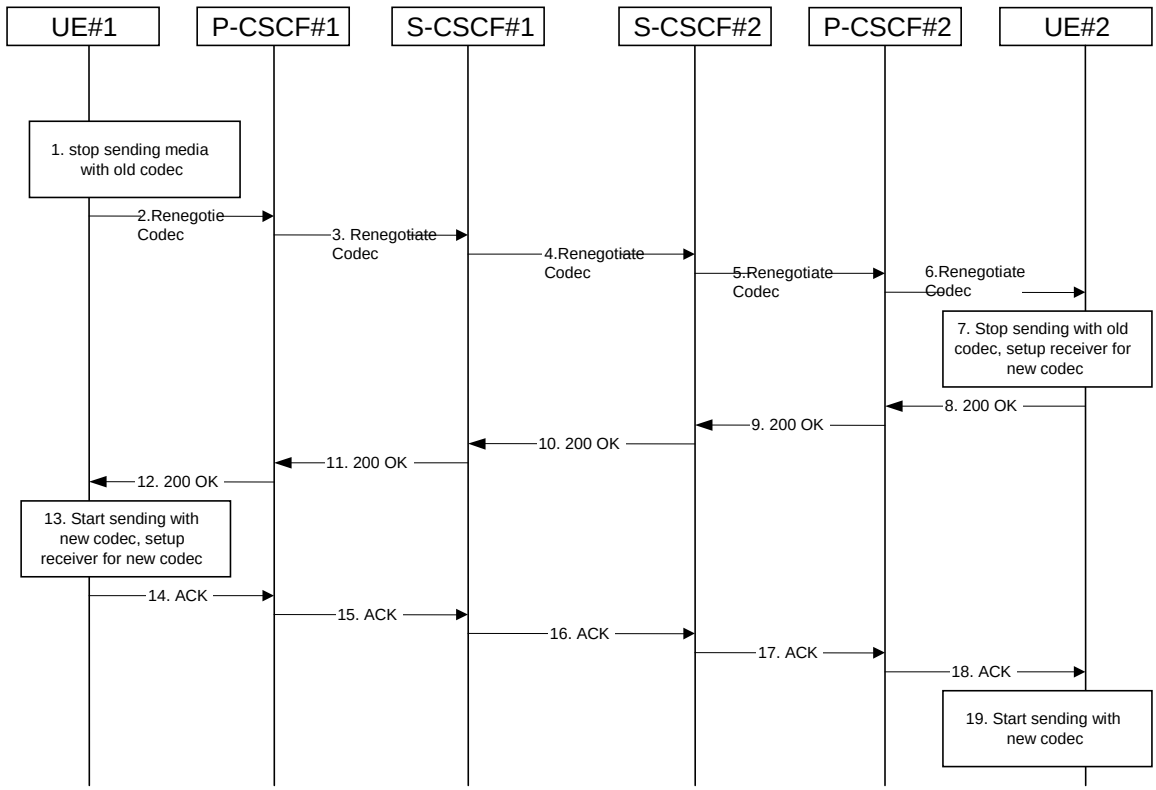


Figure 5.31: Codec or media flow change - same reservation

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 authorised, and take no further action.

7. UE#2 receives the INVITE message, and agrees that it is a change within the previous resource reservation. (If not, it would respond with a SDP message, following the procedures of 5.11.3.1). UE#2 stops sending the media streams to be deleted, and initialises its media receivers for the new codec.

8-12. UE#2 forwards a 200-OK final response to the INVITE message along the signalling path back to UE#1.

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

14-18. UE#1 sends the SIP final acknowledgement, ACK, to UE#2.

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

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

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

The flow presented here assumes that Policy and Charging Control is in use.

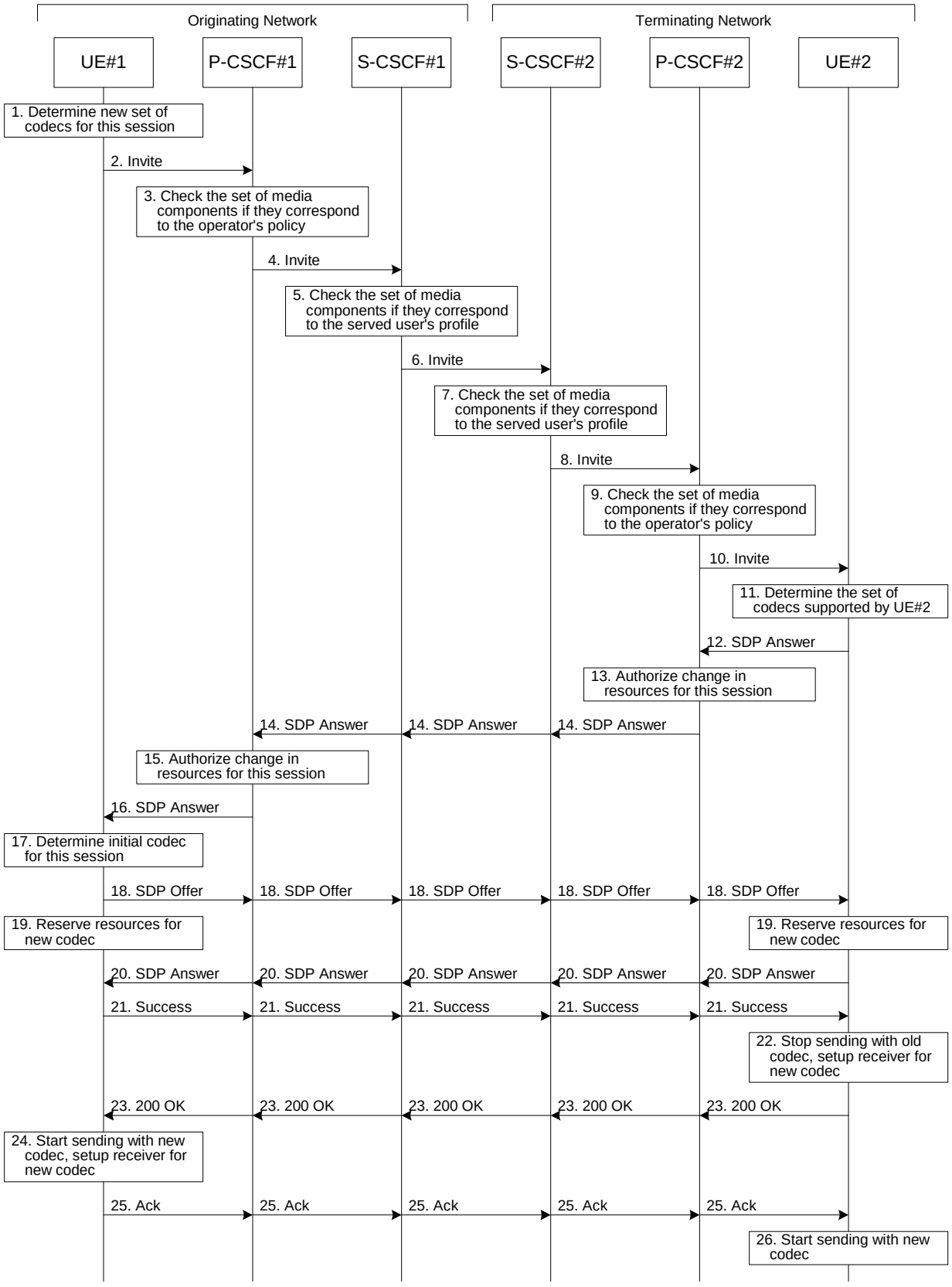


Figure 5.32: Codec or media flow change - new reservation

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 authorisation limitation information coming from the PCRF), 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 should interact with PCRF 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 authorisation limitation information coming from the PCRF), 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: Whether the P-CSCF should interact with PCRF 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 authorisation for the QoS resources, if needed, for the remaining media flows and codec choices.

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

15. P-CSCF#1 increases the authorisation 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 authorises 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.

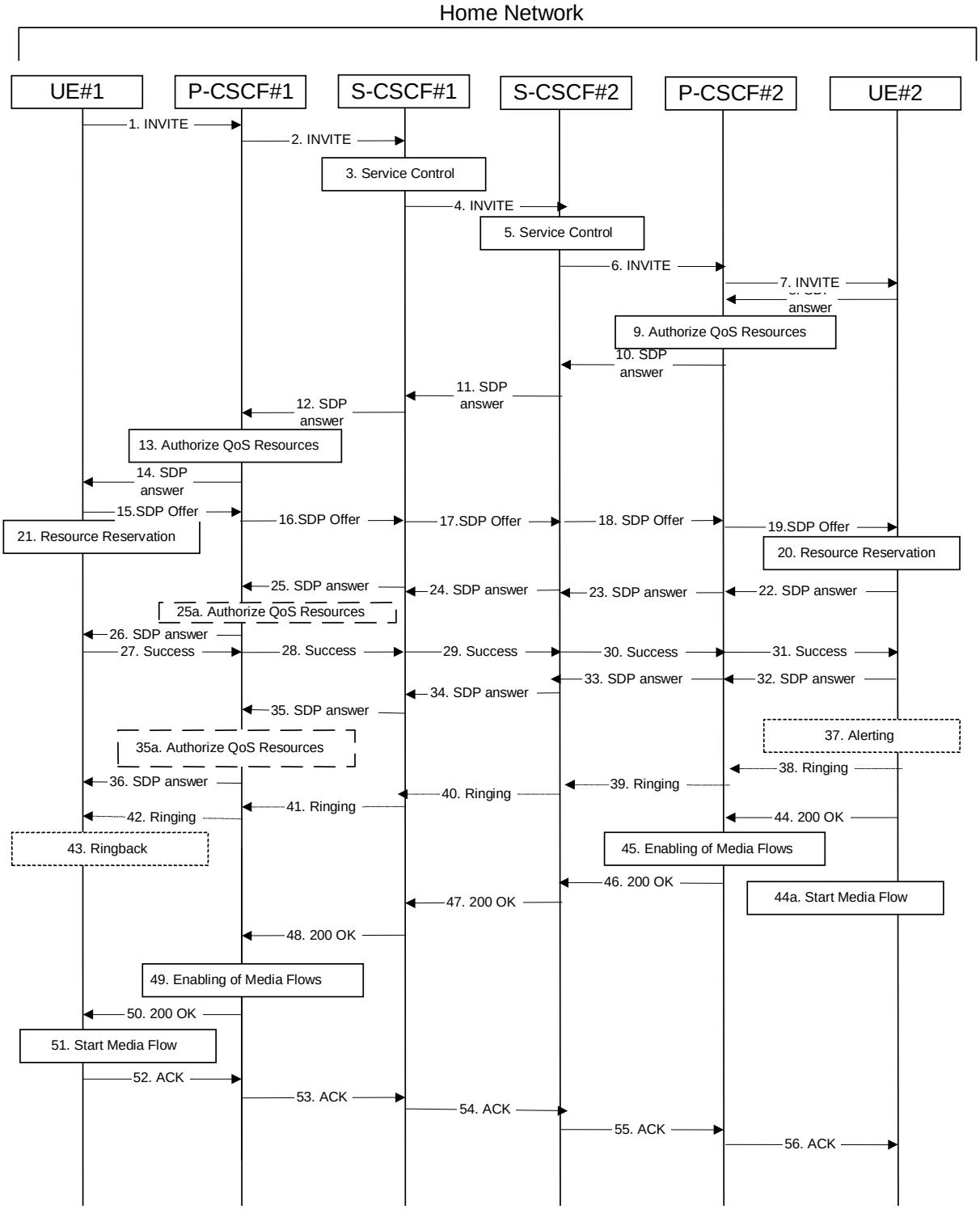


Figure 5.33: Multimedia session flow - addition of another media

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.

8. UE#2 returns the media stream capabilities of the destination to the session originator, along the signalling path established by the INVITE message.

9. P-CSCF#2 authorises the QoS resources required for this additional media.

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

11. S-CSCF#2 forwards the SDP to S-CSCF#1.

12. S-CSCF#1 forwards the SDP message to P-CSCF#1.

13. P-CSCF#1 authorises the additional resources necessary for this new media.

14. P-CSCF#1 forwards the SDP message to the originating endpoint, UE#1.

15-19. The originator decides the offered set of media streams for this media addition, and sends the offered SDP to P-CSCF#1.

20. 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 signaling path established by the INVITE message. The message is sent first to P-CSCF#1.

25a. P-CSCF#1 authorises any additional media for the proposed SDP.

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

27-31. UE#1 sends the final agreed SDP to UE#2 via the established path.

32-35. UE#2 responds to the offered final media.

35a. P-CSCF#1 authorises the media agreed.

36. The response is forwarded to UE#1.

37. UE#2 may optionally delay the session establishment in order to alert the user to the incoming additional media.

38. If UE#2 performs alerting, it sends a ringing indication to the originator via the signalling path. The message is sent first to P-CSCF#2.

39. P-CSCF#2 forwards the ringing message to S-CSCF#2.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 section 4.3.3.2).
- The display name is the user's name if available, an indication of privacy or unavailability otherwise. The display name is a text string which may identify the subscriber, the user or the terminal.

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

5.11.4.1 Procedures for providing the authenticated identity of the originating party

Authentication of the subscriber is performed during the registration procedures, as described in section 5.2.2.3. As a result of the registration procedures, one or several Public User Identity(ies) of the originating party is/are stored in P-CSCF#1. 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.

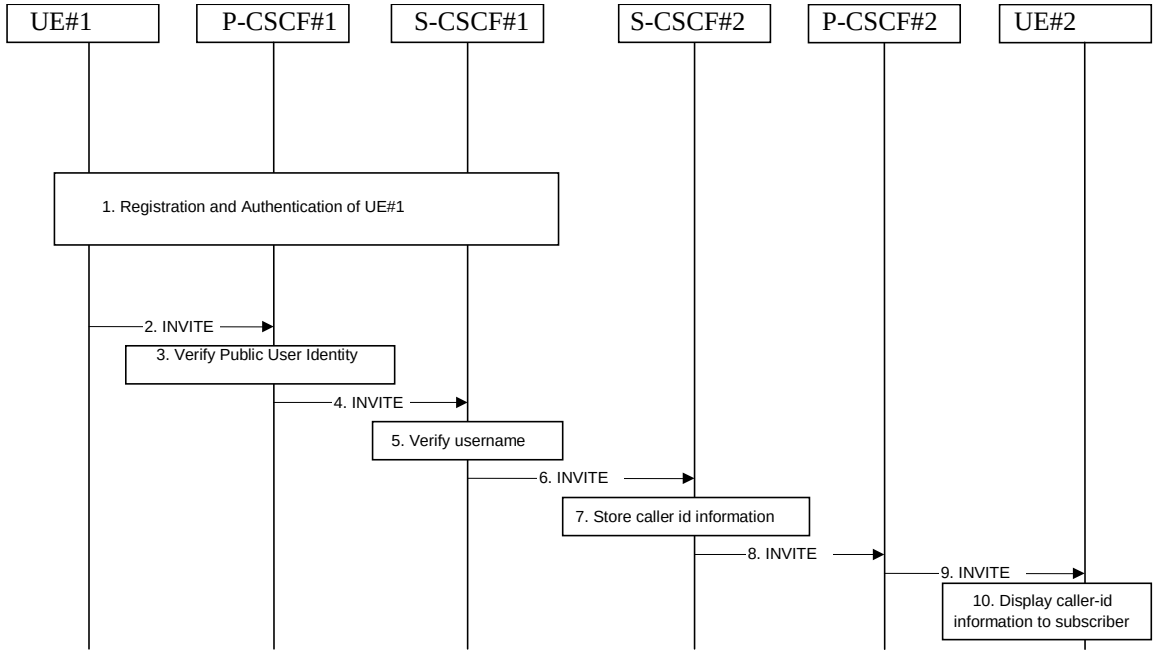


Figure 5.34: Providing the authenticated Identity of the originating party

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).

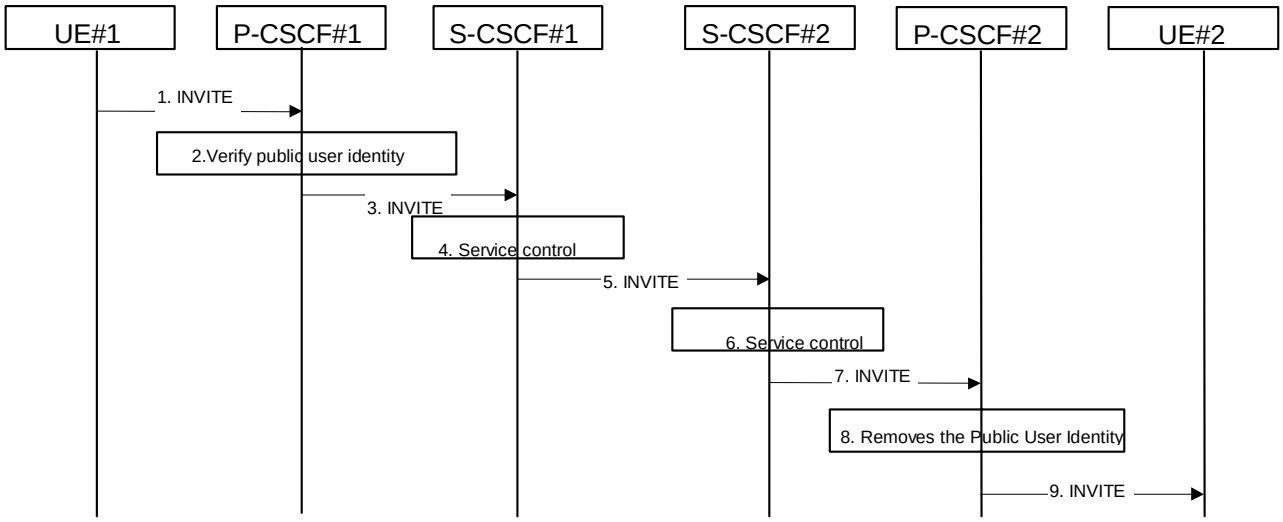


Figure 5.35: Blocking the identity of the originating party

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

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

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

5.11.5.1 Session Redirection initiated by S-CSCF to IMS

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

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

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

This is shown in the following information flow:

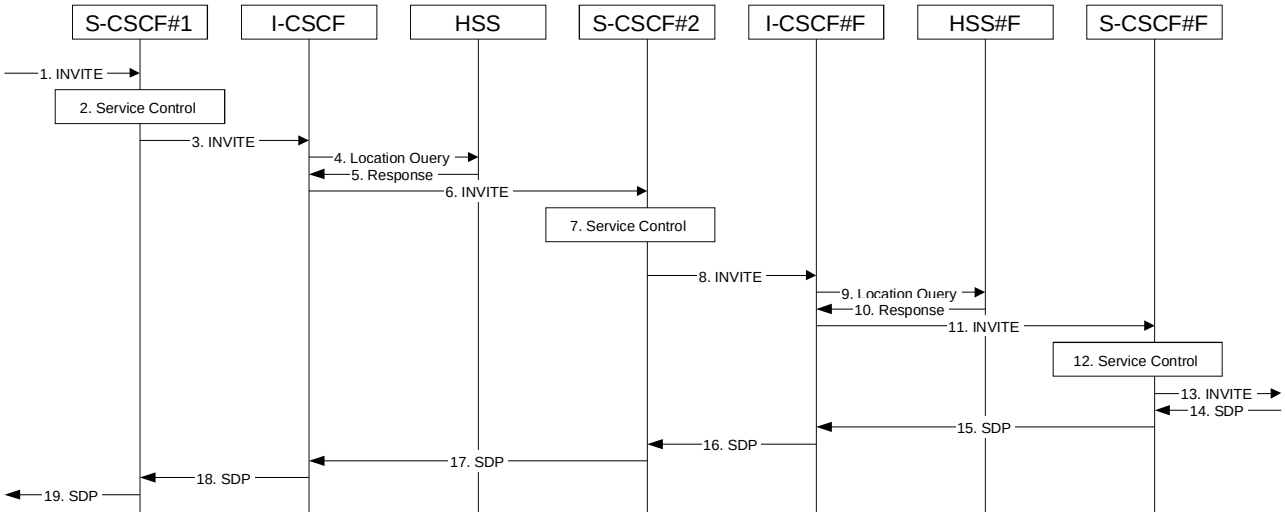


Figure 5.36: Session redirection initiated by S-CSCF to IMS

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.
2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt.
3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. The INVITE message is sent to an I-CSCF for that operator.
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:

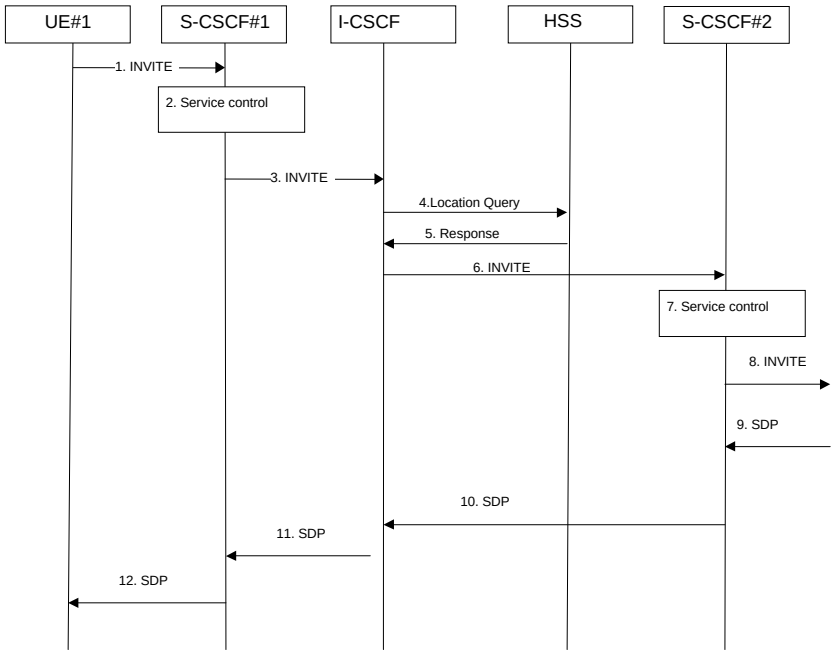


Figure 5.37: Session redirection to PSTN Termination (S-CSCF #2 forwards INVITE)

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 subclause 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 subclause 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:

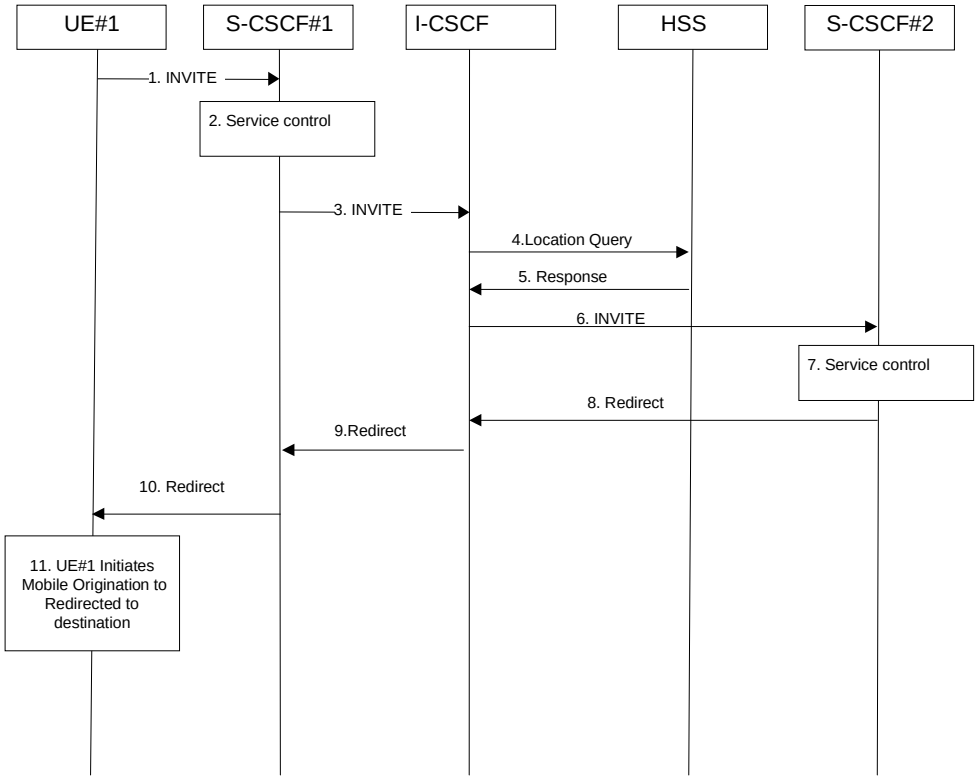


Figure 5.37a: Session redirection to PSTN Termination (REDIRECT to originating UE#1)

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:

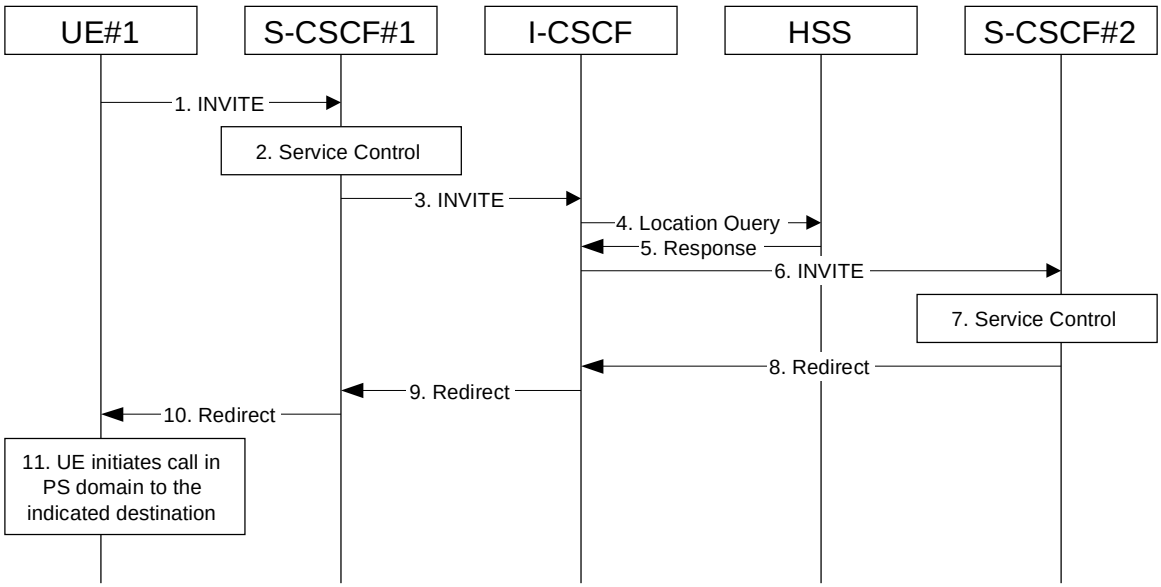


Figure 5.38: Session redirection initiated by S-CSCF to general endpoint

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 sections 1, 2, or 3 above, based on the type of destination.

This is shown in the following information flow:

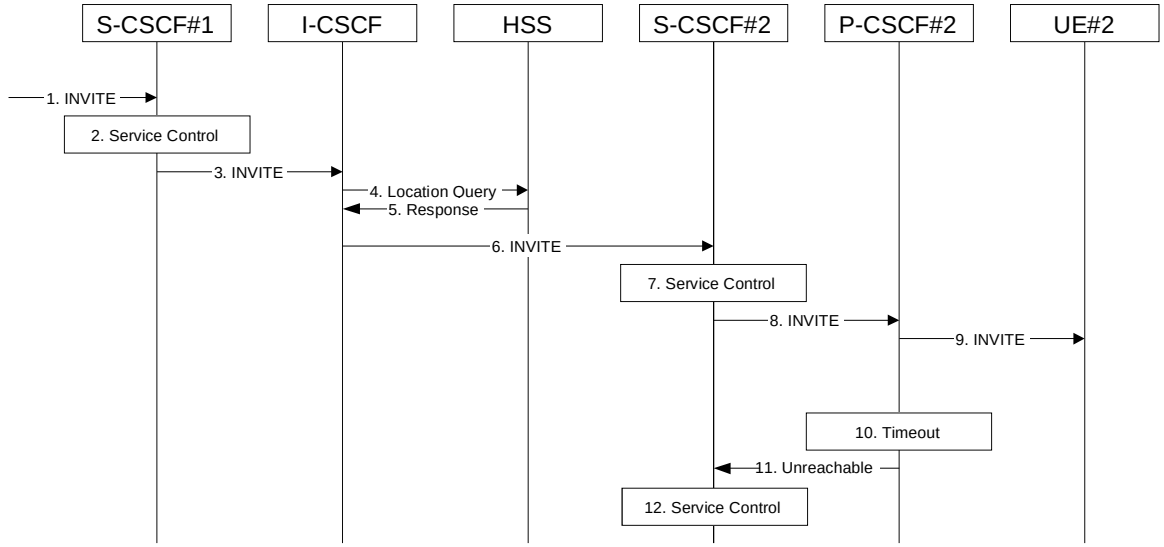


Figure 5.39: Session redirection initiated by P-CSCF

Step-by-step processing is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow.
2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt.
3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. The INVITE message is sent to an I-CSCF for that operator.
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 subsections 1, 2, or 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:

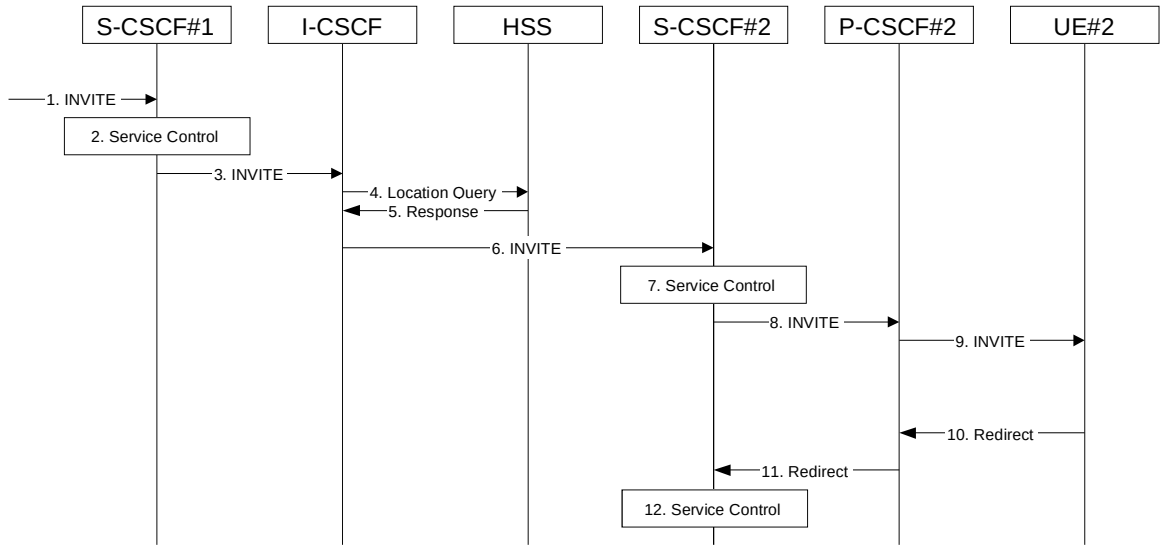


Figure 5.40: Session redirection initiated by UE

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 subsection 1, 2, or 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 signaling path to the originating endpoint, who initiates a session to the new destination.

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

The originating end point may be a UE as shown in the example flow in figure 5.41 or it may be any other type of originating entity as defined in subclause 5.4a. 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 subclause 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.

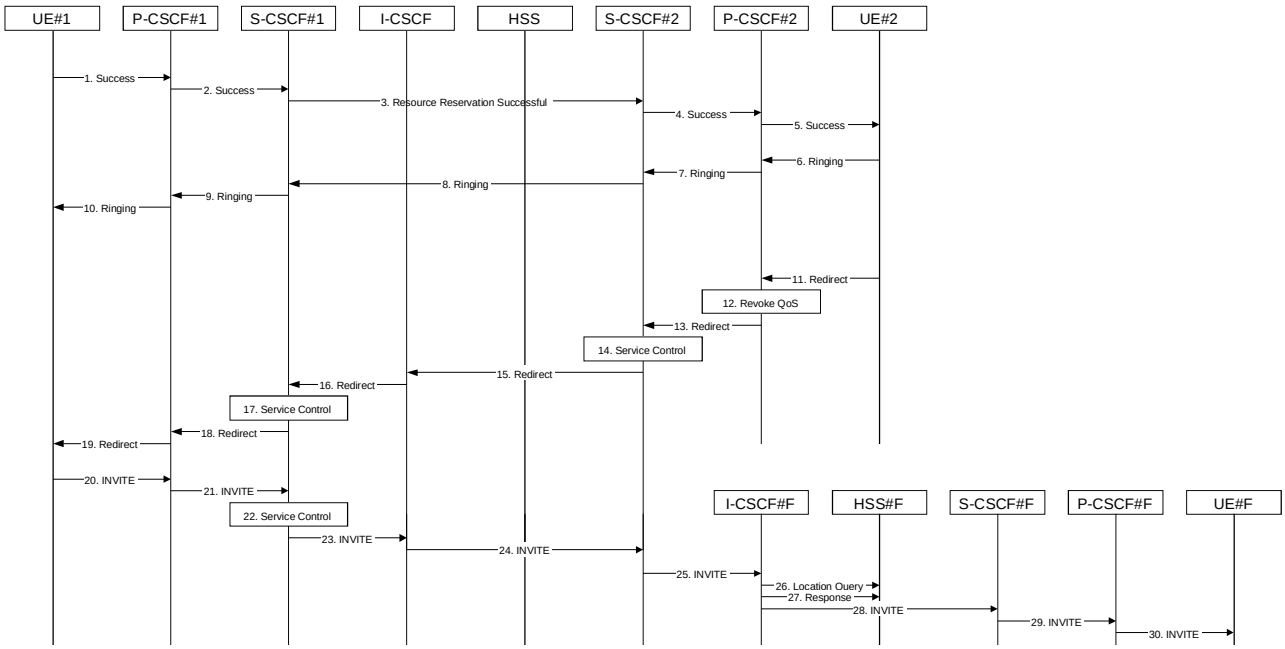


Figure 5.41: Session redirection after bearer establishment

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 authorisation for QoS for the current session.

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

14. S-CSCF#2 invokes whatever service logic is appropriate for this session redirection. If UE#2 does not subscribe to session redirection service, or did not supply a new destination 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 authorisation for QoS for the current session and sends the Redirect response to UE#1.

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

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

22. S-CSCF#1 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 section gives information flows for the procedures for performing session transfers. This is presented in two steps: first a basic primitive that can be used by endpoints to cause a multi-media session to be transferred, and second the procedures by which this primitive can be used to implement some well-known session-transfer services.

5.11.6.1 Refer operation

The refer primitive is an information flow indicating a "Refer" operation, which includes a component element "Refer-To" and a component element "Referred-By". The end point receiving a referral may be UE#1 as shown in the example flow in figure 5.42 or it may be any other type of originating entity as defined in subclause 5.4a. 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 subclause 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:

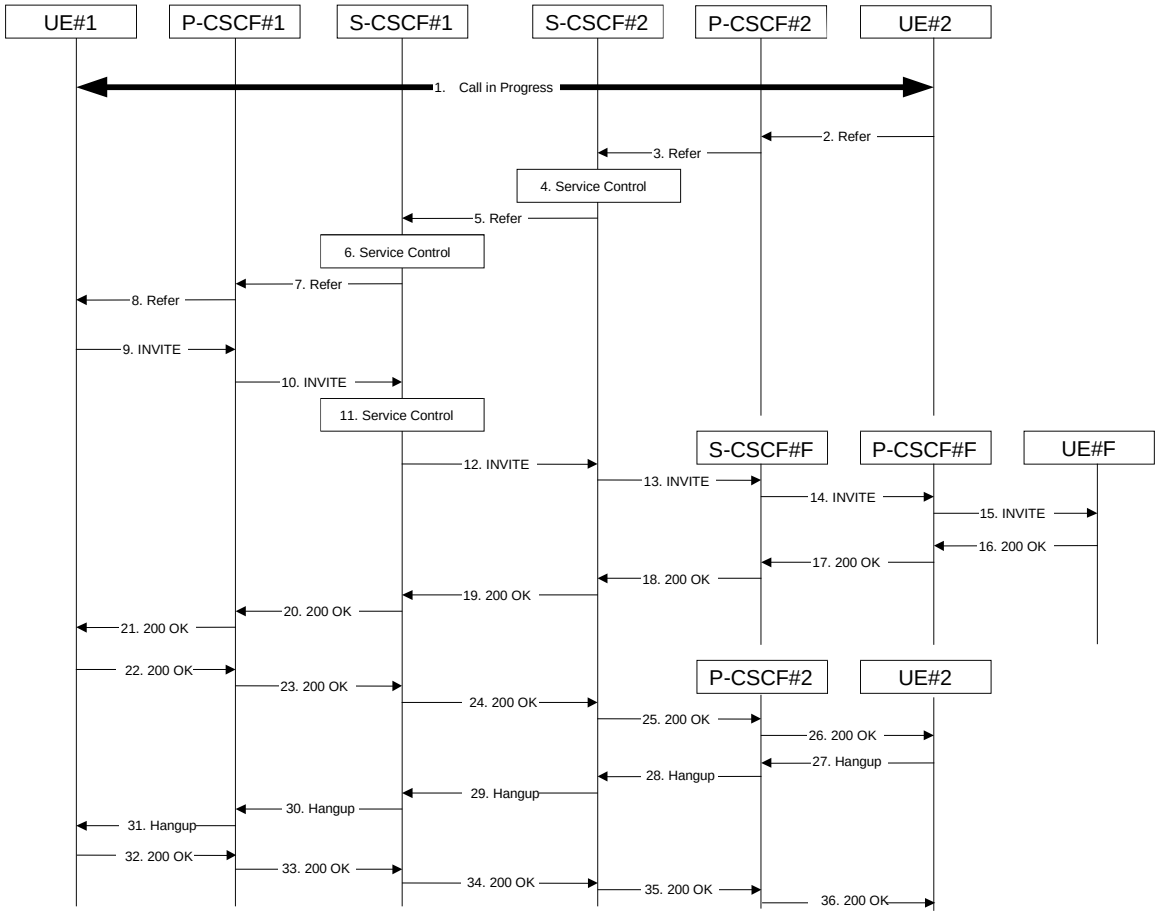


Figure 5.42: Refer operation

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 subclause.

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

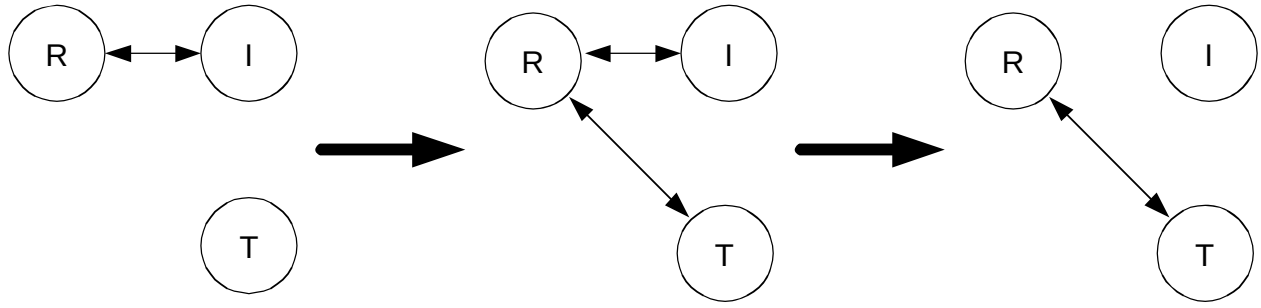
5.11.6.2.0 General

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

5.11.6.2.1 Blind Transfer and Assured Transfer

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

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

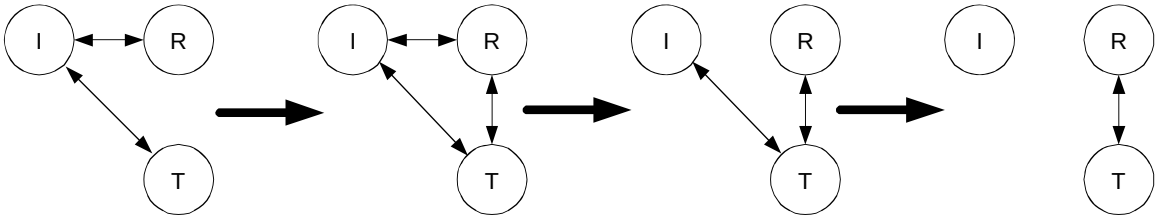


An Assured Transfer is identical to the above, except that I waits until the Refer successfully completes before issuing the BYE message to terminate its connection with R. If the new session from R to T were to fail, R would still have a session with I.

5.11.6.2.2 Consultative Transfer

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

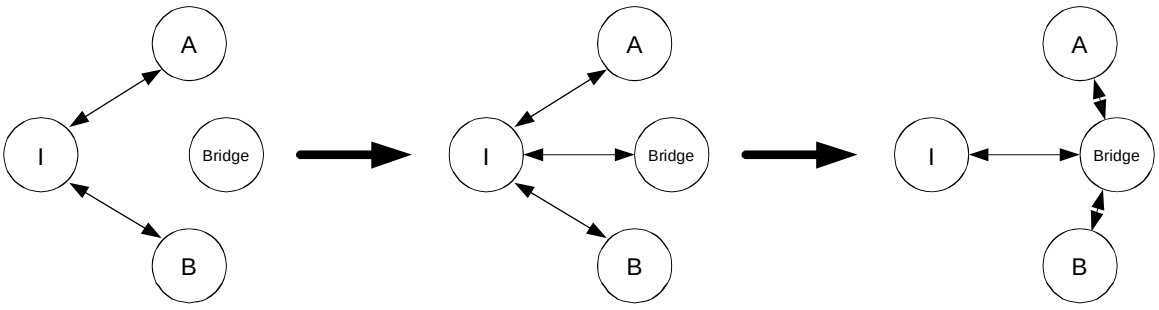
From the starting configuration, as shown in the leftmost diagram in the previous section, I places the session with R on hold and establishes a new session with T. This is shown in the leftmost diagram below. I then sends a Refer message to T, causing T to establish a session with R. This is shown in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



5.11.6.2.3 Three-way Session

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

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



The conference bridge service is in control of the termination sequence. On termination of one of the three sessions, it may either terminate the other two sessions by use of the session clearing procedures of section 5.11, or may utilize the procedures of subsection 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 section describes information flows for the procedures of Mobile Terminating call flows for unregistered IMS Public User Identities. The detection of an unregistered Public User Identity is done in HSS and if this Public User Identity has services related to unregistered state, a S-CSCF is selected for the unregistered Public User Identity. S-CSCF performs whatever further actions are appropriate for the call attempt to the unregistered IMS Public User Identity.

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

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

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

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

This is shown by the information flow in Figure 5.43:

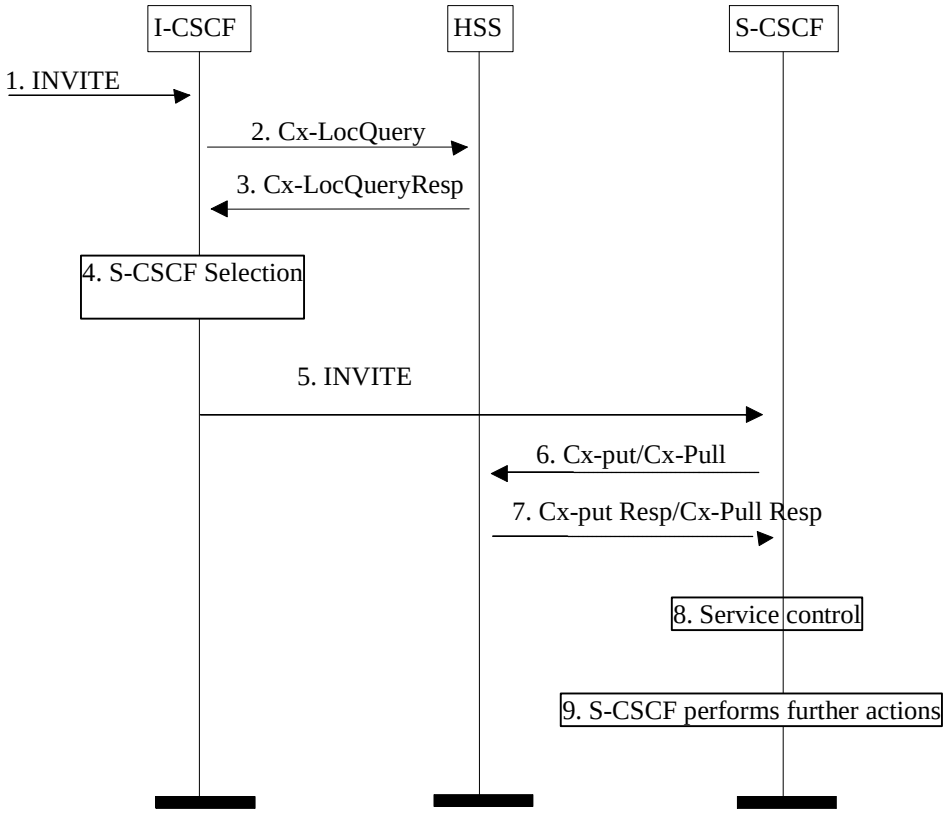


Figure 5.43: Mobile Terminating call procedures to unregistered IMS Public User Identity that has services related to unregistered state

1. I-CSCF receives an INVITE message.
2. I-CSCF queries the HSS for current location information.
3. HSS either responds with 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 (section 5.7.2a) applies).

The S-CSCF may deregister the Public User Identity at any time (e.g. according to operator network engineering requirements) by issuing a Cx-Put2 (Public User Identity, clear S-CSCF name) clearing the S-CSCF name stored in the

HSS. If S-CSCF name stored by the HSS does not match the name of the S-CSCF that originated the Cx-Put2 then the HSS will acknowledge the clearing request but take no further action.

5.12.2 Mobile Terminating call procedures to unregistered Public User 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):

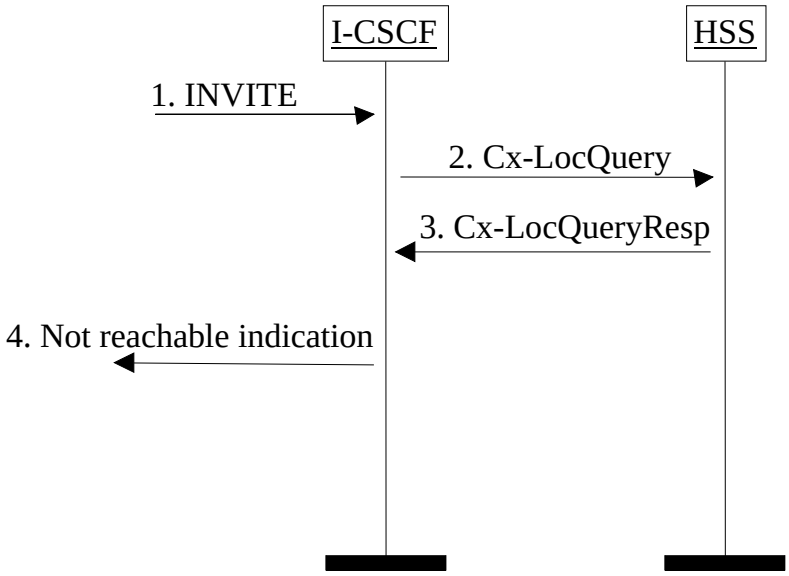


Figure 5.44: Mobile Terminating call procedures to unregistered Public User Identity that has no services related to unregistered state

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 section describes how the resources of the MRFC/MRFP are used.

5.14.1 Interactions between the UE and the MRFC

In some cases an operator may wish to make an MRFC available directly to a UE, for example to support ad-hoc multi-party sessions to be initiated by the UE. In this case, the operator advertises the name of one or more MRFCs and a UE

will invite an MRFC to a session. The session invitation would need to contain additional information indicating the specific capabilities (e.g., multi-party) desired. A conference ID would be assigned by the MRFC and returned to the UE. This would then be used by the UE in subsequent interactions with the MRFC and other UEs participating in the session.

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

5.14.2 Service control based interactions between the MRFC and the AS

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

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

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

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

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

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

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

5.15 Mobile Terminating session procedure for unknown user

5.15.0 General

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

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 section 5.15.2. The flows of figure 5.45 could include SLF determination of the HSS, however these are not shown for clarity.

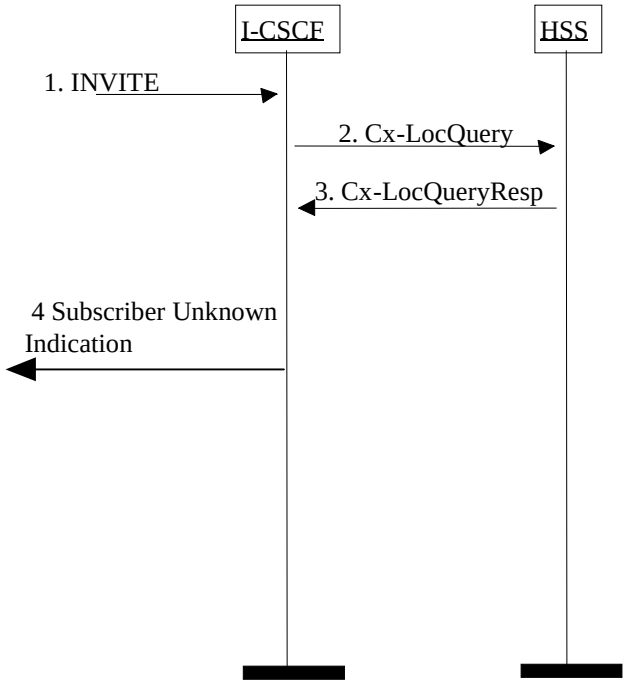


Figure 5.45: HSS determination of unknown user

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

5.15.2 Unknown user determined in the SLF

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

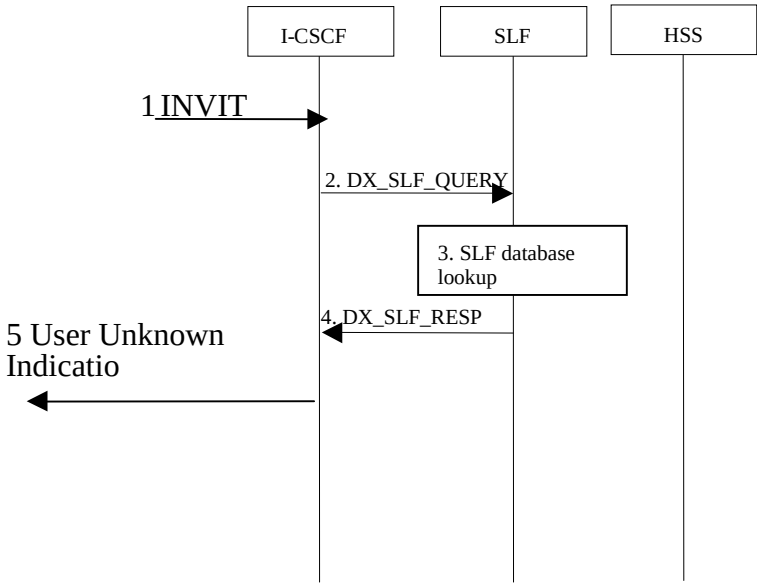


Figure 5.46: SLF determination of unknown user

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

5.16 IMS messaging concepts and procedures

5.16.0 General

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

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

5.16.1 Immediate Messaging

5.16.1.0 General

This sub-clause describes architectural concepts and procedures for 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 sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by TS 26.141 [37]

If the message size exceeds the size limit for MESSAGE requests, the UE shall use alternative means to deliver the content of the Immediate Message. Session based messaging specified in subclause 5.16.2 provides such means. 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

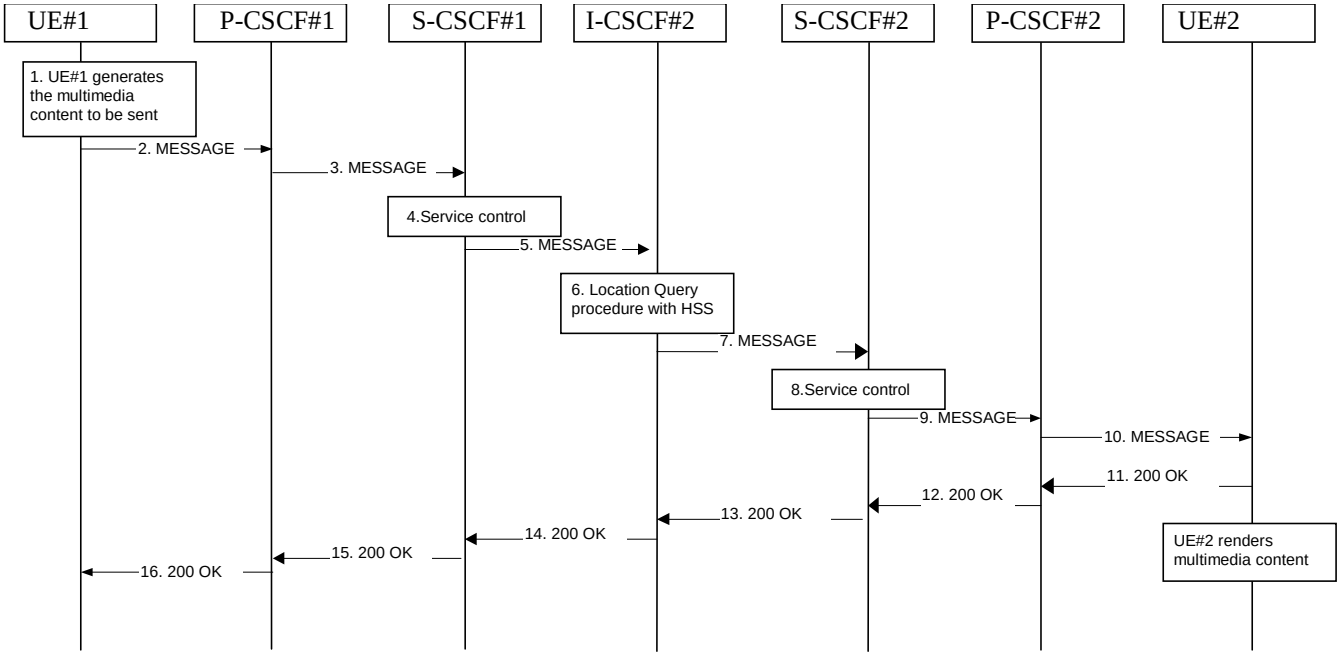


Figure 5.47: Immediate Messaging procedure to registered Public User Identity

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 criterias set by the user. The AS may then respond to the MESSAGE request with an appropriate error response.

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

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

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

5.16.1.1.2 Immediate messaging procedure to unregistered Public User Identity

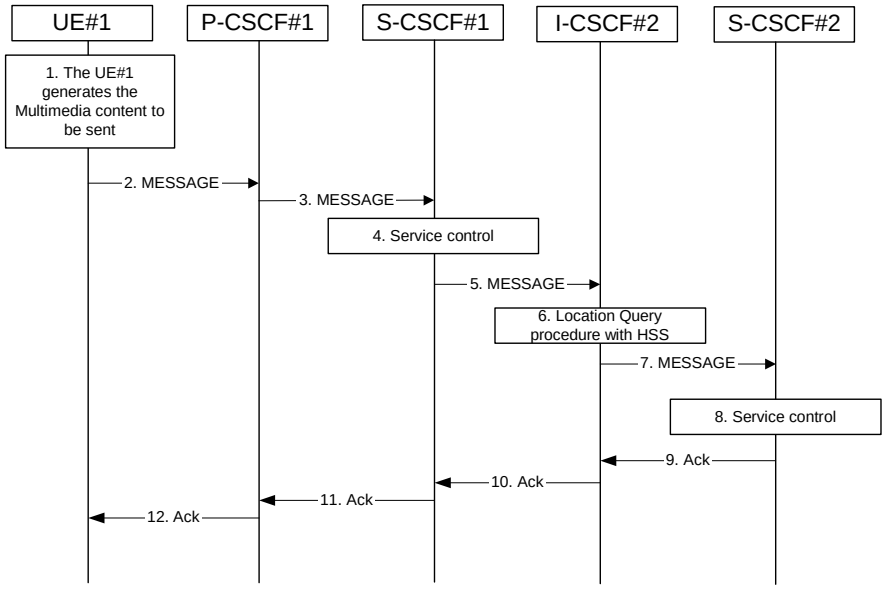


Figure 5.48: Immediate messaging to unregistered Public User Identity, service control invoked

1-5. The same actions apply as for when the Public user identity is registered, see step 1-5 in clause 5.16.1.1.1.

6. I-CSCF#2 interacts with the HSS as per the terminating procedures defined for unregistered Public User Identities in clause 5.12.1. If the Public User Identity has no services related to unregistered state activated the interaction with HSS would be as per the procedure defined in clause 5.12.2.

7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.

8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable or the UE#2 does not have a service activated that temporarily hold the MESSAGE request in the network.

   S-CSCF#2 invokes whatever service control logic appropriate for this MESSAGE request. This may include routing the MESSAGE request to an Application Server, which processes the request further on.

   For example, the UE#2 may have a service activated that allows delivery of any pending MESSAGE request. The AS may then hold the MESSAGE request and deliver the MESSAGE request when the UE#2 becomes reachable. In this case, depending on user settings UE#2 controls the delivery of the pending MESSAGEs.

9-12. The MESSAGE request is acknowledged with an appropriate acknowledgement response. The acknowledgement response traverses the transaction path back to UE#1.

5.16.1.2 Immediate messages with multiple recipients

IMS users shall be able to send a single immediate message to multiple recipients, as specified in TS 22.340 [29a]. The following means are supported to achieve this:

- A PSI identifying a new group is created in the appropriate Application Server, and members are added to this group (e.g. by the user via the Ut interface or by the operator via O&M mechanisms). Immediate messages addressed to this PSI will be routed to the AS hosting the PSI, and this AS shall create and send immediate messages addressed to a group member of the group identified by the PSI.

- The user can send an immediate message by indicating the individual addresses (Public User Identities for IMS recipients) of the intended recipients as part of the immediate message. The AS of the user shall then create and send immediate messages addressed to each one of the intended recipients.

5.16.2 Session-based Messaging

5.16.2.0 General

This subclause describes architectural concepts and procedures for 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 sub-clause. These procedures shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by TS 26.141 [37]

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 signaling flow is based on the general flow shown in chapter 5.7a of this specification.

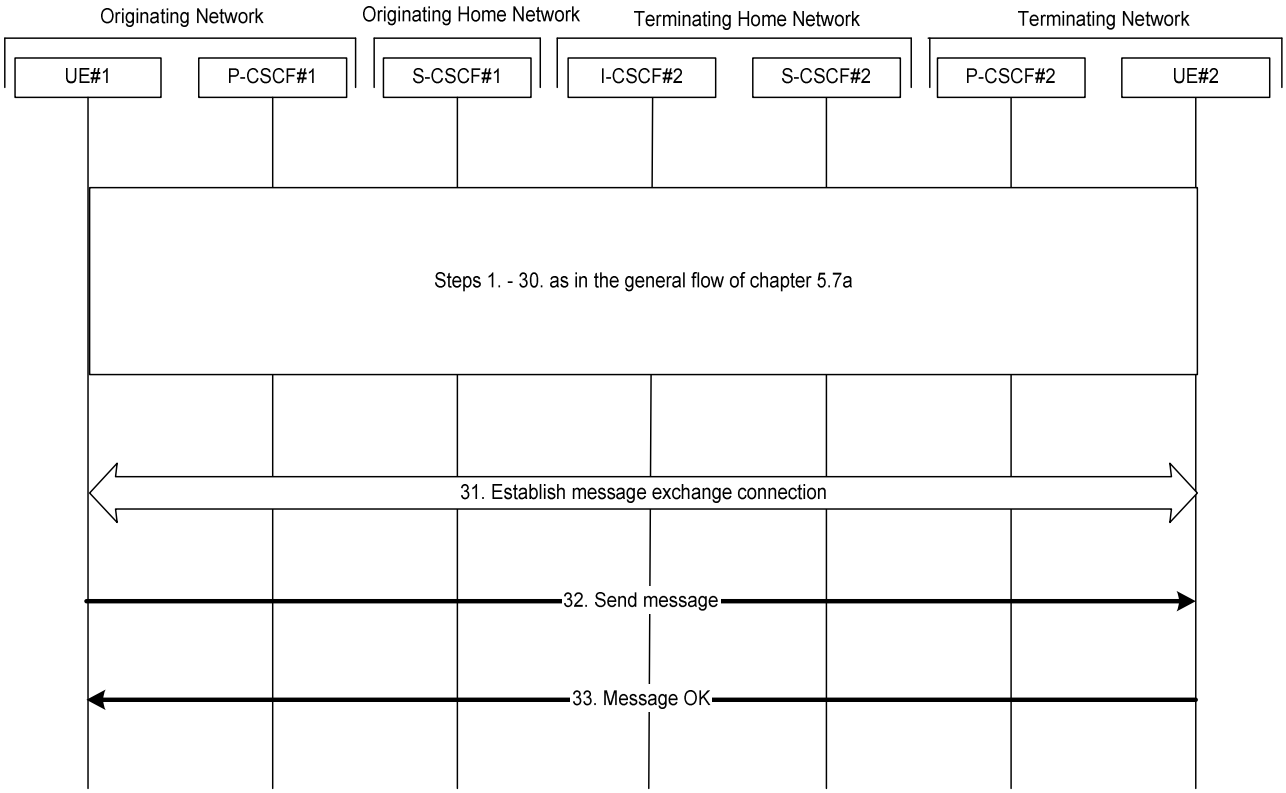


Figure 5.48a: Message session establishment

1-30. These steps are identical to the steps 1 to 30 in the flow of chapter 5.7a. After that the message session is established. For session based messaging the SDP offer in the first INVITE request may indicate the maximum message size UE#1 accepts to receive and the 200 OK (Offer response) to the INVITE request may indicate the maximum message size UE#2 accepts to receive.

31. UE#1 establishes a reliable end-to-end connection with UE#2 to exchange the message media.

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

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

Further messages may be exchanged in either direction between UE#1 and UE#2 using the established connection. The size of the messages exchanged within the session shall be within the size limits indicated by UE#1 and UE#2 respectively.

5.16.2.2.2 Session based messaging procedure using multiple UEs

Session based messaging between more than two UEs require the establishment of a session based messaging conference.

Within session based messaging conferences including multiple UEs (e.g. multiparty chat conferences) an MRFC/MRFP or an IMS AS shall be used to control the media resources.

When MRFC/MRFP are used, then conferencing principles are used to provide the chat service:

- MRFP must be able to establish message connections with all involved parties.
- MRFC/MRFP must be able to receive messages from conference participants and to distribute messages to all or some of the participants.
- In order to enable the UE managing information related to the session based messaging conference the MRFC may be co-located with an IMS AS.
- MRFC/MRFP roles and interactions with an AS are described in more detail in chapters 4.7 and 5.14.1 and 5.14.2.
- The interface for session based messaging between MRFC and MRFP is not standardised in this release. When an AS is used, then the IMS service control architecture is used to provide the chat service. Both signalling and user plane are then supported by the AS. For more details, see section 4.2.

The following flow shows the originating session based messaging set up using an intermediate server for a chat service. In this case the intermediate chat server is addressed by the UE#1 using a PSI. It is assumed that UE#1 is the first UE entering the chat session.

NOTE: Interactions between MRFC and MRFP are not shown in the flows below since these interactions are not standardized. An optional ringing response from MRFC/AS to the UE is not shown in the following procedure.

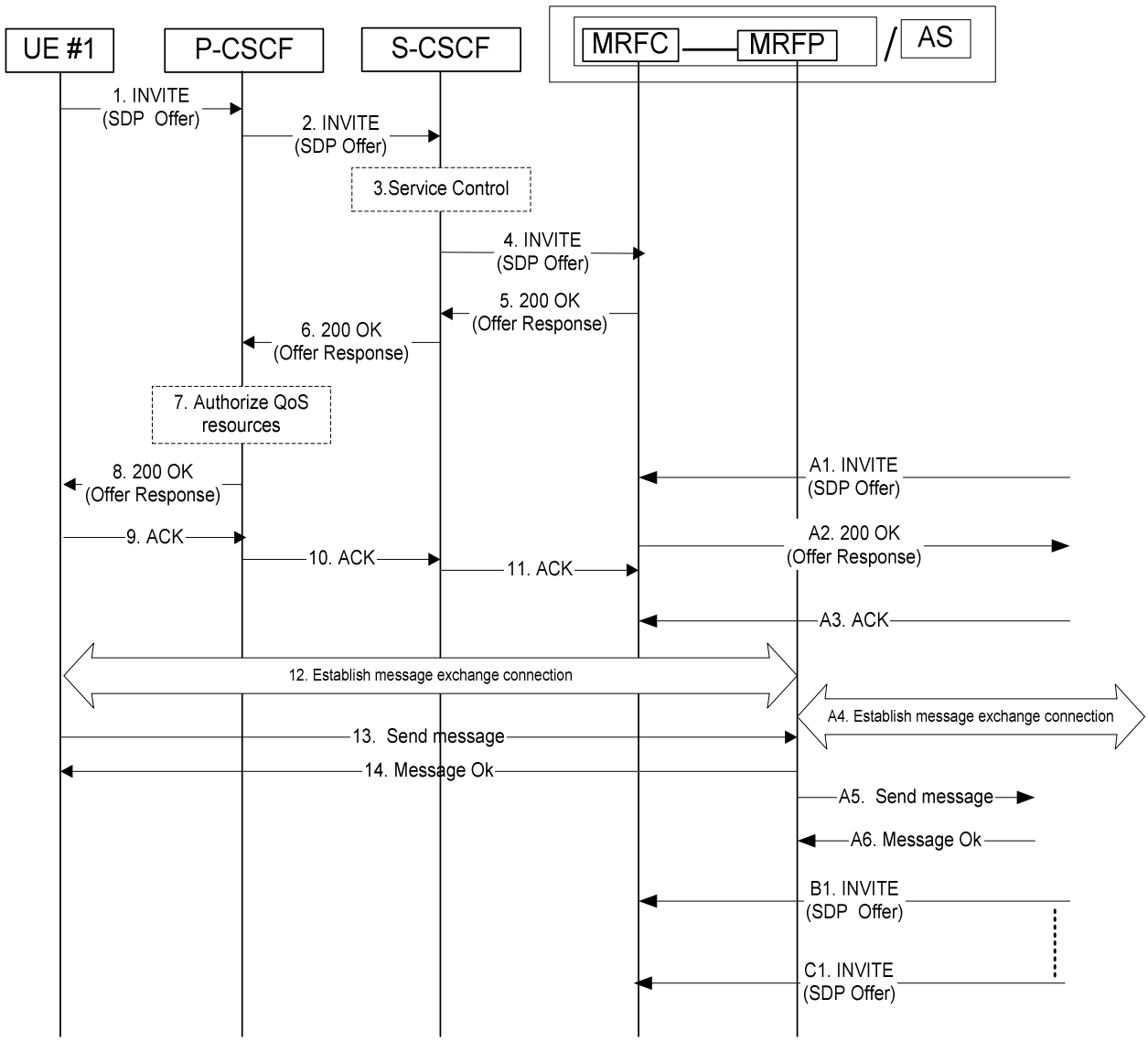


Figure 5.48b: Session based messaging using a chat server

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/PCRF may 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.

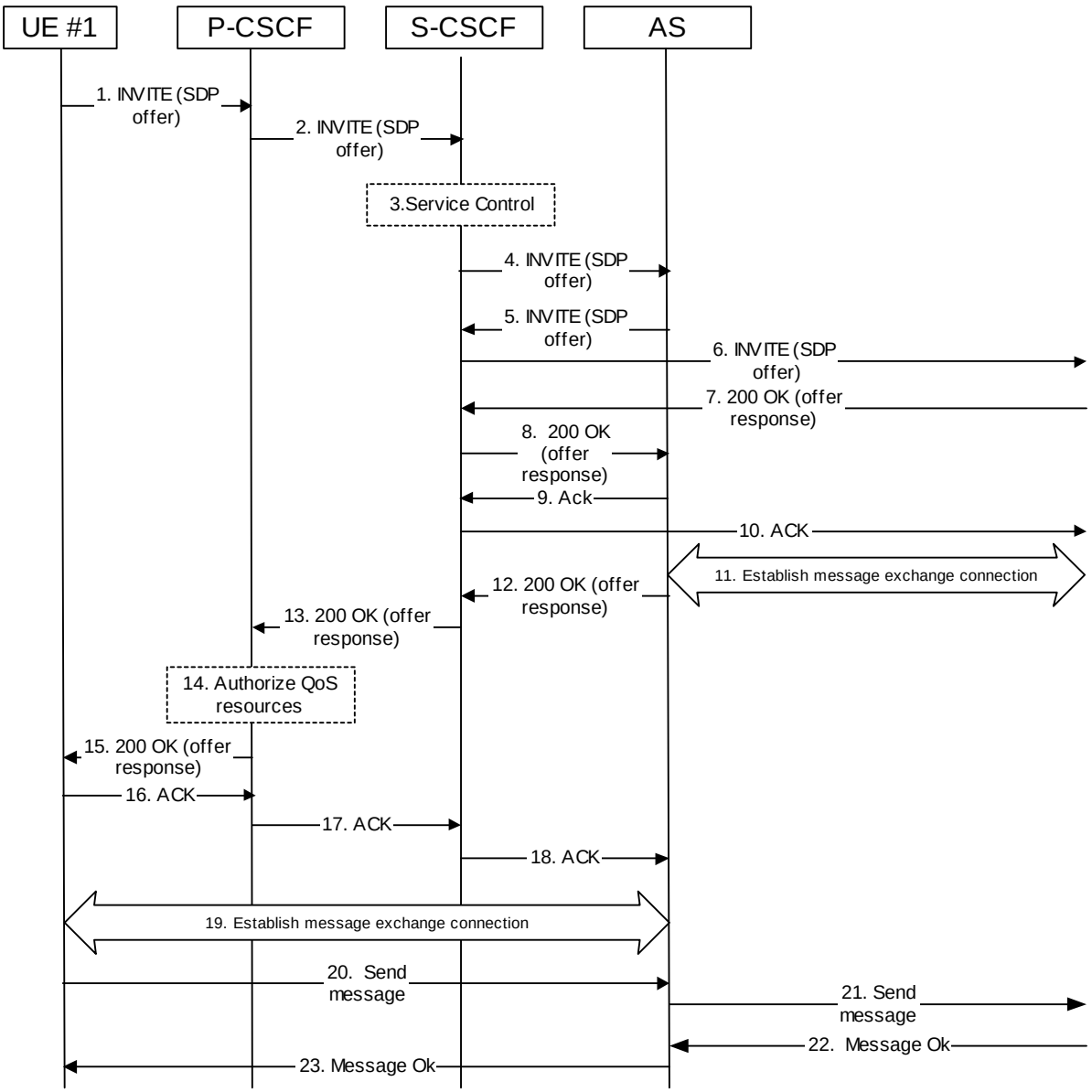


Figure 5.48c: Session based messaging with an intermediate node

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/PCRF may 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.

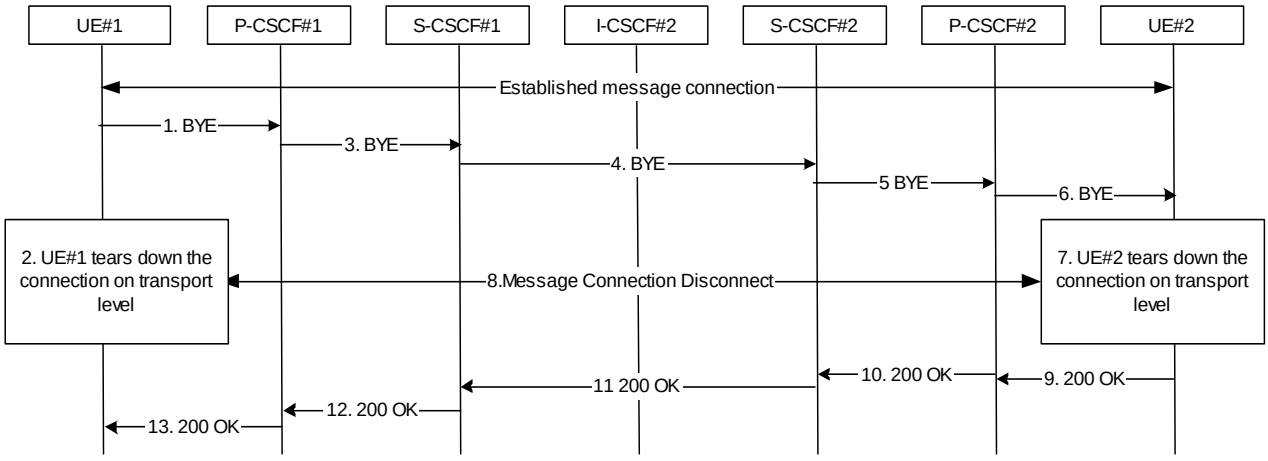


Figure 5.48d: Message session release procedure

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.

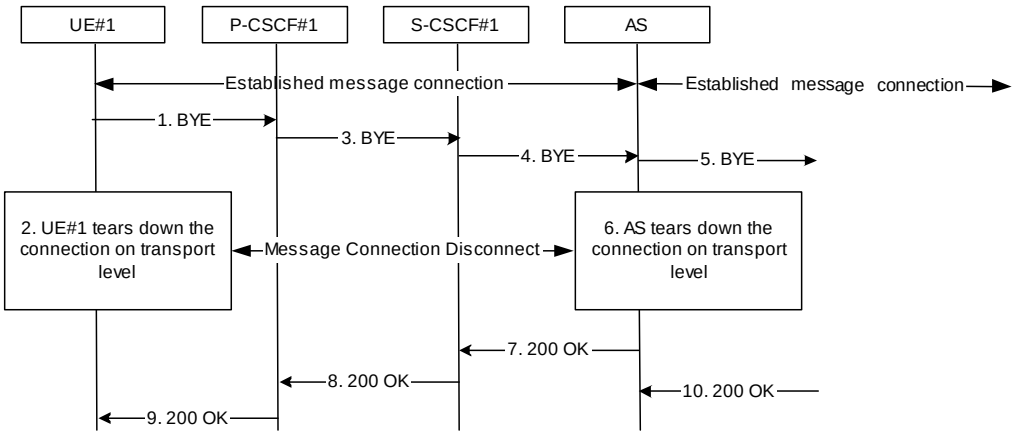


Figure 5.48e: Message session release procedure with intermediate node

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 sub-clause 5.10.3. Whether the session refresh mechanism is used for a particular session is negotiated between the endpoints of the session upon session initiation.

IMS entities acting as User Agents as defined in 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

This section 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.

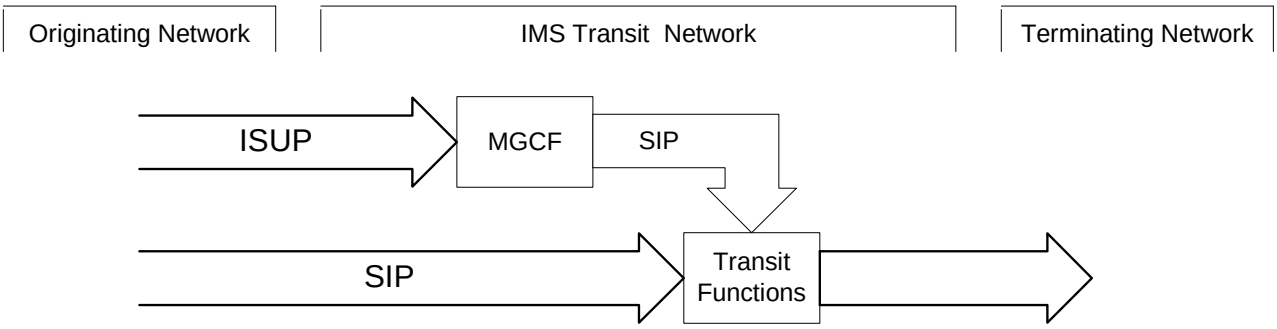


Figure 5.49: IMS transit network

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 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".

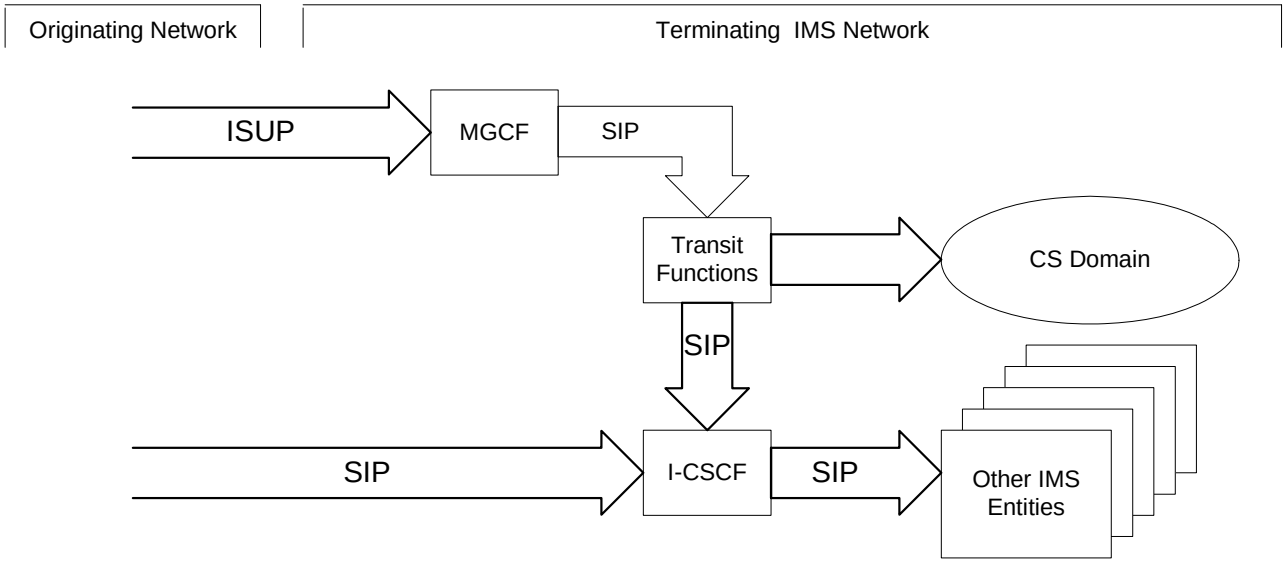


Figure 5.50: Terminating IMS network with transit support

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. Since this operator is serving its own customers, it 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. In this case, there may be an additional delay for terminating sessions destined for IMS subscribers.

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. In this case there may be an additional delay for terminating sessions destined for the CS domain subscribers.

It is the operator's choice to determine which way to route the SIP messages, first through IMS Transit Functions or directly to an I-CSCF. This may depend on whether the majority of the customers, whose calls terminate on the MGCF, are IMS or CS domain subscribers.

NOTE 2: 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 configuration where all traffic from the MGCF is routed directly to the I-CSCF, the I-CSCF then needs to support the transit functionality as described above.

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 draft-ietf-sip-gruu-10 [49] and draft-ietf-sip-outbound-04 [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 draft-ietf-sipping-gruu-reg-event-06 [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 orginations, 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 requrest 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.

Annex A (Informative): Information flow template

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

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

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

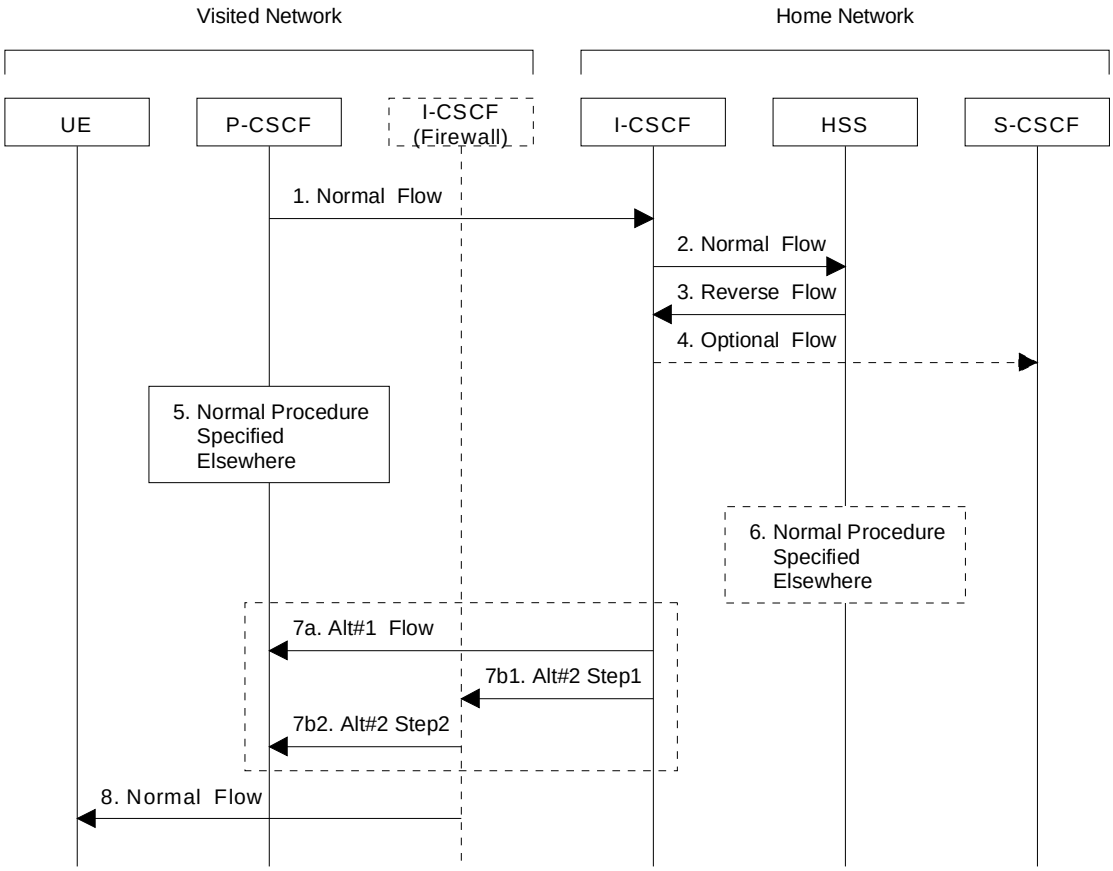


Figure A.1: Information Flow Template

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

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

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

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

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

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

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

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

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

   7b. Alternative (b) is described.

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

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

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

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

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

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

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

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

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

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

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

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

- Sequential operation is assumed unless indicated otherwise.

Annex B (Informative):
Void

Annex C:
Void

Annex D:
Void

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

E.0 General

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

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

E.1 Mobility related concepts

E.1.0 General

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

If an UE changes its IP address due to changes triggered by the GPRS/UMTS procedures or according to 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, e.g. establishing an additional IP-CAN bearer through GPRS while the UE is IMS registered over I-WLAN, 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.

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

E.1.1 Procedures for P-CSCF discovery

E.1.1.0 General

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

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

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

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

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

E.1.1.1 GPRS procedure for P-CSCF discovery

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

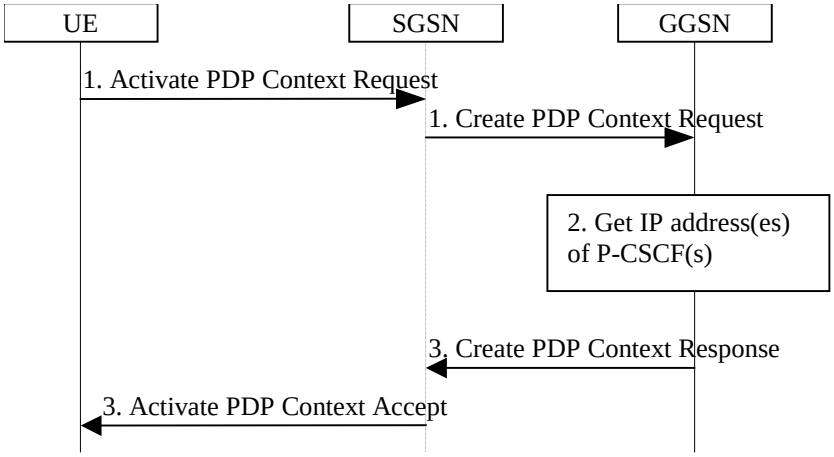


Figure E.1: P-CSCF discovery using PDP Context Activation signalling

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

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

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

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

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

E.2 QoS related concepts

E.2.1 Application Level Signalling for IMS

E.2.1.0 General

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

E.2.1.1 QoS Requirements for Application Level Signalling

It shall be possible to request prioritised handling over the radio for IM Subsystem related signalling by including the Signalling Indication in the QoS IE of the PDP Context to be used for this traffic as described in subclause E.2.1a.1.

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.

A dedicated signalling PDP context 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 by the operator of the GGSN.

If the Bearer Control Mode for the IP-CAN session is 'NW_Only', then the GGSN may provide a set of UL filters for the PDP context used for IM CN Subsystem Signalling. The UL filters provide the UE with the rules and restrictions applied by the GGSN for the dedicated IM Subsystem signalling IP-CAN bearer. The GGSN may in addition provide the IM CN subsystem signalling flag to explicitly indicate to the UE the intention of using the PDP context for IM Subsystem related signalling.

Policy and Charging Control functionality can be used to provide additional charging capabilities for dedicated signalling PDP context used for IMS signalling (as well as for a general-purpose PDP context) as described in section 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.

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, 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 IE in PDP context activation procedure. This indicates to the network (radio & core) the requirement of using the PDP context 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).

- Include the IM CN Subsystem Signalling Flag in the PCO IE in the PDP context activation procedure. This indicates to the GPRS network the requirement of using PDP context for application level signalling with restricted handling as described in sub clause E.2.1.2, after it has been negotiated with the networks.

- Utilize a general purpose PDP Context with a negotiated QoS profile (this includes the possibility of having the Signalling Indication in the QoS IE).

The IM CN Subsystem signalling flag is used to reference rules and restrictions on the PDP context used for application level signalling, as described in section E.2.2.

The Signalling Indication in QoS IE provides prioritised handling over the radio interface and is detailed in TS 23.107 [55] and subclause E.2.1a.1.

Depending on the operator's policy, one or more of the above combinations may be allowed in the GPRS network.

E.2.1a PDP context procedures for IMS

E.2.1a.1 Establishing PDP Context for IM CN Subsystem Related Signalling

It shall be possible for the UE to convey to the network the intention of using the PDP context for IM Subsystem related signalling. For this purpose it uses the mechanism described in this subclause 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 by the UE, in order to establish a PDP context for IM Subsystem related signalling, the UE shall be able to include the IM CN subsystem signalling flag in the PDP context activation procedure. This indicates to the network the intention of using the PDP context for IM Subsystem related signalling.

An IM CN Subsystem signalling flag determines any rules and restrictions that shall apply at the GGSN for that PDP context, these rules and restrictions are described in section 4.2.6. It shall not be possible to modify a general purpose PDP context into a dedicated PDP context for IM Subsystem related signalling and vice versa.

To establish a PDP context for IM 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. 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 [19].

The IM CN Signalling Flag in the PCO IE is used to reference rules and restrictions on the PDP context used for application level signalling, as described in subclause 4.2.6. Based on operator policy the "Signalling Indication" in the QoS IE 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 may be used independently of each other.

E.2.1a.2 Deletion of PDP Context used to transport IMS SIP signalling

In case 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].

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

1. QoS Signalling at Different Bearer Service Control Levels

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

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

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

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

      The QoS signalling at the UMTS BS Level is to deliver the QoS requirements from the UE (received from the GGSN in case of Bearer Control Mode being 'NW_Only') to the RAN, the CN, and the IP BS manager, where appropriate QoS negotiation and resource allocation are activated accordingly. When

UMTS QoS negotiation mechanisms are used to negotiate end-to-end QoS, the translation function in the GGSN shall co-ordinate resource allocation between UMTS BS Manager and the IP BS Manager.

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

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

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

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

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.

E.2.3 Interaction between GPRS QoS and session signaling

E.2.3.0 General

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

This clause describes the GPRS-access-specific concepts.

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

For the GPRS 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 roaming agreements. The establishment of the PDP context bearer shall use the PDP context activation procedure specified in TS 23.060 [23].

For the GPRS with Policy and Charging Control case, policy decisions (e.g., authorisation and control) are also applied to the bearer.

The GGSN 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. 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 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-Initiated PDP Context Modification respectively as defined in TS 23.060 [23].

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

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

E.2.4.0 General

In the event of loss of coverage, TS 23.060 [23] defines the Iu or RAB Release procedures. In case of PDP context with streaming or conversational class the maximum bitrate of the GTP tunnel between SGSN and GGSN is modified to 0 kbit/s in up- and downlink direction. This is indicated to the P-CSCF/PCRF by performing an IP-CAN session modification procedure (see TS 23.203 [54]) as shown in Figure E.2. This procedure also applies to PDP Contexts used for IMS SIP Signalling transport. For loss of coverage in case of other PDP contexts (background or interactive traffic class), the PDP context is preserved with no modifications and therefore no indication to the P-CSCF/PCRF.

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

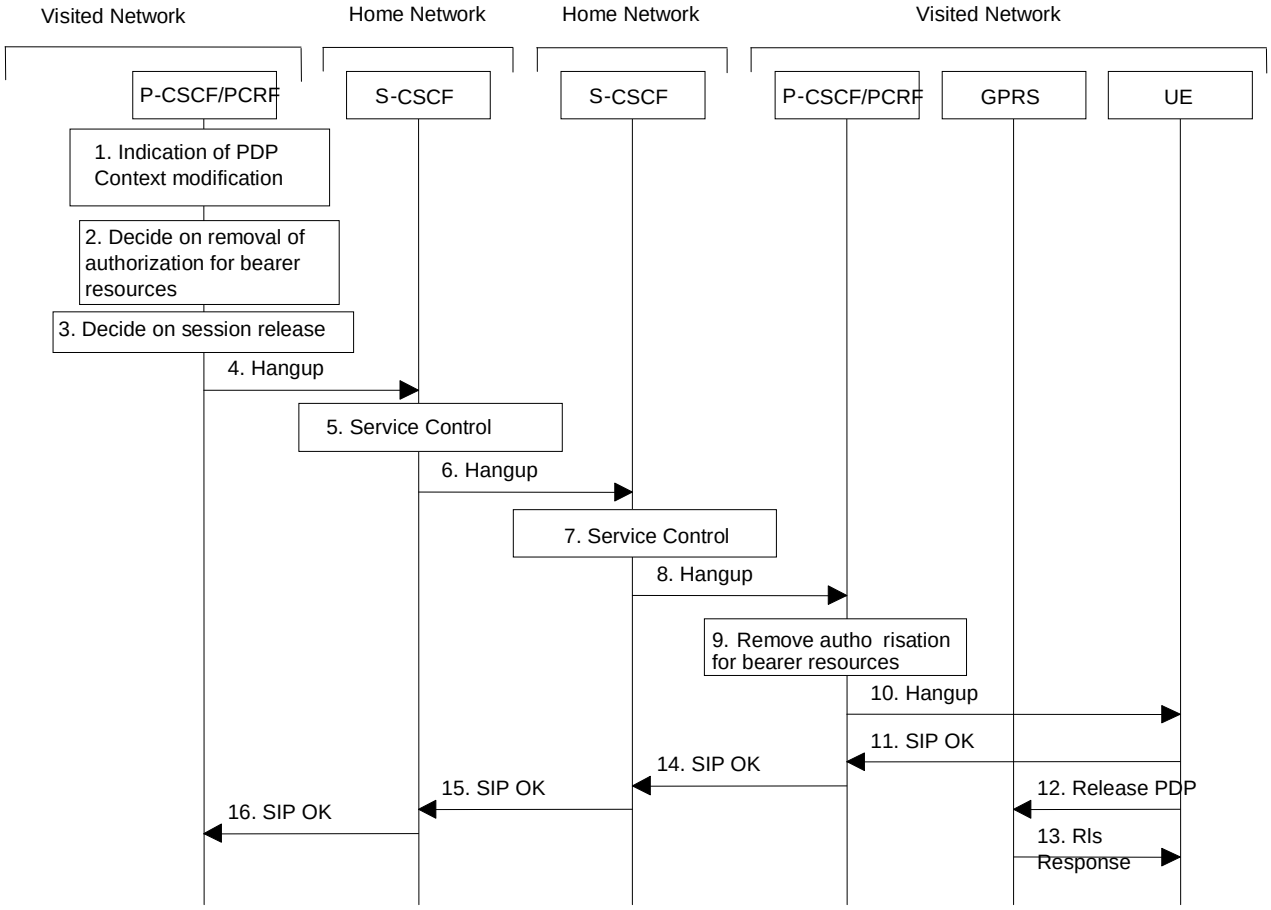


Figure E.2: Network initiated session release - P-CSCF initiated after loss of radio coverage

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

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 authorisation 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 authorisation for resources that had previously been issued for this endpoint for this session. (see TS 23.203 [54]).

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

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].

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

- A Temporary Public User identity shall be derived from the USIM's IMSI, and shall be used in SIP registration procedures. The Temporary public user identity shall take the form of a SIP URI (as defined in IETF RFC 3261 [12] and IETF RFC 2396 [13]). 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 Identity is used, the user can not initiate any sessions until the implicitly registered public identities are available in the UE.

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

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

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

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. For communication with the IMS, the UE establishes an IPv6 PDP context. Termination of this PDP context will normally trigger de-registration of IMS application first. Hence, the PDP context 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 of maintaining the IP connectivity over GPRS by maintaining the PDP contexts.

A user may be connected either to a home GGSN or a visited GGSN depending on the configuration as specified in TS 23.221 [7].

E.6 Usage of NAT in GPRS

There should be no NAT (or its existence should be kept transparent towards the UE) located between the GGSN and the P-CSCF, which is possible as they are located within the same network (see TS 23.221 [7]).

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.

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

This annex provides some background information related to subclause 5.4.5.3.

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

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

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

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

- 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 signaling 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 subclause 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.

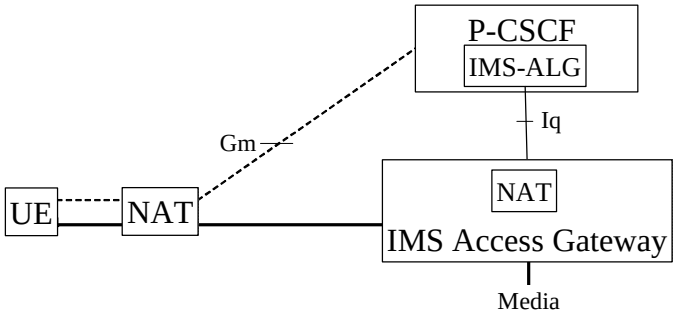


Figure G.1: Reference model for IMS access when both the signalling and media traverses NAT

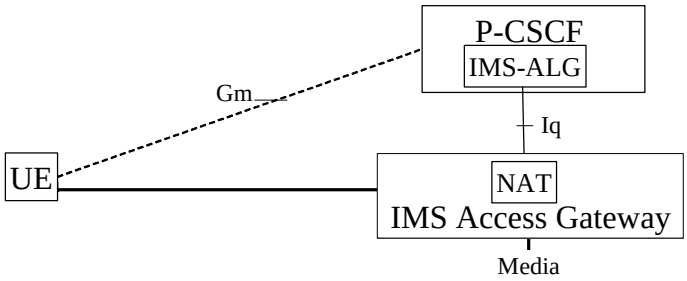


Figure G.2: Reference model for IMS access when NAT is needed between the IP-CAN and the IMS domain

Editor's note: It is for further study if the Iq reference point can be merged with the Rx+ reference point. If they are not merged then the IMS Access Gateway may be a TrGW and the Iq may be equivalent to the Ix reference point.

G.2.2 ICE and Outbound reference model

Figure G.2a presents the general reference model for IMS access when both the signaling and media traverses NAT devices. Functional elements with dashed lines represent optional functionality. The transport of the Gm signaling is also subject to the policy enforcement.

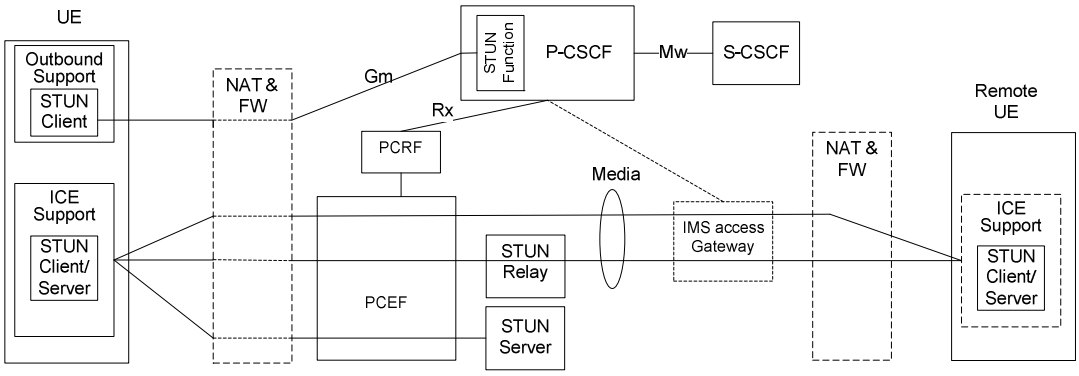


Figure G.2a: Reference model for ICE and Outbound Methodology

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 IPCAN use the same IP version and where they use different IP versions.

Further functions of the P-CSCF/IMS-ALG, e.g. to request to open and close gates on the IMS Access Gateway, are not defined in this version of the specification.

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 IPCAN use the same IP version and where they use different IP versions.

Further functions of the IMS Access Gateway, e.g. to open and close gates (pinholing), are for further study.

G.3.3 Iq reference point

The Iq reference point is between the P-CSCF and the IMS Access Gateway. It conveys the necessary information that is needed to allocate and release transport addresses.

Editor's note: It is for further study if the function of this reference point can be merged with the Rx+, or it is equivalent to the Ix.

G.4 Procedures for employing the IMS-ALG and IMS Access Gateway

Editor's note: The purpose of this clause is to define the procedures needed for NAT traversal. During the specification of this clause it shall be checked if these procedures matches the Rx+ procedures and make the decision about merging the reference points based on the result.

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.

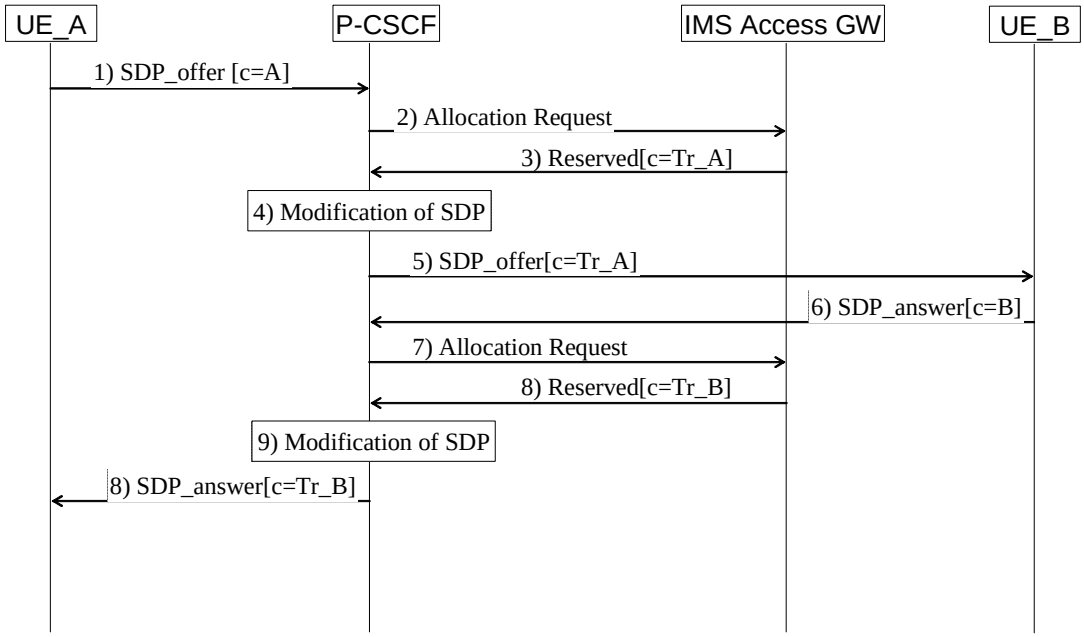


Figure G.3: Session establishment procedure with NAT traversal

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 wrt 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 section presents the media forwarding performed by the IMS Access Gateway. The behaviour presented in this clause is valid in both directions.

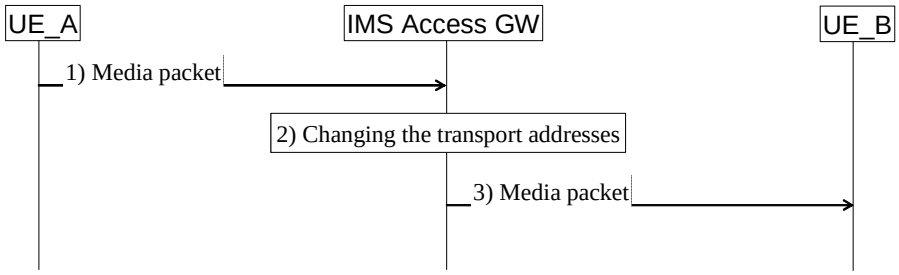


Figure G.5: Packet forwarding in the IMS Access Gateway

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) draft-ietf-mmusic-ice [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 draft-ietf-behave-turn [46] and its use is detailed in draft-ietf-mmusic-ice [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 draft-ietf-behave-rfc3489bis [47] and its use is detailed in draft-ietf-mmusic-ice [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

Managing Client Initiated Connections in the Session Initiation Protocol (outbound) draft-ietf-sip-outbound [48] defines a methodology for signaling 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 signaling, 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 draft-ietf-behave-rfc3489bis [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 signaling packets from the same port on which it expects to receive signaling 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 signaling 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 signaling packets from the same port on which it expects to receive signaling packets;

- Establishment of signaling 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: In case 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 sub-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.

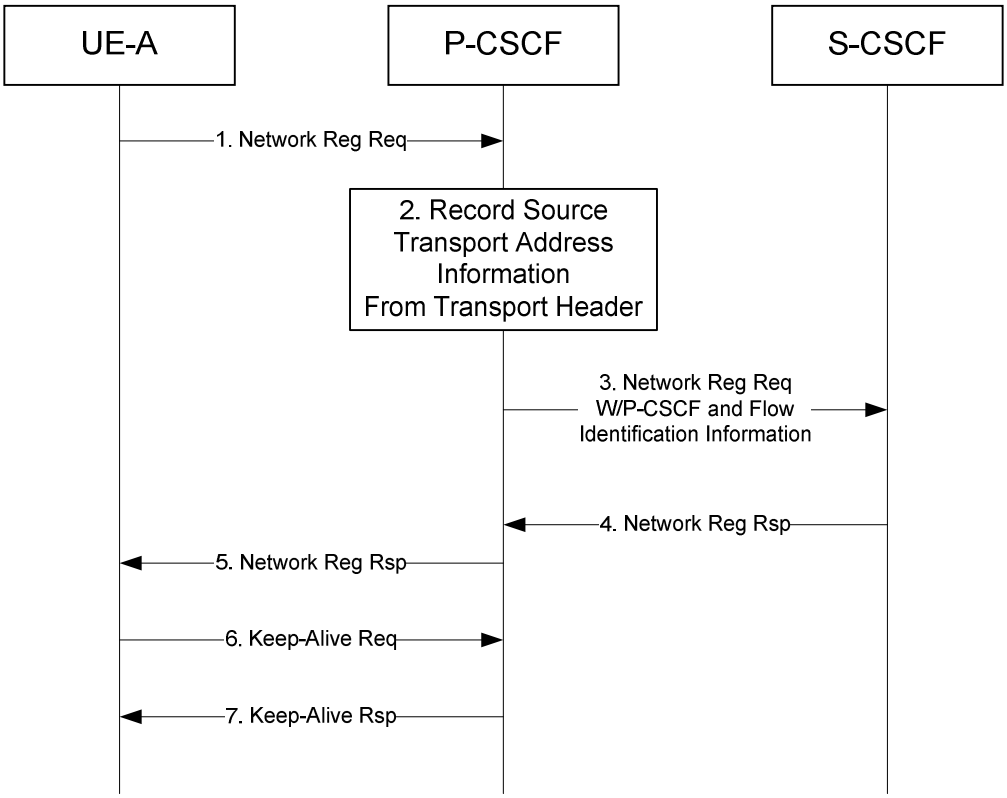


Figure G.7: Flow Establishment Procedures for Outbound

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.

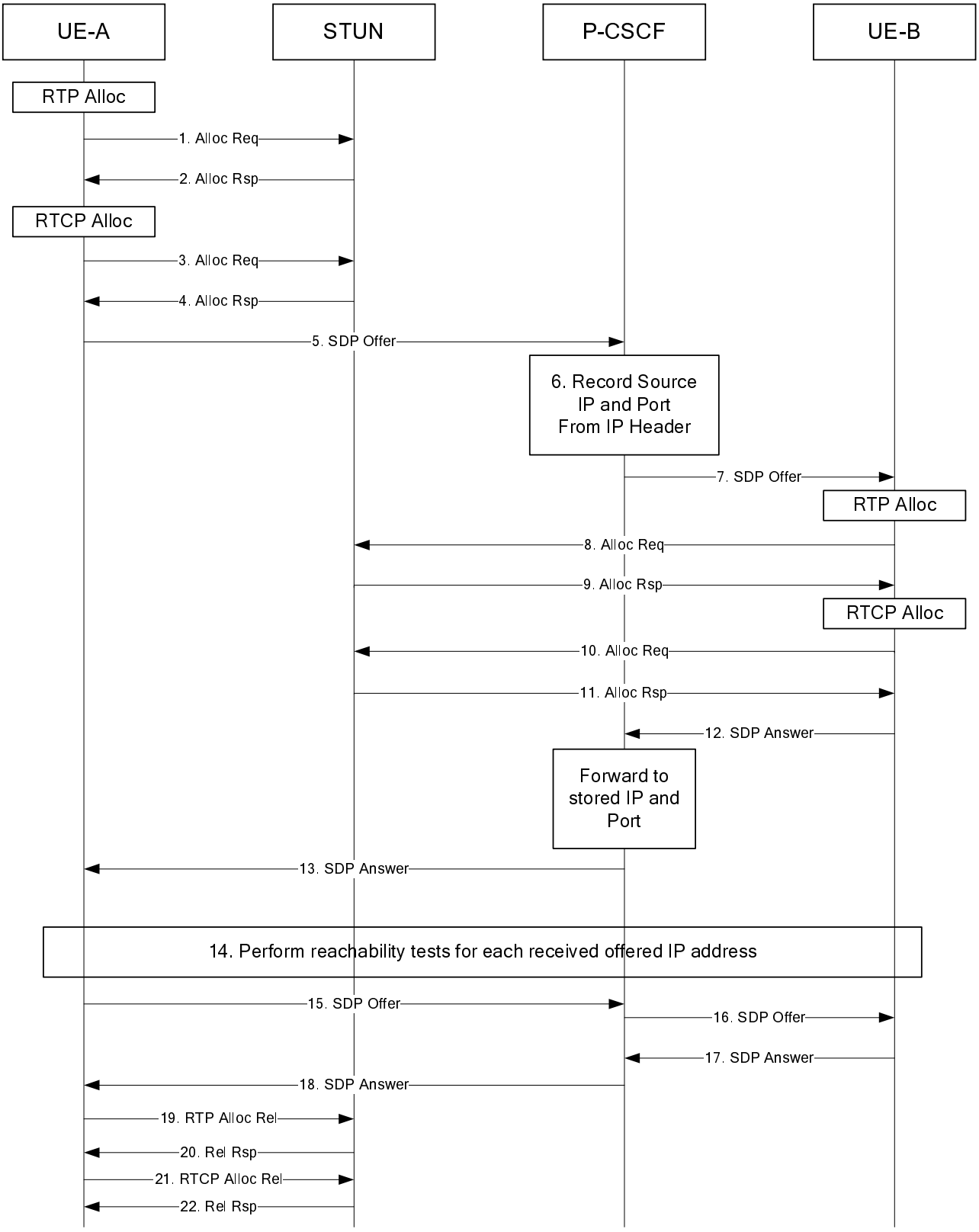


Figure G.8: Session Establishment procedure for NAT Traversal using ICE and Outbound

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 Section 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 [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.

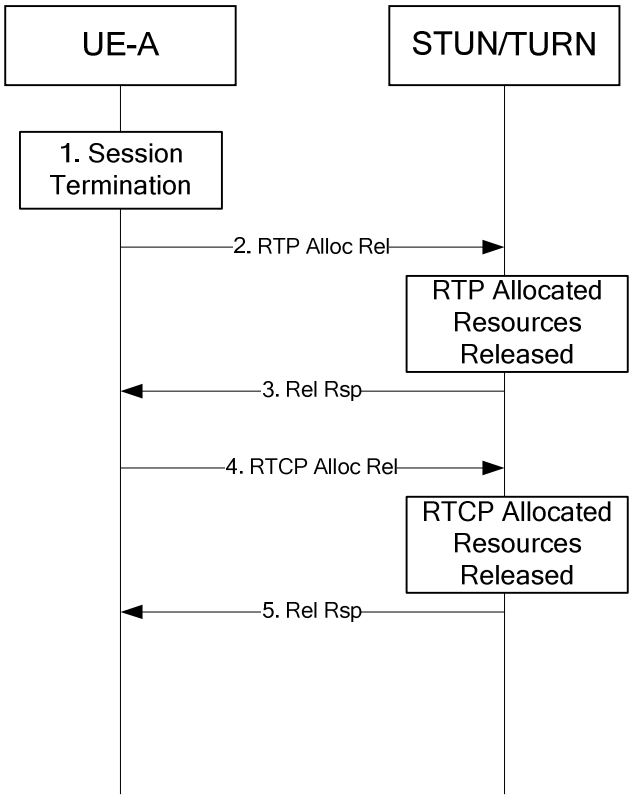


Figure G.9: Session Release Procedure with STUN Relay Resources

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 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, draft-ietf-mmusic-ice [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 section 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.

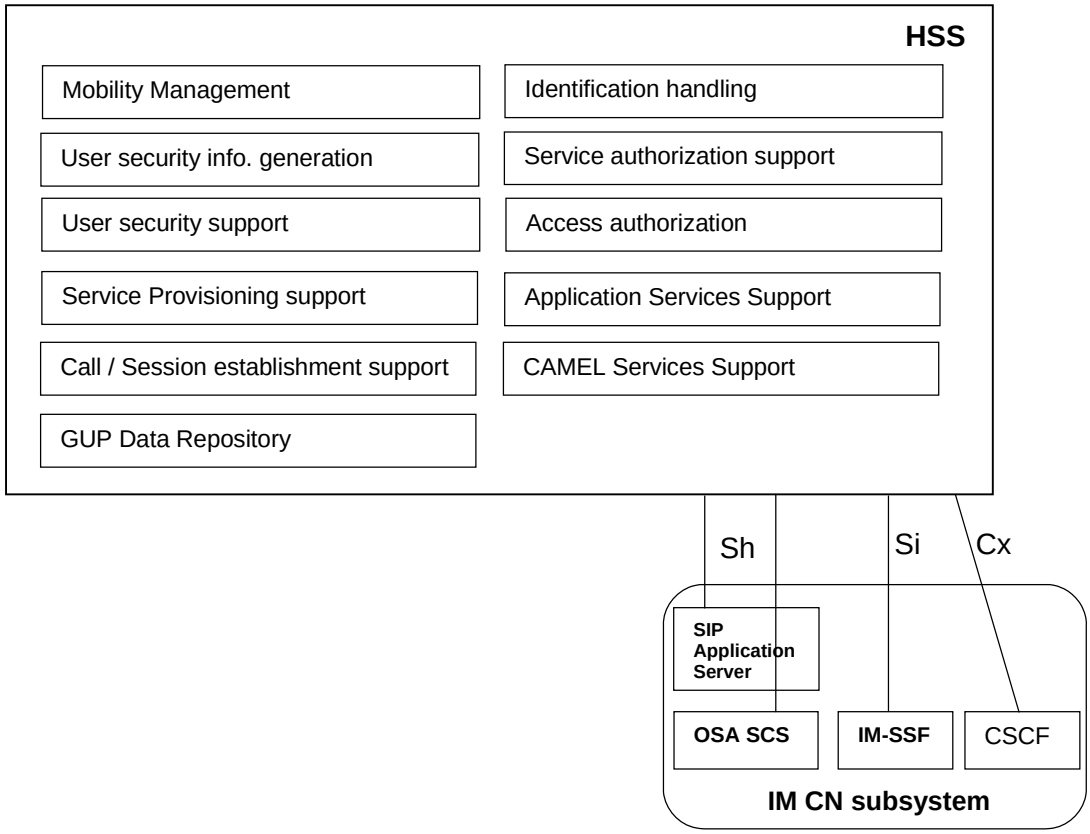


Figure H.1: HSS functional decomposition

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 onoperator configuration.

I.2 Overall architecture

Figure I.1 presents a high-level architecture diagram showing how Border Control Functions fit into the IMS architecture.

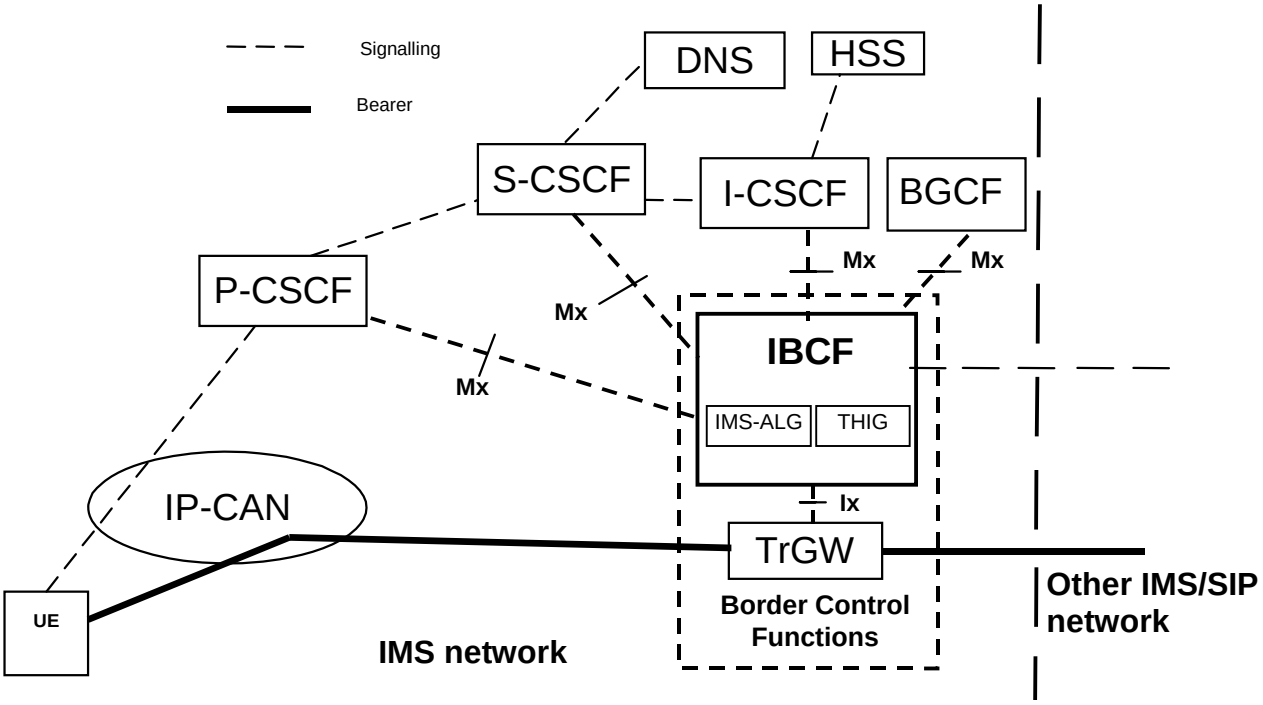


Figure I.1: Border Control Functions

NOTE: The standardisation and functional requirements of Ix reference point are FFS.

The Mx reference point allows S-CSCF/I-CSCF/P-CSCF to communicate with an IBCF in order to provide border control functions. The Mx & Ix reference points are not specified within this release of the specification.

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.

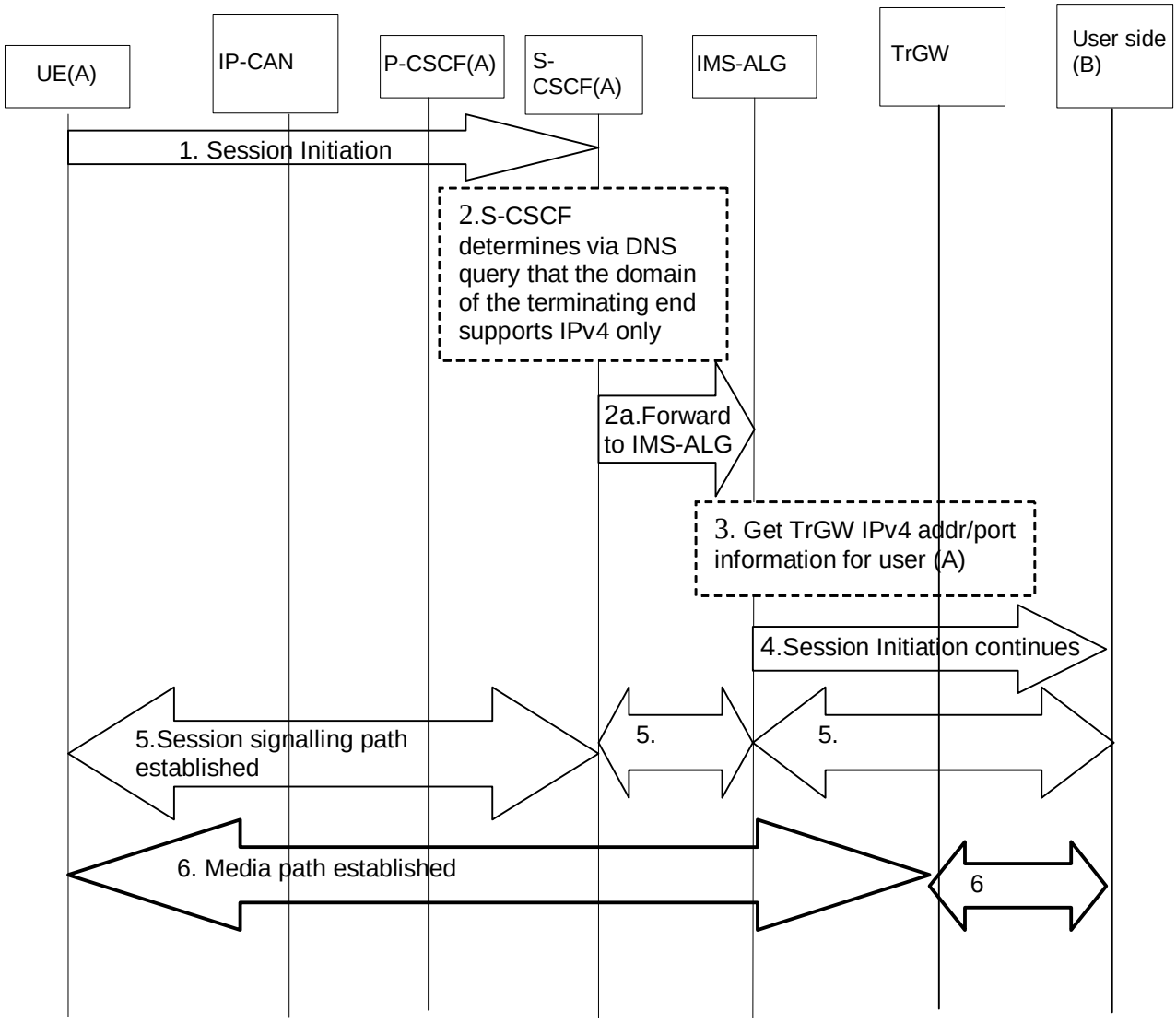


Figure I.2: Originating IMS session towards an IPv4 end point

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.

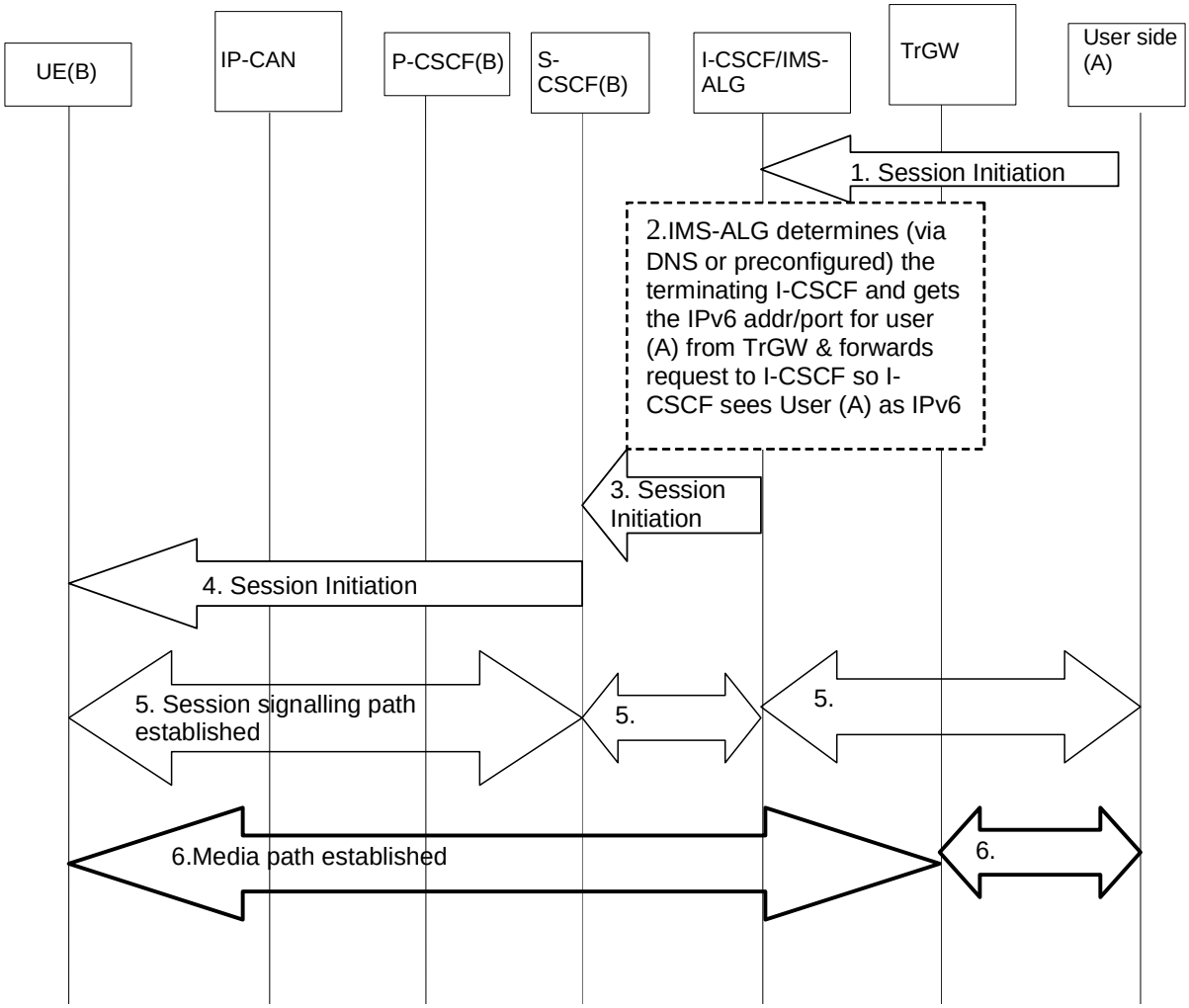


Figure I.3: Terminating IPv4 SIP session towards an IPv6 IMS user

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].

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.

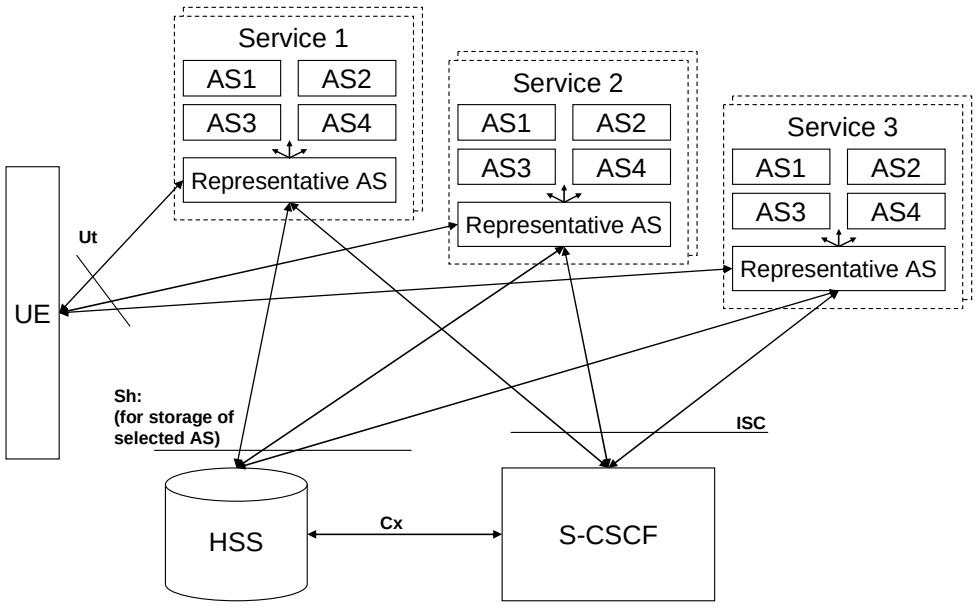


Figure J.2.1: Dynamic User Allocation using Representative AS

J.2.2 Procedures related to Representative AS

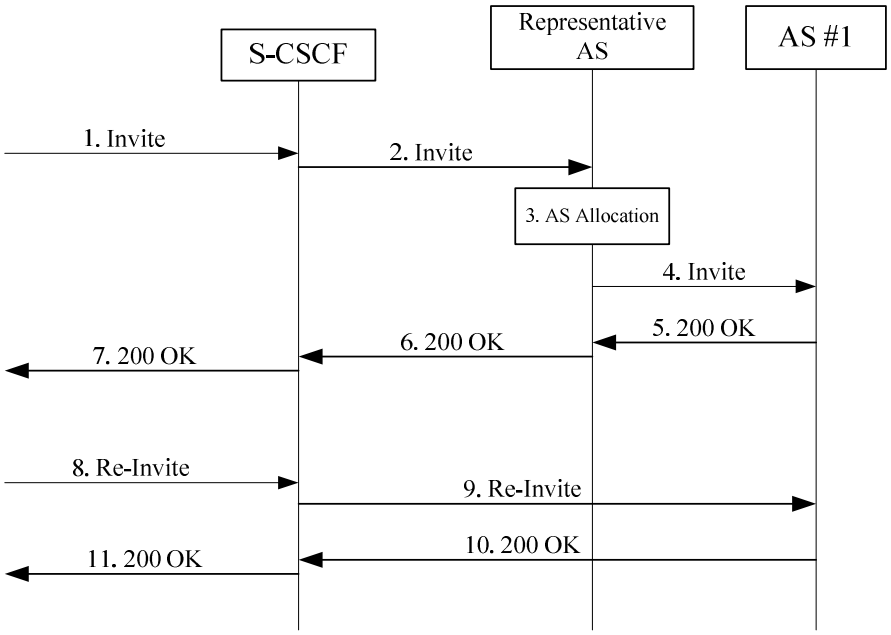


Figure J.2.2: Bypassing Representative AS procedure

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 forwared 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:

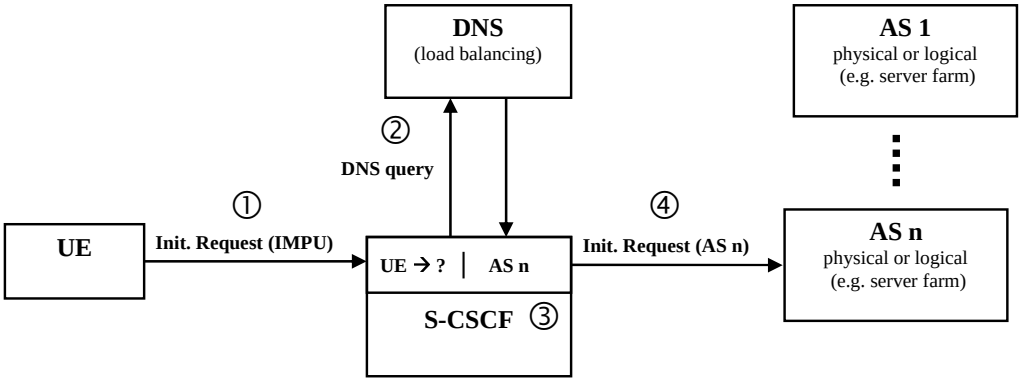


Figure J.3.2.1: Assignment of AS via DNS query during first service request

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:

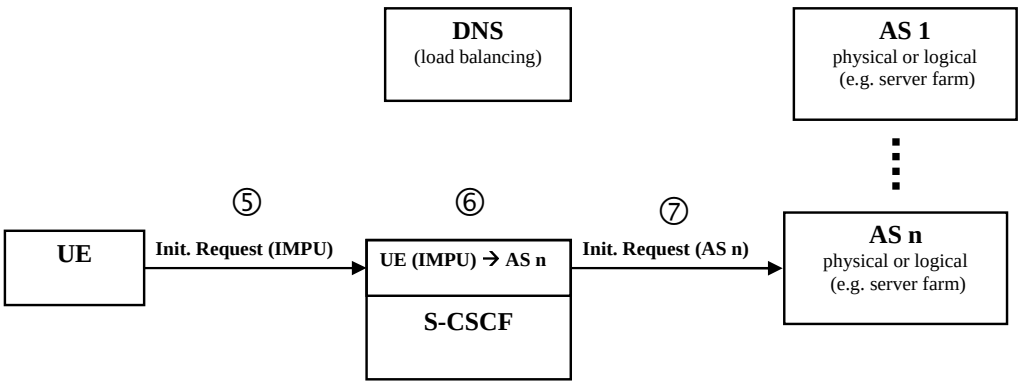


Figure J.3.2.2: S-CSCF has stored assigned AS for following service requests

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.

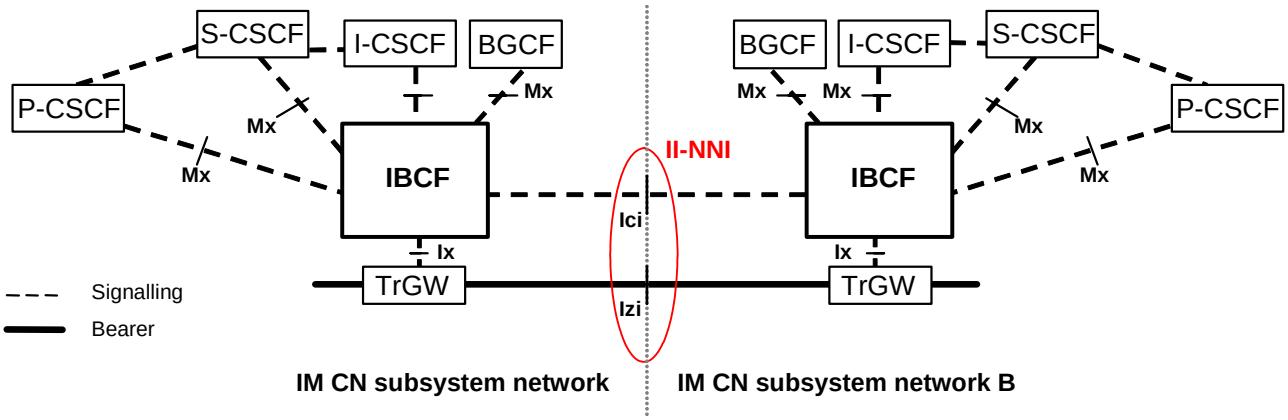


Figure K.1: Inter-IMS Network to Network Interface between two IM CN subsystem networks

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 (informative): Change history

Date	TSG #	TSG Doc.	CR#	Rev	Cat	Subject/Comment	In	Out
2003-01	SA#18	SP-020776	242	1		Cleaning up of IMS emergency session requirement	5.7.0	6.0.0
2003-01						Editorial to correct cover page to indicate Rel-6 not Rel-5	6.0.0	6.0.1
2003-03	SA#19	SP-030121	259	1		Subscribed Media	6.0.1	6.1.0
2003-03	SA#19	SP-030121	255	3		Public Service Identity	6.0.1	6.1.0
2003-03	SA#19	SP-030121	260	2		Architectural requirements to provide IMS emergency sessions	6.0.1	6.1.0
2003-03	SA#19	SP-030121	266	1		Clarification on user registration in TS 23.228	6.0.1	6.1.0
2003-03	SA#19	SP-030121	277	1		Public Service Identity Routing	6.0.1	6.1.0
2003-03	SA#19	SP-030121	278	1		Forking capabilities of IMS	6.0.1	6.1.0
2003-03	SA#19	SP-030121	275	1		Capability to route non-SIP URIs	6.0.1	6.1.0
2003-03	SA#19	SP-030121	281	1		Public Service Identity requirement	6.0.1	6.1.0
2003-03	SA#19	SP-030121	261	3		Procedures to detect and route IMS Emergency Sessions	6.0.1	6.1.0
2003-03	SA#19	SP-030181	280	3		Combined CR for CR#264 and CR#280rev1	6.0.1	6.1.0
2003-06	SA#20	SP-030303	297	3		AS use of the MRFC	6.1.0	6.2.0
2003-06	SA#20	SP-030303	314	1		Barring and roaming restrictions	6.1.0	6.2.0
2003-06	SA#20	SP-030303	295	1		Capability to route non-SIP URIs	6.1.0	6.2.0
2003-06	SA#20	SP-030303	302	1		Clarifications on multiple registrations	6.1.0	6.2.0
2003-06	SA#20	SP-030303	288	-		Corrections and Clean-Up after Re-organisation of TS 23.228	6.1.0	6.2.0
2003-06	SA#20	SP-030303	305	2		Data Format at Sh Reference Point	6.1.0	6.2.0
2003-06	SA#20	SP-030303	291	4		Enhancements for Messaging	6.1.0	6.2.0
2003-06	SA#20	SP-030303	287	2		Format of Public Service Identities	6.1.0	6.2.0
2003-06	SA#20	SP-030303	301	1		Guidelines for the UE to apply IPv6 privacy mechanism in conjunction with IMS	6.1.0	6.2.0
2003-06	SA#20	SP-030303	272	5		GUP for IMS Subscription Management	6.1.0	6.2.0
2003-06	SA#20	SP-030303	293	2		Handling of IMS signalling information in QoS and PCO IEs at GGSN	6.1.0	6.2.0
2003-06	SA#20	SP-030303	318	2		Implicit Registration with multiple Service Profiles	6.1.0	6.2.0
2003-06	SA#20	SP-030303	299	1		IMS corrections	6.1.0	6.2.0
2003-06	SA#20	SP-030303	286	3		IMS Group Management	6.1.0	6.2.0
2003-06	SA#20	SP-030303	284	2		Refreshing sessions	6.1.0	6.2.0
2003-06	SA#20	SP-030303	306	1		Public Service Identities Definition	6.1.0	6.2.0
2003-06	SA#20	SP-030303	311	1		S-CSCF requirements at registration	6.1.0	6.2.0
2003-06	SA#20	SP-030303	296	3		SLF on Sh interface	6.1.0	6.2.0
2003-06	-	-	-	-		Editorial change to move Annex E to correct position in document (MCC)	6.1.0	6.2.0
2003-09	SA#21	SP-030538	336r2	2		IMS-SIP interworking	6.2.0	6.3.0
2003-09	SA#21	SP-030380	329r1	1		IMS corrections	6.2.0	6.3.0
2003-09	SA#21	SP-030380	347r3	3		UE in a visited Network with a P-CSCF located in the Home network	6.2.0	6.3.0
2003-09	SA#21	SP-030380	349	-		Correction to Network initiated session release	6.2.0	6.3.0
2003-09	SA#21	SP-030380	320	1		Immediate IMS Messaging to multiple recipients	6.2.0	6.3.0
2003-09	SA#21	SP-030380	321	1		Some service aspects of IMS messaging	6.2.0	6.3.0
2003-09	SA#21	SP-030380	322	1		Session-based IMS messaging	6.2.0	6.3.0
2003-09	SA#21	SP-030380	324	1		Mobile-initiated Hold and Resume of a Mobile-PSTN Session	6.2.0	6.3.0
2003-09	SA#21	SP-030380	325	1		Subscription to information changes in e.g. AS or S-CSCF	6.2.0	6.3.0
2003-09	SA#21	SP-030380	326	1		Refreshing sessions	6.2.0	6.3.0
2003-09	SA#21	SP-030380	331	2		IP version interworking	6.2.0	6.3.0
2003-09	SA#21	SP-030380	340	2		Originating routing from ASs on behalf of PSIs	6.2.0	6.3.0
2003-09	SA#21	SP-030380	342	-		Signalling Path for Session Termination Procedures	6.2.0	6.3.0
2003-09	SA#21	SP-030380	343	-		Correction of cross references in Annex E	6.2.0	6.3.0
2003-09	SA#21	SP-030380	350	2		PSI configuration in the HSS	6.2.0	6.3.0
2003-09	SA#21	SP-030380	351	2		PSI configuration and routing	6.2.0	6.3.0
2003-12	SA#22	SP-030658	352	-		Terminology correction on "IMS User"	6.3.0	6.4.0
2003-12	SA#22	SP-030658	353	2		Forking preferences	6.3.0	6.4.0
2003-12	SA#22	SP-030658	358	-		Clarification of user data storage	6.3.0	6.4.0
2003-12	SA#22	SP-030658	359	2		Introduction of Session based messaging architecture	6.3.0	6.4.0

Date	TSG #	TSG Doc.	CR#	Rev	Cat	Subject/Comment	In	Out
2003-12	SA#22	SP-030658	361	-		PSTN-initiated Hold and Resume of a Mobile-PSTN Session	6.3.0	6.4.0
2003-12	SA#22	SP-030658	365	1		Transfer of CSCF capability on Cx	6.3.0	6.4.0
2003-12	SA#22	SP-030658	366	1		Support of Multi-terminals	6.3.0	6.4.0
2003-12	SA#22	SP-030658	368	2		Forking support in MGCF and AS	6.3.0	6.4.0
2003-12	SA#22	SP-030658	369	3		AS originated sessions	6.3.0	6.4.0
2003-12	SA#22	SP-030658	371	2		Requirements for IM CN Subsystem signalling flag	6.3.0	6.4.0
2003-12	SA#22	SP-030658	375	2		Terminal Capability with SIP Registration	6.3.0	6.4.0
2003-12	SA#22	SP-030658	378	1		Clarification of Trust Domain for IMS	6.3.0	6.4.0
2003-12	SA#22	SP-030658	379	1		HSS as database for the PSI handling	6.3.0	6.4.0
2003-12	SA#22	SP-030658	380	1		PSI corrections	6.3.0	6.4.0
2004-01	SA#22	SP-030778	362	2		PSI User NOTE:(version 6.4.0 never issued)	6.4.0	6.4.1
2004-03	SA#23	SP-040037	395	5		Relation of IMS sessions and PDP Contexts	6.4.1	6.5.0
2004-03	SA#23	SP-040037	381	3		Session based messaging: general principles	6.4.1	6.5.0
2004-03	SA#23	SP-040037	382	1		Session based Messaging without preconditions	6.4.1	6.5.0
2004-03	SA#23	SP-040037	384	2		Session based Messaging with AS intermediate node	6.4.1	6.5.0
2004-03	SA#23	SP-040037	385	2		Session based messaging release procedure	6.4.1	6.5.0
2004-03	SA#23	SP-040037	387	2		An optimisation in registration information flow for user not registered	6.4.1	6.5.0
2004-03	SA#23	SP-040037	390	1		Registration and Public User Identity	6.4.1	6.5.0
2004-03	SA#23	SP-040037	391	5		Record Route at S-CSCF	6.4.1	6.5.0
2004-03	SA#23	SP-040037	393	1		Alignment of headings with drafting rules	6.4.1	6.5.0
2004-03	SA#23	SP-040037	394	2		PSI clean-up	6.4.1	6.5.0
2004-03	SA#23	SP-040037	396	1		Support for Caller preferences	6.4.1	6.5.0
2004-03	SA#23	SP-040037	397	3		Message size limitations for Immediate messaging	6.4.1	6.5.0
2004-03	SA#23	SP-040037	398	4		Session based messaging requirements and flows	6.4.1	6.5.0
2004-03	SA#23	SP-040037	399	1		Reference to Local Services in Chapter 4.3.3.3a of 23.228	6.4.1	6.5.0
2004-03	SA#23	SP-040037	403	1		Proposed clarifications to MRFC/MRFP	6.4.1	6.5.0
2004-03	SA#23	SP-040037	404	1		Relationship between private user IDs and IMS subscription	6.4.1	6.5.0
2004-03	SA#23	SP-040037	405	1		Resource reservation in IMS	6.4.1	6.5.0
2004-03	SA#23	SP-040037	406	1		Architectural support for AS origination	6.4.1	6.5.0
2004-03	SA#23	SP-040037	407	2		Clarification of forking capabilities	6.4.1	6.5.0
2004-03	SA#23	SP-040037	408	1		PSIs for local services	6.4.1	6.5.0
2004-03	SA#23	SP-040037	409	2		Group management clarification	6.4.1	6.5.0
2004-06	SA#24	SP-040319	413	2		Session based messaging corrections to align with draft-ietf-simple-message-sessions-04	6.5.0	6.6.0
2004-06	SA#24	SP-040319	418	1		IPv6-IPv4 interworking	6.5.0	6.6.0
2004-06	SA#24	SP-040319	419	2		IPv4-IPv6 interworking flows	6.5.0	6.6.0
2004-06	SA#24	SP-040319	420	-		SDP acronym	6.5.0	6.6.0
2004-06	SA#24	SP-040319	421	2		Clarification of Message Charging Principles	6.5.0	6.6.0
2004-06	SA#24	SP-040319	422	4		Service indication in Session Initiation	6.5.0	6.6.0
2004-06	SA#24	SP-040319	424	2		Registration Requirement related to Application Server	6.5.0	6.6.0
2004-06	SA#24	SP-040319	425	4		Registration Status Event Sub/Notification between Application Server and S-CSCF	6.5.0	6.6.0
2004-06	SA#24	SP-040319	427	1		Definition of Private User Identity	6.5.0	6.6.0
2004-06	SA#24	SP-040319	428	2		Clarification of IMS identity sharing	6.5.0	6.6.0
2004-06	SA#24	SP-040319	430	1		Updates on the Gq interface in 23.228	6.5.0	6.6.0
2004-06	SA#24	SP-040319	431	-		IMS procedures modification for token generation	6.5.0	6.6.0
2004-06	SA#24	SP-040319	432	2		Release of Session based messaging session with intermediate node	6.5.0	6.6.0
2004-06	SA#24	SP-040319	434	1		Information storage after registration	6.5.0	6.6.0
2004-09	SA#25	SP-040523	415	1		Session based messaging size negotiation	6.6.0	6.7.0
2004-09	SA#25	SP-040523	437			Registration Requirement related to Application Server	6.6.0	6.7.0
2004-09	SA#25	SP-040523	438	1		Clarification to the Re-Registration procedure	6.6.0	6.7.0
2004-09	SA#25	SP-040523	439	-		IMS Emergency Services	6.6.0	6.7.0
2004-09	SA#25	SP-040523	440	1		Treatment of SIP forking request	6.6.0	6.7.0
2004-09	SA#25	SP-040523	441	1		Session based messaging release procedure	6.6.0	6.7.0
2004-09	SA#25	SP-040523	442	1		Generic signaling flow without preconditions	6.6.0	6.7.0
2004-09	SA#25	SP-040523	443	1		Session based messaging clean-up according latest version of IETF draft	6.6.0	6.7.0
2004-09	SA#25	SP-040523	444	-		Correction on precondition usage	6.6.0	6.7.0
2004-09	SA#25	SP-040523	445	1		Network control of PDP Context establishment for SBLP	6.6.0	6.7.0
2004-12	SA#26	SP-040896	446	3		Treatment of SIP forking request	6.7.0	6.8.0
2004-12	SA#26	SP-040896	447	1		Floor Control	6.7.0	6.8.0

Date	TSG #	TSG Doc.	CR#	Rev	Cat	Subject/Comment	In	Out
2004-12	SA#26	SP-040896	0450	1		Clarify that IMS end-points shall be able to support sending or receiving DTMF tone indications	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0451	1		Correct redirection scenarios	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0452	3		Addition of Application Server termination section	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0453	4		Revision of session set-up from external SIP client	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0454	1		Various editorial corrections	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0455	-		Missing step in identity procedure	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0456	-		Correction to PSTN Termination	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0458	1		Removal of support for local services	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0459	-		Removal of Editor's Note on ISC	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0460	-		Changes to SIP URL terminology	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0461	2		Reorganization and clarification of session flows	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0462	1		Changes for commonality in regards to token generation	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0464	1		Tel-URI related reference updates	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0466	-		Forward HSS name	6.7.0	6.8.0
2004-12	SA#26	SP-040896	0467	1		Informing AS on Registration	6.7.0	6.8.0
2005-03	SA#27	SP-050107	0473	3		Corrections to the Network initiated Application de-registration	6.8.0	6.9.0
2005-03	SA#27	SP-050107	0474	2		Correction to the Refer operation	6.8.0	6.9.0
2005-03	SA#27	SP-050107	0475	1		Editorial corrections in the identity procedures	6.8.0	6.9.0
2005-03	SA#27	SP-050107	0478	-		Corrections for errors introduced in 23.228 reorganization	6.8.0	6.9.0
2005-03	SA#27	SP-050107	0479	1		Corrections to flow for codec change	6.8.0	6.9.0
2005-03	SA#27	SP-050107	0481	1		Update of reference to TEL URI RFC 3966	6.8.0	6.9.0
2005-03	SA#27	SP-050107	0482	1		SBLP interactions correction	6.8.0	6.9.0
2005-06	SA#28	SP-050338	0483	1		Alignment of Session-based Messaging flows with stage 3	6.9.0	6.10.0
2005-06	SA#28	SP-050338	0490	1		On AS forking	6.9.0	6.10.0
2005-06	SA#28	SP-050338	0491	-		Corrections to wildcarded PSIs	6.9.0	6.10.0
2005-06	SA#28	SP-050338	0494	3		Clarification to the routing of SIP signalling within the IMS network	6.9.0	6.10.0
2005-06	SA#28	SP-050338	0496	1		Session setup with media set to inactive	6.9.0	6.10.0
2005-06	SA#28	SP-050338	0497	-		Correction to ENUM resolution for Infrastructure ENUM	6.9.0	6.10.0
2005-06	SA#28	SP-050338	0498	-		Support of Access Network NAT traversal (Creates Rel-7 version)	6.9.0	7.0.0
2005-09	SA#29	SP-050485	0477	4		Forward HSS name	7.0.0	7.1.0
2005-09	SA#29	SP-050485	0500	5		Access network NAT traversal	7.0.0	7.1.0
2005-09	SA#29	SP-050485	0503	1		Correction to flows for session setup with media set to inactive	7.0.0	7.1.0
2005-09	SA#29	SP-050474	0507	-		Correction on THIG Hiding feature	7.0.0	7.1.0
2005-09	SA#29	SP-050476	0510	1		Clarification of call flows with MGCF	7.0.0	7.1.0
2005-09	SA#29	SP-050482	0511	1		Introduction of IMS reference architecture diagram & deployment scenarios for HSS	7.0.0	7.1.0
2005-09	SA#29	SP-050476	0512	-		Clarification to the S-CSCF/MGCF-S-CSCF/MGCF procedure	7.0.0	7.1.0
2005-09	SA#29	SP-050476	0513	1		Private URI usage for redirect and refer procedures	7.0.0	7.1.0
2005-09	SA#29	SP-050476	0519	-		Introduction of Mx between BGCF and IMS ALG	7.0.0	7.1.0
2005-09	SA#29	SP-050482	0521	3		Procedures for NAT traversal	7.0.0	7.1.0
2005-09	SA#29	SP-050485	0523	2		Addition of Originating Unregistered Filter Criteria	7.0.0	7.1.0
2005-09	SA#29	SP-050476	0527	2		Update PSI activation procedure	7.0.0	7.1.0
2005-09	SA#29	SP-050476	0529	1		Correction of references	7.0.0	7.1.0
2005-09	SA#29	SP-050485	0533	2		Correction of unregistered state description	7.0.0	7.1.0
2005-12	SA#30	SP-050670	0520	5		Use of IMS as a transit network	7.1.0	7.2.0
2005-12	SA#30	SP-050820	0525	2		Identifiers grouped by service profile	7.1.0	7.2.0
2005-12	SA#30	SP-050824	0542	2		Introduction of IMS communication Service Identifier to TS 23.228	7.1.0	7.2.0
2005-12	SA#30	SP-050674	0544	1		Charging References Update	7.1.0	7.2.0
2005-12	SA#30	SP-050794	0545	1		TISPAN IBCF functionality added to IMS specs and editorial corrections from Ericsson at TSG SA#30	7.1.0	7.2.0
2006-03	SA#31	SP-060140	0546	3		Distribution of the information of the Identifiers grouped by service profile	7.2.0	7.3.0
2006-03	SA#31	SP-060133	0547	1		Introduction of IMS application reference to TS 23.228	7.2.0	7.3.0
2006-03	SA#31	SP-060178	0550	3		Editorial change request of TS 23.228, Figure 4.0	7.2.0	7.3.0
2006-03	SA#31	SP-060125	0551	1		S-CSCF reselection and failure recovery changes	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0552	2		Reference and Terminology Changes for Fixed Access	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0553	3		Transit configuration descriptions	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0554	2		Transit information flows	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0556	1		Support of local dialling plan in IMS	7.2.0	7.3.0

Date	TSG #	TSG Doc.	CR#	Rev	Cat	Subject/Comment	In	Out
2006-03	SA#31	SP-060130	0560	1		IBCF-THIG function in roaming scenarios	7.2.0	7.3.0
2006-03	SA#31	SP-060140	0561	2		Clarification of grouping Public User Identities	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0564	2		Clarification of Session modification with NAT traversal	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0566	2		Clarifications on NAT traversal	7.2.0	7.3.0
2006-03	SA#31	SP-060133	0567	-		Architectural requirements for the IMS communication identifier	7.2.0	7.3.0
2006-03	SA#31	SP-060136	0568	-		Correction on THIG Hiding feature	7.2.0	7.3.0
2006-03	SA#31	SP-060140	0570	2		Explicit use of SIP URI in the MGCF to I-CSCF messages	7.2.0	7.3.0
2006-03	SA#31	SP-060140	0571	1		Minimize drain of batteries when NATs are used	7.2.0	7.3.0
2006-03	SA#31	SP-060122	0573	-		Incorrect clause references	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0574	-		IBCF transit functions	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0575	1		IWF invoked by the IBCF	7.2.0	7.3.0
2006-03	SA#31	SP-060130	0576	1		S-CSCF selection for unregistered originating services	7.2.0	7.3.0
2006-06	SA#32	SP-060281	0580	1		The decision to send NAT Keep-alive message	7.3.0	7.4.0
2006-06	SA#32	SP-060284	0582	3		Clarification for requirement of IMS service netgotiation	7.3.0	7.4.0
2006-06	SA#32	SP-060281	0583	2		Closing of open issues of the support of local numbers in IMS	7.3.0	7.4.0
2006-06	SA#32	SP-060275	0586	1		Use of temporary public user identity in registration procedures	7.3.0	7.4.0
2006-06	SA#32	SP-060287	0587	-		Existence of NAT between IP-CAN GW and P-CSCF	7.3.0	7.4.0
2006-09	SA#33	SP-060577	0590	3	C	ICE and Outbound NAT Traversal	7.4.0	7.5.0
2006-09	SA#33	SP-060576	0591	5	B	Incorporate GRUU defintion	7.4.0	7.5.0
2006-09	SA#33	SP-060576	0592	2	B	Incorporation of GRUU Registration flows	7.4.0	7.5.0
2006-09	SA#33	SP-060576	0593	2	B	Addition of GRUU to Transfer flows	7.4.0	7.5.0
2006-09	SA#33	SP-060576	0594	2	B	Procedures for assigning, using and processing GRUUs	7.4.0	7.5.0
2006-09	SA#33	SP-060576	0595	2	B	Stage 2 GRUU specifications for non-UE UAs and B2BUAs	7.4.0	7.5.0
2006-09	SA#33	SP-060577	0596	2	C	Stage 2 Allowing an Asserted Display Name to be conveyed with a Public Identity	7.4.0	7.5.0
2006-09	SA#33	SP-060583	0598	3	B	Dynamic Service Activation Information (DSAI)	7.4.0	7.5.0
2006-09	SA#33	SP-060577	0600	3	C	IMS routing of E.164 numbers	7.4.0	7.5.0
2006-09	SA#33	SP-060577	0601	5	C	AS Originating requests on behalf of a user	7.4.0	7.5.0
2006-09	SA#33	SP-060577	0603	2	C	Clarifications to local number handling	7.4.0	7.5.0
2006-09	SA#33	SP-060577	0605	1	F	Clarification of NAT Types	7.4.0	7.5.0
2006-09	SA#33	SP-060569	0608	1	A	Corrections to Border Control Functions for Originating Session Flows	7.4.0	7.5.0
2006-09	SA#33	SP-060583	0609	2	B	The use of CSI IEs for the efficient communication with CSI capable UE	7.4.0	7.5.0
2006-09	SA#33	SP-060583	0610	1	B	Introduction of the Telephony Application Server into Normative text	7.4.0	7.5.0
2006-09	SA#33	SP-060653	0611	3	F	Corrections to NAT traversal	7.4.0	7.5.0
2006-09	SA#33	SP-060576	0612	1	B	Incorporation of GRUU for session initiation	7.4.0	7.5.0
2006-09	SA#33	SP-060577	0623	-	F	Applicability of transit procedures	7.4.0	7.5.0
2006-09	SA#33	SP-060577	0625	1	C	Stage 2 Allowing a Display Name to be conveyed with a Public Identity for calls originating from or terminating to the PSTN	7.4.0	7.5.0
2006-12	SA#34	SP-060829	0629	1	F	Clarification to the handling of alaised identifiers	7.5.0	7.6.0
2006-12	SA#34	SP-060829	0631	2	C	IMS implications for notification of loss of signalling bearer	7.5.0	7.6.0
2006-12	SA#34	SP-060830	0632	2	B	Introducing PCC to IMS	7.5.0	7.6.0
2006-12	SA#34	SP-060831	0639	2	B	AS Initiated Request on behalf of non-IMS user	7.5.0	7.6.0
2006-12	SA#34	SP-060830	0640	1	F	Impacts due to operator controlled QoS for GPRS	7.5.0	7.6.0
2006-12	SA#34	SP-060829	0641	1	F	Support of multiple simultaneous registrations	7.5.0	7.6.0
2007-03	SA#35	SP-070081	0658	2	A	Corrections to Border Control Functions for Terminating Session Flows	7.6.0	7.7.0
2007-03	SA#35	SP-070088	0651	1	F	The access of local addressing plan in IMS	7.6.0	7.7.0
2007-03	SA#35	SP-070088	0652	1	F	Co-existence of NAT traversal methods	7.6.0	7.7.0
2007-03	SA#35	SP-070220	0645	2	C	Handling of Request URIs containing a SIP URI with user=phone, and domain that does not own the target user: I-CSCF and S-CSCF	7.6.0	7.7.0
2007-03	SA#35	SP-070088	0650	2	F	The decision to send NAT Keep-alive message	7.6.0	7.7.0
2007-03	SA#35	SP-070089	0635	3	F	GRUU handling in the I-CSCF	7.6.0	7.7.0
2007-03	SA#35	SP-070089	0644	2	F	Anonymous GRUU and alignment with draft-gruu-11 and draft-gruu-reg-event-07	7.6.0	7.7.0
2007-03	SA#35	SP-070094	0647	2	F	PCC impacts on IMS	7.6.0	7.7.0

Date	TSG #	TSG Doc.	CR#	Rev	Cat	Subject/Comment	In	Out
2007-03	SA#35	SP-070237	0630	3	F	Clarification to the identification of IMS communication services	7.6.0	7.7.0
2007-03	SA#35	SP-070097	0659	2	F	Introduction of the IP-SM-GW into the TS 23.228	7.6.0	7.7.0
2007-03	SA#35	SP-070100	0660	3	B	Introducing dynamic user allocation to the application servers	7.6.0	7.7.0
2007-03	SA#35	SP-070101	0646	1	F	ICSI for Multimedia Telephony	7.6.0	7.7.0
2007-03	SA#35	SP-070101	0648	2	F	IMS subscription for notification of loss of signalling bearer	7.6.0	7.7.0
2007-03	SA#35	SP-070101	0665	2	C	Session setup principles for Multimedia Telephony	7.6.0	7.7.0
2007-03	SA#35	SP-070246	0667	3	F	Clarification use of GRUU	7.6.0	7.7.0
2007-03	SA#35	SP-070103	0663	2	B	IMS Enhancements to Support Number portability (NP) for Cable Networks	7.7.0	8.0.0
2007-03	SA#35	SP-070103	0664	2	B	IMS Enhancements to Inter-work with Preferred Circuit Carrier Access and Dial- Around for Cable networks	7.7.0	8.0.0
2007-06	SA#36	SP-070386	0669	1	A	Section alignment for AS initiated requests procedure	8.0.0	8.1.0
2007-06	SA#36	SP-070394	0671	1	A	Clarification of identification of IMS communication services	8.0.0	8.1.0
2007-06	SA#36	SP-070388	0677	-	A	Corrections to the Handling of Request URIs containing a SIP URI with user=phone	8.0.0	8.1.0
2007-06	SA#36	SP-070397	0679	2	A	Clarification of ICSI usage for multimedia telephony	8.0.0	8.1.0
2007-06	SA#36	SP-070393	0682	-	A	PCC Terminology Alignment	8.0.0	8.1.0
2007-06	SA#36	SP-070397	0684	-	A	Support for IP-CANs working on NW-only Bearer Establishment Mode	8.0.0	8.1.0
2007-06	SA#36	SP-070397	0686	2	A	Establishment of dedicated PDP Context for IMS related signalling	8.0.0	8.1.0
2007-06	SA#36	SP-070394	0688	1	A	Clarification on network providing list of supported ICSI's to UE	8.0.0	8.1.0
2007-06	SA#36	SP-070397	0692	2	A	Clarification on Identifying Alias Identities	8.0.0	8.1.0
2007-06	SA#36	SP-070389	0694	1	A	Clarification on Identifying Alias Identities	8.0.0	8.1.0
2007-06	SA#36	SP-070387	0695	2	B	Network to Network Interface between IM CN subsystem networks	8.0.0	8.1.0
2007-09	SA#37	SP-070535	0701	-	A	IMS Emergency Session support	8.1.0	8.2.0
2007-09	SA#37	SP-070541	0703	1	A	Correction to CF to enable service triggering for the forwarded-to address	8.1.0	8.2.0
2007-09	SA#37	SP-070543	0706	-	D	Renaming Ic and Iz reference points	8.1.0	8.2.0
2007-09	SA#37	SP-070541	0711	1	A	Requirement on Session Reject	8.1.0	8.2.0
2007-09	SA#37	SP-070541	0714	1	A	P-CSCF and PCRF deployment options	8.1.0	8.2.0
2007-09	SA#37	SP-070541	0716	2	A	IP Flow Terminology Alignment	8.1.0	8.2.0
2007-09	SA#37	SP-070580	0725	4	A	Handling of invalid and unauthorized media based on Communication Service Identifiers	8.1.0	8.2.0
2007-09	SA#37	SP-070541	0727	1	A	Registration of application reference	8.1.0	8.2.0
2007-09	SA#37	SP-070541	0729	1	A	S-CSCF validation of a SIP request	8.1.0	8.2.0
2007-09	SA#37	SP-070544	0730	1	B	P-CSCF awareness of access network type	8.1.0	8.2.0
2007-12	SA#38	SP-070810	0680	4	B	Support for Wildcarded public user identity for aggregated UNI support	8.2.0	8.3.0
2007-12	SA#38	SP-070803	0732	-	A	Update NAT Traversal related references to latest IETF Drafts	8.2.0	8.3.0
2007-12	SA#38	SP-070803	0734	1	A	Cleanup to address various FSS statements in Annex G	8.2.0	8.3.0
2007-12	SA#38	SP-070813	0735	3	B	Adding UE capability as one of Service Point Trigger	8.2.0	8.3.0
2007-12	SA#38	SP-070813	0738	-	A	Removal of incorrect references	8.2.0	8.3.0
2007-12	SA#38	SP-070808	0740	-	A	Clarification of served user handling in S-CSCF	8.2.0	8.3.0
2007-12	SA#38	SP-070808	0742	2	A	Establishment of Sessions with media "Inactive" indications	8.2.0	8.3.0
2007-12	SA#38	SP-070808	0744	1	A	QoS Authorization Correction	8.2.0	8.3.0
2007-12	SA#38	SP-070813	0745	1	B	Clarifications to P-CSCF access awareness requirements.	8.2.0	8.3.0
2007-12	SA#38	SP-070808	0747	-	A	Correct Mp protocol description	8.2.0	8.3.0
2007-12	SA#38	SP-070811	0748	-	F	Alignment of the definition of II-NNI	8.2.0	8.3.0
2007-12	SA#38	SP-070813	0749	1	F	Multiple simultaneous registration correction	8.2.0	8.3.0
2007-12	SA#38	SP-070808	0751	1	A	Correction of MGCF interaction	8.2.0	8.3.0
2007-12	SA#38	SP-070808	0752	2	A	Cleanup of NAT traversal procedures	8.2.0	8.3.0
2007-12	SA#38	SP-070813	0754	1	F	Correction to section number	8.2.0	8.3.0
2007-12	SA#38	SP-070808	0755	1	A	DHCP Also Provides P-CSCF IP address	8.2.0	8.3.0

History

Document history		
V8.20	January 2008	Publication
V8.3.0	January 2008	Publication