ETSI TS 133 107 V15.4.0 (2019-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
Digital cellular telecommunications system (Phase 2+) (GSM);
3G security;
Lawful interception architecture and functions
(3GPP TS 33.107 version 15.4.0 Release 15)

Reference
RTS/TSGS-0333107vf40

Keywords
GSM,LTE,SECURITY,UMTS

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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.

Modal verbs terminology

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

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

Contents

Intellectual Property Rights 2
Foreword 2
Modal verbs terminology 2
Foreword 16
Introduction 16
1 Scope 17
2 References 17
3 Definitions, symbols and abbreviations. 20
3.1 Definitions 20
3.2 Abbreviations 21
4 Functional architecture 23
5 Activation, deactivation and interrogation 31
5.0 General 31
5.1 Activation 32
5.1.0 General 32
5.1.1 X1_1-interface 33
5.1.2 X1_2-interface (IRI) 34
5.1.3 X1_3-interface (CC) 35
5.2 Deactivation 36
5.2.0 General 36
5.2.1 X1_1-interface 36
5.2.2 X1_2-interface (IRI) 36
5.2.3 X1_3-interface (CC) 37
5.3 Interrogation 37
5.3.0 General 37
5.3.1 Interrogation of the 3G ICEs 37
5.3.2 Interrogation of Delivery Functions 38
5A X Interfaces 38
5A.1 General 38
5A.2 X1 39
5A.2.1 General 39
5A.2.2 X1 Detail 39
5A.3 X2 39
5A.3.1 General 39
5A.4 X3 39
5A.4.1 General 39
6 Invocation of Lawful Interception (LI) for Circuit Switched (CS) services 40
6.0 General 40
6.1 Provision of Intercept CC - Circuit Switched 41
6.2 Provision of CC - Short Message Service 42
6.3 Provision of Intercept Related Information 43
6.3.0 General 43
6.3.1 X2-interface 43
6.3.2 Structure of the events 43
6.3.3 Call Related events 46
6.3.3.1 Call establishment 46
6.3.3.2 Answer 46
6.3.3.3 Supplementary Services 47
6.3.3.4 Handover 47
6.3.3.5 Release 47
6.3.4 Non Call Related events 48
6.3.4.1 SMS 48

6.3.4.2 Location update 48
6.3.4.3 Subscriber Controlled Input (SCI) 48
6.3.5 HLR Related events 48
6.3.5.1 Serving system 48
6.3.5.2 HLR subscriber record change 49
6.3.5.3 Cancel location 49
6.3.5.4 Register location 49
6.4 Intercept cases for circuit switched supplementary services 51
6.4.1 Interception of Multiparty call 51
6.4.2 Interception for Call Forwarding / Call Deflection / ECT 51

7 Invocation of Lawful Interception for GSN Packet Data services 52
7.0 General 52
7.1 Provision of Intercept Product - Short Message Service 53
7.2 Provision of Intercepted Content of Communications - Packet data GSN services 54
7.2.0 General 54
7.2.1 X3-interface 54
7.3 Provision of Intercept Related Information 55
7.3.0 General 55
7.3.1 X2-interface 55
7.3.2 Structure of the events 56
7.4 Packet Data related events 60
7.4.1 Mobile Station Attach 60
7.4.2 Mobile Station Detach 61
7.4.3 Packet Data PDP context activation 61
7.4.4 Start of interception with PDP context active 62
7.4.5 Packet Data PDP context deactivation 62
7.4.6 RA update 63
7.4.7 SMS 63
7.4.8 Packet Data PDP context modification 64
7.4.9 Serving System 64
7.4.10 Start of interception with mobile station attached 64
7.4.11 Packet Data Header Information 64
7.4.11.0 Introduction 64
7.4.11.1 Packet Data Header Report 65
7.4.11.2 Packet Data Summary Report 65
7.4.12 HLR subscriber record change 66
7.4.13 Cancel location 67
7.4.14 Register location 67
7.4.15 Location information request 67
7.4.16 Void 67
7.5 Void 67
7.6 Interception of the Multimedia Messaging Service (MMS) 67

7A Invocation of Lawful Interception for Packet Data Multi-media Service 68
7A.1 Provision of content of communications 68
7A.1.A Decryption for IMS Media Plane Security 68
7A.2 Provision of IRI 68
7A.2.1 Provision of IRI with SIP messaging 68
7A.2.2 Provision of IRI with XCAP messages 69
7A.2.3 Provision of IRI with Diameter or MAP messages related to HSS 69
7A.2.3.0 General 69
7A.2.3.1 Serving system 70
7A.2.3.2 Subscriber record change 71
7A.2.3.3 Registration Termination 72
7A.2.4 Provision of IRI for WebRTC 73
7A.3 Multi-media events 73
7A.3.0 General 73
7A.3.1 Mid IMS Session Interception 75
7A.3.1.0 General 75
7A.3.1.1 SDES Media Security 76
7A.4 Multi-media Call State Control Service Scenarios 76

7A.5 Push to talk over Cellular (PoC) 76
7A.6 SMS over IMS 76
7A.7 LI for KMS based IMS Media Security 76
7A.7.1 LI Architecture and functions 76
7A.7.2 Signalling over the Xk interfaces and LI events 77
7A.7.3 Cooperating KMSs 78
7A.7.4 Security 78
7A.7.5 Start of interception for an already established IMS media secured session 78
7A.8 IMS IMEI Interception 79
7A.9 Void 79

8 Security 80
8.0 General 80
8.1 Administration security 80
8.2 IRI security 80
8.2.1 Normal operation 80
8.2.2 Communication failure 80
8.3 CC security 81
8.4 Security aspects of Lawful Interception (LI) billing 81
8.5 Other security issues 81
8.5.1 Log files 81
8.5.2 Data consistency 81

9 Invocation of Lawful Interception (LI) for 3GPP WLAN interworking services 81
9.0 General 81
9.1 Provision of Intercept Product - Short Message Service 82
9.2 Provision of Intercepted Content of Communications - 3GPP WLAN Interworking services 82
9.2.0 General 82
9.2.1 X3-interface 83
9.3 Provision of Intercept Related Information 83
9.3.0 General 83
9.3.1 X2-interface 84
9.3.2 3GPP WLAN Interworking LI Events and Event Information 84
9.4 Structure of I-WLAN Events 91
9.4.1 I-WLAN Access Initiation 91
9.4.2 WLAN Access Termination 92
9.4.3 I-WLAN Tunnel Establishment 92
9.4.4 I-WLAN Tunnel Disconnect 93
9.4.5 Start of Intercept with I-WLAN Communication Active 94
9.4.6 Packet Data Header Information 95
9.4.6.0 Introduction 95
9.4.6.1 Packet Data Header Report 95
9.4.6.2 Packet Data Summary Report 96

10 Interception of Multimedia Broadcast/MultiCast Service (MBMS) 98
10.0 General 98
10.1 Provision of Content of Communications 98
10.2 Provision of Intercept Related Information 98
10.2.0 General 98
10.2.1 X2-interface 99
10.2.2 MBMS LI Events and Event Information 99
10.3 Structure of MBMS Events 101
10.3.1 Service Joining 101
10.3.2 Service Leaving 101
10.3.3 Start of Interception with Service Active 101
10.3.4 Subscription Activation 102
10.3.5 Subscription Modification 102
10.3.6 Subscription Termination 103

11 IMS Conference Services 103
11.1 Background for IMS Conference Services 103
11.1A Start of Interception for IMS Conference Services 103
11.2 Provision of Intercepted Content of Communication - IMS Conference Services 104

11.2.0 General 104
11.2.1 X3-interface 104
11.3 Provision of Intercept Related Information for IMS Conference Service 105
11.3.0 General 105
11.3.1 X2-interface 105
11.3.2 IMS Conference Events and Event Information 106
11.3.3 Structure of Conference Events 109
11.3.3.1 Start of Conference 109
11.3.3.2 Party Join 109
11.3.3.3 Party Leave 110
11.3.3.3A Conference Bearer Modification 110
11.3.3.4 Start of Intercept on an Active Conference 111
11.3.3.5 Conference End 111
11.3.3.6 Creation of Conference 112
11.3.3.7 Update of Conference 112

12 Lawful Interception for Evolved Packet System 113
12.1 LI functional architecture for EPS 113
12.2 Functional requirements for LI in case of E-UTRAN access and GTP based S5/S8. 116
12.2.0 General 116
12.2.1 Provision of Intercept Related Information 117
12.2.1.0 General 117
12.2.1.1 X2-interface 117
12.2.1.2 Structure of the events 117
12.2.2 X3-interface 122
12.2.3 EPS related events 123
12.2.3.1 Attach 123
12.2.3.2 Detach 123
12.2.3.3 Bearer activation 124
12.2.3.4 Bearer deactivation 124
12.2.3.5 Bearer modification 125
12.2.3.6 Start of interception with active bearer 126
12.2.3.7 Tracking Area/EPS Location Update 126
12.2.3.8 Serving Evolved Packet System 126
12.2.3.9 UE requested PDN connectivity 127
12.2.3.10 UE requested PDN disconnection 127
12.2.3.11 UE requested Bearer Resource Modification 127
12.2.3.12 Void 128
12.2.3.13 Start of interception with E-UTRAN attached UE 128
12.2.3.14 Packet Data Header Information 128
12.2.3.14.0 Introduction 128
12.2.3.14.1 Packet Data Header Report 129
12.2.3.14.2 Packet Data Summary Report 129
12.2.3.15 HSS subscriber record change 130
12.2.3.16 Cancel location 131
12.2.3.17 Register location 131
12.2.3.18 Location information request 131
12.3 Functional requirements for LI in case of E-UTRAN access and PMIP based S5/S8 interfaces 131
12.3.0 General 131
12.3.1 Provision of intercept related information 132
12.3.1.0 General 132
12.3.1.1 X2 interface 132
12.3.1.2 Structure of the events 133
12.3.2 X3-interface 136
12.3.3 LI events for E-UTRAN access with PMIP-based S5 or S8 136
12.3.3.1 Initial E-UTRAN Attach and UE PDN requested connectivity with PMIP-based S5 or S8 136
12.3.3.2 Detach and PDN disconnection for PMIP-based S5/S8 137
12.3.3.3 Start of interception with active tunnel for PMIP based S5/S8 137
12.3.3.4 Dedicated Bearer Procedures for E-UTRAN Access with PMIP-based S5/S8 137
12.3.3.5 PDN-GW initiated PDN-disconnection Procedure 137
12.3.3.6 PMIP Session modification 138
12.3.3.7 Packet Data Header Information 138

12.3.3.7.0 Introduction 138
12.3.3.7.1 Packet Data Header Report 138
12.3.3.7.2 Packet Data Summary Report 139
12.4 Functional requirements for LI in case of trusted non-3GPP IP access 140
12.4.0 General 140
12.4.1 Provision of Intercept Related Information 141
12.4.1.0 General 141
12.4.1.1 X2-interface 141
12.4.1.2 Structure of the events 141
12.4.2 X3-interface 146
12.4.3 LI events for trusted Non-3GPP IP access 146
12.4.3.1 Initial Attach and PDN connection activation with PMIPv6 on S2a 146
12.4.3.2 Initial Attach and PDN connection activation procedures with MIPv4 FACoA on S2a 147
12.4.3.3 Initial Attach and PDN connection activation procedures with DSMIPv6 over S2c 147
12.4.3.4 Detach and PDN disconnection with PMIPv6 on S2a 148
12.4.3.5 Detach and PDN disconnection with MIPv4 FACoA 148
12.4.3.6 Detach and PDN disconnection with DSMIPv6 on S2c 148
12.4.3.7 PDN-GW reallocation upon initial attach on s2c 149
12.4.3.8 PDN GW initiated Resource Allocation Deactivation with S2a PMIP 149
12.4.3.9 PDN GW initiated Resource Allocation Deactivation with S2a MIP v4 149
12.4.3.10 Serving Evolved Packet System 150
12.4.3.11 Start of interception with active tunnel or bearer 150
12.4.3.12 PMIP session modification 150
12.4.3.13 DSMIP session modification 150
12.4.3.14 Bearer activation 151
12.4.3.15 Bearer deactivation 151
12.4.3.16 Bearer modification 151
12.4.3.17 Packet Data Header Information 151
12.4.3.17.0 Introduction 151
12.4.3.17.1 Packet Data Header Report 151
12.4.3.17.2 Packet Data Summary Report 152
12.4.3.18 HSS subscriber record change 153
12.4.3.19 Registration Termination 154
12.4.3.20 Location Information request 154
12.5 Functional requirements for LI in case of untrusted non-3GPP IP access 155
12.5.0 Introduction 155
12.5.1 Provision of Intercept Related Information 155
12.5.1.0 General 155
12.5.1.1 X2-interface 156
12.5.1.2 Structure of the events 156
12.5.2 X3-interface 161
12.5.3 LI events for untrusted Non-3GPP IP access 161
12.5.3.1 Initial Attach and PDN connection activation with PMIPv6 on S2b 161
12.5.3.2 Initial attach and PDN connection activation for S2c in untrusted non-3GPP IP access 162
12.5.3.3 UE/ePDG-initiated Detach Procedure and UE Requested PDN disconnection with PMIP 162
12.5.3.4 Detach and PDN Disconnection for S2c in Un-trusted Non-3GPP IP access 163
12.5.3.5 Serving Evolved Packet System 163
12.5.3.6 Start of interception with active tunnel/bearer 163
12.5.3.7 PDN-GW reallocation upon initial attach on s2c 164
12.5.3.8 PDN GW initiated Resource Allocation Deactivation with S2b PMIP 164
12.5.3.9 PMIP session modification 164
12.5.3.10 DSMIP session modification 164
12.5.3.11 Packet Data Header Information 165
12.5.3.11.0 General 165
12.5.3.11.1 Packet Data Header Report 165
12.5.3.11.2 Packet Data Summary Report 166
12.5.3.12 Bearer activation 167
12.5.3.13 Bearer deactivation 167
12.5.3.14 Bearer modification 167
12.5.3.15 HSS subscriber record change 167
12.5.3.16 Registration Termination 168
12.5.3.17 Location Information request 168

12.6 Functional requirements for LI in case of Handovers between E-UTRAN and CDMA2000 Accesses.....169
12.7 Functional requirements for LI in case of interworking between SGSN and EPS nodes over S4/S12 interfaces.....169
12.8 Functional requirements for LI in case of interworking between SGSN and PDN-GW over Gn/Gp interfaces.....169
12.9 Functional Requirements for LI in case of Control and User Plane Separation.....169
12.9.1 Background.....169
12.9.2 LI Architecture with CUPS.....170
12.9.2.1 Overview.....170
12.9.2.2 Packet detection rules.....170
12.9.2.3 Forwarding action rules.....171
12.9.2.4 Intercepted packet identification rules.....171
12.9.3 Provision of Content of Communications.....171
12.9.3 1 Interception for Serving Gateway.....171
12.9.3.2 Interception for PDN Gateway.....171
12.9.4 Provision of Intercept Related Information.....172
12.9.4.1 Interception at the Serving Gateway.....172
12.9.4.2 Interception at the PDN Gateway.....172

13 Lawful Interception for 3GPP H(e)NBs.....172
13.0 General.....172
13.1 Provision of Intercepted Content of Communications for 3GPP H(e)NBs.....172
13.2 Provision of Intercept Related Information for 3GPP H(e)NBs.....173
13.2.1 X2-interface.....173
13.3 3GPP H(e)NB LI Events and Event Information.....173
13.4 UMTS Home Node B (HNB).....174
13.4.0 General.....174
13.4.1 Intercepted Content of Communications for 3GPP UMTS HNBs.....175
13.4.2 Intercept Related Information.....175
13.4.2.0 General.....175
13.4.2.1 X2-interface.....175
13.4.3 3GPP UMTS HNB LI Events and Event Information.....176
13.4.4 Structure of HNB Events.....176
13.4.4.1 Target UE Registration to HNB.....176
13.4.4.2 Target UE De-Registration from HNB.....177
13.4.4.3 Start of Intercept with HNB attached UE.....177
13.4.4.4 Target UE HNB Handover.....177
13.5 Home enhanced Node B (HeNB).....178

14 Interception of Generic Bootstrapping Architecture (GBA) Secured Communications.....179
14.1 Introduction.....179
14.2 Provision of Content of Communications.....179
14.3 Provision of Intercept Related Information.....179
14.3.1 Provision of Intercept Related Information Data Flow.....179
14.3.2 X2-interface.....180
14.3.3 GBA LI Events and Event Information.....180
14.4 Structure of GBA Events.....181
14.4.1 Bootstrapping.....181
14.4.2 Query from NAF.....182
14.4.3 Start of Interception with GBA key.....182

15 Invocation of Lawful Interception for IMS-based VoIP.....182
15.1 Overview of VoIP Interception.....182
15.2 Provision of Content of Communications.....183
15.2.0 Overview.....183
15.2.1 General Principles of CC Interception.....183
15.2.1.1 Intercept Trigger.....183
15.2.1.2 X3-Interface.....184
15.2.2 VoIP CC Interception.....184
15.2.3 Media Information Associated with the CC.....186
15.2.4 CC Interception in HPLMN with IMS Roaming.....186
15.2.5 CC Interception with CUPS.....187
15.3 Provision of Intercept Related Information for VoIP.....187

15.4 Lawful interception in the VPLMN with IMS roaming 187
15.4.1 Local breakout with P-CSCF in the VPLMN 187
15.5 Constraints for IMS VoIP Roaming Interception 187

16 LI for Group Communications using GCSE 188
16.1 Background 188
16.2 GCSE AS in Operator Network 188
16.2.0 General 188
16.2.1 Provision of Content of Communications 188
16.2.1.0 General 188
16.2.1.1 X3-interface 189
16.2.2 Provision of Intercept Related Information 189
16.2.2.0 General 189
16.2.2.1 X2-interface 190
16.2.2.2 GCSE AS LI Events and Event Information 190
16.2.2.2.0 General 190
16.2.2.2.1 Activation of GCSE Communications Group 191
16.2.2.2.2 Deactivation of GCSE Communications Group 192
16.2.2.2.3 User Added 192
16.2.2.2.4 User Dropped 193
16.2.2.2.5 Start of Intercept with an Active GCSE Communications Group 193
16.2.2.2.6 End of Intercept with an Active GCSE Communications Group 194
16.2.2.2.7 Modification of Target Connection to GCS AS 194
16.3 GCS AS outside Intercepting CSP Network 195

17 Interception for Proximity Services 195
17.1 ProSe Direct Discovery 195
17.1.1 General 195
17.1.2 Provision of Inteception of Call Content 196
17.1.3 Provision of Intercept Related Information 196
17.1.3.1 General 196
17.1.3.2 X2-interface 196
17.1.3.3 ProSe LI Events and Event Information 196
17.1.3.3.1 ProSe LI Events 196
17.1.3.3.2 ProSe LI Event Information 197
17.1.3.3.3 Structure of ProSe Events 197
17.1.3.3.3.1 Discovery Request 197
17.1.3.3.3.2 Match Report 198
17.2 ProSe One To Many Communications 198
17.2.1 General 198
17.2.2 Provision of Intercept Product - One-To-Many Communications 199
17.2.2.1 General 199
17.2.2.2 X2-interface 199
17.2.2.3 ProSe LI One-To-Many Events and Event Information 199
17.2.2.3.1 Overview of ProSe LI One-To-Many Events 199
17.2.2.3.2 Structure of ProSe LI One-To-Many Event Information 200
17.2.2.3.3 ProSe LI One-To-Many Events 201
17.3 ProSe Remote UE Communications 202
17.3.1 General 202
17.3.2 The ProSe Remote UE is a target for interception 202
17.3.3 The ProSe UE-to-NW Relay is a target for interception 203
17.3.4 X2-interface 203
17.3.4.1 Structure of the events 203
17.3.5 ProSe UE-to-NW Relay events 204
17.3.5.1 ProSe Remote UE Report 204
17.3.5.2 ProSe Remote UE Start of Communication 205
17.3.5.3 ProSe Remote UE End of Communication 205
17.3.5.4 Start of interception with ProSe Remote UE ongoing communication 205
17.3.5.5 Start of interception for ProSe UE-to-NW Relay 206
17.3.6 X3-interface 206

18 Invocation of Lawful Interception for messaging services 206
18.1 Overview of messaging services interception 206

18.2 SMS 207
18.2.1 Introduction 207
18.2.2 SMS over GPRS/UMTS 207
18.2.3 SMS over IP 207
18.2.4 SMS over NAS 208
18.2.4.0 Introduction 208
18.2.4.1 Structure of the events 208
18.2.4.2 SMS over NAS Events 208
18.2.4.3 SMS over NAS 209
18.3 MMS 210
18.3.1 Background 210
18.3.2 MMS Architecture IRI/CC Events 211
18.3.3 MMS Events 215
18.3.3.1 MMS Send 215
18.3.3.2 MMS Notification & Response 217
18.3.3.3 MMS Retrieval & Acknowledgement 218
18.3.3.4 MMS Forwarding 219
18.3.3.5 MMS Store 220
18.3.3.6 MMS Upload 221
18.3.3.7 MMS Delete (Stored in MMBox or in Proxy-Relay) 221
18.3.3.8 MMS Delivery 222
18.3.3.9 MMS Read Reply 222
18.3.3.10 MMS Cancel 223
18.3.3.12 MMS MMBox Viewing 224

19 Lawful Access Location Services (LALS) 225
19.1 General 225
19.2 Target Positioning 226
19.2.1 General 226
19.2.1 Immediate Location Provision 226
19.2.2 Periodic Location Provision 227
19.3 Enhanced Location for IRI 227
19.3.1 General 227
19.3.2 LALS Triggering Function 228
19.4 X2-interface for Target Positioning and Enhanced Location 228
19.4.1 General 228
19.4.2 LALS Information Elements 229
19.4.3 Structure of LALS Records 229
19.4.3.1 Target Positioning Reporting 229
19.4.3.2 Triggered Location Reporting 230

20 Lawful interception in the VPLMN with S8HR Roaming Architecture 230
20.1 Architecture 230
20.1.1 Overview 230
20.1.2 LI specific Reference Points 231
20.1.3 LI Specific Functions 231
20.1.3.1 Void 231
20.1.3.2 BBIFF: Bearer Binding Intercept and Forward Function 231
20.1.3.3 LMISF: LI Mirror IMS State Function 232
20.2 Provision of Content of Communications 233
20.2.1 Overview 233
20.2.1.1 General 233
20.2.1.2 S-GW/BBIFF Procedures for CC Interception 234
20.2.1.3 Void 235
20.2.1.4 LMISF Procedures for CC Interception 235
20.2.2 X3-Interface 235
20.3 Provision of Intercept Related Information 235
20.3.1 Overview 235
20.3.1.1 General 235
20.3.1.2 Void 236
20.3.1.3 S-GW/BBIFF Procedures for IRI interception 236
20.3.1.4 LMISF Procedures for IRI interception 236

20.3.2 IRI Events 237
20.3.2.1 General 237
20.3.2.2 IMEI-based interception 237
20.3.2.3 Mid-call Interception 237
20.3.2.4 Signalling Compression 237
20.3.2.5 Limitations 237
20.3.3 X2-Interface 238
20.4 Lawful Interception with CUPS architecture 238
20.5 S8HR LI and Target UE Mobility 239
20.5.1 Overview 239
20.5.2 S-GW Relocation 239

21 Invocation of Lawful Interception for Push to talk over Cellular services. 240
21.0 General 240
21.1 Provision of IRI – PTC Service 240
21.1.0 Introduction 240
21.1.1 Decryption for PTC services 241
21.1.2 Signalling over the Xk interfaces and LI events 242
21.2 Provision of Content – PTC Service 243
21.3 Provision of Interception 243
21.3.1 X3-Interface 243
21.3.2 X2-interface 244
21.3.3 LI Defined Events 244
21.3.3.1 IRI Defined Events 244
21.3.3.2 Communication Content (CC) Event 245
21.3.4 Events Elements 245
21.3.4.1 IRI Event Elements 245
21.3.4.2 CC Event Elements 249
21.4 PTC Surveillance Events 249
21.4.0 PTC General 249
21.4.1 PTC Service Registration 250
21.4.2 PTC Serving System 250
21.4.3 PTC Session Initiation 250
21.4.4 PTC Session Abandon 250
21.4.5 PTC Session Start 251
21.4.6 PTC Session End 251
21.4.7 PTC Start of Interception 252
21.4.8 PTC Pre-Established Session 252
21.4.9 PTC Instant Personal Alert 253
21.4.10 PTC Party Join event 253
21.4.11 PTC Party Drop 254
21.4.12 PTC Party Hold 254
21.4.13 PTC Party Retrieve 254
21.4.14 PTC Media Modification 255
21.4.15 PTC Group Advertisement 255
21.4.16 PTC Floor Control 255
21.4.17 PTC Target Presence 256
21.4.18 PTC Associate Presence 256
21.4.19 PTC List Management Events 257
21.4.20 PTC Access Policy event 257
21.4.21 PTC Media Type Notification 258
21.4.22 PTC Encryption Message 259
21.5 PTC Group Calls 259
21.5.1 General 259
21.5.2 Group Call Request 259
21.5.3 Group Call Response 260
21.5.4 PTC Group Interrogate 260
21.6 MCPTT Priority Calls and Alerts Messages 260
21.6.0 Background 260
21.6.1 General 261
21.6.2 MCPTT Emergency Group Call 262
21.6.3 MCPTT Emergency Group Call Cancel 262

21.6.4 MCPTT Emergency Group Alert....262
21.6.5 MCPTT Emergency Group State....263
21.6.6 MCPTT Imminent Peril Group Call....263
21.7 PTC Communication Content (CC)....263
21.7.0 General....264
21.7.1 Communication Content (CC)....264

22 Cell Supplemental Information Reporting....264
22.1 General....264
22.2 Cell Site Report Delivery....264
22.3 LI_CELL_INFO Interface....265
22.4 Cell Site Report....265

Annex A (informative): Information flows for Lawful Interception invocation of circuit switched services....266

A.1 Mobile originated circuit switched calls....266

A.2 Mobile terminated circuit switched calls....267

A.3 Call hold / call waiting....268

A.4 Multiparty calls....270

A.5 Call forwarding / call deflection....273
A.5.0 General....273
A.5.1 Unconditional call forwarding....273
A.5.2 Call forwarding on not reachable (IMSI detached)....274
A.5.3 Call forwarding on busy (network determined)....274
A.5.4 Call forwarding on not reachable (no response to paging/radio channel failure)....275
A.5.5 Call forwarding on no reply....275
A.5.6 Call forwarding on busy (user determined)/call deflection....276
A.5.7 Call waiting / call forwarding on no reply....277

A.6 Explicit call transfer....280

Annex B (informative): Information flows for Lawful Interception invocation of GSN Packet Data services....282

B.0 General....282

B.1 Mobile Station Attach....282

B.2 Mobile Initiated Mobile Station Detach....283

B.3 Network initiated Mobile Station Detach....283

B.4 Intra 3G GSN Routing Area Update....284

B.5 Inter 3G GSN Routing Area Update....284

B.6 PDP Context Activation....285

B.7 Start of interception with PDP context active....285

B.8 MS initiated PDP Context Deactivation....286

B.9 Network initiated PDP Context Deactivation....286

B.10 SMS....287

Annex C (informative): Information flows for the invocation of Lawful Interception for Packet Data with multimedia....289

C.0 General....289

C.1 Multimedia registration....289

C.2 Multimedia Session Establishment and Answer....291

C.3 Multimedia Release 292
C.4 Multimedia with Supplementary Service - Call Forwarding 292
C.5 Multimedia with Supplementary Service - Explicit Call Transfer 292
C.6 Multimedia with Supplementary Service - Subscriber Controlled input 292

Annex D (informative): Information flows for Lawful Interception invocation at the MGW using H.248 293

D.0 General 293
D.1 Mobile to Mobile call, originating side is target 293

Annex E (Informative): IMS-based VoIP Lawful Interception call scenarios 295

E.1 Overview 295
E.2 Background 295
E.3 Originating Call from the Target with CC Interception at the PDN-GW/GGSN 298
E.3.0 General 298
E.3.1 Originating Call from the Target with CC Interception at the MRF 299
E.4 Originating Call from the Target with CC Interception at the IMS-AGW 299
E.5 Terminating Call to the Target with CC Interception at the PDN-GW/GGSN 301
E.5.0 General 301
E.5.1 Terminating Call to the Target with CC Interception at the MRF 301
E.6 Terminating Call to the Target with CC Interception at the IMS-AGW 303
E.7 Intra-CSP Forwarded Call with CC Interception at the PDN-GW/GGSN 304
E.7.0 General 304
E.7.1 Intra-CSP Forwarded Call with CC Interception at the MRF 304
E.8 Intra-CSP Forwarded Call with CC Interception at the IMS-AGW 306
E.9 Inter-CSP Forwarded Call to a CS Domain 307
E.10 Inter-CSP Forwarded Call to an IMS Domain 308
E.11 Originating Call from the Target with IMS Roaming 309
E.12 Terminating Call to the Target with IMS Roaming 310
E.13 Intra-CSP Forwarded Call with IMS Roaming 311
E.14 Lawful interception in the VPLMN with IMS roaming 311
E.14.1 Local Breakout (LBO) with P-CSCF in VPLMN 311
E.14.1.1 General 311
E.14.1.2 Originating call from an Inbound Roaming Target with CC Interception at the PDN-GW/GGSN 312
E.14.1.3 Originating Call from an Inbound Roaming Target with CC Interception at the IMS-AGW 312
E.14.1.4 Terminating Call to an Inbound Roaming Target with the CC Interception at the PDN-GW/GGSN 313
E.14.1.5 Terminating Call to an Inbound Roaming Target with CC Interception at the IMS-AGW 315

Annex F (informative): Examples of IMS-based VoIP Lawful Interception (LI) call flows 316

F.1 General remarks 316
F.2 Call Originations from Target in Home CSP 316
F.2.0 Introduction 316
F.2.1 Target Originated Call - Target (Party_A) Calls Party_B 317
F.2.2 Target Originated Call - Target (Party_A) dials a Special Number 318
F.3 Call Terminations to Target - Home CSP 318
F.3.0 Introduction 318
F.4 Call Forwarding - Non Roaming 319

F.4.0 Introduction 319
F.4.1 Intra-CSP Call Forwarding Unconditional 320
F.4.2 Intra-CSP Call Forwarding No Answer 321
F.4.3 Inter-CSP Call Forwarding Unconditional 323
F.5 IMS Roaming 323
F.5.0 General 323
F.5.1 Roaming Target Originates a Call 324
F.5.1A CC Unvailable in Home CSP due to Optimal Media Routing 325
F.5.2 Call Termination to a Roaming Target 326
F.6 Interception in Visited CSP 326
F.6.0 General 326
F.6.1 Interception in Visited CSP - Target Originated Call 327
F.6.2 Interception in Visited CSP - Target Terminating Calls 328
F.6.3 Incoming Call to Roaming Target is forwarded due to Call Forwarding No Answer 329
F.7 Ad-Hoc Conference Calls established by the Target 329
F.7.0 Introduction 329
F.7.1 Party_A (target) creates the conference 330
F.7.2 Party_C joins the conference 330
F.7.3 Party_B joins the conference 332
F.7.4 Party_C drops out of the conference 334
F.7.5 Reconfiguration from Conference to two-party call 335
F.7.6 Party_A (target) places Conference on hold 336
F.7.7 Party_A (target) retrieves Conference from hold 337
Annex G (informative): Examples of CC interception for transcoded media 338
G.1 Introduction 338
G.2 CC Interception of transcoded media 338
G.3 CC Interception of transcoded media with e2ae encryption 339
G.4 CC Interception of transcoded media with e2e hop-by-hop encryption 340
G.5 CC Interception of transcoded media at the TrGW 341
Annex H (informative): Location only warrant 343
H.1 General 343
H.2 Location only warrant 343
H.3 Immediate Location warrant 343
Annex I (informative): Interception of Targets with Non-Local IDs 344
I.1 Introduction 344
I.2 Interception of outgoing calls 344
I.2.1 General 344
I.2.2 Interception at S-CSCF or P-CSCF 344
I.2.3 Interception at the IBCF/MGCF 345
I.3 Interception of incoming calls 346
I.3.1 General 346
I.3.2 Interception at S-CSCF or P-CSCF 346
I.3.3 Interception at the IBCF/MGCF 347
Annex J (informative): Lawful Interception Illustrations in VPLMN with S8HR 348
J.1 Overview 348
J.2 Process Flow 349
J.3 Call Flows 352
J.3.1 General 352

J.3.2 Originating call....352
J.3.3 Terminating call....353
J.3.4 Mid-Call Interception....354
J.3.5 Lawful Interception without CC....356
J.3.6 S-GW Relocation....356
J.4 Correlation of CC and IRI....358
J.5 UE Location Reporting....358
Annex L (informative): IP-based Handover Interface for CC of CS Intercepts....360
L.1 Background....360
L.2 Options for X3....360
L.3 Information delivered along with the CC....361
Annex M (informative): Change history....363
History....369

Foreword

This Technical Specification (TS) 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.

Introduction

This Technical Specification has been produced by the 3GPP TSG SA to allow for the standardisation in the area of lawful interception of telecommunications. This document describes in general the architecture and functions for lawful interception. Laws of individual nations and regional institutions (e.g. European Union), and sometimes licensing and operating conditions define a need to intercept telecommunications traffic and related information in modern telecommunications systems. It has to be noted that lawful interception shall always be done in accordance with the applicable national or regional laws and technical regulations.

1 Scope

The present document describes the architecture and functional requirements within a Third Generation Mobile Communication System (3GMS) and the Evolved Packet System (EPS).

The present document shows the service requirements from a Law Enforcement point of view only. The aim of this document is to define a 3GMS and EPS interception system that supports a number of regional interception regulations, but these regulations are not repeated here as they vary. Regional interception requirements shall be met by using specific (regional) mediation functions allowing only required information to be transported.

The handover interfaces for Lawful Interception (LI) of Packet-Data Services, Circuit Switched Services, and Multimedia Services within the UMTS network and Evolved Packet System for Stage 3 are described in TS 33.108 [11].

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] Void

[2] ETSI ES 201 158 (V1.2.1 April 2002): "Lawful Interception; Requirements for network functions".

[3] ETSI ES 201 671 (V3.1.1 May 2007): "Handover Interface for the lawful interception of telecommunications traffic".

[4] Void

[5] Void

[6] Void

[7] 3GPP TS 33.106: "3G Security; Lawful Interception Requirements".

[8] ANSI J-STD-025-A (April 2003): "Lawfully Authorised Electronic Surveillance".

[9] Void

[10] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description".

[11] 3GPP TS 33.108: "3G Security; Handover interface for Lawful Interception".

[12] Void

[13] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[14] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[15] 3GPP TS 23.008: "Organization of subscriber data".

[16] 3GPP TS 29.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3".

[17] 3GPP TS 24.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3".

[18] IETF RFC 1122 (October 1989): "Requirements for Internet Hosts -- Communication Layers".

[19] IETF RFC 1123 (October 1989): "Requirements for Internet Hosts -- Application and Support".

[20] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[21] 3GPP TS 24.147: "Conferencing Using the IP Multimedia (IM) Core Network (CN) subsystem 3GPP Stage 3".

[22] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[23] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[24] 3GPP TS 29.273: "Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); 3GPP EPS AAA interfaces".

[25] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[26] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[27] Void

[28] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[29] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

[30] 3GPP TS 23.272: " Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2"

[31] 3GPP TS 22.220: " Service Requirements for Home NodeBs and Home eNodeBs".

[32] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[33] 3GPP TS 25.467: "UTRAN architecture for 3G Home Node B (HNB); Stage 2"

[34] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB) ".

[35] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[36] IETF RFC 3966 (December 2004): "The Tel URILs for Telephone Numbers ".

[37] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[38] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[39] IETF RFC 791: "Internet Protocol".

[40] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[41] IEFT RFC 3697: "IPv6 Flow Label Specification".

[42] 3GPP TS 29.334: "IMS Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW); Iq Interface (Stage 3)".

[43] 3GPP TS 23.228: "IP Multimedia Subsystem; Stage 2".

[44] 3GPP TS 23.203: "Policy Charging and Control Architecture".

[45] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".

[46] 3GPP TS 29.162: "Interworking between IM CN subsystem and IP Networks".

[47] 3GPP TS 29.163:"Interworking between IP Multimedia Core Network (CN) subsystem and Circuit Switched (CS) Networks"

[48] 3GPP TS 23.334: "IP Multimedia Subsystem (IMS) Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW) interface: Procedures descriptions".

[49] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[50] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[51] 3GPP TS 22.468: "Group Communication System Enablers for LTE (GCSE_LTE)".

[52] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[53] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[54] Void.

[55] 3GPP TS 24.623: "Technical Specification Group Core Network and Terminals; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".

[56] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[57] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[58] 3GPP TS 24.333: "Proximity-services (ProSe) Management Objects (MO)".

[59] 3GPP TS 32.277: "Telecommunication management; Charging management; Proximity-based Services (ProSe) charging".

[60] 3GPP TS 22.101: "Universal Mobile Telecommunications System (UMTS); Service aspects; Service principles".

[61] 3GPP TS 29.002: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) specification ".

[62] 3GPP TS 29.228: "Technical Specification Group Core Network and Terminals; IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[63] 3GPP TS 29.328: "Technical Specification Group Core Network and Terminals; IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents".

[64] Void.

[65] GSMA IR.61: "Wi-Fi Roaming Guidelines".

[66] 3GPP TS 29.329: " Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); 3GPP EPS AAA interfaces ".

[67] 3GPP TS 22.071: "Location Services (LCS); Service description; Stage 1".

[68] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[69] IETF RFC 3320: "Signaling Compression (SigComp)".

[70] IETF RFC 4896: "Signaling Compression (SigComp) Corrections and Clarifications".

[71] GSMA IR.65: "IMS Roaming and Interworking Guidelines".

[72] MMS Architecture OMA-AD-MMS-V1_3-20110913-A.

[73] Multimedia Messaging Service Encapsulation Protocol OMA-TS-MMS_ENC-V1_3-20110913-A.

[74] 3GPP TS 22.140: "Multimedia Messaging Service (MMS); Stage 1".

[75] 3GPP TS 23.214 "Architecture enhancements for control and user plane separation of EPC; Stage 2".

[76] OMA MLP TS: "Mobile Location Protocol", [http://www.openmobilealliance.org].

[77] IETF RFC 2822: "Internet Message Format".

[78] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS);Stage 2".

[79] 3GPP TS 32.272: "Push-to-talk over Cellular (PoC) charging".

[80] 3GPP TS 24.379 "Mission Critical Push To Talk (MCPTT) call control; Protocol specification".

[81] OMA-TS-PoC_System_Description-V2_1-20110802-A.

[82] OMA-AD-PoC-V2_1-20110802-A.

[83] OMA-TS-PoC UserPlane-V2_1-20110802-A.

[84] 3GPP TS 23.179 "Functional architecture and information flows to support MCPPT Stage 2".

[85] 3GPP TS 22.179 "Mission Critical Push to Talk (MCPTT) over LTE; Stage 1".

[86] IETF RFC 3550: "Real Time Transport Protocol".

[87] IETF RFC 3998: "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping".

[88] IETF RFC 3261: "Session Initiation Protocol".

[89] ETSI TS 103 221-1 (V1.1.1): "Lawful Interception (LI); Internal Network Interface X1 for Lawful Interception".

3 Definitions, symbols and abbreviations.

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [13] and the following apply.

Application layer: As defined by Internet Engineering Task Force (IETF) in RFC 1123 [19].

Closed access mode: H(e)NB provides services only to its associated CSG members. A H(e)NB configured for closed access broadcasts a CSG Indicator and a specific CSG Identity.

CUPS: As defined in 3GPP TS 23.214 [75], represents PLMN with architecture enhancements for control and user plane separation of EPC nodes.

Hybrid access mode: H(e)NB provides services to its associated CSG members and to non-CSG members. A H(e)NB configured for hybrid access does not broadcast a CSG Indicator but does broadcast a CSG Identity.

IP layer: As defined by Internet Engineering Task Force (IETF) in RFC 1122 [18].

Interception Area: is a subset of the network service area comprised of a set of cells which defines a geographical zone.

Location Dependent Interception: is interception of a target mobile within a network service area that is restricted to one or several Interception Areas (IA).

MCPTT Identity: Attributes configured in the MCPTT service that relate to the human user of the MCPTT service.

Non-Local Identity: As defined by clause 5.1.2 General principles in TS 33.106 [7].

Open access mode: H(e)NB operates as a normal NodeB or eNodeB. A H(e)NB configured for open access does not broadcast either a CSG Indicator or CSG Identity.

Push to Talk over Cellular (PTC): This term, when used in the present document, represents either a PoC or MCPTT type service.

S8 Home Routed (S8HR): The term as used in this standard represents a roaming architecture where PDN-GW and P-CSCF are located in the HPLMN and therefore, UE IMS signalling and media are routed directly to the HPLMN through S8 reference point. Roaming architecture with S8HR for VoLTE is described in GSMA IR.65 [71] clause 2.4.3.

Other LI specific definitions are given in TS 33.108 [11].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [13] and the following apply:

3GMS	3rd Generation Mobile Communications System
3G GGSN	3rd Generation Gateway GPRS Support Node
3G GSN	3rd Generation GPRS Support Node (GGSN/SGSN)
3G MSC	3rd Generation Mobile Switching Centre
3G SGSN	3rd Generation Serving GPRS Support Node
3G UMSC	3rd Generation Unified Mobile Switching Centre
AAA	Authentication, Authorization, and Accounting
ADMF	Administration Function
AGW	Access Gateway
AN	Access Network
AP	Access Provider
AS	Application Server
BBIFF	Bearer Binding Intercept and Forwarding Function
BM-SC	Broadcast-Multicast Service Centre
BSF	Bootstrapping Serving Function
B-TID	Bootstrapping Transaction Identifier
CC	Content of Communication
CS	Circuit Switched
CSCF	Call Session Control Function
CSG	Closed Subscriber Group
CSP	Communications Service Provider
CSR	Cell Site Report
CUPS	Control and User Plane Separation of EPC nodes
DF	Delivery Function
DSMIP	Dual Stack Mobile IP
ECT	Explicit Call Transfer
EPC	Evolved Packet Core
ePDG	Evolved PDG
EPS	Evolved Packet System
E-UTRAN	Evolved UTRAN
FTP	File Transfer Protocol
GBA	Generic Bootstrapping Architecture
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSN	GPRS Support Node (SGSN or GGSN)
HA	Home Agent
HeMS	HeNB Management System
HeNB	Home enhanced NodeB
HeNB GW	HeNB Gateway
H(e)NB	Home and Home enhanced NodeB
HI	Handover Interface
HLR	Home Location Register
HMS	HNB Management System
HNB	Home NodeB
HNB GW	HNB Gateway
HRPD	High Rate Packet Data
HSS	Home Subscriber Server
IA	Interception Area

IBCF	Interconnecting Border Control Function
ICEs	Intercepting Control Elements (3G MSC Server, 3G GMSC Server, P-CSCF, S-CSCF, SGSN, GGSN, HLR, AAA Server, PDG, MME, S-GW, PDN-GW, HSS)
IETF	Internet Engineering Task Force
IM-MGW	IMS Media Gateway
IMEI	International Mobile station Equipment Identity
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Core Network Subsystem
IMS-AGW	IMS Access Gateway
IMSI	International Mobile Subscriber Identity
INEs	Intercepting Network Elements (3G MSC Server, 3G GMSC Server, P-CSCF, S-CSCF, SGSN, GGSN, MGW, HLR, AAA Server, PDG)
IP	Internet Protocol
IP-SM-GW	IP-Short-Message-Gateway
IRI	Intercept Related Information
I-WLAN	Interworking WLAN (3GPP WLAN interworking subnetwork)
LALS	Lawful Access Location Services
LAN	Local Area Network
LBO	Local Breakout
LCS	Location Services
LDI	Location Dependent Interception
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LIPA	Local IP Access
LMISF	LI Mirror IMS State Function
LTE	Long Term Evolution
MBMS	Multimedia Broadcast/Multicast Service
MC ID	Mission Critical User Identity
MCPTT	Mission Critical Push-To-Talk
MCPTT ID	Mission Critical Push to Talk Identity
MF	Mediation Function
MGCF	Media Gateway Control Function
MGW	Media Gateway
ME	Mobile Entity
MIP	Mobile IP
MM	Multimedia Message
MMBox	Multimedia Message Box
MME	Mobility Management Entity
MN	Mobile Node
MRF	Media Resource Function
MSISDN	Mobile Subscriber ISDN Number
NAF	Network Application Function
NAI	Network Access Identifier
NO	Network Operator
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
PDG	Packet Data Gateway
PDN	Packet Data Network
PDN-GW	PDN Gateway
PMIP	Proxy Mobile IP
PoC	Push to talk over Cellular
PS	Packet Switched
PTC	Push to Talk over Cellular
RA	Routing Area
RAI	Routing Area Identity
S8HR	S8 Home Routing
SAI	Service Area Identity
S-CSCF	Serving CSCF
SeGW	Security Gateway
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol

SMS	Short Message Service
S-GW	Serving Gateway
SR-VCC	Single Radio Voice Call Continuity
SX3LIF	Split X3 LI Interworking Function
TEL URI	"tel" URI, as defined in RFC 3966 [36]
TLS	Transport Layer Security
TrGW	Transit Gateway
TRF	Transit Routing Function
TWAN	Trusted WLAN Access Network
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
URI	Universal Resource Identifier
URL	Universal Resource Locator
VoIP	Voice over IP
VoLTE	Voice over LTE
WLAN	Wireless LAN
WAF	WebRTC Authorisation Function
WebRTC	Web Real Time Communications
WIC	WebRTC IMS Client
WWSF	WebRTC Web Server Function

4 Functional architecture

The following figures contain the reference configuration for the lawful interception. The circuit-switched configuration is shown in figure 1a. The packet-switched configuration is shown in figure 1b. Intercept configurations for HLR and IMS are shown in figures 1c and 1d. The WLAN interworking configuration is shown in figure 1e. The intercept configurations for IMS conferencing is shown in figure 1f. The CC intercept configuration for IMS-based VoIP is shown in figure 1g. Intercept configurations for LALS are shown in figure 1h. The intercept configuration for Non-Local ID at IBCF and MGCF is shown in figure 1i. The intercept configuration for S8HR VoLTE in the visited PLMN is shown in figure 1j. The intercept configuration for Push to Talk over Cellular (PTC) is shown in figure 1k and 1l. Within the present document PTC encompasses PoC as a service and Mission Critical Push-To-Talk (MCPTT) services. The CSP Cell Supplemental Information configuration is shown in figure 1m. The various entities and interfaces are described in more detail in the succeeding clauses. The additional intercept configurations for Evolved 3GPP Packet Switching Domain are described in clause 12.

NOTE 0: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

PS domain of the UMTS system (GSN and Multimedia Packet Data services), 3GPP-WLAN interworking network and Evolved Packet Switching Domain provide UMTS/GSM/EPS customer's mobile equipment (UE) with connectivity service to another end of the communication. Another end of the communication may be a network element (server) or another UE. Therefore, UMTS/EPS system provides IP layer TS 23.008 [15] services. Hence, UMTS/EPS NO/AP is responsible only for IP layer interception of CC data. In addition to CC data, the LI solution for UMTS/EPS offers generation of IRI records from respective control plane (signalling) messages. The IP layer connectivity service is needed to support application layer TS 29.234 [16] service provision to UMTS/GSM/EPS customers. For instance, the following are examples of application layer services: email service; web browsing service; FTP service; audio services (e.g. VoIP, PoC); other multimedia services (MBMS, video telephony); The majority of the application layer services require addition of respective server functionality to the network. Note that it is not necessary that such application layer SP should be the same commercial entity as the UMTS/EPS AP/NO in question.

When location information of the target is delivered by an ICE, the MF may need to add the civic address associated with the access network point as known by the CSP. The method used to obtain the civic address will depend on the CSP implementation. (e.g. by accessing a remote database). National regulations define whether the civic address needs to be provided.

NOTE 1: For instance in MBMS a BM-SC and especially content providing server might be operated by different commercial entity than UMTS network.

The LALS provides LCS information of the target on-demand, independently of the target's activity/events. Additionally, LALS may be triggered by any IRI event detected by an ICE to provide LCS location information of the target correlated to the triggering event.

When IA is provisioned LCS may provide enhanced geographic capabilities

For all UE locations obtained, generated or reported to the MF/DF, the ICE shall report the time at which the location was established by the location source (e.g. MME or HSS) and provide this to the MF/DF along with the location information. If this information cannot be provided by the location source the ICE shall indicate that the time is not available.

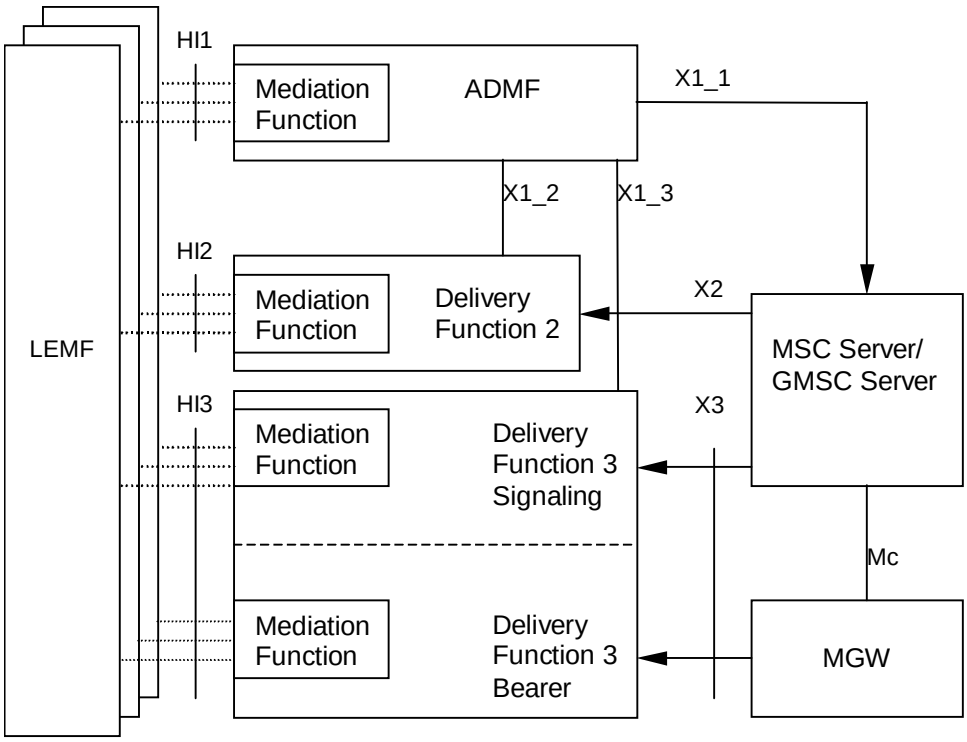


Figure 1a: Circuit switched intercept configuration

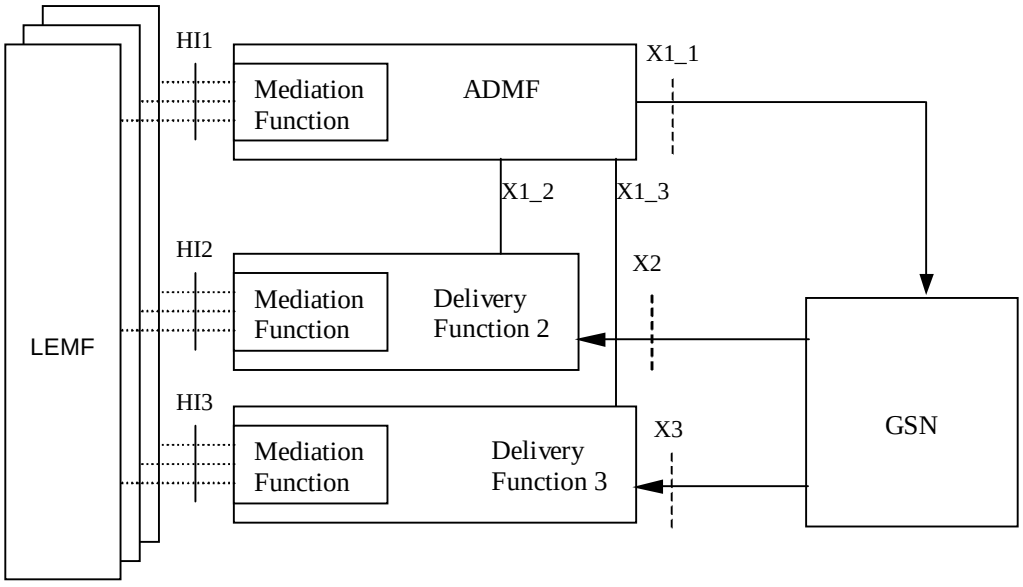


Figure 1b: Packet Switched Intercept configuration

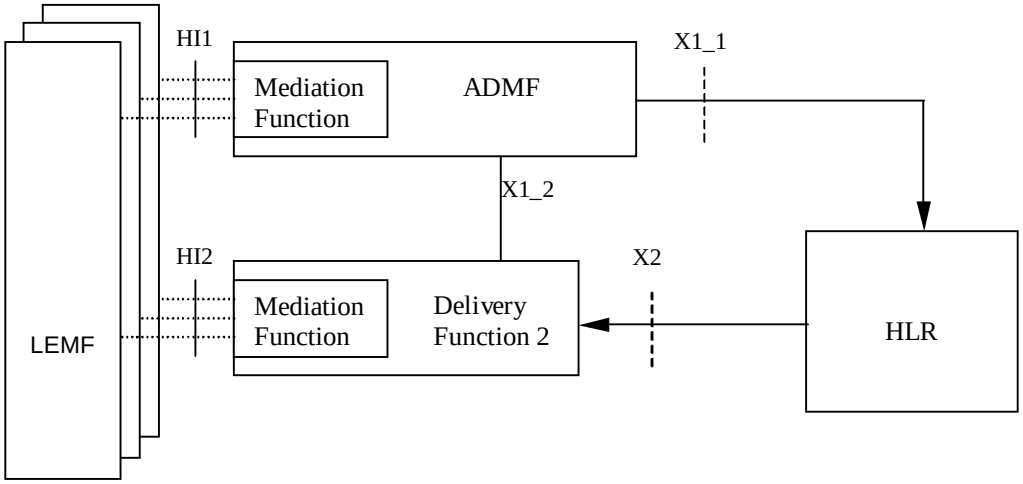


Figure 1c: HLR Intercept configuration

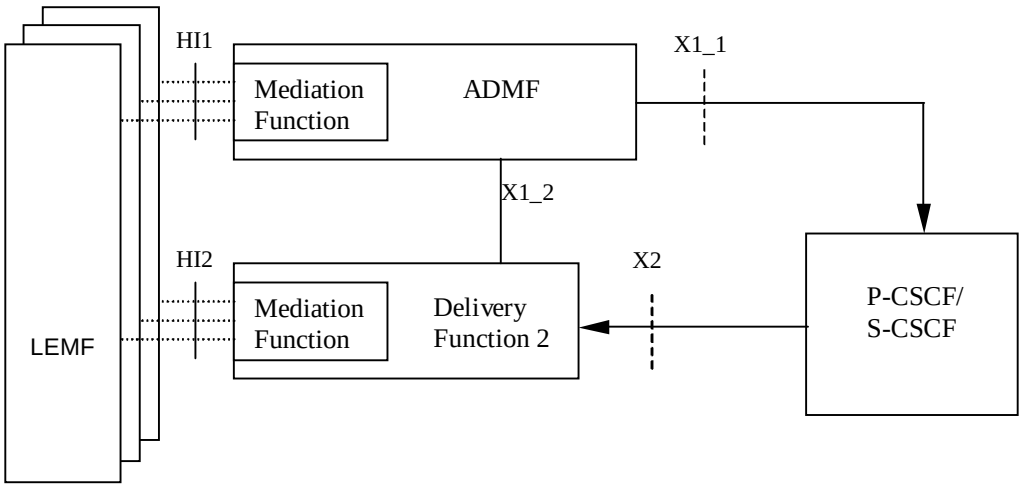


Figure 1d: IMS-CSCF Intercept configuration

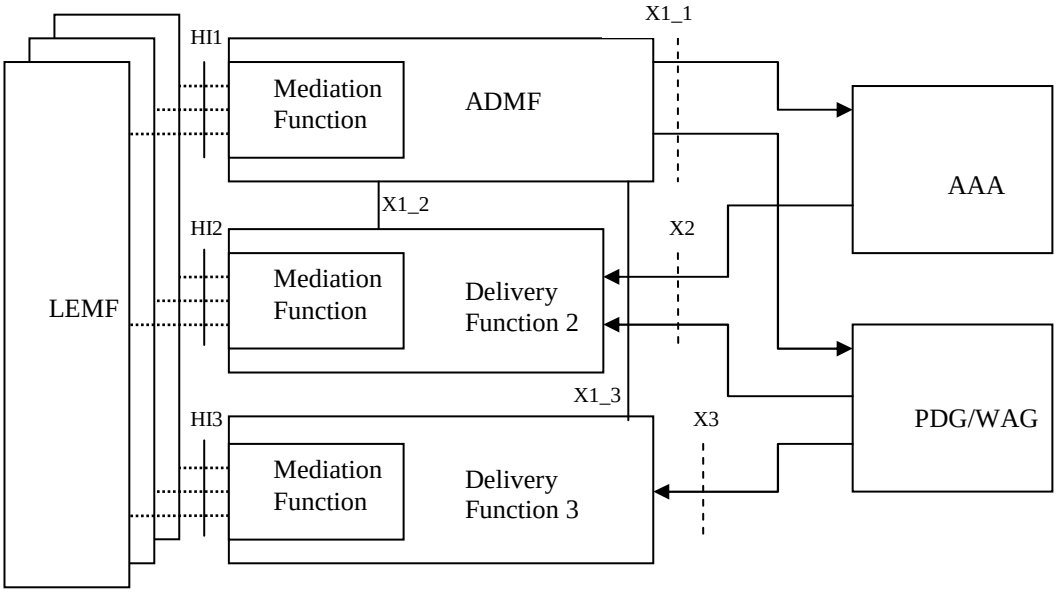


Figure 1e: WLAN Interworking Intercept configuration

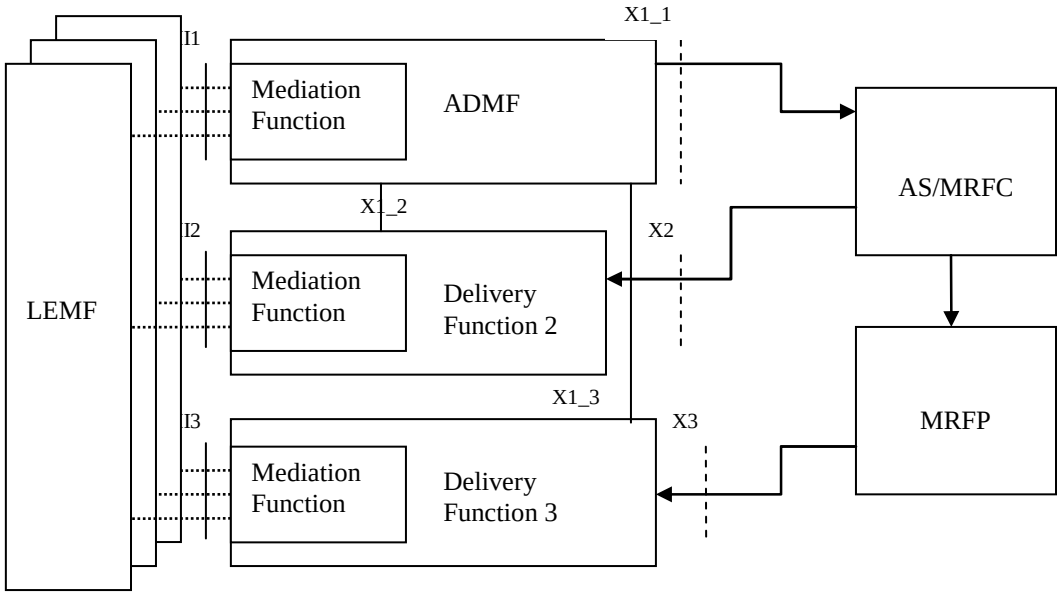


Figure 1f: IMS Conferencing Intercept configuration

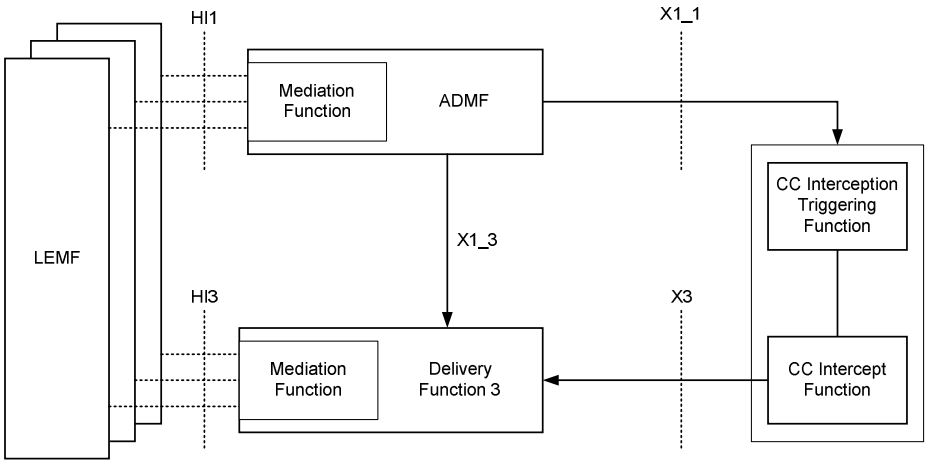


Figure 1g: VoIP CC Intercept Configuration

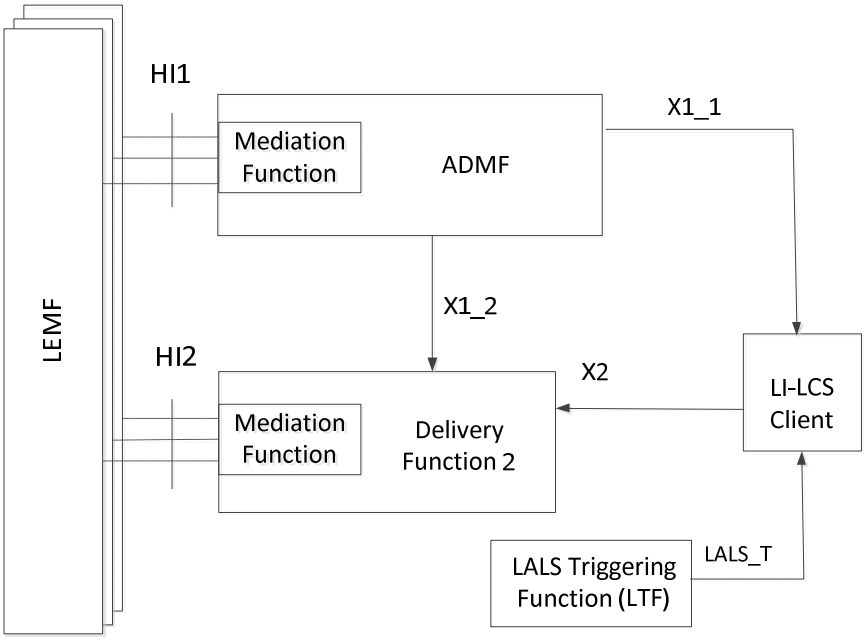


Figure 1h: LALS configuration

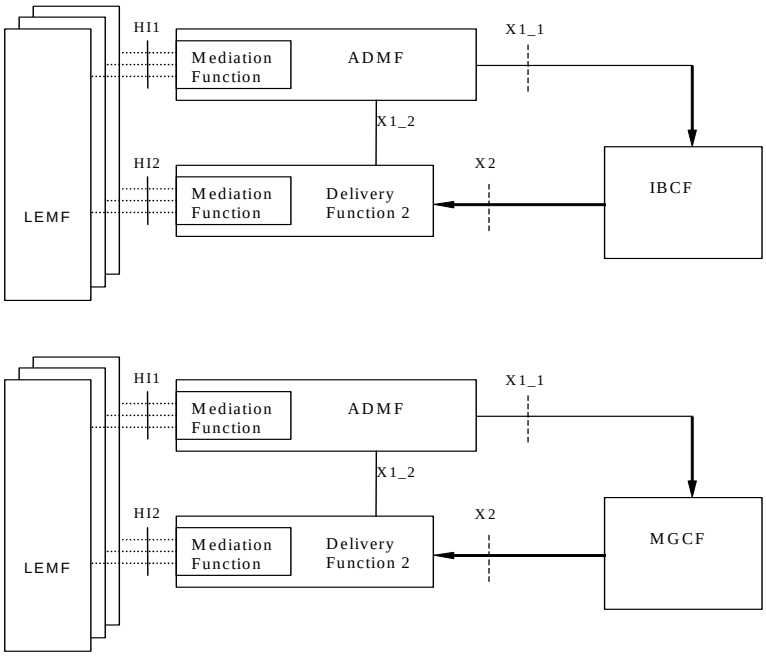


Figure 1i: Interception at IBCF and MGCF (only for Non-Local Target ID)

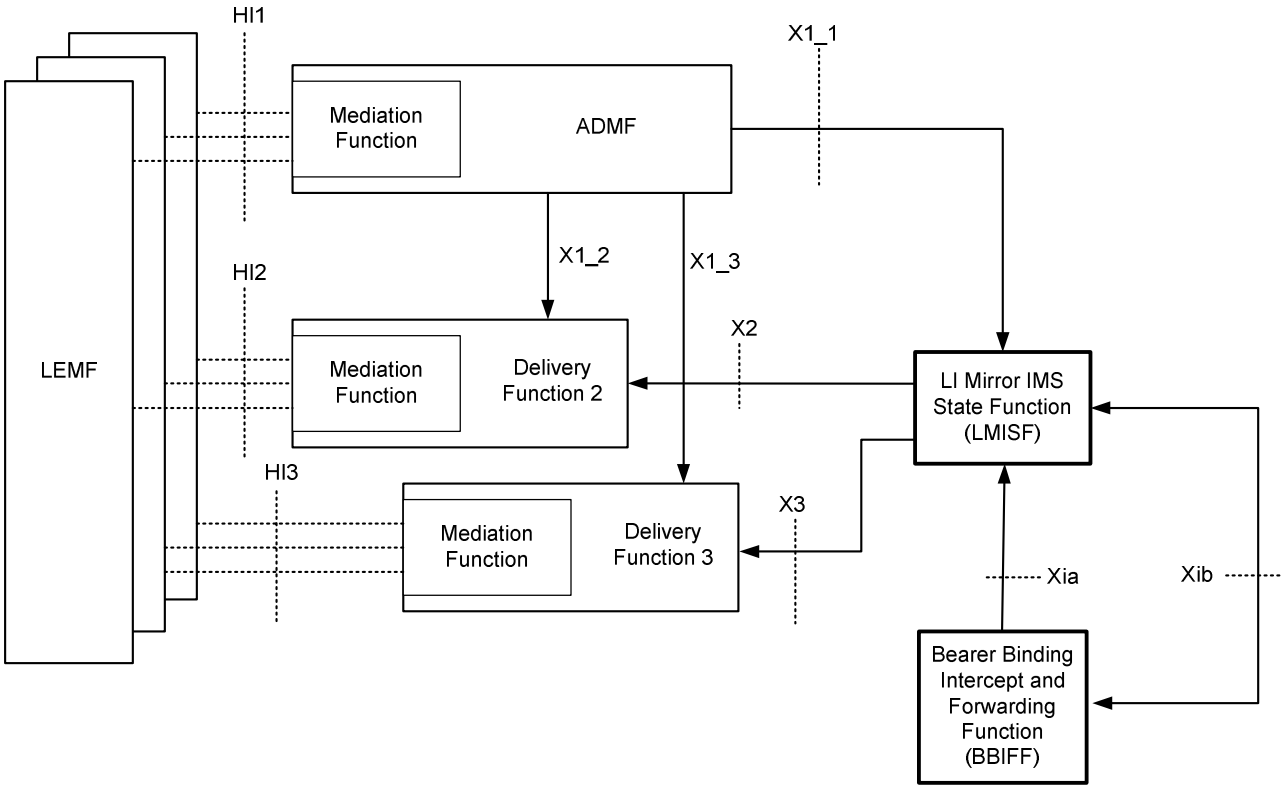


Figure 1j: S8HR VoLTE Intercept Configuration in the VPLMN

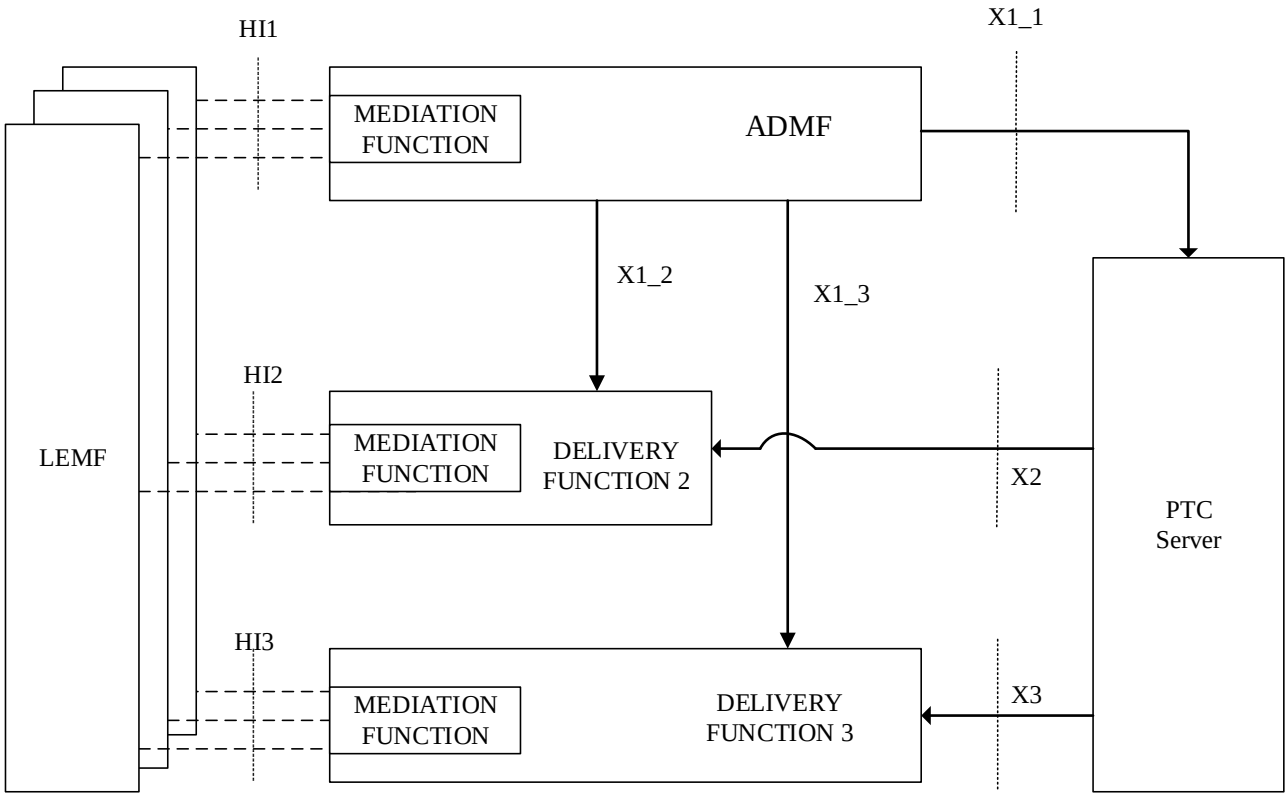


Figure 1k: PTC Interception configuration

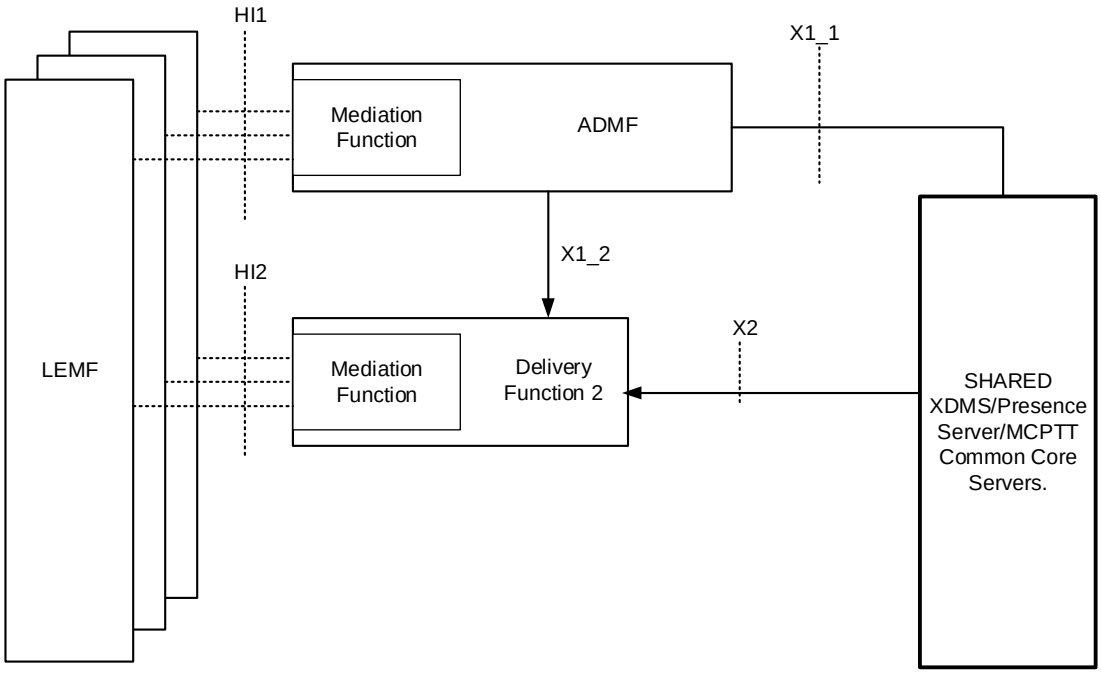


Figure 1l: PTC Interception configuration (Shared servers)

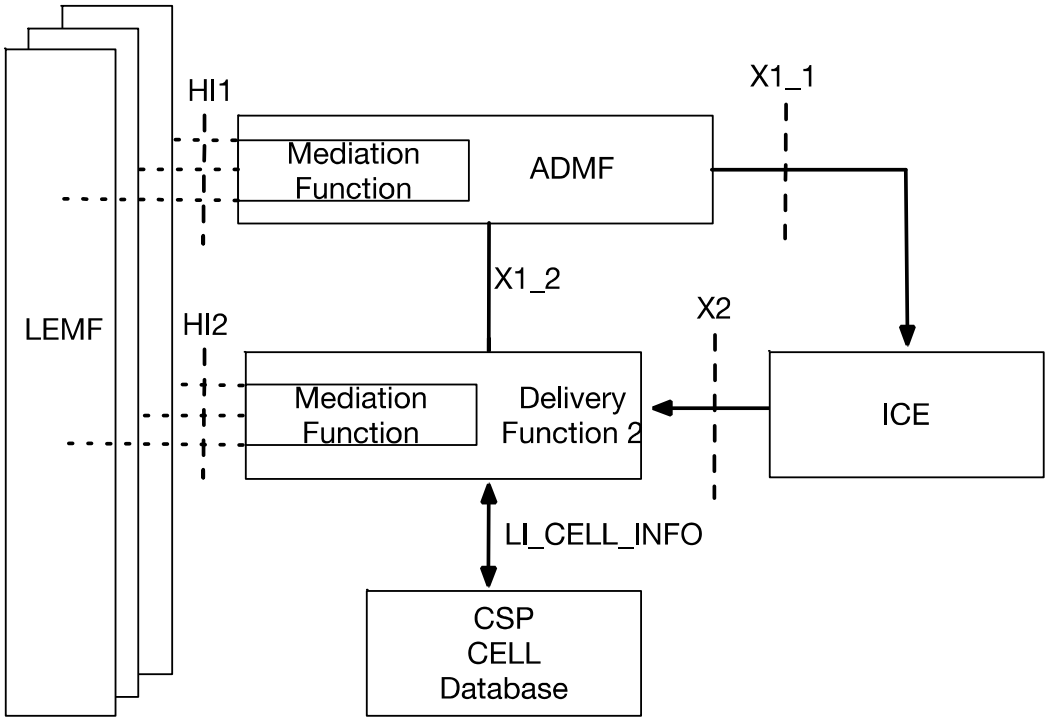


Figure 1m: CSP Cell Supplemental Information Database configuration

The LALS Triggering Function depicted in Figure 1h may be implemented as a part of either an ICE or a DF2.

See clause 20 for the definitions of LMISF and BBIFF. These functions are specifically defined for LI in reference to the interception voice services in the VPLMN when S8HR approach is used as the VoLTE roaming architecture.

The reference configuration is only a logical representation of the entities involved in lawful interception and does not mandate separate physical entities.

Regional Mediation Functions, which may be transparent or part of the administration and delivery functions, are used to convert information on the HI1, HI2 and HI3 interfaces in the format described in various national or regional specifications. For example, if ETSI ES 201 671 [3] or ANSI J-STD-025 [8] is used, then the adaptation to HI1, HI2 and HI3 will be as defined in those specifications.

There is one Administration Function (ADMF) in the network. Together with the delivery functions it is used to hide from the 3G ICEs that there might be multiple activations by different Law Enforcement Agencies (LEAs) on the same target. The administration function may be partitioned to ensure separation of the provisioning data from different agencies.

See the remaining clauses of this document for definitions of the X1_1, X1_2, X1_3, X2, X3, LALS_T, Xia and Xib interfaces. These interfaces are specifically defined for LI and are not related to other interfaces/reference points having the same name specified in other 3GPP specifications (such as e.g. X2 interface specified in the e-UTRAN architecture).

Interception at the Gateways is a national option. However, if 3G direct tunnel functionality with the GGSN is used in the network, as defined in TS 23.060 [10], then the GGSN shall perform the interception of IRI and the content of communications.

In figure 1a DF3 is responsible for two primary functions:

- Call Control (Signalling) for the Content of Communication (CC); and
- Bearer Transport for the CC.

HI3 is the interface towards the LEMF. It must be able to handle the signalling and the bearer transport for CC.

In figures 1a, 1b, 1e, 1f, 1g, 1h, 1i and 1j, the HI2 and HI3-interfaces represent the interfaces between the LEA and two delivery functions. The delivery functions are used:

- to distribute the Intercept Related Information (IRI) to the relevant LEA(s) via HI2 (based on IAs, if defined);
- to distribute the Content of Communication (CC) to the relevant LEA(s) via HI3 (based on IAs, if defined).

In figures 1c, 1d and 1h the HI2 interface represents the interface between the LEA and the delivery function. The delivery function is used to distribute the Intercept Related Information (IRI) to the relevant LEA(s) via HI2.

Figure 1g shows the CC interception configuration for VoIP. The trigger for the CC interception is provided by a SIP signalling node and identified within the figures as CC Interception Triggering Function.

Figure 1m shows the CSP Cell Supplemental Information configuration that has an optional interface (shown as LI_CELL_INFO) connecting the DF2 and the CSP maintained record(s). This interface is implementation specific to the operator. This is used to obtain cell supplemental information held by the CSP and provide it to the LEA. In particular it delivers geo-location or civic location of the cell site to the LEA. More detail is contained in clause 22.

NOTE 2: With reference to figure 1c, CC interception does not apply to HLR.

NOTE 3: For IMS, figure 1d relates to the provision of IRI for SIP messages handled by the CSCF. Interception of CC for this case can be done at the GSN under a separate activation and invocation, according to the architecture in Figure 1b (see also clause 7.A.1). For CC interception of VoIP, see figure 1g.

NOTE 4: If an operator is required to support "HI1 notification over HI2" TS 33.108 [11], the X1_2 interface carries the information coming from the ADMF to the DF2/MF that will be conveyed to the LEMF.

5 Activation, deactivation and interrogation

5.0 General

Figure 2 is an extraction from the reference intercept configuration shown in figures 1a through to 1j which is relevant for activation, deactivation and interrogation of the lawful interception.

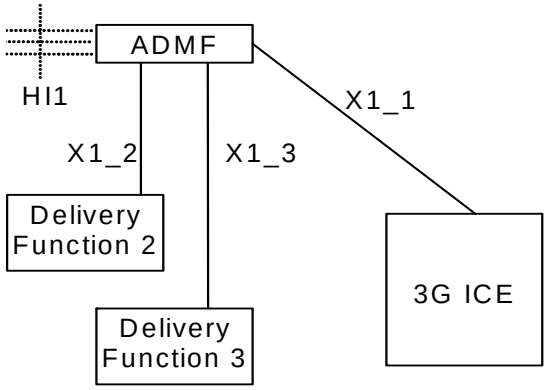


Figure 2: Functional model for Lawful Interception activation, deactivation and interrogation

In addition to the typical 3G ICEs functional entities, a new functional entity is introduced - the ADMF - the Lawful Interception administration function. The ADMF:

- interfaces with all the LEAs that may require interception in the intercepting network;
- keeps the intercept activities of individual LEAs separate;
- interfaces to the intercepting network.

Every physical 3G ICE is linked by its own X1_1-interface to the ADMF. Consequently, every single 3G ICE performs interception (activation, deactivation, interrogation as well as invocation) independently from other 3G ICEs. The HI1-interface represents the interface between the requester of the lawful interception and the Lawful administration function; it is included for completeness, but is beyond the scope of standardisation in this document.

For VoIP CC Interception, the CC Interception Triggering Function and the CC Intercept Function are treated as one 3G ICE from a Lawful Interception administration perspective.

The target identities for 3GMS CS and PS interception at the SGSN, GGSN, 3G MSC Server and 3G GMSC Server can be at least one of the following: IMSI, MSISDN (or E.164 number for optional Non-Local ID) or IMEI.

NOTE 1: Some communication content during a mobility procedure might not be intercepted when interception is based on MSISDN (only PS interception) or IMEI. The use of the IMSI does not have this limitation. For the availability of the target identities IMSI, MSISDN and IMEI (PS interception), refer to TS 23.060 [10].

The target identities for multi-media at the CSCF can be one or more of the following: SIP URI, TEL URI, or IMEI. Other identities are not defined in this release. The same identities (where available) are used as target identities for VoLTE interception in the VPLMN with S8HR. For VoLTE interception in the VPLMN with S8HR, the ADMF shall provision LMISF with the target identities.

The target identities for 3GPP WLAN Interworking interception can be MSISDN, IMSI or NAI. For the availability of the target identities in the I-WLAN nodes (AAA server, PDG, WAG), refer to TS 23.234 [14], TS 23.008 [15], TS 29.234 [16] and TS 24.234 [17].

NOTE 2: The NAI might be a temporary ID, therefore the use of MSISDN or IMSI is recommended.

NOTE 3: Void

NOTE 3A: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

The target identities for 3GPP HNB interception can be IMSI, MSISDN (or E.164 number for optional Non-Local ID), IMEI, or ME Id.

Use of the HNB ID or the CSG Identity as a target identity is FFS.

In the case of location dependent interception the following network/national options exist:

- target location versus Interception Areas (IAs) check in the 3G ICEs and Delivery Functions (DFs);
- target location versus IAs check in the DFs (physical collocation of the DFs to the 3G ICEs may be required by national law);
- location dependent interception is not applicable to CSCF.

NOTE 4: Void

The IA is previously defined by a set of cells. From the location of the target this set of cells permits to find the relevant IA.

NOTE 5: Void

It is not required that the 3G GMSC or the 3G GGSN are used for interception when Location Dependent Interception is invoked and the location of the target is not available.

NOTE 6: Location dependent intercept for the 3G MSC Server is not defined for this release.

The ADMF shall be able to provision P-CSCFs independently from S-CSCFs. If both P-CSCFs and S-CSCFs are administered within the network for intercept, redundant multi-media IRI may be presented to the agency as a result.

When Non-Local ID interception is required by national regulation, the ADMF shall be able to provision S-CSCF, P-CSCF, IBCF and MGCF independently of each other with the Non-Local ID as the target ID along with an indication that it is for a Non-Local ID interception, and nature of the interception (i.e. incoming calls and/or outgoing calls).

5.1 Activation

5.1.0 General

Figures 3, 4 and 5 show the information flow for the activation of Lawful Interception.

5.1.1 X1_1-interface

The messages sent from the ADMF to the 3G ICEs (X1_1-interface) contain the:

- target identities (MSISDN, IMSI, IMEI, SIP URI or TEL URI, NAI) (see notes 4, 5, 6);
- information whether the Content of Communication (CC) shall be provided (see note 1);
- address of Delivery Function 2 (DF2) for the intercept related information (see note 2);
- address of Delivery Function 3 (DF3) for the intercepted content of communications (see note 3);
- IA in the case of location dependent interception:
- indication whether the LALS Enhanced Location for IRI shall be provided. This indication is used to arm the LALS Triggering Function in the case when the LALS Triggering Function is associated with the ICE;
- type of location report required (immediate or periodic) in the case of Target Positioning provision;
- address of SX3LIF if CUPS is supported.

NOTE 1: Void

As an option, the filtering whether intercept content of communications and/or intercept related information has to be provided can be part of the delivery functions. (Note that intercept content of communications options do not apply at the CSCF, HLR, LI LCS Client and AAA server). If the option is used, the corresponding information can be omitted on the X1_1-interface, while "information not present" means "intercept content of communications and related information has to be provided" for the ICE. Furthermore the delivery function which is not requested has to be "pseudo-activated", in order to prevent error cases at invocation.

NOTE 2: Void

As an option, only a single DF2 is used by and known to every 3G ICE. In this case the address of DF2 can be omitted.

NOTE 3: Void

As an option, only a single DF3 is used by and known to every 3G ICE (except at the CSCFs, HLR, LI LCS Client and AAA server). In this case the address of DF3 can be omitted.

NOTE 4: Since the IMEI is not available, interception based on IMEI is not applicable at the 3G Gateway. Moreover, in case the IMEI is not available, interception based on IMEI is not applicable at 3G ICEs.

NOTE 5: Void

Interception at the CSCFs is based upon either SIP URI, TEL URI or IMEI. The interception at the LMISF is also based on SIP URI, TEL URI or IMEI. SIP URI and TEL URI as target identities are not supported by the other ICEs. The related CC interception also uses the SIP URI, TEL URI or IMEI.

NOTE 6: Interception based on NAI is only applicable at AAA server, PDG, and WAG. As the NAI could be encrypted or based on temporary identity at the PDG and WAG, interception based on the NAI is not applicable in those cases in these nodes.

NOTE 7: Void

If after activation subsequent Content of Communications (CC) or Intercept Related Information (IRI) has to be activated (or deactivated) an "activation change request" with the same identity of the target is to be sent.

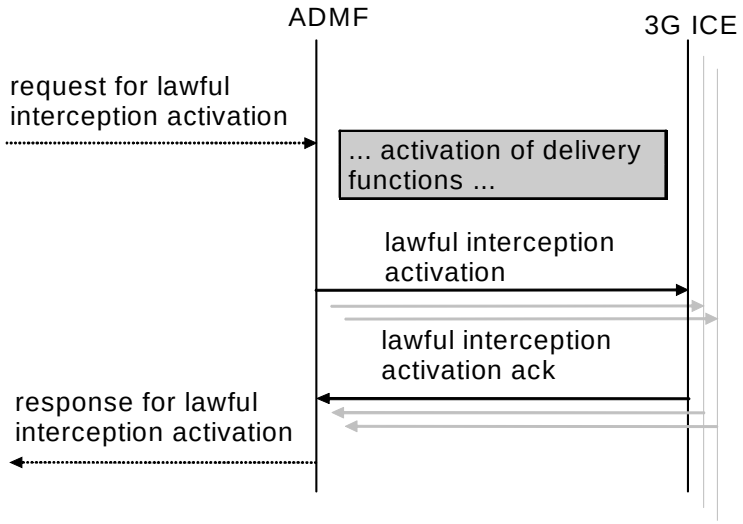


Figure 3: Information flow on X1_1-interface for Lawful Interception activation

Interception of a target can be activated on request from different LEAs and each LEA may request interception via a different identity. In this case, each target identity on which to intercept will need to be sent via separate activation messages from ADMF to the 3G ICEs on the X1_1-interface. Each activation can be for IRI only, or both CC and IRI.

When several LEAs request activation on the same identity and the ADMF determines that there is an existing activation on the identity, the ADMF may (as an implementation option) send additional activation message(s) to the 3G ICEs. When the activation needs to change from IRI only to CC and IRI an activation change message will be sent to the 3G ICEs.

In the case of a secondary interception activation only the relevant LEAs will get the relevant IRIs.

5.1.2 X1_2-interface (IRI)

For the activation of IRI the message sent from the ADMF to the DF contains:

- the target identity;
- the address(es) for delivery of IRI (= LEMF address);
  - optionally multiple addresses for distributed delivery of IRI to a single LEMF;
  - optionally a primary and failover address(es) for delivery of IRI to either a single LEMF or two different LEMFs for the same LIID.
- Which subset of information shall be delivered;
- an indication whether the LALS Enhanced Location for IRI shall be delivered. This indication is used to arm the LALS Triggering Function in the case when the LALS Triggering Function is associated with the DF;
- a DF2 activation identity, which uniquely identifies the activation for DF2 and is used for further interrogation or deactivation, respectively;
- the IA in case of location dependent interception;
- interception of international outbound roaming IMS VoIP interception (allowed/not allowed);
- the warrant reference number if required by national option.

If a target is intercepted for several LEAs and/or several identities simultaneously, a single activation of delivery is necessary for each combination of LEA and identity.

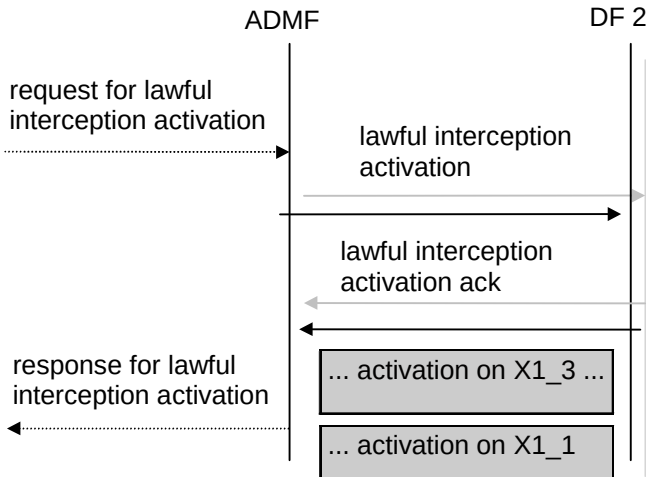


Figure 4: Information flow on X1_2-interface for Lawful Interception activation

5.1.3 X1_3-interface (CC)

For the activation of intercepted Content of Communications the message sent from the ADMF to the Delivery Function contains:

- the target identity;
- the address(es) of delivery for CC (= LEMF address);
  - optionally multiple addresses for delivery of CC to a single LEMF;
  - optionally a primary and failover address(es) for delivery of CC to either a single LEMF or two different LEMFs for the same LIID.
- A DF3 activation identity, which uniquely identifies the activation for DF3 and is used for further interrogation or deactivation, respectively;
- the IA in case of location dependent interception;
- interception of international outbound roaming IMS VoIP interception (allowed/not allowed);
- the warrant reference number if required by national option.

If a target is intercepted by several LEAs and/or several identities simultaneously, a single activation of delivery is necessary for each combination of LEA and identity.

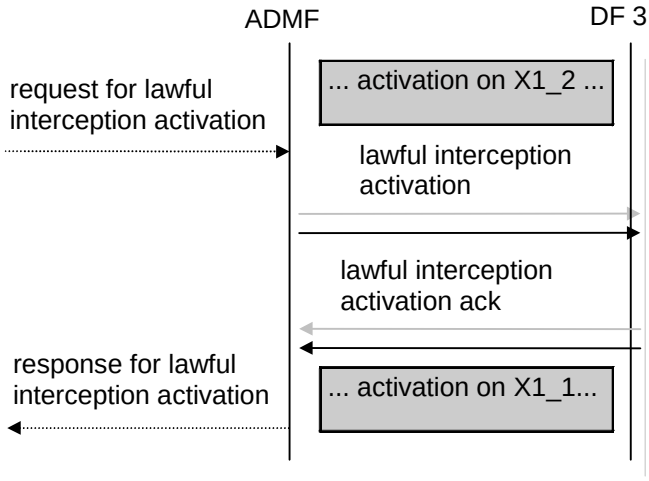


Figure 5: Information flow on X1_3-interface for Lawful Interception activation

5.2 Deactivation

5.2.0 General

Figures 6, 7 and 8 show the information flow for the deactivation of the Lawful interception.

5.2.1 X1_1-interface

The messages sent from the ADMF to the 3G ICEs for deactivation contain:

- the target identity;
- the possible relevant IAs in case of location dependent interception.

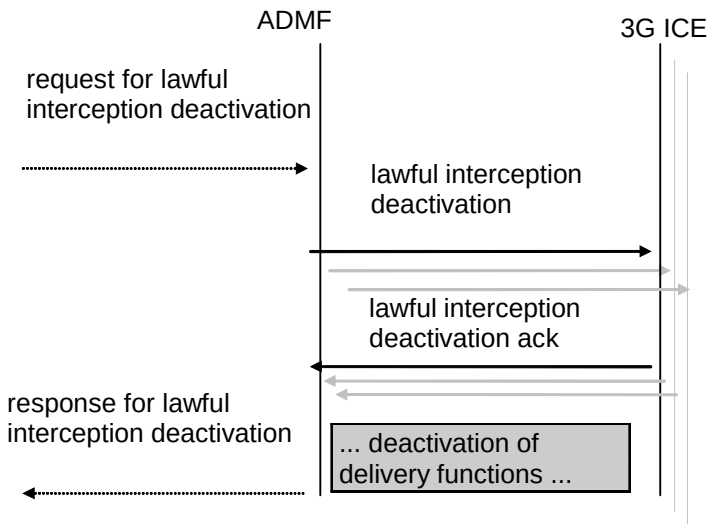


Figure 6: Information flow on X1_1-interface for Lawful Interception deactivation

If interception of a target has been activated via different identities then a separate deactivation message will need to be sent from the ADMF to the 3G ICEs for each identity.

When several LEAs requested activation on the same identity and subsequently request deactivation then the ADMF determines that there are remaining activations on the identity. In this case, the ADMF will not send a deactivation message to the 3G ICEs except when the activation needs to change from CC and IRI to IRI only. In that case an activation change message will be sent to the 3G ICEs.

5.2.2 X1_2-interface (IRI)

The message(s) sent from the ADMF to Delivery Function 2 for the deactivation of the Intercept Related Information contains:

- a DF2 activation ID, which uniquely identifies the activation to be deactivated for DF2.

If a target is intercepted by several LEAs and/or several identities simultaneously, a single deactivation is necessary for each combination of LEA and identity.

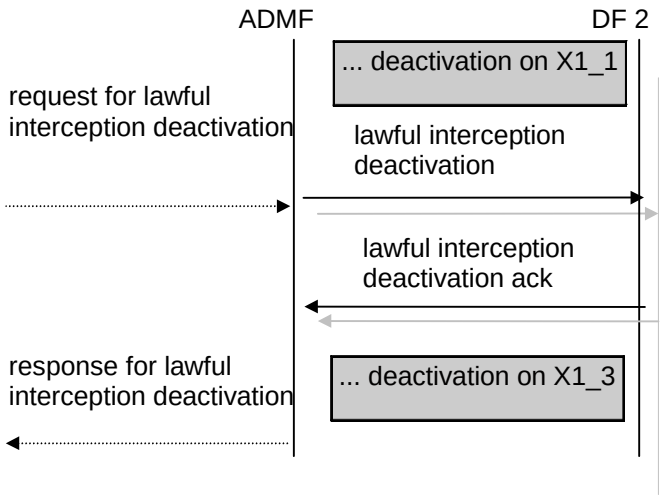


Figure 7: Information flow on X1_2-interface for Lawful Interception deactivation

5.2.3 X1_3-interface (CC)

For deactivating the delivery of the CC the message(s) sent from the ADMF to DF3 contains:

- a DF3 activation ID, which uniquely identifies the activation to be deactivated for DF3.

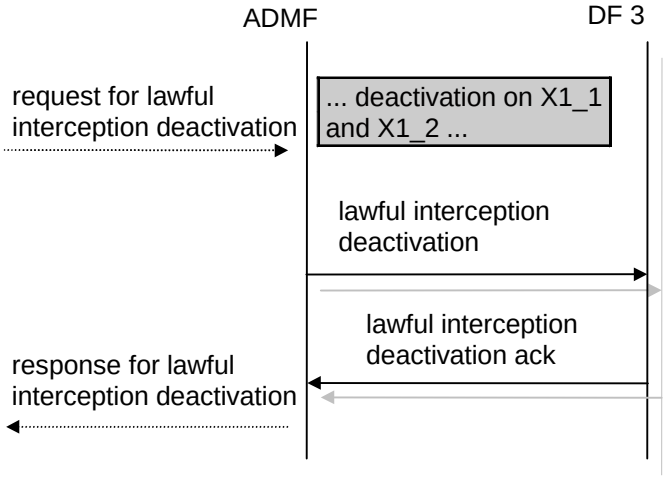


Figure 8: Information flow on X1_3-interface for Lawful Interception deactivation

5.3 Interrogation

5.3.0 General

Interrogation provides the current status of the interception activation in the system. Interrogation of all activations for a given LEA is an ADMF function.

5.3.1 Interrogation of the 3G ICEs

Figure 9 shows the information flow for the interrogation of the Lawful Interception. It shall be possible to interrogate:

- a specific activation at each relevant 3G ICEs;
- all activations at each relevant 3G ICEs.

As a result of the interrogation the activation status and data are returned.

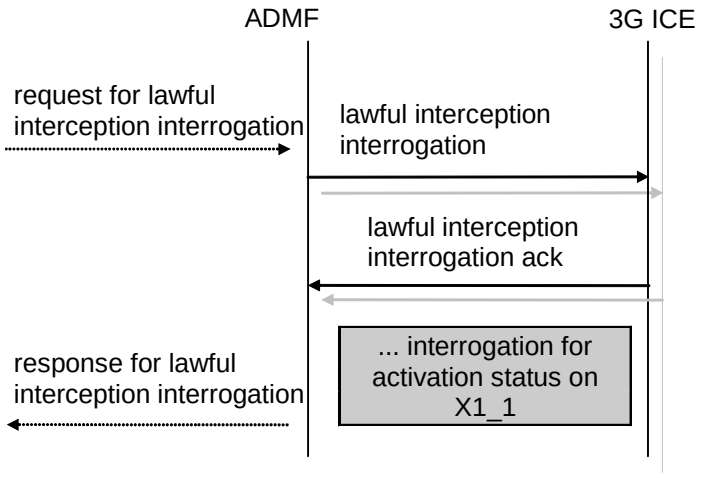


Figure 9: Interrogation of the Lawful Interception (3G ICEs)

5.3.2 Interrogation of Delivery Functions

Figure 10 shows the information flow for the interrogation of the Lawful Interception. It shall be possible to interrogate:

- a specific activation at a DF;
- all activations at a DF for a given target identity;
- all activations at a DF.

As a result of the interrogation the activation status and data are returned.

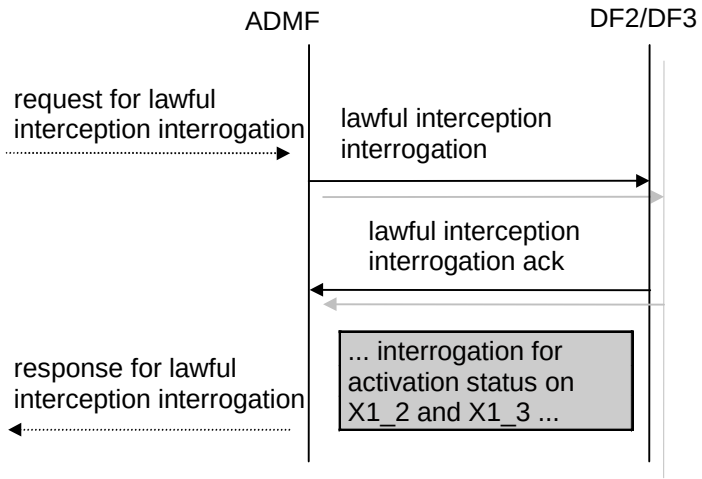


Figure 10: Interrogation of the Lawful Interception (Delivery Functions)

5A X Interfaces

5A.1 General

X interfaces as defined in clause 4 and used throughout the present document, are used to control interception (X1), transport intercepted IRI (X2) and CC (X3) to the MF/DF. This clause defines the use of standardised X interfaces.

X1, X2 and X3 as defined in the present document shall support the requirements in clause 5A.2, 5A.3 and 5A.4.

When circuit switched services defined in clause 6, are supported, requirements in 5A.2, 5A.3, and 5A.4 are optional for CS functions defined in clause 6.

ADMFs, MFs/DFs and points of interception (e.g. ICEs) may support already existing proprietary X interfaces.

NOTE: Deployments must ensure that X interfaces are only provided in network functions which are specifically required to support LI in a given CSP implementation.

5A.2 X1

5A.2.1 General

The X1 interface is used to activate, manage and terminate interception as defined in clause 5. The present document defines three X1 interfaces as follows:

X1_1 between the ADMF and the points of interception;

X1_2 between the ADMF and the MF/DF2;

X1_3 between the ADMF and the MF/DF3.

X1_1, X1_2, X1_3 shall support the use of ETSI TS 103 221-1 [89] for transport of X1 messages / information. However, default configurations, information element formats and other parameters as defined in the present document shall apply regardless of generic default options specified in TS 103 221-1 [89].

5A.2.2 X1 Detail

Editor's Note: This clause will define 3GPP specific use of TS 103 221-1 [89], including header parameters, mandatory parameters and other 3GPP specific issues. X1 message contents are defined in applicable service specific sections.

5A.3 X2

5A.3.1 General

The X2 interface is used to transport IRI from the point of interception to the MF/DF2. In the present document, service specific IRI required to be transported over the X2 interface is defined in subsequent network access or service clauses.

Support for fully standardised X2 is not defined in the present document.

5A.4 X3

5A.4.1 General

The X3 interface is used to transport CC from the point of interception to the MF/DF3. In the present document, service specific CC required to be transported over the X3 interface is defined in subsequent network access or service clauses.

Support for fully standardised X3 is not defined in the present document.

6 Invocation of Lawful Interception (LI) for Circuit Switched (CS) services

6.0 General

Figure 11 shows an extraction from the reference configuration in figure 1a which is relevant for the invocation of the lawful interception.

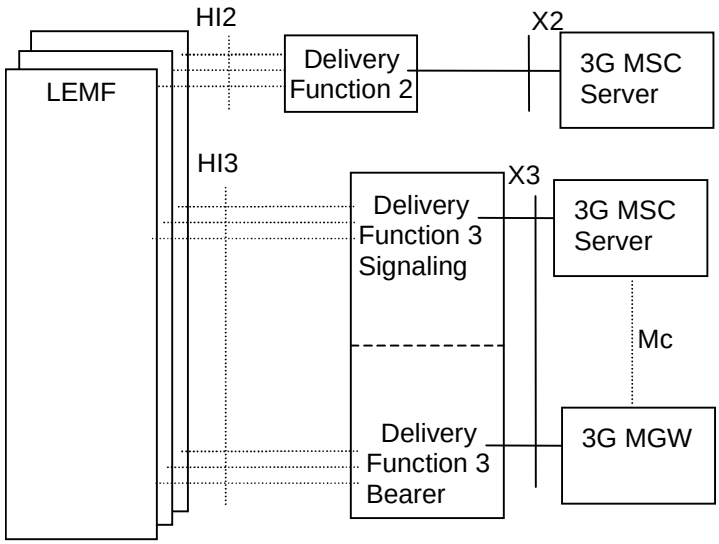


Figure 11: Functional model for Lawful Interception invocation

The HI2 and HI3 interfaces represent the interfaces between the LEMF and two delivery functions. Both interfaces are subject to national requirements. They are included for completeness, but are beyond the scope of standardization in this document. The delivery functions are used:

- to convert the information on the X2-interface to the corresponding information on the HI2-interface;
- to convert the information on the X3-interface to the corresponding information on the HI3-interface;
- to distribute the intercept related information to the relevant LEA(s) (based on IAs, if defined);
- to distribute the intercept content of communications to the relevant LEA(s) (based on IAs, if defined).

For the delivery of the CC and IRI, the 3G MSC Server provides a correlation number and target identity to the DF2 and DF3 which is used to select the different LEAs to which the product shall be delivered.

NOTE: Void

If interception has been activated for both parties of the call both CC and IRI will be delivered for each party as separate intercept activity.

The Mc interface between the 3G MSC Server and MGW is used to establish intercept and deliver the bearer to DF3.

When the Gateway MSC is anchoring the call and the call to target cannot be intercepted by the serving MSC within the same network, the Gateway MSC shall have the capability to limit interception to the following cases:

- call forwarding unconditional;
- roaming in another CSP’s network.

For Location Dependent Interception, the location dependency check occurs at the establishment of each call. Subsequent dependency checks for simultaneous calls are not required, but can be a national option.

If a target is marked using an IA in the 3G MSC Server, the 3G MSC Server shall perform a location dependency check at call set-up. Only if the target's location matches the IA then the call is intercepted.

If a target is marked using an IA in the DF2, the DF2 shall perform a location dependency check at reception of the first IRI for the call. Only if the target's location matches the IA for certain LEAs is IRI the relayed to these LEAs. All subsequent IRIs for the call are sent to the same LEAs.

If a target is marked using an IA in the DF3, the DF3 signalling function shall perform a location dependency check at reception of the CC. Only if the target's location matches the IA for certain LEAs is the CC relayed to these LEAs.

National regulations may require the interception based in the HLR, using the DF2 with a delivery through the HI2 interface.

When LALS is used to report location for CS services, the LI LCS Client shall deliver this using the DF2 through the HI2 interface. This is further defined in Clause 19.

6.1 Provision of Intercept CC - Circuit Switched

Figure 12 shows the access method for the delivering of CC. The access method shall be a bridged/ T-connection. Based on the mutual agreement between the intercepting CSPs and the LEAs, the CC may be delivered to the LEAs over CS-based or an IP-based handover interface. The system shall be able to support both handover methods for an intercepted call, since there can be multiple LEAs intercept the same call and the chosen approach for the handover interface may be different for different LEAs.

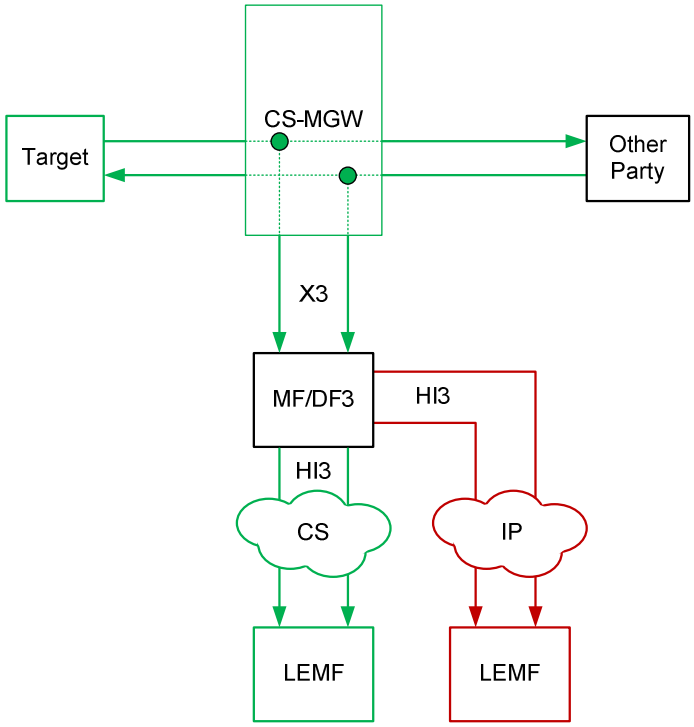


Figure 12: Example of delivery configuration to the LEMF for the interception of a circuit switched call

The figure 12 shows that CS-MGW provides the access point for the CC irrespective of the method used at the handover interface. With CS-based handover interface, the CC is delivered over CS circuits to the LEAs. With IP-based handover interface, the payload of the CC may be in the RTP (RFC 3550 [86]) format. The payload description (e.g. codec information) is sent along with the CC to the LEAs.

See Annex L for informative architectural descriptions related to the use of IP-based handover interface for delivering the CC to LEAs.

The signals of both parties of the configuration to be intercepted are delivered separately to the LEMF. The delivery function has no impact on the connection between the subscribers.

The two stublines towards the LEMF are established in parallel to the call set up. For both stublines the address is used which has been provided during activation.

Bearer, and only bearer, is sent from the MGW to the bearer function of DF3.

NOTE 1: Void

For data calls it is necessary to provide means for fast call establishment towards the LEMF to help ensure that the beginning of the data transmission is delivered.

The following information needs to be transferred from the 3G MSC Server to the DF3 in order to allow the DF3 to perform its functionality:

- target identity (MSISDN or E. 164 Number (for optional Non-Local ID), IMSI or IMEI, for DF3 internal use only);
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of location (if target location provided);
- correlation number (IRI <-> CC);
- direction indication - (Signal from target or signal to target).

NOTE 2: Void.

Additional information may be provided if required by national laws.

6.2 Provision of CC - Short Message Service

Figure 14 shows an SMS transfer from the 3G MSC Server to the LEMF. Quasi-parallel to the delivery from / to the mobile subscriber a message, which contains the contents of the SMS with the header, is generated and sent via the Delivery Function 2 to the LEMF in the same way as the Intercept Related Information.

The IRI will be delivered to the LEMF:

- for a SMS-MO. Dependent on national requirements, delivery shall occur in the following cases:
  - when the 3G MSC receives the SMS from the target MS, or when the 3G MSC detects that an SMS is to the Non-Local ID target.
  - when the 3G MSC receives notification that the SMS-Centre successfully received the SMS that was originated from the target MS, or sent to the Non-Local ID target.
- for a SMS-MT. Dependent on national requirements, delivery shall occur in the following cases:
  - when the 3G MSC receives the SMS from the SMS-Centre when the SMS was originated from a Non-Local ID target, or will have to be sent to a target MS.
  - when the 3G MSC receives notification that recipient MS has received the SMS successfully. The recipient MS is the target MS when the SMS is sent to the target. The recipient MS may not be the target when the SMS was originating from a Non-Local ID target.

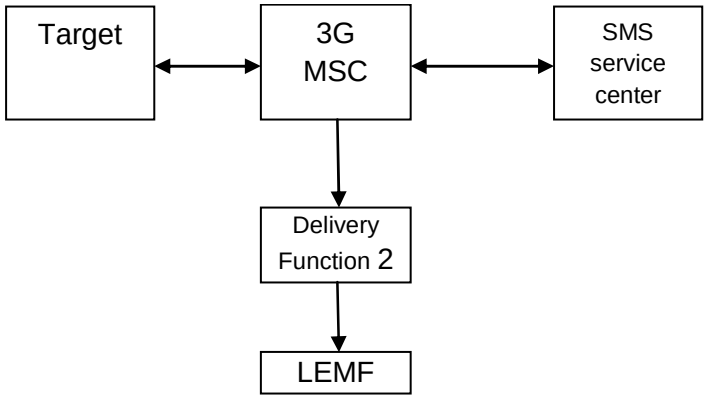


Figure 14: Provision of Content of Communication - Short Message Service

6.3 Provision of Intercept Related Information

6.3.0 General

Intercept Related Information (Events) are necessary at the Begin and End of the call, for all supplementary services during a call and for information which is not call associated. There are call related events and non-call related events.

On top of IRI generated by events from the 3G MSC Server, national regulations may require to complement them by IRI produced by a Delivery Function 2 associated to the HLR and/ or LI LCS Client.

Figure 15 shows the transfer of intercept related information to the DF2. If an event for / from a mobile subscriber occurs, the 3G MSC Server sends the relevant data to the DF2.

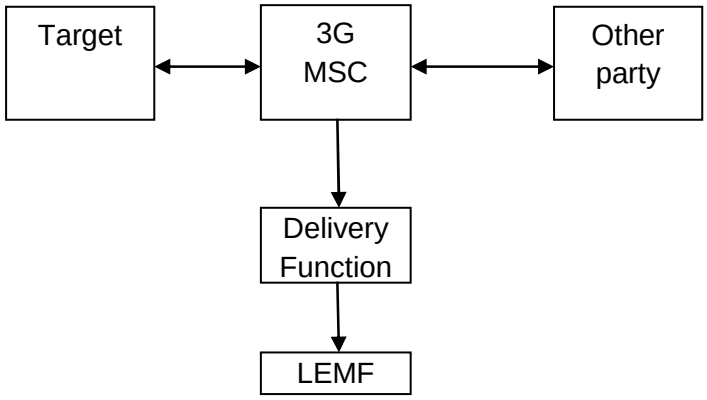


Figure 15: Provision of Intercept Related Information

6.3.1 X2-interface

The following information needs to be transferred from the 3G MSC Server or the HLR and/ or LI LCS Client to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (MSISDN, IMSI or IMEI);
- in case of location dependent interception, the IAs and/or target cell ID shall be provided;
- events and associated parameters as defined in clauses 6.3.3 and 6.3.4 may be provided.

The IRI should be sent to DF2 with a reliable transport mechanism.

6.3.2 Structure of the events

The information sent to DF2 is triggered by different call related and non-call related events/reports. Details are described in following clause. The events and reports for interception are configurable (if they are sent to DF2) in the 3G MSC Server, HLR and LI LCS Client. They can be suppressed in the DF2. The events are listed as follows:

Call Related Events (applicable to the 3G MSC Server):

- Call Establishment;
- Answer;
- Supplementary Service;
- Handover;
- Release.

Non Call Related Events (applicable to the 3G MSC Server):

- SMS;
- Location Update;

- Subscriber Controlled Input.

HLR Related Events:

- Serving System;
- HLR subscriber record change;
- Cancel location;
- Register location;
- Location information request;

LALS Reports (see Clause 19):

- Report for LALS Target Positioning;
- Report for LALS Enhanced Location for IRI.

Table 1 below shows the set of information that can be associated with the events. The events and LALS reports trigger the transmission of the information from the 3G MSC Server, HLR or from the LI LCS Client to DF2. Available IEs from this set of information can be extended in the 3G MSC Server, HLR or in the LI LCS Client, if this is necessary in a specific country. DF2 can extend available information if this is necessary in a specific country e.g. a unique number for each surveillance warrant.

Table 1: Information Elements for Circuit Event records

Observed MSISDN Target Identifier with the MSISDN of the target.
Observed IMSI Target Identifier with the IMSI of the target.
Observed IMEI Target Identifier with the IMEI of the target. It shall be checked for each call over the radio interface
Observed Non-Local ID Target Identifier with the E. 164 number of Non-Local ID target.
event type Description which type of event is delivered: Establishment, Answer, Supplementary service, Handover, Release, SMS, Location update, Subscriber controlled input, HLR subscriber record change, ServingSystem, cancel location, register location, location information request. In case of LALS report the event type is absent.
event date Date of the event generation in the 3G MSC Server or in the HLR, or the report generation in the LI LCS Client
event time Time of the event generation in the 3G MSC Server or in the HLR, the report generation in the LI LCS Client
dialled number Dialled phone number before digit modification, IN-modification etc.
Connected number Number of the answering party
other party address Directory number of the other party for MOC Calling party for MTC
call direction Information if the target is calling or called e.g. MOC/MTC or originating/ terminatingin or/out
Correlation number Unique number for each call sent to the DF, to help the LEA, to have a correlation between eachCall and the IRI
Network Element Identifier Unique identifier for the element reporting the ICE.
Location Information Location information is the service area identity and/or location area identity that is present at the 3G MSC Serveror at the HLR, and/ or as provided by the LI LCS Client at the time of event or report record production. Country and network IDs can be considered as location information. In some traffic cases the available location information can be the one received from the MME, i.e. the TrackingArea Identity (TAI) and/or the E-UTRAN Cell Global Identification (ECGI) as specified in the TS 23.272 [30].
Time of Location Date/Time of location. The time when location was obtained by the location source node.
basic service Information about Tele service or bearer service.
Supplementary service Supplementary services used by the target e.g. CF, CW, ECT
Forwarded to number Forwarded to number at CF
call release reason Call release reason of the target call
SMS initiator SMS indicator whether the SMS is MO, MT, or undefined
SMS Message The SMS content with header which is sent with the SMS-service
Redirecting number The number which invokes the call forwarding towards the target. This is provided if available.
SCI Non call related Subscriber Controlled Input (SCI) which the 3G MSC Server receives from the ME
Other update: Carrier specific information related to its implementation or subscription process on its HLR.
location error code LALS positioning error identification code

6.3.3 Call Related events

6.3.3.1 Call establishment

For call establishment a call establishment-event is generated. This event is generated at the beginning of a call when the 3G MSC Server attempts to reach the subscriber. This information will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Observed Non-Local ID
event type
event date
event time
dialled number
other party address
call direction
Correlation number
Redirecting number
Network Element Identifier
Location Information
Time of Location
basic service
Supplementary service

6.3.3.2 Answer

If the called party answers, an answer- event is generated. This information will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Observed Non-Local ID
event type
event date
event time
dialled number
other party address
Connected party
call direction
Correlation number
Redirecting number
Network Element Identifier
Location Information
Time of Location
basic service
Supplementary service

6.3.3.3 Supplementary Services

For supplementary services events are generated with the information which supplementary service is used e.g. Call Forwarding (CF), Call Waiting (CW), Explicit Call Transfer (ECT), Multi Party (MPTY), Call Hold and information correlated to the service like the forwarded to number. This information will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Observed Non-Local ID
event type
event date
event time
dialled number
other party address
call direction
Correlation number
Network Element Identifier
Location Information
Time of Location
basic service
Supplementary service
Forwarded to number

6.3.3.4 Handover

For each handover that is realised at the 3G MSC Server due to a change in target location information, a handover-event with the new location information is generated. This information will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
event type
event date
event time
Correlation number
Network Element Identifier
Location Information
Time of Location

6.3.3.5 Release

For the release or failed attempt of a target call, a release event with the following information is generated. This information will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Observed Non-Local ID
event type
event date
event time
dialled number
other party address
call direction
Correlation number
Network Element Identifier
Location Information
Time of Location
basic service
call release reason

6.3.4 Non Call Related events

6.3.4.1 SMS

For MO-SMS the event is generated in the 3G MSC Server. Dependent on national requirements, event generation shall occur either when the 3G MSC Server receives the SMS from the target MS (or from the party of the Non-Local ID target) or when the 3G MSC Server receives notification that the SMSC successfully receives the SMS; for MT-SMS the event is generated in the 3G MSC Server. Dependent on national requirements, event generation shall occur either when the 3G MSC Server receives the SMS from the SMSC or when the 3G MSC Server receives notification that the target MS (or from the party of the Non-Local ID target) successfully received the message. This information will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed Non-Local ID
event type
event date
event time
Network Element Identifier
Location Information
Time of Location
SMS initiator
SMS Message

6.3.4.2 Location update

For location updates a Location update-event is generated, with the new location information. This information will be delivered to the DF2 if available:

Observed MSISDN
observed IMSI
event type
event date
event time
Network Element Identifier
Location Information
Time of Location

6.3.4.3 Subscriber Controlled Input (SCI)

SCI includes subscriber initiated changes in service activation and deactivation. SCI does not include any information available in the CC. For subscriber controlled inputs - a SCI-event is generated with information about the SCI. This information will be delivered to the DF2 if available:

observed MSISDN
observed IMSI
event type
event date
event time
Network Element Identifier
Location Information
Time of Location
SCI

6.3.5 HLR Related events

6.3.5.1 Serving system

The Serving System report event is generated at the HLR, when the HLR has detected that the target has roamed, mainly with messages such as MAP_UPDATE_LOCATION (clause 8.1.2 of TS 29.002 [61]) or

MAP_SEND_AUTHENTICATION_INFO (clause 8.5 of TS 29.002 [61]). The elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Serving System Address (VLR Number...)

6.3.5.2 HLR subscriber record change

This event will be used to report any change of association between IMSI or MSISDN or IMEI of the target, mainly with messages such as MAP_INSERT_SUBSCRIBER_DATA or MAP_DELETE_SUBSCRIBER_DATA (clause of 8.8 of TS 29.002 [61]).

The following elements, such as old and new IMSI or MSISDN or IMEI will be delivered to DF2, if available:

New Observed MSISDN
Observed MSISDN
New Observed IMSI
Observed IMSI
New Observed IMEI (if available)
Observed IMEI (if available)
Event Type
Event Time
Event Date
Network Element Identifier (HLR id...)
IMSI or MSISDN or IMEI change type
Other update: carrier specific

NOTE: The change of IMEI can be detected by the HLR. Automatic Device Detection function clause 7.4 of TS 22.101 [60], may require IMEI to be notified to HLR especially in case of update location service, clause 8.1.2 TS 29.002 [61].

6.3.5.3 Cancel location

This event "Cancel Location" will be used to report to DF2 when HLR send to the 3G MSC Server one cancel location or purge to serving system. Any typical MAP message such as "MAP_CANCEL_LOCATION" (clause 8.1 of TS 29.002 [61]) or such as "MAP_PURGE_MS" (clause 8.1.6 of TS 29.002 [61]) could trigger the generation of information to the DF2, as soon as it has the following elements below, and least the previous serving system identifiers of the target.

The following elements will be delivered to DF2:

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HLR Id...)
Previous serving system identifiers (VPLMN id, VLR Number, MSC Number…)

6.3.5.4 Register location

This event will be used to report one update location message to the HLR for a target. A typical MAP message such as "MAP_SEND_AUTHENTICATION" (clause 8.5 of TS 29.002 [61]) could trigger the generation of information to the DF2. The elements of previous and current serving system ID will be delivered to DF2, if available:

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HLR id...)
Previous serving system identifier (Previous VPLMN id)
Current serving system identifier (Current VPLMN id)

6.3.5.5 Location Information request

This event will be used to report any location information of the target request activity from any interworking node, such as SMS Centre or IP-SM-GW or GMLC or from a GMSC (case of call transfer or ported number) that are not a part of HPLMN. Typical messages that have to trigger the transfer of information to DF2 are MAP-ANY-TIME-INTERROGATION (clause 8.11.1 of TS 29.002 [61]) or MAP-SEND-ROUTING-INFO (clause 10.1.2 of TS 29.002 [61]) or MAP-SEND-ROUTING-INFO-FOR-SM (clause 12.1 of TS 29.002 [61]), but only in roaming case.

The elements, observed IMSI, MSISDN, the identifier of the requesting node type and network, will be delivered to DF2, if available:

Observed MSISDN
Observed IMSI
Requesting network identifier (country identifier included)
Requesting node type
Event Type
Event Time
Event Date
Network Element Identifier (HLR id...)

NOTE: Void

In addition to the E 164 identity of a location requesting network node, i.e. MT SMS Target Node identity or SMS Router, the presence of Diameter Name/Realm shall be provided (clause 12.1.4 of TS 29.002 [61]).

6.4 Intercept cases for circuit switched supplementary services

6.4.1 Interception of Multiparty call

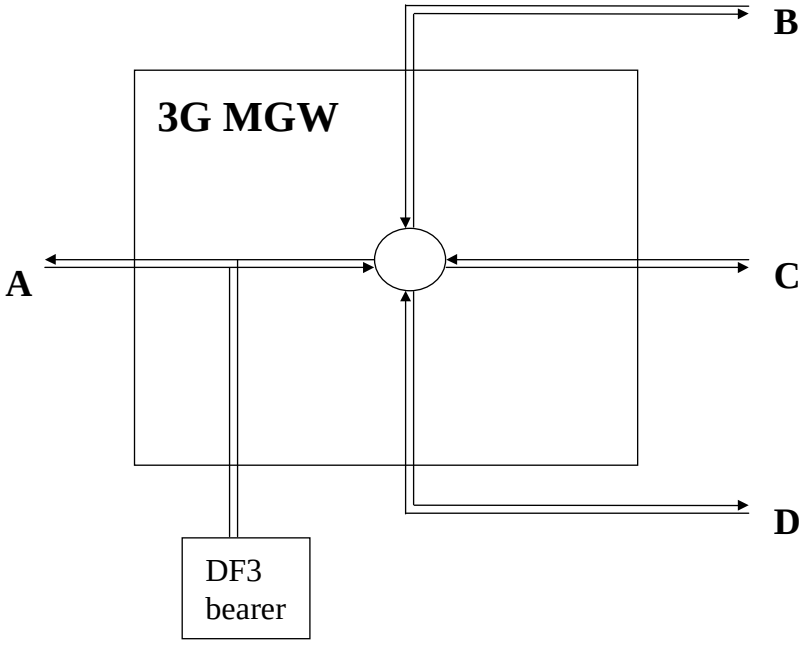


Figure 16: Interception of Multiparty for CC

Figure 16 shows the delivery of CC from intercepted multiparty call where party A is the target of interception.

One pair of call content channels are delivered to the delivery function. Party A is delivered to the DF3 on one channel and the sum of the balance of the parties, B,C and D is delivered on the second channel.

It should be noted that if parties B,C or D is a target of interception, that intercept is treated as a simple call intercept.

The events contain information about B, C and D if subscriber A is monitored. If one of B, C or D is monitored, events contain the information about A but not the other parties of the conference.

6.4.2 Interception for Call Forwarding / Call Deflection / ECT

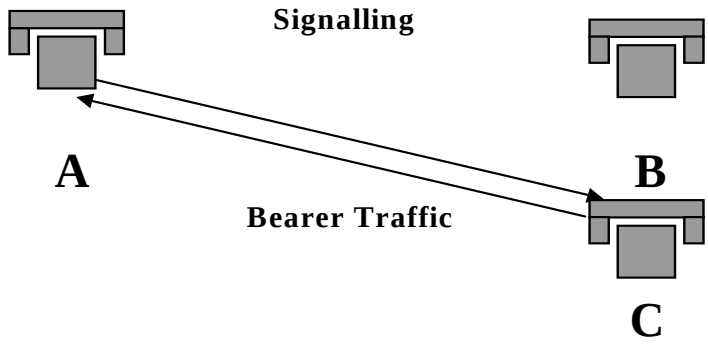


Figure 17: Interception for Call Forwarding / Deflection / ECT

The interception of party B once the supplementary service is invoked is a national option.

For Intercept Related Information it depends who is monitored:

- If subscriber A is monitored the number of A and B are mandatory in the event information and the number of C if available.
- If subscriber B is monitored the number of B and C are mandatory in the event information and the number of A if available.
- If subscriber C is monitored the number of C is mandatory in the event information and the number of A and B if available.

Intercept requirements for CS multi-media is not defined in this release.

7 Invocation of Lawful Interception for GSN Packet Data services

7.0 General

Figure 18 shows the extract from the reference configuration which is relevant for the invocation of the Lawful Interception of the packet data GSN network.

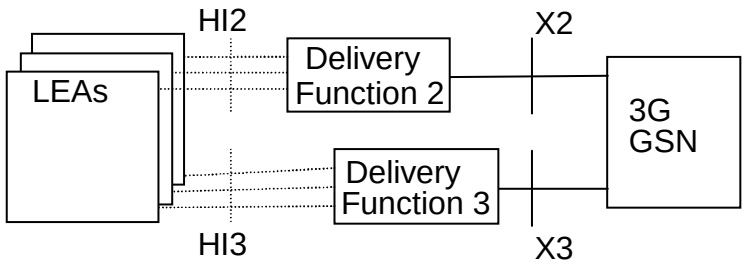


Figure 18: Functional model for Packet Data GSN Network Lawful Interception invocation

The HI2 and HI3 interfaces represent the interfaces between the LEA and two delivery functions. Both interfaces are subject to national requirements. They are included for completeness, but are beyond the scope of this specification. The delivery functions are used:

- to convert the information on the X2-interface to the corresponding information on the HI2 interface;
- to distribute the intercept related information to the relevant LEA(s);
- to distribute the intercept product to the relevant LEA(s).

For the delivery of the CC and IRI the 3G SGSN and/or, per national option 3G GGSN provides correlation number and target identity to the DF2 and DF3 which is used there in order to select the different LEAs where the product shall be delivered. When the SGSN connects an UE to a S-GW through the S4 interface (TS 23.060 [10], see also note 3), the SGSN is not required to provide CC for that communication (see note 4).

The correlation number is unique in the whole PLMN and is used to correlate CC with IRI and the different IRI's of one PDP context.

The correlation number shall be generated by using existing parameters related to the PDP context.

When the SGSN connects an UE to a S-GW through the S4 interface (TS 23.060 [10], see also note 3), the SGSN is not required to provide IRIs for PDP contexts associated with CC and correlation for that communication (see note 4).

NOTE 1: Void

If interception has been activated for both parties of the Packet Data communication both CC and IRI shall be delivered for each party as separate intercept activity.

In case of location dependent interception:

- for each target, the location dependency check occurs at each Packet Data session establishment or release and at each Routing Area (RA) update to determine permanently the relevant IAs (and deduce, the possible LEAs within these IAs);

- concerning the IRI:

  - when an IA is left, either a Mobile Station Detach event is sent when changing servicing 3G GSNs, or an RA update event is sent;

  - RA update event is sent to DF2 when changing IAs inside the same servicing 3G SGSN;

  - when a new IA is entered a RA update event is sent to DF2 and, optionally, a "Start of interception with PDP context active" event for each PDP context;

- concerning the CC, when crossing IAs, the CC is not sent anymore to the DF3 of the old IA but sent to the DF3 of the new IA.

Both in case of location dependent and location independent interception:

"Start of interception with PDP context active" event is sent by the new SGSN if an Inter-SGSN RA update procedure, which involves different PLMNs, takes place for a target, which has at least one active PDP context.

NOTE 2: An SGSN can differentiate "Inter PLMN" type of Inter-SGSN RA update procedure from "Intra PLMN" type of Inter-SGSN RA update procedure by inspecting the old RAI parameter, which is being received by the SGSN as part of the procedure (see TS 23.060 [10], clause 6.9.1.2.2 and TS 23.003, clause 4.2).

Optionally, it is possible to send "Start of interception with PDP context active" for all cases of inter- SGSN RA update when at least one PDP context is active.

NOTE 3: S4 is an intra-PLMN reference point between the SGSN and the S-GW.

NOTE 4: Void

When the SGSN connects an UE to a S-GW through the S4 interface, the S-GW provides IRI, CC and correlation for the EPS bearer associated to the PDP context, as specified in clause 12.

National regulations on a per interception basis may limit delivery of communications (CC and IRI) of an outbound international roaming target by the HPLMN as described in clause 5.1.4 of TS 33.106 [7].

If roaming interception is not allowed in the HPLMN and it is determined that the target is outside the country, the HPLMN shall not report IRI and CC for the target’s.

Non-communications-associated IRI (e.g. those identified by the HSS) are not affected by this requirement.

7.1 Provision of Intercept Product - Short Message Service

Figure 19 shows an SMS transfer from the 3G SGSN node to the LEA. Quasi-parallel to the delivery from / to the mobile subscriber a SMS event, which contains the content and header of the SMS, is generated and sent via the Delivery Function 2 to the LEA in the same way as the Intercept Related Information. National regulations and warrant type determine if a SMS event shall contain only SMS header, or SMS header and SMS content. Non-Local ID targeting is optional and may require traffic analysis.

The IRI will be delivered to the LEA:

- for a MO-SMS. Dependent on national requirements, delivery shall occur in the following cases:

  - when the 3G SGSN receives the SMS from the target MS, or when the 3G SGSN detects that an SMS is to the Non-Local ID target.

  - when the 3G SGSN receives notification that the SMS-Centre successfully received the SMS that was originated from the target MS, or sent to the Non-Local ID target;

- for a MT-SMS. Dependent on national requirements, delivery shall occur in the following cases:

  - when the 3G SGSN receives the SMS from the SMS-Centre when the SMS was originated from a Non-Local ID target, or will have to be sent to a target MS.

- when the 3G SGSN receives notification that recipient MS has received the SMS successfully. The recipient MS is the target MS when the SMS is sent to the target. The recipient MS may not be the target when the SMS was originating from a Non-Local ID target.

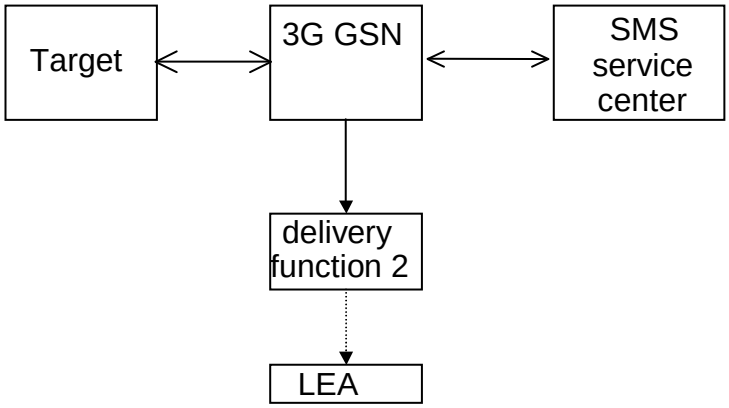


Figure 19: Provision of Intercept Product - Short Message Service

7.2 Provision of Intercepted Content of Communications - Packet data GSN services

7.2.0 General

The access method for the delivering of Packet Data GSN Intercept Product is based on duplication of packets without modification at 3G GSN. The duplicated packets with additional information in a header, as described in 7.2.1, are sent to DF3 for further delivery to the LEA.

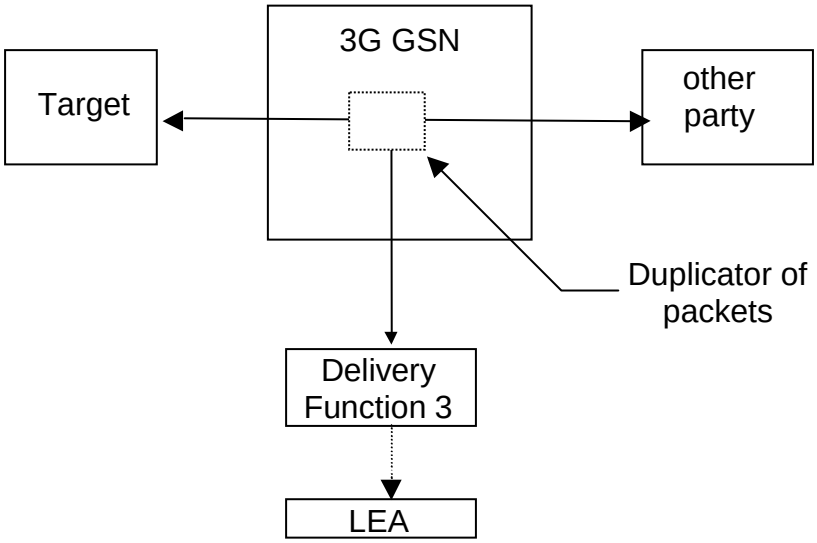


Figure 20: Configuration for interception of Packet Data GSN product data

7.2.1 X3-interface

In addition to the intercepted content of communications, the following information needs to be transferred from the 3G GSN to the DF3 in order to allow the DF3 to perform its functionality:

- target identity;
- correlation number;
- time stamp - optional;
- direction (indicates whether T-PDU is MO or MT) - optional;

- the target location (if available) or the IAs in case of location dependent interception;
- date/time of location (if target location provided).

As a national option, in the case where the 3G GGSN is performing interception of the content of communications, the target is handed off to another SGSN and the same 3G GGSN continues to handle the content of communications subject to roaming agreements, the 3G GGSN shall continue to perform the interception of the content of communication.

If 3G direct tunnel functionality with the GGSN, as defined in TS 23.060 [10], is used in the network, then the GGSN shall perform the interception of the content of communications.

7.3 Provision of Intercept Related Information

7.3.0 General

Intercept Related Information (Events) are necessary at the Mobile Station Attach, Mobile Station Detach, PDP Context Activation, Start of intercept with PDP context active, PDP Context Deactivation, RA update, Serving System, Packet Data Header Information, and SMS events.

Other HLR, Non-Local ID targeting for SMS (e.g. based on traffic analysis), LI LCS Client related and Serving System events reporting are national options.

Packet Data Header Information reporting is a national option.

Figure 21 shows the transfer of intercept related information to the DF2. If an event for / from a mobile subscriber occurs, the 3G GSN, LI LCS Client or the Home Location Register (HLR) sends the relevant data to the DF2. For Packet Data Header Information reporting, a 3G GSN either isolates the relevant data and sends it to the DF2 or sends the packet stream to another entity in the network (e.g., DF3) for isolation which then provides the relevant data to the DF2.

See clause 7A for multi-media Intercept Related Information produced at the CSCF.

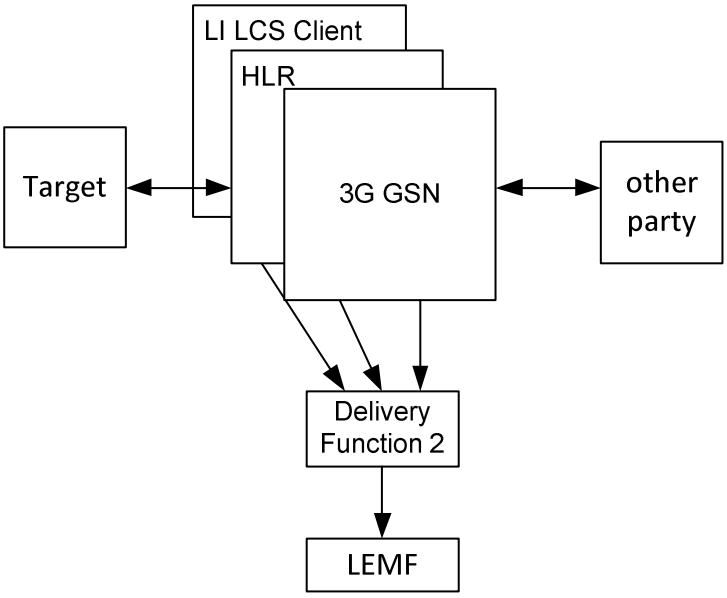


Figure 21: Provision of Intercept Related Information

7.3.1 X2-interface

The following information needs to be transferred from the 3G GSN, LI LCS Client or the HLR to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (MSISDN or E. 164 number for Non-Local ID, IMSI, IMEI);

- events and associated parameters as defined in clauses 7.3.2 and 7.4 may be provided;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of location (if target location provided);
- Correlation number;
- Quality of Service (QoS) identifier;
- Encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

The IRI should be sent to DF2 using a reliable transport mechanism.

The 3G GSN detects packets containing packet data header information in the communications path but the information needed for Packet Data Header Information reporting may need to be transferred from the 3G GSN either directly to the DF2 or via another entity in order to allow the DF2 to perform its functionality.

7.3.2 Structure of the events

There are several different events in which the information is sent to the DF2 if this is required. Details are described in the following clause. The events for interception are configurable (if they are sent to DF2) in the 3G GSN, LI LCS Client or the HLR and can be suppressed in the DF2.

The following events are applicable to 3G SGSN:

- Mobile Station Attach;
- Mobile Station Detach;
- PDP context activation;
- Start of interception with mobile station attached (national option);
- Start of intercept with PDP context active;
- PDP context modification;
- PDP context deactivation;
- RA update;
- SMS;
- Packet Data Header Information.

NOTE: Void

3G GGSN interception is a national option. Location information may not be available in this case. If interception is performed at the 3G GGSN, then Packet Data Header Information reporting shall also be performed at the 3G GGSN and not at the 3G SGSN.

If 3G direct tunnel functionality with the GGSN, as defined in TS 23.060 [10], is used in the network, then both the SGSN and the GGSN shall perform the interception of intercept related information.

When the SGSN connects an UE to a S-GW through the S4 interface (TS 23.060 [10]), the SGSN is not required to report events PDP context activation (successful), Start of intercept with PDP context active, PDP context modification, PDP context deactivation; the SGSN shall report unsuccessful PDP context activation event.

The following events are applicable to the 3G GGSN:

- PDP context activation;
- PDP context modification;
- PDP context deactivation;
- Start of interception with PDP context active;

- Packet Data Header Information.

The following events are applicable to the HLR:

- Serving System;
- HLR subscriber record change;
- Cancel location;
- Register location;
- Location information request.

The following LALS Reports are applicable to Packet Data services (see Clause 19):

- Report for LALS Target Positioning;
- Report for LALS Enhanced Location for IRI.

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from 3G GSN, LI LCS Client or HLR to DF2, perhaps via a MF in the case of Packet Data Header Information. Available IEs from this set of elements as shown below can be extended in the 3G GSN or HLR, if this is necessary as a national option. DF2 can extend available information if this is necessary as a national option e.g. a unique number for each surveillance warrant.

Table 2: Information Elements for Packet Data Event Records

Observed MSISDN MSISDN of the target.
Observed IMSI IMSI of the target.
Observed IMEI IMEI of the target, it shall be checked for each activation over the radio interface.
Old observed MSISDN Old MSISDN of the target before a change.
Old observed IMSI Old IMSI of the target before a change.
Observed Non-Local ID
Event type Description which type of event is delivered: MS attach, MS detach, PDP context activation, Start of intercept with PDP context active, PDP context deactivation, SMS, Serving System, Packet Data Header Information, Cell and/or RA update, HLR subscriber record change, Cancel location, Register location, Location information request. In case of LALS report the event type is absent.
Event date Date of the event generation in the 3G GSN or the HLR, or the report generation in the LI LCS Client.
Event time Time of the event generation in the 3G GSN or the HLR, or the report generation in the LI LCS Client. Timestamp shall be generated relative to GSN or HLR internal clock.
PDP address The PDP address of the target. Note that this address might be dynamic. In case the PDP type is IPv4v6, the parameter may carry two IP addresses.
Access Point Name The APN of the access point. (Typically the GGSN of the other party).
Location Information Location Information is the Service Area Identity (SAI), RAI and/or location area identity that is present at the GSN or present in the LI LCS Client at the time of event record production. Country and network IDs can be considered as location information.
Time of Location Date/Time of location. The time when location was obtained by the location source node.
Old Location Information Location Information of the subscriber before Routing Area Update
PDP Type The used PDP type.
Correlation Number The correlation number is used to correlate CC and IRI.
SMS The SMS content with header which is sent with the SMS-service. The header also includes the SMS-Centre address.
Network Element Identifier Unique identifier for the element reporting the ICE.
Failed attach reason Reason for failed attach of the target.
Failed context activation reason Reason for failed context activation of the target.
IAs The observed Interception Areas.
Initiator The initiator of the PDP context activation, deactivation or modification request either the network or the 3G MS.
SMS Initiator SMS indicator whether the SMS is MO or MT or undefined.
Deactivation / termination cause The termination cause of the PDP context.
QoS This field indicates the Quality of Service associated with the PDP Context procedure.
Serving System Address Information about the serving system (e.g. serving SGSN number or serving SGSN address).
NSAPI Network layer Service Access Point Identifier The NSAPI information element contains an NSAPI identifying a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control Plane. This is an optional parameter to help DF/MF and LEA's to distinguish between the sending mobile access networks when the GGSN is used as element of the PDG according TS 23.234 [14], Annex F.

ULI Timestamp Indicates the time when the User Location Information was acquired. The parameter is specified in TS 29.060 [37].
Destination IP Address The IP address, including type IPv4 or IPv6, of the destination of the IP packet.
Destination Port Number The port number of the destination of the IP packet.
Flow Label (IPv6 only) The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [41]).
Packet Count The number of packets detected and reported (for a particular summary period).
Packet Data Summary Reason The reason for a Packet Data Summary message being sent to the LEMF (e.g., timed out, counter expiration, end of session)
Packet Size The size of the packet. (i.e. Total Length Field in IPv4 or Payload Length field in IPv6)
Source IP Address The IP address, including type IPv4 or IPv6, of the source of the IP packet.
Source Port Number The port number of the source of the IP packet.
Sum of Packet Sizes (for a particular summary period) The sum of values contained in the Total Length fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.
Summary Period Includes the dates and times of the first and last packets in a particular packet data interval.
Transport Protocol (e.g. TCP) The identification of the transport protocol of the packet or packet flow being reported.
Other update: Carrier specific information related to its implementation or subscription process on its HLR.
IMSI or MSISDN or IMEI change type Identifies the type of subscriber information change in the HLR.
Previous serving system identifier The VPLMN ID of the previous serving system.
Current serving system identifier The VPLMN ID of the current serving system.
Requesting network identifier Is the identifier (including country identifier) of the network requesting the target's location.
Requesting node type Identifies the type of node in the requesting network that is requesting the target's location.
location error code LALS positioning error identification code

7.4 Packet Data related events

7.4.1 Mobile Station Attach

For attach an attach-event is generated. When an attach activation is generated from the mobile to serving 3G G SN this event is generated. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
Time of Location
Failed attach reason
IAs (if applicable)

7.4.2 Mobile Station Detach

For detach a detach-event is generated, this is for the common (end) detach. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
Time of Location
IAs (if applicable)

7.4.3 Packet Data PDP context activation

When a PDP context activation is generated a PDP context activation-event is generated. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
PDP address of observed party
Event Type
Event Time
Event Date
Correlation number
Access Point Name
PDP Type
Network Element Identifier
Location Information
Time of Location
Failed context activation reason
IAs (if applicable)
Initiator (optional)
QoS (optional)
NSAPI (optional)

7.4.4 Start of interception with PDP context active

This event will be generated if interception for a target is started and if the target has at least one PDP context active. If more than one PDP context is open, for each of them an event record is generated. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
PDP address of observed party
Event Type
Event Time
Event Date
Correlation number
Access Point Name
PDP Type
Network Element Identifier
Location Information
Time of Location
Old Location Information (optional)
IAs (if applicable)
QoS (optional)
Initiator (optional)
NSAPI (optional)

Presence of the optional Old Location Information field indicates that PDP context was already active, and being intercepted. However, the absence of this information does not imply that interception has not started in the old location SGSN for an active PDP context.

Start of interception with PDP context active shall be sent regardless of whether a Start of interception with mobile station attached has already been sent.

7.4.5 Packet Data PDP context deactivation

At PDP context deactivation a PDP context deactivation-event is generated. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
PDP address of observed party
Event Type
Event Time
Event Date
Correlation number
Access point name
Network Element Identifier
Location Information
Time of Location
IAs (if applicable)
Deactivation cause
Initiator (optional)
NSAPI (optional)
ULI Timestamp

7.4.6 RA update

For each RA update an update-event with the elements about the new location is generated. New SGSN shall send the event, and the old SGSN may optionally send the event as well. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Location Information (only for the new SGSN)
Time of Location
Old Location Information (only for the old SGSN)
IAs (if applicable)

NOTE: Once target moves out of the interception area, an RAU event reported by the old SGSN may not be comprehensive since normally, the old SGSN does not receive the new SGSN's RAI, while the new SGSN does receive the old SGSN's RAI from UE with the RAU Request message.

7.4.7 SMS

For SMS-MO, the event is generated in the 3G SGSN. Dependent on national requirements, event generation shall occur in the following cases:

- when the 3G SGSN receives the SMS from the target MS, or when the 3G SGSN detects that an SMS is to the Non-Local ID target.

- when the 3G SGSN receives notification that the SMS-Centre successfully received the SMS that was originated from the target MS, or sent to the Non-Local ID target.

For SMS-MT, the event is generated in the 3G SGSN. Dependent on national requirements, event generation shall occur in the following cases:

- when the 3G SGSN receives the SMS from the SMS-Centre when the SMS was originated from a Non-Local ID target, or will have to be sent to a target MS.

- when the 3G SGSN receives notification that recipient MS has received the SMS successfully. The recipient MS is the target MS when the SMS is sent to the target. The recipient MS may not be the target when the SMS was originating from a Non-Local ID target.

These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Observed Non-Local ID
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
Time of Location
SMS
SMS Initiator
IAs (if applicable)

7.4.8 Packet Data PDP context modification

This event will be generated if an active PDP context for the target is modified. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
PDP address of observed party
Event Type
Event Time
Event Date
Correlation number
Access Point Name
PDP Type
Network Element Identifier
Location Information
Time of Location
IAs (if applicable)
Initiator
QoS

7.4.9 Serving System

The Serving System report event is generated at the HLR, when the HLR has detected that the target has roamed. The elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Serving System Address

7.4.10 Start of interception with mobile station attached

This event will be generated if interception has started for the already attached target. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
Time of Location
IAs (if applicable)

7.4.11 Packet Data Header Information

7.4.11.0 Introduction

Packet Data Header Information reporting can be done either on a per-packet (i.e., non-summarized) basis or in a summary report.

7.4.11.1 Packet Data Header Report

This event is used to provide packet header reports on a per packet basis (non-summarized reporting) and is triggered by each packet sent or received by the target. These elements will be delivered either directly to DF2 or via another network entity if available:

Observed MSISDN
Observed IMSI
Observed IMEI
PDP address of observed party
Event Type
Event Time
Event Date
Correlation Number
Access Point Name
PDP Type
Network Element Identifier
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Packet Size
Flow Label (IPv6 only)

7.4.11.2 Packet Data Summary Report

This event is used to report:

1) the source and destination information derived from the packet headers, including:

   a) source and destination IP Addresses,

   b) IP next-layer protocol,

   c) Layer-4 ports, and

   d) Flow label, if the packet is IPv6

2) summary information for the number of packets and bytes transmitted or received by the target for each unique packet flow within a PDP context, and

3) the date and the time of the first and last packets associated with that packet flow. A packet flow is defined as the 6-tuple of source/destination IP address/port number and the layer 4 protocol, and PDP Context.

   IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported.

The event provides packet summary reports for each unique packet data session (PDP context) and packet flow, and is triggered by one of the following:

- start of a packet flow associated with a PDP Context
- an interim report for a packet flow associated with a PDP Context is to be reported
- end of a packet flow associated with a PDP Context (including end of the PDP Context itself).

An interim report can be triggered by

- The expiration of a configurable timer per intercept (called a Summary Timer). The Summary Timer is configurable in units of seconds;
- A per-intercept configurable count threshold is reached.

These elements will be delivered either directly to DF2 or via an MF for each packet flow if available:

Observed MSISDN
Observed IMSI
Observed IMEI
PDP address of observed party
Event Type
Event Time
Event Date
Correlation Number
Access Point Name
PDP Type
Network Element Identifier
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Flow Label (IPv6 only)
Summary Period
Packet Count (for this summary period)
Sum of Packet Sizes (for this summary period)

If the packets are IPv4, the sum of all observed packet sizes is the sum of the values contained in the Total Length field of each packet as specified in IETF RFC 791[39].

If the packet is IPv6, the sum of all observed packet sizes is the sum of the values contained in the Payload Length field for each packet as specified in IETF RFC 2460 [40].

If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report shall not be sent.

7.4.12 HLR subscriber record change

This event will be used to report any change of association between IMSI or MSISDN of the target.

The following elements, such as old and new IMSI or MSISDN will be delivered to DF2, if available:

New observed MSISDN
New observed IMSI
New observed IMEI
Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier (HLR id...)
IMSI or MSISDN or IMEI change type
Other update: carrier specific

7.4.13 Cancel location

This event "Cancel Location" will be used to report to DF2 when HLR send to SGN one cancel location or purge to serving system.

The following elements such as the previous serving system of the target will be delivered to DF2:

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HLR Id...)
Previous serving system identifier (VPLMN id…)

7.4.14 Register location

This event will be used to report one update location message to the HLR for a target. The elements of previous and current serving system ID will be delivered to DF2, if available:

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HLR id...)
Previous serving system identifier (Previous VPLMN id)
Current serving system identifier (Current VPLMN id)

7.4.15 Location information request

This event will be used to report any location information of the target request activity.

The elements, observed IMSI, MSISDN, the identifier of the requesting node type and network, will be delivered to DF2, if available:

Observed MSISDN
Observed IMSI
Requesting network identifier (country identifier included)
Requesting node type
Event Type
Event Time
Event Date
Network Element Identifier (HLR id...)

7.4.16 Void

7.5 Void

7.6 Interception of the Multimedia Messaging Service (MMS)

The Multimedia Messaging Service (MMS) is a service running over the 3GPP PS-domain. Both mobile originating and mobile terminating MMS messages must pass through PS domain GSN nodes en route to or from Multimedia Message

Service Centres (MMSCs). Therefore, interception of MMS messages shall be performed at the GSN in exactly the same way as for other PS-domain bearer services.

The GSN is not responsible for recovering individual MMS messages from the user PDP context IP stream.

No MMS specific HI2 records are defined to be delivered to the LEMF over the DF2 other than those listed in clause 7.4 of this specification. CC records shall be sent to the LEMF over the DF3 as specified in clause 7.3.

Interception of a user PDP context IP stream will occur as described in clause 7.2. Such a stream may or may not contain MMS messages.

7A Invocation of Lawful Interception for Packet Data Multi-media Service

7A.1 Provision of content of communications

Interception of the content of communications for GSN packet data services is explained in clause 7.2.. Activation and invocation of lawful interception for multi-media service only at the CSCF(s) does not produce interception of content of communications. Consequently, a separate activation and invocation of lawful interception must occur at a node that has access to the CC (e.g., in case of GPRS / UMTS (PS domain) interception of CC occurs at the GSN).

Interception at the GSN is only possible for a basic call. For the interception of content of communications of IMS-based voice services including CC for forwarded and transferred calls, refer to clause 15.

7A.1.A Decryption for IMS Media Plane Security

This clause describes how the TSP can meet the national requirements in Clause 5.1.2 of TS 33.106 [7] to deliver intercepted communications decrypted when the TSP uses TS 33.328 [25] IMS Media Plane Security options. If an ICE, in TSP IMS network using Security options TS 33.328 [25], allows interception of Content of Communication in clear then this clause does not apply.

If Session Description Protocol (SDP) Security Descriptions for Media Streams (SDES) is used, the DF2 shall identify the SDES keys from the SDP offer and SDP answer messages and provide the DF3 with the necessary SDES related parameters. In this case, the DF3 shall perform the decryption prior to delivery to the LEMF. For the CC delivered to the LEMF in a decrypted form, the DF2 shall remove the SDES keys when present from the SDP offer and SDP answer messages sent to the LEMF over HI2. The interface between the DF2 and DF3 to support the transfer of session keys is outside the scope of this specification.

When SDES is used in end-to-access edge mode, the P-CSCF shall intercept SDES keys from SDP messages and shall deliver them to the DF2.

If a Key Management Service (KMS) and Multimedia Internet KEYing ticket (MIKEY-TICKET) is used, the TSP may use the mechanism as defined in Clause 7A.7.1, which results in the DF2 receiving the sessions keys needed to decrypt the intercepted communications. Clause 7A.7.1 defines that the DF2 delivers the keys to the LEMF as IRI in order for the LEMF to decrypt the intercepted traffic.

If the network is to decrypt the content of communications prior to delivery to the LEMF via HI3, the DF2 shall provide the DF3 with the sessions keys as defined in Clause 7A.7.1 instead of to the LEMF. In this case, the DF3 shall perform the decryption prior to delivery to the LEMF. The interface between the DF2 and DF3 to support the transfer of session keys is outside the scope of this specification.

7A.2 Provision of IRI

7A.2.1 Provision of IRI with SIP messaging

SIP messaging is reported as Intercept Related Information for the interception of multi-media service. As shown in figure 22 below, all SIP messages executed on behalf of a target are subject to intercept at the S-CSCF and Optionally P-CSCF. Based upon network configuration, the ADMF shall provision P-CSCFs, or S-CSCFs, or both P-CSCFs and S-CSCFs with SIP URI, TEL URI, or IMEI target identifiers. For Non-Local ID interception, the target identifiers are SIP URI or TEL URI. These resulting intercepted SIP messages shall be sent to DF2 for mediation prior to transmittal across the HI2 interface.

For roaming scenarios, interception at the P-CSCF shall be Mandatory, in order to provide IRI Interception in the visited network, where the P-CSCF is located in the Visited Network. Where the P-CSCF is located in the Home Network, interception at the P-CSCF shall be Optional, subject to national regulation. When S8HR is the roaming architecture, the P-CSCF is located in the HPLMN. Refer to clause 20 for the description of related lawful interception capabilities.

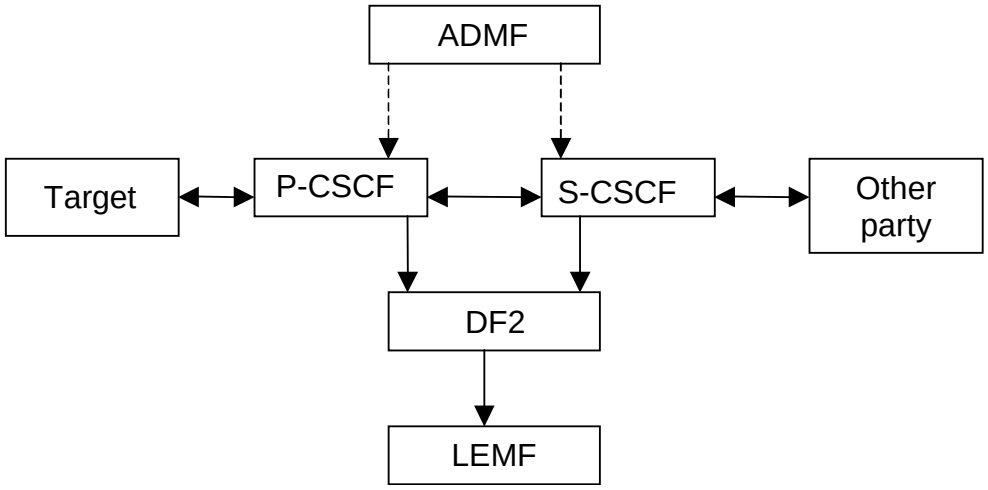


Figure 22: Provision of Intercept Related Information for multi-media

When Non-Local ID interception is required for incoming calls, ICE shall trigger interception by target id in any of the SIP headers used to identify the calling party information and redirecting party information present in the incoming SIP message. The examples are: P-Asserted Id, From headers and History-Info, Diversion headers.

When Non-Local ID interception is required for outgoing calls, ICE shall trigger interception by target id in any of the SIP headers used to identify the called party information present in the outgoing SIP message. The examples are: Request URI and To headers.

7A.2.2 Provision of IRI with XCAP messages

The AS that store the XCAP data of the target shall intercept and transmit to the DF2 any XCAP based messages related to actions by the target, related to the supplementary service and other target's service settings, defined in TS 24.623 [55]:

- on the Ut interface,
- on other interface to any AS with XCAP server capability that uses XCAP protocol.

The DF2 will encapsulate the information as an IRI to the LEMF.

NOTE 1: The XCAP services separation through XCAP filtering or the application of Operator Policy function for national regulation is outside of the scope of this specification as an implementation issue.

Every successful or unsuccessful IMS supplementary services setting modification management request and response between UEs and IMS service nodes, or from other access to the target's XCAP servers shall be reported. In case of IRI only, any filtering of XCAP messages based on operator policy or national regulation is for further studies.

NOTE 2: Report of events related to target's XCAP data and resources access by non XCAP protocol are for further studies.

7A.2.3 Provision of IRI with Diameter or MAP messages related to HSS

7A.2.3.0 General

National regulations may require IRI produced by a Delivery Function 2 associated to the HSS.

HSS shall support LI based on SIP-URI, Tel-URI, IMPI.

IMSI shall be supported as target identity if it is available in the subscription data stored in the HSS and the association with IMS identities can be done.

IMEI and MSISDN shall be supported as target identities if the HSS is shared with access services (e.g. PS, EPS) and the association with IMS identities can be done.

Intercept Related Information (Events) are listed as follows:

- Serving System;
- When IMPU or IMPI is changed in a HSS subscriber record change
- Registration termination
- Location information request.

Table 7A.2.3.0 below shows the set of information that may be associated with the events if available. The events trigger the transmission of the information from the HSS to DF2.

Table 7A.2.3.0: Information Elements for HSS Event records

Observed IMPI or Tel URI or SIP URI Target Identifier with the IMPI, Tel URI or SIP URI of the target (if available).
Observed IMSI Target Identifier with the IMSI of the target.
Observed IMEI Target Identifier with the IMEI of the target (if available).
Observed MSISDN Target Identifier with the MSISDN of the target (if available).
Event type Description which type of event is delivered: Subscriber record change, Serving System, Registration Termination, location information request.
Event date Date of the event generation in the HSS.
Event time Time of the event generation in the HSS.
Network Code (Country Code included) In case of roaming, the country code and the network code of the serving network, or of a third network in the diameter message to or from the HSS (AVP name such as Visited-PLMN-Id)
Network Element Identifier Unique identifier for the element reporting the ICE.
Reason of de-registration (Deregistration-Reason AVP, Reason-code AVP)
Serving System Identifier Provides an identifier that allows the home network to identify the visited network.
Any Associated-Identities (AVP Name): any change of any associated identities of the target
Other Public User Identities Other IMPU or IMPI that was allocated to Target and will be deregistered (if available)
Requesting network identifier The requesting network identifier PLMN id (Mobile Country Code and Mobile Network Code).
Requesting node identifier The identifier of the node requesting location/routing information for a target to the HSS
Requesting node type It indicates the type of node that requests the location of the target (if available)

7A.2.3.1 Serving system

The Serving System report event is generated at the HSS during the IMS registration process, when the HSS has detected that the target has roamed.

In addition, the event shall be provided in case of mobility events between different access types, if they are visible at the HSS, unless they are already provided by the HSS itself at access level (e.g. PS, EPS).

Such events could be mainly triggered by Diameter messages such as:

- Through Cx interface, Query and Select Pull in case of command of User-Authorization-Request from I-CSCF to HSS: see clause A.2 of TS 29.228 [62];

- Through Cx interface, AuthDataReq in case of command of Multimedia-Authentication-Request from S-CSCF to HSS: see clause A.2 of TS 29.228 [62];

- Through Sh interface, Pull in case of User-Data-Request from AS (with interworking to AS from target) to HSS: see clause A.2 of TS 29.328 [63].

- Through Cx interface, Server-Assignment-Request in case of command of S-CSCF to HSS (see clause A.2 of TS 29.228 [62]);

- Through SWx interface, Server-Assignment-Request in case of command of 3GPP AAA to HSS (see clause A of TS 29.273 [24], and clause 5 of GSMA IR.61 [65]).

The elements of table 7A.2.3.1 will be delivered to the DF2 if available.

Table 7A.2.3.1: Information Elements for Serving System Event

Observed MSISDN
Observed TEL URI
Observed SIP URI
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Current Serving System Identifier (AVP name such as Visited-PLMN-Id)
Any other IMPU or IMPI of the target (if available)

7A.2.3.2 Subscriber record change

This event will be only used to report when there is a change of association between IMSI, MSISDN/IMPU/IMPI/TEL URI/ SIP URI, or IMEI of the target. It is induced mainly by Subscriber Profile management by the HSS or the CSP administration tools through the HSS.

Such events could be mainly triggered by Diameter messages such as:

- Through Sh interface, Pull Resp in case of command of User-Data-Answer from HSS to AS, see clause A.2 of TS 29.328 [63];

- Through Sh interface, Update Resp in case of command of Profile-Update-Answer from HSS to AS, see clause A.2 of TS 29.328 [63];

- Through Sh interface, Subs-Notif Resp in case of command of Subscribe-Notifications-Answer from HSS to AS, see clause A.2 of TS 29.328 [63];

- Through Sh interface, Notif Resp in case of command of Push Notification-Answer from AS to HSS, see clause A.2 of TS 29.328 [63];

- Through Cx interface, Update_Subscr_Data Resp in case of command that update the target profile from S-CSCF to HSS. The message may include the elements, such as old and new IMSI or MSISDN/TEL URI/SIP URI or IMEI: see clause A.2 of TS 29.228 [62];

- Through Cx interface, Push-Profile-Answer This message is sent by the HSS to S-CSCF to update profile on S-CSCF if profile is changed by administrator at HSS: see clause A.2 of TS 29.228 [62];

- Through SWx interface, -Push-Profile-Request (PPR) in case of command of HSS to 3GPP AAA Server: see clause A of TS 29.273 [24].

The elements of table 7A.2.3.2 will be delivered to DF2, if available.

Table 7A.2.3.2: Information Elements for Subscriber Record Change Event

New observed MSISDN
New observed TEL URI
New observed SIP URI
New observed IMSI
New Observed IMEI (if available)
New observed IMPI
Old observed MSISDN
Old observed TEL URI
Old observed SIP URI
Old observed IMSI
Old observed IMEI (if available)
Old observed IMPI
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)
Other update: carrier specific.

NOTE: The change of IMEI can be detected by the HSS. Automatic Device Detection function clause 7.4 of TS 22.101 [60], can cause the IMEI to be notified to HLR especially in case of update location service, clause 8.1.2 TS 29.002 [61].

7A.2.3.3 Registration Termination

This event "Registration Termination" will be used to report to DF2 when HSS send to S-CSCF or 3GPP AAA Server. It is the equivalent of cancel location or purge to serving system in CS domain. This kind of event is induced by the registration of the target. The event will be triggered by the following Diameter messages:

- Through Cx interface, Server-Assignment-Request indicating deregistration from S-CSCF to HSS: see clause A.2 of TS 29.228 [62];
- Through Cx interface, Registration-Termination- Request from HSS to S-CSCF: see clause A.2 of TS 29.228 [62];
- Through SWx interface, Server-Assignment-Request indicating deregistration from 3GPP AAA Server to HSS: see clause A of TS 29.273 [24];
- Through SWx interface, Registration-Termination- Request from HSS to 3GPP AAA Server: see clause A of TS 29.273 [24].

The elements of table 7A.2.3.3 such as the previous serving system of the target will be delivered to DF2.

Table 7A.2.3.3: Information Elements for Registration Termination Event

Observed MSISDN
Observed TEL URI
Observed SIP URI
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Other Public User Identities Other IMPU or IMPI that was allocated to Target and will be deregistered (if available)
Reason of de-registration (Deregistration-Reason AVP, Reason-code AVP) (if available)
Network Element Identifier (HSS Id...)
Previous serving system identifier (VPLMN id…) (if available)

7A.2.3.4 Location Information request

This event will be used, if required by national regulations, to report any location information request on the IMS target by a node outside the HPLMN to HSS. As example, a location information request could be generated by a GMLC from another Network through a MAP request to the HSS of the target. The event will be triggered by any message coming from outside the HPLMN requesting routing or location information for the target.

This event shall not be generated when the request is issued from a node belonging to the HPLMN.

The elements included in table 7A.2.3.4 will be delivered to DF2, if available.

Table 7A.2.3.4: Information Elements for Location Information Request Event

Observed MSISDN
Observed TEL URI
Observed SIP URI
Observed IMSI
Observed IMEI
Requesting node identifier
Requesting network identifier
Requesting node type
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)
Any other IMPU or IMPI (if available)

7A.2.4 Provision of IRI for WebRTC

The enhanced P-CSCF (eP-CSCF) shall adhere to all LI requirements pertaining to the P-CSCF described in clause 7A.2.1. Any additional LI requirements pertaining to the support of WebRTC Interworking, as specified in TS 23.228 [43], that only apply to the eP-CSCF are described distinctly.

WebRTC Web Server Function (WWSF), if provided by the CSP, is an ICE that is used to copy and transmit via the DF to the LEMF the IP address and port used by the target as viewed by the WWSF. This IP address may be a public or private address depending on how the target accesses the WWSF.

WebRTC Authorisation Function (WAF), if provided by the CSP, is an ICE that creates a time-stamped authentication event associated with the target including relevant information such as the user's identity provided to the WAF.

Further details of the WWSF and WAF are FFS.

7A.3 Multi-media events

7A.3.0 General

- All SIP messages to or from a target, and all SIP messages executed on behalf of a target for multi-media session control are intercepted by the S-CSCF and Optionally P-CSCF and sent to DF2. The target identifier used to trigger the intercept will also be sent with the SIP message. This standard does not require nor prohibit redundant information from being reported to DF2.

  - Where a CSCF which provides lawful interception makes changes to a SIP message, sent to or from or executed on behalf of a target then the CSCF shall report both the original message and the modified message to the DF2.

  - Where a CSCF which provides lawful interception changes identities within a SIP message (e.g. IMPI/IMPU changes or due to call forwarding etc.) and the new identity is the target, then both the original and modified SIP messages shall be reported to DF2.

  - Where a CSCF which provides lawful interception changes identities within a SIP message (e.g. IMPI/IMPU changes or due to call forwarding etc.) and the new identity is not the target, then both the original and modified SIP messages shall be reported to DF2.

- P-CSCF event reports may be redundant with S-CSCF event reports when the P-CSCF and S-CSCF reside in the same network, however, this standard does not require nor prohibit redundant information from being reported to DF2.

- Non-Local ID interception will be made by S-CSCF or P-CSCF (optional in a non-roaming case, and mandatory in the roaming case when LBO approach is used as the roaming architecture). As national option, the interception functions may also be provided by the IBCF or MGCF for a non-roaming case. Of the two approaches S-CSCF/P-CSCF Vs IBCF/MGCF used for non-roaming case, only one approach is required to be supported within a CSP's network. With S8HR as the roaming architecture, the Non-Local ID interception in the VPLMN will be made by the LMISF (see clause 20).

- For interception of incoming calls of Non-Local ID, any of the SIP headers used to identify the calling party information and redirecting party information present in the incoming SIP message. The examples are: P-Asserted Id, From headers and History-Info, Diversion headers.

- For interception of outgoing calls of Non-Local ID, any of the SIP headers used to identify the called party information present in the outgoing SIP message. The examples are: Request URI and To headers.

- The IRI should be sent to DF2 with a reliable transport mechanism.

- Correlation for SIP to bearer shall be supported within the domain of one provider.

- An intercepted SIP event sent to DF2 is shown below:

  - Observed SIP URI

  - Observed TEL URI

  - Observed IMEI (Not in the case of Non-Local ID interception)

  - Event Time and Date

  - Network element identifier

  - SIP Message Header

  - SIP Message Payload

  - VPLMN ID

NOTE 1: The Observed IMEI is obtained from the +sip.instance.id of the intercepted SIP message (as defined in TS 24.229 [49]).

- All IMS XCAP messages to or from a target for multi-media or supplementary services are intercepted by the AS, or the group of AS in charge to transmit, manipulate and store any IMS XCAP of that target. The data have to be transmitted either "en clair" or encrypted with all elements to let the LEMF decrypt the data. The generated IRI should be sent in any case to DF2.

NOTE 2: The data related to XCAP management and the XCAP documents modification of the target, as supplementary services, or as the 3GPP or OMA presence services (TS 24.141 , OMA Presence SIMPLE specification and IETF RFC 4827), are reported through the DF2. However, these are points are currently not covered:

1) other data (XCAP management and the XCAP documents modification by the target) to be transmitted but related to other multimedia services;

2) the case of XCAP messages that are based on different interfaces than Ut interface;

3) the specific architecture related to encrypted data;

4) Detailed XCAP events, related to authentication.

- An intercepted XCAP report sent to DF2 is shown below:

  - Observed SIP URI or Tel URI, based on XUI (described in IETF RFC 4825 [56]) or information in the XCAP payload (if available).

- Observed XUI or any other identities (if available).
- Event Time and Date.
- Network element identifier.
- XCAP Message (the entire elements of the HTTP Header and the XCAP payload).

NOTE 3: Void.

The interpretation of XCAP messages, such as HTTP request through the Ut interface between the target's UE and related XCAP server may sometime be insufficient to let the LEA to understand what was modified as directed by the UE, therefore a later HTTP response is needed to understand the success or failure of the request.

Specific Diameter messages, to or from or related to a target, are intercepted by the HSS in charge of that target. The generated IRI should be sent in any case to DF2. Events and IRI are described below:

Such events are:

- Serving System;
- When IMPU or IMPI is changed in a HSS subscriber record change;
- Registration termination
- Location information request.

Contents of such IRI report related to HSS sent to DF2, is shown below:

- Observed SIP URI or Tel URI or IMSI;
- Observed any other identities (if available);
- Event Time and Date;
- Network element identifiers;
- Network Identifier (if available and only in case of roaming)
- Target profile or data elements (if available).

7A.3.1 Mid IMS Session Interception

7A.3.1.0 General

Mid IMS Session interception functionality applies in addition to other IMS LI functional requirements as defined in section 7A.

Where LI is activated on a target within a CSCF after an IMS session has already been established the CSCF shall do one of the following;

- Where the CSCF has stored the media session information which occurred prior to the interception activiation, the CSCF shall provide a "start of interception with IMS session" event message, to the DF2/MF over the X2 interface, including the parameter and information listed in table 7A.3.1, if available.
- Where the CSCF has not stored media session information which occurred prior to the interception activation, the CSCF shall report all future SIP messages which the CSCF is able to identify as associated with an ongoing target session. In this case, the event "start of interception with IMS session" is not applicable.

It is a national option whether the CSCF shall be mandated to store the necessary information to support reporting of session establishment parameters, in order to support mid IMS session interception, or whether the CSCF shall only report SIP messages which occur after the interception is applied and the CSCF is able to identify as related to an ongoing target session. If information is stored then it shall be possible to set a maximum storage time according to national and/or operator requirements.

Table 7A.3.1 Start of interception with established IMS session event

Observed SIP URI
Observed TEL URL
Observed IMEI
Event type
Event Time
Event Date
Network Element Identifier
SIP message header offer (NOTE)
SIP message header answer (NOTE)
SDP offer
SDP answer
Correlation information
VPLMN ID

NOTE: Void.

The SIP messages that carry the SDP offer and answer shall be reported. In case there are multiple SDP offers/answers during the session establishment, the SIP messages that carry the latest SDP offer/answer shall be provided.

The points above on requirements in this clause applicable to CSCF support of mid IMS Session interception, shall apply to IBCF which incorporate ICE for Non-Local ID interception.

7A.3.1.1 SDES Media Security

If an SDES crypto attribute is included in the SDP, the DF2/MF forwards the "start of interception with IMS session" event message to the LEMF over HI2 without additional key processing.

NOTE: The SDES Crypto attribute contains the cryptographic key required for decrypting the encrypted IMS media.

If SDES mid session support is required then storing of media information as per 7A.3.1 is mandatory.

7A.4 Multi-media Call State Control Service Scenarios

Annex C shows examples of the delivery of intercepted events and product under various call scenarios.

7A.5 Push to talk over Cellular (PoC)

PoC is a service of the IMS Domain and interception is accomplished according to the definitions in clause 7A.3. Interception of CC is possible with the current implementations in the GSNs.

This clause applies if regulatory requirements require separate reporting of Push to Talk over Cellular (PTC). PTC consists of Push to talk over Cellular (PoC) [82], and Mission Critical Push To Talk (MCPTT) [85].

7A.6 SMS over IMS

SMS over IMS shall be intercepted in accordance with normal IMS interception as described in 7A.3, also for Non-Local ID interception. SMS IRI (including originating and destination addresses, SMS direction, and SMS Centre Address) are reported, if available, for IRI-only intercepts.

7A.7 LI for KMS based IMS Media Security

7A.7.1 LI Architecture and functions

KMS based IMS media security is specified in TS 33.328 [25]. The present clause specifies LI architecture and functions needed to provide session encryption keys generated by the KMS to protect IMS media for a subscriber who is a target for interception in the IMS nodes. This section is applicable to the cases in which the KMS is under responsibility of the Operator providing the IMS network infrastructure. Other scenarios such as the one in which the KMS is run by an independent legal entity are outside the scope of this specification.

NOTE 1: It is FFS whether the Xk interface defined in this section can be used also by the LEMF to directly query the KMS as an additional option.

NOTE 2: This section covers the scenario in which encrypted content of communication is provided to the LEMF together with encryption keys, to allow decryption at LEMF.

Figure 7A.7.1 shows the LI architecture for the case in which decryption is performed by the LEMF and a KMS is used to support IMS media security, with a Xk interface defined between the DF2/MF and the KMS, in addition to the interfaces and functional entities needed to support LI in the P-CSCF/S-CSCF.

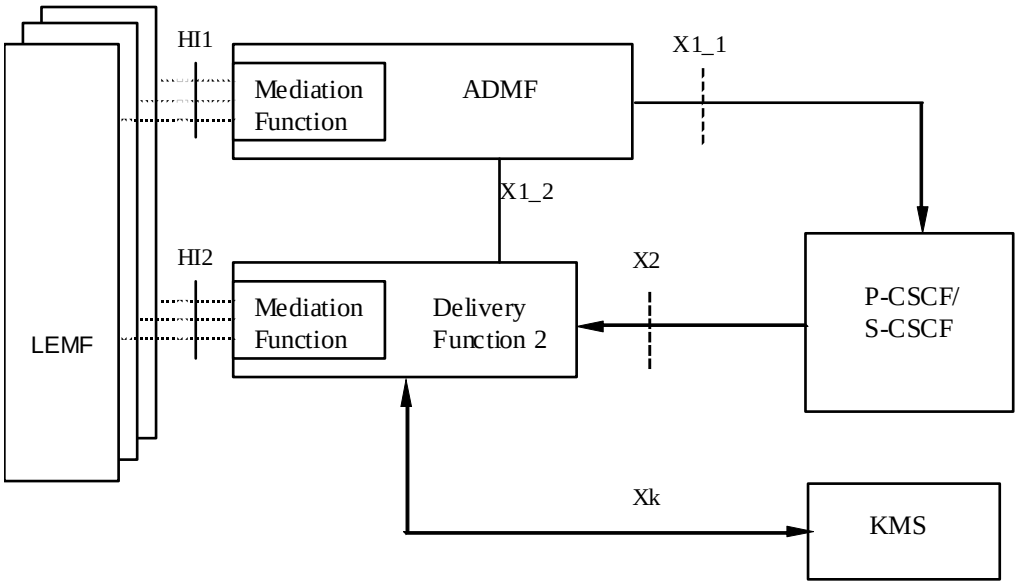


Figure 7A.7.1: KMS Intercept configuration

When LI has been activated in the P/S-CSCF for a target, the node will report SIP messages events on the X2 interface, as specified in section 7.A and subsections. The DF2/MF shall extract from the intercepted SIP signalling the information related to the encryption and send a request over the Xk interface to the KMS to derive the encryption keys; the request will carry also the reference to the ticket transferred by the SIP signalling between the parties involved in the communication. The KMS shall then, based on the information received from the DF2, resolve the ticket and provide the session keys to the DF2/MF over the Xk interface.

7A.7.2 Signalling over the Xk interfaces and LI events

The following messages are defined over the Xk interface:

- get_keys
- get_keys_response

The message get_keys shall be sent by the DF2/MF to the KMS in order to ask the KMS to provide session keys for an ongoing communication.

The message get_keys_response shall be sent by the KMS to the DF2/MF in order to provide the session keys.

The message get_key_response defines a LI event provided by the KMS to the DF2/MF which shall then be sent by the DF2/MF to the LEMF in a proper IRI record over the HI2 interface.

Table 7A.7.2.1 provides the list of parameters, which shall be carried by the message get_keys, in order to transfer to the KMS the information, as specified in TS 33.328 [25], needed to provide the session encryption keys:

Table 7A.7.2.1: Parameters and information in message get_keys

Public KMS Identity of the target user
TRANSFER_INIT
TRANSFER_RESP

Upon reception of get_keys message, the KMS shall verify that the key management information is related to the targeted user.

A timer may be defined in the DF2/MF in order to specify the amount of time that the DF2/MF shall wait for the response from the KMS. If this timer expires, a failure indication shall be sent to the LEMF.

Table 7A.7.2.2 provides the list of parameters, which shall be carried by the message get_keys_response, in order to provide the DF2/MF with the session keys:

Table 7A.7.2.2: Parameters and information in message get_keys_response

Crypto Session ID
Session key
Salt
Failure indication (optional)

With reference to table 7A.7.2.2, in case of failure in providing any of the decryption information, the KMS may provide a decryption failure indication.

Upon reception of get_keys_response message or in case of timer expiry, the following information shall be provided to the LEMF by the DF2/MF:

- Lawful interception identifier
- Observed target identity(ies)
- Correlation number (in order to correlate the keys to IMS session under interception at the CSCF(s))
- Event type (session encryption keys available)
- Crypto Session ID (if provided by the KMS)
- Session key (if provided by the KMS)
- Salt (if provided by the KMS)
- MediaSec key retrieval failure indication (in case of e.g. timer expiry, or failure indication received from the KMS).

7A.7.3 Cooperating KMSs

As specified in TS 33.328 [25], in some scenarios the parties involved in an encrypted IMS based communication may use two different KMSs. In these cases, no additional LI specific signalling between the KMSs shall take place. The KMS may need to cache the session keys retrieved as result of the ticket resolution for possible LI needs at later stage.

7A.7.4 Security

Xk interface and its configuration shall only be accessible to authorized personnel.

The Xk interface shall have strong integrity and confidentiality protection. The Xk interface shall be protected by TLS unless protected by IPsec for LI purposes. TLS and certificate profiling shall be according to TS 33.310 [28]; IPsec profiling shall be according to TS 33.310 [28] and TS 33.210 [29].

7A.7.5 Start of interception for an already established IMS media secured session

This function is invoked when LI is activated in the network for a target who has already established an IMS session with secure media.

In order to provide information needed to decrypt the content of communication, the LI function in the CSCFs needs to have access to SDP information and SIP headers exchanged in the SIP signalling between the parties during the IMS session setup for possible later retrieval in case LI is activated during the ongoing session.

With reference to fig. 7A.7.1, if LI is activated by the ADMF over the X1_1 interface for a target, the CSCF shall check if the given target has an ongoing IMS media secured session. In this case, the CSCF shall provide a "Start of interception with established IMS session" event message to the DF2/MF over the X2 interface, as specified in section 7A.3.1.

Upon reception of Start of interception with established IMS secure session event, the DF2/MF shall check if a MIKEY-TICKET is included in the SDP. In this case the DF2/MF, in addition to forwarding the event to the LEMF over HI2, shall contact the KMS to resolve the ticket and retrieve the session keys and additional encryption related information as specified in in section 7A.7.2.

7A.8 IMS IMEI Interception

The use of Instance ID in TS 24.229 [49] is mandatory in IMS in order to support IMEI based LI in the CSCF. The CSCF is required to have access to the Instance IDs for all active IMS registrations regardless of whether LI has been requested prior to UE registration for a given IMEI. The CSCF shall be responsible for extracting the IMEI from the Instance ID where required for a specific target interception and providing the IMEI to the DF2. The IMEI (when available) shall be provided by the CSCF to the DF2 for all intercepted communication regardless of whether the IMEI or another identifier has been used as the target for interception.

Based on the national regulations, IMEI-based LI shall be possible for IMS sessions originated from, or terminated to, the UE with that IMEI.

7A.9 Void

8 Security

8.0 General

The security requirements are valid for the whole Lawful Interception system, i.e. rules and procedures shall be used for all involved entities, such as 3G GSN and the DF.

8.1 Administration security

The administration of the LI function, i.e. Activation, Deactivation and Interrogation of Lawful Interception, in the 3G ICEs and the DFs shall be done securely as described below:

- It shall be possible to configure the authorised user access within the serving network to Activate, Deactivate and Interrogate Lawful Interception separately for every physical or logical port at the 3G ICEs and DF. It shall be possible to password protect user access.
- Only the ADMF is allowed to have access to the LI functionality in the 3G ICEs and DF.
- The communication links between ADMF, 3G GSN, 3G MSC Servers or any ICEs of this specification, LI LCS Client, CSCF, DF2, and DF3 may be required by national option to support security mechanisms. Options for security mechanisms include:
  - CUG / VPN;
  - COLP;
  - CLIP;
  - authentication;
  - encryption.

Through the use of user access restrictions, no unauthorised network entities or remote equipment shall be able to view or manipulate LI data in the 3G GSN, 3G MSC Server, LI LCS Client, CSCF, 3GPP ICE, any 3GPP nodes, and Administration nodes of this specification or the DFs.

8.2 IRI security

8.2.1 Normal operation

The transmission of the IRI shall be done in a secure manner.

When DFs are physically separate from the 3G ICEs or any nodes described in this specification for IRI creations, the X2-interface may be required by national option to support security mechanisms. Options for security mechanisms include:

- CUG/VPN;
- COLP;
- CLIP;
- authentication;
- encryption.

8.2.2 Communication failure

Depending on the national law in case of communication failure IRI may be buffered in the 3G INEs or other node elements used in this specification. After successful transmission of IRI the whole buffer shall be deleted. It shall be possible to delete the content buffer via command or a timer, in an un-restorable fashion.

8.3 CC security

The transmission of the CC shall be done in a secure manner.

When DFs are physically separate from the 3G INEs or any other nodes used for interception mentioned in this specification, the X3-interface may be required by national option to support security mechanisms. Options for security mechanisms include:

- CUG/VPN;
- COLP;
- CLIP;
- authentication;
- encryption.

In case of transmission failure no buffering is required within the intercepting network.

8.4 Security aspects of Lawful Interception (LI) billing

Billing information may be suppressed or made available at the DFs and the ADMF. Billing information for Lawful Interception shall be separated from "regular" billing data.

Billing data transmission to the Lawful Interception billing system may be done in a secure manner per national option.

In case of transmission failure billing-data shall be buffered/stored in a secure way. After successful transmission billing data shall be deleted in an un-restorable fashion.

8.5 Other security issues

8.5.1 Log files

Log files shall be generated by the ADMF, DF2, DF3, 3G MSC Servers, or any 3GPP nodes of this specification, LI LCS Client, CSCF and the 3G GSN. All log files are retrievable by the ADMF, and are maintained by the ADMF in a secure manner.

8.5.2 Data consistency

The administration function in the 3GMS or any nodes described in this specification shall be capable of performing a periodic consistency check to ensure that the target list of target identities in all involved 3G MSC Servers or any 3GPP nodes of this specification, LI LCS Client, CSCFs, 3G GSNs in the 3GMS and the DFs contain the appropriate target Ids consistent with the intercept orders in the ADMF. The reference data base is the ADMF data base.

9 Invocation of Lawful Interception (LI) for 3GPP WLAN interworking services

9.0 General

WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards.

This clause 9 is therefore no longer maintained.

Figure 23 shows the extract from the reference configuration which is relevant for the invocation of the Lawful Interception of the packet data 3GPP WLAN Interworking network.

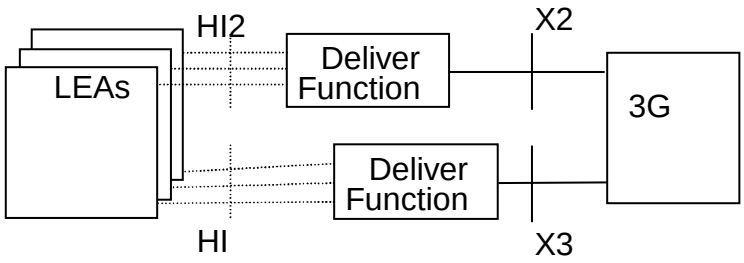


Figure 23: Functional model for invocation of Lawful Interception for 3GPP WLAN Interworking Services

The HI2 and HI3 interfaces represent the interfaces between the LEA and two delivery functions. Both interfaces are subject to national requirements. They are included for completeness, but are beyond the scope of this specification.

The delivery functions are used:

- to convert the information on the X2-interface to the corresponding information on the HI2 interface;
- to distribute the intercept related information to the relevant LEA(s);
- to distribute the intercept product to the relevant LEA(s).

Interception at a WAG applies for the roaming users where the PDG is not in the visited network.

For most WLAN Interworking cases, the Packet Data Gateway (PDG) handles the bearer level interception, specifically interception of CC and IRI related to tunnel establishment and release in which case there is no need to perform interception at a WAG. This includes the case where the PDG is in the intercepting carrier's network (whether it be home or visited). For the case where a visited network is to intercept WLAN related tunnel and the PDG for the tunnel is not in the visited network, the Wireless Access Gateway (WAG) is used to intercept the CC and IRI related to tunnel establishment and release. It should be noted that the CC available at the WAG may be encrypted.

9.1 Provision of Intercept Product - Short Message Service

LI for SMS in the 3GPP-WLAN Interworking case is described in Clause 7A.4.

9.2 Provision of Intercepted Content of Communications - 3GPP WLAN Interworking services

9.2.0 General

The access method for the delivering of 3GPP WLAN Interworking Intercept Product is based on duplication of packets without modification at the PDG or WAG. The duplicated packets with additional information in the header, as described in the following sections, are sent to DF3 for further delivery. Note that CC available at the WAG is likely to be encrypted.

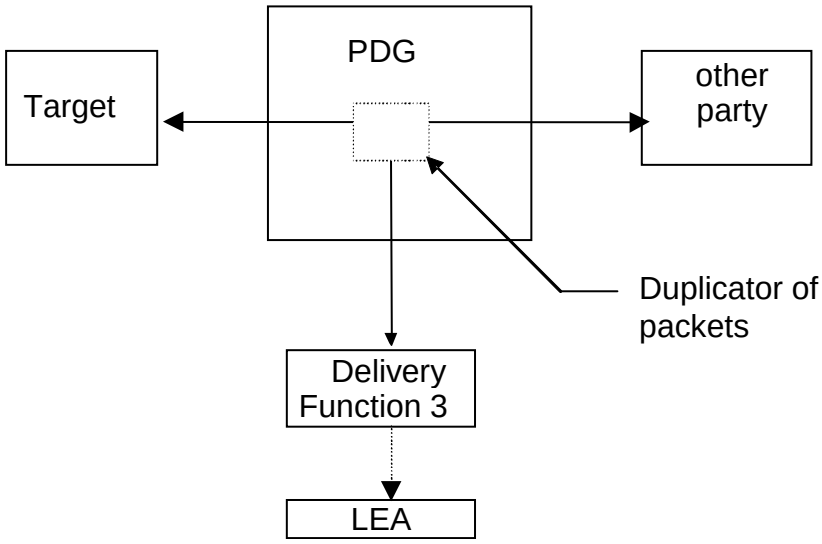


Figure 24: Configuration for interception of 3GPP WLAN Interworking product data

9.2.1 X3-interface

In addition to the intercepted content of communications, the following information needs to be transferred from the PDG or WAG to the DF3 in order to allow the DF3 to perform its functionality:

- target identity;
- correlation number;
- time stamp - optional;
- direction (indicates whether T-PDU is MO or MT) - optional;
- the target location (if available in the intercepting node).

9.3 Provision of Intercept Related Information

9.3.0 General

Figure 25 shows the transfer of intercept related information to the DF2. If an event for / from a mobile subscriber occurs, the PDG, WAG, or the AAA Server sends the relevant data to the DF2. Packet Data Header Information reporting is a national option. For Packet Data Header Information reporting, a PDG/WAG either isolates the relevant data and sends it to the DF2 or sends the packet stream to another entity in the network (e.g., DF3) for isolation which then provides the relevant data to the DF2.

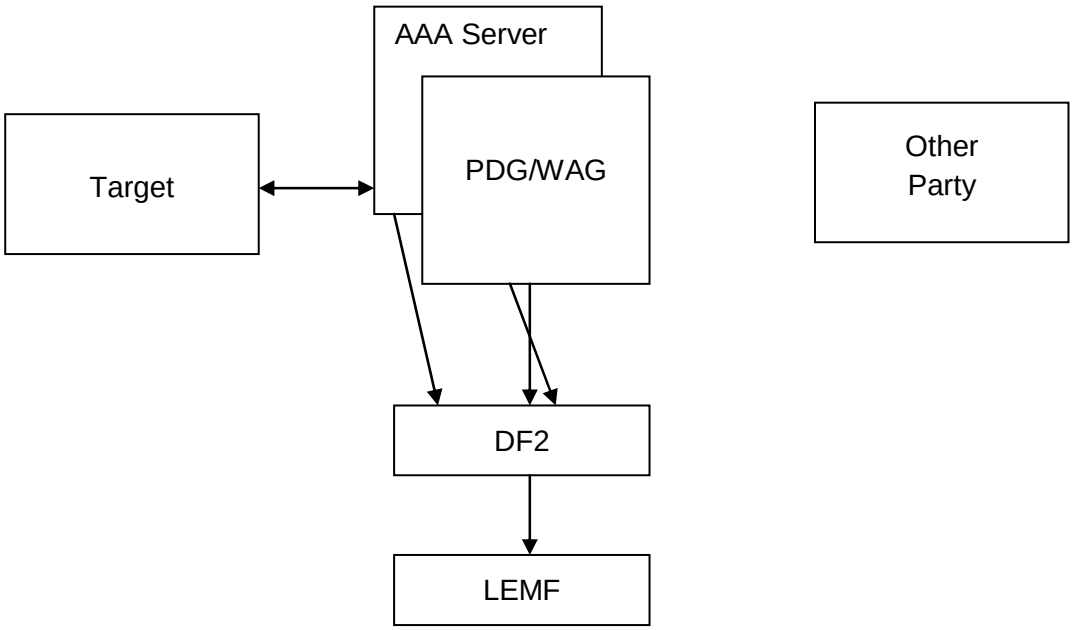


Figure 25: Provision of Intercept Related Information

9.3.1 X2-interface

The following information needs to be transferred from the PDG, WAG or the AAA server to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMSI, NAI, or MSISDN);
- events and associated parameters as defined in section 9.3.2 may be provided;
- the target location (if available);
- Correlation number;
- Quality of Service (QoS) identifier (if available).

The IRI should be sent to DF2 using a reliable transport mechanism.

The PDG/WAG detects packets containing packet data header information in the communications path but the information needed for Packet Data Header Information reporting may need to be transferred from the PDG/WAG either directly to the DF2 or via another network entity in order to allow the DF2 to perform its functionality.

9.3.2 3GPP WLAN Interworking LI Events and Event Information

The following events are applicable to AAA Server:

- I-WLAN Access Initiation;
- I-WLAN re-authentication,
- I-WLAN Access Termination;
- I-WLAN Tunnel Establishment;
- I-WLAN Tunnel Disconnect;
- Start of Intercept with I-WLAN Communication Active;

The following events are applicable to the PDG and WAG:

- I-WLAN Tunnel Establishment;
- I-WLAN Tunnel Disconnect;

- Start of Intercept with I-WLAN Communication Active.
- Packet Data Header Information.

A set of possible elements as shown below is used to generate the events. Information associated with the events are transmitted from the PDG, WAG or AAA server to DF2.

NOTE: Void.

Some of these parameters apply to the PDG or WAG and some apply to the AAA server. Parameters sent from the PDG, WAG or AAA server is dependent on what is available at the network element. If interception is performed at the PDG, then Packet Data Header Information reporting shall also be performed at the PDG and not at the WAG.

Table 3: Information Events for WLAN Interworking Event Records

Element	PDG	AAA Server
Observed MSISDN MSISDN of the target.	Available, see TS 29.234 [16]	Available, see TS 29.234 [16]
Observed NAI NAI of the target.	Not available	Available, see TS 29.234 [16]
Observed IMSI IMSI of the target.	Available, see TS 29.234 [16]	Available, see TS 29.234 [16]
Event type Description which type of event is delivered: I-WLAN Access Initiation, I-WLAN Access Termination, I-WLAN Tunnel Establishment, I-WLAN Tunnel Disconnect, Start of Intercept with I-WLAN Communication Active, Packet Data Header Information.	Available from ICE	Available from ICE
Event date Date of the event generation in the PDG or the AAA server.	Available from ICE	Available from ICE
Event time Time of the event generation in the PDG or the AAA server. Timestamp shall be generated relative to the PDG or AAA server internal clock.	Available from ICE	Available from ICE
WLAN UE Local IP address The WLAN UE Local IP address of observed party. The WLAN UE Local IP address field specified in TS 24.234 [17] and IETF RFC 2409, represents the IPv4/IPv6 address of the WLAN UE in the WLAN AN. It is an address used to deliver the packet to a WLAN UE in a WLAN AN. Note that this address might be dynamic.	Available, see TS 24.234 [17] and IETF RFC 2409	Not available
WLAN UE MAC address The WLAN MAC address of the target. Note that this address might be dynamic and the validity of the MAC Address is outside of the scope of 3GPP.	Not available	Available, see TS 29.234 [16]
WLAN UE Remote IP address The WLAN UE Remote IP address of observed party. The WLAN UE Remote IP address field specified in TS 24.234 [17], represents the IPv4/IPv6 address of the WLAN UE in the network being accessed by the WLAN AN. It is an address used in the data packet encapsulated by the WLAN UE-initiated tunnel and is the source address used by applications in the WLAN UE. Note that this address might be dynamic.	Available, see TS 24.234 [17]	Not available
WLAN Access Point Name The W-APN of the access point.	Available, see TS 24.234 [17]	Available, see TS 29.234 [16]
WLAN Operator Name The name of the WLAN operator name serving the target.	Not available	Available, see TS 29.234 [16]
WLAN Location Data The location of the WLAN serving the target (e.g., string like "coffee shop" or "airport", etc.).	Not available	Available, see TS 29.234 [16]
WLAN Location Information Location Information regarding the WLAN as provided in RADIUS or DIAMETER signalling exchanged with the AAA server.	Not available	Available, see TS 29.234 [16]
Correlation Number The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records. In case of the AAA server, the Correlation Number is only used to correlate IRI records.	Generated for LI by PDG	Generated for LI by AAA server
Network Element Identifier Unique identifier for the element reporting the ICE.	Generated for LI by PDG	Generated for LI by AAA server
Initiator The initiator of the request either the network or the WLAN UE.	Generated for LI by PDG	Generated for LI by AAA server
NAS IP/IPv6 address The IP or IPv6 address of the NAS in the WLAN.	Not available	Available, see TS 29.234 [16]

Visited PLMN ID Identity of the visited PLMN to which the user is terminating their WLAN tunnels or through which the user is establishing their WLAN tunnels.	Not available	Available, see TS 29.234 [16]
Session Alive Time The amount of time in seconds during which the target can be registered for WLAN access.	Not available	Available, see TS 29.234 [16]
Failed access reason Provides the reason for why a WLAN access attempt failed ("Authentication Failed").	Not available	Available from ICE
Session termination reason Provides a reason for why a WLAN access session is terminated.	Not available	Available, see TS 29.234 [16]
Failed tunnel establishment reason Provides a reason for why a WLAN tunnel establishment failed ("Authentication failed" or "Authorization failed").	Available from ICE	Available from ICE
NSAPI Network layer Service Access Point Identifier The NSAPI information element contains an NSAPI identifying a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control Plane. This is an optional parameter to help DF/MF and LEA's to distinguish between the sending mobile access networks	Optional available according TS 23.234 [14] Annex F; defined TS 29.060 [37] 7.7.17	Not available
Destination IP Address The IP address, including type IPv4 or IPv6, of the destination of the IP packet.	Available from ICE	Available from ICE
Destination Port Number The port number of the destination of the IP packet.	Available from ICE	Available from ICE
Flow Label (IPv6 only) The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [41]).	Available from ICE	Available from ICE
Packet Count The number of packets detected and reported (for a particular summary period).	Available from ICE	Available from ICE
Packet Data Summary Reason The reason for a Packet Data Summary message being sent to the LEMF (e.g., timed out, counter expiration, end of session)	Available from ICE	Available from ICE
Packet Size The size of the packet. (i.e., Total Length Field in IPv4 or Payload Length field in IPv6)	Available from ICE	Available from ICE
Source IP Address The IP address, including type IPv4 or IPv6, of the source of the IP packet.	Available from ICE	Available from ICE
Source Port Number The port number of the source of the IP packet.	Available from ICE	Available from ICE
Sum of Packet Sizes (for a particular summary period) The sum of values contained in the Total Length fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.	Available from ICE	Available from ICE
Summary Period Includes the dates and times of the first and last packets in a particular packet data interval.	Available from ICE	Available from ICE
Transport Protocol (e.g., TCP) The identification of the transport protocol of the packet or packet flow being reported.	Available from ICE	Available from ICE

Table 3a: Information Events for WLAN Interworking Event Records - WAG

Element	WAG
Observed MSISDN MSISDN of the target.	Available, see TS 29.234 [16]
Observed IMSI IMSI of the target.	Available, see TS 29.234 [16]
Event type Description which type of event is delivered: I-WLAN Tunnel Establishment, I-WLAN Tunnel Disconnect, Start of Intercept with I-WLAN Communication Active, Packet Data Header Information.	Available from ICE
Event date Date of the event generation in the PDG/WAG or the AAA server.	Available from ICE
Event time Time of the event generation in the PDG/WAG or the AAA server. Timestamp shall be generated relative to the PDG/WAG or AAA server internal clock.	Available from ICE
WLAN UE IP address The WLAN UE IP address of observed party. The WLAN UE IP address field contains the IPv4/IPv6 address (specified by TS 29.234 [16]) of the WLAN UE tunnel endpoint as seen by the WAG. Note that this address might be dynamic.	Available, see TS 29.234 [16]
WLAN PDG Tunnel Endpoint IP address The WLAN PDG Tunnel Endpoint IP address field contains the IPv4/IPv6 address of the PDG (as specified in TS 29.234 [16]) as seen by the WAG. Note that this address might be dynamic.	Available, see TS 29.234 [16]
WLAN Access Point Name The W-APN of the access point.	Available, see TS 29.234 [16]
Correlation Number The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records.	Generated for LI by WAG
Network Element Identifier Unique identifier for the element reporting the ICE.	Generated for LI by WAG
NAS IP/IPv6 address The IP or IPv6 address of the NAS in the WLAN.	Available, see TS 29.234 [16]
Tunnel Protocol The Tunnel Protocol as defined in the Routing-Policy AVP in TS 29.234 [16].	Available, see TS 29.234 [16]
Source Ports The list or range of source ports as specified in the Routing-Policy AVP provided by the AAA server in TS 29.234 [16].	Available, see TS 29.234 [16]
Destination Ports The list or range of destination ports as specified in the Routing-Policy AVP provided by the AAA server in TS 29.234 [16].	Available, see TS 29.234 [16]
Session Alive Time The amount of time in seconds during which the target can be registered for WLAN access.	Available, see TS 29.234 [16]
Destination IP Address The IP address, including type IPv4 or IPv6, of the destination of the IP packet.	Available from ICE
Destination Port Number The port number of the destination of the IP packet.	Available from ICE
Flow Label (IPv6 only) The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [41]).	Available from ICE
Packet Count The number of packets detected and reported (for a particular summary period).	Available from ICE
Packet Data Summary Reason The reason for a Packet Data Summary message being sent to the LEMF (e.g., timed out, counter expiration, end of session)	Available from ICE

Packet Size The size of the packet. (i.e., Total Length Field in IPv4 or Payload Length field in IPv6)	Available from ICE
Source IP Address The IP address, including type IPv4 or IPv6, of the source of the IP packet.	Available from ICE
Source Port Number The port number of the source of the IP packet.	Available from ICE
Sum of Packet Sizes (for a particular summary period) The sum of values contained in the Total Length fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.	Available from ICE
Summary Period Includes the dates and times of the first and last packets in a particular packet data interval.	Available from ICE
Transport Protocol (e.g., TCP) The identification of the transport protocol of the packet or packet flow being reported.	Available from ICE

9.4 Structure of I-WLAN Events

9.4.1 I-WLAN Access Initiation

For I-WLAN Access Initiation including I-WLAN re-authentication, for both I-WLAN Access Initiation-event is generated. The elements, shown in Table 4, will be delivered to the DF2, if available, by the AAA server.

Table 4: I-WLAN Access Initiation - AAA Server

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Network Element Identifier
WLAN Operator Name
WLAN LocationData
WLAN Location Information
NAS IP/IPv6 Address
WLAN UE MAC Address
Visited PLMN ID
Session Alive Time
Failed Access reason

9.4.2 WLAN Access Termination

For WLAN Access Termination or the immediate purging of a user from a WLAN access, a WLAN access termination-event is generated. The elements, shown in Table 5, will be delivered to the DF2, if available, by the AAA server.

Table 5: I-WLAN Access Termination - AAA Server

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Network Element Identifier
WLAN Operator Name
WLAN Location Data
WLAN Location Information
NAS IP/IPv6 Address
WLAN UE MAC Address
Session Termination reason

9.4.3 I-WLAN Tunnel Establishment

For I-WLAN Tunnel Establishment, a I-WLAN tunnel establishment-event is generated. The elements, shown in Table 6, 6a, and Table 7, will be delivered to the DF2 if available, by the PDG, WAG or AAA server, respectively.

Table 6: I-WLAN Tunnel Establishment - PDG

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation number
WLAN UE Local IP address
WLAN UE Remote IP address
WLAN Access Point Name
Network Element Identifier
Failed tunnel establishment reason
NSAPI (optional)

Table 6a: I-WLAN Tunnel Establishment - WAG

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
WLAN UE IP address
WLAN PDG Tunnel Endpoint IP address
WLAN Access Point Name
NAS IP/IPv6 address
Tunnel Protocol
Source Ports
Destination Ports
Session Alive Time
Network Element Identifier

Table 7: I-WLAN Tunnel Establishment - AAA Server

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation number
WLAN Access Point Name
Network Element Identifier
Visited PLMN ID
Failed tunnel establishment reason

9.4.4 I-WLAN Tunnel Disconnect

At I-WLAN Tunnel Disconnect, a I-WLAN tunnel disconnect event is generated. The elements, shown in Table 8, 8a, and Table 9, will be delivered to the DF2, if available, by the PDG, WAG or AAA server, respectively.

Table 8: I-WLAN Tunnel Disconnect - PDG

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation number
WLAN UE Local IP Address
WLAN UE Remote IP address
WLAN Access Point Name
Network Element Identifier
Initiator (optional)

Table 8a: I-WLAN Tunnel Disconnect - WAG

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
WLAN UE IP address
WLAN PDG Tunnel Endpoint IP address
WLAN Access Point Name
NAS IP/IPv6 address
Tunnel Protocol
Source Ports
Destination Ports
Network Element Identifier

Table 9: I-WLAN Tunnel Disconnect - AAA Server

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation number
Tunnel address of observed party
WLAN Access Point Name
Network Element Identifier
Initiator (optional)

9.4.5 Start of Intercept with I-WLAN Communication Active

This event will be generated if interception for a target is started and if the target has one or more active I-WLAN Access sessions or one or more I-WLAN Tunnels established. The elements, shown in Table 10,10a, and Table 11, will be delivered to the DF2, if available, by the PDG, WAG or AAA server, respectively.

Table 10: Start of Intercept with I-WLAN Communication Active - PDG

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation Number
WLAN UE Local IP Address
WLAN UE Remote IP address
WLAN Access Point Name
Network Element Identifier

Table 10a: Start of Intercept with I-WLAN Communication Active - WAG

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
WLAN UE IP address
WLAN PDG Tunnel Endpoint IP address
WLAN Access Point Name
NAS IP/IPv6 address
Tunnel Protocol
Source Ports
Destination Ports
Session Alive Time
Network Element Identifier

Table 11: Start of Intercept with I-WLAN Communication Active - AAA Server

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation Number
WLAN Access Point Name
Network Element Identifier
WLAN Operator Name
WLAN Location Data
WLAN Location Information
NAS IP/IPv6 address
Visited PLMN ID

9.4.6 Packet Data Header Information

9.4.6.0 Introduction

Packet Data Header Information reporting can be done either on a per-packet (i.e., non-summarized) basis or in a summary report.

9.4.6.1 Packet Data Header Report

This event is used to provide packet header reports on a per packet basis (non-summarized reporting) and is triggered by each packet sent or received by the target. These elements will be delivered either directly to DF2 or via another network entity if available:

Table A: I-WLAN Packet Data Header Report - PDG

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation number
WLAN UE Local IP Address
WLAN UE Remote IP address
WLAN Access Point Name
Network Element Identifier
Initiator (optional)
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Packet Size
Flow Label (IPv6 only)

Table B: I-WLAN Packet Data Header Report - WAG

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
WLAN UE IP address
WLAN PDG Tunnel Endpoint IP address
WLAN Access Point Name
NAS IP/IPv6 address
Tunnel Protocol
Source Ports
Destination Ports
Network Element Identifier
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Packet Size
Flow Label (IPv6 only)

9.4.6.2 Packet Data Summary Report

This event is used to report:

1) the source and destination information derived from the packet headers, including:

   a) source and destination IP Addresses,

   b) IP next-layer protocol,

   c) Layer-4 ports, and

   d) Flow label, if the packet is IPv6

2) summary information for the number of packets and bytes transmitted or received by the target for each unique packet flow within a WLAN tunnel, and

3) the date and the time of the first and last packets associated with that packet flow. A packet flow is defined as the 6-tuple of source/destination IP address/port number and the layer 4 protocol and WLAN tunnel.

   IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported.

The event provides packet summary reports for each unique packet data session (PDP context) and packet flow, and is triggered by one of the following:

- start of a packet flow associated with a WLAN Tunnel
- an interim report for a packet flow associated with a WLAN Tunnel is to be reported
- end of a packet flow associated with a WLAN Tunnel (including end of the WLAN Tunnel itself).

An interim report can be triggered by

- The expiration of a configurable timer per intercept (called a Summary Timer). The Summary Timer is configurable in units of seconds;
- A per-intercept configurable count threshold is reached.

These elements will be delivered either directly to DF2 or via an MF for each packet flow if available:

Table C: I-WLAN Packet Data Summary Report - PDG

Observed MSISDN
Observed IMSI
Observed NAI
Event Type
Event Time
Event Date
Correlation number
WLAN UE Local IP Address
WLAN UE Remote IP address
WLAN Access Point Name
Network Element Identifier
Initiator (optional)
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Flow Label (IPv6 only)
Summary Period
Packet Count (for this summary period)
Sum of Packet Sizes (for this summary period)

Table D: I-WLAN Packet Data Summary Report - WAG

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
WLAN UE IP address
WLAN PDG Tunnel Endpoint IP address
WLAN Access Point Name
NAS IP/IPv6 address
Tunnel Protocol
Source Ports
Destination Ports
Network Element Identifier
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Flow Label (IPv6 only)
Summary Period
Packet Count (for this summary period)
Sum of Packet Sizes (for this summary period)

If the packets are IPv4, the sum of all observed packet sizes is the sum of the values contained in the Total Length field of each packet as specified in IETF RFC 791 [39].

If the packet is IPv6, the sum of all observed packet sizes is the sum of the values contained in the Payload Length field for each packet as specified in IETF RFC 2460 [40].

If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report shall not be sent.

10 Interception of Multimedia Broadcast/MultiCast Service (MBMS)

10.0 General

MBMS provides video or similar streamed services via either point to point multicast or cell broadcast mechanisms between an operator content server (BM-SC) and UEs as defined in TS 23.246 [20]. This section details the stage 2 Lawful Interception requirements for MBMS.

NOTE: Generic Broadcast services where the UE receives the broadcast in IDLE mode and there is no subscription relationship between the UE and the BM-SC are out of scope. In addition 3rd party BM-SC services where the operator is not responsible for content encryption and subscription management are out of scope.

Figure 10.1 shows the extract from the reference configuration which is relevant for the invocation of the Lawful Interception of the MBMS Services.

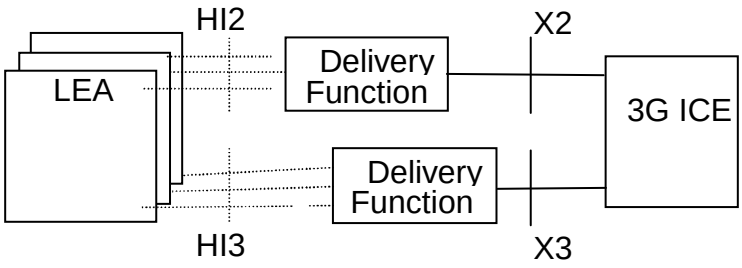


Figure 10.1: Functional model for invocation of Lawful Interception for MBMS Services

10.1 Provision of Content of Communications

Interception of the content of communications for MBMS services if available, may be provided by the underlying transport bearer interception functionality (e.g. GSN, PDG or NGN network) and is therefore subject to the current transport bearer interception functionality detailed in other parts of this specification.

10.2 Provision of Intercept Related Information

10.2.0 General

Figure 10.2 shows the transfer of intercept related information to the DF2. If an event for / from a mobile subscriber occurs, the BM-SC shall send the relevant data to the DF2.

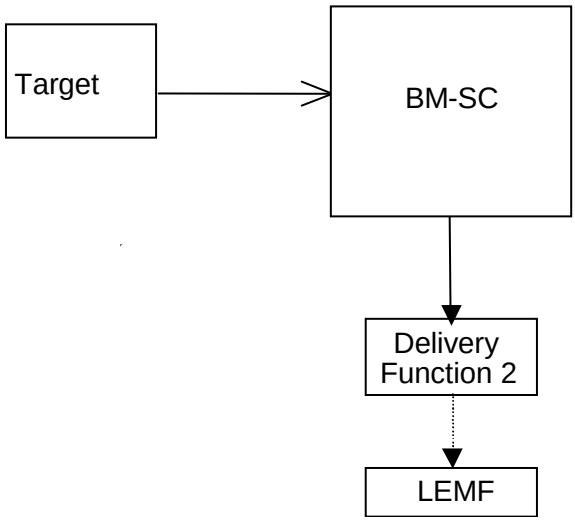


Figure 10.2: Provision of Intercept Related Information

10.2.1 X2-interface

The following information needs to be transferred from the BM-SC to the DF2 in order to allow a DF2 to perform its functionality:

- target identity;
- events and associated parameters as defined in clauses 10.3.2 may be provided;
- For Further Study:- Encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

The IRI should be sent to DF2 using a reliable transport mechanism.

10.2.2 MBMS LI Events and Event Information

Intercept Related Information (Events) are necessary are necessary for the following;

- Service Joining.
- Service Leaving.
- Start of Interception with Service Active.
- Subscription Activation.
- Subscription Modification.
- Subscription Termination.

Events shall include changes resulting from direct communication between the UE and BM-SC and off-line subscription changes (e.g. changes made by operator customer services on behalf of the subscriber).

A set of possible elements as shown in Table 10.2.2 are used to generate the events.

Table 10.2.2: Information Events for MBMS Event Records

Element
Observed IMSI IMSI of the target.
Observed Other Identity Other Identity of the target.
Event type Description which type of event is delivered:- Service Joining; Service Leaving; Subscription Activation; Subscription Modification; Subscription Termination.
Event date Date of the event generation in the BM-SC.
Event time Time of the event generation in the BM-SC. Timestamp shall be generated relative to the BM-SC server internal clock.
MBMS Subscribed Service Details of the MBMS Service to which the target has subscribed.
MBMS Service Joining Time Requested MBMS Service Joining Time
MBMS Service Subscription List List of all users subscribed to MBMS Service to which target has requested Joining.
Correlation Number The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records.
Network Element Identifier Unique identifier for the element reporting the ICE.
Initiator The initiator of the request either the UE or Off-line BM-SC access (eg customer services agent or internet).
Visited PLMN ID Identity of the visited PLMN to which the user is registered
APN Access Point Name on which this IP multicast address is defined.
Multicast/Broadcast Mode MBMS bearer service in broadcast or multicast mode
IP IP/IPv6 multicast address(multicast mode only) IP or IPv6 multicast address identifying the MBMS bearer described by this MBMS Bearer Context.
List of Downstream Nodes List of downstream nodes that have requested the MBMS bearer service and to which notifications and MBMS data have to be forwarded.
MBMS Leaving Reason Indicates whether UE initiated/requested leaving, or whether BM-SC/network terminated the Service to the UE (e.g. GSN session dropped or BM-SC subscription expired etc).

NOTE: Generation of Correlation Number is FFS.

10.3 Structure of MBMS Events

10.3.1 Service Joining

For MBMS Service Joining, a Service Joining event is generated. The elements, shown in Table 10.,3.1 will be delivered to the DF2, if available, by the BM-SC. A new Service Joining Event shall be generated for each individual service joined.

Table 10.3.1: Service Joining

Observed IMSI	
Event Type	
Event Time	
Event Date	
MBMS Subscribed Service	
MBMS Service Joining Time	
Network Element Identifier	
Initiator	
IP/IPv6 Multicast Address	(If Applicable)
Visited PLMN ID	(If Applicable)
Multicast/Broadcast Mode	
APN (If Available)	
List of Downstream Nodes	(If Available)
MBMS Service Subscription List	(Optional)

10.3.2 Service Leaving

For MBMS Service Leaving, a Service Leaving event is generated. The elements, shown in Table 10.3.2 will be delivered to the DF2, if available, by the BM-SC. A new Service Leaving Event shall be generated for each individual service leaving.

Table 10.3.2: Service Leaving

Observed IMSI	
Event Type	
Event Time	
Event Date	
MBMS Subscribed Service	
Network Element Identifier	
Initiator	
IP/IPv6 Multicast Address	(If Applicable)
Visited PLMN ID	(If Applicable)
MBMS Service Subscription List	(Optional)
MBMS Service Leaving Reason	

10.3.3 Start of Interception with Service Active

For Start of Interception where MBMS Service Joining has already occurred prior to start of interception, a Start of Interception with Service Active event is generated. The elements, shown in Table 10.3.3 will be delivered to the DF2,

if available, by the BM-SC. A new Start of Interception with Service Active Event shall be generated for each individual service the target is subscribed to.

Table 10.3.3: Start of Interception with Service Active

Observed IMSI	
Event Type	
Event Time	
Event Date	
MBMS Subscribed Service	
MBMS Service Joining Time	
Network Element Identifier	
Initiator	
IP/IPv6 Multicast Address	(If Applicable)
Visited PLMN ID	(If Applicable)
Multicast/Broadcast Mode	
APN (If Available)	
List of Downstream Nodes	(If Available)
MBMS Service Subscription List	(Optional)

10.3.4 Subscription Activation

For MBMS Subscription Activation, a Subscription Activation event is generated. The elements, shown in Table 10.3.4 will be delivered to the DF2, if available, by the BM-SC. If Subscription Activation is performed simultaneously for more than one service, a separate event shall be generated for each service activated.

Table 10.3.4: Subscription Activation

Observed IMSI	
Event Type	
Event Time	
Event Date	
MBMS Subscribed Service	
Network Element Identifier	
Initiator	
IP/IPv6 Address	(If Applicable)
Visited PLMN ID	(If Applicable)
MBMS Service Subscription List	(Optional)

10.3.5 Subscription Modification

For MBMS Subscription Modification, a Subscription Modification event is generated. The elements, shown in Table 10.3.5, will be delivered to the DF2, if available, by the BM-SC. If Subscription Modification is performed simultaneously for more than one service, a separate event shall be generated for each service modified.

Table 10.3.5: Subscription Modification

Observed IMSI	
Event Type	
Event Time	
Event Date	
MBMS Subscribed Service	
Network Element Identifier	
Initiator	
IP/IPv6 Address	(If Applicable)
Visited PLMN ID	(If Applicable)
MBMS Service Subscription List	(Optional)

10.3.6 Subscription Termination

For MBMS Subscription Termination, a Subscription Termination event is generated. The elements, shown in Table 10.3.6 will be delivered to the DF2, if available, by the BM-SC. If Subscription Termination is performed simultaneously for more than one service, a separate event shall be generated for each service performed.

Table 10.3.6: Subscription Modification

Observed IMSI	
Event Type	
Event Time	
Event Date	
MBMS Subscribed Service	
Network Element Identifier	
Initiator	
IP/IPv6 Address	(If Applicable)
Visited PLMN ID	(If Applicable)
MBMS Service Subscription List	(Optional)

11 IMS Conference Services

11.1 Background for IMS Conference Services

The entire clause 11 is a national option and is subject to national regulations. The covered cases are where the conference services are in the domain of the intercepting operator. The following cases are covered.

1. A target's conference call is the target. This may be where the target is the head of the conference. IRI and CC for this conference is reported. The following are examples of information that is reported.

   a. For example, the starting and ending of a conference as well as any parties joined or removed from the conference call are reported.

   b. Reporting of CC for held conferences initiated by the target.

2. A conference that itself is directly the target of interception. This case is applicable only provided that the conference is identified by a proper identity for LI in IMS domain (Conference URI or Conference Factory URI). The IRI and CC for this conference is reported.

   a. For example, the starting and ending or a conference as well as any parties joined or removed from the conference call are reported.

The case when an target joins an associate's conference is for further study.

The key elements for interception of conference services are the AS/MRFC and MRFP. IRI associated with the conference services that are to be intercepted is reported by the AS/MRFC while the CC associated with the conference service is reported by the MRFP.

National regulations on a per interception basis may limit delivery of communications (CC and IRI) of an outbound international roaming target by the HPLMN as described in clause 5.1.4 of TS 33.106 [7].

If roaming interception is not allowed and it is determined that the target is outside the country, the HPLMN shall act as follows:

- The HPLMN shall not report IRI and CC for the target’s conferencing services while the target is in the VPLMN and is connected to the HPLMN conferencing service.

Non-communications-associated IRI (e.g. those identified by the HSS) are not affected by this requirement.

11.1A Start of Interception for IMS Conference Services

Interception (as defined in 11.1) for IMS Conference Services is started when the first of any one of the following occurs:

- When a target requests that a conference be created
- When a target successfully provisions a conference
- When a target provisioned or requested conference is started (i.e., the first party is joined to the conference)
- When a conference that is a target of interception is started (i.e., the first party is joined to the conference)
- When interception is activated (on a conference or a conference owner) during an ongoing conference
- When parties have joined a conference and communication is started or enabled by the conference server in cases where the conference is a target of interception or when it is a target's conference.

If the target of interception has provisioned or requested a conference to be created, interception on IMS Conference Services shall begin regardless whether the target of interception has joined the conference. Interception of IMS Conference Services shall continue if the target of interception is on hold and the conference continues.

11.2 Provision of Intercepted Content of Communication - IMS Conference Services

11.2.0 General

The access method for the delivery of IMS conference services intercept content of communication (CC) is based on duplication of packets without modification at the MRFP for conferences that are to be intercepted. The duplicated packets with additional information in the header, as described in the following sections, are sent to DF3 for further delivery. For a target's conference call held by the target, the MRFP duplicates the CC for conference call held by the target, in accordance with national regulations. For a conference call that is the target of interception, the MRFP duplicates the CC for the conference.

NOTE: Void

There is an issue of combined versus separated delivery. With combined delivery, one method for intercepting the CC would be to create a virtual conference port (not visible to others) through which a copy of the combined CC is passed over the X3 interface (Y conferees means 1 content stream). With the separated delivery approach, each conferee's connection to the conference shall be intercepted and passed over the X3 interface (Y conferees, means Y pairs of bi-directional content streams).

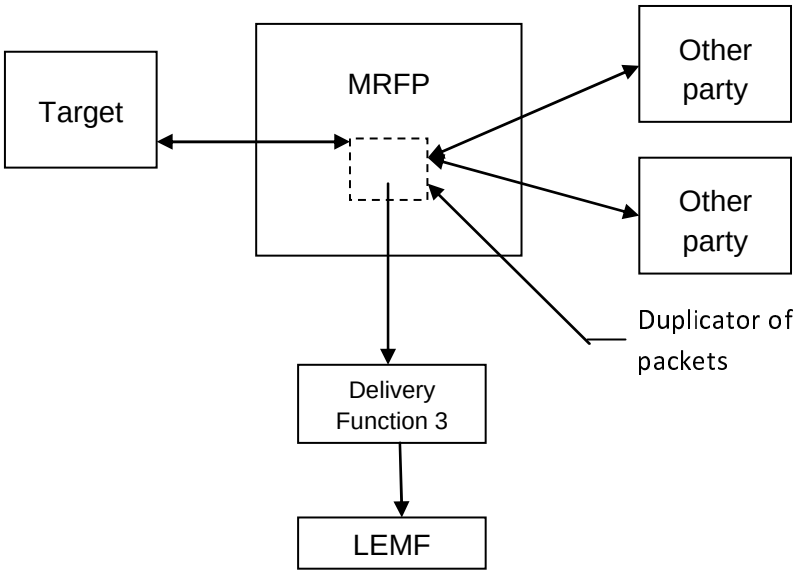


Figure 11.1: Configuration for interception of IMS Conference Services CC

11.2.1 X3-interface

In addition to the intercepted content of communications, the following information may need to be transferred from the MRFP to the DF3 in order to allow the DF3 to perform its functionality:

- identity used for interception;
- correlation number.

NOTE 1: Void.

Information passed between the MRFC and MRFP for correlation shall uniquely identify the mixing of associated media streams for a conference distinct from any other mixing or media handling. An example is how H.248 uses a context identifier to do this.

- the identity of source (i.e., conference party identity) of a media stream;
- time stamp - optional;
- direction (incoming or outgoing stream) - optional.

NOTE 2: When the media is delivered in a mixed format, the identity of the media stream source might be unknown.

11.3 Provision of Intercept Related Information for IMS Conference Service

11.3.0 General

Figure 11.2 shows the transfer of intercept related information to the DF2. If an event for / from or associated with a conference server occurs, the AS/MRFC sends the relevant data to the DF2.

NOTE: Reporting of non-transmission related actions of a target's subscriber controlled input (e.g., signalling "mute" commands) is for further study.

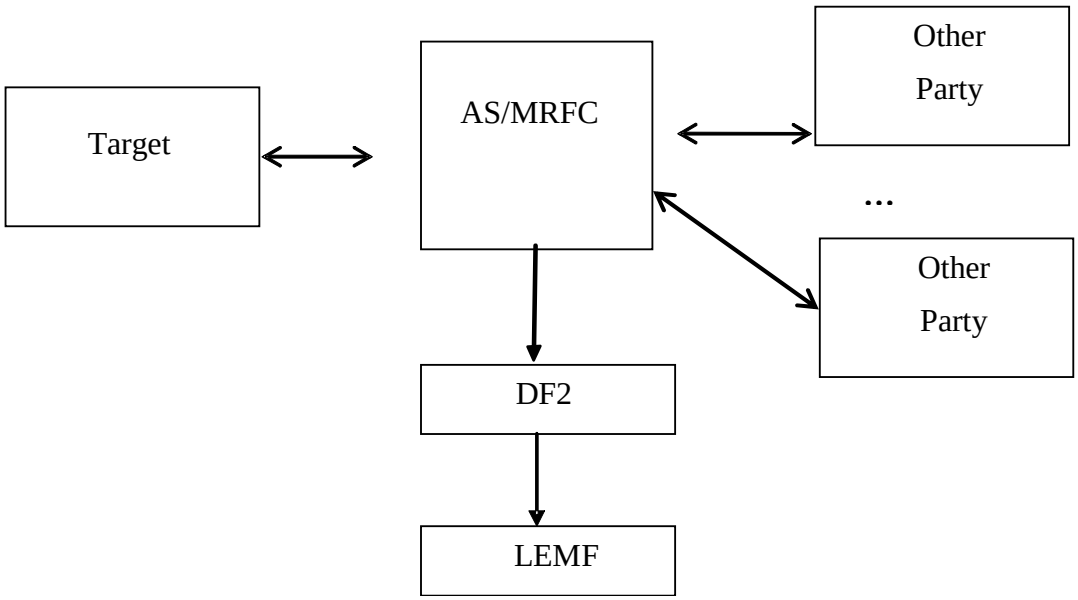


Figure 11.2: Provision of Intercept Related Information for IMS Conferencing

11.3.1 X2-interface

The following information may need to be transferred from the AS/MRFC to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMPU, IMPI, Conference URI);
- events and associated parameters as defined in section 11.3.3 "Structure of Conference Events" may be provided;

- Correlation number;
- Bandwidth and media descriptions (e.g., as associated with SDP negotiation) associated with the parties' bearer connection to the conference.

The IRI should be sent to DF2 using a reliable transport mechanism.

11.3.2 IMS Conference Events and Event Information

The following events are applicable to AS/MRFC:

- Start of Conference
- Party Join;
- Party Leave;
- Conference Bearer Modification;
- Start of Intercept on an Active Conference;
- End of Conference;
- Creation of Conference;
- Update of Conference.

NOTE 1: Reporting of Floor Control events from the MRFP is FFS.

A set of possible elements as shown below that may be reported with the events. Information associated with the events is transmitted from the AS/MRFC server to DF2.

Table 11.3.1: Information Elements for Conference Events

Element
Observed IMPU IMS Public User identity (IMPU) of the target. In some cases, this identity may not be observed by the MRFC. Also see Note 1.
Observed IMPI IMS Private User identity (IMPI) of the target. In some cases, this identity may not be observed by the MRFC. Also see Note 1.
Observed Other Identity Target Identifier with the NAI of the target.
Event Type Description which type of event is delivered: Start of Conference, Party Join, Party Leave, Start of Intercept on an Active Conference, Conference End.
Event Date Date of the event generation in the AS/MRFC.
Event Time Time of the event generation in the AS/MRFC server. Timestamp shall be generated relative to the AS/MRFC internal clock.
Correlation Number The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records.
Network Element Identifier Unique identifier for the element reporting the ICE.
Initiator The initiator of a request, for example, the target, the network, a conferee.
Join Party ID Identity of the party successfully joining or attempting to join the conference.
Leave Party ID Identity of the party leaving or being requested to leave the conference.
List of Potential Conferees Identifies each of the parties to be invited to a conference or permitted to join the conference (if available).
Observed Conference URI A URI associated with the conference being monitored.
Temporary Conference URI A temporarily allocated URI associated with a conference being monitored.
List of Conferees Identifies each of the conferees currently on a conference (e.g., via SIP URI or TEL URI).
Failed Conference Start Reason Provides a reason for why a conference start attempt failed.
Failed Party Join Reason Provides a reason for why a party join attempt failed.
Party Leave Reason Provides a reason for the party leaving.
Failed Party Leave reason Provides a reason for why a party leave attempt failed.
Conference End Reason Provides a reason for why the conference ended.
Potential Conference Start Date and Time The expected start date and time of the conference, if start time information is configured in the system.
Potential Conference End Date and Time The expected end date and time of the conference, if such end information is configured in the system.
Recurrence Information Information indicating the recurrence pattern for the event as configured for the created conference.
Identity(ies) of Conference Controller Identifies the parties that have control privileges on the conference, if such information is configured in the system.
Bearer Modify ID Identifies the party modifying a conference bearer.
Failed Bearer Modify Reason Provides a reason for a bearer modification attempt failed.
Failed Conference End Reason Provides a reason why a conference end attempt failed.
Join Party Supported Bearers Identifies the bearer types supported by the party joining the conference.
List of Waiting Conferees Identifies each of the parties that have called into a conference but have not yet joined.
Media Modification Identifies how the media was modified (i.e., added, removed, changed)

Parties Affected by Bearer Modification Identifies all conference party identities affected by the bearer modification.
Supported Bearers Identifies all bearer types supported by a conferee in a conference.
Update Type Indicates what update was done to a conference (e.g., update List of Potential Conferees, update of Start Time, update of End Time, Update of Recurrence Information, Cancellation of Conference, etc.).

NOTE 2: In most cases, either the IMPU or IMPI may be available, but not necessarily both.

11.3.3 Structure of Conference Events

11.3.3.1 Start of Conference

For the start of a conference, a Start of Conference-event is generated in the following cases:

- When a target provisioned or requested conference or a conference that is the target of interception is started. The conference is started when the first party is joined to the conference.;
- When a conference that is a target of interception or when a target provisioned or requested conference fails to start.

The fields, shown in Table 11.3.2, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.2: Start of Conference

Observed IMPU
Observed IMPI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
List of Potential Conferees
List of Conferees
List of Waiting Conferees
Supported Bearers
Observed Conference URI
Temporary Conference URI
Failed Conference Start Reason

11.3.3.2 Party Join

A Party Join-event is generated in the following cases:

- When a party successfully joins the target's conference or a conference that is the target of interception.
- When a party unsuccessfully attempts to join the target's conference or a conference that is the target of interception.

The fields, shown in Table 11.3.3, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.3: Party Join

Observed IMPU
Observed IMPI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Join Party ID
Join Party Supported Bearers
Initiator (of the Party Join request)
Observed Conference URI
Temporary Conference URI
Failed Party Join Reason (e.g., not available)

11.3.3.3 Party Leave

A Party Leave-event is generated in the following cases:

- When a party leaves a target's conference or a conference that is the target of interception. This includes situations where the party simply disconnects themselves from the conference (hang up), the party's connection to the conference is broken (e.g., party leaves wireless coverage area), and where the party's connection to the conference is forcefully terminated due to another party's drop request or operator policy.

- When a party unsuccessfully attempts to drop another party from the conference. This applies to all the conferencing scenarios described earlier.

The fields, shown in Table 11.3.4, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.4: Party Leave

Observed IMPU
Observed IMPI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Leave Party ID
Supported Bearers (of Leaving Party)
Initiator (of the Party Leave request)
Observed Conference URI
Temporary Conference URI
Party Leave Reason - see Note.
Failed Party Leave Reason

NOTE: A party could drop off the conference for normal reasons (e.g., just hang up) or could be removed by a conference controller.

11.3.3.3A Conference Bearer Modification

A Conference Bearer Modification-event is generated for the following cases:

- When a party to a conference successfully modifies (i.e., add, remove, change) a bearer stream in the conference;

- When a party to a conference unsuccessfully attempts to modify (i.e., add, remove, change) a bearer stream in the conference.

The fields, shown in Table 11.3.4A, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.4A: Conference Bearer Modification

Observed IMPU
Observed IMPI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Observed Conference URI
Temporary Conference URI
Bearer Modify ID
Media Modification
Parties Affected by Bearer Modification
Failed Bearer Modify Reason

11.3.3.4 Start of Intercept on an Active Conference

A Start of Intercept on an Active Conference-event (a conference with at least one party) is generated for the following cases:

- When interception is activated during an ongoing conference call.

The fields, shown in Table 11.3.5, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.5: Start of Intercept with an Active Conference

Observed IMPU
Observed IMPI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
List of Conferees
Supported Bearers
Observed Conference URI
Temporary Conference URI

11.3.3.5 Conference End

When a conference is terminated, a Conference End-event is generated in the following cases:

- When a target provisioned or requested conference is terminated. This occurs when the last party on the conference leaves or the conference is terminated by the conference server;

- When there is an unsuccessful attempt to terminate a target provisioned or requested conference or a conference that is the target of interception.

The fields, shown in Table 11.3.6, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.6 End of Conference

Observed IMPU
Observed IMPI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Initiator (e.g., target, network, conferee) - see Note
Observed Conference URI
Temporary Conference URI
Conference End Reason
Failed Conference End Reason

NOTE: The initiator can indicate that the decision to end the conference was the target or conferee, if the target or conferee sends an explicit command to end the conference. It could be the network, if it determines the time length for the conference is ended.

11.3.3.6 Creation of Conference

When a conference is created, a Creation of Conference-event is generated in the following cases:

- When a target successfully provisions or requests a conference to be created.

This event is applicable provided that at least one of the two identities (IMPU, IMPI) are available at the AS/MRFC. Other scenarios, such as in case the creation is done via a web interface and the IMPU/IMPI cannot be seen are outside the scope of this specification.

The fields, shown in Table 11.3.7, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.7 Creation of Conference

Observed IMPU
Observed IMPI
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
List of Potential Conferees (if available)
Observed Conference URI
Temporary Conference URI
Potential Conference Start Date and Time (if available) - See Note 1
Potential Conference End Date and Time (if available) - See Note 1
Recurrence Information - See Note 2.
Identity(ies) of Conference Controller

NOTE 1: This information is statically provisioned information and is not correlated to the timestamp requirements for LI.

NOTE 2: Recurrence information indicates the frequency or pattern of recurrence of the created conference.

11.3.3.7 Update of Conference

When a conference is updated, an Update of Conference-event is generated in the following cases:

- When a target successfully provisions or requests a conference to be updated (e.g., changes to List of Potential Conferees, Start Time, End Time, Recurrence Information, or Cancellation of Conference).

This event is applicable provided that at least one of the two identities (IMPU, IMPI) are available at the AS/MRFC. Other scenarios, such as in case the update is done via a web interface and the IMPU/IMPI cannot be seen are outside the scope of this specification.

The fields, shown in Table 11.3.8, will be delivered to the DF2, if available, by the AS/MRFC.

Table 11.3.8 Update of Conference

Observed IMPU
Observed IMPI
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Update Type
List of Potential Conferees (if available)
Observed Conference URI
Temporary Conference URI
Potential Conference Start Date and Time (if available) - See Note 1
Potential Conference End Date and Time (if available) - See Note 1
Recurrence Information - See Note 2.
Identity(ies) of Conference Controller

NOTE 1: This information is statically provisioned information and is not correlated to the timestamp requirements for LI.

NOTE 2: Recurrence information indicates the frequency or pattern of recurrence of the created conference.

12 Lawful Interception for Evolved Packet System

12.1 LI functional architecture for EPS

In addition to the reference configurations applicable to PS interception, the following figures contain the reference configuration applicable for the lawful interception in the EPS nodes (TS 23.401 [22], TS 23.402 [23]):

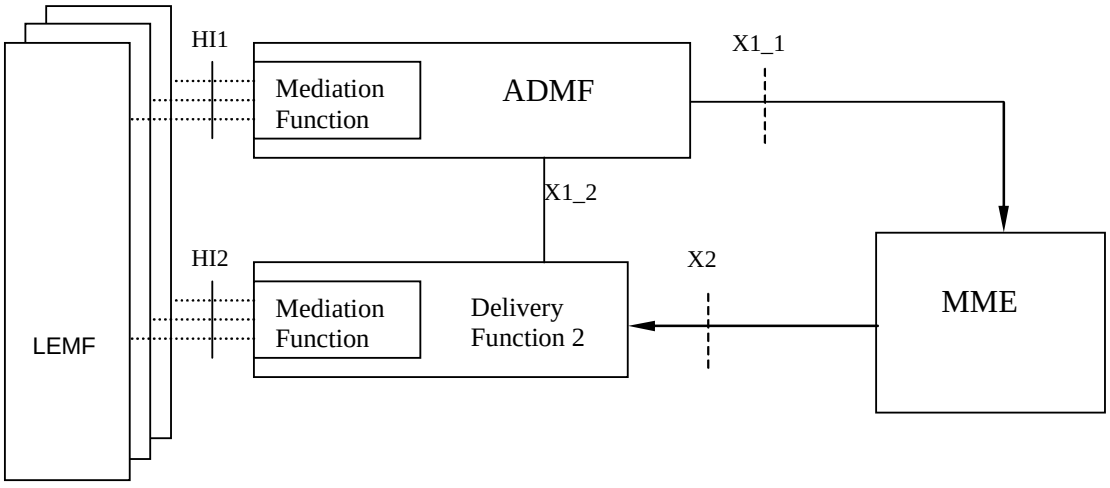


Figure 12.1.1: MME Intercept configuration

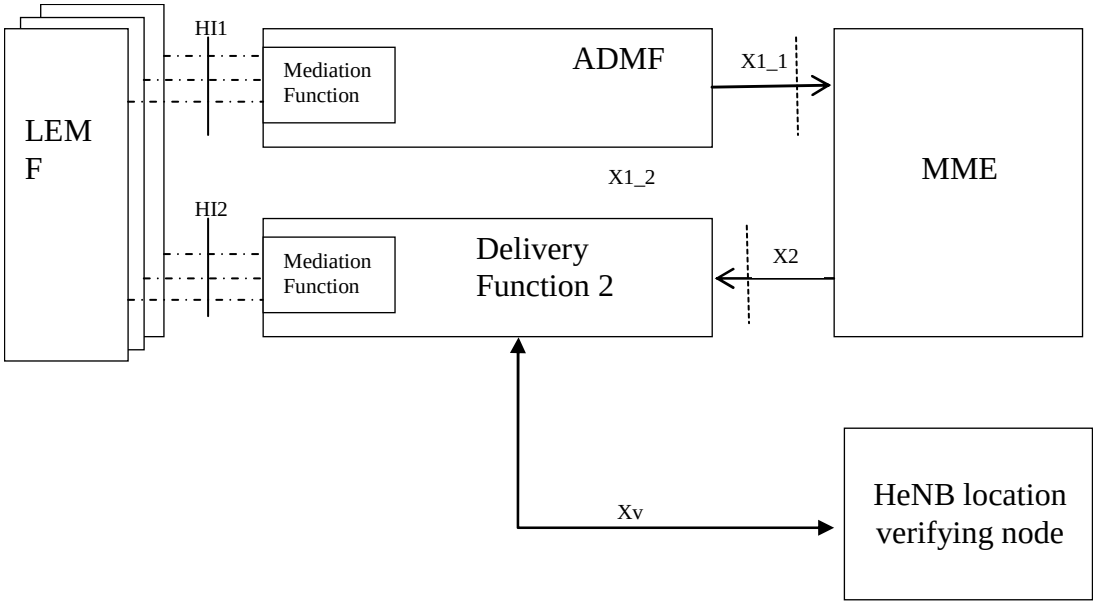


Figure 12.1.1a: Configuration for Intercept of HeNB

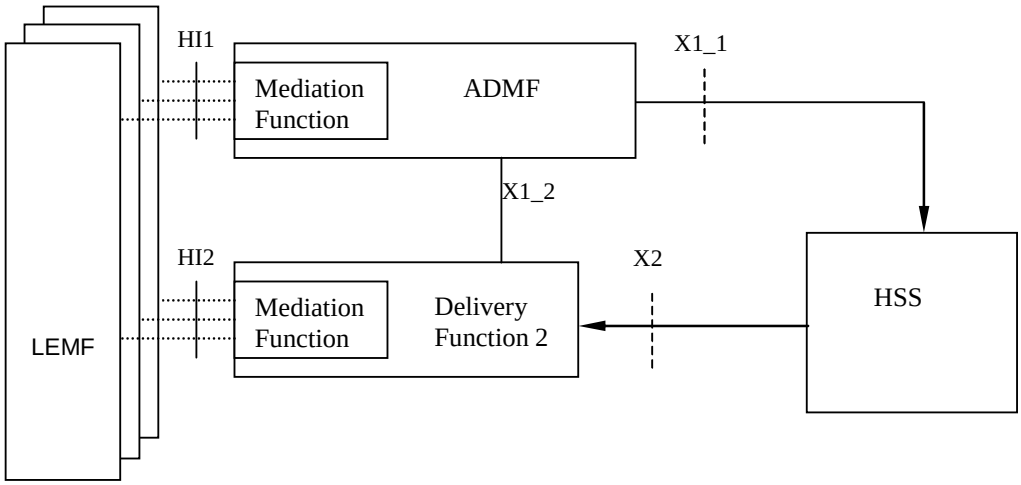


Figure 12.1.2: HSS Intercept configuration

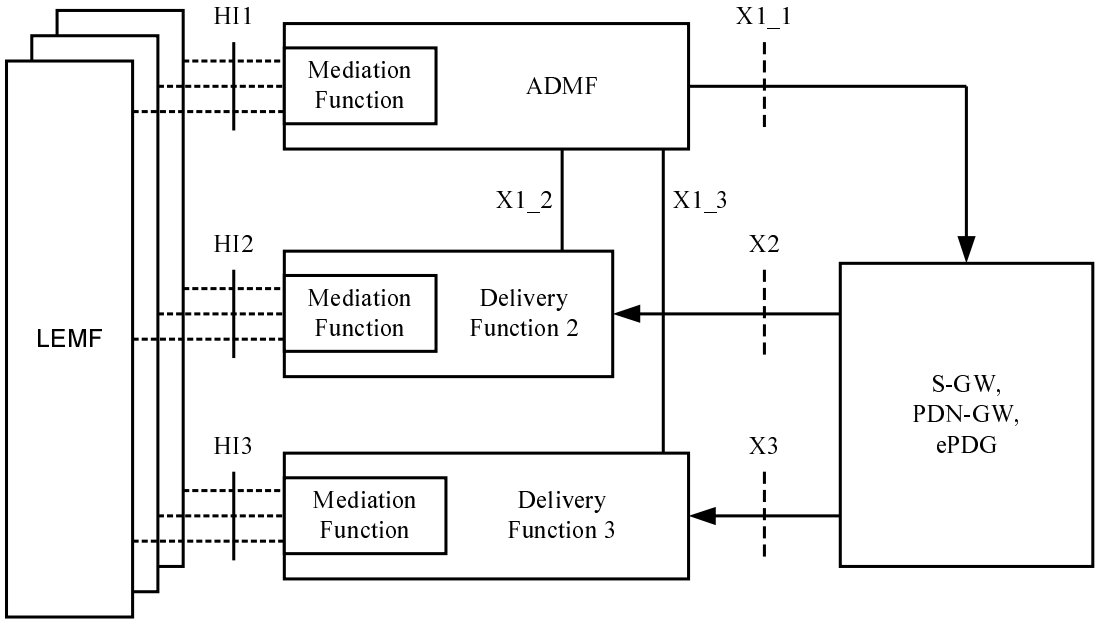


Figure 12.1.3: S-GW, PDN-GW, ePDG Intercept configuration

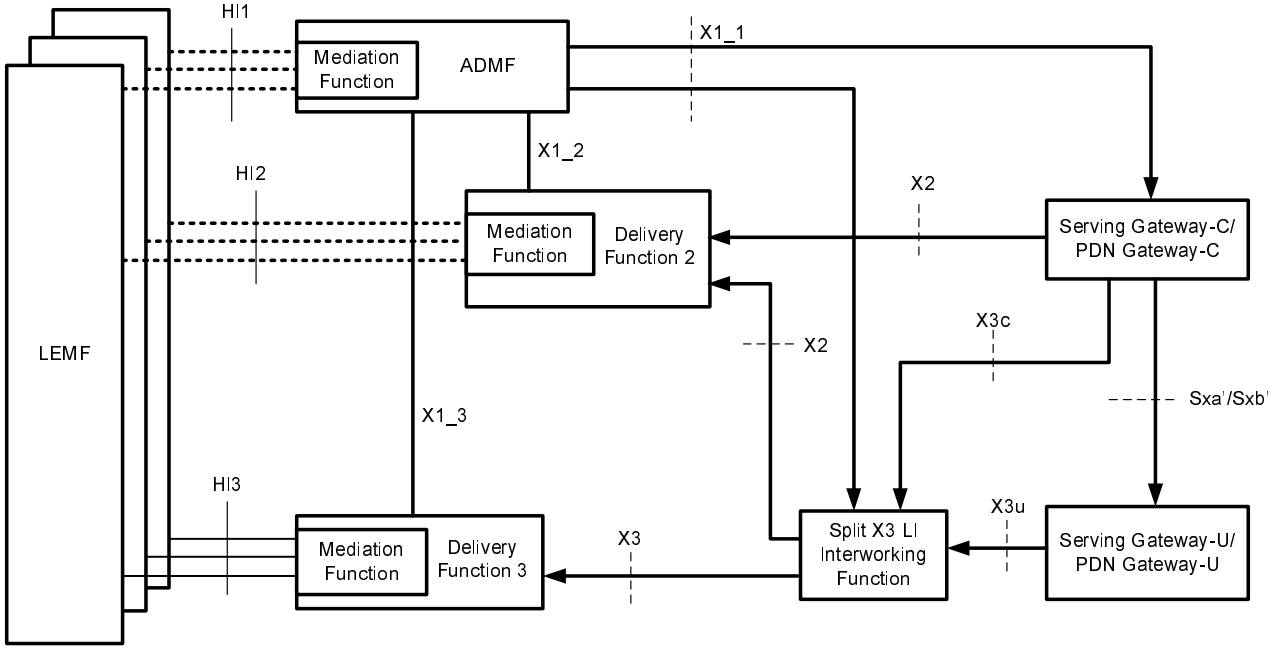


Figure 12.1.4: Intercept Configuration for SGW and PGW with CUPS

The definition of the LI functional entities (ADMF, DF, MF, LEMF) and interfaces (X, HI) is the same as for 3G as given in chapter 4. Packet Header Information Reporting is a national option. For Packet Data Header Information reporting, a S-GW/PDN-GW either isolates the relevant data and sends it to the DF2 or sends the packet stream to another entity in the network (e.g., DF3) for isolation which then provides the relevant data to the DF2.

National regulations on a per interception basis may limit delivery of communications (CC and IRI) of an outbound international roaming target by the MME/S-GW/PDN-GW as described in clause 5.1.4 of TS 33.106 [7].

If roaming is not allowed and it is determined that the target is outside the country, the HPLMN shall act as follows:

- all session related EPS events defined in clause 12 are subject to this mechanism;
- the HPLMN shall not report IRI and CC for Evolued Packet services while the target is in the VPLMN.

Non-communications-associated IRI (e.g. those identified by the HSS) are not affected by this requirement.

Procedures for LI activation, deactivation and interrogation are the same as for 3G as given in chapter 5, provided that:

- the 3G ICE is replaced by the EPS node;
- the proper target identity applicable to EPS node is used.

When the SGSN is used as node in the Evolved Packet System, to support 2G/3G access and mobility between E-UTRAN and pre-E-UTRAN 3GPP radio access technologies, it is subjected to all the related PS requirements specified throughout this document.

Figure 12.1.1a depicts how the HeNB location information is transferred from the HeNB location verifying node per TS 33.320 [34] to the DF2 via an Xv interface, in order to allow the DF2 to perform its functionality. The public IP Address of the HeNB is provided to the HeNB location verifying node. The manner that the HeNB location verifying node provides the DF2 with the HeNB location and HeNB IP Address is outside the scope of this document. Additional information on HeNB interception is found in Clause 13.

Figure 12.1.4 depicts the LI configuration for SGW and PGW with PLMN implementing CUPS (see 3GPP TS 23.214 [75]). This is described in subclause 12.9. The Sxa' and SXb' are the LI specific instances of Sxa and Sxb reference points. The X2 reference point support at SX3LIF is required only if the first option described in sub-clauses 12.9.4.1 and 12.9.4.2 are used to generate the IRI events that require access to the user plane packets (e.g. packet data header information). The IRI events generated by the SX3LIF are therefore limited to the IRI events that require access to user plane packets. The administrative information passed onto the SX3LIF is to provide the DF2 and DF3 addresses to enable SX3LIF to deliver those IRI events to the DF2, and the CC to the DF3.

The target identities for 3GPP HeNB interception can be IMSI, MSISDN, IMEI, or ME Id. Use of the HeNB ID or the CSG ID as a target identity is FFS.

12.2 Functional requirements for LI in case of E-UTRAN access and GTP based S5/S8.

12.2.0 General

The target identities for interception at the MME, HSS, S-GW , PDN-GW and LI LCS Client are IMSI, MSISDN and ME (Mobile Equipment) Identity.

NOTE 1: Void.

Details about information included in the ME Identity and the relationship with IMEI needs to be considered. The term Mobile Equipment Identity is used in this text according to TS 23.401 [22] so as to indicate that the EPC should support multiple equipment identity formats (e.g. those from 3GPP2, WiMAX, etc) as well as the IMEISV.

NOTE 2: In case of local breakout the PDN Gateway is in the VPLMN. In this case LI relevant information in the H-PLMN might be available at the H-PCRF. Interception at the H-PCRF is FFS.

NOTE 3: In case the ME Identity and/or MSISDN is not available in a node, interception based on the missing identity is not applicable at that node.

NOTE 4: MSISDN is a possible identity available in the EPC nodes, which may be provided by the HSS to the MME and then forwarded to the S-GW/PDN-GW.

As the MME only handles control plane, interception of Content of Communication is applicable only at the S-GW and PDN-GW. As the HSS only handles signaling, interception of Content of Communication is not applicable at this node.

LI in the PDN-GW is a national option.

For the delivery of the CC and IRI the S-GW and/or, per national option PDN-GW provides correlation number and target identity to the DF2 and DF3 which is used there in order to select the different LEAs where the product shall be delivered.

The correlation number is unique in the whole PLMN and is used to correlate CC with IRI and the different IRI's of one EPS bearer.

The correlation number shall be generated by using existing parameters related to the EPS bearer.

NOTE 5: Void.

If interception has been activated for both parties of the Packet Data communication both CC and IRI shall be delivered for each party as separate intercept activity.

Editor's note: Location Dependent Interception for EPC is FFS.

NOTE 6: For LALS, any UE (including inbound roamers) served by the PLMN can be targeted.

12.2.1 Provision of Intercept Related Information

12.2.1.0 General

Intercept Related Information (Events) shall be sent at the Mobile Entity Attach, Mobile Entity Detach, Tracking Area/EPS Location Update, LALS Location Report, Bearer activation (valid for both Default and Dedicated bearer), Start of Intercept with bearer active, Start of Interception with E-UTRAN attached UE, Bearer Modification, Bearer Deactivation, Serving Evolved Packet System (applicable to the HSS), UE requested PDN connectivity, UE requested PDN disconnection, and UE requested bearer resource modification.

Serving Evolved Packet System and HSS related events event reporting are national options.

12.2.1.1 X2-interface

The following information needs to be transferred from the EPS nodes or the HSS to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMSI, MSISDN, ME identity);
- events and associated parameters as defined in clauses 12.2.1.2 and 12.2.3 may be provided;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of Location (if target location provided);
- correlation number;
- Quality of Service (QoS) information (if available);
- encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

For HeNB interception, the MME shall provide in addition the following:

- HeNB Identity;
- HeNB location.

HeNB location information needs to be transferred from the HeNB location verifying node to the DF2 in order to allow the DF2 to perform its functionality.

The EPS nodes detect packets containing packet header information in the communications path but the information needed for Packet Header Information Reporting may need to be transferred from the EPS nodes either directly to the DF2 or via another network entity in order to allow the DF2 to perform its functionality.

The IRI should be sent to DF2 using a reliable transport mechanism.

12.2.1.2 Structure of the events

There are several different events in which the information is sent to the DF2 if this is required. Details are described in the following clause. The events for interception are configurable (if they are sent to DF2) in the EPC nodes or the HSS and can be suppressed in the DF2. The network procedures for which the events are generated are defined in TS 23.401 [22].

The following events are applicable to the MME:

- Attach;

- Detach;
- Tracking Area/EPS Location Update;
- UE requested PDN connectivity;
- UE Requested PDN disconnection;
- Start of interception with E-UTRAN attached UE.

The following events are applicable to the Serving GW and PDN GW:

- Bearer activation (valid for both Default and Dedicated bearer);
- Start of intercept with bearer active;
- Bearer modification;
- Bearer deactivation;
- UE Requested Bearer Resource Modification;
- Packet Data Header Information.

The following events are applicable to the HSS:

- Serving Evolved Packet System.
- HSS subscriber record change;
- Cancel location
- Register location;
- Location information request.

The following LALS Reports are applicable to the EPS (see Clause 19):

- Report for LALS Target Positioning;
- Report for LALS Enhanced Location for IRI.

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from the nodes to DF2. Available IEs from this set of elements as shown below can be extended in the nodes, if this is necessary as a national option. DF2 can extend available information if this is necessary as a national option. If interception is performed at the PDN GW, then Packet Data Header Information reporting shall also be performed at the PDN GW and not at the Serving GW.

A number of elements shown below can be also associated with the LALS reports. The transmission of the information from the LI LCS Client to DF2 is triggered by an LCS Server/GMLC response to the LI LCS Client request.

Observed MSISDN MSISDN of the target.
Observed IMSI IMSI of the target.
Observed ME Id ME Id of the target; when it coincides with the IMEI, it shall be checked for each activation over the radio interface.
Event type Indicates which type of event is delivered: Attach, Detach, Tracking Area Update, UE requested PDN connectivity, UE Requested PDN disconnection, UE Requested Bearer Resource Modification, Bearer activation, Start of intercept with bearer active, Start of interception with E-UTRAN attached UE, Bearer deactivation, Bearer modification, Serving Evolved Packet System, Packet Data Header Information, HSS subscriber record change, Cancel location, Register location, Location information request. In case of LALS report the event type is absent.
Event date Date of the event generation in the ICE.
Event time Time of the event generation in the ICE. Timestamp shall be generated relative to ICE internal clock.
Change Type This indicates what has been changed (MSISDN, A-MSISDN or IMSI) in the Subscriber Change Record
PDN Type The parameter is applicable to the MME only and provides the IP version (IPv4, IPv4/IPv6, IPv6) requested by the UE.
PDN Address Allocation The parameter is applicable to the S-GW and PDN-GW; it provides the IP version (IPv4, IPv4/IPv6, IPv6) and IP address(es) allocated for the UE.
Protocol Configuration Options Are used to transfer parameters between the UE and the PDN-GW (e.g. Address Allocation Preference by DHCP).
Attach type Indicates the type of attach (may carry indication of handover in case of mobility with non-3GPP access).
Location Information Location Information is the Tracking Area Identity (TAI), TA List assigned to the UE, E-CGI and/or location area identity or the derived Location from the LI LCS Client that is present at the node at the time of event record production. In case of Tracking Area Update event, the last visited TAI of the UE may be applicable. Country and network IDs can be considered as location information, by some national regulations.
Time of Location Date/Time of location. The time when location was obtained by the location source node.
PDN address(es) The UE IP address(es) for the PDN connection.
APN When provided by the MME, the parameter carries the Access Point Name provided by the UE. When provided by the S-GW/PDN-GW, it is the Access Point Name used for the connection.
RAT type The Radio Access Type
APN-AMBR The Aggregate Maximum Bit Rate for the APN.
Handover indication Provides information from the GTPv2 protocol that the procedure is triggered as part of a handover.
Procedure Transaction Identifier Identifies a set of messages belonging to the same procedure; the parameter is dynamically allocated by the UE.
EPS bearer identity An EPS bearer identity uniquely identifies an EPS bearer for one UE accessing via E-UTRAN. The EPS Bearer Identity is allocated by the MME.
Bearer activation/deactivation type Indicates the type of bearer being activated/deactivated, i.e. default or dedicated.
Linked EPS bearer identity Indicates, in case of dedicated bearer, the EPS bearer identity of the default bearer.
Initiator The initiator of the procedure, either the network, HeNB, or the UE.
Switch off indicator Indicates whether a detach procedure is due to a switch off situation or not.
Detach type Parameter sent by the network to the UE to indicate the type of detach.
Traffic Flow Template (TFT) The EPS bearer traffic flow template (TFT) is the collection of all packet filters associated with that EPS bearer.
Traffic Aggregate Description (TAD) The TAD consists of the description of the packet filter(s) for the traffic flow aggregate.
Serving MME address The address of the serving MME.

Old Location Information Location Information of the subscriber before Tracking Area Update.
Correlation Number The correlation number is used to correlate CC and IRI.
Network Element Identifier Unique identifier for the ICE reporting the event.
Logical Function Information Used to distinguish between multiple logical functions operating in a single physical network element.
Failed attach reason Reason for failed attach of the target.
Failed bearer activation reason Reason for failed bearer activation for the target.
Failed Bearer Modification reason The reason for failure of Bearer Modification.
IAs The observed Interception Areas.
Bearer Deactivation cause The cause of deactivation of the PDP context.
EPS Bearer QoS This field indicates the Quality of Service associated with the Bearer procedure.
Request type Indicates the type of request in an UE requested PDN connectivity, i.e. initial request or handover.
CSG Identity Uniquely identifies a CSG within one PLMN. Note: Open HeNBs do not have associated CSGs.
CSG List Identifies the membership of a given CSG (i.e., CSG Identities and associated expiration data for the UEs).
HeNB Identity Uniquely identifies a HeNB (i.e., HeNB equipment ID and HeNB name).
HeNB IP Address The public IP address of the HeNB provided to the HeNB location verifying node
HeNB Location Reports the location of the HeNB used during location verification.
ISP Operator Identity Identifies the ISP through which the HeNB is connected to the SeGW (e.g., IP address).
Security Gateway IP Address The IP Address of the Security Gateway that terminates the tunnel from the HeNB.
Tunnel Protocol The tunnel protocol used between the HeNB and the SeGW.
ULI Timestamp Indicates the time when the User Location Information was acquired. The parameter is specified in TS 29.274 [38].
Destination IP Address The IP address, including type IPv4 or IPv6, of the destination of the IP packet.
Destination Port Number The port number of the destination of the IP packet.
Flow Label (IPv6 only) The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [41]).
Packet Count The number of packets detected and reported (for a particular summary period).
Packet Data Summary Reason The reason for a Packet Data Summary message being sent to the LEMF (e.g., timed out, counter expiration, end of session)
Packet Size The size of the packet. (i.e., Total Length Field in IPv4 or Payload Length field in IPv6)
Source IP Address The IP address, including type IPv4 or IPv6, of the source of the IP packet.
Source Port Number The port number of the source of the IP packet.
Sum of Packet Sizes (for a particular summary period) The sum of values contained in the Total Length fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.
Summary Period Includes the dates and times of the first and last packets in a particular packet data interval.
Transport Protocol (e.g., TCP) The identification of the transport protocol of the packet or packet flow being reported.

UE Local IP Address The UE local IP address (IP SEC terminal Point) reported over GTP based S2b interface TS 29.274 [38] based on local policy for Fixed Broadband access network interworking.
UE UDP Port Used in case of GTP based S2b interface TS 29.274 [38] if NAT is detected and UE Local IP Address is present for Fixed Broadband access network interworking.
WLAN location information Used in case of GTP based S2b interface TS 29.274 [38]. Provides location information in form of TWAN Identifier, if available at ePDG/PDN-GW.
WLAN location timestamp Used in case of GTP based S2b interface TS 29.274 [38]. Provides location information timestamp in form of TWAN Identifier Timestamp, if available at ePDG/PDN-GW.
ProSe Remote UE IDs The identities of the ProSe remote UE connected to the Prose UE-to-NW Relay, see clause 17.3.
ProSe Remote UE IP info The IP address(es) of the ProSe Remote UE connected to the ProSe UE-to-NW Relay, see clause 17.3
location error code LALS positioning error identification code

12.2.2 X3-interface

The access method for the delivering of S-GW and/or PDN-GW Intercept Product is based on duplication of packets without modification at the S-GW and/or PDN-GW. The duplicated packets with additional information in a header are sent to DF3 for further delivery to the LEA.

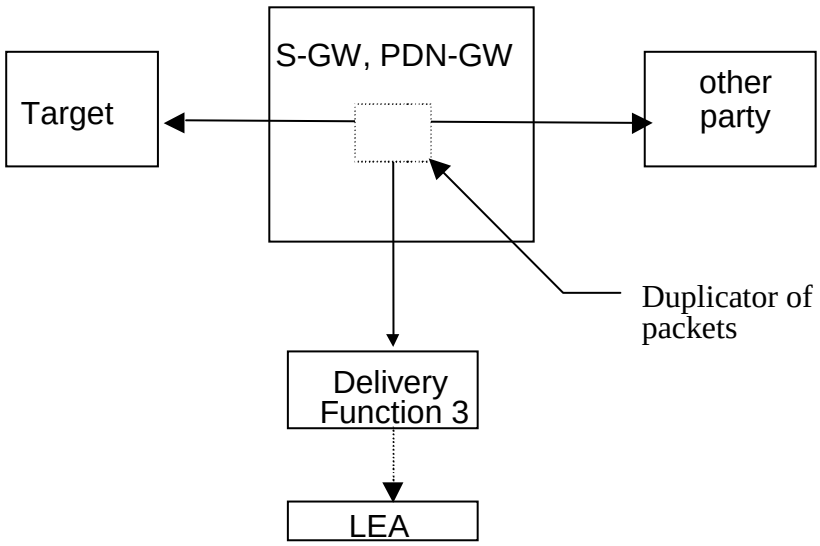


Figure 12.2.2.1: Configuration for interception of S-GW/PDN-GW product data

In addition to the intercepted content of communication, the following information needs to be transferred from the S-GW and/or the PDN-GW to the DF3 to perform its functionality:

- target identity;
- correlation number;
- time stamp (optional);
- direction (indicates whether T-PDU is MO or MT) - optional;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of Location (if target location provided).

NOTE: Location dependent interception for EPC is FFS.

12.2.3 EPS related events

12.2.3.1 Attach

When an attach activation is generated from the mobile an attach event is generated by the MME. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Location Information
Time of Location
Failed attach reason
IAs (if applicable)
PDN Type
APN
Protocol Configuration Options
Attach type
EPS bearer identity
CSG Identity (if closed/hybrid H(e)NB)*
CSG List (if closed/hybrid H(e)NB)*
HeNB Identity*
HeNB IP Address*
HeNB Location*
Security Gateway IP address*
Tunnel Protocol*
ISP Operator Identity*

* These elements are applicable for HeNB interception only.

12.2.3.2 Detach

For detach a detach-event is generated. The following elements will be delivered by the MME to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Location Information
Time of Location
IAs (if applicable)
Detach initiator
Switch off indicator
Detach type
CSG Identity (if closed or hybrid HeNB)*
HeNB Identity*
HeNB IP Address*
HeNB Location*

* These elements are applicable for HeNB interception only.

12.2.3.3 Bearer activation

When a bearer activation is generated a bearer activation-event is generated by the S-GW/PDN-GW. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
RAT type (note 1)
PDN address allocation (note 1)
Event Type
Event Time
Event Date
Correlation number
APN (Access Point Name) (note 1)
Bearer activation Type (default, dedicated)
Network Element Identifier
Logical Function Information
Location Information
Time of Location
Failed bearer activation reason
IAs (if applicable)
EPS bearer QoS (note 2)
APN-AMBR (note 3)
EPS bearer id (NSAPI)
Protocol Configuration Options
Initiator
Procedure Transaction Identifier
Linked EPS bearer identity (note 2)
Traffic Flow Template(s) (TFT) (note 4)
Handover indication
UE Local IP Address (note 5)
UE UDP Port (note 5)
WLAN location information (note 5)
WLAN location timestamp (note 5)

NOTE 1: Only in case of default bearer activation; the parameter includes both PDN type and PDN address(es).

NOTE 2: In case of unsuccessful default bearer activation, the parameter carries the requested EPS bearer QoS, otherwise it carries the EPS bearer QoS associated to the established bearer.

NOTE 3: In case of unsuccessful default bearer activation, the parameter carries the subscribed APN-AMBR, otherwise it carries the APN-AMBR used for the established bearer.

NOTE 4: TFT is applicable only in the case of dedicated bearer.

NOTE 5: Applicable only to ePDG and PDN-GW in case of S2b interface.

NOTE 6: Void.

12.2.3.4 Bearer deactivation

When a bearer deactivation is generated a bearer deactivation-event is generated by the S-GW/PDN-GW. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Correlation number
Bearer deactivation Type (default, dedicated)
Network Element Identifier
Logical Function Information
Location Information
Time of Location
IAs (if applicable)
EPS bearer id
Initiator
Procedure Transaction Identifier
Bearer deactivation Cause (note)
ULI Timestamp
UE Local IP Address
UE UDP Port
WLAN location information
WLAN location timestamp

In case all the bearers belonging to the same PDN connection are released at the same time, one event shall be sent for each bearer.

NOTE: Cause can be present e.g. in case of inter S-GW TAU, when the new S-GW sends a bearer deactivation request to the old S-GW.

12.2.3.5 Bearer modification

When a bearer modification is detected, a bearer modification event shall be generated. These elements will be delivered by the S-GW/PDN-GW to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Location Information
Time of Location
IAs (if applicable)
Initiator
EPS Bearer QoS (Note 1)
EPS bearer id
Procedure Transaction Identifier
RAT type
APN-AMBR (Note 2)
Traffic Flow Template(s) (TFT)
Handover indication
Failed Bearer Modification reason
UE Local IP Address
UE UDP Port
WLAN location information
WLAN location timestamp

NOTE 1: In case of unsuccessful default bearer modification, the parameter carries the requested EPS bearer QoS, otherwise it carries the EPS bearer QoS associated to the modified bearer.

NOTE 2: In case of unsuccessful default bearer modification, the parameter carries the subscribed APN-AMBR, otherwise it carries the APN-AMBR used for the modified bearer.

The event may also be used by the PDN-GW to indicate a handover between different accesses. In this case, the RAT type indicates the new access after the handover.

12.2.3.6 Start of interception with active bearer

This event will be generated if interception for a target is started and if the target has at least the default bearer active. If more then one bearer is active, for each of them an event record is generated. The parameters which are defined for bearer activation (see related section) will be sent, if available, by the S-GW/PDN-GW to the DF2.

As an option, in case the event is sent due to a change of the involved S-GW, the new S-GW may provide as additional parameter, the "old location information". However, the absence of this information does not imply that interception has not started in the old location S-GW for an active bearer.

12.2.3.7 Tracking Area/EPS Location Update

For each TA/EPS Location Update an update-event with the elements about the new location is generated. The event shall be sent in case of Tracking Area Update, UE triggered Service Request, X2 based handover, S1 based handover, as specified in TS 23.401 [22]. In case of change of MME, the new MME shall send the event, and the old MME may optionally send the event as well. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Location Information (only for the new MME)
Old Location Information (only for the old MME)
Time of Location
IAs (if applicable)
Failure reason
HeNB Identity (NOTE1)
HeNB IP Address (NOTE1)
HeNB Location (NOTE1)
ProSe Remote UE(s) IDs (NOTE 2)
ProSe Remote UE(s) IP Info (NOTE 2)

NOTE 1: These elements are applicable for HeNB interception only.

NOTE 2: These elements identify the ProSe remote UEs connected to the ProSe UE-to-NW relay when the ProSe UE-to-NW relay is the target and are applicable only in case the target UE is a ProSe UE-to-NW Relay, see clause 17.3.

12.2.3.8 Serving Evolved Packet System

The Serving Evolved Packet System report event is generated at the HSS, when the HSS has detected that the target has roamed. The elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Serving MME Address

12.2.3.9 UE requested PDN connectivity

When a PDN connectivity is requested from the mobile to allow multiple PDN connections (TS 23.401 [22]), an UE requested PDN connectivity event is generated by the MME. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Location Information
Time of Location
APN
Request type
PDN type
Failed reason
IAs (if applicable)
Protocol Configuration Options
EPS bearer identity
HeNB Identity*
HeNB IP Address*
HeNB Location*

* These elements are applicable for HeNB interception only.

12.2.3.10 UE requested PDN disconnection

When a PDN disconnection is requested from the mobile to request for disconnection from one PDN (TS 23.401 [22]), an UE requested PDN disconnection event is generated by the MME. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Location Information
Time of Location
IAs (if applicable)
Linked EPS bearer identity
HeNB Identity*
HeNB IP Address*
HeNB Location*

* These elements are applicable for HeNB interception only.

12.2.3.11 UE requested Bearer Resource Modification

When UE requested Bearer Resource Modification TS 23.401 [22] is detected at the S-GW/PDN-GW, an UE requested Bearer Resource Modification event is generated. These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Location Information
Time of Location
IAs (if applicable)
Linked EPS bearer identity
EPS bearer identity
Procedure Transaction Identifier
EPS bearer QoS
Traffic Aggregate Description
Failed Bearer Modification reason
Protocol Configuration Options

12.2.3.12 Void

12.2.3.13 Start of interception with E-UTRAN attached UE

This event will be generated if interception for a target is started and if the target is already E-UTRAN attached. If there are multiple PDN connections active for the target then for each them an event report is generated.

These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME id
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Location Information
Time of Location
APN
PDN type
IAs (if applicable)
EPS bearer identity of the default bearer
CGS Identity (if closed or hybrid HeNB)*
CSG List (if closed or hybrid HeNB)*
HeNB Identity*
HeNB IP Address*
HeNB Location *
Security Gateway IP address*
Tunnel Protocol*
ISP Operator Identity*

* These elements are applicable for HeNB interception only.

12.2.3.14 Packet Data Header Information

12.2.3.14.0 Introduction

Packet Data Header Information reporting can be done either on a per-packet (i.e., non-summarized) basis or in a summary report.

12.2.3.14.1 Packet Data Header Report

This event is used to provide packet header reports on a per packet basis (non-summarized reporting) and is triggered by each packet sent or received by the target. These elements will be delivered by the S-GW/PDN-GW either directly to DF2 or via another network entity, if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Location Information
Time of Location
IAs (if applicable)
Initiator
EPS bearer id
Handover indication
PDN Address Allocation
PDN address(es)
APN
Source IP Address
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Packet Size
Flow Label (IPv6 only)

12.2.3.14.2 Packet Data Summary Report

This event is used to report:

1) the source and destination information derived from the packet headers, including:

   a) source and destination IP Addresses,

   b) IP next-layer protocol,

   c) Layer-4 ports, and

   d) Flow label, if the packet is IPv6

2) summary information for the number of packets and bytes transmitted or received by the target for each unique packet flow within an EPS bearer, and

3) the date and the time of the first and last packets associated with that packet flow. A packet flow is defined as the 6-tuple of source/destination IP address/port number and the layer 4 protocol and EPS bearer.

   IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported.

The event provides packet summary reports for each unique packet data session (EPS bearer) and packet flow, and is triggered by one of the following:

- start of a packet flow associated with an EPS bearer
- an interim report for a packet flow associated with an EPS bearer is to be reported
- end of a packet flow associated with an EPS bearer (including end of the EPS bearer itself).

An interim report can be triggered by

- The expiration of a configurable timer per intercept (called a Summary Timer). The Summary Timer is configurable in units of seconds;

- A per-intercept configurable count threshold is reached.

These elements will be delivered either directly to DF2 or via a MF for each packet flow if available:

Observed MSISDN
Observed IMSI
Observed ME Id
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Location Information
Time of Location
IAs (if applicable)
Initiator
EPS bearer id
Handover indication
PDN Address Allocation
PDN address(es)
APN
Care of address
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Flow Label (IPv6 only)
Summary Period
Packet Count (for this summary period)
Sum of Packet Sizes (for this summary period)

If the packets are IPv4, the sum of all observed packet sizes is the sum of the values contained in the Total Length field of each packet as specified in IETF RFC 791[39].

If the packet is IPv6, the sum of all observed packet sizes is the sum of the values contained in the Payload Length field for each packet as specified in IETF RFC 2460 [40].

If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report shall not be sent.

12.2.3.15 HSS subscriber record change

This event will be used to report any change of association between IMSI or MSISDN of the target.

The following elements, such as old and new IMSI or MSISDN will be delivered to DF2, if available:

New observed MSISDN or A MSISDN
New observed IMSI
Old observed MSISDN or A MSISDN
Old observed IMSI
Event Type
Event Time
Event Date
Change Type (MSISDN, A-MSISDN or IMSI)
Network Element Identifier (HSS id...)
Other update: carrier specific

12.2.3.16 Cancel location

This event "Cancel Location" will be used to report to DF2 when HSS send to MME one cancel location or purge to serving system.

The following elements such as the old serving system of the target will be delivered to DF2:

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HSS Id...)
Previous visited MME Identifier

12.2.3.17 Register location

This event will be used to report one update location to the HSS for a target. The elements of previous and current serving system id will be delivered to DF2, if available:

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)
Previous visited MME Identifier
Current visited MME Identifier

12.2.3.18 Location information request

This event will be used to report any location information of the target request activity.

The elements, observed IMSI, MSISDN, the identifier of the requesting node type and network, will be delivered to DF2, if available:

Observed MSISDN
Observed IMSI
Requesting network identifier (country identifier included)
Requesting node type
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)

12.3 Functional requirements for LI in case of E-UTRAN access and PMIP based S5/S8 interfaces

12.3.0 General

Functional requirements for LI in the MME, S-GW, LI LCS Client and HSS do not differ from the ones applicable to the case of GTP based S5-S8 interfaces, as specified in clause 12.2 and subclauses.

LI in the PDN-GW is a national option.

Interception in the PDN-GW and in the LI LCS Client shall be based on one or more of NAI, MSISDN, IMEI.

For the delivery of the CC and IRI, the PDN-GW provides correlation number and target identity to the DF2 and DF3 which is used there in order to select the different LEAs where the product shall be delivered.

The correlation number is unique in the whole PLMN and is used to correlate CC with IRI and the different IRI's of one IP-CAN session. However, when different protocols (i.e. GTP and PMIP) are used in the network, different values can be generated by different nodes.

The correlation number shall be generated by using existing parameters related to the IP-CAN session.

NOTE: Void

If interception has been activated for both parties of the Packet Data communication both CC and IRI shall be delivered for each party as separate intercept activity.

12.3.1 Provision of intercept related information

12.3.1.0 General

Intercept Related Information (Events) shall be sent at attach/tunnel activation, detach/tunnel deactivation, start of interception with active PMIP tunnel, PMIP session modification, PDN-GW initiated PDN-disconnection, UE requested PDN connectivity, Serving Evolved Packet System, subscriber record change, registration termination, location information request , and LALS Location Report.

LI based on HSS reporting is a national option. Requirements on the HSS specified in section 12.2 and subsections apply also to the case in which S5/S8 interfaces are PMIP based.

12.3.1.1 X2 interface

The following information needs to be transferred from the PDN-GW to the DF2 in order to allow a DF2 to perform its functionality:

- target identity;
- events and associated parameters as defined in clause 12.3.1.2 and 12.3.3 may be provided;
- the target location (if available) or the IAs in case of location dependent interception; (FFS);
- date/time of Location (if target location provided);
- correlation number;
- Quality of Service (QoS) information, if available;
- encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

The PDN-GW detect packets containing packet data header information in the communications path but the information needed for Packet Data Header Information reporting may need to be transferred from the PDN-GW either directly to the DF2 or via another network entity in order to allow the DF2 to perform its functionality.

The IRI should be sent to DF2 using a reliable transport mechanism.

For the LALS Reports the following information needs to be transferred from the LI LCS Client to the DF2 in order to allow a DF2 to perform its functionality:

- target identities;
- the target location (if available);
- date/time of Location (if target location provided);
- error code (if positioning fails);
- Correlation Identifier (in the case of report for Enhanced Location for IRI).

The IRI should be sent to DF2 using a reliable transport mechanism.

12.3.1.2 Structure of the events

There are several different events in which the information is sent to the DF2 if this is required. The events for interception are configurable (if they are sent to DF2) in the PDN-GW, LI LCS Client and can be suppressed in the DF2. The network procedures for which the events are generated are defined in TS 23.402 [23].

The following events are applicable to the PDN-GW:

- PMIP Attach/tunnel activation;
- PMIP Detach/tunnel deactivation;
- PMIP session modification
- Start of interception with active PMIP tunnel;
- PMIP PDN-GW initiated PDN-disconnection;
- Packet Data Header Information.

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from the nodes to DF2. Available IEs from this set of elements as shown below can be extended in the nodes, if this is necessary as a national option. DF2 can extend available information if this is necessary as a national option.

Observed MN NAI The Network Access Identifier of the Mobile Node (target identity).
Observed MSISDN MSISDN of the target.
Observed IMEI IMEI of the target
Event type Indicates which type of event is delivered: PMIP attach/tunnel activation, PMIP detach/tunnel deactivation, PMIP Session modification, Start of interception with active PMIP tunnel, PMIP PDN-GW initiated PDN disconnection, , Packet Data Header Information.
Event time Time of the event generation in the ICE. Time stamp shall be generated relative to ICE internal clock.
Event date Date of the event generation in the ICE.
Correlation number The correlation number is used to correlate CC and IRI.
Network Element Identifier Unique identifier for the ICE reporting the event.
Logical Function Information Used to distinguish between multiple logical functions operating in a single physical network element.
Lifetime Indicates the lifetime of the tunnel; it is set to a nonzero value in the case of registration; is set to zero in case of deregistration.
Failed attach reason Reason for the failed attach/tunnel deactivation of the target.
Access technology type Indicates the Radio Access Type.
Handover indicator Provides information on whether the procedure is triggered as part of a handover.
APN The Access Point Name used for the connection.
UE address info Includes one or more IP addresses allocated to the UE.
Additional Parameters Additional information provided by the UE, such as protocol configuration options.
PDN address(es) The UE IP address(es) for the PDN connection.
Revocation trigger Indicates the reason which triggered the PDN-GW initiated PDN-disconnection procedure
Serving Network Identifies the serving network the UE is attached to
DHCP v4 Address Allocation Indication Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE
Location Information Provides, if received from the PCRF, and/ or from the LI LCS Client, location information of the target.
Time of Location Date/Time of location. The time when location was obtained by the location source node.
Destination IP Address The IP address, including type IPv4 or IPv6, of the destination of the IP packet.
Destination Port Number The port number of the destination of the IP packet.
Flow Label (IPv6 only) The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [41]).
Packet Count The number of packets detected and reported (for a particular summary period).
Packet Data Summary Reason The reason for a Packet Data Summary message being sent to the LEMF (e.g., timed out, counter expiration, end of session)
Packet Size The size of the packet. (i.e., Total Length Field in IPv4 or Payload Length field in IPv6)
Source IP Address The IP address, including type IPv4 or IPv6, of the source of the IP packet.
Source Port Number The port number of the source of the IP packet.
Sum of Packet Sizes (for a particular summary period) The sum of values contained in the Total Length fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.

Summary Period Includes the dates and times of the first and last packets in a particular packet data interval.
Transport Protocol (e.g., TCP) The identification of the transport protocol of the packet or packet flow being reported.

12.3.2 X3-interface

The access method for the delivering of PDN-GW Intercept Product is based on duplication of packets without modification at the PDN-GW. The duplicated packets with additional information in a header are sent to DF3 for further delivery to the LEA.

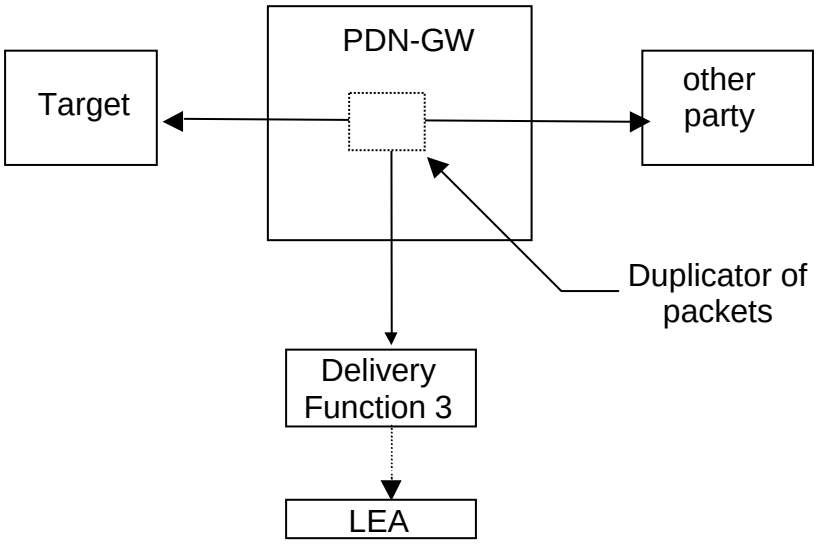


Figure 12.3.2.1: Configuration for interception of PDN-GW product data

In addition to the intercepted content of communication, the following information needs to be transferred from the PDN-GW to the DF3 to perform its functionality:

- target identity;
- correlation number;
- time stamp (optional);
- direction (indicates whether T-PDU is MO or MT) - optional;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of Location (if target location provided).

NOTE: Location dependent interception for EPC is FFS.

12.3.3 LI events for E-UTRAN access with PMIP-based S5 or S8

12.3.3.1 Initial E-UTRAN Attach and UE PDN requested connectivity with PMIP-based S5 or S8

When the E-UTRAN Attach or UE requested PDN connectivity is detected at the PMIP based PDN-GW, a **PMIP attach/tunnel activation** event shall be generated by the PDN-GW. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Lifetime
Failed attach reason
Access Technology Type
Handover Indicator
APN
UE Address Info
Additional Parameters
Serving Network
DHCPv4 Address Allocation Indication
Location information
Time of Location

12.3.3.2 Detach and PDN disconnection for PMIP-based S5/S8

When the Detach or PDN disconnection is detected at the PMIP based PDN-GW, a **PMIP detach/tunnel deactivation** event shall be generated by the PDN-GW. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
APN
Additional Parameters
Failed reason
Location information
Time of Location

12.3.3.3 Start of interception with active tunnel for PMIP based S5/S8

This event shall be generated by the PDN-GW if interception for a target is started and if the target has an active PMIP tunnel. If more than one connection is active, for each of them an event record is generated. The parameters which are defined for PMIP attach/tunnel activation (see related section) will be sent, if available, by the PDN-GW to the DF2.

12.3.3.4 Dedicated Bearer Procedures for E-UTRAN Access with PMIP-based S5/S8

All the procedures can be intercepted at the S-GW according to the requirements specified for LI in case of GTP based S5/S8.

PDN-GW is not involved in these procedures, except for the case of **PDN-GW initiated PDN-disconnection Procedure**.

12.3.3.5 PDN-GW initiated PDN-disconnection Procedure

When a PDN-GW initiated PDN-disconnection procedure is detected, a **PMIP PDN-GW initiated PDN-disconnection** event shall be generated by the PDN-GW. The following elements will be delivered to the DF2:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
PDN Address(es)
Revocation trigger
Location information
Time of Location

12.3.3.6 PMIP Session modification

When a session modification is detected at the PDN-GW, a **PMIP Session modification** event shall be generated by the PDN-GW. The following elements will be delivered to the DF2:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Failed reason
Serving Network
Handover indicator
DHCPv4 Address Allocation Indication
Location information
Time of Location

12.3.3.7 Packet Data Header Information

12.3.3.7.0 Introduction

Packet Data Header Information reporting can be done either on a per-packet (i.e., non-summarized) basis or in a summary report.

12.3.3.7.1 Packet Data Header Report

This event is used to provide packet header reports on a per packet basis (non-summarized reporting) and is triggered by each packet sent or received by the target. These elements will be delivered by the PDN-GW either directly to DF2 or via another network entity if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Serving Network
Handover indicator
DHCPv4 Address Allocation Indication
Location information
Time of Location
Source IP Address
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Packet Size
Flow Label (IPv6 only)

12.3.3.7.2 Packet Data Summary Report

This event is used to report:

1) the source and destination information derived from the packet headers, including:

   a) source and destination IP Addresses,

   b) IP next-layer protocol,

   c) Layer-4 ports, and

   d) Flow label, if the packet is IPv6

2) summary information for the number of packets and bytes transmitted or received by the target for each unique packet flow within an EPS bearer, and

3) the date and the time of the first and last packets associated with that packet flow. A packet flow is defined as the 6-tuple of source/destination IP address/port number and the layer 4 protocol and EPS bearer.

   IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported.

The event provides packet summary reports for each unique packet data session (EPS bearer) and packet flow, and is triggered by one of the following:

- start of a packet flow associated with an EPS bearer
- an interim report for a packet flow associated with an EPS bearer is to be reported
- end of a packet flow associated with an EPS bearer (including end of the EPS bearer itself).

An interim report can be triggered by

- The expiration of a configurable timer per intercept (called a Summary Timer). The Summary Timer is configurable in units of seconds;
- A per-intercept configurable count threshold is reached.

These elements will be delivered either directly to DF2 or via DF3 for each packet flow if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Serving Network
Handover indicator
DHCPv4 Address Allocation Indication
Location information
Time of Location
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Flow Label (IPv6 only)
Summary Period
Packet Count (for this summary period)
Sum of Packet Sizes (for this summary period)
Packet Summary Reason

If the packets are IPv4, the sum of all observed packet sizes is the sum of the values contained in the Total Length field of each packet as specified in IETF RFC 791[39].

If the packet is IPv6, the sum of all observed packet sizes is the sum of the values contained in the Payload Length field for each packet as specified in IETF RFC 2460 [40].

If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report shall not be sent.

12.4 Functional requirements for LI in case of trusted non-3GPP IP access

12.4.0 General

Differently to what happens in E-UTRAN case, in which the user traffic passes through the S-GW and then through the PDN-GW, there are two cases of access to the network through S2a (trusted Non-3GPP access) that require additional consideration. Specifically, the PDN-GW is the only possible ICE in the 3GPP network in the case of non-roaming (PDN-GW in the HPLMN) and in the case of roaming with local breakout (PDN-GW is located in the VPLMN) Therefore, in these cases, interception at the PDN-GW is required.

LI based on HSS reporting is a national option. Requirements on the HSS specified in clause7A.2 and subsections apply also to the case in which non-3GPP IP access and 3GPP AAA server are based. Intercept Related Information (Events) are in such case: serving system, subscriber record change, registration termination, and location information request.In case of access to the network through S2a (trusted Non-3GPP access) for roaming without local breakout (PDN-GW in the HPLMN and S-GW in the VPLMN), interception at the PDN-GW is a national option.

Interception in the S-GW and PDN-GW shall be based on IMSI or NAI.

NOTE 1: The NAI may be a temporary ID, therefore the use of IMSI is recommended.

For the delivery of the CC and IRI, the S-GW and/or PDN-GW provides correlation number and target identity to the DF2 and DF3 which is used there in order to select the different LEAs where the product shall be delivered.

The correlation number is unique in the whole PLMN and is used to correlate CC with IRI and the different IRI's of one IP-CAN session. However, when different protocols (i.e. GTP and PMIP) are used in the network, different values can be generated by different nodes

The correlation number shall be generated by using existing parameters related to the IP-CAN session.

NOTE 2: Void.

If interception has been activated for both parties of the Packet Data communication both CC and IRI shall be delivered for each party as separate intercept activity.

12.4.1 Provision of Intercept Related Information

12.4.1.0 General

Intercept Related Information (Events) shall be sent at attach/tunnel activation on interfaces s2a and s2c, session modification, detach/tunnel deactivation, start of interception with active tunnel, PDN-GW reallocation upon initial attach on s2c, PDN GW initiated resource allocation Deactivation on s2a, Serving Evolved Packet System.

Serving Evolved Packet System reporting is a national option.

12.4.1.1 X2-interface

The following information needs to be transferred from the S-GW, PDN-GW or the HSS to the DF2 in order to allow a DF2 to perform its functionality:

- target identity;
- events and associated parameters as defined in clause 12.4.1.2 and 12.4.3 may be provided;
- the target location (if available) or the IAs in case of location dependent interception; (FFS)
- date/time of Location (if target location provided);
- correlation number;
- Quality of Service (QoS) information, if available;
- encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

The PDN-GW/S-GW detect packets containing packet header information in the communications path but the information needed for Packet Data Header Information Reporting may need to be transferred from the PDN-GW/S-GW either directly to the DF2 or via another network entity in order to allow the DF2 to perform its functionality.

The IRI should be sent to DF2 using a reliable transport mechanism.

12.4.1.2 Structure of the events

There are several different events in which the information is sent to the DF2 if this is required. The events for interception are configurable (if they are sent to DF2) in the S-GW, PDN-GW or the HSS and can be suppressed in the DF2.

The following events are applicable to the S-GW:

- PMIP attach/tunnel activation;
- PMIP detach/tunnel deactivation;
- PMIP session modification;
- Start of interception with active PMIP tunnel;
- Packet Data Header Information.

The following events are applicable to the PDN-GW:

- PMIP attach/tunnel activation;

- PMIP detach/tunnel deactivation;
- PMIP session modification;
- Start of interception with active PMIP tunnel;
- MIP registration/tunnel activation;
- DSMIP registration/tunnel activation;
- DSMIP session modification;
- MIP deregistration/tunnel deactivation;
- DSMIP deregistration/tunnel deactivation;
- Start of interception with active MIP tunnel;
- Start of interception with active DSMIP tunnel;
- DSMIP HA Switch;
- PMIP Resource Allocation Deactivation;
- MIP Resource Allocation Deactivation;
- Bearer activation;
- Bearer deactivation;
- Bearer modification;
- Start of interception with active bearer;
- Packet Data Header Information.

NOTE: Bearer activation, bearer deactivation, bearer modification and start of interception with active bearer are applicable to trusted non-3GPP access when the GTP protocol is used over s2a interface as specified in TS 23.402 [23].

The following event is applicable to the HSS, which may be requested by national regulations:

- Serving Evolved Packet System;
- Subscriber record change;
- Registration termination;
- Location information request.

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from the nodes to DF2. Available IEs from this set of elements as shown below can be extended in the nodes, if this is necessary as a national option. DF2 can extend available information if this is necessary as a national option. In case GTP protocol is used over s2a interface, elements from table 12.2.1.2 are included in the applicable events. If interception is performed at the PDN GW, then Packet Data Header Information reporting shall also be performed at the PDN GW and not at the Serving GW.

Table 12.4.1.2: elements included to trusted Non-3GPP access Events

Observed MN NAI The Network Access Identifier of the Mobile Node (target identity).
Observed IMSI The IMSI of the target
New observed MN NAI The new Network Access Identifier of the Mobile Node (target identity).
New observed IMSI The new IMSI of the target
Old observed MN NAI of the target (if available)
Old observed IMSI of the target (if available)
Event type Indicates which type of event is delivered: PMIP attach/tunnel activation, PMIP detach/tunnel deactivation, PMIP session modification, Start of interception with active PMIP tunnel, MIP registration/tunnel activation, DSMIP registration/tunnel activation, DSMIP session modification, MIP deregistration/tunnel deactivation, DSMIP deregistration/tunnel deactivation, Start of interception with active MIP tunnel, Start of interception with active DSMIP tunnel, DSMIP HA Switch, PMIP resource Allocation Deactivation, MIP Resource Allocation Deactivation, Serving Evolved Packet System, Subscriber record change, Registration termination, Location information request, Packet Data Header Information.
Event time Time of the event generation in the ICE. Time stamp shall be generated relative to ICE internal clock.
Event date Date of the event generation in the ICE.
Change type This indicates what has been changed (MSISDN, IMSI, or IMEI) in the Subscriber Change Record
Correlation number The correlation number is used to correlate CC and IRI.
Network Element Identifier Unique identifier for the ICE reporting the event.
Logical Function Information Used to distinguish between multiple logical functions operating in a single physical network element.
Lifetime Indicates the lifetime of the tunnel; must be set to a nonzero value in the case of registration or lifetime extension; is set to zero in case of deregistration.
Failed attach reason Reason for the failed attach/tunnel deactivation of the target.
Session modification failure reason Reason for a failure of a session modification attempt for the target
Access technology type Indicates the Radio Access Type.
Handover indicator Provides information on whether the triggered as part of a handover.
APN The Access Point Name used for the connection.
UE address info Includes one or more IP addresses allocated to the UE.
Additional Parameters Additional information provided by the UE, such as protocol configuration options.
PDN address(es) The UE IP address(es) for the PDN connection.
Home address Contains the UE Home IP address.
Home Agent address Contains the IP address of the Home Agent.
Requested IPv6 Home Prefix The IPv6 Home Prefix requested by the UE.
IPv6 home prefix The IPv6 home prefix assigned by the PDN GW to the UE.
Care of Address The Local IP address assigned to the UE by the Access Network, used as Care of Address for DSMIPv6 over S2c reference point.
HSS/AAA address The address of the HSS/AAA triggering the PDN-GW reallocation.
Target PDN-GW address The address of the PDN-GW which the UE will be reallocated to.
Revocation trigger Contains the cause for the revocation procedure.

Foreign domain address The relevant IP address in the foreign domain.
Visited network identifier An identifier that allows the home network to identify the visited network TS 29.273 [24]
Location Information Location information of the target, e.g. 3GPP2-BSID TS 29.212 [26]. Provided if available from the PCRF.
Time of Location Date/Time of location. The time when location was obtained by the location source node.
Initiator The initiator of the procedure, either the network or the UE.
Destination IP Address The IP address, including type IPv4 or IPv6, of the destination of the IP packet.
Destination Port Number The port number of the destination of the IP packet.
Flow Label (IPv6 only) The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [41]).
Packet Count The number of packets detected and reported (for a particular summary period).
Packet Data Summary Reason The reason for a Packet Data Summary message being sent to the LEMF (e.g., timed out, counter expiration, end of session)
Packet Size The size of the packet. (i.e., Total Length Field in IPv4 or Payload Length field in IPv6)
Source IP Address The IP address, including type IPv4 or IPv6, of the source of the IP packet.
Source Port Number The port number of the source of the IP packet.
Sum of Packet Sizes (for a particular summary period) The sum of values contained in the Total Length fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.
Summary Period Includes the dates and times of the first and last packets in a particular packet data interval.
Transport Protocol (e.g., TCP) The identification of the transport protocol of the packet or packet flow being reported.
Any User-Data (AVP Name): any change in the profit and identities of the target (if available in the Diameter message)
Any Associated-Identities (AVP Name): any change of any associated identities of the target
Request direction : Information if the serving node is requesting to the HSS, or requested by the HSS.
Other update: carrier specific of target's data that are in the intercepted diameter messages
Other Public User Identities Other IMPU or IMPI that was allocated to Target and will be deregistered (if available)
Requesting node identifier (I CSCF; AS) that are interfaced directly in the HSS and transmitting a diameter message from a network
Requesting network node identifier such as IP-SM-GW Id, GMSC Id, SGSN Id, MME Id GMLC Id (country identifier is included in such request) that are in the different diameter messages related to location request for information (to route the right SMS or Call attempt, or GMLC based location request, to the right node on which is attached the target.)
Requesting node type (IP-SM-GW AS, GMSC, SGSN, MME, GMLC) (if available)

12.4.2 X3-interface

The access method for the delivering of S-GW and/or PDN-GW Intercept Product is based on duplication of packets without modification at the S-GW and/or PDN-GW. The duplicated packets with additional information in a header are sent to DF3 for further delivery to the LEA.

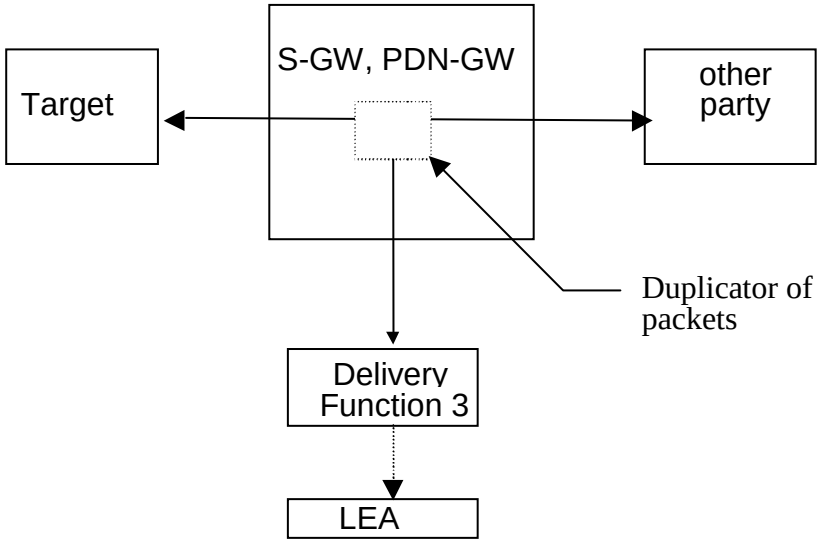


Figure 12.4.2.1: Configuration for interception of S-GW/PDN-GW product data

n addition to the intercepted content of communication, the following information needs to be transferred from the S-GW and/or the PDN-GW to the DF3 to perform its functionality:

- target identity;
- correlation number;
- time stamp (optional);
- direction (indicates whether T-PDU is MO or MT) - optional;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of Location (if target location provided).

NOTE: location dependent interception for EPC is FFS.

12.4.3 LI events for trusted Non-3GPP IP access

12.4.3.1 Initial Attach and PDN connection activation with PMIPv6 on S2a

When the Attach or PDN connectivity activation is detected over PMIP at the S-GW, PDN-GW, a **PMIP attach/tunnel activation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Lifetime
Failed attach reason
Access Technology Type
Handover Indicator
APN
UE Address Info
Additional Parameters
Location Information
Time of Location

12.4.3.2 Initial Attach and PDN connection activation procedures with MIPv4 FACoA on S2a

When the Attach or PDN connectivity activation is detected over MIP at the PDN-GW, a **MIP registration/tunnel activation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Lifetime
Failed attach reason
Home Address
Care of Address
Home Agent Address
APN

NOTE: Void.

As the S-GW has no Home Agent function, the event is not applicable to the S-GW. The use of MIPv4 in roaming case requires Local Breakout (PDN-GW in VPLMN), so LI in the PDN-GW is mandatory in order to intercept in this scenario.

12.4.3.3 Initial Attach and PDN connection activation procedures with DSMIPv6 over S2c

When the Attach or PDN connectivity activation is detected over DSMIP at the PDN-GW, a **DSMIP registration/tunnel activation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Correlation number
Network Element Identifier
Logical Function Information
Lifetime
Requested IPv6 home prefix
Home address
APN
Care of Address
Failed attach reason

12.4.3.4 Detach and PDN disconnection with PMIPv6 on S2a

When a Detach or PDN disconnection is detected over PMIP at the S-GW, PDN-GW, a **PMIP detach/tunnel deactivation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Correlation number
Network Element Identifier
Logical Function Information
APN
Initiator
Location Information
Time of Location

12.4.3.5 Detach and PDN disconnection with MIPv4 FACoA

When a Detach or PDN disconnection is detected over MIP at the PDN-GW, a **MIP deregistration/tunnel deactivation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Correlation number
Network Element Identifier
Logical Function Information
Home Address
Home Agent Address
Care of address
Initiator

12.4.3.6 Detach and PDN disconnection with DSMIPv6 on S2c

When a Detach or PDN disconnection is detected over DSMIP at the PDN-GW, a **DSMIP deregistration/tunnel deactivation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Correlation number
Network Element Identifier
Logical Function Information
Home Address
Initiator

12.4.3.7 PDN-GW reallocation upon initial attach on s2c

When a PDN GW reallocation procedure is detected by the PDN-GW, a **DSMIP HA Switch event** shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Network Element Identifier
Logical Function Information
HSS/AAA address
Target PDN-GW address

12.4.3.8 PDN GW initiated Resource Allocation Deactivation with S2a PMIP

When a PDN GW initiated resource allocation deactivation is detected by the S-GW/PDN-GW, a **PMIP Resource Allocation Deactivation** event shall be sent. The following elements will be delivered to DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Network Element Identifier
Logical Function Information
Revocation trigger
UE address info
Correlation number
Location Information
Time of Location

12.4.3.9 PDN GW initiated Resource Allocation Deactivation with S2a MIP v4

When a PDN GW initiated resource allocation deactivation is detected, a **MIP Resource Allocation Deactivation** event shall be sent. The following elements will be delivered to DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Network Element Identifier
Logical Function Information
Home Address
Foreign domain address
Correlation number

12.4.3.10 Serving Evolved Packet System

The Serving Evolved Packet System report event is generated at the HSS, when the HSS has detected that the target has roamed. Such events could be mainly triggered by Diameter messages such as:

Through SWx interface, Server-Assignment-Request in case of command of 3GPP AAA to HSS (see clause A of TS 29.273 [24], and clause 5 of GSMA IR.61 [65]).

The elements of table 12.4.3.10 will be delivered to the DF2 if available:

Table 12.4.3.10: Information Elements for Serving Evolved Packet Event

Observed MSISDN
Observed IMSI
Observed ME Identity
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Visited Network Identifier (for example: AVP name such as Visited-PLMN-Id)

12.4.3.11 Start of interception with active tunnel or bearer

When interception is started at the S-GW, PDN-GW and the target has an already active tunnel or bearer, a start of interception with active tunnel/bearer shall be generated. Separate events are defined for the different protocols. The event shall be detected by the same node for which tunnel/bearer activation reporting is applicable and reported with the same parameters required for the specific protocol (PMIP, MIP, DSMIP, GTP) tunnel/bearer activation event, as defined in the related sections. One event shall be sent for each active tunnel/bearer.

12.4.3.12 PMIP session modification

When a session modification is detected at the S-GW/PDN-GW, a **PMIP session modification** event shall be generated by the S-GW/PDN-GW. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Session modification failure reason
Serving Network
Handover indicator
DHCPv4 Address Allocation Indication
Location information
Time of Location

12.4.3.13 DSMIP session modification

When the session modification is detected over DS-MIPv6 at the PDN-GW, a **DSMIP session modification** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Lifetime
Session modification failure reason
Home address
Care of Address
APN
Requested IPv6 Home Prefix

12.4.3.14 Bearer activation

When the Initial attach in WLAN on GTP S2a (TS 23.402 [23]) or the Dedicated bearer activation in WLAN on GTP S2a (TS 23.402 [23]) is detected in the PDN-GW, a **Bearer activation** event shall be generated. The elements listed in the section 12.2.3.3 will be delivered to the DF2 if available.

12.4.3.15 Bearer deactivation

When the Detach and PDN disconnection in WLAN on GTP S2a (TS 23.402 [23]) or the PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2 (TS 23.402 [23] is detected in the PDN-GW, a **Bearer deactivation** event shall be generated. The elements listed in the section 12.2.3.4 will be delivered to the DF2 if available.

12.4.3.16 Bearer modification

When the Network initiated bearer modification in WLAN on GTP S2a (TS 23.402 [23]) is detected in the PDN-GW, a **Bearer modification** event shall be generated. The elements listed in the section 12.2.3.5 will be delivered by the PDN-GW to the DF2 if available.

12.4.3.17 Packet Data Header Information

12.4.3.17.0 Introduction

Packet Data Header Information reporting can be done either on a per-packet (i.e., non-summarized) basis or in a summary report.

12.4.3.17.1 Packet Data Header Report

This event is used to provide packet header reports on a per packet basis (non-summarized reporting) and is triggered by each packet sent or received by the target. These elements will be delivered by the S-GW/PDN-GW either directly to the DF2 or via another network entity if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Serving Network
Home address
Care of Address
APN
Location information
Time of Location
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Packet Size
Flow Label (IPv6 only)

12.4.3.17.2 Packet Data Summary Report

This event is used to report:

1) the source and destination information derived from the packet headers, including:

   a) source and destination IP Addresses,

   b) IP next-layer protocol,

   c) Layer-4 ports, and

   d) Flow label, if the packet is IPv6

2) summary information for the number of packets and bytes transmitted or received by the target for each unique packet flow within an EPS bearer, and

3) the date and the time of the first and last packets associated with that packet flow. A packet flow is defined as the 6-tuple of source/destination IP address/port number and the layer 4 protocol and EPS bearer.

   IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported.

The event provides packet summary reports for each unique packet data session (EPS bearer) and packet flow, and is triggered by one of the following:

- start of a packet flow associated with an EPS bearer
- an interim report for a packet flow associated with an EPS bearer is to be reported
- end of a packet flow associated with an EPS bearer (including end of the EPS bearer itself).

An interim report can be triggered by

- The expiration of a configurable timer per intercept (called a Summary Timer). The Summary Timer is configurable in units of seconds;
- A per-intercept configurable count threshold is reached.

These elements will be delivered either directly to the DF2 or via a MF for each packet flow if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Serving Network
Home address
Care of Address
APN
Location information
Time of Location
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Flow Label (IPv6 only)
Summary Period
Packet Count (for this summary period)
Sum of Packet Sizes (for this summary period)

If the packets are IPv4, the sum of all observed packet sizes is the sum of the values contained in the Total Length field of each packet as specified in IETF RFC 791[39].

If the packet is IPv6, the sum of all observed packet sizes is the sum of the values contained in the Payload Length field for each packet as specified in IETF RFC 2460 [40].

If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report shall not be sent.

12.4.3.18 HSS subscriber record change

This event will be only used to report when there is a change of association between IMSI, MSISDN or IMEI of the target. It is induced mainly by Subscriber Profile management by the HSS or the CSP administration tools through the HSS.

Such events could be mainly triggered by Diameter messages such as:

> Through SWx interface, -Push-Profile-Request (PPR) in case of command of HSS to 3GPP AAA Server: see clause A of TS 29.273 [24].

The elements of table 12.4.3.18 will be delivered to DF2, if available.

Table 12.4.3.18: Information Elements for Subscriber Record Change Event

New observed MSISDN
New observed IMSI
New Observed IMEI (if available)
Old observed MSISDN
Old observed IMSI
Old observed IMEI (if available)
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)
Change Type (MSISDN, IMSI or IMEI)
Other update: carrier specific.

12.4.3.19 Registration Termination

This event "Registration Termination" will be used to report to DF2 when HSS send to 3GPP AAA Server It is the equivalent of cancel location or purge to serving system in CS domain. This kind of event is induced by the registration of the target. The event will be triggered by the following Diameter messages:

- Through SWx interface, Server-Assignment-Request indicating deregistration from 3GPP AAA Server to HSS: see clause A of TS 29.273 [24];

- Through SWx interface, Registration-Termination- Request from HSS to 3GPP AAA Server: see clause A of TS 29.273 [24].

The elements of table 12.4.3.19 will be delivered to DF2.

Table 12.4.3.19: Information Elements for Termination Request Event

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HSS Id...)
Previous serving system identifier (if available)

12.4.3.20 Location Information request

This event will be used to report any location information request on the target by a node to HSS, when the target is connected to trusted non-3GPP IP access. A location information request could be generated by an IP-SM-GW AS (as an SMS Centre) or GMSC or SGSN or MME from another Network through a diameter request transmitted by either an AS or the I CSCF of the home network to the HSS of the target. The event will be triggered by the following Diameter messages:

- Through Sh interface, User Data Request with content related to update location from AS to HSS, see clause A.2 of TS 29.328 [63] and TS 29.329 [66];

- Through Cx interface, Location Info Request from I CSCF to HSS; see clause A.2 of TS 29.228 [62].

The elements, observed IMSI, MSISDN, the identifier of the requesting node type and network, of table 12.4.3.20 will be delivered to DF2, if available.

Table 12.4.3.20: Information Elements for Location Information Request Event

Observed MSISDN
Observed IMSI
Requesting network identifier such as PLMN Id (country identifier included),
Requesting node type (IP-SM-GW AS, GMSC, SGSN, MME, GMLC)
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)

12.5 Functional requirements for LI in case of untrusted non-3GPP IP access

12.5.0 Introduction

This clause specifies functional requirements applicable to the PDN-GW and HSS. In addition, this clause specifies requirements applicable to the ePDG in case this node is using a GTPv2 based protocol over s2b interface as specified in TS 23.402 [23].

The e-PDG not using a GTPv2 based protocol over s2b interface and the AAA server are subjected to all the requirements specified in this document for PDG and AAA server for the case of I-WLAN interworking.

NOTE 1: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

Interception in the PDN-GW is a national option.

Interception in the PDN-GW shall be based on IMSI or NAI. In case of GTPv2 based protocol, interception at the ePDG and PDN-GW shall be based on IMSI.

NOTE 2: The NAI may be a temporary ID, therefore the use of IMSI is recommended.

For the delivery of the CC and IRI, the PDN-GW and ePDG provides correlation number and target identity to the DF2 and DF3 which is used there in order to select the different LEAs where the product shall be delivered.

LI based on HSS reporting is a national option. Requirements on the HSS specified in clause 7A.2 and subsections apply also to the case in which non-3GPP IP access and 3GPP AAA server are based. Intercept Related Information (Events) are serving system, subscriber record change, registration termination, and location information request.

12.5.1 Provision of Intercept Related Information

12.5.1.0 General

Intercept Related Information (Events) shall be sent at attach/tunnel activation on interfaces s2b and s2c, detach/tunnel deactivation, session modification, start of interception with active tunnel, Serving Evolved Packet System.

In case of GTPv2 based s2b, Intercept Related Information shall be sent at attach/bearer activation, detach/bearer deactivation, bearer modification and start of interception with active bearer.

The following event is applicable to the HSS, which is a national option:

- Serving Evolved Packet System;
- Subscriber record change;
- Registration termination;
- Location information request.

12.5.1.1 X2-interface

The following information needs to be transferred from the PDN-GW, ePDG or the HSS to the DF2 in order to allow a DF2 to perform its functionality:

- target identity;
- events and associated parameters as defined in clause 12.5.1.2 and 12.5.3 may be provided;
- the target location (if available) or the IAs in case of location dependent interception; (FFS)
- date/time of Location (if target location provided);
- correlation number;
- Quality of Service (QoS) information, if available;
- encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

The PDN-GW detect packets containing packet header information in the communications path but the information needed for Packet Data Header Information reporting may need to be transferred from the PDN-GW either directly to the DF2 or via another network entity in order to allow the DF2 to perform its functionality.

The IRI should be sent to DF2 using a reliable transport mechanism.

12.5.1.2 Structure of the events

There are several different events in which the information is sent to the DF2 if this is required. The events for interception are configurable (if they are sent to DF2) in the PDN-GW, ePDG or the HSS and can be suppressed in the DF2.

The following events are applicable to the PDN-GW:

- PMIP attach/tunnel activation;
- PMIP detach/tunnel deactivation;
- PMIP session modification;
- Start of interception with active PMIP tunnel;
- DSMIP registration/tunnel activation;
- DSMIP deregistration/tunnel deactivation;
- DSMIP session modification;
- Start of interception with active DSMIP tunnel;
- DSMIP HA Switch;
- PMIP Resource Allocation Deactivation ;
- Packet Data Header Information
- Bearer activation;
- Bearer deactivation;
- Bearer modification;
- Start of interception with active bearer.

The following events are applicable to the ePDG:

- Bearer activation;
- Bearer deactivation;

- Bearer modification:
- Start of interception with active bearer.

The following events are applicable to the HSS, which is national option:

- Serving Evolved Packet System;
  - Subscriber record change;
  - Registration termination;
  - Location information request.

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from the nodes to DF2. Available IEs from this set of elements as shown below can be extended in the nodes, if this is necessary as a national option. DF2 can extend available information if this is necessary as a national option. When the GTP protocol is used over the s2b interface, elements from table 12.2.1.2 are included in the applicable events.

Table 12.5.1.2: Elements that are Associated to Events of Untrusted Non-3GPP IP Access Events

Observed MN NAI The Network Access Identifier of the Mobile Node (target identity).
Observed IMSI The IMSI of the target.
New observed MN NAI The Network Access Identifier of the Mobile Node (target identity).
New observed IMSI The IMSI of the target
Old observed IMSI of the target (if available)
Old observed MN NAI of the target (if available)
Any other IMPU or IMPI (if available) available in the diameter message associated to the target
Event type Indicates which type of event is delivered: PMIP attach/tunnel activation, PMIP detach/tunnel deactivation, Start of interception with active PMIP tunnel, DSMIP registration/tunnel activation, DSMIP deregistration/tunnel deactivation, Start of interception with active DSMIP tunnel, DSMIP HA Switch, PMIP resource Allocation Deactivation, Serving Evolved Packet System, Subscriber record change, Registration termination, Location information request, Packet Data Header Information.
Event time Time of the event generation in the ICE. Time stamp shall be generated relative to ICE internal clock.
Event date Date of the event generation in the ICE.
Change Type This indicates what has been changed (MSISDN, IMSI, or IMEI) in the Subscriber Change Record
Correlation number The correlation number is used to correlate CC and IRI.
Network Element Identifier Unique identifier for the ICE reporting the event.
Logical Function Information Used to distinguish between multiple logical functions operating in a single physical network element.
Lifetime Indicates the lifetime of the tunnel; must be set to a nonzero value in the case of registration or lifetime extension; is set to zero in case of deregistration.
Failed attach reason Reason for the failed attach/tunnel deactivation of the target.
Session modification failure reason Reason for a failure of a session modification attempt for the target
Access technology type Indicates the Radio Access Type.
Handover indicator Provides information on whether the triggered as part of a handover.
APN The Access Point Name used for the connection.
UE address info Includes one or more IP addresses allocated to the UE.
Additional Parameters Additional information provided by the UE, such as protocol configuration options.
Home Agent address Contains the IP address of the Home Agent.
Care of Address The Local IP address assigned to the UE by the Access Network, used as Care of Address for DSMIPv6 over S2c reference point.
HSS/AAA address The address of the HSS/AAA triggering the PDN-GW reallocation.
Target PDN-GW address The address of the PDN-GW which the UE will be reallocated to.
Revocation trigger Contains the cause for the revocation procedure.
Foreign domain address The relevant IP address in the foreign domain.
Visited network identifier An identifier that allows the home network to identify the visited network TS 29.273 [24].
Requested IPv6 Home Prefix The IPv6 Home Prefix requested by the UE.
IPv6 home prefix The IPv6 home prefix assigned by the PDN GW to the UE.
Home address Contains the UE Home IP address.

Destination IP Address The IP address, including type IPv4 or IPv6, of the destination of the IP packet.
Destination Port Number The port number of the destination of the IP packet.
Flow Label (IPv6 only) The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [41]).
Packet Count The number of packets detected and reported (for a particular summary period).
Packet Data Summary Reason The reason for a Packet Data Summary message being sent to the LEMF (e.g., timed out, counter expiration, end of session)
Packet Size The size of the packet. (i.e., Total Length Field in IPv4 or Payload Length field in IPv6)
Source IP Address The IP address, including type IPv4 or IPv6, of the source of the IP packet.
Source Port Number The port number of the source of the IP packet.
Sum of Packet Sizes (for a particular summary period) The sum of values contained in the Total Length fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.
Summary Period Includes the dates and times of the first and last packets in a particular packet data interval.
Transport Protocol (e.g., TCP) The identification of the transport protocol of the packet or packet flow being reported.
Any User-Data (AVP Name): any change in the profit and identities of the target (if available in the Diameter message)
Any Associated-Identities (AVP Name): any change of any associated identities of the target
Request direction : Information if the serving node is requesting to the HSS, or requested by the HSS.
Other update: carrier specific of target's data that are in the intercepted diameter messages
Other Public User Identities Other IMPU or IMPI that was allocated to Target and will be deregistered (if available)
Requesting node identifier (I CSCF; AS) that are interfaced directly in the HSS and transmitting a diameter message from a network
Requesting network node identifier such as IP-SM-GW Id, GMSC Id, SGSN Id, MME Id GMLC Id (country identifier is included in such request) that are in the different diameter messages related to location request for information (to route the right SMS or Call attempt, or GMLC based location request, to the right node on which is attached the target.)
Requesting node type (IP-SM-GW AS, GMSC, SGSN, MME, GMLC) (if available)

12.5.2 X3-interface

The access method for the delivering of PDN-GW and/or ePDG Intercept Product is based on duplication of packets without modification at the intercepting node. The duplicated packets with additional information in a header are sent to DF3 for further delivery to the LEA.

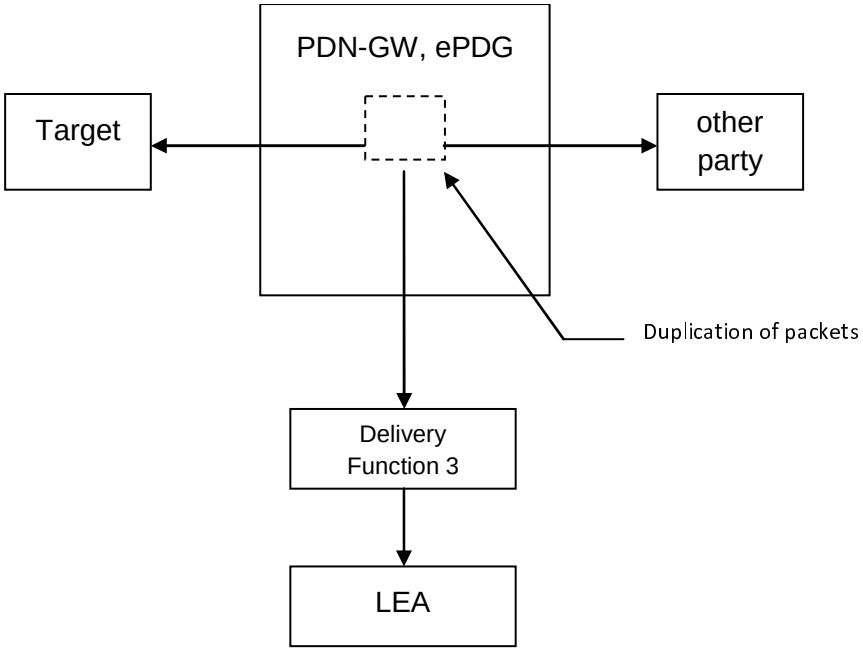


Figure 12.5.2.1: Configuration for interception of PDN-GW, ePDG product data

In addition to the intercepted content of communication, the following information needs to be transferred from the PDN-GW and/or ePDG to the DF3 to perform its functionality:

- target identity;
- correlation number;
- time stamp (optional);
- direction (indicates whether T-PDU is MO or MT) - optional;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of Location (if target location provided).

NOTE: Location dependent interception for EPC is FFS.

12.5.3 LI events for untrusted Non-3GPP IP access

12.5.3.1 Initial Attach and PDN connection activation with PMIPv6 on S2b

In the VPLMN, LI shall be done at the ePDG according to LI requirements for I-WLAN; no additional requirement applies to the S-GW for this case.

NOTE: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

When the attach or PDN connectivity activation is detected over PMIP at the PDN-GW, a **PMIP attach/tunnel activation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Logical Function Information
Network Element Identifier
Lifetime
Failed attach reason
Access Technology Type
Handoff Indicator
APN
UE Address Info
Additional Parameters

12.5.3.2 Initial attach and PDN connection activation for S2c in untrusted non-3GPP IP access

In the VPLMN, LI shall be done at the ePDG according to LI requirements for PDG for I-WLAN.

NOTE: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

When the attach or PDN connectivity activation is detected over DS-MIPv6 at the PDN-GW, a **DSMIP registration/tunnel activation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Lifetime
Failed attach reason
Home address
Care of Address
APN
Requested IPv6 Home Prefix

12.5.3.3 UE/ePDG-initiated Detach Procedure and UE Requested PDN disconnection with PMIP

In the VPLMN, LI shall be done at the ePDG according to LI requirements for PDG for I-WLAN; no additional requirement applies to the S-GW for this case.

NOTE: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

When the detach or UE requested PDN disconnection is detected over PMIP at the PDN-GW, a **PMIP detach/tunnel deactivation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
APN

12.5.3.4 Detach and PDN Disconnection for S2c in Un-trusted Non-3GPP IP access

In the VPLMN, LI shall be done at the ePDG according to LI requirements for PDG for I-WLAN.

When the detach or PDN disconnection is detected over DS-MIPv6 at the PDN-GW, a **DSMIP deregistration/tunnel deactivation** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Home address
Logical Function Information
Initiator
Care of Address

12.5.3.5 Serving Evolved Packet System

The Serving Evolved Packet System report event is generated at the HSS, when the HSS has detected that the target has roamed. Such events could be mainly triggered by Diameter messages such as:

- Through SWx interface, Server-Assignment-Request in case of command of 3GPP AAA to HSS (see clause A of TS 29 273 [24], and clause 5 of GSMA IR.61 [65]).

The elements of table 12.5.3.5 will be delivered to the DF2, if available.

Table 12.5.3.5: Information Elements for Serving Evolved Packet Event

Observed MSISDN
Observed IMSI
Observed ME Identity
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Visited Network Identifier (for example, AVP name such as Visited-PLMN-Id)

12.5.3.6 Start of interception with active tunnel/bearer

When interception is started at the PDN-GW/ePDG and the target has an already active tunnel/bearer, a start of interception with active tunnel/bearer shall be generated. The event shall be detected by the same node for which tunnel/bearer activation reporting is applicable and reported. Separate events are defined for the specific protocol (PMIP, DSMIP, GTP). When the GTP protocol is used for the s2b interface, the event Start of interception with active bearer is applicable as specified in section 12.2.3.6. The parameter applicable to the tunnel activation event, as defined in the related sections, will be delivered to the DF2 if available. One event shall be sent for each active tunnel.

12.5.3.7 PDN-GW reallocation upon initial attach on s2c

When a PDN GW reallocation procedure is detected by the PDN-GW, a **DSMIP HA Switch event** shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Network Element Identifier
Logical Function Information
HSS/AAA address
Target PDN-GW address

12.5.3.8 PDN GW initiated Resource Allocation Deactivation with S2b PMIP

When a PDN GW initiated resource allocation deactivation is detected, a **PMIP Resource Allocation Deactivation** event shall be sent. The following elements will be delivered to DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Date
Event Time
Network Element Identifier
Logical Function Information
Revocation trigger
UE address info
Correlation number

12.5.3.9 PMIP session modification

In the VPLMN, LI shall be done at the ePDG according to LI requirements for PDG for I-WLAN; no additional requirement applies to the S-GW for this case.

NOTE: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

When a session modification is detected at the PDN-GW, a **PMIP session modification** event shall be generated by the PDN-GW. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Session failure modification reason
Handover indicator

12.5.3.10 DSMIP session modification

In the VPLMN, LI shall be done at the ePDG according to LI requirements for PDG for I-WLAN.

NOTE: WLAN Interworking specifications (TS 23.234 [14], TS 24.234 [17] and TS 29.234 [16]) are no longer maintained for Release 12 onwards. This clause is therefore no longer maintained for WLAN Interworking.

When the session modification is detected over DS-MIPv6 at the PDN-GW, a **DSMIP session modification** event shall be generated. The following elements will be delivered to the DF2 if available:

Observed MN NAI
Observed IMSI
Event Type
Event Time
Event Date
Correlation number
Network Element Identifier
Logical Function Information
Lifetime
Session failure modification reason
Home address
Care of Address
APN
Requested IPv6 Home Prefix

12.5.3.11 Packet Data Header Information

12.5.3.11.0 General

Packet Data Header Information reporting can be done either on a per-packet (i.e., non-summarized) basis or in a summary report.

12.5.3.11.1 Packet Data Header Report

This event is used to provide packet header reports on a per packet basis (non-summarized reporting) and is triggered by each packet sent or received by the target. These elements will be delivered by the PDN-GW either directly to the DF2 or via another network entity if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation number
Logical Function Information
Lifetime
UE Address Info
Access Technology Type
Serving Network
Home address
Care of Address
APN
Location information
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Packet Size
Flow Label (IPv6 only)

12.5.3.11.2 Packet Data Summary Report

This event is used to report:

1) the source and destination information derived from the packet headers, including:

   a) source and destination IP Addresses,

   b) IP next-layer protocol,

   c) Layer-4 ports, and

   d) Flow label, if the packet is IPv6

2) summary information for the number of packets and bytes transmitted or received by the target for each unique packet flow within an EPS bearer, and

3) the date and the time of the first and last packets associated with that packet flow. A packet flow is defined as the 6-tuple of source/destination IP address/port number and the layer 4 protocol and EPS bearer.

   IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported.

The event provides packet summary reports for each unique packet data session (EPS bearer) and packet flow, and is triggered by one of the following:

- start of a packet flow associated with an EPS bearer
- an interim report for a packet flow associated with an EPS bearer is to be reported
- end of a packet flow associated with an EPS bearer (including end of the EPS bearer itself).

An interim report can be triggered by

- The expiration of a configurable timer per intercept (called a Summary Timer). The Summary Timer is configurable in units of seconds;
- A per-intercept configurable count threshold is reached.

These elements will be delivered either directly to DF2 or via DF3 for each packet flow if available:

Observed MN NAI
Observed MSISDN
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Logical Function Information
Correlation number
Lifetime
UE Address Info
Access Technology Type
Serving Network
Home address
Care of Address
APN
Location information
Source IP Address
Source Port Number
Destination IP Address
Destination Port Number
Transport Protocol (e.g., TCP)
Flow Label (IPv6 only)
Summary Period
Packet Count (for this summary period)
Sum of Packet Sizes (for this summary period)

If the packets are IPv4, the sum of all observed packet sizes is the sum of the values contained in the Total Length field of each packet as specified in IETF RFC 791[39].

If the packet is IPv6, the sum of all observed packet sizes is the sum of the values contained in the Payload Length field for each packet as specified in IETF RFC 2460 [40].

If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report shall not be sent.

12.5.3.12 Bearer activation

When the Attach is handled by the ePDG over the GTP based s2b interface (TS 23.402 [23]), or the Dedicated bearer activation on the GTP based S2b interface (TS 23.402 [23]) is detected by the ePDG, or a Bearer activation is detected at the PDN-GW, a **Bearer activation** event shall be generated. The elements listed in section 12.2.3.3 will be delivered to the DF2 if available.

12.5.3.13 Bearer deactivation

When the Detach is handled by the ePDG over GTP S2b interface (TS 23.402 [23]), or a Bearer deactivation is detected at the PDN-GW, or the PDN GW initiated Resource Allocation Deactivation is detected by the ePDG on GTP based s2b interface, a **Bearer deactivation** event shall be generated. The elements listed in section 12.2.3.4 will be delivered to the DF2 if available.

12.5.3.14 Bearer modification

When a Bearer Modification is handled by the ePDG over GTP S2b interface (TS 23.402 [23]), or a Bearer modification is detected at the PDN-GW, a **Bearer modification** event shall be generated. The elements listed in section 12.2.3.5 will be delivered by the ePDG to the DF2 if available.

12.5.3.15 HSS subscriber record change

This event will be only used to report when there is a change of association between IMSI, MSISDN or IMEI of the target. It is induced mainly by Subscriber Profile management by the HSS or the CSP administration tools through the HSS.

Such events could be mainly triggered by Diameter messages such as:

- Through SWx interface, -Push-Profile-Request (PPR) in case of command of HSS to 3GPP AAA Server: see clause A of TS 29.273 [24].

The elements of table 12.5.3.15 will be delivered to DF2, if available.

Table 12.5.3.15: Information Elements for Subscriber Record Change Event

New observed MSISDN
New observed IMSI
New Observed IMEI (if available)
Old observed MSISDN
Old observed IMSI
Old observed IMEI (if available)
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)
Change Type (MSISDN, IMSI or IMEI)
Other update: carrier specific.

12.5.3.16 Registration Termination

This event "Registration Termination" will be used to report to DF2 when HSS send to 3GPP AAA Server It is the equivalent of cancel location or purge to serving system in CS domain. This kind of event is induced by the registration of the target.

The event will be triggered by the following Diameter messages:

- Through SWx interface, Server-Assignment-Request indicating deregistration from 3GPP AAA Server to HSS: see clause A of TS 29.273 [24];

- Through SWx interface, Registration-Termination- Request from HSS to 3GPP AAA Server: see clause A of TS 29.273 [24].

The following elements of table 12.5.3.16 such as the previous serving system of the target will be delivered to DF2.

Table 12.5.3.16: Information Elements for Registration Termination Event

Observed MSISDN
Observed IMSI
Event Type
Event Time
Event Date
Network Element Identifier (HSS Id...)
Previous serving system identifier (if available)

12.5.3.17 Location Information request

This event will be used to report any location information request on the target by a node to HSS, when the target is connected to trusted non-3GPP IP access. A location information request could be generated by an IP-SM-GW AS (as an SMS Centre) or GMSC or SGSN or MME from another Network through a diameter request transmitted by either an AS or the I CSCF of the home network to the HSS of the target. The event will be triggered by the following Diameter messages:

- Through Sh interface, User Data Request with content related to update location from AS to HSS, see clause A.2 of TS 29.328 [63] and TS 29.329 [66];

- Through Cx interface, Location Info Request from I CSCF to HSS; see clause A.2 of TS 29.228 [62].

The elements of table 12.5.3.17, observed IMSI, MSISDN, the identifier of the requesting node type and network, will be delivered to DF2, if available.

Table 12.5.3.17: Information Elements for Location Information Request Event

Observed MSISDN
Observed IMSI
Requesting network identifier such as PLMN Id (country identifier included),
Requesting node type (IP-SM-GW AS, GMSC, SGSN, MME, GMLC)
Event Type
Event Time
Event Date
Network Element Identifier (HSS id...)

12.6 Functional requirements for LI in case of Handovers between E-UTRAN and CDMA2000 Accesses.

When an handover is performed from CDMA2000 Access to E-UTRAN, the MME shall intercept the attach event received from the HRPD AN based on IMSI.

Interception at S-GW and PDN-GW shall be done according to the requirements given in section 12.2 or 12.3 and related subsections, depending on the protocol used over the S5/S8 interface.

12.7 Functional requirements for LI in case of interworking between SGSN and EPS nodes over S4/S12 interfaces

The SGSN and the HSS are subjected to the requirements applicable to these nodes for PS interception, as specified throughout this document.

The S-GW is subjected to the requirements specified in section 12.2 and subsections. The applicable events shall be reported also when received from the SGSN over S4 interface. CC shall be also reported when received over S4/S12 interfaces. The network procedures for which the events applicable to the S-GW, defined in section 12.2 and subsections, are generated when the S-GW is connected over S4/S12 interfaces to a SGSN are defined in TS 23.060 [10].

The PDN-GW is subjected to the requirements specified in section 12.2 or 12.3 and related subsections, depending on the protocol used on S5/S8 interfaces, which are applicable also to the case in which the PDN-GW is involved for a target for which a S4 based SGSN is used.

12.8 Functional requirements for LI in case of interworking between SGSN and PDN-GW over Gn/Gp interfaces

According to TS 23.060 [10] and TS 23.401 [22] a PDN-GW may provide a Gn/Gp interface for interworking with the SGSN. When this interface is provided, from LI perspective the PDN-GW acts as a GGSN towards the involved SGSN. In this case, in addition to the requirements specified in this clause, all the requirements specified by this document for the GGSN are applicable to the PDN-GW.

The PDN-GW shall use the same correlation number in records when the PDP context/EPS bearer modification signalling is detected due to the handover between different accesses involving a Gn/Gp interface (i.e. from E-UTRAN to 2G/3G and vice versa). After the handover, the PDN-GW shall report the events applicable to the new access and continue to use the same correlation number inside the same PDP context/EPS bearer.

The SGSN is subjected to the requirements applicable to this node for PS interception, as specified throughout this document.

12.9 Functional Requirements for LI in case of Control and User Plane Separation

12.9.1 Background

As defined in 3GPP TS 23.214 [75], the Serving Gateway and PDN Gateway may have separated control plane and user plane functions. The control plane (CP) functions (Serving Gateway-C and PDN Gateway-C) provide the traffic

forwarding rules (referred to as Forward Action Rules in 3GPP TS 23.214 [75]) to the user plane (UP) functions (Serving Gateway-U and PDN Gateway-U). The UP functions forward the user plane traffic as per the Forward Action Rules.

As defined in subclause 12.1 of the present document, the Serving Gateway and PDN Gateway provide the LI functions for the EPC packet data interception. As defined in subclause 15.2, a PDN Gateway can also provide the CC Intercept Function for an IMS-based VoLTE. As defined in clause 20, the BBIFF functions of an S8HR LI functions may be implemented within a Serving Gateway. Therefore, the LI functions available in the Serving Gateway and PDN Gateway shall be carried over to the split Serving Gateway and PDN Gateway with the new CUPS architecture.

12.9.2 LI Architecture with CUPS

12.9.2.1 Overview

The LI architecture for EPC packet data interception with CUPS is depicted in figure 12.1.4.

With CUPS, all the signalling related interfaces (i.e., control plane data) terminate at the Serving Gateway C and PDN Gateway-C. Therefore, the IRI related LI functions provided within a Serving Gateway and PDN Gateway for EPC packet data interception shall be provided by the Serving Gateway-C and PDN Gateway-C respectively. The X2 reference point terminates at the Serving Gateway-C and PDN Gateway-C.

With CUPS, user plane data pass through the Serving Gateway-U and PDN Gateway-U. Therefore, the duplication of user plane data to support the CC interception for EPC packet data shall be done at the Serving Gateway-U and PDN Gateway-U. A new LI specific functional element referred to as Split X3 LI Interworking Function (SX3LIF) is defined.

NOTE 1: The SX3LIF can be co-located with a UP function or a CP function or can be a standalone point.

The UP function duplicates the user plane packets of the traffic to be intercepted (identified by the packet detection rules) as instructed by the CP function and then sends the duplicated user plane packets to the SX3LIF over the X3u reference point. The CP function also provides the forwarding action rules to the UP function which enables the UP function to determine how to send the duplicated user plane packets over the X3u reference point to the SX3LIF. The CP function provides the intercept control information (such as correlation identifier, target identity, and intercepted packet identification rules) to the SX3LIF over the X3c reference point. The SX3LIF receives the user plane packets from the UP function (over the X3u reference point), associates the user plane packets to the target interception based on the intercept related information that it received from the CP function (over the X3c reference point) and then delivers the CC to the DF3 over the X3 reference point.

NOTE 2: The present document defines an LI architecture for CUPS where CUPS has been applied to single operator PLMN.

Figure 12.1.4 also shows an X2 reference point between SX3LIF and DF2. Only the IRI events that require access to the user plane packets (e.g. packet data header information) are passed on this X2 reference point from SX3LIF to DF2. In an alternate option, when such IRI events are generated by the DF3, this X2 reference point between SX3LIF and DF2 is not necessary.

Figure 12.1.4 also shows an X1_1 reference point between ADMF and the SX3LIF. This reference point is used to provide the DF2 address and DF3 address to the SX3LIF. Provision of DF2 address is required only when the IRI events that require access to the user plane packets are generated by the SX3LIF.

12.9.2.2 Packet detection rules

The packet detection rules allow the UP function to determine which user plane packets are duplicated and sent to the SX3LIF.

NOTE: The packet detection rules may be different for Serving Gateway-U and PDN Gateway-U. For example, the packet detection Rules for a Serving Gateway-U may be based on the GTP tunnel Id of the bearer from which the user plane packets are to be duplicated and forwarded to SX3LIF. The Packet detection rules for a PDN Gateway-U may be based e.g. on the UE IP address sent to, received from, which the user plane packets are to be duplicated and forwarded to SX3LIF.

12.9.2.3 Forwarding action rules

The forwarding action rules indicate how the UP function is to forward the duplicated packets to the SX3LIF over the X3u reference point. The information such as the destination IP address at the SX3LIF and the GTP tunnel Id of the tunnel toward which the duplicated packets are sent on the X3u reference point may be part of the forwarding action rules.

12.9.2.4 Intercepted packet identification rules

The intercepted packet identification rules allow the SX3LIF to identify and associate the user plane packets received over the X3u reference point to the target intercept information. Part of the forwarding action rules (e.g. the information such as destination IP address of X3u tunnel, GTP tunnel Id of the X3u tunnel), target identity and correlation identifier are part of the intercepted packet identification rules.

The SX3LIF uses the IP address and the GTP tunnel Id of the tunnel on the X3u reference point to associate the received user plane packets with the target intercept information that it receives from the CP function over X3c reference point.

12.9.3 Provision of Content of Communications

12.9.3 1 Interception for Serving Gateway

When the CC interception is required and is to be done at the Serving Gateway, the Serving Gateway-C shall send/activate the following information to the Serving Gateway-U:

- Packet detection rules as described in subclause 12.9.2.2
- Forwarding action rules as described in 12.9.2.3
- An indication to perform the packet duplication and forward the same to the SX3LIF.

In addition, the Serving Gateway-C shall send the following information to the SX3LIF:

- target identity
- correlation identifier
- Intercepted packet identification rules as described in subclause 12.9.2.4.

The Serving Gateway-U shall identify the user plane packets as per the packet detection rules (subsclause 12.9.2.2) and shall forward the packets to the SX3LIF over the X3u reference point as per the forwarding action rules (subclause 12.9.2.3). The SX3LIF shall associate the user plane packets to the target interception as per the intercepted packet identification rules and shall deliver the CC to DF3 over the X3 reference point as defined in the subclause12.2.2 and subclause 12.4.2.

12.9.3.2 Interception for PDN Gateway

When the CC interception is required and is to be done at the PDN Gateway, the PDN Gateway-C shall/activate send the following information to the PDN Gateway-U.

- Packet detection rules as described in 12.9.2.2
- Forwarding action rules as described in 12.9.2.3
- An indication to perform the packet duplication and forward the same to the SX3LIF.

In addition, the PDN Gateway-C shall send the following information to the SX3LIF:

- target identity
- correlation identifier
- Intercepted packet identification rules as described in 12.9.2.4.

The PDN Gateway-U shall identify the user plane packets as per the packet detection rules (subsclause 12.9.2.2) and shall forward the packets to the SX3LIF over the X3u reference point as per the forwarding action rules (subclause

12.9.2.3). The SX3LIF shall associate the user plane packets to the target interception as per the intercepted packet identification rules and shall deliver the CC to DF3 over the X3 reference point as defined subclause 12.4.2 and subclause 12.5.2.

12.9.4 Provision of Intercept Related Information

12.9.4.1 Interception at the Serving Gateway

When the IRI interception is to be done at the Serving Gateway, the Serving Gateway-C shall deliver the IRI over the X2 reference point to DF2 as defined in subclause 12.2.3, and subclause 12.4.3.

When the IRI events are to be generated from the user plane packets, the Serving Gateway-C shall provide the information to the Serving Gateway-U as it does for the CC interception in accordance to 12.9.3.1. The IRI event that requires access to the user plane packets (e.g. packet data header information) can be generated in one of the following two ways:

- Serving Gateway-C informing the SX3LIF to generate the IRI events that require access to the user plane packets (e.g. packet data header information), and SX3LIF delivering the IRI events that require access to the user plane packets (e.g. packet data header information) to the DF2

- DF3 generating the IRI event based on the user plane packets and then delivering the event to the DF2.

When the second approach (i.e. DF3-based) is used, SX3LIF does not require to support the X2 reference point.

12.9.4.2 Interception at the PDN Gateway

When the IRI interception is to be done at the PDN Gateway, the PDN Gateway-C shall deliver the IRI over the X2 reference point to DF2 as defined in subclause 12.2.3, subclause 12.3.3, subclause 12.4.3 and subclause 12.5.3.

When the IRI events are to be generated from the user plane packets, the PDN Gateway-C shall provide the information to the PDN Gateway-U as it does for the CC interception in accordance to 12.9.3.2. The IRI event that requires access to the user plane packets (e.g. packet data header information) can be generated in one of the following two ways:

- PDN Gateway-C informing the SX3LIF to generate the IRI events that require access to the user plane packets (e.g. packet data header information), and SX3LIF delivering the IRI events that require access to the user plane packets (e.g. packet data header information) to the DF2

- DF3 generating the IRI event based on the user plane packets and then delivering the event to the DF2.

When the second approach (i.e. DF3-based) is used, SX3LIF does not require to support the X2 reference point.

13 Lawful Interception for 3GPP H(e)NBs

13.0 General

Home Node B (HNB) and Home enhanced Node B (HeNB) are jointly referred to as H(e)NB as defined in TS 22.220 [31]. As identified in TS 33.106 [7], lawful interception for 3GPP H(e)NBs can be based on three different targets: a target accessing a H(e)NB, a target CSG of a H(e)NB, and a target H(e)NB.

LI for a target CSG is FFS.

LI for a target H(e)NB is FFS.

LI for Local IP Access (LIPA) via a H(e)NB is FFS.

13.1 Provision of Intercepted Content of Communications for 3GPP H(e)NBs

The access method for the delivery of intercepted content of communications (CC) is based on duplication of packets without modification.

See clause 13.4 for UMTS HNB specifics and 13.5 for HeNB specifics.

NOTE: In the case where the UE is the target of intercept, from the perspective of the core network, a H(e)NB is treated the same as a NodeB or eNodeB for CC interception purposes (i.e., no additional LI functionality is required).

13.2 Provision of Intercept Related Information for 3GPP H(e)NBs

13.2.1 X2-interface

The following information needs to be transferred to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMSI, IMEI, MSISDN, ME Id);
- events and associated parameters as defined in sections 13.4.3 may be provided;
- the H(e)NB location (if available);
- date/time of H(e)NB location (if H(e)NB location provided);
- H(e)NB ID.

H(e)NB location information needs to be transferred from the location verifying nodes per TS 33.320 [34]to the DF2 in order to allow the DF2 to perform its functionality. The manner that the location verifying node provides the DF2 with the H(e)NB location is outside the scope of this document.

The IRI should be sent to DF2 using a reliable transport mechanism.

13.33GPP H(e)NB LI Events and Event Information

For a target UE that is attached to any H(e)NB, LI events and messages for 3GPP H(e)NBs defined in this clause shall be reported in addition to the LI events and messages defined in other clauses of this document. H(e)NB LI events and event information are included in 13.4 for UMTS HNBs and 13.5 for HeNBs.

A set of possible elements as shown below is used to generate the events. Information associated with the events is transmitted from the IRI ICES to DF2.

Table 13: Information Events for H(e)NB Event Records

Element	Definition/Usage
Cause	Reason for an error or an action
Context-Id	Unique identifier for a UE used by the HNB and HNB GW.
CSG Identity	Uniquely identifies a CSG within one PLMN. Note: Open H(e)NBs do not have associated CSGs.
CSG List	Identifies the membership of a given CSG (i.e., CSG Identities and associated expiration data for the UEs).
Destination cell ID	Resultant cell ID after handover (HNB ID or PLMN cell ID)
Event type	Description which type of event is delivered
Event date	Date of the event generation
Event time	Time of the event generation.
Handover Direction	Identifies if the handover is inbound (from macro network to H(e)NB), outbound (from H(e)NB to macro network) or intra-H(e)NB (between H(e)NBs).
H(e)NB Identity	Uniquely identifies a H(e)NB (i.e., H(e)NB equipment ID and H(e)NB name)
H(e)NB IP Address	Reports the location of the H(e)NB used during location verification..
H(e)NB Location	When authorized, reports the location of the H(e)NB used during location verification prior to H(e)NB activation.
H(e)NB Time of Location	Date/Time of H(e)NB location. The time when location was obtained by the location source node.
IAs	The observed Interception Areas
Initiator	The initiator of an action (e.g., network or specific network entity, target, associate)
ISP Operator Identity	Identifies the ISP through which the H(e)NB is connected to the SeGW
Network Identifier	Unique identifier for the operator and the element carrying out the LI operations
Observed MSISDN	MSISDN of the target.
Observed IMSI	IMSI of the target.
Observed IMEI	IMEI of the target.
Observed ME Id	ME Id of the target; when it coincides with the IMEI, it shall be checked for each activation over the radio interface
Security Gateway IP Address	The IP Address of the Security Gateway used by the H(e)NB to terminate the tunnel from the H(e)NB
Source Cell ID	Original cell ID prior to handover (HNB ID or PLMN cell ID)
Tunnel Protocol	The tunnel protocol used between the H(e)NB and the SeGW

13.4 UMTS Home Node B (HNB)

13.4.0 General

Figures 13-1 shows the reference architectures upon which Lawful Interception for 3GPP HNBs is based.

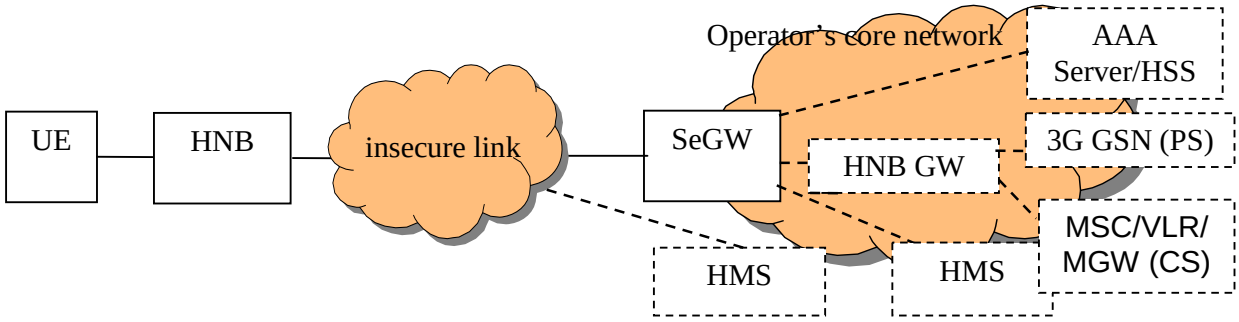


Figure 13-1: 3GPP UMTS HNB Architecture Basis for Lawful Interception

13.4.1 Intercepted Content of Communications for 3GPP UMTS HNBs

Editor's note: This section is a place holder for the scenarios where the target of interception is either a CSG or a HNB.

13.4.2 Intercept Related Information

13.4.2.0 General

Figures 13-2 show the transfer of intercept related information to the DF2.

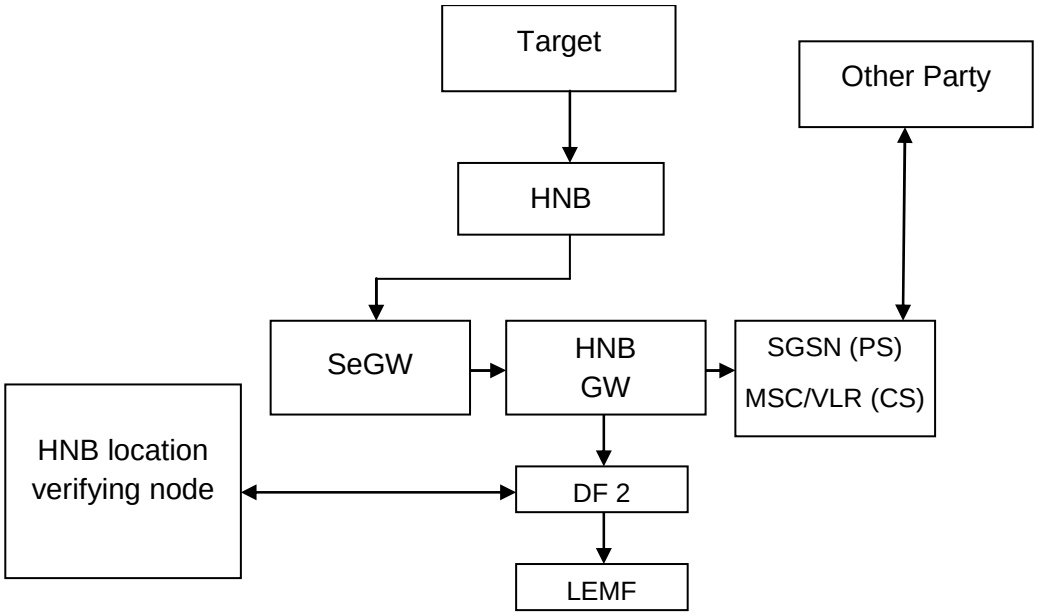


Figure 13-2: Provision of Intercept Related Information for 3GPP UMTS HNB

13.4.2.1 X2-interface

The following information needs to be transferred from the HNB GW to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMSI, IMEI, MSISDN, ME Id);
- events and associated parameters as defined in section 13.4.3 may be provided;
- the HNB location (if available);
- date/time of HNB location (if HNB location provided);

- HNB Identity.

HNB location information needs to be transferred from the location verifying node to the DF2 in order to allow the DF2 to perform its functionality.

The IRI should be sent to DF2 using a reliable transport mechanism.

13.4.3 3GPP UMTS HNB LI Events and Event Information

The following events are applicable at the HNB GW:

- Target UE Registration to HNB;
- Target UE De-Registration from HNB;
- Start of Interception with HNB attached UE;
- Target UE HNB Handover.

A set of possible elements used to generate the events is found in clause 13.3 in Table 13. Information associated with the events is transmitted from the HNB GW to DF2.

13.4.4 Structure of HNB Events

13.4.4.1 Target UE Registration to HNB

This event reports when a target UE is attempting to register to any HNB. This event is generated when

- a HNB GW sends a UE REGISTRATION ACCEPT message towards a target UE, or
- a HNB GW sends a UE REGISTRATION REJECT message towards a target UE, or
- a HNB GW receives an SCCP Connection Confirm (CC) or Connection Refused (CREF) messages from the Core Network

The elements, shown in Table 13a, will be delivered to the DF2, if available.

Table 13a: UE Registration to HNB

Observed MSISDN
Observed IMSI
Observed IMEI
Observed ME Id
Event Type
Event Time
Event Date
Network Identifier
Context-ID (for successful connection)
H(e)NB Identity
H(e)NB Location
H(e)NB Time of Location
H(e)NB IP Address
Security Gateway IP address
Tunnel Protocol
ISP Operator Identity
Cause (of failed connection, e.g., "Refusal Cause" of SCCP CREF)
CSG Identity (if closed/hybrid HNB)
CSG List (if closed/hybrid HNB) - See Note 1
IAs (if applicable)

NOTE: In a HNB GW, the CSG List is the Access Control List.

13.4.4.2 Target UE De-Registration from HNB

This event reports a when a target UE is de-registered to any HNB. This event is generated when

- a HNB GW receives a UE DE-REGISTER message from the HNB, or
- a HNB GW receives a RANAP Release Iu Connection Command message from the Core Network

The elements, shown in Table 13b, will be delivered to the DF2, if available.

Table 13b: UE De-Registration from HNB

Observed MSISDN
Observed IMSI
Observed IMEI
Observed ME Id
CSG Identity (if closed or hybrid H(e)NB)
Event Type
Event Time
Event Date
Network Identifier
H(e)NB Identity
H(e)NB Location
H(e)NB Time of Location
Initiator (i.e., HNB or Network)
Cause (of de-registration action, if known)
IAs (if applicable)

13.4.4.3 Start of Intercept with HNB attached UE

This event will be generated if interception for a target UE is started when the target UE has already registered and is receiving service from a HNB. The elements, shown in Table 13c, will be delivered to the DF2, if available.

Table 13c: Start of Intercept with Target UE active on a HNB

Observed MSISDN
Observed IMSI
Observed IMEI
Observed ME Id
H(e)NB Identity
CGS Identity (if closed or hybrid H(e)NB)
Event Time
Event Date
Network Identifier
H(e)NB IP Address
Security Gateway IP address
Tunnel Protocol
ISP Operator Identity
CSG List (if closed or hybrid HNB) - See Note 1
H(e)NB Location
H(e)NB Time of Location
IAs (if applicable)

NOTE: In a HNB GW, the CSG List is the Access Control List.

13.4.4.4 Target UE HNB Handover

This event reports a when a registered target UE moves from a cell on the serving PLMN to a HNB, from a HNB to a cell on the serving PLMN, or from a HNB to another HNB. This event is generated when

- a HNB GW receives an inbound UE relocation trigger (e.g., RANAP Relocation Request message from the Core Network), or

- a HNB GW receives a HNBAP: UE RELOCATION COMPLETE message from the Destination HNB (i.e., the "Target HNB" per TS 25.467 [33]) , or

- a HNB GW acts as a Iurh proxy and sends a RADIO LINK RESTORE INDICATION message from the "Drift HNB" to the "Serving HNB" per TS 25.467 [33]) (i.e., a target UE is involved in a soft handover between HNBs)

The elements, shown in Table 13d, will be delivered to the DF2, if available.

Table 13d: UE Handover

Observed MSISDN
Observed IMSI
Observed IMEI
Observed ME Id
Event Type
Event Time
Event Date
Network Identifier
Context-ID (for successful connection)
Cause (of failed connection, e.g., "Refusal Cause" of SCCP CREF)
CSG Identity (if closed/hybrid HNB)
CSG List (if closed/hybrid HNB) - See Note 1
Handover Direction
Source cell ID (HNB ID or PLMN cell ID)
Destination cell ID (HNB ID or PLMN cell ID)
IAs (if applicable)

NOTE 1: In a HNB GW, the CSG List is the Access Control List.

NOTE 2: The soft handover between HNBs that are directly connected and the HNB GW is not involved is not part of 3GPP specifications.

13.5 Home enhanced Node B (HeNB)

Figure 13-3 show the reference architectures upon which Lawful Interception for 3GPP HeNBs is based. Per TS 36.300 [32], HeNB GW is optional.

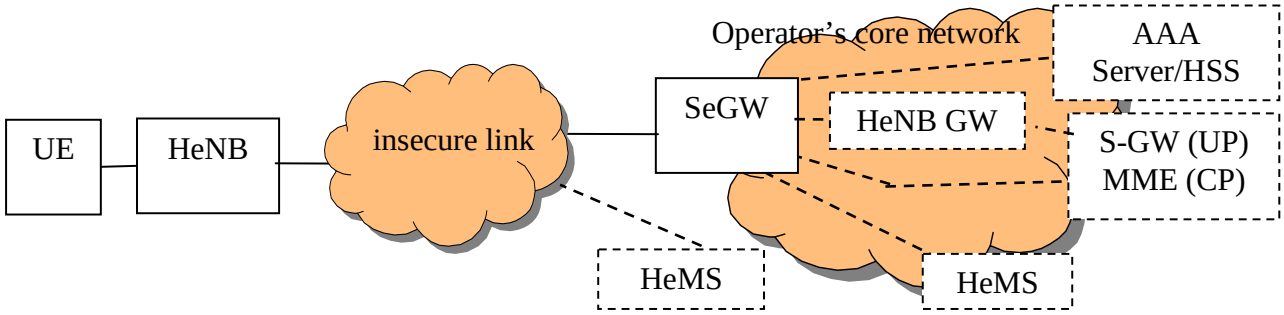


Figure 13-3: 3GPP HeNBs Architecture Basis for Lawful Interception

In the case where the UE is the target of intercept, LI functionality is specified in clause 12.

14 Interception of Generic Bootstrapping Architecture (GBA) Secured Communications

14.1 Introduction

The Generic Bootstrapping Architecure (GBA) is defined in the TS 33.220 [35]. This section details the stage 2 Lawful Interception architecture and functions that are needed to provide the GBA based application specific encryption keys from the GBA architecture towards the DF2 for a subscriber that is target of interception.

Figure 14.1 shows the LI architecture for the GBA where the BSF provides the events and associated information towards the DF2 over the X2 interface.

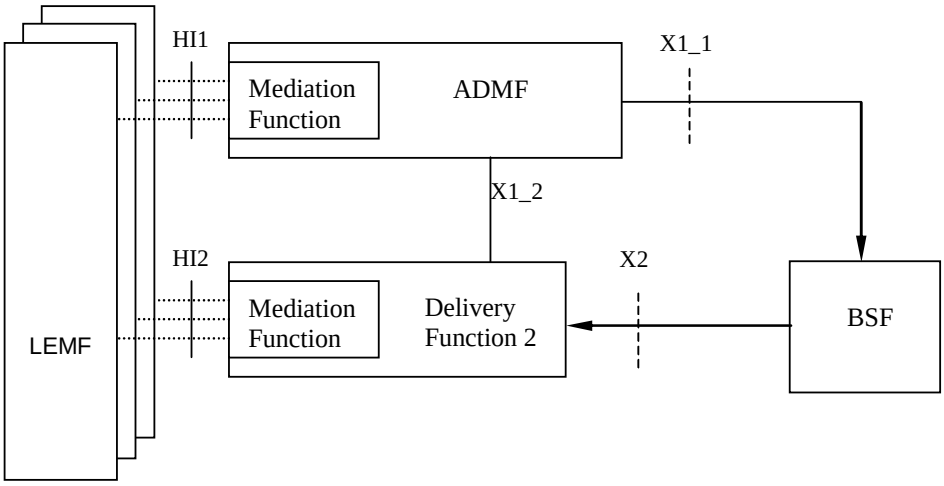


Figure 14.1: GBA Intercept Configuration

14.2 Provision of Content of Communications

The GBA interception provides the application specific cryptographic keys (aka GBA application specific keys) which are used to decrypt the intercepted communication secured using those GBA application specific keys. Interception of the content of communications for GBA secured services is not part of this section and can be achieved via other methods outlined in this specification. The Ua protocol Id and the NAF Id along with the GBA application specific keys will allow the LEMF to decrypt the received intercepted packets.

NOTE 1: The details of LI capabilities for GBA in a roaming scenario is for further study.

NOTE 2: The delivery by the CSP of intercepted packets in a decrypted form is for further study.

14.3 Provision of Intercept Related Information

14.3.1 Provision of Intercept Related Information Data Flow

Figure 14.2 shows the transfer of intercept related information to the DF2. If an event related to a target occurs, the BSF shall send the relevant data to the DF2.

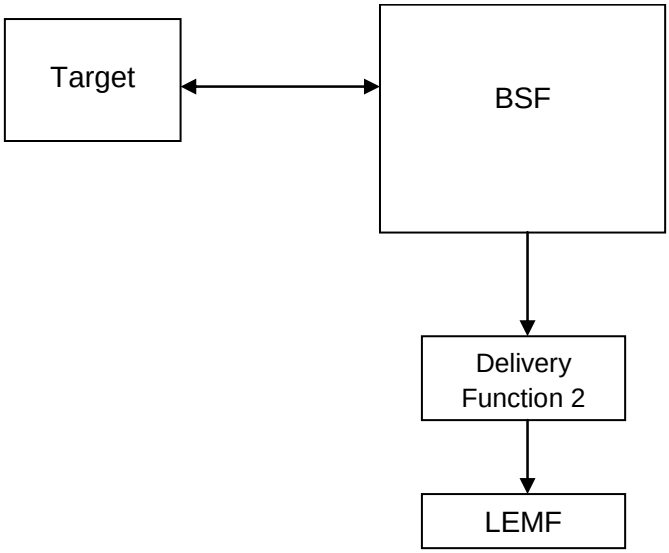


Figure 14.2: Provision of Intercept Related Information

14.3.2 X2-interface

The following information needs to be transferred from the BSF to the DF2 in order to allow a DF2 to perform its functionality:

- target identity;
- events and associated parameters as defined in clauses 14.3.3 may be provided;

The IRI should be sent to DF2 using a reliable transport mechanism.

14.3.3 GBA LI Events and Event Information

Intercept Related Information (Events) are necessary for the following;

- Bootstrapping
- Query from NAF
- Start of interception with GBA key

A set of possible elements as shown in Table 14.3.1 are used to generate the events.

Table 14.3.1: Information Events for GBA Event Records

Element
Observed IMSI IMSI of the target.
Observed Other Identity Other Identity of the target.
Event type Description which type of event is delivered: Bootstrapping, Query from NAF, Start of interception with GBA key
Event date Date of the event generation in the BSF
Event time Time of the event generation in the BSF.
Network Element Identifier Unique identifier for the element reporting the BSF.
B-TID Bootstrapping transaction identifier, TS 33.220 [35].
Key lifetime The lifetime of the key material is set according to the local policy of the BSF, TS 33.220 [35].
Bootstrapping time The timestamp of the bootstrapping event.
Ks_int_NAF GBA application specific key (internal), if GBA_U has been used, TS 33.220 [35].
Ks_ext_NAF GBA application specific key (external), if GBA_U has been used, TS 33.220 [35].
Ks_NAF GBA application specific key, if GBA_ME has been used, TS 33.220 [35].
Ua protocol id Ua interface security protocol id defined in clause Annex H in TS 33.220 [35].
NAF_Id The FQDN of the NAF, concatenated with the Ua security protocol identifier, TS 33.220 [35].

14.4 Structure of GBA Events

14.4.1 Bootstrapping

This event will be generated when the UE triggers a bootstrapping procedure towards the BSF when the UE wants to interact with a NAF. The actual bootstrapping procedure is defined in the TS 33.220 [35], in sections 4.5.2 and in 5.3.2. The information elements shown in Table 14.4.1 table, if available, will be delivered to the DF2, by the BSF.

Table 14.4.1: Bootstrapping

Observed IMSI
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
B-TID
Key lifetime
Bootstrapping time

14.4.2 Query from NAF

The Query from NAF event is generated when the BSF receives an application specific key query from a NAF in order to retrieve GBA based application specific keys and related information. A new event is generated for each individual query events. The information elements shown in Table 14.4.2 will be delivered to the DF2, if available, by the BSF.

Table 14.4.2: Query from NAF

Observed IMSI
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Ks_ext_NAF
NAF_Id
Ks_int_NAF
Ks_NAF
Key lifetime
Bootstrapping time
Ua protocol id

14.4.3 Start of Interception with GBA key

For start of interception where GBA application specific key is already in use a Start of Interception with GBA key event is generated. The elements, shown in Table 14.4.3 will be delivered to the DF2, if available, by the BSF.

Table 14.4.3: Start of Interception with GBA key

Observed IMSI
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
B-TID [Note]
NAF_Id [Note]
Ks_ext_NAF [Note]
Ks_int_NAF [Note]
Ks_NAF [Note]
Key lifetime [Note]
Bootstrapping time [Note]
Ua protocol id [Note]

NOTE: These are repeated for each GBA application specific key associated with the target.

15 Invocation of Lawful Interception for IMS-based VoIP

15.1 Overview of VoIP Interception

The capabilities defined in this clause apply when the interception of content of communications for IMS-based VoIP is to be separated from the interception of content of communication at the packet data network. Non-Local ID targeting described in clause 7.A is also valid in such case.

The network nodes, involved in providing the interception of an IMS-based VoIP call, shall be determined based on the deployment configuration and the call scenario. The scenarios where the media transport nodes and signalling nodes are handled by different CSPs are beyond the scope of this standard.

NOTE: Lawful interception of VoIP as it applies SR-VCC (see TS 23.237 [45]) is for further study.

The interception of IRI for a VoIP call shall be done according to 15.3. The interception of VoIP CC shall be done according to 15.2.

15.2 Provision of Content of Communications

15.2.0 Overview

As the interception of CC needs to be done at a network node that has access to the voice media, and that interception of CC is required for all targeted calls, including forwarded calls and transferred calls, the CSP needs to support the capability to dynamically trigger CC interception for a call at a network node that has access to the voice media. Depending on the CSP's network configuration and the call scenario, different network elements will intercept the CC.

The interception and delivery of CC for VoIP may be done at the following functional element:

1) PDN-GW/GGSN;

2) IMS-AGW;

3) TrGW;

4) IM-MGW;

5) MRF.

NOTE 2: Other functional elements may also be applicable in specific deployment scenarios.

NOTE 3: The redirection of target communications to a specific network element purely for LI purposes is undesirable.

The functional elements that provide the signalling to generate the trigger for the CC interception may be any of the following functional elements:

- P-CSCF, for PDN-GW/GGSN and IMS-AGW;
- IBCF for TrGW;
- MGCF for IM-MGW;
- S-CSCF or AS for MRF.

At any given time, for a specific target and for any given call, only one functional element is required to provide the CC interception. The functional element that provides the CC interception may vary, primarily, based on the call scenario.

Annex E shows scenarios where the use of the above functional elements is applicable.

15.2.1 General Principles of CC Interception

15.2.1.1 Intercept Trigger

As the interception of IRI and CC is required for all targeted VoIP calls, including forwarded and transferred calls, the CC shall be correlated with the IRI. The CC Interception Triggering Function triggers the CC interception for a call at the CC Intercept Function. The placement of the CC Interception Triggering Function is dependent on CSP network implementation, the call scenario, and the placement of network nodes that have access to the voice media.

The CC Interception Triggering Functions sends a CC intercept trigger to the CC Interception Function to activate CC interception for a call.

The intercept trigger, at the minimum, shall consist of the following:

- Correlation Identifier;
- Media Identifier

The Correlation Identifier is used correlate the CC with the corresponding IRI data and is delivered from the CC Intercept Function in the intercepted media packet (i.e., CC) over the X3 interface to the Delivery Function 3.

The Media Identifier is used to identify the media packets that have to be intercepted. The technique used in defining the Media Identifier is implementation specific.

The information passed in this CC intercept trigger shall adhere to the security requirements outlined in clause 8.

The mechanism used to provide the correlation between CC and IRI is implementation specific. For instance:

- The CC Interception Triggering Function may send the correlation identifier value to the CC Interception Function that forwards it to DF3 onto X3 interface;
- The CC Interception Triggering Function may send the correlation identifier (onto X2 interface) to the DF2 that forwards it to DF3. In this case the SDP information may be used to associate the CC packets with the IRI.

15.2.1.2 X3-Interface

For the delivery of intercepted media packets, the following information shall be passed from the CC Intercept Function to the Delivery Function 3 in addition to the intercepted media packets:

- target identity;
- correlation identifier;
- SDP information (optional);
- time stamp (optional);
- direction (indicates media is from or to the target) - optional;

The Delivery Function 3 delivers the information to the LEMF over the HI3 interface based on the national regulations.

15.2.2 VoIP CC Interception

The capabilities defined in this clause apply for the following cases:

- When a target originates a call or receives an incoming call - the target's media passes through the indicated CC Intercept Function.
- When an incoming call to the target is forwarded, the media of the forwarded call passes through the indicated CC Intercept Function.

The term "CC Intercept Function" is a generic term used to denote a network function that has access to the voice media of an intercepted call. The term "CC Interception Triggering Function" is a generic term used to denote a network function that provides a trigger to intercept the CC. The examples of CC Intercept Function and CC Interception Triggering Function are listed at the beginning of clause 15.2

Figure 15.1 illustrates the CC interception at the CC Intercept Function for a basic call. Figure 15.2 illustrates the CC interception at the CC Intercept Function for a forwarded call.

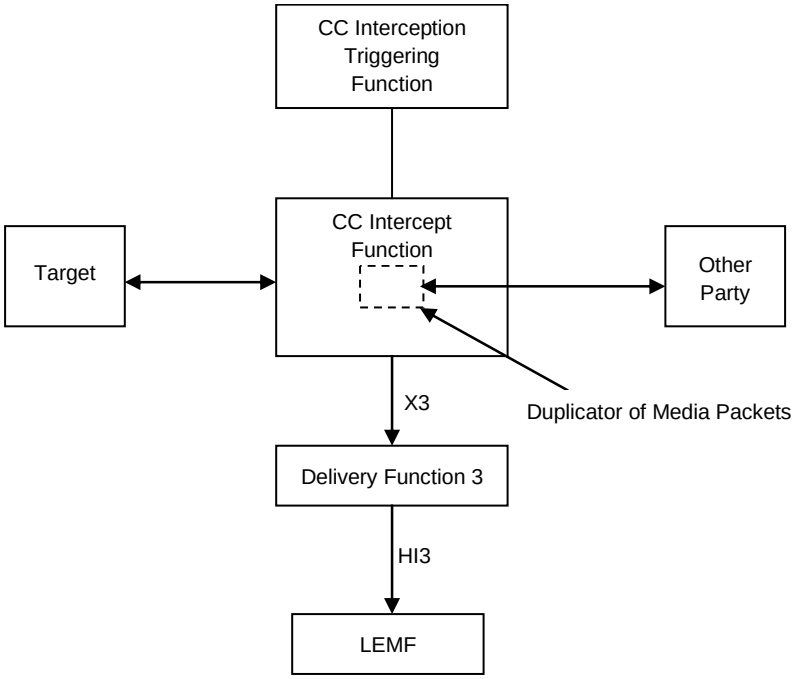


Figure 15.1: VoIP CC Interception for basic calls

In figure 15.1, the Target is the target and the Other Party is the called party when the target originates a call; and the Other Party is the calling party when the target receives an incoming call. In both cases, the media passes through the CC Intercept Function present on the side of target's access network.

In figure 15.2 (below), there is no Target (i.e., target) shown because this is the scenario where an incoming call to a target gets forwarded. The figure 15.2 shows the calling party who originated call and the forwarded-to-party who receives the forwarded call. The media passes through the CC Intercept Function associated with the forwarded-to-party.

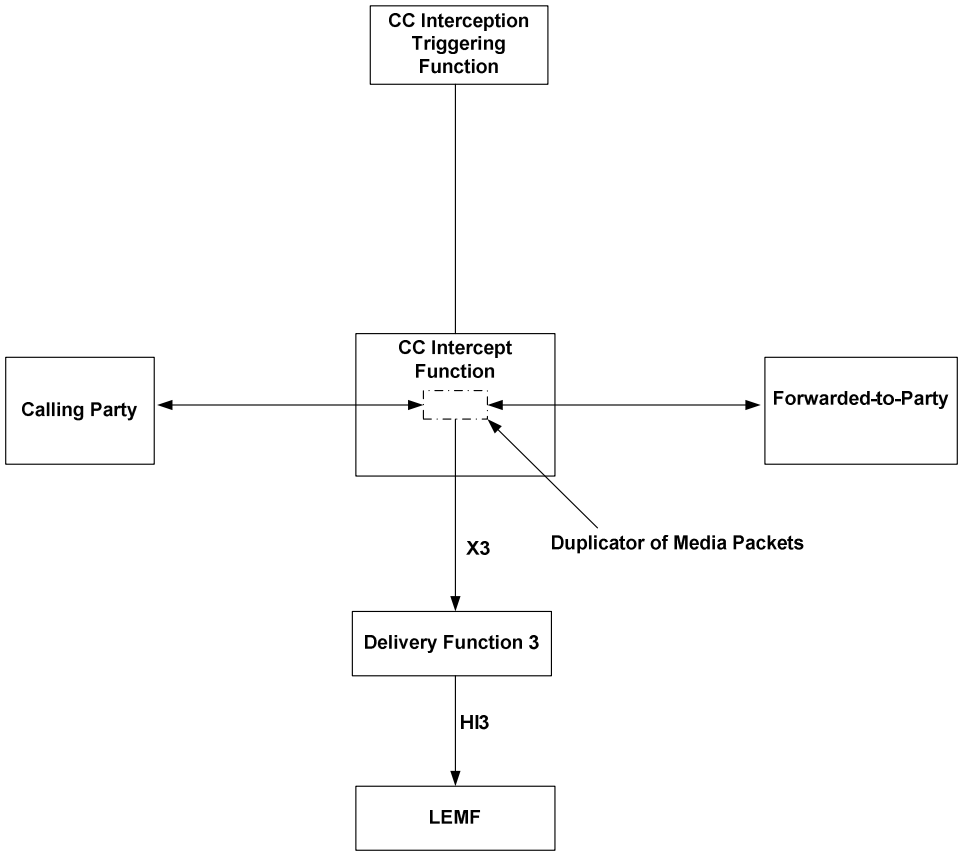


Figure 15.2: VoIP CC Interception for forwarded calls

The CC Interception Triggering Function sends the CC intercept trigger to the CC Intercept Function according 15.2.1.1. The CC Intercept Function intercepts media packets for the call (identified based on the Media Identifier information received over the intercept trigger) and delivers the media packets as according to 15.2.1.2.

See Annex E and Annex F for details of Call Forwarding related scenarios and call flows.

15.2.3 Media Information Associated with the CC

When the media description known through the SDP offer and answer at the IRI ICE is different from the media description known to the CC Intercept Function, then CC Intercept Triggering Function may have to send the media description to the DF2 for reporting to the LEMF. See Annex G for illustrative examples.

NOTE: In case the CC Intercept Triggering Function is included in the P-CSCF this may be achieved by using the X2 interface between the P-CSCF and DF2/MF.

The media description associated with the CC delivered to the LEMF over HI3 shall also be reported to the LEMF in case it is different from both of the above indicated media descriptions.

15.2.4 CC Interception in HPLMN with IMS Roaming

For roaming targets who are physically not in the legal jurisdiction of the home network, depending on the roaming architecture deployed, media of the target may not enter the HPLMN for certain call scenarios. In such situations, based on the national option, the HPLMN served with the intercept order shall do the following:

- Perform the interception without the CC and report to the LEMF that the CC is unavailable due to target's roaming situation. Note that the Evolved Serving System message (when EPS is part of the IP-CAN) also indicates to the LEMF that the target is roaming.

See TS 33.108 [11] for the method used to report the CC unavailability indication.

15.2.5 CC Interception with CUPS

With control and user plane separation of PDN-GW, the LI architecture defined in subclause 12.9 shall be used to provide the CC Intercept Function at the PDN-GW with the following extensions:

- The PDN Gateway-C shall receive the CC intercept trigger from the CC Intercept Triggering Function.
- The PDN Gateway-C shall use the target identity and correlation identifier received from the CC Intercept Triggering Function to notify the SX3LIF.
- The PDN Gateway-C shall send the packet detection rules (as described in subclause 12.9.2) to intercept the user plane packets from the media bearer to the PDN Gateway-U.

The PDN Gateway-U shall forward user plane packets to the SX3LIF as described in subclause 12.9. The SX3LIF shall deliver the CC to the DF3 over X3 as described in subclause 12.9 and subclause 15.2.

15.3 Provision of Intercept Related Information for VoIP

See clause 7.A.

15.4 Lawful interception in the VPLMN with IMS roaming

15.4.1 Local breakout with P-CSCF in the VPLMN

LBO (as defined in TS 23.228 [43]) as a roaming architecture used for VoLTE is one of the examples of IMS roaming. Local Breakout architecture has several options (LBO Home Routing, LBO Visited Routing: the interception of IRI and CC in the VPLMN are independent of such options).

When an inbound roaming target originates a call or receives a terminating call, the P-CSCF present in the VPLMN provides IRI interception functions as described in clause 7A. The PDN-GW/GGSN or the IMS-AGW deployed in the VPLMN provides the CC interception as described in clause 15.2. The P-CSCF sends the CC intercept trigger to the PDN-GW/GGSN or to the IMS-AGW as described in clause 15.2.

NOTE: The extent of the LI capabilities available in the VPLMN is limited to the information available in the VPLMN. In addition, almost all the supplement services are handled in the HPLMN. Hence, where supplementary services are exclusively handled in the HPLMN and information related to that service is not available in the VPLMN, LI for that service might be limited or even not available in the VPLMN. For example, when an incoming call to the inbound roaming target is forwarded (by the HPLMN), the VPLMN is not involved in that call forwarding and therefore, no reporting will be done by the VPLMN. For call forwarding no answer, the initial reporting might be done, however, once the forwarding happens, the VPLMN reports that the call has ended.

Annex E illustrates a few scenarios of lawful interception in the VPLMN for inbound roaming target.

15.5 Constraints for IMS VoIP Roaming Interception

National regulations may limit delivery of communications (CC and communications-associated IRI) of an outbound international roaming target by the HPLMN as described in clause 5.1.4 of TS 33.106 [7].

If roaming interception is allowed, IMS VoIP interception and delivery to the LEMF by the HPLMN shall proceed normally as described elsewhere in this specification when the target is roaming outside the country as well as when the target is within the country.

If roaming interception is not allowed and it is determined that the target is outside the country, the HPLMN shall act as follows:

The HPLMN shall report IRI and CC for IMS VoIP sessions where the target is not participating in the IMS VoIP services which can be the result of the activation, invocation, or operation of any supplemental services that are performed entirely by the HPLMN. This can include invocation before an IMS VoIP session, at the beginning of an IMS VoIP session, mid IMS VoIP session, or at the end of an IMS VoIP session. Examples of such supplemental services include diversion services such as call forwarding (all calls, busy calls, etc.). Services where the target is still participating in the IMS VoIP session would not be reported (e.g., call hold, conferencing).

16 LI for Group Communications using GCSE

16.1 Background

There are several scenarios possible for the interception of group communications involving GCSE (see TS 22.468 [51] and TS 23.468 [53]). First is where the GCSE AS is part of an operator's network. Second is where the GCSE AS is outside of the intercepting operator's network. This clause specifies LI solutions for both cases.

16.2 GCSE AS in Operator Network

16.2.0 General

In the case where the GCSE AS is in the operator's network, the ICE in this case will be the GCSE AS as it is fully aware of the group communications as well as the parties on the communications. The solution is very similar to the conferencing solution specified in Clause 11, where the main difference is that a single functional entity (the GCSE AS) is utilized for GCSE, rather than two functional entities.

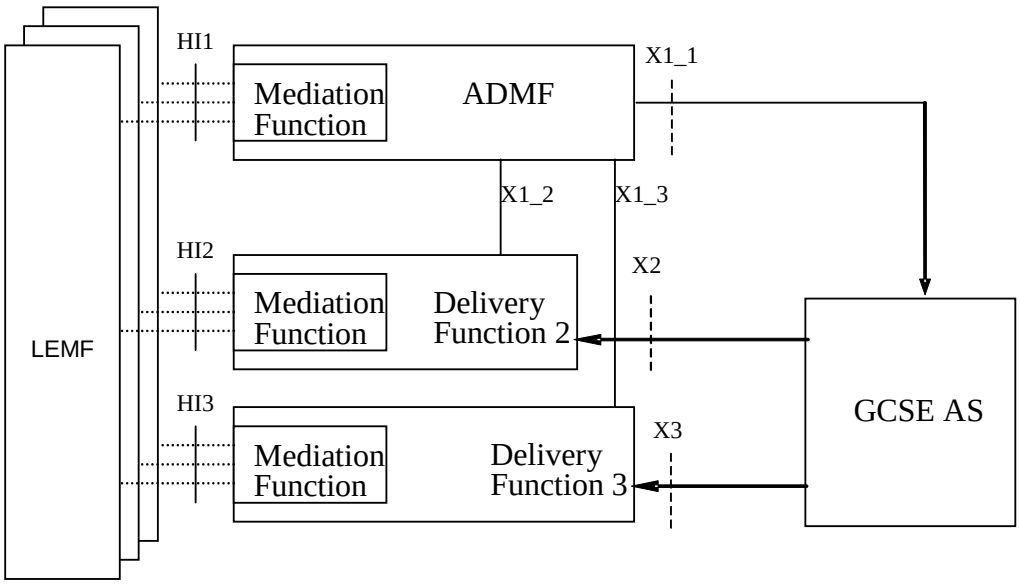


Figure 16.1: GCSE AS Intercept configuration

16.2.1 Provision of Content of Communications

16.2.1.0 General

Figure 16.2 shows the interception of the content of communications for GCSE at the GCSE AS is performed based on identifying the target of interception being a member of a group communication at the GCSE AS.

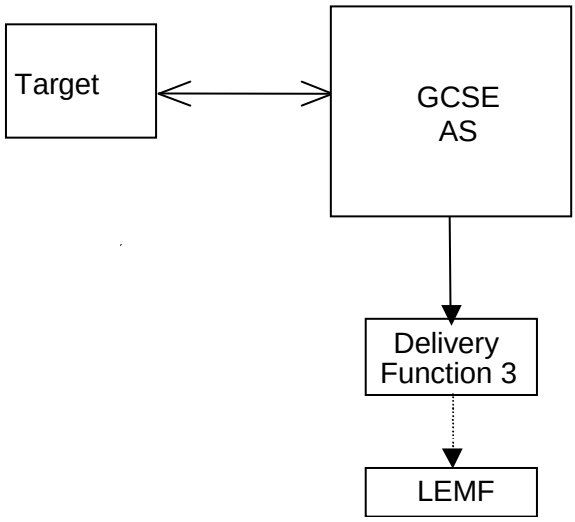


Figure 16.2: Provision of Intercept Product from GCSE AS

16.2.1.1 X3-interface

In addition to the intercepted content of communications, the following information may need to be transferred from the GCSE AS to the DF3 in order to allow the DF3 to perform its functionality:

- identity used for interception include IMSI, IMEI, ProSe UE ID (see TS 22.278 [50] and TS 23.303 [52]);
- correlation number;
- the identity of source (i.e. group communications party identity) of a media stream;
- time stamp;
- direction (from target or to target).

16.2.2 Provision of Intercept Related Information

16.2.2.0 General

Figure 16.3 shows the transfer of intercept related information to the DF2. If an event for / from a GCSE user occurs, the GCSE ASshall send the relevant data to the DF2.

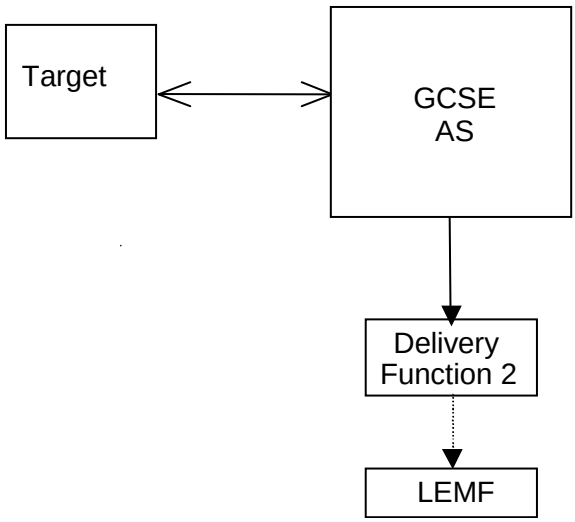


Figure 16.3: Provision of Intercept Related Information

16.2.2.1 X2-interface

The following information needs to be transferred from the GCSE AS to the DF2 in order to allow a DF2 to perform its functionality:

- target identity include IMSI, IMEI, ProSe UE ID;
- events and associated parameters as defined in clauses 12.2.1.2 and 12.2.3 may be provided.

The IRI should be sent to DF2 using a reliable transport mechanism.

16.2.2.2 GCSE AS LI Events and Event Information

16.2.2.2.0 General

Intercept Related Information events to be reported by the GCS AS include:

- When GCSE communications group involving a target of interception is activated (enabled for communications)
- When GCSE communications group involving a target of interception is deactivated (no longer enabled for communications)
- When a User is added to an active GCSE communications group
- When a User is dropped from an active GCSE communications group
- Start of Interception with an Active GCSE communications Group
- End of Interception with an Active GCSE communications Group
- Modification of Target Connection to GCS AS.

A set of possible elements as shown in Table 16.4 are used to generate the events.

Table 16.4: Information Events for GCS AS Event Records

Element
Observed IMSI IMSI of the target.
Observed IMEI IMEI of the target.
Observed ProSe UE ID ProSe UE ID of the target.
Observed Other Identity Other Identity of the target
Event type Description which type of event is delivered: Group Activated, Group Deactivated. Group Add Member, Group Drop Member, Start of Intercept with Active Group, End of Intercept with Active Group, Modification of Active Group.
Event date Date of the event generation in the GCS AS.
Event time Time of the event generation in the GCS AS. Timestamp shall be generated relative to the GCS AS internal clock.
Observed Communications Group ID Identifies the GCSE communications group at the GCS AS.
GCSE Group Communication Characteristics Details of the Group Communications Service to which the Target is a member including such characteristics such as voice, video, and data communications.
GCSE Communications Group Membership List List of all users that are members of the GCSE communications group. Not all members may be participants in a group communications.
GCSE Communications Group Participants List of all users that are participating in the GCSE communications group.
Correlation Number The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records.
Network Element Identifier Unique identifier for the element reporting the ICE.
Added User ID Identity of the party successfully added to an active GCSE Communications Group.
Dropped User ID Identity of the party successfully dropped from an active GCSE Communications Group.
Target Connection Method Identifies the current target connection method with the GCS AS including whether the target is connected at all.
Modified Target Connection Method Identifies the modified target connection method with the GCS AS when the target connection method changes including whether the target is connected at all.
Identity of Visited Network Identifies the visited network from which the target is connecting to the GCS AS.
Length of TMGI Reservation Time Identifies the length of time reserved for use of a TMGI for a GCSE Communications Group.
Reserved TMGI Identifies the TMGI reserved for use by a GCSE Communications Group.
Location information Location information of the target, e.g., Cell ID as known by the GCS AS.
Time of Location Date/Time of location. The time when location was obtained by the location source node.

NOTE: Generation of Correlation Number is FFS.

16.2.2.2.1 Activation of GCSE Communications Group

When a GCSE communications group is activated at the GCS AS (i.e., enabled for communications), an Activation of GCSE Communications Group event is generated in the following cases:

- When the GCS AS successfully activates a GCSE communications group in which a member is a target of interception.

The fields, shown in Table 16.5, will be delivered to the DF2, if available, by the GCS AS.

Table 16.5: Activation of GCSE Communications Group

Observed IMSI
Observed IMEI
Observed ProSe UE ID
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Target Connection Method
GCSE communications group membership list
GCSE communications group participants
Group Communications Characteristics
Observed Communications Group ID
Reserved TMGI
Length of TMGI reservation time (if known)
Identity of Visited Network (if known)

16.2.2.2.2 Deactivation of GCSE Communications Group

When a GCSE communications group is deactivated (not enabled for communications) at the GCS AS, a Deactivation of GCSE Communications Group event is generated in the following cases:

- When the GCS AS successfully releases a GCSE communications group in which a member is a target of interception.

The fields, shown in Table 16.6, will be delivered to the DF2, if available, by the GCS AS.

Table 16.6: Deactivation of GCSE Communications Group

Observed IMSI
Observed IMEI
ProSe UE ID
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
GCSE communications group membership list
Observed Communications Group ID
Reserved TMGI
Length of TMGI reservation time (if known)
Identity of Visited Network (if known)
Location Information
Time of Location

16.2.2.2.3 User Added

A User Added-event is generated in the following cases:

- When a user is successfully added to a GCSE communications group in which a member is a target of interception.

The fields, shown in Table 16.7, will be delivered to the DF2, if available, by the GCS AS.

Table 16.7: User Added

Observed IMSI
Observed IMEI
Observed ProSe UE ID
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Added User ID
GCSE communications group membership list
Observed Communications Group ID
GCSE communications group participants
Reserved TMGI
Identity of Visited Network (if known)

16.2.2.2.4 User Dropped

A User Dropped-event is generated in the following cases:

- When a user is successfully dropped from a GCSE communications group in which a member is a target of interception.

The fields, shown in Table 16.8, will be delivered to the DF2, if available, by the GCS AS.

Table 16.8: User Dropped

Observed IMSI
Observed IMEI
Observed ProSe UE ID
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Dropped User ID
GCSE communications group membership list
Observed Communications Group ID
GCSE communications group participants
Reserved TMGI
Identity of Visited Network (if known)

16.2.2.2.5 Start of Intercept with an Active GCSE Communications Group

When an intercept is started with an active GCSE communications group, a Start of Intercept for GCSE Communications Group event is generated in the following cases:

- When a target of interception is successfully added to an active GCSE communications group.
- When interception is activated for a target of interception who is already a member of an active GCSE communications group.

The fields, shown in Table 16.9, will be delivered to the DF2, if available, by the GCS AS.

Table 16.9: Start of Intercept with an Active GCSE Communications Group

Observed IMSI
Observed IMEI
Observed ProSe UE ID
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Target Connection Method
GCSE communications group membership list
Group Communications Characteristics
Observed Communications Group ID
GCSE communications group participants
Reserved TMGI
Length of TMGI reservation time (if known)
Identity of Visited Network (if known)
Location Information
Time of Location

16.2.2.2.6 End of Intercept with an Active GCSE Communications Group

When an intercept is ended with an active GCSE communications group, an End of Intercept for GCSE Communications Group event is generated in the following cases:

- When a target of interception is successfully dropped from an active GCSE communications group.

The fields, shown in Table 16.10, will be delivered to the DF2, if available, by the GCS AS.

Table 16.10: End of Intercept with an Active GCSE Communications Group

Observed IMSI
Observed IMEI
Observed ProSe UE ID
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
GCSE communications group membership list
Observed Communications Group ID
GCSE communications group participants
Reserved TMGI
Length of TMGI reservation time (if known)
Identity of Visited Network (if known)
Location Information
Time of Location

16.2.2.2.7 Modification of Target Connection to GCS AS

When a modification to a target connection to the GCS AS occurs, a Modification of Target Connection event is generated in the following cases:

- When a target of interception changes the current downlink communications reception method to now receive only via a unicast link, only via a multicast link, or via both unicast and multicast links.

- When the target of interception changes the uplink and downlink connection method from not connected to one of the connected connection methods, and vice versa.

The fields, shown in Table 16.11, will be delivered to the DF2, if available, by the GCS AS.

Table 16.11: Modification of Target Connection to GCSE AS

Observed IMSI
Observed IMEI
Observed ProSe UE ID
Observed Other Identity
Event Type
Event Time
Event Date
Network Element Identifier
Correlation Number
Modified Target Connection Method
GCSE communications group membership list
Group Communications Characteristics
Observed Communications Group ID
GCSE communications group participants
Reserved TMGI
Length of TMGI reservation time (if known)
Identity of Visited Network (if known)
Location Information
Time of Location

16.3 GCS AS outside Intercepting CSP Network

Interception of group communications by the intercepting CSP when the GCS AS is outside of the CSP's network, is not provided in this release. Packet data interception capabilities can be used to intercept and report a target's communication.

17 Interception for Proximity Services

17.1 ProSe Direct Discovery

17.1.1 General

Proximity Service (ProSe) are specified in TS 23.303 [52]. This includes Direct Discovery where two UEs may discover that they are in proximity using direct signalling between the UEs, where such signalling both controlled by and reported to the ProSe Function.

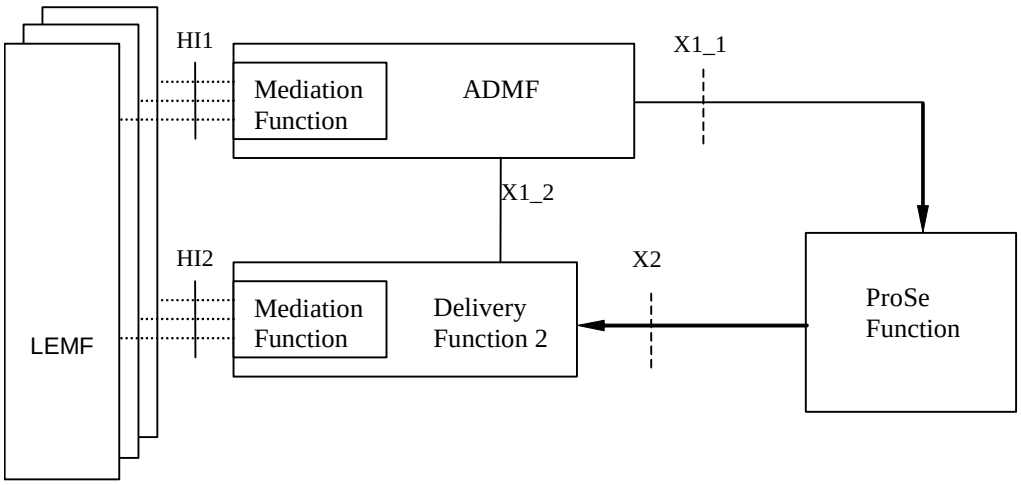


Figure 17.1-1: ProSe Direct Discovery Intercept configuration

Figure 17.1-1 shows the IRI interception configuration for ProSe Direct Discovery. The HI2 interface represents the interface between the LEA and the delivery function. The delivery function is used to distribute the Intercept Related Information (IRI) to the relevant LEA(s) via HI2. See Clause 4 for more information on the ADMF and other interfaces.

The target identity for ProSe Direct Discovery interception is the IMSI. The activation, deactivation, and interrogation of interception regarding the ProSe Function shall follow the requirements of Clause 5.

17.1.2 Provision of Inteception of Call Content

Interception of direct discovery does not have a call content component as all the information useful to the LEA is provided as part of the IRI interception.

17.1.3 Provision of Intercept Related Information

17.1.3.1 General

Figure 17.1.3.1-1 shows the transfer of intercept related information (IRI) to the DF2. If an event involving a target occurs, the ProSe Function shall send the relevant data to the DF2. A UE always contacts the ProSe Function in its HPLM, which then contacts the other relevant ProSe Functions to complete the UEs request.In the case of Match Report event, it is possible that a non-target monitoring UE will tigger interception of a target UE when it reports a code announced by that target UE.

This is illustrated in the following figure where it should be noted that only one subcriber to HPLMN ProSe Function interaction is needed to trigger an interception event.

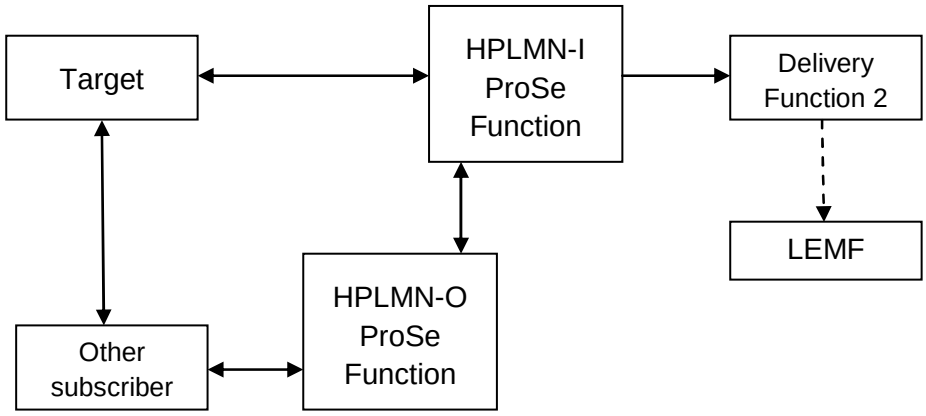


Figure 17.1.3.1-1: Provision of Intercept Related Information for discovery

17.1.3.2 X2-interface

The following information needs to be transferred from the ProSe Function to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMSI);
- events and associated parameters, as defined in section 17.1.3.3;

The IRI should be sent to DF2 using a reliable transport mechanism.

17.1.3.3 ProSe LI Events and Event Information

17.1.3.3.1 ProSe LI Events

The following events are applicable to the interception of direct discovery:

- Discovery Request
- Match Report

Interception of these events is mandatory in the ProSe Function of the PLMN that is used for direct discovery.

17.1.3.3.2 ProSe LI Event Information

A set of possible elements as shown below is used to generate the events.

Table: 17.1.3.3.2-1: Information Events for ProSe Event Records

Element
Observed IMSI IMSI of the target
Event type Description which type of event is delivered:- Discovery Request, Match Report
Event date Date of the event generation in the ProSe Function
Event time Time of the event generation in the ProSe Function. Timestamp shall be generated relative to the ProSe Function internal clock.
Role of the target Whether the target is an announcing or a monitoring UE
Discovery PLMN identity PLMN used or to be used for the discovery
ProSe Application ID Name Identity of a user within the context of a specific application
Metadata Metadata relating to a ProSe Application ID Name of the announcing UE
Network Element Identifier Unique identifier for the element reporting the ICE.
Timer The "Validity Timer" or "Time to Live" value assigned by the network to a specific ProSe Application Code or Filter, that controls how long the UE can announce/monitor it
Identity of the other UE In Match reports, there is a second UE involved.
ProSe Application Code Bitstring that is actually announced over the air or included in a discovery filter applied by UE
ProSe App Mask Bitmask that allows the monitoring UE to perform full or partial matching. Multiple Masks may be included in a Discovery Filter. The length of the mask is the same as the length of ProSe Application Code

17.1.3.3.3 Structure of ProSe Events

17.1.3.3.3.1 Discovery Request

For ProSe Discovery Requests, a Discovery Request event is generated. The elements shown in Table 17.1.3.3.1-1 will be delivered by the ProSe Function to the DF2, if available. A new Discovery Request Event shall be generated for each individual ProSe Discovery Request received by the ProSe Function.

Table 17.1.3.3.3.1-1: Discovery Request

Observed IMSI	
Event Type	
Event Time	
Event Date	
Role of the target	
Network Element Identifier	
Discovery PLMN identity	
ProSe Application ID Name	
Timer	
Metadata	(If Applicable)
ProSe Application Code	
ProSe App Mask	(If Applicable)

17.1.3.3.3.2 Match Report

For ProSe Match Report, a Match Report event is generated. The elements shown in Table 17.1.3.3.2-1 will be delivered by the ProSe Function to the DF2, if available. A new Match Report Event shall be generated for each individual ProSe Match Report received by the ProSe Function.

Table 17.1.3.3.3.2-1: Match Report

Observed IMSI	
Event Type	
Event Time	
Event Date	
Role of the target	
Network Element Identifier	
Discovery PLMN identity	
ProSe Application ID Name	
Timer	
Metadata	(If Applicable)
Identity of the other UE	(If Available)
ProSe Application Code	

17.2 ProSe One To Many Communications

17.2.1 General

Proximity Service (ProSe) are specified in TS 23.303 [52]. This includes one to many communications among Public Safety ProSe UEs with such communication occuring while the UEs are in proximity. There are several procedures that takes place with network elements as part of a typical one-to-many commuication. The UE needs to be authorised by the ProSe Function, and receive keys from the ProSe Key Management Function (PKMF - see TS 33.303 [57], TS 23.228 [43]). After such a communication, the UE reports the relevant usage information to the ProSe Function. This subclause details the interception at the ProSe Function and ProSe Key Management Function.

NOTE: The present document does not provide a solution for the interception of content of communication.

Editor's note: Interception of ProSe one-to-many communication with the group as the target is FFS.

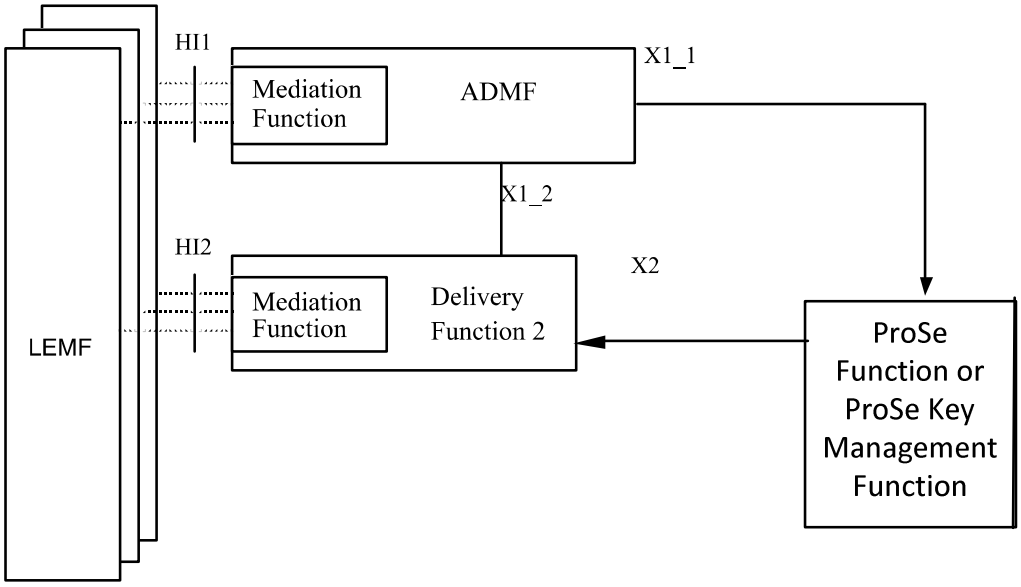


Figure 17.2-1: ProSe One To Many Communications Intercept configuration

Figure 17.2-1 shows the IRI interception configuration for ProSe one to many communications. The HI2 interface represents the interface between the LEMF and the delivery function. The delivery function is used to distribute the

Intercept Related Information (IRI) to the relevant LEMF(s) via HI2. See clause 4 for more information on the ADMF and other interfaces.

The target identity for interception is the IMSI. The activation, deactivation, and interrogation of interception regarding the ProSe Function shall follow the requirements of clause 5.

17.2.2 Provision of Intercept Product - One-To-Many Communications

17.2.2.1 General

Figure 17.2.2.1-1 shows the transfer of IRI relating to the one to many communications from the ProSe Function and ProSe Key Management Function to the DF2 and to the LEMF. If a target UE interacts with the ProSe Function or ProSe Key Management Function relating to one-to-many communications, a One-To-Many IRI event, is generated and sent via the Delivery Function 2 to the LEMF.

If an event involving an target occurs, the ProSe Function or ProSe Key Management Function shall send the relevant data to the DF2 for formatting and delivery to the LEMF.

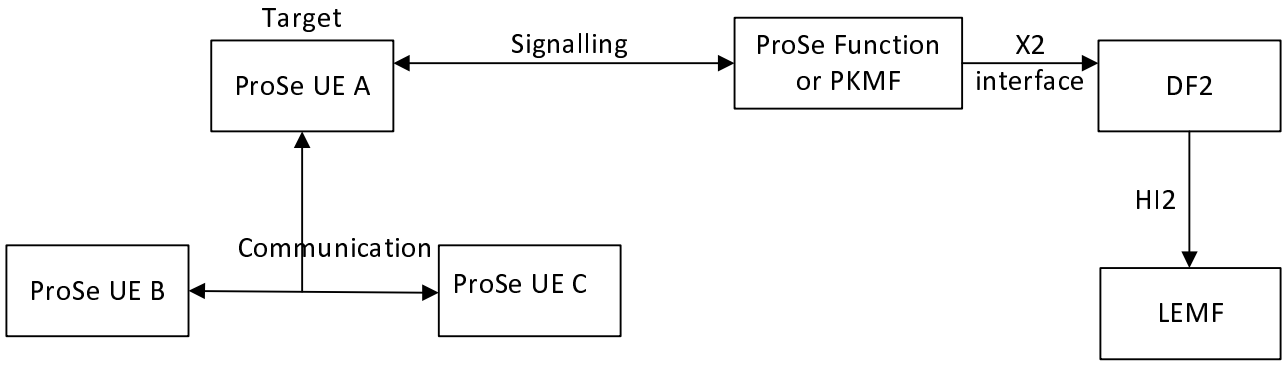


Figure 17.2.2.1-1: Provision of Intercept Product for Public Safety One-To-Many Communications

NOTE: There is signalling between the non-target ProSe UEs and the ProSe Function and PKMF, which is not shown in figure 17.2.2.1-1. This signalling is not relevant to the interception of the target UE.

17.2.2.2 X2-interface

The following information needs to be transferred from the ProSe Function or ProSe Key Management Function to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMSI);
- events and associated parameters, as defined in section 17.2.2.3;
- the target location (if available) or the IAs in case of location dependent interception;
- Quality of Service (QoS) identifier;
- Encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

The IRI should be sent to DF2 using a reliable transport mechanism.

17.2.2.3 ProSe LI One-To-Many Events and Event Information

17.2.2.3.1 Overview of ProSe LI One-To-Many Events

The following event are applicable to the interception of one to many communications:

- ProSe Function sends authorisation to perform one-To-many communications to the target UE.
- ProSe Key Management Function sends keys to use in one-to-may commuications to the target UE.
- ProSe Function receives a one-to-many communications usage information report from the target UE.

Interception of these events is mandatory. .

17.2.2.3.2 Structure of ProSe LI One-To-Many Event Information

A set of possible elements as shown below is used to generate the events.

Table 17.2.2.3.2-1: Information Elements for Event Records relating to one-to-many communications

Element
Observed IMSI IMSI of the target
Event date Date of the event generation.
Event time Time of the event generation. Timestamp shall be generated relative to the intercepting node's internal clock.
PLMN Identity The PLMN that the UE is being authorised to perform one-to-many communication in.
Sender ID Identifies the sender of the One-To-Many Communications - also known as the ProSe UE ID or the Group member identity.
ProSe Layer-2 Group ID Identifies the group of the One-To-Many Communications - also known as the destination ID.
Network Identifier Operator ID plus unique identifier for the element reporting the ICE.
IP address type The type of IP address, i.e IPv4 or IPv6, used for this one-to-many communication.
IP multicast address The IP address to be used when doing one-to-many communication
PKMF address The IP address of the ProSe Key Management Function that will provides keys for this one-to-may communication
Source IP address The IP source address to be used by the UE as a source address
Communication Authorisation Validity timer Indicates in minutes how long the authorisation is valid for
Confidentiality algorithm The confidentiality algorithm used with this group
PGK ProSe Group Key that can be used to protect data for this group
PGK ID The identity of the PGK within this group
PGK lifetime The lifetime of the PGK
Location list List of locations of the UE when in coverage and the corresponding timestamps
E-UTRAN coverage timestamps List of timestamps when the UE goes in/out of E-UTRAN coverage
First communication timestamp Timestamp of the first one-to-may communication transmission/reception
Transmitter identities Identities of the transmitters in the one-to-many communication session
Data transmitted in coverage List of amount of data transmitted by UE when in E-UTRAN coverage at each location, with ECGI and the corresponding timestamps
Data transmitted out of coverage List of amount of data transmitted by UE for each E-UTRAN out of coverage and the corresponding timestamps
Data received in coverage List of amount of data received by UE when in E-UTRAN coverage at each location, with ECGI and the corresponding timestamps
Data received out of coverage List of amount of data received by UE for each out of E-UTRAN coverage period and the corresponding timestamps

17.2.2.3.3 ProSe LI One-To-Many Events

If ProSe Function sends authorisation to use ProSe one-to-many communication to the target UE, a One-To-Many-Auth Event shall be generated. These elements if available will be delivered to the DF2 (see TS 24.333 [58] for more information on the elements):

Table 17.2.2.3.3-1 One-To-Many-Auth Event

Observed IMSI
Event type
Event Time
Event Date
Network Identifier (including network element identifier)
PLMN Identity
Communication Authorisation Validity timer
ProSe Layer-2 Group ID
IP address type
IP multicast address
PKMF address (if applicable)
Source IP address (if applicable)

If a ProSe Key Management Function sends keys for one-to-many communication to a target UE, a One-To-Many-Keys Event shall be generated. These elements if available will be delivered to the DF2 (see TS 33.303 [57] for more information on the elements):

Table 17.2.2.3.3-2 One-To-Many-Keys Event

Observed IMSI
Event type
Event Time
Event Date
Network Identifier (including network element identifier)
ProSe Layer-2 Group ID
Sender ID
Confidentiality algorithm
PGK
PGK ID
PGK lifetime

If a ProSe Function receives a usage information report for ProSe one-to-many communication to a ProSe Function from a target UE, a One-To-Many-Usage Event shall be generated. These elements if available will be delivered to the DF2 (see TS 32.277 [59] for more information on the elements):

Table 17.2.2.3.3-3 One-To-Many-Usage Event

Observed IMSI
Event type
Event Time
Event Date
Network Identifier (including network element identifier)
Location list
E-UTRAN coverage timestamps
Sender ID
ProSe Layer-2 Group ID
IP address type
IP multicast address
Source IP address (if applicable)
First communication timestamp
Transmitter identities
Data transmitted in coverage
Data transmitted out of coverage
Data received in coverage
Data received out of coverage

NOTE: The UE periodically generates usage event reports for charging purposes from which this event is generated. Therefore there may be a significantly delay between the generation of this event and the communications for which the usage report is generated by the UE.

Editor's note: The above table is based on the stage 2 of the PC3ch interface as decribed in TS 32.277 [59]. Some of the above information may need to be changed once the stage 3 for PC3ch is complete.

Editor's note: The application of LI requirements in TS 33.106 [7] to the CTF (TS 32.277 [59]) within the ProSe function when it is physically separated from the ProSe Function is FFS.

17.3 ProSe Remote UE Communications

17.3.1 General

A ProSe Remote UE can initiate communications via a ProSe UE-to-NW Relay and the core network as described in TS 23.303 [52].

From LI perspective, the following scenarios can be identified:

1. The ProSe Remote UE is a target for interception
2. The ProSe UE-to-NW Relay is a target for interception
3. Both the ProSe Remote UE and the ProSe UE-to-NW Relay are target for interception.

NOTE: The ProSe Remote UE and the ProSe UE-to-NW Relay are considered target for interception if any of the identities (MSISDN, IMSI, IMEI) related to the UE or the user is target for interception.

In the following subclauses, scenarios 1 and 2 are addressed, scenario 3 is covered by using both scenario 1 and 2.

Interception in the PDN-GW is a national option.

17.3.2 The ProSe Remote UE is a target for interception

When a ProSe Remote UE connects to the ProSe UE-to-NW Relay, the core network (MME, S-GW, PDN-GW) receives the related information from the ProSe UE-to-NW Relay. If the ProSe Remote UE is a target, a ProSe Remote UE start of communication event shall be generated by the S-GW, PDN-GW.

If the warrant requires to intercept also CC, considering that the PDN connection used by the ProSe UE-to-NW Relay can be used also for other, non-target, ProSe Remote UEs, the S-GW/PDN-GW shall isolate the target ProSe remote UE's communication from any content of communication not associated to the remote UE under interception. CC related to the target ProSe Remote UE shall be sent over X3 interface.

When a target ProSe Remote UE disconnects from the ProSe UE-to-NW Relay, a ProSe Remote UE end of communication event shall be generated by the S-GW, PDN-GW. CC interception for the target ProSe Remote UE shall be stopped.

In both cases of connection and disconnection of a target ProSe Remote UE, the MME shall generate a ProSe Remote UE Report event.

In case the whole PDN connection used by the ProSe UE-to-NW Relay is closed for any reason while a target Remote UE is connected to the ProSe UE-to-NW relay, a ProSe Remote UE end of communication event shall be generated by the S-GW/PDN-GW and sent to the DF2.

If interception is started after that the ProSe remote UE is already connected to the network through a ProSe UE-to-NW Relay, a Start of interception with ProSe Remote UE ongoing communication event shall be provided by the S-GW/PDN-GW. The same event shall also be sent by the new S-GW in case, due to ProSe UE-to-NW Relay mobility, there is a change of S-GW. The ICEs shall than start intercepting the target UEs communication by extracting it from the PDN connection used by the ProSe UE-to-NW Relay UE.

17.3.3 The ProSe UE-to-NW Relay is a target for interception

The ProSe UE-to-NW Relay uses one or more PDN connections for any activity/communication which is not related to relaying. In such case all the requirements specified for EPS interception in clause 12 apply. In addition, IRIs related specified in clause 12 are also applicable to the PDN connection used for relay.

This clause specifies additional functional requirements which are applicable to the PDN connection(s) established by the ProSe UE-to-NW Relay.

PDN connection(s) used for relaying only carry communications for the ProSe remote UEs. So, unless any of them is also a target for interception (for which clause 17.3.2 apply), no content of communication shall be intercepted from such PDN connection(s), unless required by national regulation, in which case all requirements specified in clause 12 apply also to these PDN connection(s).

In case ProSe remote UEs are connected to or disconnected from the target ProSe UE-to-NW Relay, the ICEs (MME, S-GW, PDN-GW) shall provide a ProSe Remote UE Report event, including the identities and IP info of ProSe remote UE(s) being connected/ disconnected.

In case interception is activated for a ProSe UE-to-NW Relay with already connected ProSe remote UE(s), the ICEs shall provide a Start of interception for ProSeUE-to-NW Relay, including the identities and IP info of ProSe remote UEs already connected to the relay. The same event shall also be sent by the new S-GW in case, due to ProSe UE-to-NW Relay mobility, there is a change of S-GW.

In case a Tracking Area/EPS Location Update event is provided for a target ProSe UE-to-NW Relay, it shall carry also information related to the connected ProSe remote UE(s).

17.3.4 X2-interface

The following information needs to be transferred from the EPS nodes (MME, S-GW, PDN-GW) to the DF2 in order to allow a DF2 to perform its functionality:

- target identity (IMSI, MSISDN, IMEI);
- events and associated parameters as defined in clause 17.3.4.1.

17.3.4.1 Structure of the events

There are several different events in which the information is sent to the DF2 if this is required. Details are described in the following clauses. The events for interception are configurable (if they are sent to DF2) in the EPC nodes.

The following event is applicable to the MME:

- ProSe Remote UE Report;

The following events are applicable to the S-GW and PDN-GW:

- ProSe Remote UE start of communication;
- ProSe Remote UE end of communication;
- Start of interception with ProSe Remote UE ongoing communication;
- Start of interception for ProSe UE-to-NW Relay.

A set of possible elements as shown below is used to generate the events.

Table: 17.3.4.1-1: Information Events for ProSe communication Event Records

Element
Observed MSISDN MSISDN of the target
Observed IMSI IMSI of the target
Observed IMEI IMEI of the target
Event type Indicates which type of event is delivered: ProSe Remote UE Report, ProSe Remote UE start of communication, ProSe Remote UE end of communication, Start of interception with ProSe Remote UE ongoing communication, Start of interception for ProSe UE-to-NW Relay.
Event date Date of the event generation in the ICE
Event time Time of the event generation in the ICE. Timestamp shall be generated relative to the ICE internal clock.
Target type Indicates whether the target is a ProSe Remote UE or a ProSe UE-to-NW Relay
ProSe Remote UE IDs The identities of the connected or disconnected ProSe remote UEs.
ProSe Remote UE IP info The IP address(es) of the connected or disconnected ProSe Remote UE(s) provided by the ProSe UE-to-NW Relay.
APN The Access Point Name used by the ProSe UE-to-NW Relay for the connection
MSISDN of the Prose UE-to-NW Relay (only applicable when the ProSe Remote UE is the target)
IMSI of the Prose UE-to-NW Relay (only applicable when the ProSe Remote UE is the target)
IMEI of the Prose UE-to-NW Relay (only applicable when the ProSe Remote UE is the target)
PDN address(es) The ProSe UE-to-NW Relay IP address(es) for the PDN connection.
Network Element Identifier Unique identifier for the element reporting the ICE.
Correlation number The correlation number is used to correlate CC and IRI (in case the target is a ProSe remote UE) or IRIs (in case the target is a ProSe UE-to-NW Relay).
Location information The location of the ProSe UE-to-NW Relay. National regulations may require to provide the E-CGI of the ProSe UE-to-NW Relay when the target is the ProSe Remote UE.

17.3.5 ProSe UE-to-NW Relay events

17.3.5.1 ProSe Remote UE Report

This event shall be sent by the MME, S-GW and PDN-GW when the node detects that a ProSe Remote UE has been connected to or disconnected from the ProSe UE-to-NW Relay and the ProSe Remote UE or the ProSe UE-to-NW Relay is a target for interception. The following parameters shall be provided if available.

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Target type
ProSe Remote UE(s) connected IDs
ProSe Remote UE(s) connected IP info
ProSe Remote UE(s) disconnected IDs
ProSe Remote UE(s) disconnected IP info
MSISDN of the Prose UE-to-NW Relay
IMSI of the Prose UE-to-NW Relay
IMEI of the Prose UE-to-NW Relay
APN
PDN Address(es)
Location information

17.3.5.2 ProSe Remote UE Start of Communication

This event shall be sent by the S-GW and PDN-GW when the node detects that a target ProSe Remote UE has been connected to a ProSe UE-to-NW Relay. The following parameters shall be provided if available.

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation number
MSISDN of the Prose UE-to-NW Relay
IMSI of the Prose UE-to-NW Relay
IMEI of the Prose UE-to-NW Relay
APN
PDN Address(es)
Location information

17.3.5.3 ProSe Remote UE End of Communication

This event shall be sent by the S-GW and PDN-GW when the node detects that a target ProSe Remote UE has been disconnected from a ProSe UE-to-NW Relay. The event shall also be sent in case the PDN connection used for relay used by the target ProSe remote UE is closed. The following parameters shall be provided if available.

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation number
Location information

17.3.5.4 Start of interception with ProSe Remote UE ongoing communication

This event shall be sent by the S-GW and PDN-GW when interception is started for a ProSe Remote UE which is already connected to a ProSe UE-to-NW Relay. The event shall also be sent by the new S-GW in case, due to ProSe UE-to-NW Relay mobility, there is a S-GW change. The following parameters shall be provided if available.

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Correlation number
MSISDN of the Prose UE-to-NW Relay
IMSI of the Prose UE-to-NW Relay
IMEI of the Prose UE-to-NW Relay
APN
PDN Address(es)
Location information

17.3.5.5 Start of interception for ProSe UE-to-NW Relay

This event shall be sent by the S-GW and PDN-GW when interception is started on a UE which is already acting as ProSe UE-to-NW Relay for any Remote UE. The event shall also be sent by the new S-GW in case, due to ProSe UE-to-NW Relay mobility, there is a S-GW change. The following parameters shall be provided if available.

Observed MSISDN
Observed IMSI
Observed IMEI
Event Type
Event Time
Event Date
Network Element Identifier
Target type
ProSe Remote UE(s) connected IDs
ProSe Remote UE(s) connected IP info
APN
PDN Address(es)
Location information

17.3.6 X3-interface

Functional requirements specified in clause 12.3.2 are applicable. Interception of CC is subjected to conditions specified in clauses 17.3.2 and 17.3.3.

18 Invocation of Lawful Interception for messaging services

18.1 Overview of messaging services interception

The capabilities defined in this clause apply when the interception of messaging services shall be separated from the interception of all other services. This clause applies to the messaging services identified in clause 5.13 of TS 33.106 [7].

For messaging services, separated delivery when SMS events are detected, the CSP shall be able to use existing intercept capabilities defined in this specification, but isolatable to only deliver messaging services when specified by a lawful authorisation.

The network nodes, involved in providing the interception of messaging services, shall be determined based on the deployment configuration and the messaging scenario. For SMS over NAS, the MME shall be an ICE.

When lawfully authorized, Law Enforcement requires access to CC and IRI for the events pertaining to the target's authorization, access to, and use of message services, independent of the deployed service architecture. This includes

where the communications between the target and associates are sent and received over separate channels, or may be accessed at different ICEs at different geographical locations in the service provider's network.

For MMS, implementation options considered in this standard are: interception at the MMS level or normal packet session CC interception at an PS/IMS/EPS ICE and transferred to the DF2/DF3 which then subsequently isolates and delivers the MMS IRI and/or CC associated with the messaging service separate from all other services. Details of IRI and CC reporting for MMS events are for further study.

National regulations on a per interception basis may limit delivery of communications (CC and IRI) of an outbound international roaming target by the messaging service as described in clause 5.1.4 of TS 33.106 [7].

If roaming interception is not allowed and it is determined that the target is outside the country, reporting by the HPLMN for messaging services shall be as follows:

- All related messsaging service events defined in this clause are subject to this mechanism with the exception that messaging service events in the HPLMN involving communications to the target that are not transmitted to the target are not subject to this mechanism.

Non-communications-associated IRI (e.g. those identified by the HSS) are not affected by this requirement.

18.2 SMS

18.2.1 Introduction

LI for SMS over a GPRS and UMTS access is specified in clause 7. LI for SMS over IP (using IMS SIP signalling handled by the core network) which can be used in conjunction with LTE access as well as other non-3GPP IP based access is defined in clause 7A.6.

18.2.2 SMS over GPRS/UMTS

For separate delivery of SMS when SMS is used in conjunction with GPRS or UMTS access, the following events shall be reported by the ICE to the DF:

1) SMS (clause 7.4.7)

2) HLR Related events

   a. Serving System (clause 7.4.9)

   b. HLR subscriber record change (clause 7.4.12)

   c. Cancel location (clause 7.4.13);

   d. Register location (clause 7.4.14);

   e. Location information request (clause 7.4.15).

The above events shall be reported from the ICE to the DF independent of any other services that may or may not be intercepted.

18.2.3 SMS over IP

For separate delivery of SMS when SMS over IP (using IMS SIP signalling handled by the core network) is used, the following events shall be reported by the ICE to the DF:

1) Intercepted SIP event as described in clause 7A.3.0

2) HSS related events

   a. Serving System (clause 7A.2.3.1) for use when roaming

   b. IMPU or IMPI changed in a HSS subscriber record change (clause 7A.2.3.2);

   c. Registration termination (clause 7A.2.3.3);

d. Location information request (clause 7A.2.3.4).

The above events shall be able to be reported from the ICE to the DF independent of and to the exclusion of any other services that may or may not be intercepted.

18.2.4 SMS over NAS

18.2.4.0 Introduction

SMS over NAS reporting uses the architecture and interfaces defined in Clause 12 *Lawful Interception for Evolved Packet System.*

18.2.4.1 Structure of the events

SMS over NAS uses the MME as an ICE.

The following events are applicable to the MME:

- SMS over NAS Report (Clause 18.2.4.2)

18.2.4.2 SMS over NAS Events

For separate delivery of SMS when the NAS infrastructure is used, the following events shall be reported from the MME to the DF:

1) SMS over NAS (clause 18.2.4.3)

In addition, the following HSS events shall be reported:

2) HSS Related events

   a. Serving Evolved Packet System (clauses 12.2.3.8, 12.4.3.10, 12.5.3.5)

   b. HSS subscriber record change (clauses 12.2.3.15, 12.3.4.18, 12.5.3.15)

   c. Cancel location (clause 12.2.3.16)

   d. Register Termination (clauses 12.3.3.16, 12.3.4.19)

   e Register location (clauses 12.2.3.17, 12.4.3.20)

   f. Location information request (clauses 12.2.3.18, 12.4.3.20, 12.5.3.17).

The above events shall be reported from the ICE to the DF independent of any other services that may or may not be intercepted.

Table 18.2.4.2. SMS over NAS Information Elements

Observed MSISDN MSISDN of the target.
Observed IMSI IMSI of the target.
Observed IMEI IMEI of the target; when it coincides with the IMEI, it shall be checked for each activation over the radio interface.
Observed Non-Local ID Target Identifier with the E. 164 number of Non-Local ID target.
Event type indicating SMS over NAS.
Event date Date of the event generation in the ICE.
Event time Time of the event generation in the ICE. Timestamp shall be generated relative to ICE internal clock.
Location Information (if available).
Time of Location Date/Time of location. The time when location was obtained by the location source node.
Network Element Identifier Unique identifier for the ICE reporting the event.
SMS The SMS content with SMS header which is sent with the SMS-service. The header also includes the SMS-Centre address.
SMS Initiator SMS indicator whether the SMS is MO or MT or undefined.
IAs The observed Interception Areas.

18.2.4.3 SMS over NAS

For SMS-MO, the event is generated in the MME. Dependent on national requirements, event generation shall occur in the following cases:

- when the MME receives the SMS from the target MS, or when the MME detects that an SMS is to the Non-Local ID target.

- when the SMS that was originated from the target MS, or sent to the Non-Local ID target.

For SMS-MT, the event is generated in the MME. Dependent on national requirements, event generation shall occur in the following cases:

- when the MME receives the SMS originated from a Non-Local ID target, or one that will have to be sent to a target MS.

- when the MME receives notification that recipient MS has received the SMS successfully. The recipient MS is the target MS when the SMS is sent to the target. The recipient MS may not be the target when the SMS was originating from a Non-Local ID target.

Data over NAS for Internet of Things is for further study.

These elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed IMEI
Observed Non-Local ID
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
Time of Location
SMS
SMS Initiator
IAs (if applicable)

18.3 MMS

18.3.1 Background

Clause 7.6 defines an interception solution for MMS over GPRS/UMTS whereby the packet IP stream is sent to the DF and onto to the LEMF for LE to extract the MMS information. However, that solution does not allow for the separate delivery of MMS from other services. In fact, that approach necessitates the interception and delivery of a packet data session which may not be authorized for interception. This clause defines an approach to intercept and deliver only MMS related events and deliver those separate from any other services that may or may not be intercepted.

It is a national option for the CSP and LEA to agree on the maximum size of and MMS to be delivered to the LEMF. If the MMS is bigger than the agreed size it is a national option for what to do (e.g. don't deliver it to the LEMF).

MMS service is defined in TS 22.140 [74], OMA's MMS Architecture OMA-AD-MMS-V1_3-20110913-A [72], and OMA's Multimedia Messaging Service Encapsulation Protocol OMA-TS-MMS_ENC-V1_3-20110913-A [73].

The key network elements involved in the support of MMS is the MMS Proxy-Relay. The MMS Proxy-Relay is responsible for:

1) receiving a MMS from a served UE and forwarding that to the MMS Proxy-Relay of the destination UE,

2) receiving a MMS from an originating MMS Proxy-Relay and forwarding this MMS or a notification of it to its served UE,

3) receiving a request for retrieval of an MMS from a served UE and delivering that MMS to the served UE,

4) providing the served UE with delivery status and read reports of served UE originated MMS

5) providing a MMS/Relay of another UE with delivery status and read reports of MMS received for the served UE.

When a Non-Local Id is used as target identity, the interception shall be performed at the MMS Proxy Relay. For MMS messages originated from a target wth Non-Local ID, the target is identified from FROM field. For MMS messages to the target with Non-Local ID, the target are identified from TO, CC and BCC fields. The interception may be triggered on the value address defined in the clause 8 of MMS addressing model of OMA's Multimedia Messaging Service Encapsulation Protocol OMA-TS-MMS_ENC-V1_3-20110913-A [73].

LI for MMS requires IRI and CC related to the MMS to be detected by the MMS Proxy-Relay and forwarded to the DF.

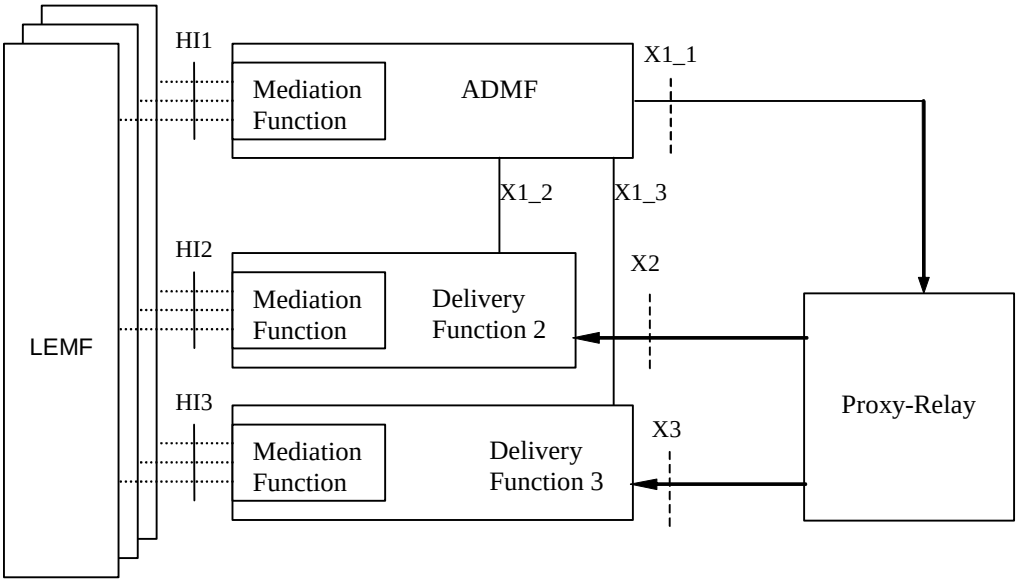


Figure 18.1: MMS Proxy-Relay Intercept configuration

18.3.2 MMS Architecture IRI/CC Events

The MMS architecture is provided in Clause 5 of MMS Architecture [72]. The two interfaces considered in developing the events and event information to be reported are the MMS_M interface (between the MMS client and the MMS Proxy-Relay) and the MMS_R interface (i.e., between two MMS Proxy-Relay nodes).

For separate delivery of MMS, the following events shall be reported by the ICE to the DF:

1) MMS Send
2) MMS Notification & Confirmation
3) MMS Retrieval Confirmation & Acknowledgement
4) MMS Forwarding
5) MMS Store Requests
6) MMS Viewing Requests & Responses
7) MMS Deletion Requests (delete from MMBox and Proxy-Relay)
8) MMS Cancel Requests
9) MMS Delivery Reports
10) MMS Read Report.

The above events shall be reported from the ICE to the DF independent of any other services that may or may not be intercepted.

The following events shall be reported by the HSS:

1) Serving System (clause 7.4.9)
2) Serving Evolved Packet System (clauses 12.2.3.8, 12.4.3.10, 12.5.3.5).

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from the nodes to DF2. Available IEs from this set of elements as shown below can be extended in the nodes, if this is necessary as a national option. DF2 can extend available information if this is necessary as a national option. Where MMS CC is available during an event, in addition to the IRI event reported to DF2, an MMS CC event is reported to DF3.

Table 18.3.2-1 Table of MMS Information Elements

Observed MSISDN MSISDN of the target.
Observed IMSI IMSI of the target.
Observed MMS Address An address in a format as specified in [73]. This is where a SIP URI would be included.
Observed MMS Address for Non-Local ID An address in a format as specified in [73] that will be intercepted as Non-Local ID target.
Observed IPv4/IPv6 Address An IPv4 or IPv6 address of the target.
Observed shortcode An address in a format as specified in [73].
Event type Indicates which type of event is delivered: MMS Send, MMS Notification, MMS Notification Response, MMS Retrieval, MMS Retrieval Acknowledgement, MMS Forwarding, MMS Store, MMS Upload, MMS Delete from MMBox, MMS Delete from Proxy-Relay, MMS MMBox View, MMS Delivery, MMS Read Reply, MMS Cancel, MMS Cancel Confirm, MMS MMBox View Request, MMS MMBox View Confirm, Serving System, Serving Evolved System.
Event time Time of the event generation in the ICE. Time stamp shall be generated relative to ICE internal clock.
Event date Date of the event generation in the ICE.
Network Element Identifier Unique identifier for the ICE (MMS Relay/Proxy) reporting the event.
To Recipient(s) address(es) Address of a recipient; the "To" field may include addresses of multiple recipients. When address translation occurs, both the pre and post translated addresses (with appropriate correlation) are included.
CC Recipient(s) address(es) Address of a recipient; the "CC" field may include addresses of multiple recipients. When address translation occurs, both the pre and post translated addresses (with appropriate correlation) are included.
BCC Recipient(s) address(es) Address of a recipient; the "BCC" field may include addresses of multiple recipients. When address translation occurs, both the pre and post translated addresses (with appropriate correlation) are included.
From address Address of the sender of the MM or read reply. The sender may be the originator or a forwarding user. When address translation occurs (in the case of a token sent by the client and replaced with a proper address by the MMS Proxy/Relay), both the pre and post translated addresses (with appropriate correlation) are included.
MMS Version The version of MMS used by the target.
Transaction ID An ID used to correlate an MMS request and response between the target and the MMS Proxy-Relay.
Message ID An ID assigned by the MMS Proxy-Relay to uniquely identify an MMS message.
Message Reference A reference, e.g., URI, for the MM which refers to the stored MM within the MMS Proxy-Relay or the MMBox.
Stored Message Reference A reference, e.g., URI, for the MM which refers to the newly stored MM within the MMS Proxy-Relay or the MMBox.
MMS Date/Time Date and Time when the MM was last handled (either originated or forwarded). For origination, included by the sending MMS client or the originating MMS Proxy-Relay.
Subject Subject of the MM.
Message Class Class of the MM. For example, a value of "auto" is automatically generated by the UE. If the field is not present, the class should be interpreted as "personal".
Expiry Length of time the MM will be stored in MMS Proxy- Relay or time to delete the MM. The field has two formats, either absolute or relative.
Desired Delivery Time Date and Time of desired delivery. Indicates the earliest possible delivery of the MM to the recipient.
Priority Priority of the MM assigned by the originator MMS UE.
Sender Visibility An indication that the sender's address should not be delivered to the recipient.
Delivery Report Specifies whether the originator MMS UE requests a delivery report from each recipient.
Read Report Specifies whether the originator MMS UE requests a read report from each recipient.

Store Specifies whether the originator MMS UE wants the submitted MM to be saved in the user's MMBox, in addition to sending it.
Applic-ID Identification of the originating application of the original MM.
Reply-Applic-ID Identification of the destination application of the original MM.
Aux-Applic-Info Auxiliary application addressing information as indicated in the original MM.
Content Class Classifies the content of the MM to the smallest content class to which the message belongs.
DRM Content Indicates if the MM contains any DRM-protected element.
Adaptation Allowed Indicates if the originator wishes the MM to be adapted or not. This wish can be overridden by DRM protection rules or MMS service provider / network operator configuration.
Content Type The content type of the MM.
Previously Sent By Address of the MMS Client that forwarded or originally sent the message and a sequence number. A higher sequence number indicates a forwarding event at a later point in time. This header field MAY appear multiple times.
Previously Sent by Date/Time Date and time of a forwarding or original send transaction of the message and a sequence number. The sequence number indicates the correspondence to the MMS Client's address in the "X-Mms-Previously- Sent-By" header field with the same sequence number. This header field MAY appear multiple times.
MM State Identifies the value of the MM State associated with a to be stored or stored MM.
MM Flags Identifies a keyword to add or remove from the list of keywords associated with a stored MM.
Content Location This field defines the location of the content to be retrieved.
Response Status MMS specific status.
Response Status Text Text that qualifies the Response Status.
Store Status Indicates if the MM was successfully stored in the MMBox.
Store Status Text Text that qualifies the Store Status.
Message Size Identifies the size of the MM.
Distribution Indicator Identifies whether the originator (e.g., a Value Added Service Provider) allows the MM to be further distributed. A "No" value indicates to the user that the originator requested the content of the MM is not supposed to be distributed further.
Element Descriptor Contains the Content-Reference associated with the corresponding top level message content of the MM waiting for retrieval and MAY additionally contain the type/format of the message content.
Retrieval Mode Indicates whether manual retrieval mode is recommended for the MM.
Retrieval Mode Text Explains why manual retrieval mode is recommended for the MM.
Retrieve Status MMS specific status.
Retrieve Status Text Text that qualifies the Retrieve Status.
Replace ID This field indicates the reference (i.e. Message-ID) of the previous MM that is replaced by the current MM.
MMS Status Provides a MMS status. A status of "retrieved" is only signalled by the retrieving UE after retrieval of the MM.
MMS Status Text Text that qualifies the MMS Status.
Report Allowed Indication whether or not the sending of delivery report is allowed by the recipient MMS Client.
MMS Forward Req Date/Time Date and Time that the MM was requested to be forwarded.

Read Status Status of the MM regarding whether it was read or not, e.g. Read, Deleted without being read.
Read Status text Text explanation corresponding to the Read Status.
Cancel ID This field includes the Message ID identifying the message to be cancelled.
Cancel Status Provides the status of the cancel request.
MMS Start A number, indicating the index of the first MM of those selected to have information returned in the response.
MMS Limit A number indicating the maximum number of selected MMs whose information are to be returned in the response. If this is absent, information elements from all remaining MMs are to be returned. If this is zero then no MM-related information are to be returned.
MMS Attributes A list of information elements that should appear in the view for each selected message.
MMS Totals Indicates a request for or the actual count of messages currently stored in the MMBox.
MMS Quotas Indicates a request for or the actual quotas for the user's MMBox in messages or bytes.
MMS Message Count Identifies the number of messages in the content part of the PDU.
Correlation ID Provides a mechanism to correlate IRI for MMS with CC for MMS based on a single MMS event.
MMS Content The actual contents of the MM that is carried in the payload field of MMS messages.

Most of the parameters contained in Table 18.3.2-1 can be mapped to specific parameters defined in [73].

Editor's Note: Specific mapping for the parameters of Table 18.3.2-1 should be added in an update to the present document.

Clause 8 of [73] defines procedures for address translation for MMS and it is those procedures that are referenced whenever Clause 18.3 of the present document refers to address translation.

18.3.3 MMS Events

18.3.3.1 MMS Send

The MMS Send event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a M-Send.conf (as defined in [73]) to the target. According to [73], the Proxy-Relay sends a M-Send.conf to the target in response to a M-Send.req (as defined in [73]) received from the target for sending an MM to one or more destination party(ies).

The elements of Table 18.3.3.1 will be delivered to the DF2, if available.

Table 18.3.3.1: Information Elements for MMS Send Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
To Recipient(s) address(es) (untranslated and translated)
CC Recipient(s) address(es) (untranslated and translated)
BCC Recipient(s) address(es) (untranslated and translated)
From address (includes both target provided address and if translation occurs, network substituted post-translation address.
MMS Version
Transaction ID
Message ID
MMS Date/Time
Message Class
Expiry
Desired Delivery Time
Priority
Sender Visibility
Delivery Report
Read Report
Store
Applic ID
Reply Applic ID
Content Class
DRM Content
Adaptation Allowed
Content Type
Content Location (from M-Send.conf)
Response Status (from M-Send.conf)
Response Status Text (from M-Send.conf)
Store Status (from M-Send.conf)
Store Status Text (from M-Send.conf)
Correlation (only if MMS CC is also intercepted)

When the MMS Send event is generated and interception of CC is required, the MMS Send CC event is also generated. In this case, the elements of Table 18.3.3.2 will be delivered to the DF3, if available.

Table 18.3.3.2: Information Elements for MMS Send CC Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Correlation ID
Subject
MMS Content

18.3.3.2 MMS Notification & Response

The MMS Notification report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a MMS Notification (M-Notification.ind as defined in [73]) to the target indicating the arrival of an MMS for the target.

The elements of Table 18.3.3.3 will be delivered to the DF2, if available.

Table 18.3.3.3: Information Elements for MMS Notification Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
To Recipient(s) addresses
CC Recipient(s) addresses
BCC Recipient(s) addresses
From address (included regardless of anonymity)
MMS Version
Transaction ID
Message ID
MMS Date/Time (Timestamp when this MMS was last handled [either originated or forwarded])
Previously Sent By
Previously Sent By Date/Time (May appear multiple times)
MM State
Message Class
Priority
Message Size
Expiry
Distribution Indicator
Element Descriptor
Retrieval Mode
Retrieval Mode Text
Sender Visibility
Delivery Report
Applic ID
Reply Applic ID
Aux Applic Info
DRM Content
Replace ID
Content Location
Correlation ID (only if MMS CC is to be delivered)

The MMS Notification Response report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay receives a MMS Notification Response (M-NotifyResp.ind as defined in [73]) from the target acknowledging the MMS Notification.

The elements of Table 18.3.3.4 will be delivered to the DF2, if available.

Table 18.3.3.4: Information Elements for MMS Notification Response Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Transaction ID
Message ID
MMS Status
Report Allowed

18.3.3.3 MMS Retrieval & Acknowledgement

The MMS Retrieval report event is generated at the MMS Proxy-Relay when the MMS Proxy-Relay sends a Retrieve.conf PDU (as defined in [73]) to the target. According to [73], the MMS Proxy-Relay sends a Retrieve.conf PDU to the target in response to a MMS retrieval request from the target.

The elements of Table 18.3.3.5 will be delivered to the DF2, if available.

Table 18.3.3.5: Information Elements for MMS Retrieval Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
To Recipient(s) addresses
CC Recipient(s) addresses
BCC Recipient(s) addresses
From address (included regardless of anonymity)
MMS Version
Transaction ID
Message ID
MMS Date/Time (Timestamp when this MMS was last handled [either originated or forwarded])
Previously Sent By
Previously Sent By Date/Time (May appear multiple times)
MM State
Message Class
Priority
Sender Visibility
Delivery Report
Read Report
Retrieve Status
Retrieve Status Text
Distribution Indicator
Applic ID
Reply Applic ID
Aux Applic Info
Content Class
DRM Content
Replace ID
Correlation ID (only if MMS CC is also intercepted)

When the MMS Retrieval event is generated and CC interception is required, the MMS Retrieval CC event shall also be generated. In this case, the elements of Table 18.3.3.6 will be delivered to the DF3, if available.

Table 18.3.3.6: Information Elements for MMS Retrieval CC Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Subject
Correlation ID
MMS Content

The MMS Retrieval Acknowledgement report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay receives a MMS Retrieval Acknowledgement (M-Acknowledge.ind as defined in [73]) from the target acknowledging the transaction to the MMS Proxy-Relay.

The elements of Table 18.3.3.7 will be delivered to the DF2, if available.

Table 18.3.3.7: Information Elements for MMS Retrieval Acknowledgement Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Transaction ID
Message ID
Report Allowed

18.3.3.4 MMS Forwarding

The MMS Forwarding report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a M-Forward.conf (as defined in [73]) to the target. According to [73], the MMS Proxy-Relay sends a M-Forward.conf (as defined in [73]) to the target is response to a received a MMS Forwarding Request (M-Forward.ind as defined in [73]) from the target.

The elements of Table 18.3.3.8 will be delivered to the DF2, if available.

Table 18.3.3.8: Information Elements for MMS Forwarding Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
To Recipient(s) address(es) (untranslated and translated)
CC Recipient(s) address(es) (untranslated and translated)
BCC Recipient(s) address(es) (untranslated and translated)
From address (includes both target provided address and if translation occurs, network substituted post-translation target address.
MMS Version
Transaction ID
Message ID
MMS Forward Req Date/Time
Message Class
Expiry
Desired Delivery Time
Priority
Sender Visibility
Delivery Report Allowed
Delivery Report
Read Report
Store
MM State
Content Location
Response Status (from M-Forward.conf)
Response Status Text (from M-Forward.conf)
Store Status (from M-Forward.conf)
Store Status Text (from M-Forward.conf)

18.3.3.5 MMS Store

The MMS Store report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a M-Mmbox-Store.conf (defined in [73]) to the target. According to [73], the Proxy-Relay sends a M-Mmbox-Store.conf) to the target in response to a received MMS Store Request (M-Mmbox-Store.req as defined in [73]) from the target for a MM that has not been retrieved yet.

The elements of Table 18.3.3.9 will be delivered to the DF2, if available.

Table 18.3.3.9: Information Elements for MMS Store Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
Transaction ID
MMS Version
Content Location
MM State
MM Flags
Store Status
Store Status Text

18.3.3.6 MMS Upload

The MMS Upload report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a M-Mmbox-Upload.conf (defined in [73]) to the target. According to [73], the MSM Proxy-Relay sends a M-Mmbox-Upload.conf to the target in response to a received MMS Upload Request (M-Mmbox-Upload.req as (defined in [73]) from the target.

The elements of Table 18.3.3.10 will be delivered to the DF2, if available.

Table 18.3.3.10: Information Elements for MMS Upload Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
Transaction ID
MMS Version
MM State
MM Flags
Content Type
MM Description PDU (see Table 18.3.3.19)
Content Location (from M-Mmbox-Upload.conf)
Store Status (from M-Mmbox-Upload.conf)
Store Status Text (from M-Mmbox-Upload.conf)
Correlation ID (only if MMS CC is also intercepted)

When the MMS Upload event is generated and CC interception is also required, an MMS Upload CC event is also generated at the MMS Proxy-Relay. In this case, the elements of Table 18.3.3.11 will be delivered to the DF3, if available.

Table 18.3.3.11: Information Elements for MMS Upload CC Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Correlation ID
MMS Content

18.3.3.7 MMS Delete (Stored in MMBox or in Proxy-Relay)

The MMS Delete event is generated at the MMS Proxy-Relay when the MMS Proxy-Relay sends a M-Mmbox-Delete.conf (defined in [73]) to the target. According to [73], the MMS Proxy-Relay sends a M-Mmbox-Delete.conf to the target in response to a received a MMS Delete Request (M-Mmbox-Delete.req as defined in [73]) from the target to delete an MM from the target's MMBox.

The elements of Table 18.3.3.12 will be delivered to the DF2, if available.

Table 18.3.3.12: Information Elements for MMS Delete Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
Transaction ID
MMS Version
Content Location
Response Status
Response Status Text

18.3.3.8 MMS Delivery

The MMS Delivery report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a MMS Delivery Notification (M-Delivery.ind as defined in [73]) to the target.

The elements of Table 18.3.3.13 will be delivered to the DF2, if available.

Table 18.3.3.13: Information Elements for MMS Delivery Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
To Recipient address
Handled Date/Time
Message ID
MMS Status
MMS Status text
Applic-ID
Reply-Applic-ID
Aux-Applic-Info

18.3.3.9 MMS Read Reply

The MMS Read Reply-From-Target report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay receives a MMS Read Reply Notification (M-Read-Rec.ind as defined in [73]) from the target. The elements of Table 18.3.3.14 will be delivered to the DF2, if available.

The MMS Read Reply-To-Target report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a MMS Read Reply Notification (M-Read-Orig.ind as defined in [73]) to the target. The elements of Table 18.3.3.15 will be delivered to the DF2, if available.

Table 18.3.3.14: Information Elements for MMS Read Reply from Target Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
To (MMS sender's address)
From address (includes both target provided address and if translation occurs, network substituted post-translation target address).
Message ID
Read Status
Applic-ID
Reply-Applic-ID
Aux-Applic-Info

Table 18.3.3.15: Information Elements for MMS Read Reply to Target Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
To (target's address)
From address (address of read reply source).
Message ID
Read Status
Read Status text
Applic-ID
Reply-Applic-ID
Aux-Applic-Info

18.3.3.10 MMS Cancel

The MMS Cancel report event is generated at the MMS Proxy-Relay, when the MMS Proxy-Relay sends a MMS Cancel Request (M-Cancel.req as defined in [73]) to the target.

The elements of Table 18.3.3.16 will be delivered to the DF2, if available.

Table 18.3.3.16: Information Elements for MMS Cancel Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Cancel ID (includes the Message ID identifying the message to be cancelled)
Cancel Status

18.3.3.12 MMS MMBox Viewing

The MMS MMBox View Request event is generated at the MMS Proxy-Relay when the MMS Proxy-Relay receives a MMS MMBox Viewing Request (M-Mbox-View.req as defined in [73]) from the target. In this case, the elements of Table 18.3.3.17 will be delivered to the DF2, if available.

The MMS MMBox View Confirm event is generated at the MMS Proxy-Relay when the MMS Proxy-Relay sends a M-Mbox-View.conf (defined in [73]). In this case, the elements of Table 18.3.3.18 will be delivered to the DF2, if available.

Table 18.3.3.17: Information Elements for MMS MMbox View Request Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Transaction ID
MM State
MM Flags
Content Location
MMS Start
MMS Limit
MMS Attributes
MMS Totals
MMS Quotas

Table 18.3.3.18: Information Elements for MMS MMbox View Confirm Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Transaction ID
MM State
MM Flags
Content Location
MMS Start
MMS Limit
MMS Attributes
MMS Totals
MMS Quotas
Response Status
Response Status Text
MMS Message Count
Content Type
Correlation ID (only if MMS CC is also intercepted)
MMBox Description PDU (see Table 18.3.3.19)

Table 18.3.3.19: MM Description PDU

Correlation ID
To Recipient(s) addresses
CC Recipient(s) addresses
BCC Recipient(s) addresses
From address (included regardless of anonymity)
Message ID
MMS Date/Time
Previously Sent By (May appear multiple times)
Previously Sent By Date/Time (May appear multiple times)
MM State
MM Flags
Message Class
Priority
Delivery Time
Expiry
Sender Visibility
Delivery Report
Read Report
Message Size
Content Location
Content Type

When the MMS MMBox View Confirm event is generated at the MMS Proxy-Relay and CC interception is also required, the MMS Proxy-Relay also generates a MMS MMBox View Confirm CC event. In this case, the elements of Table 18.3.3.20 will be delivered to the DF3, if available.

Table 18.3.3.20: Information Elements for MMS MMbox View Confirm CC Event

Observed MSISDN
Observed IMSI
Observed IMEI
Observed MMS Address
Observed IPv4/IPv6 Address
Event Type
Event Time
Event Date
Network Element Identifier
MMS Version
Correlation ID
MMS Content

19 Lawful Access Location Services (LALS)

19.1 General

LALS provides lawful access to the target's location using the Location Services (LCS) capabilities defined in the TS 23.271 [68] and OMA MLP TS [76]. The present clause details the stage 2 Lawful Interception architecture and functions that are needed to provide the LCS information to the DF2 for a target of interception for subsequent delivery to the LEMF. Commercial LCS shall meet Clause 8 security requirements and provide priority to Lawful interception requests.

NOTE 1: For inbound roamers, if the VPLMN LCS Server/GMLC queries HSS/HLR in the HPLMN, this may cause detectability issues. Similarly for outbound roamers, sending location requests to the VPLMN may cause detectability issues.

For LALS the subscriber location privacy settings shall be overridden.

Depending on national requirements and LCS capabilities of the network operator, the location information provided by LALS may vary in location information types (mobile network location format, location shape and geo-coordinates,

civic address, or a combination of those), in the set of additional location parameters (map data, motion state, speed, etc.), as well as in the accuracy of provided location information.

NOTE 2: The accuracy of positioning for any particular technology is a trade-off for the location acquisition delay. It also depends on other technology specific factors.

The parameters controlling the LALS output are either delivered per authorization over HI1/X1 interface or pre-configured in the LI-LCS client.

There are two types of the location interception defined in the present specification: the Target Positioning and the Enhanced Location for IRI.

The Target Positioning is used to determine the target's location independently of the services used by the target.

The Enhanced Location for IRI is used to determine the LCS-based location of the target when specific user service events related to the target occur.

The authorizations for Target Positioning and for Enhanced Location for the same target may be independent of each other and may be overlapping in time or combined in a single intercept authorization by LEA.

There may be multiple active LALS authorizations from different LEAs at any given time.

19.2 Target Positioning

19.2.1 General

There are two Target Positioning provision variants supported in the current specification - the Immediate Location and the Periodic Location.

Figure 19.2.1 shows the architecture for the LALS where the LI LCS Client provides the target's location and associated information towards the DF2 over the X2 interface fulfilling the Target Positioning ADMF authorization delivered over X1_1 interface.

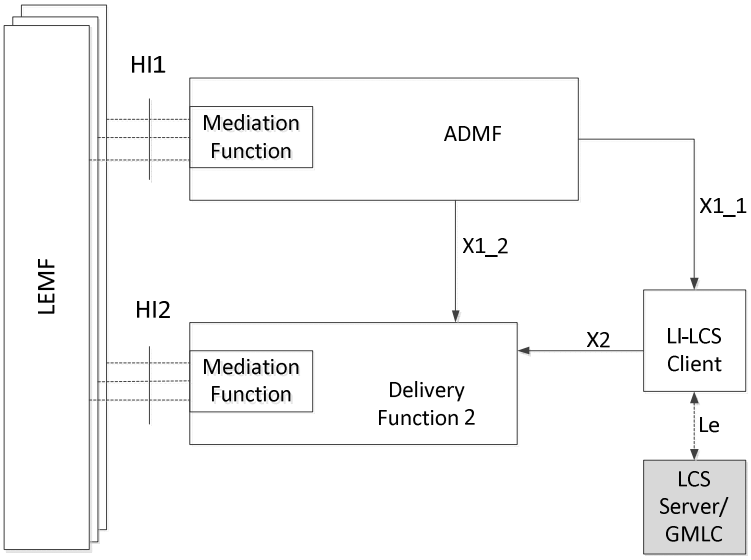


Figure 19.2.1: LALS Model for Target Positioning

19.2.1 Immediate Location Provision

The authorization for Immediate Location provision is delivered to LI LCS Client over X1_1 interface. Upon receiving the authorization the LI LCS Client initiates a Location Immediate Request (LIR, see TS 23.271 [68]) with the LCS Server/GMLC over Le interface and reports the acquired location to the DF2 over X2.

During the period of active authorization for Immediate Location the LI LCS client may receive and process additional Immediate Location requests from AMDF over the X1_1.

NOTE: The LCS Server/GMLC may be optimized to provide the same single location estimation in response to multiple positioning requests arriving in temporal proximity of each other.

The resulting Immediate Location intercept product is delivered over X2 to the DF2 and propagated to the LEMF over HI2.

19.2.2 Periodic Location Provision

The authorization for Periodic Location provision is delivered to LI LCS Client over X1_1 interface.

During the Periodic Location authorization the LI LCS Client shall produce the LALS Reports with the specified periodicity.

The periodicity shall be controlled by the LI LCS Client. The LI LCS Client shall issue a series of Location Immediate Requests (LIR, see TS 23.271 [68]) at required time intervals.

The LI LCS Client provides the acquired location reports to the DF2 over X2.

The Request for Periodic Location from ADMF to LI LCS Client may be accompanied by a set of parameters defining the time interval for reporting, report periodicity, etc. The description of the service response parameters is provided in clause 19.4. The Periodic Location intercept product is delivered over X2 to the DF2 and propagated to LEMF over HI2.

19.3 Enhanced Location for IRI

19.3.1 General

The Enhanced Location for IRI refers to a capability providing LCS-based location information when specific user service events related to the target of interception occur. An example of such service events are the events of IMS session initiation and termination.

Figure 19.3.1-1 depicts the architecture of Enhanced Location acquisition and delivery for the case when the LTF is associated with an IRI ICE.

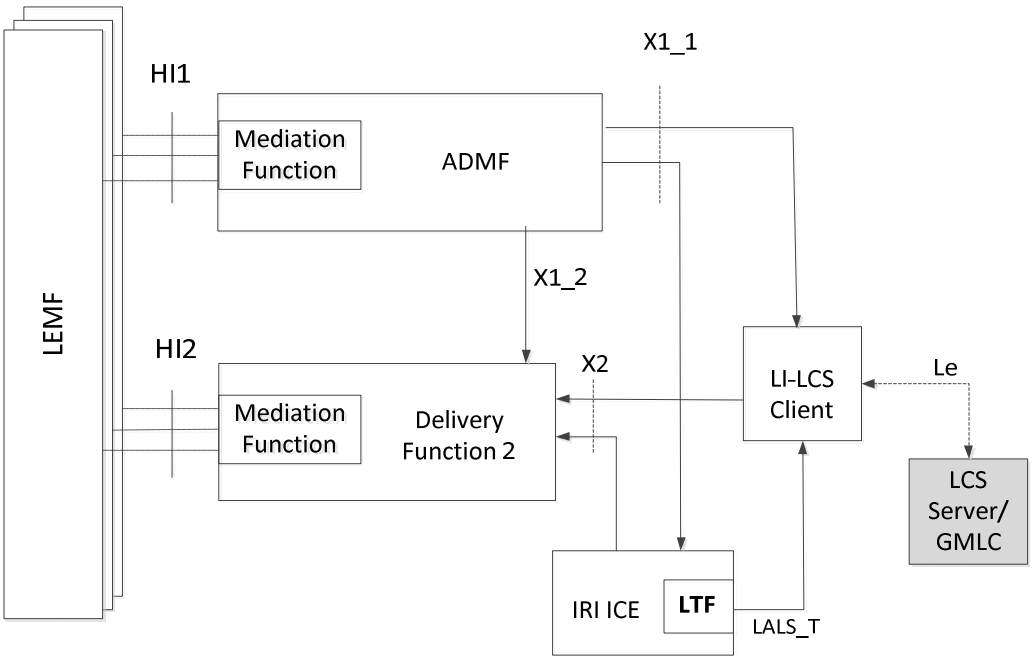


Figure 19.3.1-1: LALS Model for Enhanced Location for IRI (ICE/LTF option)

Figure 19.3.1-2 depicts the architecture of Enhanced Location acquisition and delivery for the case when the LTF is associated with a DF2.

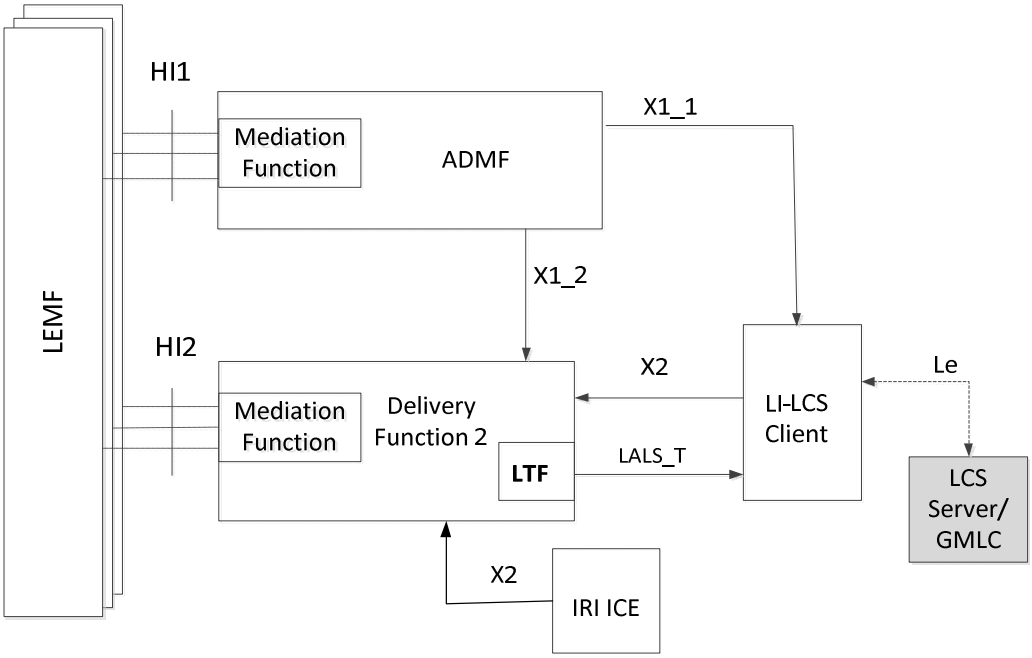


Figure 19.3.1-2: LALS Model for Enhanced Location for IRI (DF/LTF option)

19.3.2 LALS Triggering Function

The LALS Enhanced Location architecture in Figures 19.3.1-1 and 19.3.1-2 depicts the LALS Triggering Function (LTF). LTF is associated with an IRI ICE or with a DF2/MF and is responsible for triggering the LI LCS Client when a specific event related to the target is observed at the IRI ICE, or received at the DF2.

The request for Enhanced Location reporting for IRI is delivered from ADMF to either an ICE over X1_1 or to a DF2 over X1_2 interface along with other parameters of IRI intercept authorization/activation. The ICE(s) or the DF2 then arm the LTF(s).

The ICE nodes that may have an associated LTF include P/S-CSCF, IMS AS, HLR, HSS, MSC Server, MME, S/GGSN, P/S-GW.

The LTF triggers the LI LCS Client over the LALS_T interface.

The LALS intercept product is delivered to DF2 from the LI LCS client over X2 interface asynchronously with the associated IRI event reports generated by an IRI ICE. To enable correlation between the LALS Reports and the associated IRI Events the LTF shall include the Correlation Identifier from the IRI Event, if available, into the LALS_T trigger.

NOTE 1: The IRI events may contain the location information obtained by other means, e.g. NPLI. The LALS reports are augmenting that information with extra details and accuracy.

The LALS_T interface for the LALS intercept trigger shall adhere to the security requirements outlined in Clause 8.

NOTE 2: Detailed definition of the LALS_T interface is out of scope of the current specification.

19.4 X2-interface for Target Positioning and Enhanced Location

19.4.1 General

The following information needs to be transferred from the LI LCS Client to the DF2 in order to allow a DF2 to perform its functionality:

- target identity;
- other target identities, if available;
- event date/time;

- target location and extended location parameters, if available;
- date/time of Location (if target location provided);
- correlation information (in case of Extended Location for IRI reporting);
- error code, if the positioning fails.

19.4.2 LALS Information Elements

A set of possible elements as shown in Table 19.4.2-1 are used to generate the reports.

Table 19.4.2-1: Information Elements for LALS Records

Element
Observed IMSI IMSI of the target.
Observed Other Identities Other Identities of the target (MSISDN, IMEI, SIP-URI, TEL-URI)
Event date Date of the report generation by the LI LCS Client
Event time Time of the report generation by the LI LCS Client
Network Element Identifier Unique identifier of the LI LCS Client
Location Information Geographical Location and/or Civic Location
Time of Location Date/Time of location. The time when location was obtained by the location source node.
Extended Location Parameters Additional location information and associated QoS information
Correlation Identifier Correlation information to allow the DF2 and/or LEMF to correlate LALS events with the triggering IRI events for the Enhanced Location for IRI
Additional location information and associated QoS information

19.4.3 Structure of LALS Records

19.4.3.1 Target Positioning Reporting

This record will be generated when a response to the LIR (Location Immediate Request) is received from LCS for either Immediate or Periodic Target Positioning service.

If the target cannot be located, i.e. no response is received from the LCS in a predefined period or the LCS indicates failure to position the target, the record will contain an error code instead of the location information.

NOTE 1: Void

The information elements shown in Table 19.4.3.1-1, if available, will be delivered to the DF2 by the LI LCS Client.

Table 19.4.3.1-1: Target Positioning Report

Observed IMSI
Observed Other Identities
Event Time
Event Date
Network Element Identifier
Location Information
Time of Location
Extended Location Parameters
Location Error Code

NOTE 2: Each target may have multiple active Periodic Location authorizations with different periodicity settings.

19.4.3.2 Triggered Location Reporting

This record is generated when an LCS response to LI LCS request triggered by an IRI ICE is received (for Enhanced Location for IRI service). The elements, shown in Table 19.4.3.2-1 will be delivered to the DF2, if available. This record contains a Correlation Identifier parameter allowing to correlate the Location Reports with the corresponding IRI events.

If the target cannot be located, i.e. no response is received from the LCS in a predefined period after the triggering or the LCS server indicates failure to position the target, the record will contain an error code instead of the location information.

Table 19.4.3.2-1: Triggered Location

Observed IMSI
Observed Other Identities
Event Time
Event Date
Network Element Identifier
Location Information
Time of Location
Extended Location Parameters
Correlation Identifier

20 Lawful interception in the VPLMN with S8HR Roaming Architecture

20.1 Architecture

20.1.1 Overview

When S8HR approach is used as the roaming architecture for VoLTE, all of the IMS nodes reside in the HPLMN. National regulations may require the VPLMN to have the capabilities to perform the lawful interception of voice services involving the inbound roaming targets. The LI capabilities provided in the VPLMN with S8HR approach as the roaming architecture shall be to the same extent as the LI capabilities provided in the VPLMN with LBO approach as the roaming architecture.

The IMS signalling messages are exchanged between the UE and the P-CSCF (in HPLMN with S8HR) and the media is exchanged between the UE and the PDN-GW (in HPLMN with S8HR). Within the VPLMN with S8HR, the IMS signalling messages are carried over the GTP tunnel that corresponds to the IMS Signalling Bearer and the media packets are carried over the GTP tunnel that corresponds to the Media Bearer. (i.e. a dedicated EPS Bearer used to carry the media packets). The present document assumes that the EPS Bearer ID of the IMS Signalling Bearer is always linked to the dedicated EPS Bearer used as a Media Bearer.

New LI-specific functions are introduced to examine the packets that flow through the VPLMN packet core network nodes (i.e. S-GW) to generate IRI and CC when the communication involves an inbound roaming target. The LI architecture diagram shown in figure 1j is redrawn below with focus on the new LI specific functions and the reference points.

NOTE: The overall architecture and functions related to the lawful interception of voice services of inbound roaming targets with S8HR as the roaming architecture is also referred in the present document as S8HR LI.

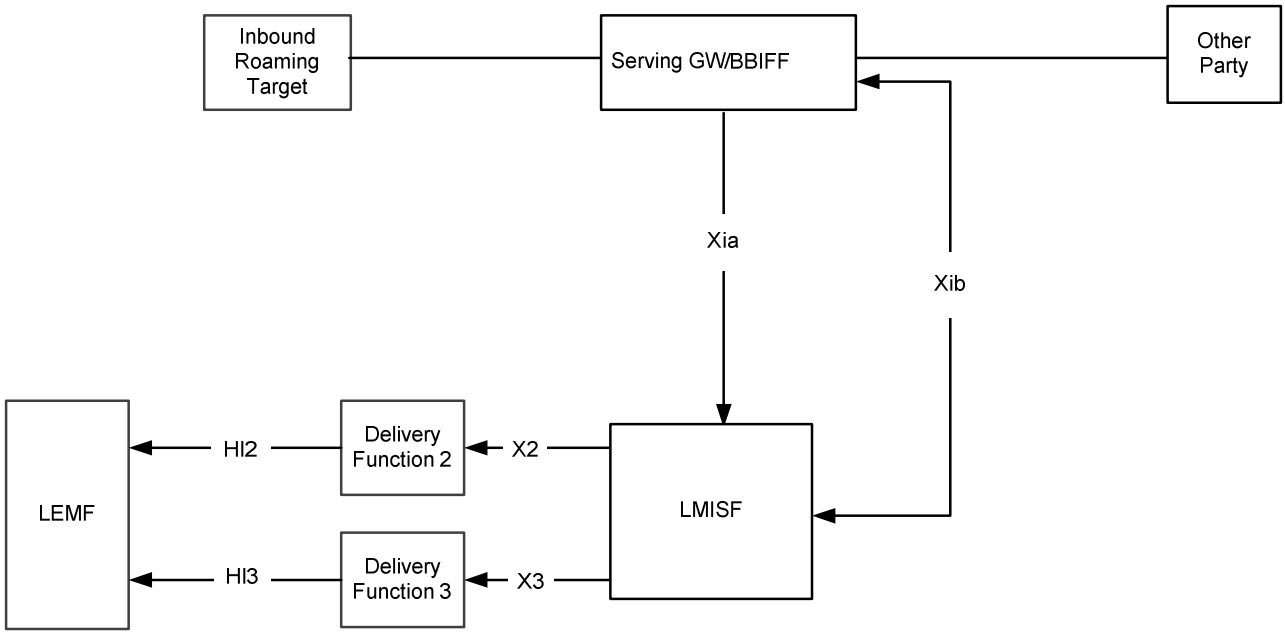


Figure 20.1 S8HR LI Architecture

All the functions and reference points shown in figure 20.1 shall adhere to the security requirements specified in clause 8.

A condition required for the operation of S8HR LI is that the IMS signalling messages and the media packets are not encrypted at S-GW/BBIFF. Furthermore, the S8HR LI solution requires that APNs can be identified as being used for S8HR and therefore those APNs can be used to identify the EPS Bearers used for inbound roamers with S8HR.

Refer to Annex J for the detailed illustration of this architecture in reference to S8HR, the process flow steps and the call flows.

20.1.2 LI specific Reference Points

Xia: Reference point between S-GW/BBIFF and LMISF. This reference point is used to carry the user plane information from the S-GW/BBIFF to the LMISF.

Xib: Reference point between LMISF and the S-GW/BBIFF. This reference point is used to exchange the control plane information between the LMISF and the S-GW/BBIFF.

20.1.3 LI Specific Functions

20.1.3.1 Void

20.1.3.2 BBIFF: Bearer Binding Intercept and Forward Function

BBIFF is a LI specific function introduced to support the lawful interception of voice services in the VPLMN when S8HR is used as the roaming architecture.

BBIFF shall provide the following functions:

- Receive a list of S8HR APNs and the packet forwarding rules that apply to all users from the LMISF over the Xib reference point.
- As per the LMISF instruction, notify the LMISF over Xib reference point whenever the IMS Signalling Bearer or the Media Bearer with S8HR APN is created, modified or deleted. In that notification, the UE location information received from the MME shall be included.
- As per the packet forwarding rules (i.e. as instructed by the LMISF), deliver the packets of all GTP tunnels used for IMS Signalling Bearer with S8HR APN to the LMISF over the Xia reference point.

- Receive the intercepted IMS Signalling Bearer information from the LMISF over the Xib reference point along with the packet forwarding rules.
- Identify the dedicated EPS Bearer used as the Media Bearer linked to the above-indicated intercepted IMS Signalling Bearer.
- As per the packet forwarding rules (i.e. as instructed by the LMISF), deliver the packets of the GTP tunnel used for Media Bearer associated with the intercepted IMS Signalling Bearer to the LMISF over the Xia reference point.
- When instructed by the LMISF, stop delivering the packets of the GTP tunnels used for Media Bearers associated with the IMS Signalling Bearer with a deactivated interception.

NOTE: The present document assumes that BBIFF is closely coupled to S-GW in the VPLMN. Therefore, present document refers to BBIFF as S-GW/BBIFF.

20.1.3.3 LMISF: LI Mirror IMS State Function

LMISF is a LI specific function introduced to support the lawful interception of voice services in the VPLMN when S8HR is used as the roaming architecture.

The LMISF shall provide the following functions:

- Provide S8HR APN information to the S-GW/BBIFF over the Xib reference point.
- Instruct S-GW/BBIFF over Xib reference point to notify (to LMISF) whenever an IMS Signalling Bearer or a Media Bearer with S8HR APN is created, modified or deleted.
- Instruct S-GW/BBIFF over the Xib reference point to start delivering the packets (to LMISF) of all IMS Signalling Bearers with S8HR APN.
- Receive target identity information from the ADMF over the X1_1 reference point as described in clause 5.1.
- Receive the notification from S-GW/BBIFF over the Xib reference point whenever an IMS Signalling Bearer or a Media Bearer with S8HR APN is created, modified or deleted.
- Store the IMS Signalling Bearer information (e.g. EPS Bearer ID) along with the IMSI associated with the UE to which the IMS Signalling Bearer was created, modified or deleted. Store or update the most recent UE location information received along with the IMS Signalling Bearer or the Media Bearer information.
- Receive and examine the IMS signalling messages delivered by the S-GW/BBIFF over the Xia reference point.
- Receive media packets delivered by the S-GW/BBIFF over the Xia reference point. Identify the intercepted IMS session that relates to the media packets.
- Maintain an IMS signalling state for all inbound roamers with S8HR that are registered to the network or in an IMS session. Part of this function is to track all IMS registrations, re-registrations and de-registrations of inbound roamers with S8HR.
- After examining and determining that the IMS signalling messages involves a target, establish and maintain a map between the target identity and the IMS Signalling Bearer information or the Media Bearer (e.g. EPS Bearer ID along with the IMSI value of the UE). When the IMS signalling messages do not involve a target, establish and maintain a map between the IMS Signalling Bearer or the Media Bearer information and the potential target identities.
- Generate and deliver the IRI to the Delivery Function 2 as described in clause 20.3.
- Inform the S-GW/BBIFF over the Xib reference point with the IMS Signalling Bearer information associated with an intercepted IMS session that requires CC interception and instruct the S-GW/BBIFF to start delivering the packets of the Media Bearer associated with that IMS Signalling Bearer.
- Inform the S-GW/BBIFF over the Xib reference point with the IMS Signalling Bearer information associated with a deactivated interception and instruct the S-GW/BBIFF to stop delivering the packets of the Media Bearer associated with that IMS Signalling Bearer. Generate and deliver the IRI messages to the Delivery Function 2 as described in clause 20.3.

- Generate and deliver the CC to the Delivery Function 3 as described in clause 20.2.
- When target identity is received from the ADMF, determine whether any IMS Signalling Bearer is associated to the target identity. If yes, start the interception process as described in clause 20.3.
- Provide the decompression of IMS signalling messages upon detecting the compression.

20.2 Provision of Content of Communications

20.2.1 Overview

20.2.1.1 General

For interception of content of communications of voice services involving the inbound roamers with S8HR, the following shall occur:

- For each IMS session that is intercepted, LMISF determines whether a CC interception is required.
- When the CC is interception required, LMISF provides the IMS Signalling Bearer information to the S-GW/BBIFFF (as described in clause 20.1.3.3) and instructs the S-GW/BBIFF (as described in clause 20.1.3.3) to start delivering the media packets (i.e. packets from the Media Bearer) associated with that IMS Signalling Bearer.
- S-GW/BBIFF delivers the media packets (i.e. packets from the Media Bearer) associated with the IMS Signalling Bearer (as described in clause 20.1.3.2) to the LMISF.

The S-GW/BBIFF shall provide the LMISF a means to link the intercepted media packets with the associated IMS Signalling Bearer information provided by the LMISF (e.g. the delivered media packets include the EPS Bearer ID of the IMS Signalling Bearer along with the IMSI value of the UE).

The LMISF shall include the Correlation Information (associated with the IMS session) in the CC delivered to the Delivery Function 3 over the X3 reference point. A pictorial view of the CC interception is illustrated in figure 20.2 below:

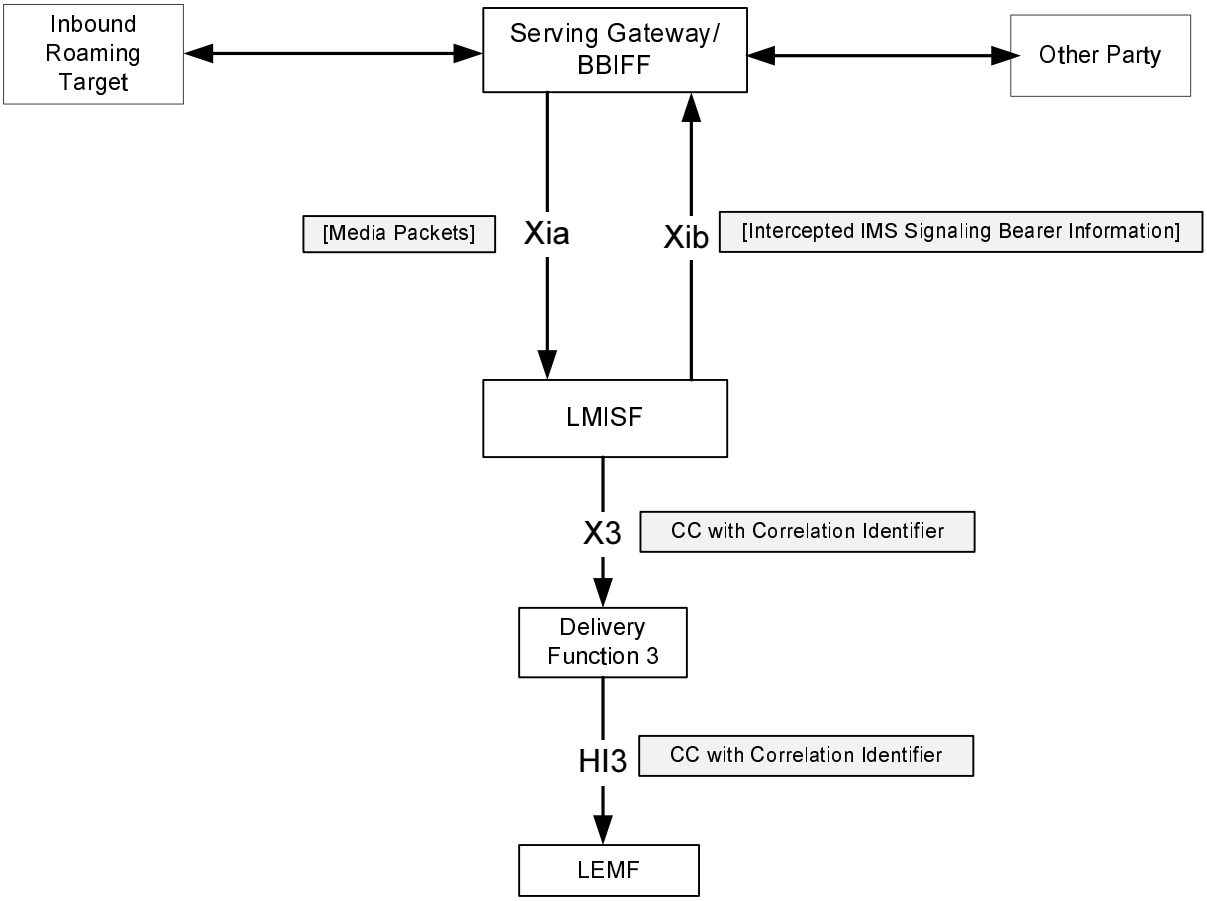


Figure 20.2: CC Interception of voice calls involving the inbound roaming target with S8HR

The figure 20.2 shows that LMISF provides the IMS Signalling Bearer Information to the S-GW/BBIFF. The S-GW/BBIFF uses the IMS Signalling Bearer information to find the associated Media Bearer.

When the LMISF identifies that the CC interception is to be stopped, the following shall occur:

- LMISF stops delivering the CC to Delivery Function 3 over the X3 reference point.
- LMISF provides the IMS Signalling Bearer information to the S-GW/BBIFF with an instruction (as described in clause 20.1.3.3) to stop the delivery of media packets (i.e. packets from the Media Bearer) associated with the IMS Signalling Bearer.
- S-GW/BBIFF stops the delivery of the media packets associated with the IMS Signalling Bearer (as described in clause 20.1.3.2) to the LMISF.

20.2.1.2 S-GW/BBIFF Procedures for CC Interception

When instructed by the LMISF, the S-GW/BBIFF shall use the IMS Signalling Bearer information that it received from the LMISF to determine the media packets of which EPS Bearer (i.e. the Media Bearer) has to be delivered to the LMISF (e.g. EPS Bearer ID of IMS Signalling Bearer is linked to the EPS Bearer used as the Media Bearer). Then, the S-GW/BBIFF shall deliver all the octets above the GTP layer of the GTP tunnel used for the Media Bearer to the LMISF.

S-GW/BBIFF shall indicate to the LMISF whether the media packets were travelling to or from the HPLMN (e.g. based on tunnel end point IDs).

When instructed by the LMISF, the S-GW/BBIFF shall stop the delivery of media packets to the LMISF.

20.2.1.3 Void

20.2.1.4 LMISF Procedures for CC Interception

Upon determining that the CC interception is required or is to be stopped for an IMS session, LMISF shall pass the IMS Signalling Bearer information to the S-GW/BBIFF with an instruction that indicates to the S-GW/BBIFF whether the packets from the Media Bearer associated with the IMS Signalling Bearer shall be delivered, or not delivered, to the LMISF.

When the media packets are received from the S-GW/BBIFF, the LMISF shall determine whether the interception is active on the IMS session. If active, the LMISF shall determine the Correlation Identifier (or Correlation Number) associated with the IMS session to which the media corresponds. If the interception is not active, the LMISF shall discard the media packets.

The LMISF shall construct the CC and deliver the same to the Delivery Function 3 over X3 reference point (see clause 20.2.2).

20.2.2 X3-Interface

For the delivery of intercepted media packets, the following information shall be passed from the LMISF to the Delivery Function 3 in addition to the intercepted media packets:

- target identity;
- Correlation identifier;
- Time stamp (optional);
- Direction (indicates media is from or to the target) - optional.

The Delivery Function 3 delivers the information to the LEMF over the HI3 interface based on the national regulations.

20.3 Provision of Intercept Related Information

20.3.1 Overview

20.3.1.1 General

For interception of intercept related information of voice services involving the inbound roaming targets with S8HR, the following shall occur:

- LMISF provides the S8HR APNs to the S-GW/BBIFF with an indication that all packets from the IMS Signalling Bearer with the S8HR APN are to be delivered to the LMISF.
- S-GW/BBIFF delivers the IMS signalling packets from the S8HR IMS Signalling Bearers to the LMISF.
- LMISF examines whether the IMS signalling messages involve a target and if so, it generates and delivers the IRI to the Delivery Function 2.

The LMISF shall generate the IRI from the IMS signalling messages and deliver the same to the Delivery Function 2 over X2 reference point. All SIP messages executed on behalf of a target shall be delivered as IRI.

The S-GW/BBIFF also notifies the LMISF whenever an S8HR IMS Signalling Bearer or a Media Bearer is created, modified, or deleted along with the IMSI value of the target UE and the location of the UE.

A pictorial view of the general overview of IRI interception is illustrated in figure 20.3 below:

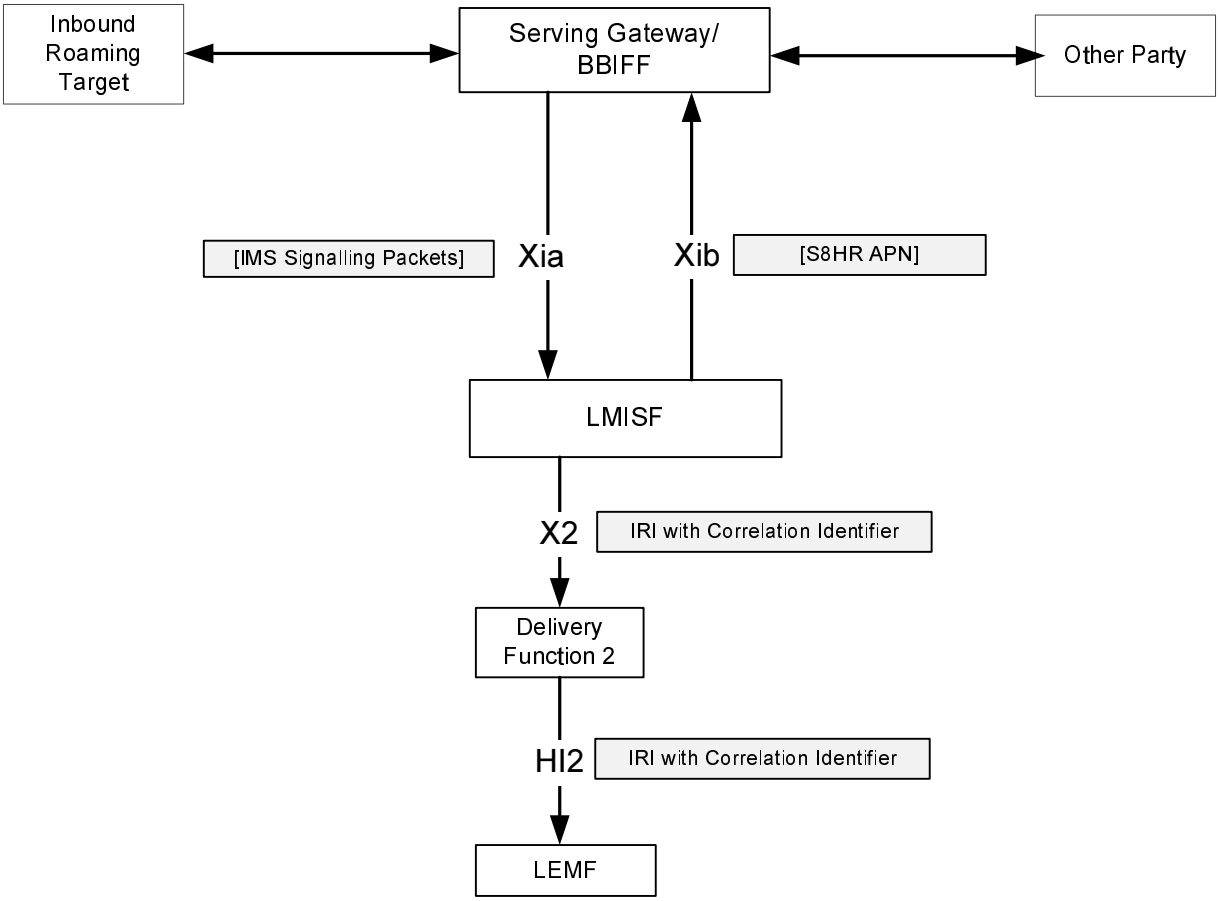


Figure 20.3: IRI Interception of voice calls involving the inbound roamer with S8HR

The figure 20.3 shows that LMISF provides the S8HR APNs to the S-GW/BBIFF. When the IMS signalling messages correspond to a target, the LMISF generates the IRI and deliver the same to the Delivery Function 2 which in turn delivers the IRI to the LEMF.

To support the mid-call interception, the LMISF maintains the IMS call state (including any necessary information from the SIP messages). When the target identity provisioned into the LMISF is involved in an ongoing IMS call, the LMISF shall start the interception as described in clause 20.3.2.

20.3.1.2 Void

20.3.1.3 S-GW/BBIFF Procedures for IRI interception

When instructed by the LMISF, the S-GW/BBIFF shall notify the LMISF whenever the IMS Signalling Bearer or the Media Bearer with S8HR APN is created, modified or deleted.

When instructed by the LMISF, the S-GW/BBIFF shall deliver all the octets above the GTP layer of GTP tunnel used for IMS Signalling Bearer to the LMISF along with the associated with IMS Signalling Bearer information.

20.3.1.4 LMISF Procedures for IRI interception

The LMISF shall receive the notification from S-GW/BBIFF whenever a GTP tunnel for IMS Signalling Bearer or a Media Bearer with S8HR APN is created, modified or deleted. The LMISF shall store the Tunnel information (Tunnel ID) of the GTP tunnel along with the IMSI associated with the UE to which the GTP tunnel was created. If delivered, the LMISF shall also store the UE location information along with the time that it has received the same from S-GW/BBIFF.

The LMISF shall receive and examine the IMS signalling messages delivered by the S-GW/BBIFF. After examining and determining that an IMS signalling message involves a target, LMISF shall deliver the SIP message to the Delivery Function 2 over the X2 reference point (see clause 20.3.2). The up-to-date UE location information stored in the LMISF, as available, shall also be delivered to the Delivery Function 2. LMISF shall maintain an IMS call state for all

inbound roaming users (for the target identity or potential target identity). The maintained current IMS call state (along with the stored necessary information from the SIP messages) shall be sufficient to support the mid-call interception.

When the received IMS signalling message involves compression, the LMISF shall perform the decompression of SIP messages (as defined in clause 8 of TS 24.229 [49]) and follow the steps used to process the uncompressed SIP messages.

Refer to clause 20.1.3.3 for a complete list of LMISF functions that also include a few functions that aid the overall interception capabilities of voice services involving the inbound roamers with S8HR as the roaming architecture.

20.3.2 IRI Events

20.3.2.1 General

In general, the IRI events applicable to S8HR LI are similar to the IRI events defined in clause 7A except that the LMISF (instead of CSCF) examines and generates the IRI events. However, since the interception in LMISF is used only for S8HR LI (i.e. roaming case), certain events defined in clause 7A are not applicable:

Any SIP messages sent to, and received from, the target UE as observed at the S-GW/BBIFF shall be delivered as IRI with the additional information as listed in clause 20.3.3. The LMISF shall include the UE location (along with timestamp) received from the Serving Gateway/BBIFF in the appropriate events.

The provisioned target identity can be a SIP URL, a TEL URL or an IMEI. The method used to verify a target identity is dependent on the call direction. S-GW/BBIFF shall indicate to the LMISF whether the IMS signalling packets were travelling to or from the HPLMN (e.g. based tunnel end point IDs).

For calls originating from the inbound roaming target, calling party identity (e.g. SIP headers: P-Preferred-Id, From) is used verify the target identity. For calls terminating to the inbound roaming target, called party identity (e.g. SIP headers: Request URI, P-Called-Party-Id, To) is used to verify the target.

For incoming calls to an inbound roaming user from a Non-Local-Id as the target, calling party identity (P-Asserted-Id, From) or redirecting party identity (History-Info, Diversion) are used to verify the target. For outgoing calls from an inbound roaming user to a Non-Local-Id as the target, the called party identity (Request-URI, To) is used to verify the target. See Annex I for an informative illustration of Non-Local-Id target interception cases. The LMISF will have to provide the functions provided by the P-CSCF (Annex I) in the VPLMN.

20.3.2.2 IMEI-based interception

To support the IMEI-based interception, the LMISF shall provide (if possible) the functions equivalent to functions defined for CSCF in clause 7A.8.

NOTE: The format of the Instance Id used in clause 7A.8 is under the control of HPLMN.

20.3.2.3 Mid-call Interception

The mid-call interception is performed using the procedures described in clause 7A.3.1 except that LMISF (instead of CSCF as described in clause 7A.3.1) maintains the IMS call state, stores the SIP messages and generates the IRI.

When a lawfully authorized interception is deactivated while the target is on an IMS session, the LMISF shall stop delivering the IRI events to the Delivery Function 2.

20.3.2.4 Signalling Compression

If compression of the IMS signalling traffic is detected (as defined in RFC 3320 [69] and RFC 4896 [70]), then the SIP messages are first decompressed (as defined in clause 8 of TS 24.229 [49]) and processed with the steps used to process the uncompressed SIP messages.

20.3.2.5 Limitations

The limitations described in the NOTE of clause 15.4.1 apply to lawful interception capabilities provided in the VPLMN for voice services involving the inbound roamers with S8HR as the roaming architecture.

20.3.3 X2-Interface

For the delivery of intercepted SIP messages, the following information shall be passed from the LMISF to the Delivery Function 2 on the X2 reference point:

- Target Identity (SIP URL, TEL URL, IMEI);
- Correlation Identifier;
- Event Time and Date;
- Network Element Identifier;
- UE Location (conditional, as applicable, e.g. IMS session establishment events);
- date/time of Location (if target location provided);
- SIP Header;
- SIP payload.

The Delivery Function 2 delivers the IRI to the LEMF over the HI2 interface based on the national regulations.

20.4 Lawful Interception with CUPS architecture

When Control and User Plane Separated (CUPS) architecture is used for S-GW, the S-GW/BBIFF functions may have to be split as shown in figure 20.4.

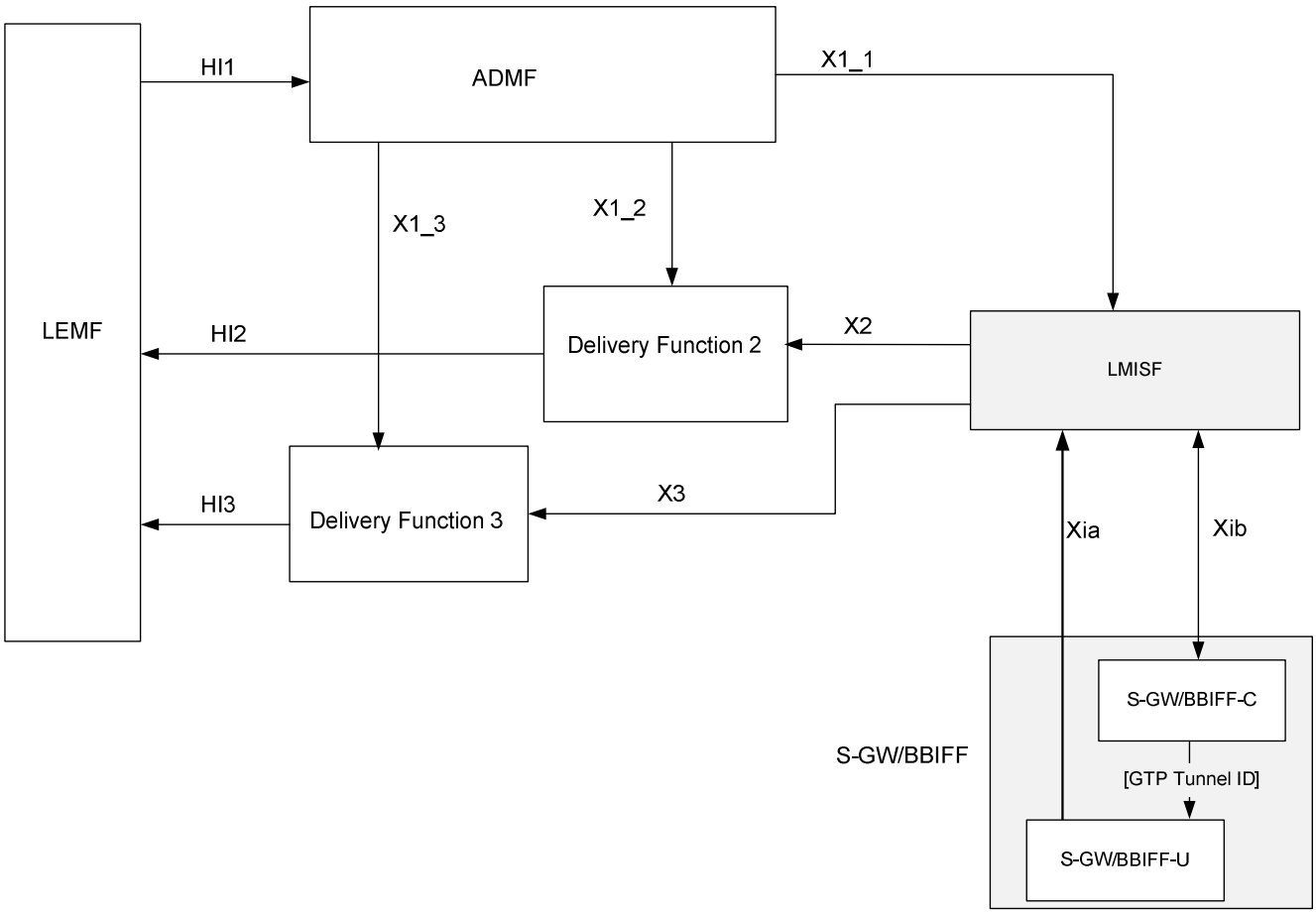


Figure 20.4: CUPS LI architecture for voice services of inbound roamers with S8HR

The S-GW/BBIFF-C receives the S8HR APN information over the Xib reference point from the LMISF.

The S-GW/BBIFF-C shall notify the LMISF over the Xib reference point whenever an IMS Signalling Bearer for S8HR APN is created, modified or deleted along with the IMSI value of the UE. In that notification, the UE location information received from the MME shall be included.

The S-GW/BBIFF-C shall provide packet detection rules with the GTP tunnel Id of the IMS Signalling Bearer (associated with S8HR APN) to the S-GW/BBIFF-U with an indication to instruct the S-GW/BBIFF-U to send the IMS signalling packets to the LMISF. Accordingly, the S-GW/BBIFF-U shall send the IMS signalling packets to the LMISF over the Xia reference point.

When the CC interception is required, the LMISF would have passed on the IMS Signalling Bearer Id of the intercepted IMS session to the S-GW/BBIFF-C. The S-GW/BBIFF-C shall determine the GTP tunnel of the Media Bearer linked to that IMS Signalling Bearer and pass the packet detection rules with the GTP tunnel Id of the Media Bearer to the S-GW/BBIFF-U. The S-GW/BBIFF-U shall send the packets of that GTP tunnel (i.e. of Media Bearer) to the LMISF over the Xia reference point.

The method used to transfer the GTP tunnel Id along with the packet delivery indication from S-GW/BBIFF-C to S-GW/BBIFF-U shall be done as described in subclause 12.9.

NOTE: The X3c, X3u reference points and the Split X3 LI Interworking Function (SX3LIF) described in subclause 12.9 are not used for S8HR LI when a Serving Gateway is deployed with CUPS architecture.

20.5 S8HR LI and Target UE Mobility

20.5.1 Overview

During a session (packet data or voice) that involves the target UE, the S-GW/BBIFF that provides the IMS Signalling packets and Media packets to the LMISF can change (i.e. S-GW/BBIFF relocation).

The lawful interception of voice calls involving the target shall continue when the S-GW/BBIFF relocation happens. The IRI events and the CC delivered before and after the relocation shall be correlated.

20.5.2 S-GW Relocation

As described in sub-clause 20.1.3.3, the LMISF provides the S8HR APNs to the S-GW/BBIFF and the S-GW/BBIFF notifies the LMISF whenever an IMS Signalling Bearer for the S8HR APN is created, modified or deleted along with the IMSI value of the UE and the UE location. This happens independently of S-GW relocation. When the IMS signalling packets are received from the S-GW/BBIFF, the LMISF delivers the IRI events to the DF2 if the IMS signalling packets are associated with an intercepted IMS session, This, also happens independent of S-GW relocation.

When a target UE is on an IMS session and if the S-GW that has the associated IMS Signalling Bearer changes, the IMS Signalling Bearer is created at the new S-GW/BBIFF as well. The new S-GW/BBIFF that notifies the LMISF about the IMS Signalling Bearer shall include an indication in the notification to inform the LMISF that a S-GW relocation has occurred.

The LMISF shall provide the following functions to support the continued and correlated interception for the CC:

- When a notification is received from the S-GW/BBIFF (over the Xib reference point) indicating that an IMS Signalling Bearer is created due to S-GW relocation, examine to see whether the IMS Signalling Bearer is associated with an IMS session that is being intercepted.

- If the IMS Signalling Bearer is associated with an intercepted IMS session, examine to see whether the intercepted IMS session requires the CC interception.

- If the intercepted IMS session requires CC interception, inform the S-GW/BBIFF (over the Xib reference point) with the IMS Signalling Bearer information (e.g. IMS Signalling Bearer ID, IMSI value) with an instruction to deliver (to LMISF) the packets from the Media Bearer associated with the IMS Signalling Bearer.

The new S-GW/BBIFF delivers the packets from the Media Bearer associated with the IMS Signalling Bearer to the LMISF as described in sub-clause to 20.2.1.2. The LMISF delivers the received media packets to the DF3 as CC along with the correlation information as described in clause 20.2.1.4.

The LMISF shall not disrupt the ongoing interception of IRI and CC, if a IMS Signalling Bearer deletion notification is received from the old S-GW/BBIFF.

21 Invocation of Lawful Interception for Push to talk over Cellular services.

21.0 General

In the present clause, ”PTC” will be used to reference events or services that occur in either of the two different architectures unless specified otherwise, e.g., MCPTT or PoC.

The HI2 and HI3 interfaces in clause 4 of the present document, Figures 1k and 1l, represent the interfaces between the LEA and two delivery functions. Both interfaces are subject to national requirements. They are included for completeness, but are beyond the scope of this specification.

In figure 1l the DF2 delivery function is used:

- to convert the information on the X2-interface to the corresponding information on the HI2 interface;
- to distribute the intercept related information to the relevant LEAs.

In figure 1k the DF3 is responsible:

- for Content of Communication (CC) delivery to the LEA.

The following is a list of servers which support either type of PTC architecture; any combination of these servers could be deployed together to support both services if the SP chooses to do so. These servers will require an ICE to generate IRI for the events depicted in the following clauses.

MCPTT servers (Common services core):

- Group management, Configuration, Identity, Key.

PoC servers (Shared XDMS):

- Shared List, Group, Policy, Presence, NW PoC Box, Aggregation Proxy, External Media Content server.

SIP/IP Core servers:

- Presence.

If interception has been activated for one or more parties as per the applicable warrant of the PTC communication both CC and IRI shall be delivered for each party as separate intercept activity.

21.1 Provision of IRI – PTC Service

21.1.0 Introduction

PoC and MCPTT use similar architectures for service delivery, and LI shall primarily occur at the PoC or MCPTT server for that service.

Intercept Related Information events are necessary at the PTC Mobile Station Attach, PTC Mobile Station Detach, PTC session Activation, Start of intercept with PTC context active, PTC Context Deactivation, PTC Serving System, and PTC events.

For PTC services that provide KMS based encryption, clause 21.1.1 specifies LI architecture and functions needed to provide session encryption keys generated by the KMS to protect a UE that is a target for interception. This clause is applicable to the cases in which the KMS is under responsibility of the Operator providing the PTC network infrastructure. Other scenarios such as the one in which the KMS is run by an independent legal entity are outside the scope of the present document.

Other HSS events, Non-Local ID targeting for PTC events (e.g. based on traffic analysis), related and Serving System events reporting are national options.

Figure 21.1.1 shows the transfer of intercept related information to the DF2. If an event for / from a PTC MS occurs, the Shared XDMS/MCPTT common core servers or the Home Subscriber Service (HSS) sends the relevant data to the DF2 for delivery to the LEA.

For a PTC MS, dependent on national requirements, delivery shall occur in the following cases:

- when the PoC/MCPTT server detects a PTC session event (e.g. when receiving a PTC signalling message or sends a PTC signalling message to the PTC target;
- when the Shared XDMS/MCPTT Common Core servers detects the PTC event (e.g. when receiving a PTC signalling message from the target MS, or when sending a PTC signalling message to the PTC target.

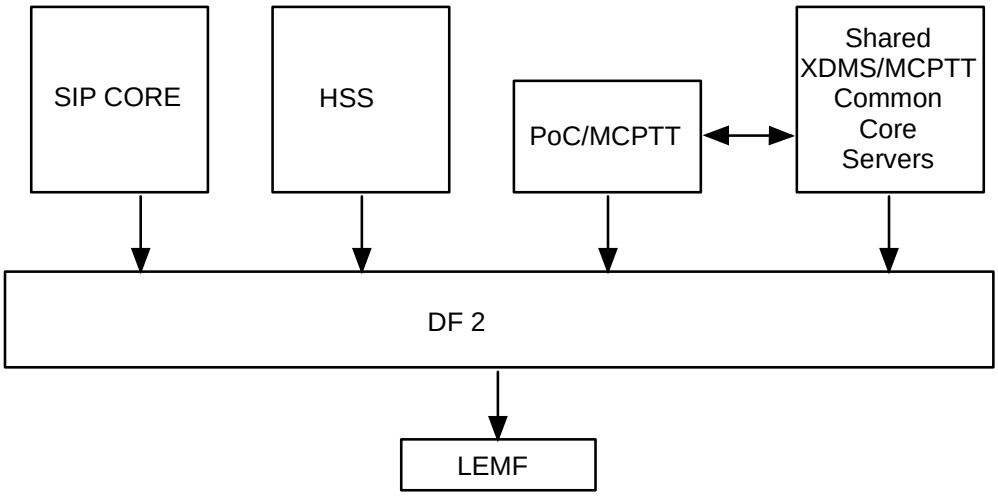


Figure 21.1.1: Provision of Intercept Related Information - PTC

21.1.1 Decryption for PTC services

This clause describes how the CSP can provide the session encryption keys generated by the KMS to the LEMF when the CSP has PTC services with Security options. If an ICE allows interception of IRI or Content of Communication in clear then this clause does not apply.

If a Key Management Service (KMS) is used for PTC type services to provide encryption for security, the CSP may use the mechanism as defined in Figure 21.1.1.1 to deliver the session's keys and the specific parameters needed to decrypt the intercepted communications.

Once this security information is retrieved, DF2 may deliver this security information to the LEMF as IRI in order for the LEMF to decrypt the intercepted traffic.

The LI architecture and functions needed for delivery of the encryption parameters are shown below to provide session encryption keys and specific parameters generated by the KMS. This section is applicable to the cases in which the KMS is under responsibility of the Operator providing the PTC infrastructure. Other scenarios such as the one in which the KMS is run by an independent legal entity are outside the scope of the present document.

NOTE: This section covers the scenario in which encrypted content of communication is provided to the LEMF together with encryption keys, to allow decryption at LEMF.

Figure 21.1.1.1 shows the LI architecture for the case in which decryption is performed by the LEMF and a KMS is used to support PTC security with a Xk interface defined between the DF2/MF and the KMS, in addition to the interfaces and functional entities needed to support LI in the SIP core in the P-CSCF/S-CSCF as shown in clause 7A.7.1 and Figure 7A.7.1 within the present document.

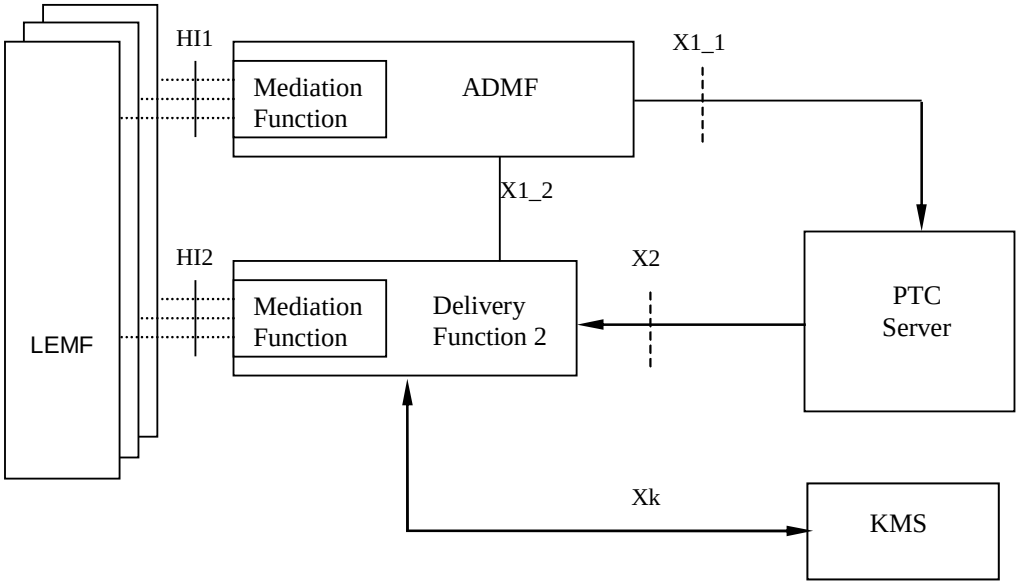


Figure 21.1.1.1: KMS Intercept configuration

As discussed in clause 7A.7.1 when LI has been activated in the P/S-CSCF for a target, the node will report SIP messages events on the X2 interface, as specified in section 7.A and subsections. The DF2/MF shall extract from the intercepted SIP signalling the information related to the encryption and send a request over the Xk interface to the KMS to derive the encryption keys; the request will carry also the reference to the ticket transferred by the SIP signalling between the parties involved in the communication. The KMS shall then, based on the information received from the DF2, resolve the ticket and provide the session keys to the DF2/MF over the Xk interface.

21.1.2 Signalling over the Xk interfaces and LI events

The following messages are defined over the Xk interface:

- get_keys;
- get_keys_response.

The message get_keys shall be sent by the DF2/MF to the KMS in order to ask the KMS to provide session keys for an ongoing communication.

The message get_keys_response shall be sent by the KMS to the DF2/MF in order to provide the session keys.

The message get_key_response defines a LI event provided by the KMS to the DF2/MF which shall then be sent by the DF2/MF to the LEMF in a proper IRI record over the HI2 interface.

Table 21.1.2.1 provides the list of parameters, which shall be carried by the message get_keys, in order to transfer to the KMS the information, as specified in TS 33.328 [25], needed to provide the session encryption keys:

Table 21.1.2.1: Parameters and information in message get_keys

Public KMS Identity of the target user
TRANSFER_INIT
TRANSFER_RESP

Upon reception of get_keys message, the KMS shall verify that the key management information is related to the targeted user.

A timer may be defined in the DF2/MF in order to specify the amount of time that the DF2/MF shall wait for the response from the KMS. If this timer expires, a failure indication shall be sent to the LEMF.

Table 21.1.2.2 provides the list of parameters, which shall be carried by the message get_keys_response, in order to provide the DF2/MF with the session keys:

Table 21.1.2.2: Parameters and information in message get_keys_response

Crypto Session ID
Session key
Salt
Failure indication (optional)

With reference to table 21.1.2.2, in case of failure in providing any of the decryption information, the KMS may provide a decryption failure indication.

Upon reception of get_keys_response message or in case of timer expiry, the following information shall be provided to the LEMF by the DF2/MF:

- Lawful interception identifier;
- Observed target identity(ies);
- Correlation number (in order to correlate the keys to IMS session under interception at the CSCF(s));
- Event type (session encryption keys available);
- Crypto Session ID (if provided by the KMS);
- Session key (if provided by the KMS);
- Salt (if provided by the KMS);
- MediaSec key retrieval failure indication (in case of e.g. timer expiry, or failure indication received from the KMS).

21.2 Provision of Content – PTC Service

The access method for the delivering of PTC Intercept Product is based on duplication of packets without modification at PoC/MCPTT server. The duplicated packets with additional information in a header, as shown in figure 21.2.1, are sent to DF3 for further delivery to the LEA.

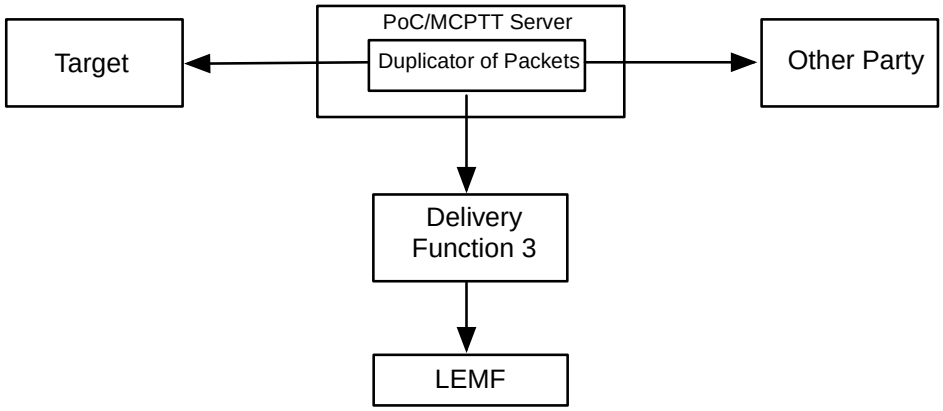


Figure 21.2.1: Configuration for interception of Content- PTC

21.3 Provision of Interception

21.3.1 X3-Interface

In addition to the intercepted content of communications, the following information needs to be transferred from the PTC ICE to the DF3 in order to allow the DF3 to perform its functionality:

- target identity;

- correlation number;
- time stamp - optional;
- direction (indicates whether T-PDU is from the target or to the target) - optional;
- identity of source of media (communications content) for group calls;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of Location (if target location provided).

21.3.2 X2-interface

The following information needs to be transferred from the SIP Core, or the HSS to the DF2 in order to allow a DF2 to perform its functionality:

- target identity;
- events and associated parameters as defined in table 21.3.4.1 and 21.4 shall be provided;
- the target location (if available) or the IAs in case of location dependent interception;
- date/time of Location (if target location provided);
- correlation number;
- parameters (keys and associated parameters for decrypting CC), if available and necessary;
- Encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.

21.3.3 LI Defined Events

21.3.3.1 IRI Defined Events

The LI event information is sent to the DF2/DF3 is triggered by different PTC session related and non-call related events/reports. Details for each event are described in the following clauses.

The following events are applicable to both the PoC and MCPTT service ICE:

- PTC Session Initiation;
- PTC Session Abandon;
- PTC Session Start;
- PTC Session End;
- PTC Start of Interception;
- PTC Pre-Established Session;
- PTC Instant Personal Alert;
- PTC Party Join;
- PTC Party Drop;
- PTC Party Hold;
- PTC Party Retrieve;
- PTC Media Type Notification;
- PTC Group Advertisement;
- PTC Floor Control;

- PTC Target Presence;
- PTC Associate Presence;
- PTC List Management;
- PTC Access Policy;
- PTC Group Request;
- PTC Encryption.

The following events are applicable to the HSS:

- PTC Serving System;
- HSS subscriber record change;
- Cancel location;
- Register location;
- Location information request.

The following events are applicable to the SIP Core:

- Service Registration.

A set of elements as shown below can be associated with the events above. The events trigger the transmission of the information from the PTC server ICE, or HSS to DF2. Available IEs from this set of elements as shown below can be extended in the HSS, if this is a requirement as a national option. DF2 can extend available information if this is necessary as a national option e.g. a unique number for each surveillance warrant.

21.3.3.2 Communication Content (CC) Event

The following event information is sent to the DF3 when CC is authorized for delivery. The following are applicable to both the PoC and MCPTT service ICE:

PTC Communication Content (CC) Delivery.

21.3.4 Events Elements

21.3.4.1 IRI Event Elements

The LI IRI event information is sent to the DF2/DF3 is triggered by different PTC session related and non-call related events/reports. Details for each event are described in the following clauses.

Within Table 21.3.4.1: IRI Information Elements for PTC Event Records, a provisioned target identity can be a SIP URI, TEL URI , MCPTT ID or an IMEI.

A PTC Client may support multiple PTC Addresses and be involved in one or more PTC Sessions at the same time using the same or different PTC Addresses.

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from PTC ICE to DF2. Available IEs from this set of elements as shown below can be extended in the PTC ICE, if this is necessary as a national option. DF2 can extend available information if this is necessary as a national option e.g. a unique number for each surveillance warrant.

Table 21.3.4.1: IRI Information Elements for PTC Event Records

AbandonCause - Identifies the reason for the abandoned PTC Session.
Access_PolicyFailure - Reports the error code or reason for failure when Access Policy Request is unsuccessful.
Access_Policy_Type – Identifies the type of access policy list being managed or queried by the PTC Intercept target.
Access_Policy_event - Identifies the choice the target or an associate makes within access policy selection which can be by user or group to allow or block the incoming PTC session, Auto Answer, or allow or block a conference type.
Ad-hoc PoC Group Session - A PoC Group Session established by a PoC User to PoC Users listed on the invitation. The list includes PoC Users or PoC Groups or both.
Alert indicator - Indicates an emergency alert sent, received or cancelled.
AssociatePresenceStatus - Provides the Associate Presence Status, which is a list of: *PresenceID*: Identity of PTC Client(s) or PTC group, when known *PresenceType*: Identifies type of ID [PTC Client(s) or PTC group]. *PresenceStatus*: Presence state of each ID.
Broadcast indicator - Indicates that the group call request is for a broadcast group call.
Charging Correlation ID – PTC supports both subscription based charging and traffic based charging. Provide any charging events, e.g., service activation, correlation ID between the PoC service charging data and the packet data services.
Cipher - The name of the cipher.
Contact_Identity - Identity of the contact in the list, one contact per Contact List or Group List.
CryptoContext - If further information is needed to associate the encryption information with a specific session or stream, this parameter shall be included to identify the context to which this encryption message applies.
PTC Party - Join/Drop/Hold/Retrieve, MCPPT emergency/imminent group/peril etc.
Emergency indicator - Indicates the request is an MCPTT emergency call.
Event Date - Date of the event generation in the PTC Server or Client.
Event Time - Time of the event generation in the PTC Server or Client
Event Type - Description of which type of event is delivered: PTC Session Initiation, Abandon, Start, End, End Cause, Start of Interception, Pre-Established Session, Instant Personal Alert, Floor Control, Target Presence, Associate Presence, a PTC Party Join, Party Drop, Party Hold, Party Retrieve, PTC Media Modification, PTC Group Advertisement. Group Request, Group Response, Group Interrogate, PTC Media Type Notification, Bearer Capability, MCPTT Emergency Group Call, Cancel, Alert, State, MCPTT Imminent Peril Group Call. PTC Serving System, PTC List Management and Access Policy.
Failure_Code – The reason or code for the failure or closing of the session.
Floor_Request - Indicates that the originating client requests the floor.
FloorSpeakerIdentity - Identification of the PTC Client that has the Talk Burst.
Group_Ad_Receiver – The group administrator who was the receiver of the group call.
Group_Ad_Sender – The group administrator who was the originator of the group call.
Group_Identity - Identifies the PTC Group Identity, Nick Name, and characteristics.
GroupAuthorizationRules - Identifies the action requested by the target to the PTC Group authorization rules.
Hold_retrieve_Indication - The PTC Session is put on hold (deactivate Media Bursts) or a new Primary PTC Session is activated or another PTC Session is locked for talking/listening.
Hold_Retrieve_user – Identifies the PTC user who removed their PTC Session from hold.
Imminent peril indicator - Indicates that the PTC call is an imminent peril call.
Implicit floor request - When originating client requests the floor.
InitationCause - The network receives an invitation from the PTC Intercept Target to initiate a PTC session.
Invited_PTC_Client - A PTC Client that is invited to a PTC Session
Inviting_PTC_user – The PTC User who has been invited to a PTC Session.
Key - The key needed to decipher.
KeyEncoding - Shall be included to provide the encoding of the key if the encoding is other than binary
IPAPartyIdentity - Instant Personal Alert - Identifies the party that receives the Instant Personal Alert from the PTC Intercept target or the associate that sends the Instant Personal Alert to the PTC Intercept target.
Join_PTC_user – Identity of the PTC User who has joined the session, i.e., associate identity or targets.
ListManagmentAction –Identifies the action requested by the PTC Intercept target to the Contact Lists or Group Lists. Identifies the PTC-specific documents stored in the network that the target attempts to modify or that changes were made to the targets PTC-specific documents stored in the network and identifies what action was taken by the target or the associate i.e., create, modify, retrieve, delete, notify.
List_ManagementFailure - Reports the error code or reason for failure when List Management modifications should fail, when known i.e., not authorized, time out, etc.
ListManagementType – Different PTC Group lists: ContactListManagementAttempt, GroupListManagementAttempt, and GroupListManagementResult. Identifies the PTC-specific documents stored in the network that the target attempts to modify or that changes were made to the targets PTC-specific documents stored in the network and identifies which list was modified i.e., list or group.

Location - Report when a PTC Session is initiated by the intercept target.This parameter is not reported when the PTC Intercept Target receives an invitation to join a PTC Session; rather this information is reported by the PTC Session Start event (see PTC Session Start event for usage). Include when reporting of the PTC Intercept Target's location information is authorized and known.
Time of Location - Date/Time of location. The time when location was obtained by the location source node.
Max_TB_Time - Include the maximum duration value for the talkburst before the permission is revoked, provide when known.
MCPTT CorrelationID - Uniquely identifies the MCPTT Session, correlates CII messages, and correlates CII and CC messages.
MCPTT group ID - The Mission Critical Push To Talk group Identity.
MCPTT ID - Mission Critical Push To Talk identity.
MCPTT indicator – Indicates direction of the received request as either from the client or from the group to the client.
MCPTT Location – Indicates the location of the target.
MCPTT Organization name – Name of the organization that the Mission Critical device belongs to.
MediaStream_Availability – Indicates if the PTC intercept target's PTC Client is not able/willing to receive media streams immediately. Provide when Pre-established session is established.
Network Element Identifier - Unique identifier for the network element reporting the event.
Observed IMEI - The provisioned International Mobile Equipment Identity target identity.
Observed SIP URI - The provisioned target identity can be a SIP URI
Observed TEL URI - The provisioned target identity can be a TEL URI
Party_Drop - Member of a PTC Group Session and leaves the PTC Session, provide when known.
PreEstablishedSessionID – Identifies the PTC Pre-established Session.
PreEstablishedStatus – Indicates if the Pre-Established Session is established (setup completed), modified, or released.
PTCCorrelationId - Uniquely identifies the PTC Session, correlates CII messages, and correlates CII and CC messages.
PTC group ID - The PTC group ID of the group on which the call is initiated.
PTCHost - Indentifies the PTC participant who has authority to initiate and administrate an active PTC Group Session. Provide when known.
PTC_ID_List - The list of PTC IDs of the PTC group members.
PTC Location – Indicates the location of the target (if authorized for delivery).
PTCOriginatingId - Identifies the originating party. Provided when known.
PTCOther - Other information that is required to decrypt the data.
PTCParticipants - Identifies the invited PTC participants, when known, if other than the PTC Intercept Target.
PTCSessionInfo - Provides PTC Session information such as PTC Session URI, PTC Session type, and Nickname.
PTCUserAccessPolicy – Identifies the action requested by the PTC Intercept Target related to the PTC user access policy.
Queued_FloorControl - Indicates if queuing is supported by the PTC Server and the intercept target's PTC Client.
Queued_Position_Status - If queued floor control is supported, indicates the queue position.
RegistrationRequest - Identifies the type of registration request (e.g., register, re-register, de-register).
RegistrationOutcome - Identifies success or failure of registration and the failure reason.
RTP_Setting – The IP address and the port number at the PTC Server for the RTP Session.
Salt - Include to provide the initial salt value if the cipher requires a salt value.
SDP – Answer, offer and SDP parameter negotiations. Report when known.
SIP_message_header - Answer, offer and SIP parameter negotiations. Report when known.
TalkburstControl_Setting – The offered Talk Burst Control Protocol, e.g., Talk Burst parameter(s) and the port numbers. Provide when Pre-established session is established.
TargetIdentity - The PTC identifier for the PTC Intercept Target.
TargetPresenceStatus - PTC-related presence information of the PTC intercept target.
Talk_burst_priority - If more than one level of priority is supported, indicates the talk burst priority level of the PTC Client.
Talk_burst_reason_code – Identifies the reason code for the denial or revoke of a talk burst.
TBCP_Deny - Indicates that the PTC Server has notified a PTC Client that it has been denied permission to send a Talk Burst.
TBCP_Granted - Indicates that the PTC Server has notified the PTC Client that it has been granted permission to send a Talk Burst.
TBCP_Idle - Used by the PTC Server to notify all PTC Clients that no one has the permission to send a Talk Burst at the moment and that it may accept the TBCP Talk Burst Request message.
TBCP_Queued - Indicates the request to talk is queued, if queued floor control is supported. Include identification of the PTC Client that has the queued Talk Burst, if known.
TBCP_Release - Indicates the request to talk has completed.
TBCP_Request - Indicates that the PTC Client has requested permission from the PTC Server to send a Talk Burst.
TBCP_Revoke - Indicates that the PTC Server has revoked the media resource from a PTC Client and can be used for preemption functionality, but is also used by the system to prevent overly long use of the media resource.
TBCP_Taken - Indicates that the PTC Server has notified all PTC Clients, except the PTC Client that has been given permission to send a Talk Burst, that another PTC Client has been given permission to send a Talk Burst.

21.3.4.2 CC Event Elements

The following event information is sent to the DF3 when CC is authorized for delivery. The following events are applicable to both the PoC and MCPTT service ICE.

Table 21.3.4.2: CC Information Elements

Observed IMEI - The provisioned International Mobile Equipment Identity target identity.
Observed SIP URI - The provisioned target identity can be a SIP URI
Observed TEL URI - The provisioned target identity can be a TEL URI
MCPTT ID - Mission Critical Push To Talk identity.
Event Date - Date of the event generation in the PTC Server or Client.
Event Time - Time of the event generation in the PTC Server or Client
Event Type - Description of which type of event is delivered: PTC Communication Content (CC).
Network Element Identifier - Unique identifier for the network element reporting the event.
PTC group ID - The PTC group ID of the group on which the call is initiated.
MCPTT group ID - The Mission Critical Push To Talk group Identity.
PTCSessionInfo - Provides PTC Session information such as PTC Session URI, PTC Session type, and Nickname.
PTCCorrelationId - Uniquely identifies the PTC Session, correlates CII messages, and correlates CII and CC messages.
PTC Location – Indicates the location of the target (if authorized)
Time of Location - Date/Time of location. The time when location was obtained by the location source node.
PTC CC Payload – The intercepted communications content encapsulated packet of a PTC session.

21.4 PTC Surveillance Events

21.4.0 PTC General

PTC Service events defined below are using the PTC Surveillance Events from Table 21.3. 4.1. These events are deliverable for either type of service provided by the SP, i.e. PoC or MCPTT.

21.4.1 PTC Service Registration

The PTC Service Registration event occurs when the target registers, re-registers, or deregisters for a PTC service, regardless of whether it is successful or unsuccessful.

Table 21.4.1: PTC Service Registration

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event Type
Event Time
Event Date
Network Element Identifier
Any other IMPU or IMPI of the target (if available)
RegistrationRequest
RegistrationOutcome

21.4.2 PTC Serving System

A PTC Serving System event is generated when there is a change to the SP serving the PTC target access network (i.e. for mobility).

Table 21.4.2: PTC Serving System

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
Serving System Address (AVP name such as Visited-PLMN-Id)
Any other IMPU or IMPI of the target (if available)

21.4.3 PTC Session Initiation

A PTC Session Initiation event occurs when the PTC target initiates a session or the target receives an invitation to join a session regardless of the success or the final disposition of the invitation.

Table 21.4.3: PTC Session Initiation

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
PTCHost
PTCOriginatingID
PTCParticipants
AssociatePresenceStatus
Location
Time of Location
InitationCause
BearerCapability

21.4.4 PTC Session Abandon

The PTC Session Abandon event is triggered when the PTC Session is not established and the request is abandoned before the PTC Session established end to end connectivity.

Table 21.4.4: PTC Session Abandon

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCorrelationID
PTCSessionInfo
TargetIdentity
PTCOriginatingId
PTCParticipants
AssociatePresenceStatus:
Location
Time of Location
AbandonCause

21.4.5 PTC Session Start

This event occurs when a PTC Session (e.g. One-to-One, One-to-Many, or One-to-Many-to-One) is answered, and voice communication begins. The PTC client may use the pre-established session for PTC session Start.

Table 21.4.5: PTC Session Start

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
PTCOriginatingId
PTCParticipants
AssociatePresenceStatus:
Location
Time of Location
BearerCapability

21.4.6 PTC Session End

The PTC Session End event occurs when the PTC Session is released for any reason (i.e. normal or abnormal release) and voice communications ends. The PTC client may use the pre-established session for terminating a PTC session.

Table 21.4.6: PTC Session End

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
PTCParticipants
Location
Time of Location
Cause

21.4.7 PTC Start of Interception

This event occurs when interception is started and there is an on-going PTC session.

Table 21.4.7: PTC Start of Interception

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
PTCOriginatingID
PTCHost
PTCParticipants
BearerCapability
Correlation information

21.4.8 PTC Pre-Established Session

This event occurs when a pre-established session is setup between the PTC service client present within the target's UE and the PTC server associated with the PTC client. The PTC client may use the pre-established session for originating

or terminating calls after pre-established session establishment, regardless of whether the PTC target is actively transmitting or receiving talk bursts.

Table 21.4.8: PTC Pre-Established Session

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
TargetIdentity
PTC_Server_URI
RTP_Setting
PTC_Media_Capability
PreEstablishSessionId
PreEstablishedStatus
TalkburstControl_Setting
MediaStream_Availability
Location
Time of Location
BearerCapability
Correlation information

21.4.9 PTC Instant Personal Alert

This event occurs when an Instant Personal Alert (i.e. a request for one PTC subscriber to initiate a PTC Session at a later time) is initiated or sent to the PTC target.

Table 21.4.9: PTC Instant Personal Alert

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
TargetIdentity
IPAPartyIdentity

21.4.10 PTC Party Join event

This event occurs when a request to join (or re-joins) a PTC Group Session (i.e. Chat Group) that is already in progress is received from the PTC target.

Table 21.4.10: PTC Party Join event

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationId
PTCSessionInfo
TargetIdentity
Inviting_PTC_user
Join_PTC_user
AssociatePresenceStatus
BearerCapability

21.4.11 PTC Party Drop

This occurs when the target is a participating member of a PTC Group Session and leaves the PTC Session in which the PTC target is also participating.

Table 21.4.11: PTC Party Drop

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
Party_Drop
AssociatePresenceStatus:

21.4.12 PTC Party Hold

A PTC Party Hold event occurs when the target places an on-going PTC Session on hold in on-going PTC Session.

Table 21.4.12: PTC Party Hold

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
Hold_ Indication
Hold_User

21.4.13 PTC Party Retrieve

A PTC Party Retrieve event occurs when the target retrieves an on-going PTC Session.

Table 21.4.13: PTC Party Retrieve

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
Retrieve_Indication
Retrieve_User

21.4.14 PTC Media Modification

During the PTC Session, a PTC Client may modify the voice frame packetization or voice codec mode by Out-of-band signalling using SDP payload within SIP messages. The Media Modification event is generated when a re-negotiation of the media parameters occurs during a PTC Session involving the target MS.

Table 21.4.14: PTC Media Modification

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTCCorrelationID
PTCSessionInfo
TargetIdentity
BearerCapability

21.4.15 PTC Group Advertisement

This event is generated when a PTC Intercept Target sends Group Advertisement information to a single PTC user, a list of PTC users or to all members of the Group using the Group Identity.

Table 21.4.15: PTC Group Advertisement

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
TargetIdentity
Group_Identity
Group_Ad_Sender
Group_Ad_Receiver
PTCHost
Group_Characteristics

21.4.16 PTC Floor Control

Floor Control arbitrates requests from the PTC Clients for the right to send media (i.e. the right to speak). Note, the term “Floor Control” is used to mean the same as term “Talk Burst Control”. When the PTC target is participating in a PTC Session, a Floor Control event is generated when the target requests to speak (e.g., presses the PTT mechanism) or the target is given permission to speak in response to a request (e.g. the network responds positively to the PTC

Subscriber's request) or is refused the request to speak and when the target is finished speaking (e.g. the PTC Intercept target releases the PTT mechanism).

Table 21.4.16: PTC Floor Control

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
TargetIdentity
PTCCorrelationID
PTCSessionInfo
FloorActivity Choice of: TBCP_Request TBCP_Granted TBCP_Deny TBCP_Queued TBCP_Release TBCP_Revoke
FloorSpeakerIdentity
Queued_FloorControl
Queued_Position_Status
Max_TB_Time
Talk_burst_priority
Talk_burst_reason_code

21.4.17 PTC Target Presence

If the Presence functionality is supported by the PTC Server and the PTC Server assumes the role of a Presence Source, this event is generated when the PTC Server publishes network presence information to the Presence server on behalf of PTC target.

Table 21.4.17: PTC Target Presence

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
TargetIdentity
TargetPresenceStatus

21.4.18 PTC Associate Presence

This event is generated when the PTC Server receives presence status notifications from the Presence Servers after having subscribed to the PTC presence status of other PTC Clients (i.e. Associates of the PTC Intercept target).

Table 21.4.18: PTC Associate Presence

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
TargetIdentity
AssociatePresenceStatus:

21.4.19 PTC List Management Events

This event is generated when the target PTC Client attempts to change their own contact list or their own PTC Group list(s). This event is also generated when the network notifies the Intercept target's PTC Client of changes made to their PTC-specific documents stored in the network (i.e. contact lists or PTC Group lists).

Table 21.4.19: PTC List Management Events

Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
SIP message header offer
SIP message header answer
SDP offer
SDP answer
TargetIdentity
ListManagementType Choice of: ContactListManagementAttempt GroupListManagementAttempt ContactListManagementResult GroupListManagementResult Request unsuccessful
ListManagmentAction Choice of: Create Modify Retrieve Delete Notify
Contact_Identity
Group_Identity
PTCHost
List_ManagementFailure

21.4.20 PTC Access Policy event

This event is generated when the PTC Intercept target attempts to change the access control lists (e.g. PTC user access policy and PTC Group authorization rules). In addition this event is generated when the network responds to a

modification or query by the PTC Intercept target to the access control lists (e.g. PTC user access policy and PTC Group authorization rules).

Table 21.4.20: PTC Access Policy event

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
TargetIdentity
Access_Policy_Type Choice of: PTCUserAccessPolicyAttempt GroupAuthorizationRulesAttempt PTCUserAccessPolicyQuery GroupAuthorizationRulesQuery PTCUserAccessPolicyResult GroupAuthorizationRulesResult Request unsuccessful
PTCUserAccessPolicy Choice of: Allow_Incoming_PTC_Session_request Block_Incoming_PTC_Session_request Allow_Auto_Answer_Mode Allow_Override_Manual_Answer_Mode
GroupAuthorizationRules Choice of: Allow_Initiating_Conference Block_Initiating_Conference Allow_Joining_Conference Block_Joining_Conference Allow_Add_Participants Block_Add_Participants Allow_Subscription_Conference_State Block_Subscription_Conference_State Allow_Anonymity Forbid_Anonymity
Contact_Identity
Group_Identity
PTCHost
Access_PolicyFailure

21.4.21 PTC Media Type Notification

This event is generated for media detected at the ICE for media types other than PTC speech (e.g. video, images, text, and files) directed to/from the targets PTC client. Media Types are either real-time or non-real time, i.e., Audio (e.g. music), Video Discrete Media (e.g. still image, formatted and non-formatted text, file), or Real Time Streaming Media (RTSP). Media parameters are SIP/SDP based information exchanged between the PTC server and the targets PTC

client, between the PTC server and the PoC Box and between PTC servers that specify the characteristics of the Media for a PTC session being established or that already exists.

Table 21.4.21: PTC Media Type Notification

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
SIP message header offer
SIP message header answer
SDP offer
SDP answer
PTCCorrelationID
PTCSessionInfo
TargetIdentity
BearerCapability

21.4.22 PTC Encryption Message

The CSP shall provide the encryption method, specific parameters and the encryption keys to LE when a CSP service uses encryption that is provided or managed by the CSP.

The Encryption message is sent by the DF2 to the LEMF when there is a need to pass the decryption information associated with intercepted content. If rekeying is deployed, one or more new Encryption messages are sent coincident with the change in keys.

Table 21.4.22 Encryption Message Parameters

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event Type
Event Time
Event Date
CryptoContext
Cipher
Key
Salt
KeyEncoding
PTCOther

21.5 PTC Group Calls

21.5.1 General

A PTC Group Session supports a One-to-One, One-to-Many, or One-to-Many-to-One with the following events; Session initiation request/response, Session modification, joining/leaving, termination, voice communication begins, ends, or forced disconnected. When detected at the ICE, these events can originate from the targets PTC Client to the PTC Server or from the PTC Server to the targets PTC Client or PTC server to PTC Server on the behalf of the target.

21.5.2 Group Call Request

This event is generated when received at the PTC server serving the target or sent to the targets PTC client for a PTC Group Call request to join, rejoin, or release of the group call. This can be a Group Call Request event received at the

PTC Server serving the target from a separate PTC server (outside the SP architecture) to the target. This event would be generated for each instance as described.

Table 21.5.2: Group Call Request

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTC group ID
PTC ID list
SDP offer
SDP Answer
Floor Request
Broadcast indicator

21.5.3 Group Call Response

A Group Call Response event is generated upon sending a group call response to the target or received at the PTC Server from the target or on behalf of the target to a separate PTC server (outside the SP architecture).

Table 21.5.3: Group Call Response

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTC group ID
SDP answer

21.5.4 PTC Group Interrogate

This event is generated when a group interrogate request or a response is received at the PTC Server serving the target.

Table 21.5.4: Group Interrogate

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTC group ID
PTC ID list

21.6 MCPTT Priority Calls and Alerts Messages

21.6.0 Background

MCPTT emergency group calls are defined by TS 23.379 [3] and TS 22.179 [2]. Group calls are enabled in both on-network and off-network but interception of these events are at the on-network MCPTT Server serving the target. Off-

network MCPTT interception is for future study (FFS). If there are multiple events for or to the target for each of these separate events detected an event report is generated.

21.6.1 General

A MCPTT Emergency Group Session can support a One-to-One, One-to-Many, or One-to-Many-to-One with the following events; Group Call initiation request/response, Group Call Session modification, joining/leaving, termination, voice communication begins, ends, or forced disconnected, an Imminent Peril Group Call or alerts. When detected at the ICE, these events can originate from the targets MCPTT Client to the MCPTT Server or from the MCPTT Server to

the targets MCPTT Client or the targets serving MCPTT server to another domain MCPTT Server on the behalf of the target.

21.6.2 MCPTT Emergency Group Call

When the MCPTT Emergency Group Call Request or Response is detected at the MCPTT Server, it can originate from the targets MCPTT client or be sent to the targets MCPTT client from a MCPTT Group.

Table 21.6.2: Emergency Group Call

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
MCPTT group ID
Emergency indicator
Alert indicator
MCPTT group ID
MCPTT indicator
MCPTT CorrelationID
MCPTT Location
Time of Location

21.6.3 MCPTT Emergency Group Call Cancel

When a MCPTT Emergency Group Call Cancel is detected at the MCPTT Server, it can originate from the targets MCPTT client or towards the targets MCPTT client from a MCPTT Group.

Table 21.6.3: Emergency Group Call Cancel

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
Emergency indicator
Alert indicator
MCPTT group ID
MCPTT indicator
MCPTT CorrelationID
MCPTT Location
Time of Location

21.6.4 MCPTT Emergency Group Alert

When a MCPTT Emergency Alert Notification, Response, Request or Cancel is detected at the MCPTT Server, it can originate from the targets MCPTT client or towards the targets MCPTT client from a MCPTT Group.

Table 21.6.4: Emergency Group Alert

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
MCPTT group ID
Alert indicator
MCPTT Organization name
MCPTT CorrelationID
MCPTT Location
Time of Location

21.6.5 MCPTT Emergency Group State

When the MCPTT Emergency State Response, Request or Cancel is detected at the MCPTT Server, it can originate from the targets MCPTT client or to the targets MCPTT client from a MCPTT Group.

Table 21.6.5: Emergency Group State

Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
MCPTT group ID
Client emergency state inform (See NOTE)
Client emergency state response (See NOTE)
Client emergency state cancel inform (See NOTE))
Client emergency state cancel response (See NOTE)
Group emergency condition inform (See NOTE)
Group emergency condition response (See NOTE)
Group emergency condition cancel request (See NOTE)
Group emergency condition cancel response (See NOTE)
NOTE: At least one of these information elements shall be present

21.6.6 MCPTT Imminent Peril Group Call

When the MCPTT Imminent Peril Group Call Request, Response or Cancel is detected at the MCPTT Server, it can originate from the targets MCPTT client or to the targets MCPTT client from a MCPTT Group.

Table 21.6.6: Imminent Peril Group Call

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
MCPTT group ID
MCPTT Imminent peril indicator
MCPTT indicator
MCPTT CorrelationID
MCPTT Location
Time of Location

21.7 PTC Communication Content (CC)

21.7.0 General

When communication content (CC) delivery is authorized the CSP shall access and deliver communication content for the target for the duration of any of the different types of PTC sessions (i.e., One-to-One, One-to-Many, or One-to-Many-to-One, MCPTT or Private Calls). Any CC that are originated by, redirected by and terminated to the surveillance target's equipment, facilities, or service when the surveillance target is part of the PTC session or the target is connected to the PTC Session under surveillance shall be delivered to the DF3 as identified parameters in table 2.1.3.4.2.

21.7.1 Communication Content (CC)

The *Communication Content* event is used to encapsulate communications content packets for transfer over the interface to the DF3, in accordance with this standard.

Table 21.7.1: Communication Content

Observed SIP URI
Observed TEL URI
Observed IMEI
MCPTT ID
Event type
Event Time
Event Date
Network Element Identifier
PTC Group ID
MCPTT group ID
PTCSessionInfo
PTCCorrelationID
PTC Location
PTC CC Payload
Time of Location

22 Cell Supplemental Information Reporting

22.1 General

The LEAs, when location reporting is authorized, have a need to identify the geo-location or civic location of a cell site when only a Cell Identity is provided in IRI. When this Cell Identity is provided in the IRI for location, the CSP has an obligation to provide the specific Cell site information servicing the target. A Cell Site Reporting capability is an option for an operator to provide this supplemental cell site location information in automated fashion to the LEAs. Other means may be possible, e.g. the capability to send the all or selected sets of Cell Supplemental Information records directly to the LEMF on a one-way update at a time chosen by the operator, but are not specified here. The DF will be tasked to deliver a Cell Site Report (CSR) that is inclusive of the cell site information retained in a CSP Cell Database. It is assumed that the source of information for this comes from CSP network engineering and network planning facilities.

When a Cell Identity is encountered in the IRI being reported to the LEA, the CSP may consult internal network records and assemble the geo-location or civic location information, and add this supplemental cell information to the IRI being reported to the LEA, if the IRI event has been sent to the LEMF the DF will generate a CSR.

22.2 Cell Site Report Delivery

The report process is initiated when a DF determines a Cell Identity is contained in an IRI event and when location reporting is authorized.

If the specific Cell supplemental information has not been sent for the interception in the IRI event, the DFs reporting process will produce a report called CSR for the Cell Identity reported in the IRI and forward this report to the LEA.

If the Cell supplemental information for the current Cell Identity has been previously sent for the interception, based on operator policy, the CSR delivery process shall be able to assume that the LEA has retained the Cell supplemental information and not resend this Cell supplemental information. When the Cell Identity changes, during the session for whatever reason, and this new cell supplemental information has changed from what was previously sent for the

interception, the new Cell site information shall be reported in the location parameter of the new IRI event or a new CSR report based on operator policy will be sent to the LEMF.

22.3 LI_CELL_INFO Interface

The LI_CELL_INFO interface is implementation specific between the DF2 and the source(s) of operator's cell site information regarding the PLMN. The source(s) of this cell site information may be consulted to produce the CSR. The details of this interface are outside the scope of this specification.

22.4 Cell Site Report

Once the Cell site is identified and operator specific cell site information source(s) consulted the DF shall add appropriate cell location related elements within the database to the location parameter in the IRI event or provide the CSR. Once a Cell site is reported during a LI, the operator shall be able to assume that the LEA will retain the Cell site reports for the duration of the LI reportable session and redundant reports may be suppressed based on operator policy. The following parameters in Table 22.4.1 are considered as a high level view of information that can be reported as an example of a report to be sent to the MF/DF.

Table 22.4.1: Example Cell Site Report parameters

Parameter	MOC	Description
Cell Identity	M	The Cell Identifier as reported in IRI.
AlternativeID	C	If used by CSPs with an alternative naming scheme for cells.
Time Stamp	M	Shall include the Date and Time of the report.
OperatorID	O	Shall include the Operator ID.
Cell Azimuth	C	If known, to include the azimuth of the direction the antenna is pointing (in degrees).
Cell_LatAndLong	C	If known, the geo-position of the cell site (latitude and longitude).
Civic Address	C	If known, shall include the civic address of the cell site.
Other operator specific information	C	Based on operator policy, other information that is CSP specific can be reported as Carrier-specific information whose format is not standardized. If the CSP chooses to report Carrier-specific information the CSP shall provide LE with details of the structure of the information to allow LEA interpretation of the data.

Annex A (informative): Information flows for Lawful Interception invocation of circuit switched services

The following figures show the information flows for the invocation of Lawful Interception for various types of calls. The figures show some of the basic signalling messages of the target calls and the events on the X2 and X3-interfaces. The call control messages to and from the network are shown for informational purposes only; some of them may not be sent or may be combined in certain networks. The handling of the bearers for the basic calls is not shown. The bearer points are established in a manner to minimise content loss without delaying the call to the target. The bearer establishment to agency will be in parallel or immediately following the bearer establishment to the target. The flows portray both forward and backward bearer establishment and release to the agency.

A.1 Mobile originated circuit switched calls

Figure A.1 shows the interception of a basic mobile originated circuit switched speech or data call where the originating mobile (A) is the target for interception. B is not necessarily also a mobile subscriber and resides on a different exchange.

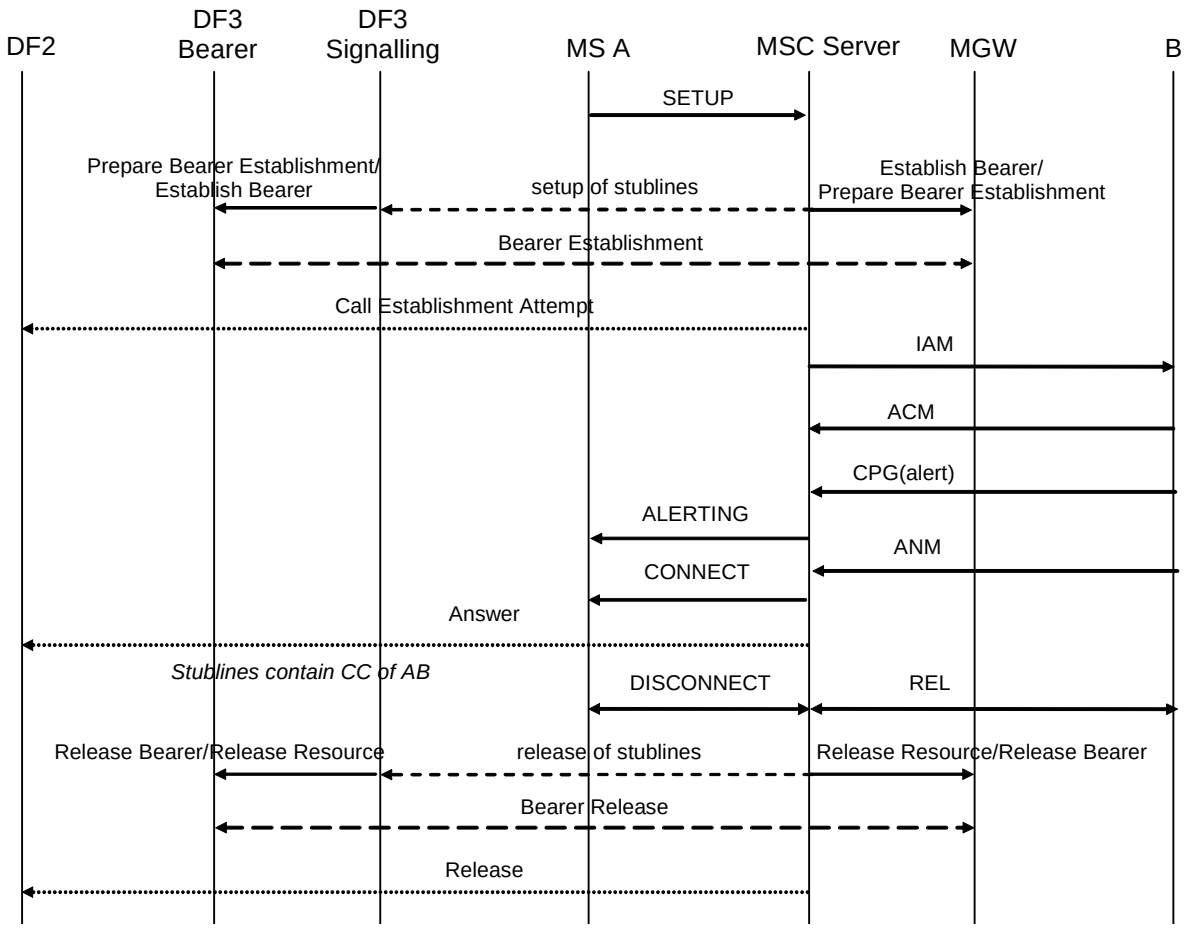


Figure A.1: Interception of mobile originated circuit switched calls

In figure A.1 the result (answer) of the set-up of the stublines is not shown. This assumes no special action is taken in case of failure.

A.2 Mobile terminated circuit switched calls

Figure A.2 shows the interception of a basic mobile terminated circuit switched speech or data call where the terminating mobile (B) is the target for interception. A is not necessarily also a mobile subscriber and resides on a different exchange.

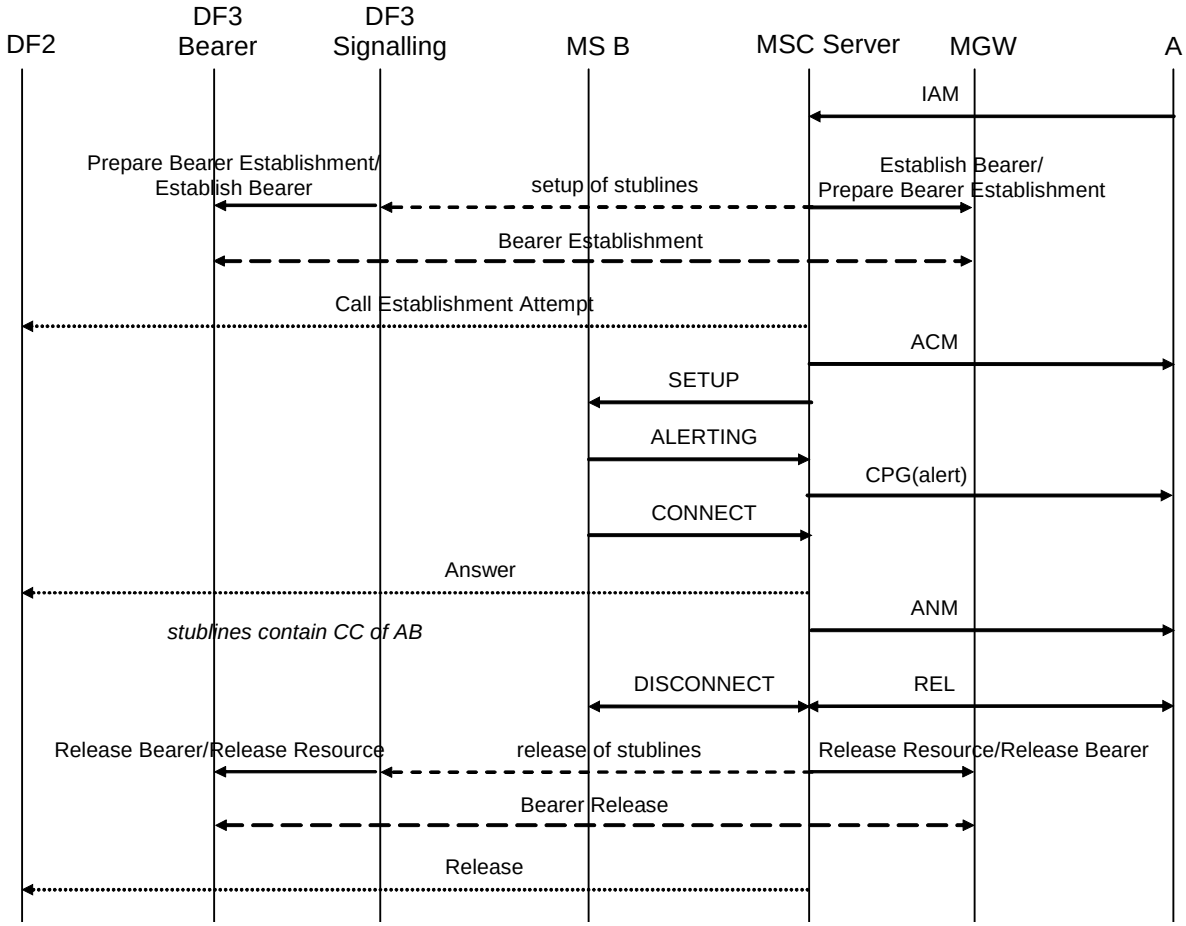


Figure A.2: Interception of mobile terminated circuit switched calls

A.3 Call hold / call waiting

Figures A.3 and A.4 show the interception of calls involving call hold / call waiting. Figure A.3 covers the case where one pair of stublines is used per target, figure A.4 covers the case where a separate pair of stublines is used for each target call. The mobile that receives the waiting call (A) is the target for interception.

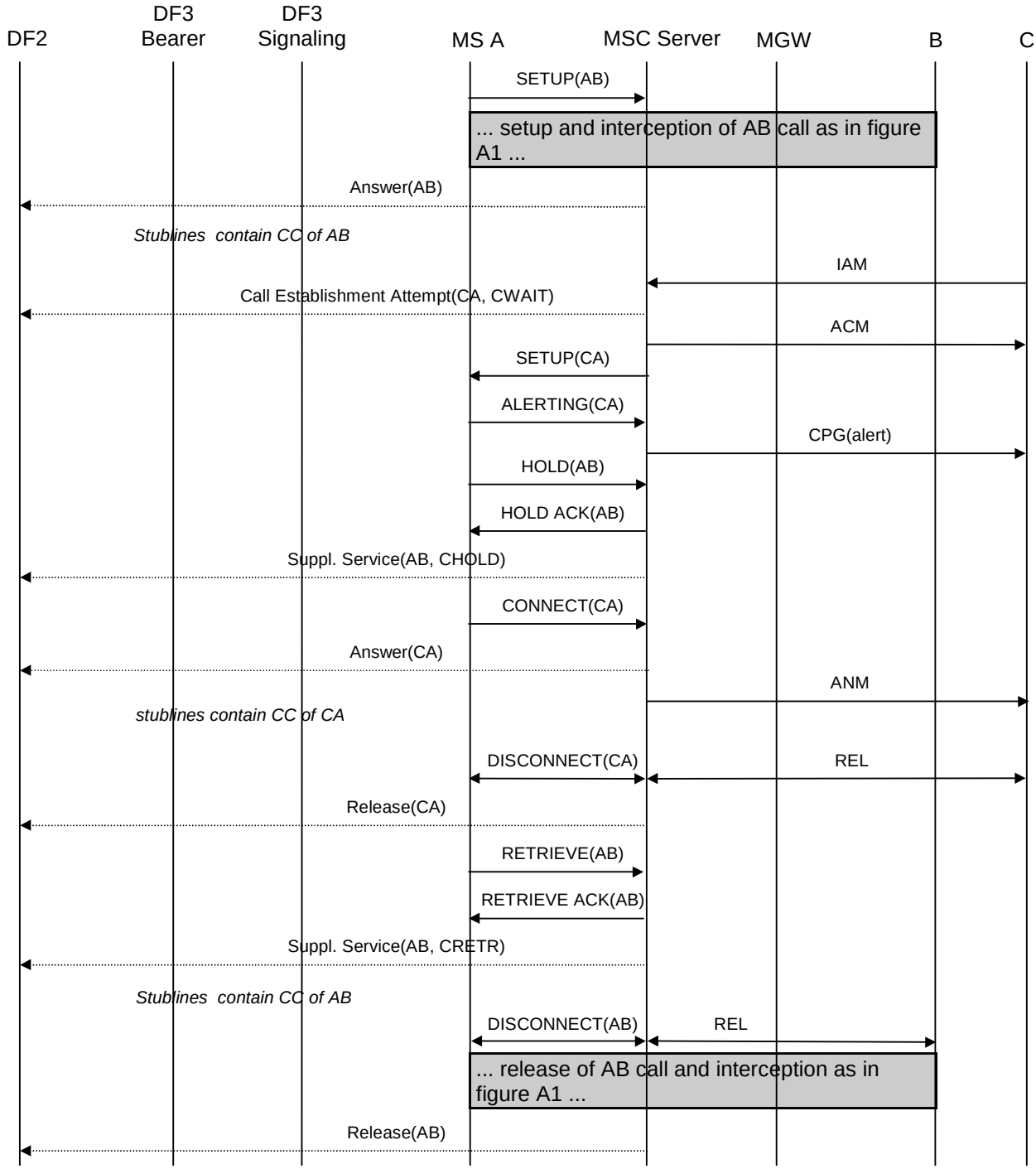


Figure A.3: Interception of call hold / call waiting - stublines per target

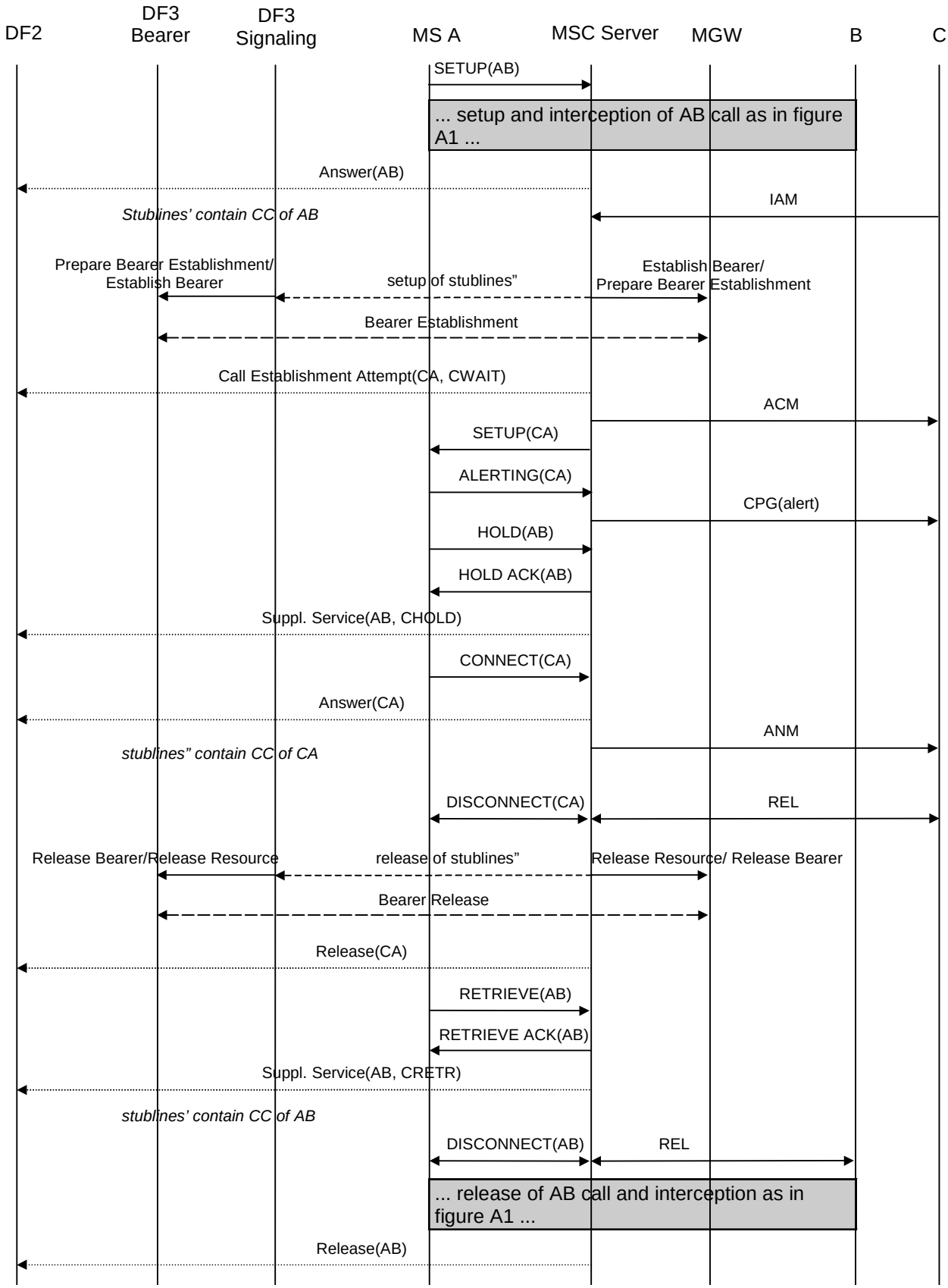


Figure A.4: Interception of call hold / call waiting - stublines per target call

A.4 Multiparty calls

Figures A.5 and A.6 show the interception of multiparty calls. Figure A.5 covers the case where one pair of stublines is used per target, figure A.6 covers the case where a separate pair of stublines is used for each target call. The mobile setting up the multiparty call (A) is the target for interception.

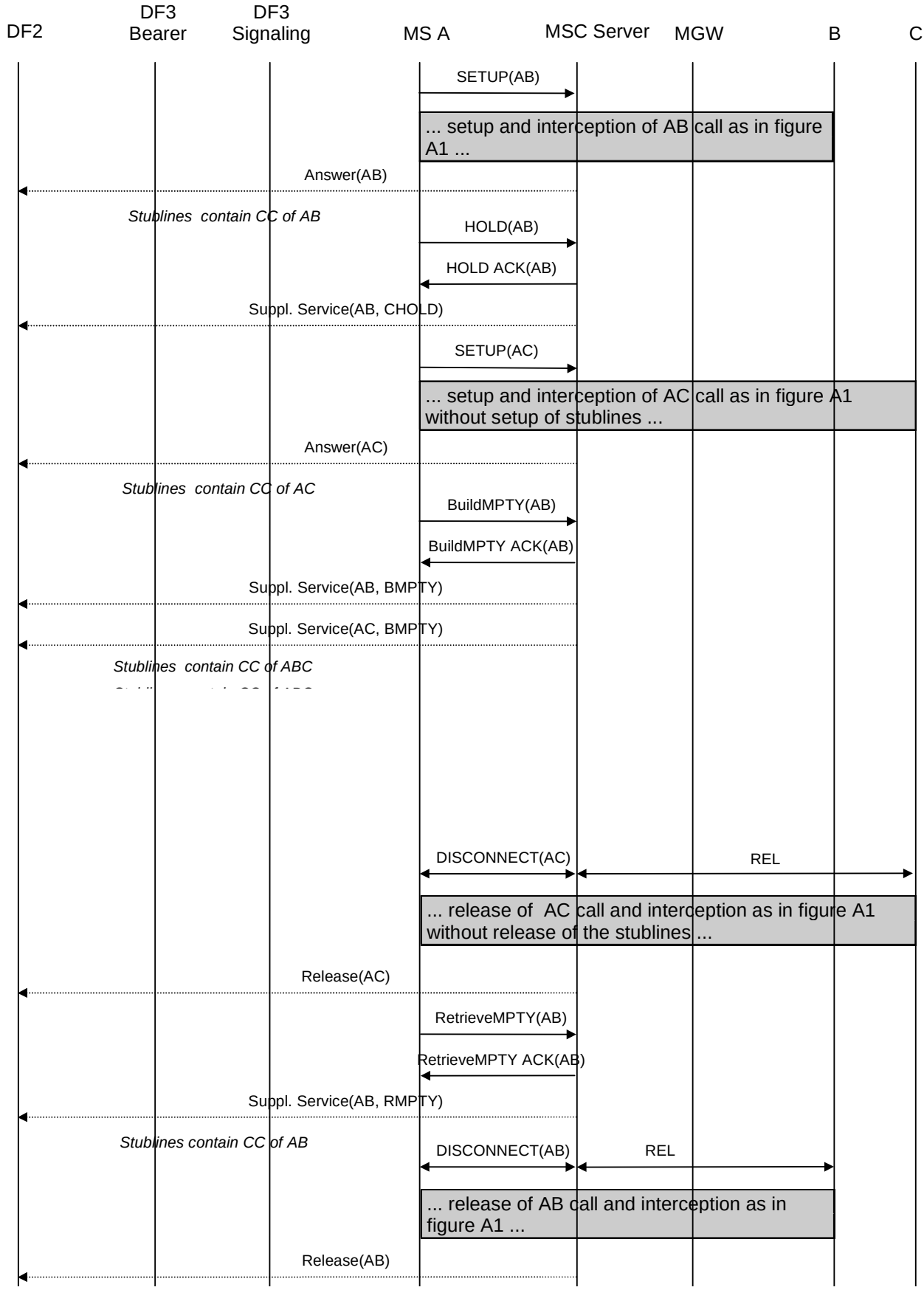


Figure A.5: Interception of multiparty calls - stublines per target

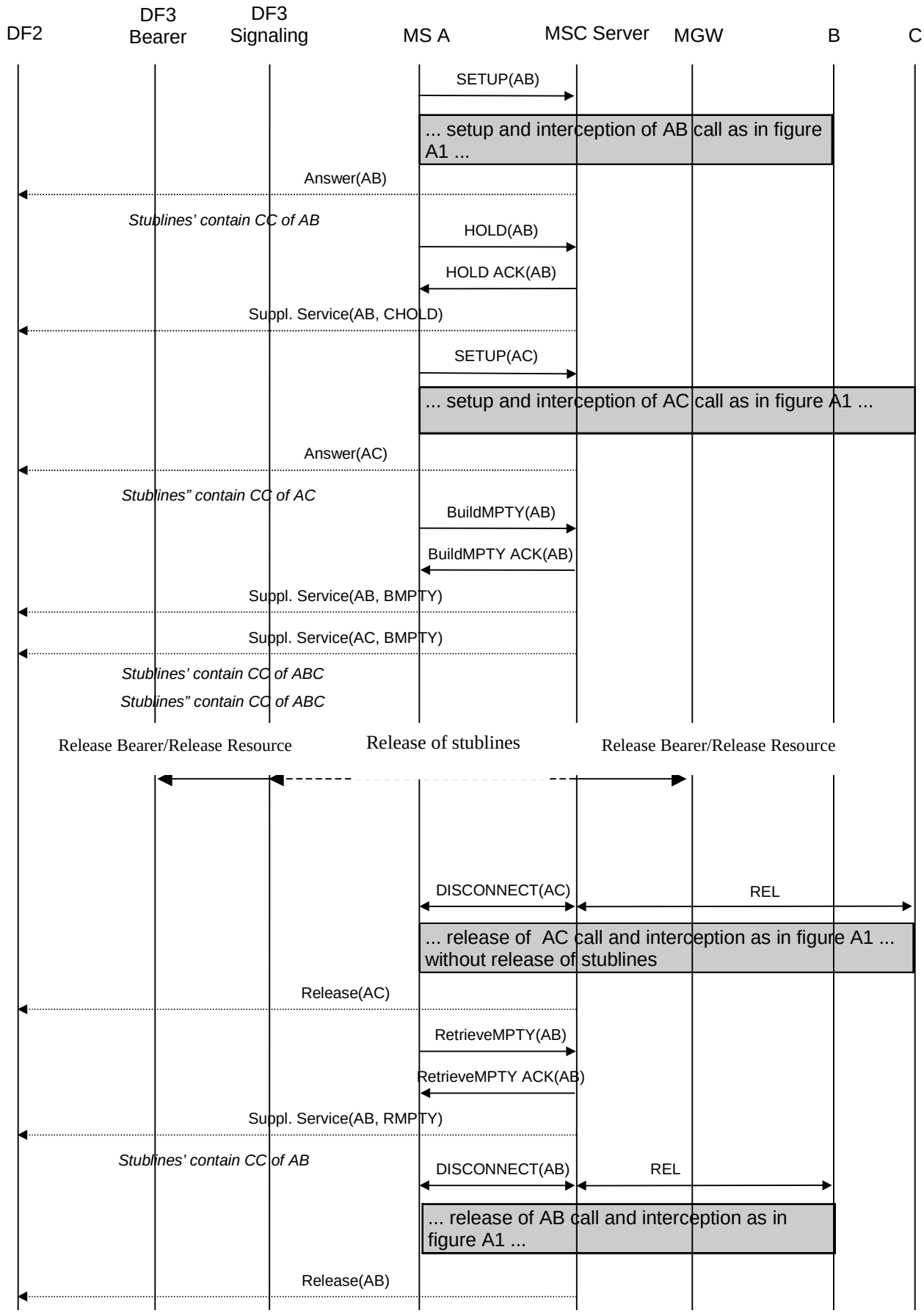


Figure A.6: Interception of multiparty calls - stublines per target call

A.5 Call forwarding / call deflection

A.5.0 General

The following pictures show the information flows for the interception of forwarded calls. Information flows will be given for three typical cases of call forwarding. All other types of call forwarding / call deflection are intercepted similar to one of these.

A.5.1 Unconditional call forwarding

Figure A.7 shows the interception of unconditionally forwarded calls. The mobile that activated unconditional call forwarding (B) is the target for interception. In this case interception will be performed at the 3G GMSC, where the Service Request Indicator (SRI) request for B is issued and subsequently the SRI response indicating that the call shall be forwarded is received.

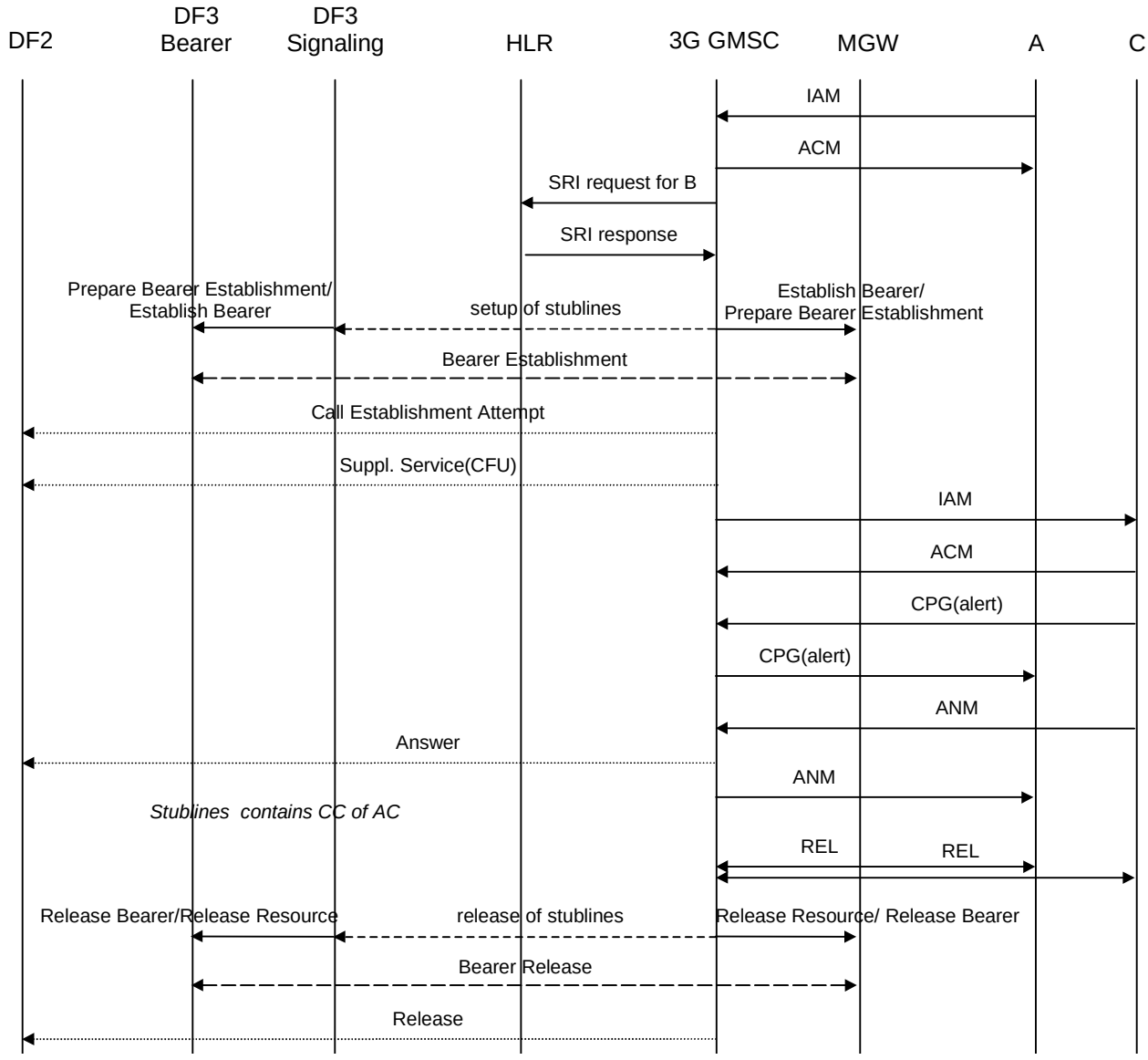


Figure A.7: Interception of unconditional call forwarding

A.5.2 Call forwarding on not reachable (IMSI detached)

Call forwarding on not reachable because the IMSI is detached is also handled on the 3G GMSC. Interception of this type of call forwarding is similar to interception of unconditional call forwarding.

A.5.3 Call forwarding on busy (network determined)

Figure A.8 shows the interception of call forwarding on busy (network determined). The mobile that activated call forwarding on busy (B) is the target for interception. In this case interception will be performed at the 3G MSC where B resides, where the busy condition is detected and the call is forwarded.

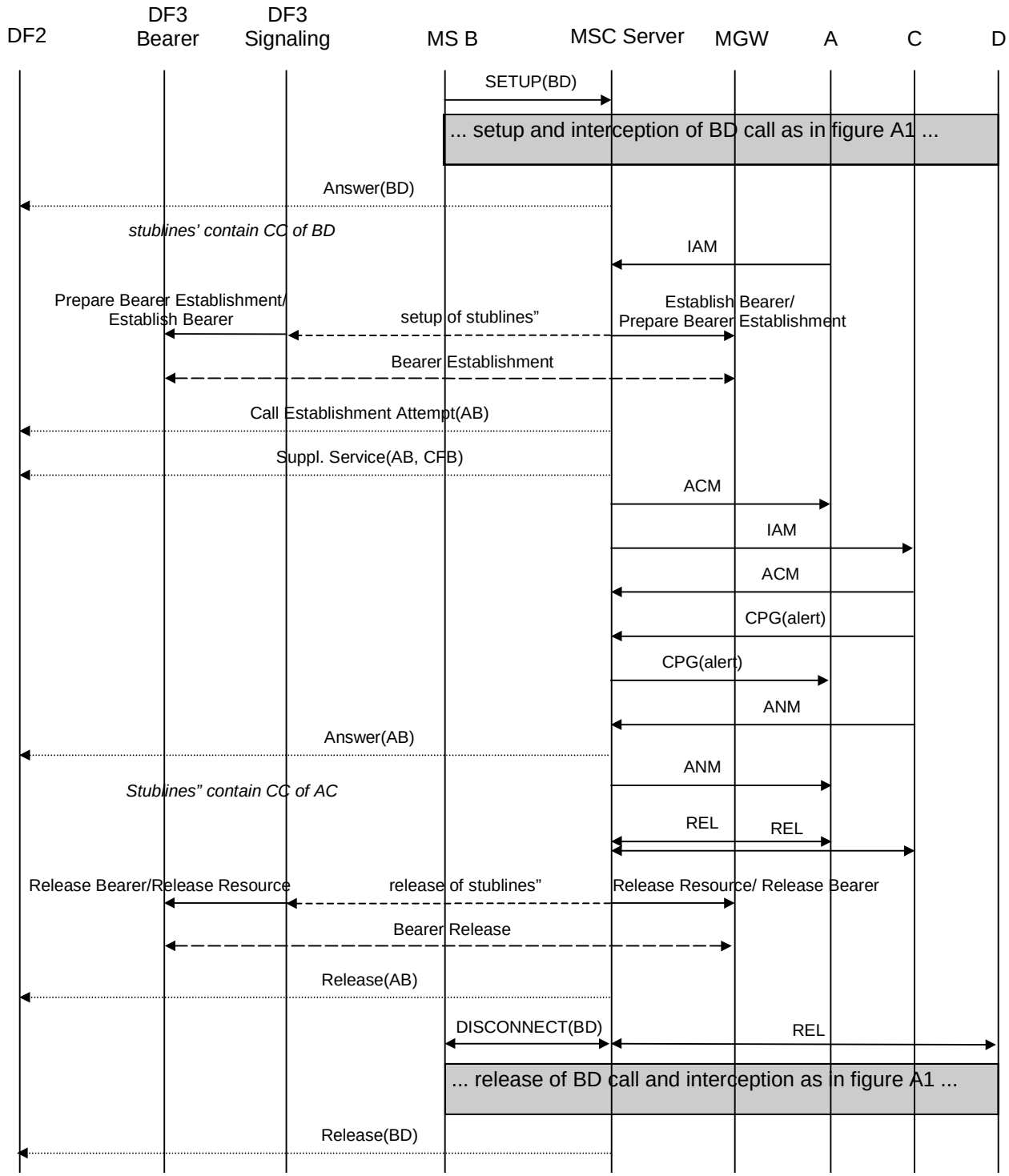


Figure A.8: Interception of call forwarding on busy (network determined)

A.5.4 Call forwarding on not reachable (no response to paging/radio channel failure)

Call forwarding on not reachable because of no response to paging or radio channel failure is also handled on the 3G MSC similar to call forwarding on busy (network determined). Interception of this type of call forwarding is therefore done in the same way (see clause A.5.3).

A.5.5 Call forwarding on no reply

Figure A.9 shows the interception of call forwarding on no reply. The mobile that activated call forwarding on no reply (B) is the target for interception. In this case interception will be performed at the 3G MSC where B resides, where the no reply condition is detected and the call is forwarded. Initially, the interception is similar to the interception of a basic mobile terminated circuit switched speech of data call. On no reply time-out, the interception will continue on the forwarded call to C.

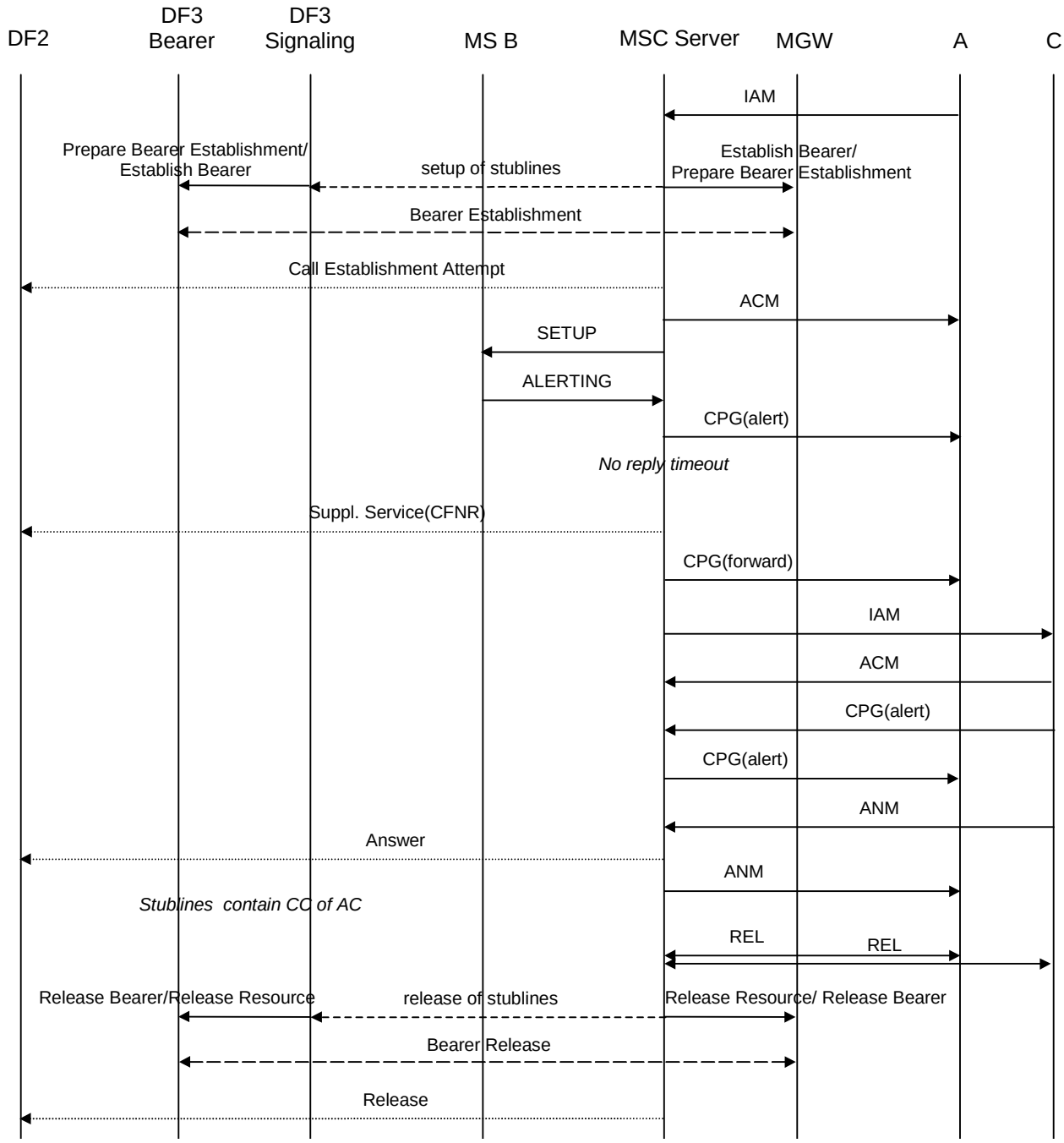


Figure A.9: Interception of call forwarding on no reply

In figure A.9 the release of the stublines is done after the forwarded call is released by A or C. It is a national option not to support interception of forwarded calls. In that case, the release of the stublines is done after the call is forwarded and B is no longer involved.

A.5.6 Call forwarding on busy (user determined)/call deflection

Call forwarding on busy (user determined) and call deflection are also handled on the 3G MSC similar to call forwarding on no reply. Interception of this type of call forwarding is therefore done in the same way (see A5.5).

A.5.7 Call waiting / call forwarding on no reply

Figures A.10 and A.11 show the interception of a call involving both call waiting and call forwarding on no reply. Figure A.10 covers the case where one pair of stublines is used per target, figure A.11 covers the case where a separate pair of stublines is used for each target call. The mobile that activated call forwarding on no reply and receives the waiting call (B) is the target for interception. In figure A.10 a new pair of stublines needs to be set up when the call is forwarded since the first pair of stublines is still used for the initial call.

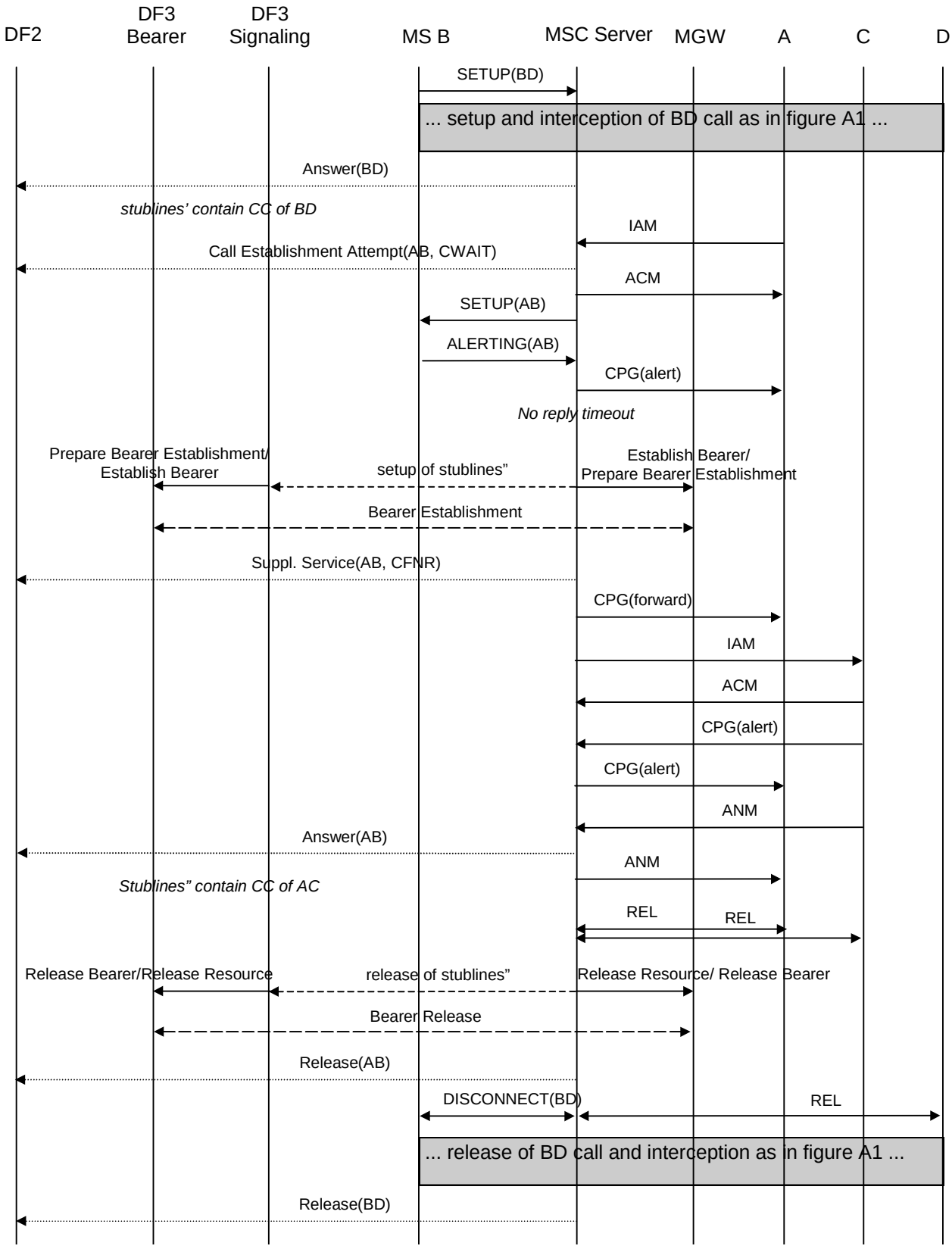


Figure A.10: Interception of call waiting / call forwarding on no reply - stublines per target

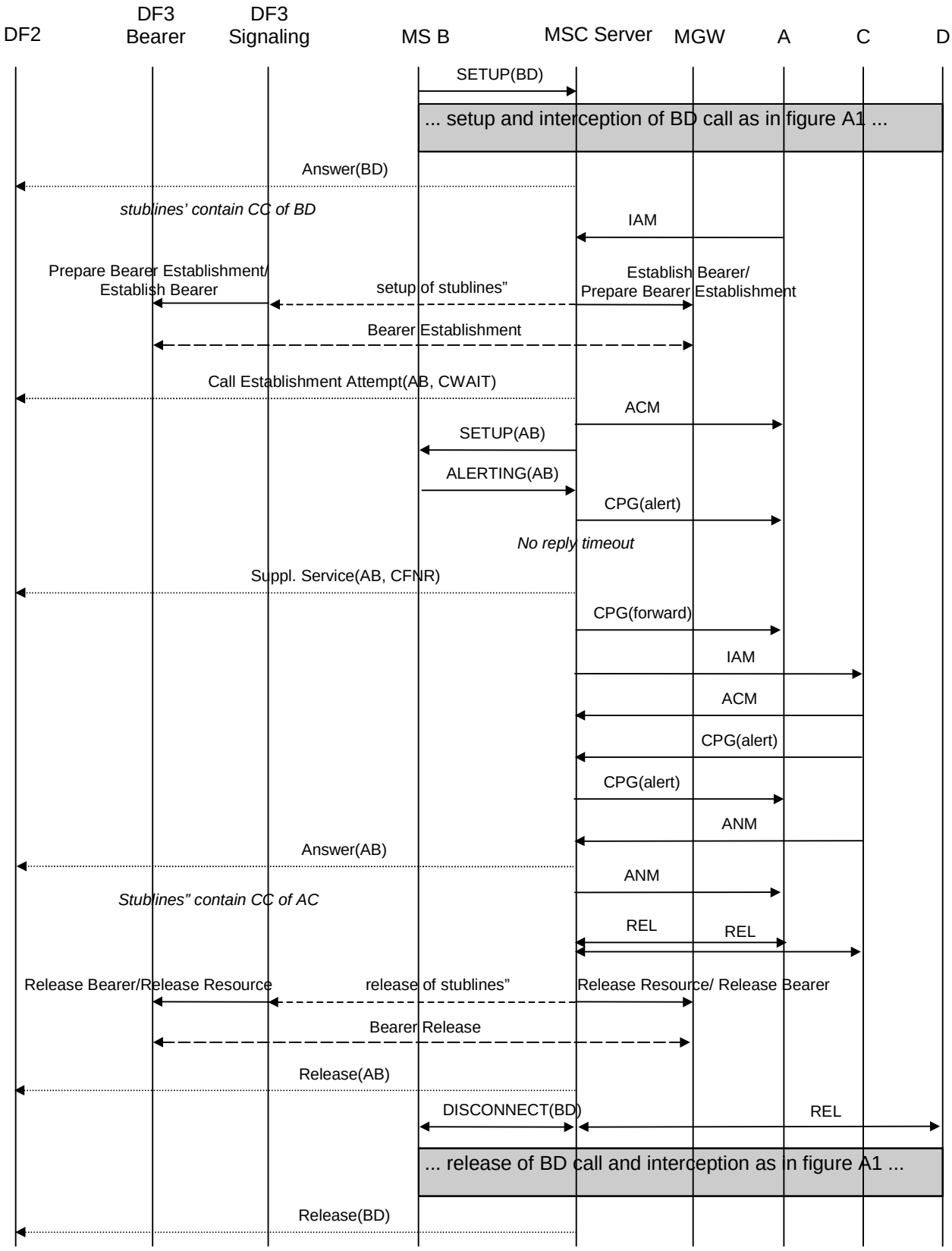


Figure A.11: Interception of call waiting / call forwarding on no reply - stublines per target call

A.6 Explicit call transfer

Figures A.12 and A.13 show the interception of explicit call transfer. Figure A.12 covers the case where one pair of stublines is used per target, figure A.13 covers the case where a separate pair of stublines is used for each target call. The mobile transferring the call (B) is the target for interception.

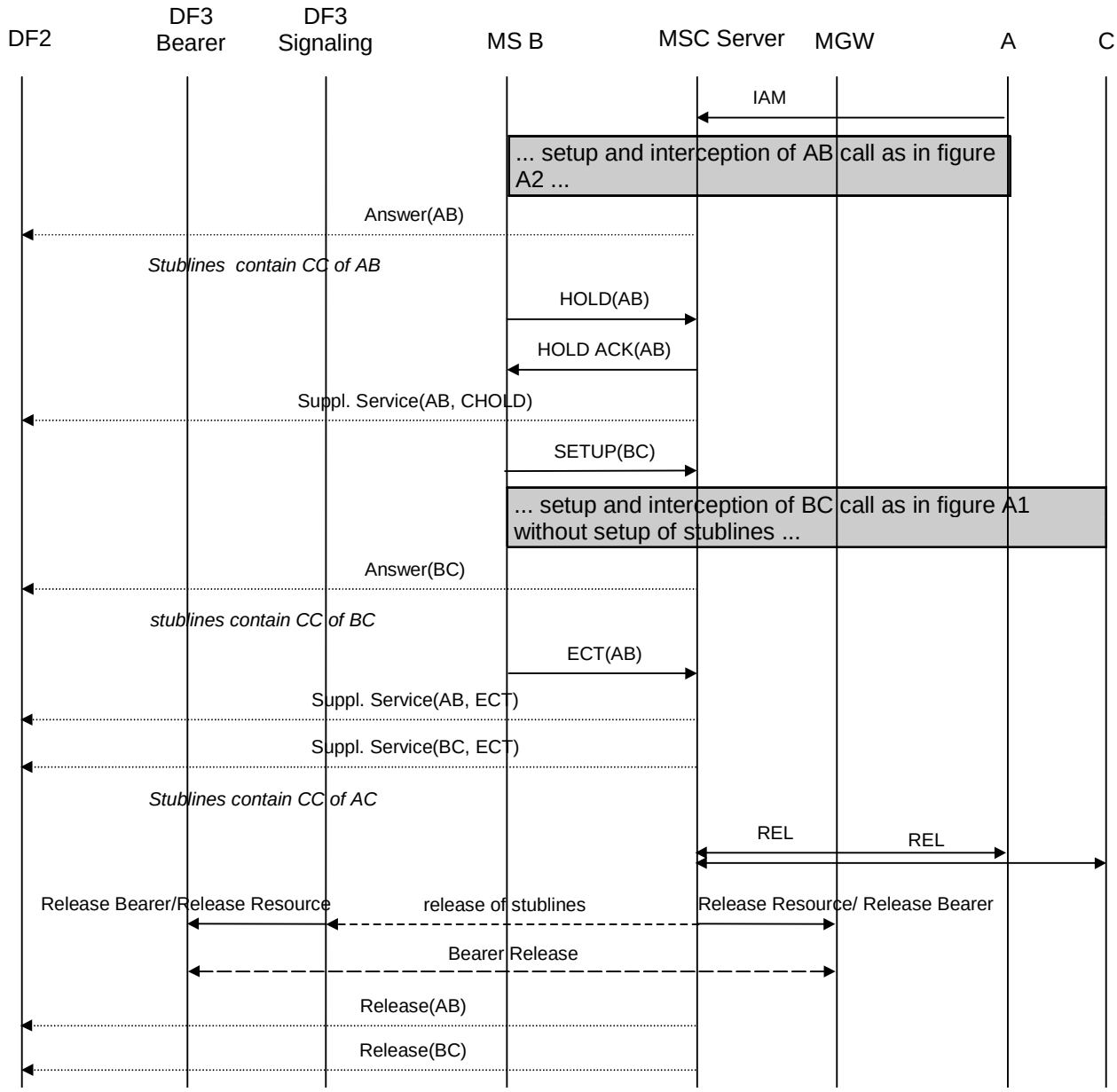


Figure A.12: Interception of explicit call transfer - stublines per target

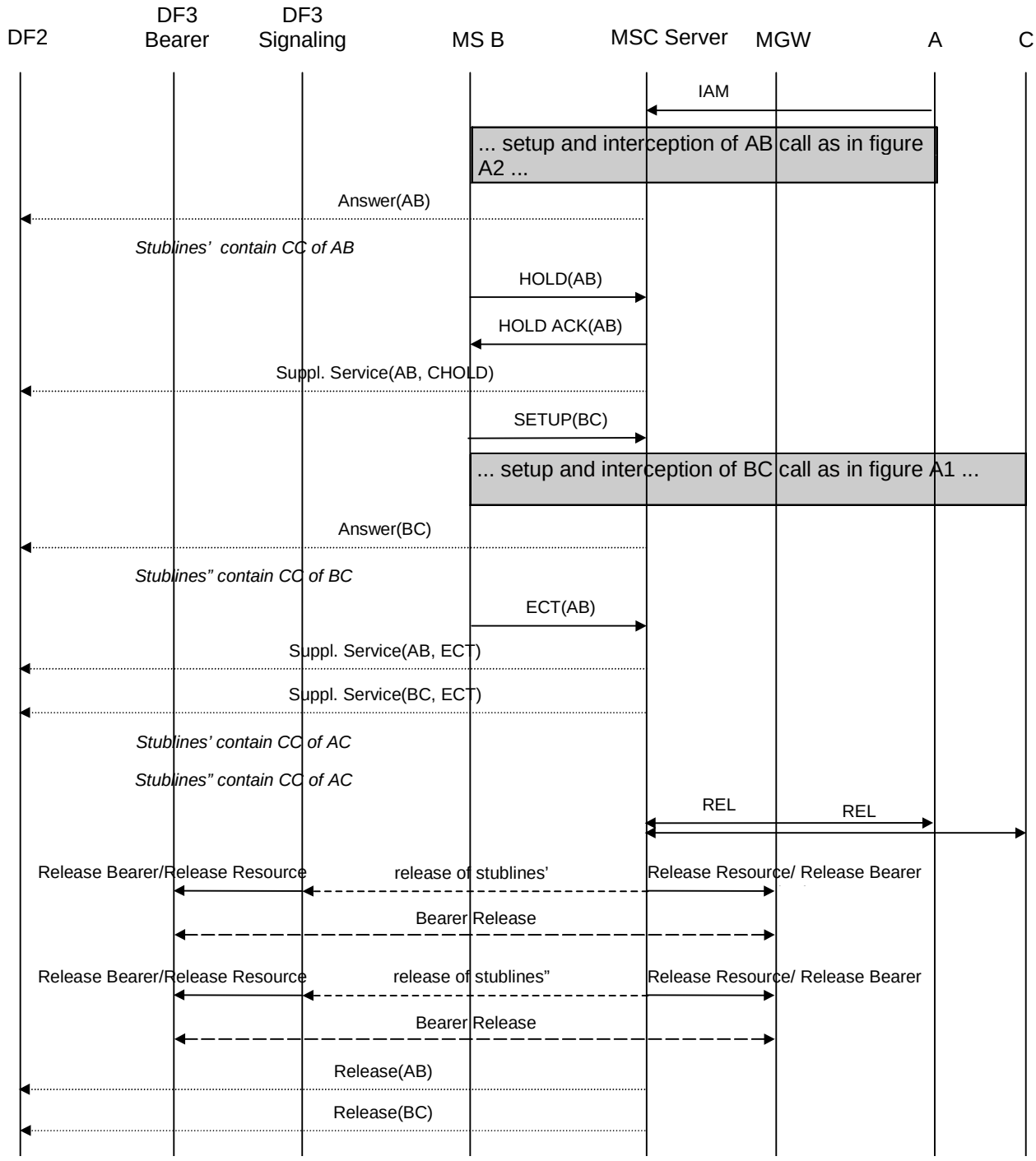


Figure A.13: Interception of explicit call transfer - stublines per target call

In figures A.12 and A.13 the release of the stublines is done after the transferred call is released by A or C. It is a national option not to support interception of transferred calls. In that case, the release of the stublines is done after the call is transferred and B is no longer involved.

Annex B (informative): Information flows for Lawful Interception invocation of GSN Packet Data services

B.0 General

The following figures show the information flows for the invocation of Lawful Interception for Packet Data and typical scenarios. The figures show some of the basic signalling messages of the target Packet Data communication and the events on the X2 and X3 interfaces. The dotted lines indicate signalling depending on whether CC and/or IRI information has been requested. The Gateway 3G GGSN may setup/release packet tunnels and send IRI information depending on national requirements.

The use of the Gateway 3G GGSN for interception is a national option.

B.1 Mobile Station Attach

Figure B.1 shows the interception of a basic Mobile Station Attach where the mobile (A) is the target for interception.

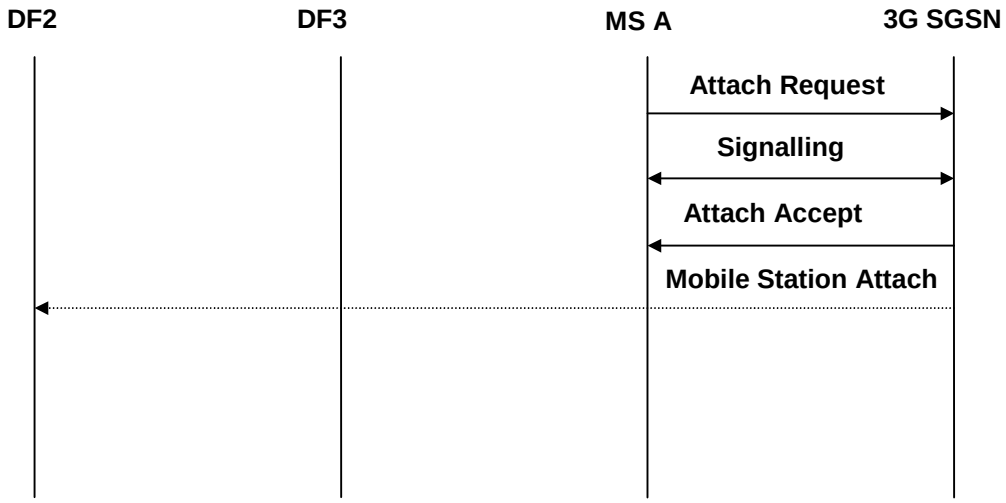


Figure B.1: Interception of mobile originated Mobile Station Attachment

B.2 Mobile Initiated Mobile Station Detach

Figure B.2 shows the interception of a Mobile Initiated Mobile Station Detach where the originating mobile (A) is the target for interception.

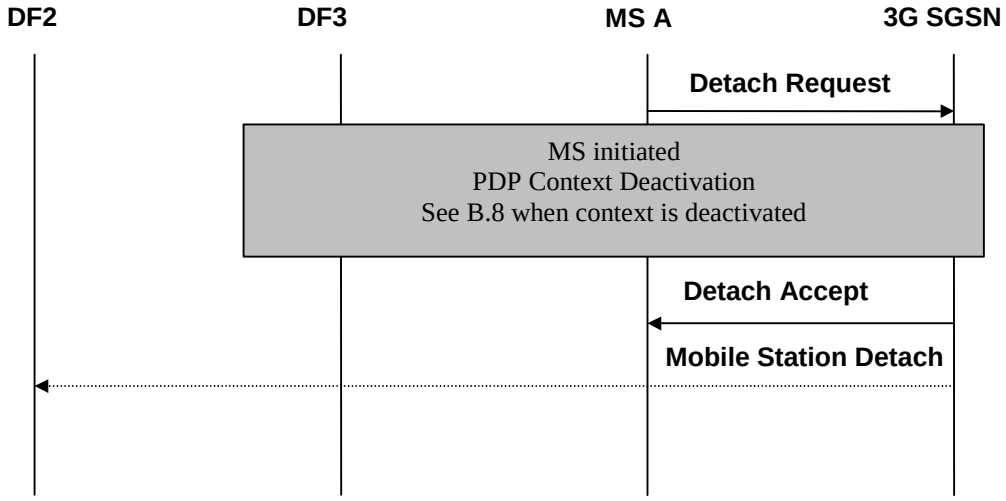
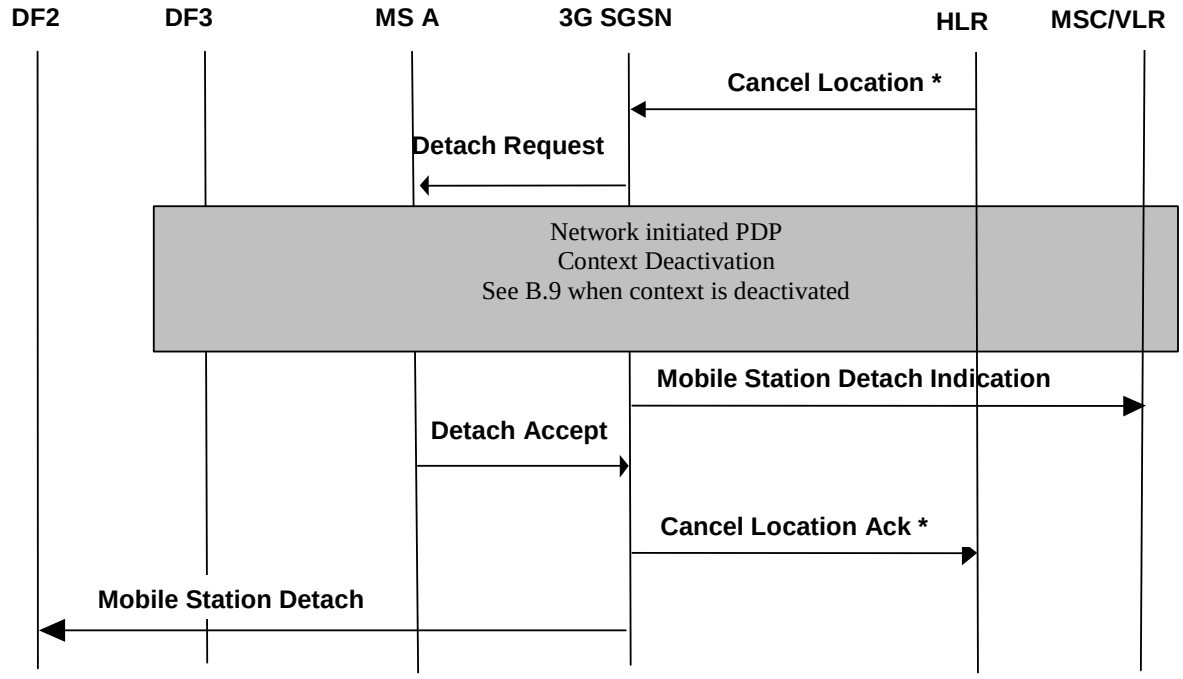


Figure B.2: Interception of mobile originated Mobile Station Detachment

B.3 Network initiated Mobile Station Detach

Figure B.3 shows the interception of a network initiated (by 3G SGSN or HLR) Mobile Station Detach where the mobile (A) is the target for interception.



NOTE: * Additional signals in case of HLR initiated.

Figure B.3: Interception of network initiated Mobile Station Detach

B.4 Intra 3G GSN Routing Area Update

Figure B.4 shows the interception of an Intra Routing Area Update where the mobile (A) is the target for interception. The sequence is the same for the combined RA / LA Update procedure but additional signalling is performed between the current 3G SGSN and the prior 3G SGSN before the Routing Area Update Accept message is sent to the MS.

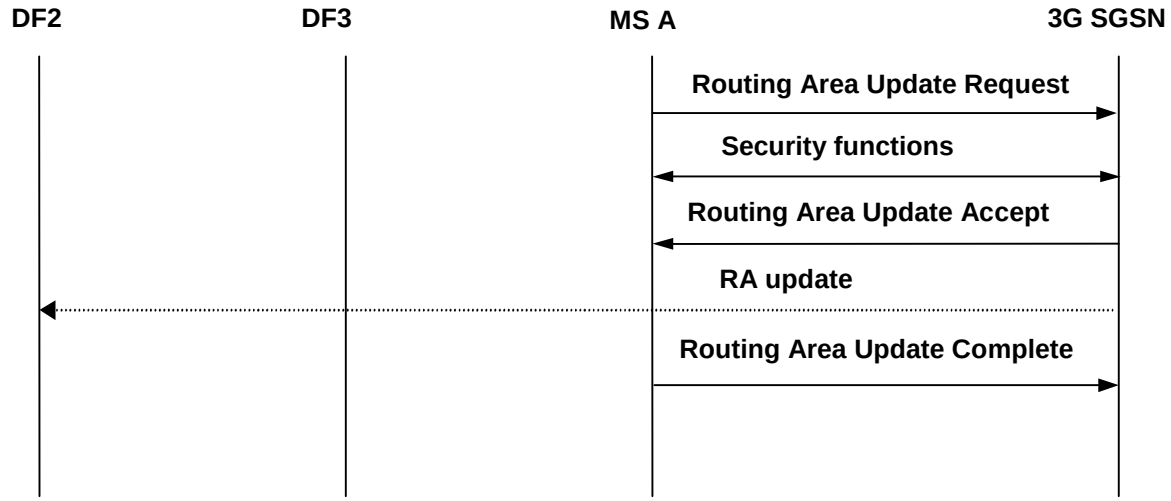


Figure B.4: Interception of an Intra Routing Area Update

B.5 Inter 3G GSN Routing Area Update

Figure B.5 shows the interception of an Inter Routing Area Update where the mobile (A) is the target for interception. The sequence is the same for the combined RA / LA Update procedure but additional signalling is performed between the 3G GSN, HLR and the old 3G GSN before the Routing Area Update Accept message is sent to the MS. In case of PDP context not being active less signalling is required.

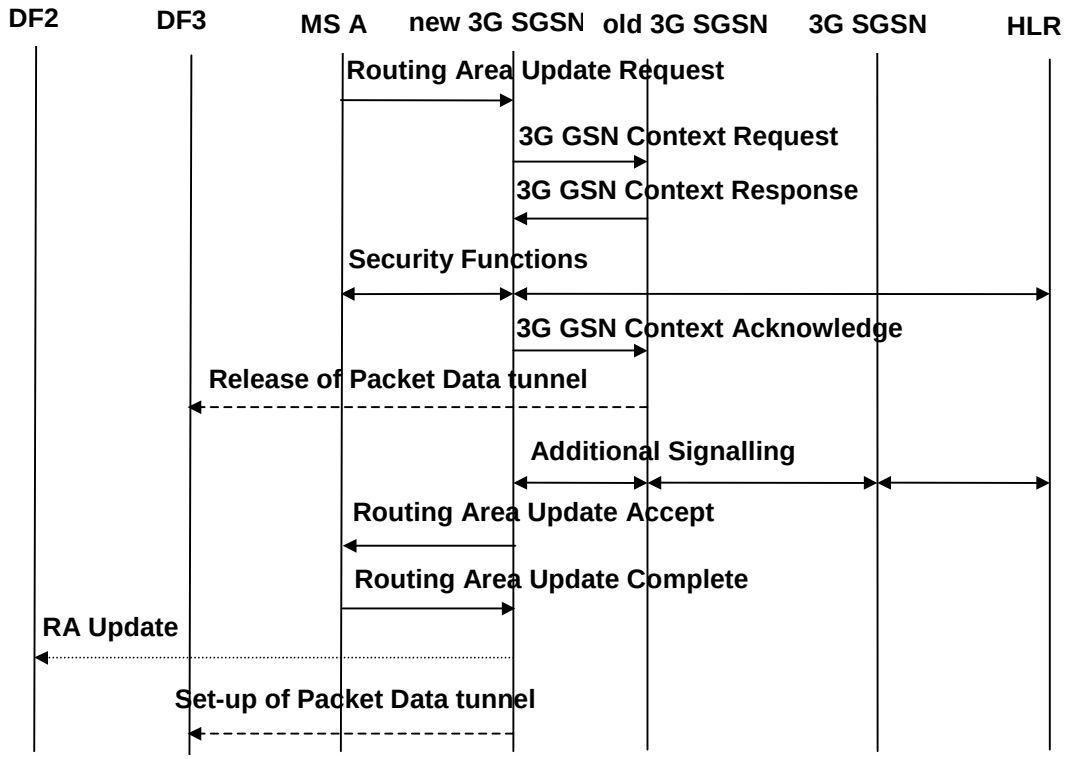


Figure B.5: Interception of an Inter Routing Area Update

B.6 PDP Context Activation

Figure B.6 shows the interception of a PDP Context activation where the mobile (A) is the target for interception. The sequence for a network initiated PDP Context activation is analogous but is preceded by the 3G GSN sending a Request PDP Context Activation to the MS.

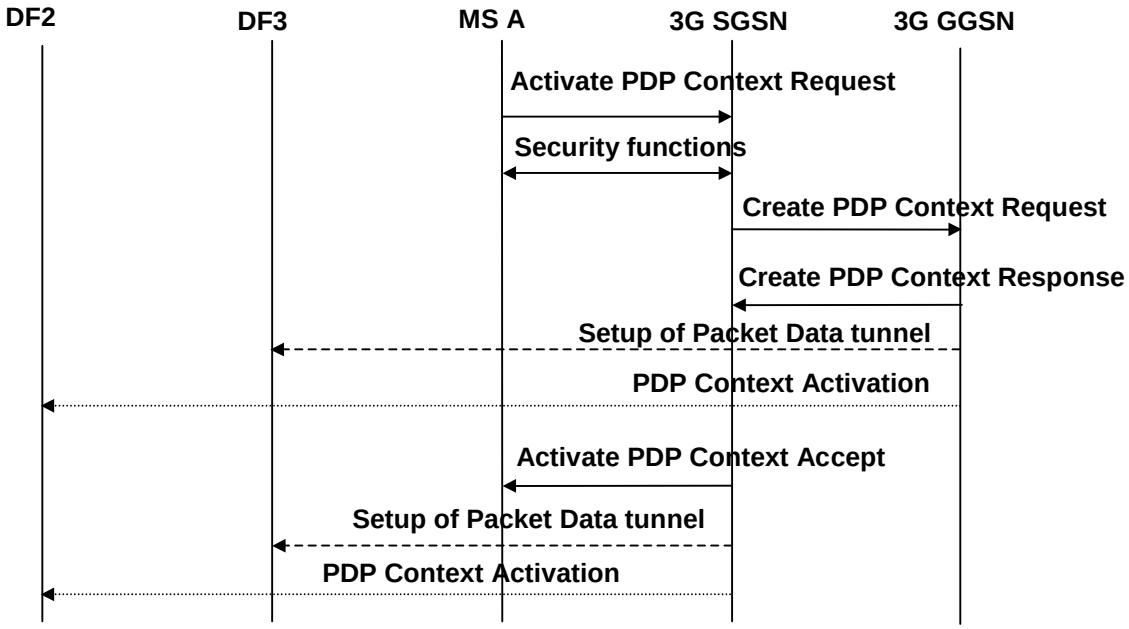


Figure B.6: Interception of a PDP Context Activation

B.7 Start of interception with PDP context active

A tunnel is established to DF3 and an event is sent to DF2.

B.8 MS initiated PDP Context Deactivation

Figure B.7 shows the interception of a MS initiated PDP Context deactivation where the mobile (A) is the target for interception.

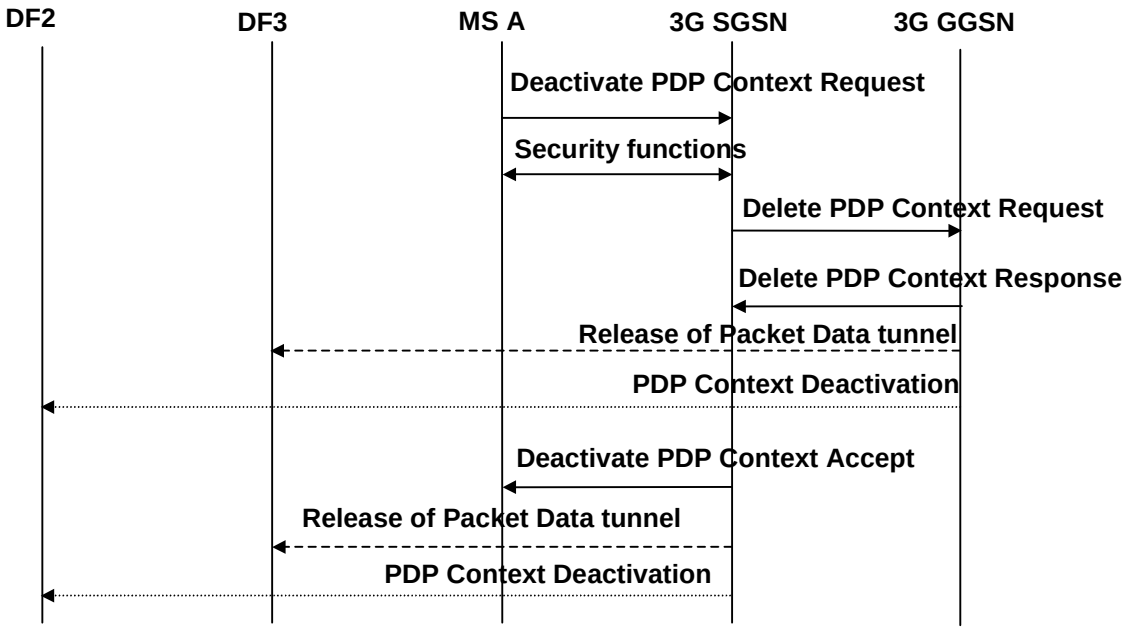


Figure B.7: Interception of a PDP Context Deactivation

B.9 Network initiated PDP Context Deactivation

Figure B.8 shows the interception of a Network initiated PDP Context deactivation where the mobile (A) is the target for interception. The 3G GGSN may send, (depending on national requirements) the PDP Context deactivation and release the Packet Data tunnel after the Delete PDP Context Response has been sent or received, (signalling between the 3G SGSN and the 3G GGSN is not shown here).

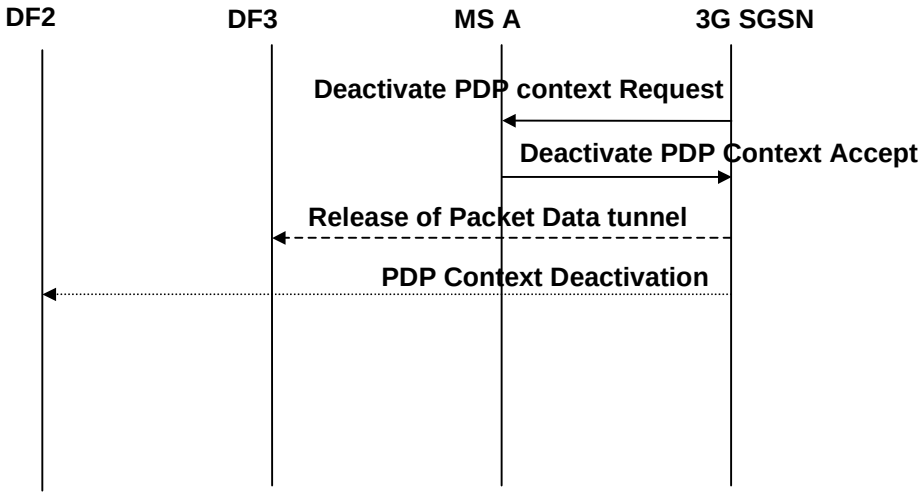


Figure B.8: Interception of a Network initiated PDP Context Deactivation

B.10 SMS

Figures B.9a and B.9b show the interception of a Mobile-terminated SMS. Figures B.10a and B.10b show the interception of a Mobile-originated SMS. In all the scenarios, the mobile subscriber (A) is the target for interception.

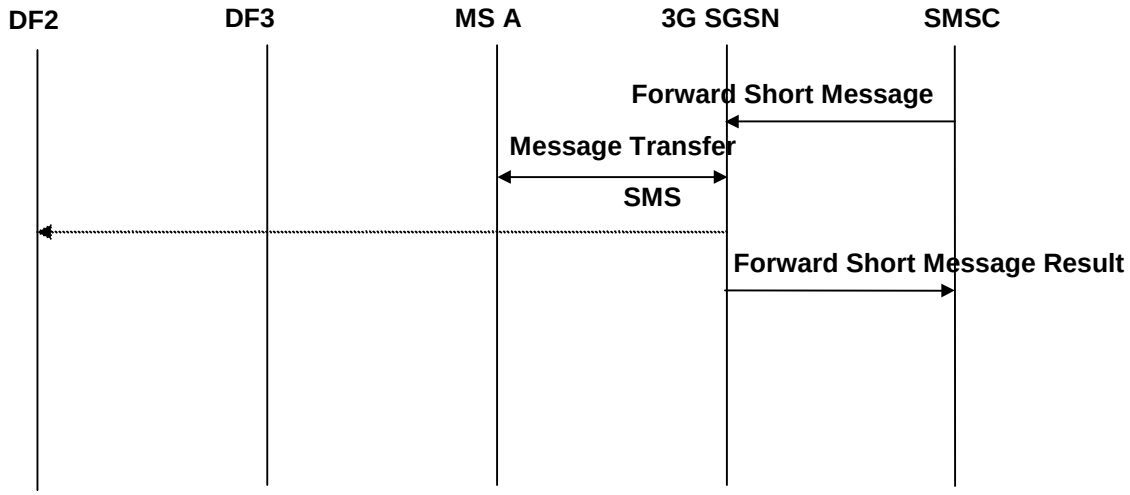


Figure B.9a: MT-SMS interception after 3G SGSN receives notification of SMS delivery to MS(A)

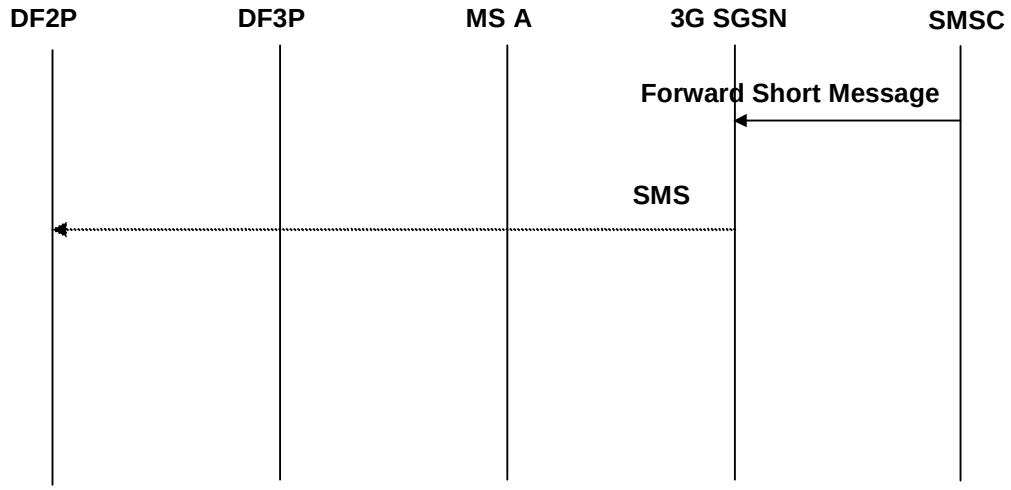


Figure B.9b: MT-SMS interception after 3G SGSN receives SMS from SMSC

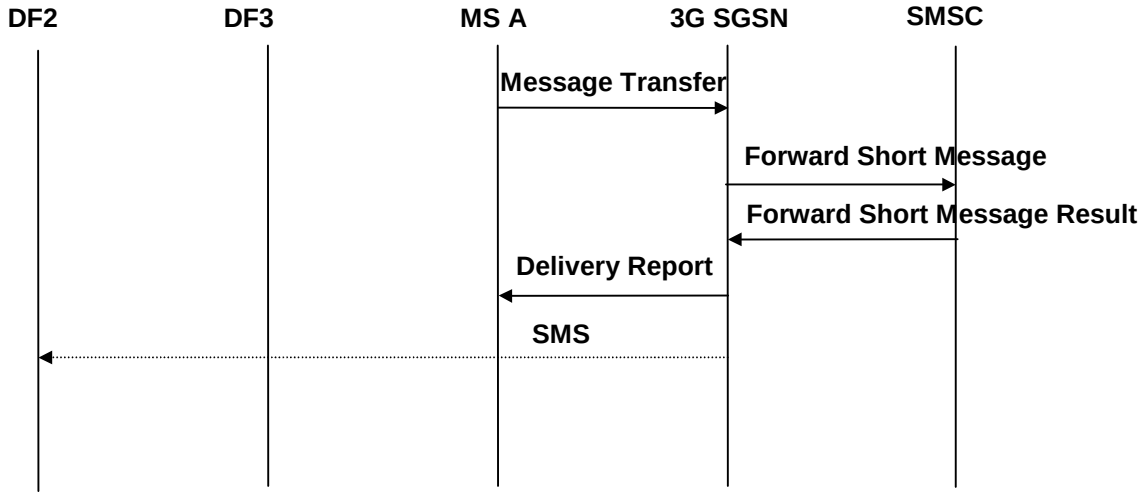


Figure B.10a: MO-SMS interception after 3G SGSN receives notification of SMS delivery from SMSC

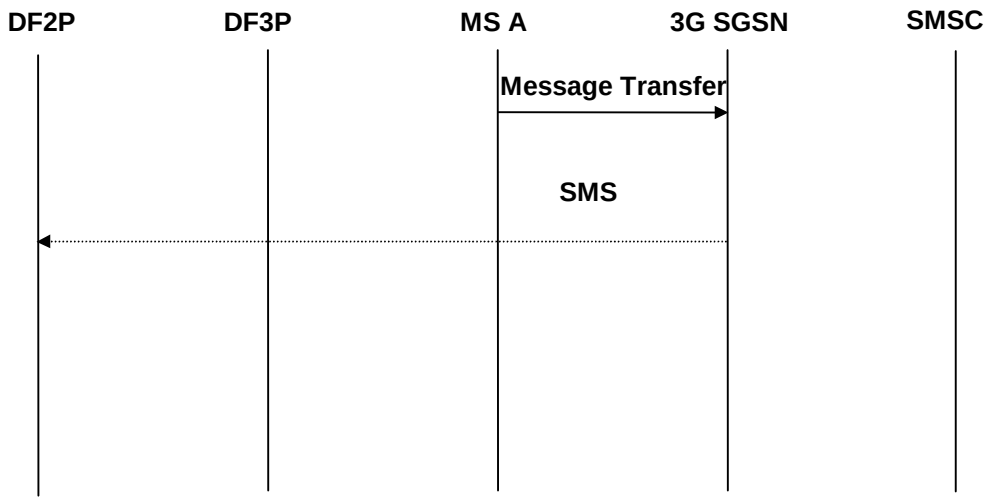


Figure B.10b: MO-SMS interception after 3G SGSN receives SMS from MS(A)

Annex C (informative): Information flows for the invocation of Lawful Interception for Packet Data with multimedia

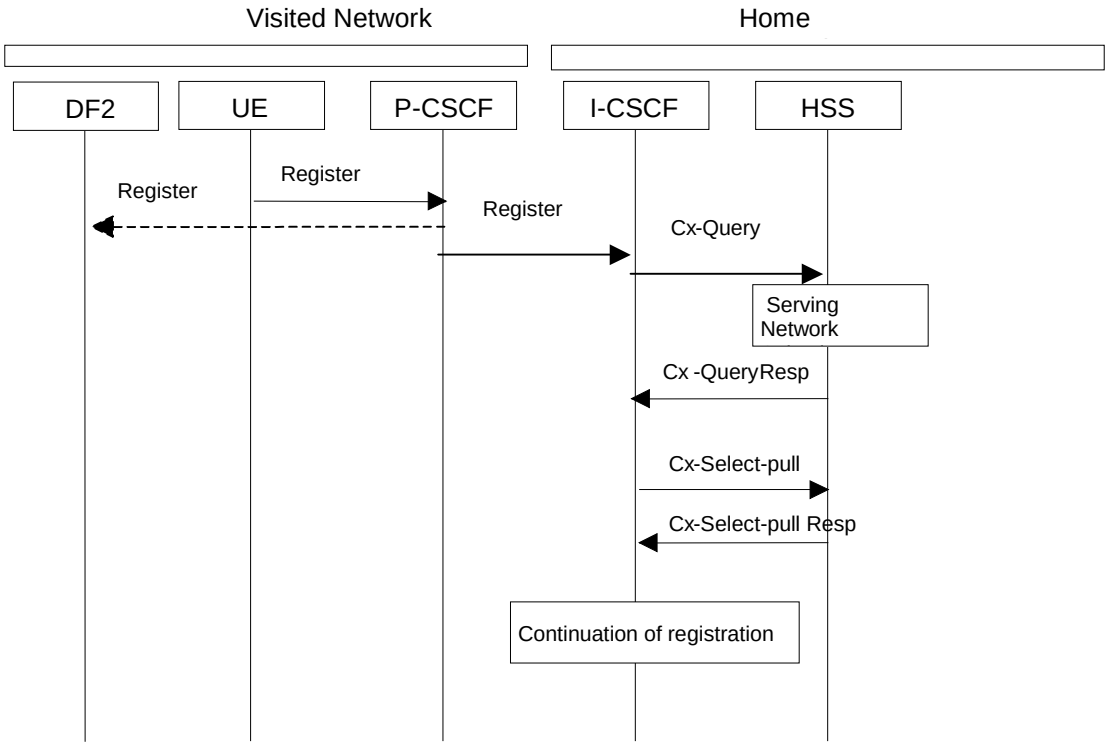
C.0 General

The following figures show the information flows for the invocation of Lawful Interception for Packet Data with multimedia. The figures show some of the basic signalling messages of the target Packet Data communication and the events on the X2 interfaces. The dotted lines indicate signalling depending on whether IRI information has been requested. The figures illustrate interception in the visited network.

The figures in this annex only apply to scenarios where the P-CSCF is located in the visited network. In some operator deployment scenarios, the P-CSCF will be in the Home Network. Where the P-CSCF is located in the Home Network and UE to P-CSCF signalling encryption is applied, all SIP messages between the P-CSCF and the UE will be encrypted within the visited network and therefore plain text interception in the visited network may not be possible.

C.1 Multimedia registration

Figures C.1.1 and C.1.2 show the intercept of the Multimedia registration for the case of visited network interception (refer to TS 23.228 [43] clauses 5.3.2.4 and 5.3.2.5).



Figures C.1.1 and C.1.2 show the intercept of the Multimedia registration for the case of visited network interception, where the P-CSCF is located in the Visited Network (refer to TS 23.228 [43] clauses 5.3.2.4 and 5.3.2.5).

Figure C.1.1: Intercept of Start of Multimedia Registration

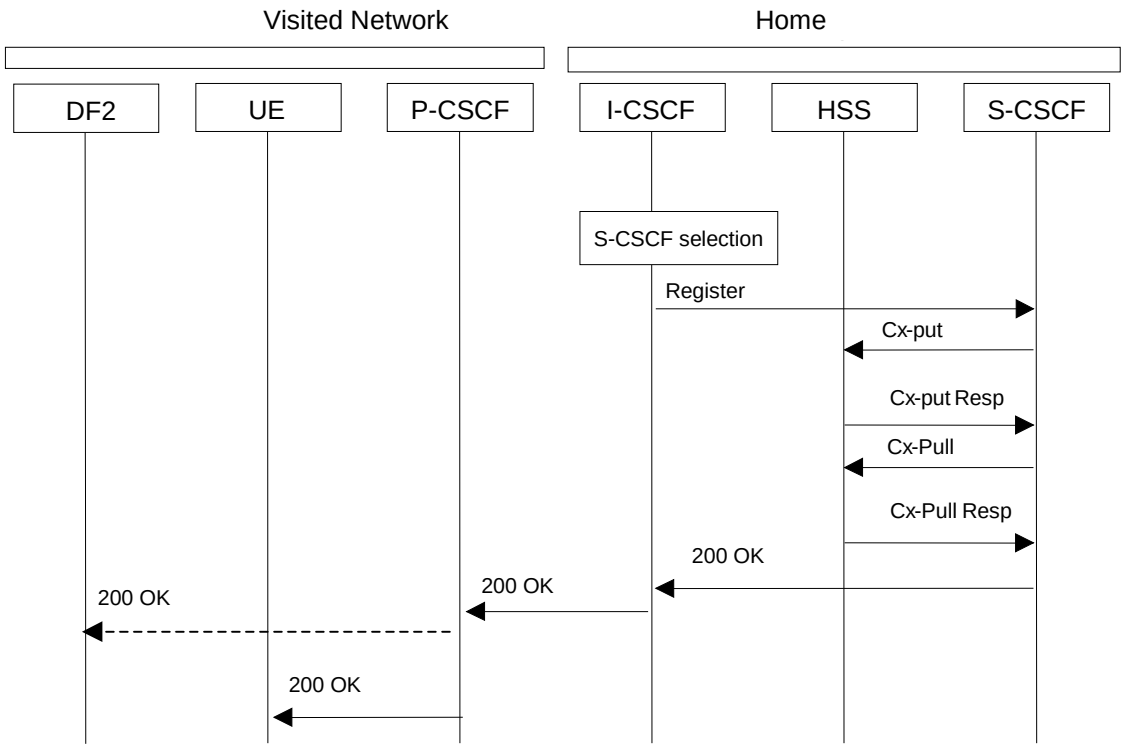


Figure C.1.2: Intercept of Continuation of Multimedia Registration

NOTE: The same SIP Registration command is used for the initial registration and any registration updates. Registration deletion request is accomplished with a Registration command that indicates a '*' contact or zero expiration time.

C.2 Multimedia Session Establishment and Answer

Figure C2 shows the intercept of the Multimedia Establishment and Answer in the visited network, where the P-CSCF is located in the Visited Network (refer to TS 23.228 [43], clause 5.7.1).

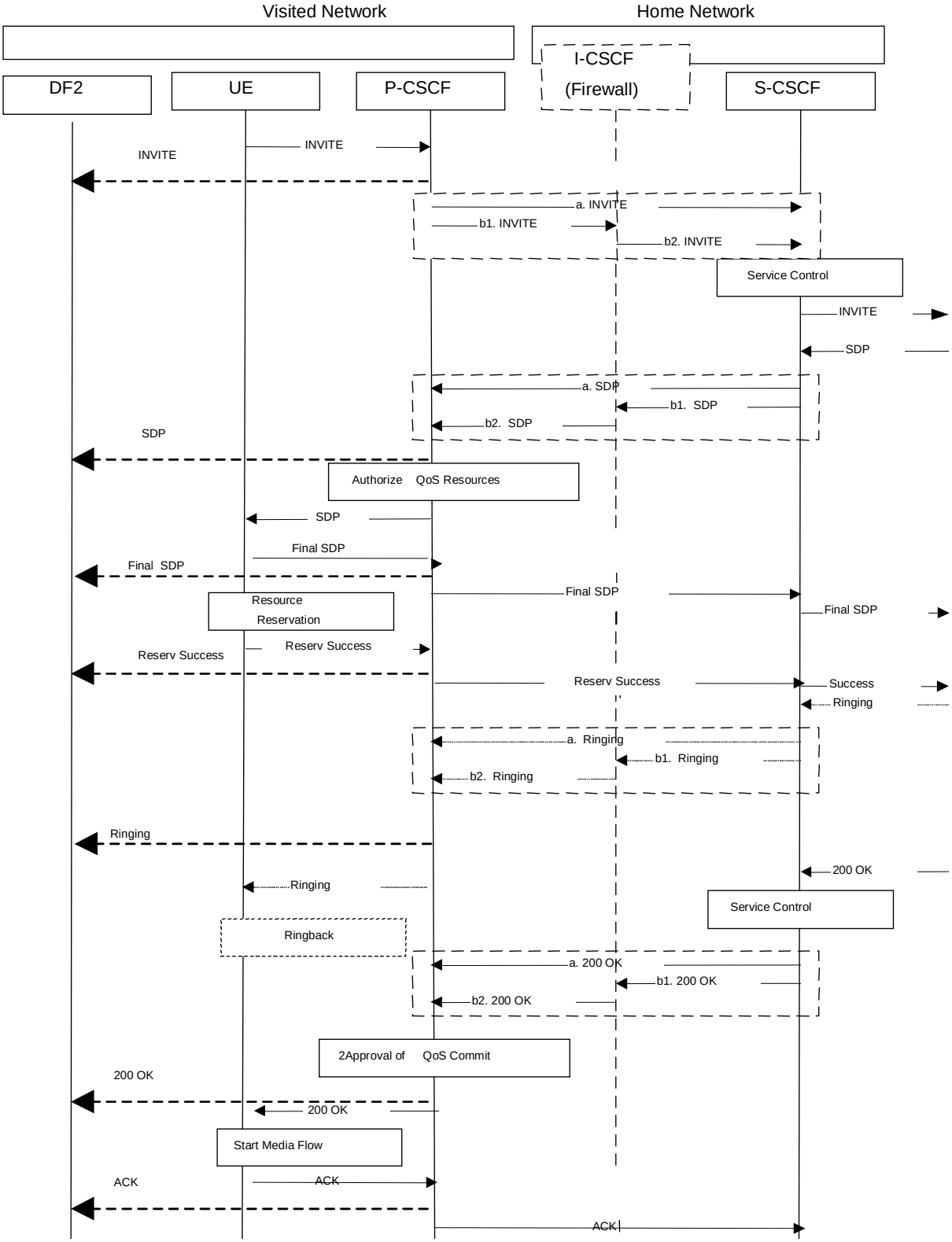


Figure C.2 Intercept of Multimedia Establishment and Answer at Visiting Network

C.3 Multimedia Release

Figure C.3 shows the intercept of the Multimedia Release in the visited network, where the P-CSCF is located in the Visited Network (TS 23.228 [43], clause C.2.1 reference available).

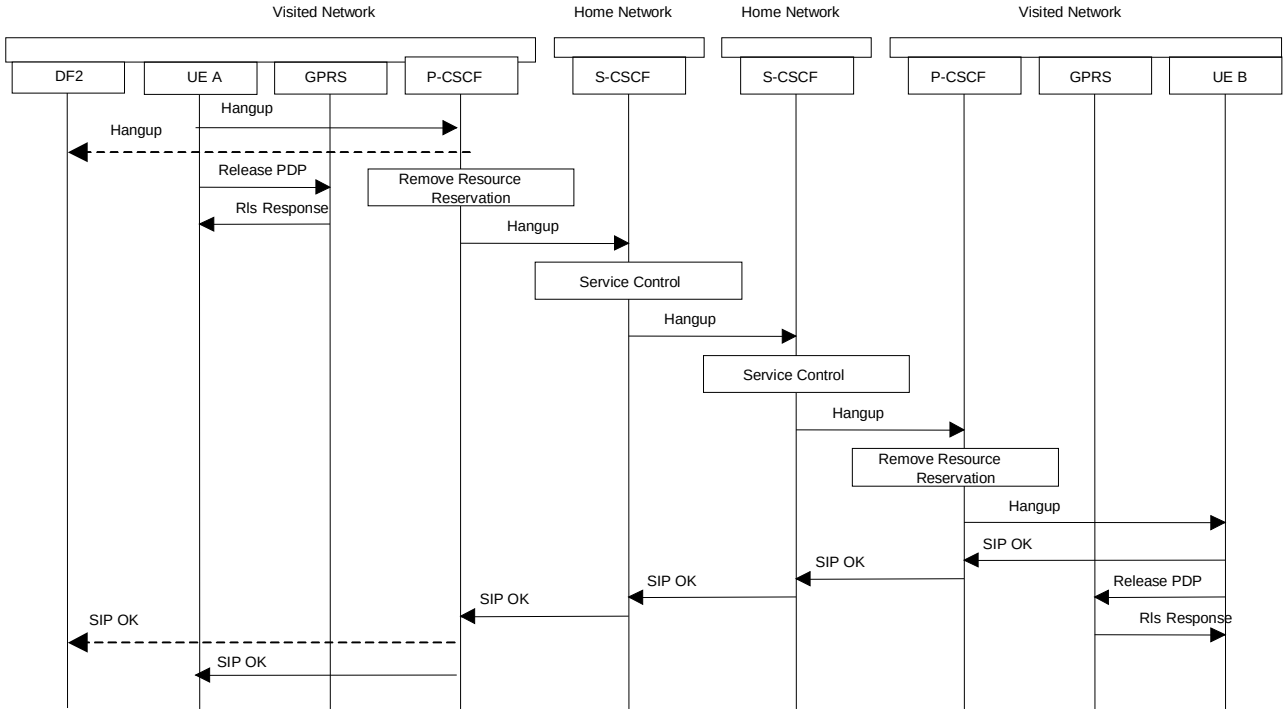


Figure C.3 Intercept of Multimedia Release at Visiting Network

C.4 Multimedia with Supplementary Service - Call Forwarding

Not defined in this release.

C.5 Multimedia with Supplementary Service - Explicit Call Transfer

Not defined in this release.

C.6 Multimedia with Supplementary Service - Subscriber Controlled input

Not defined in this release.

Annex D (informative): Information flows for Lawful Interception invocation at the MGW using H.248

D.0 General

The following figures show the use of H.248 in setting up a bearer intercept point at the MGW.

D.1 Mobile to Mobile call, originating side is target

Figure D.1 shows the network model for interception of a mobile-to-mobile call, where the originating mobile subscriber is the target for interception.

Figure D.2 message sequence only shows the H.248 elements related to the necessary topology, which could be used in this example.

Normal call establishment using other H.248 elements shall be in accordance with TS 23.205.
It should be noted that other means exist with H.248 to achieve similar interception.

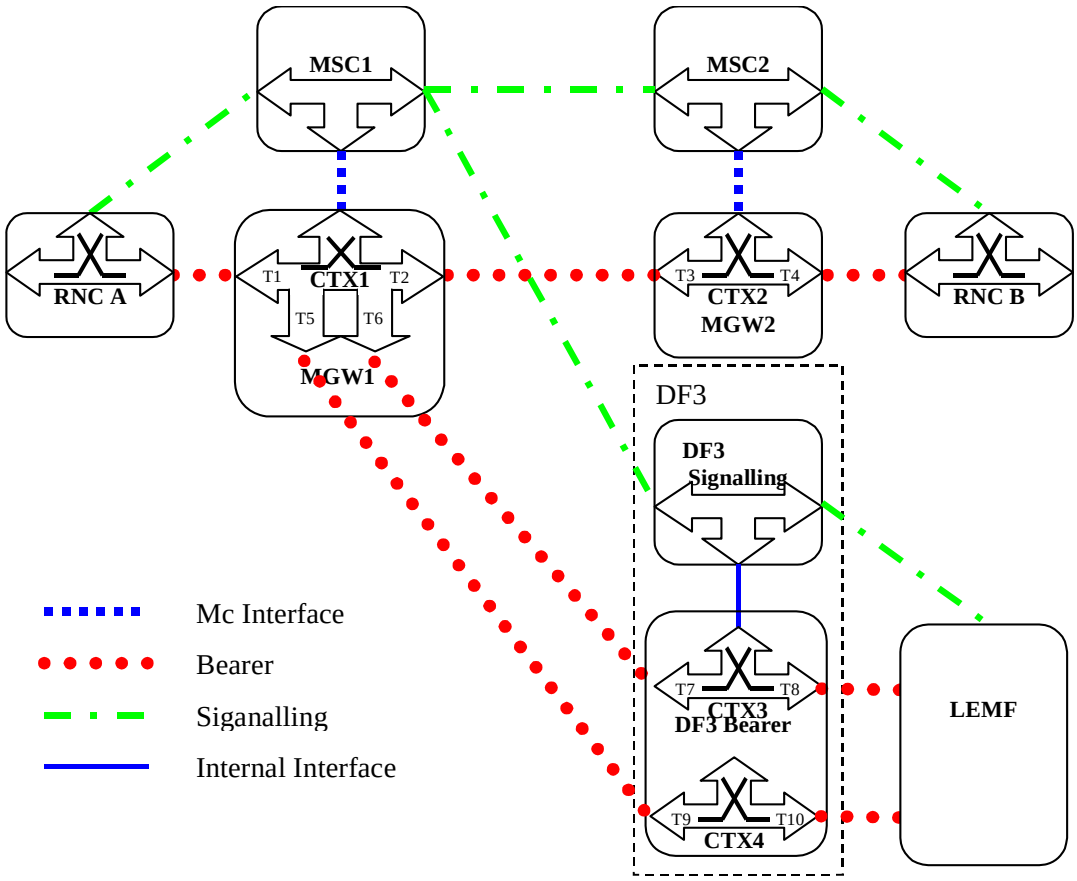


Figure D.1: Mobile to Mobile call originating side is target (network model)

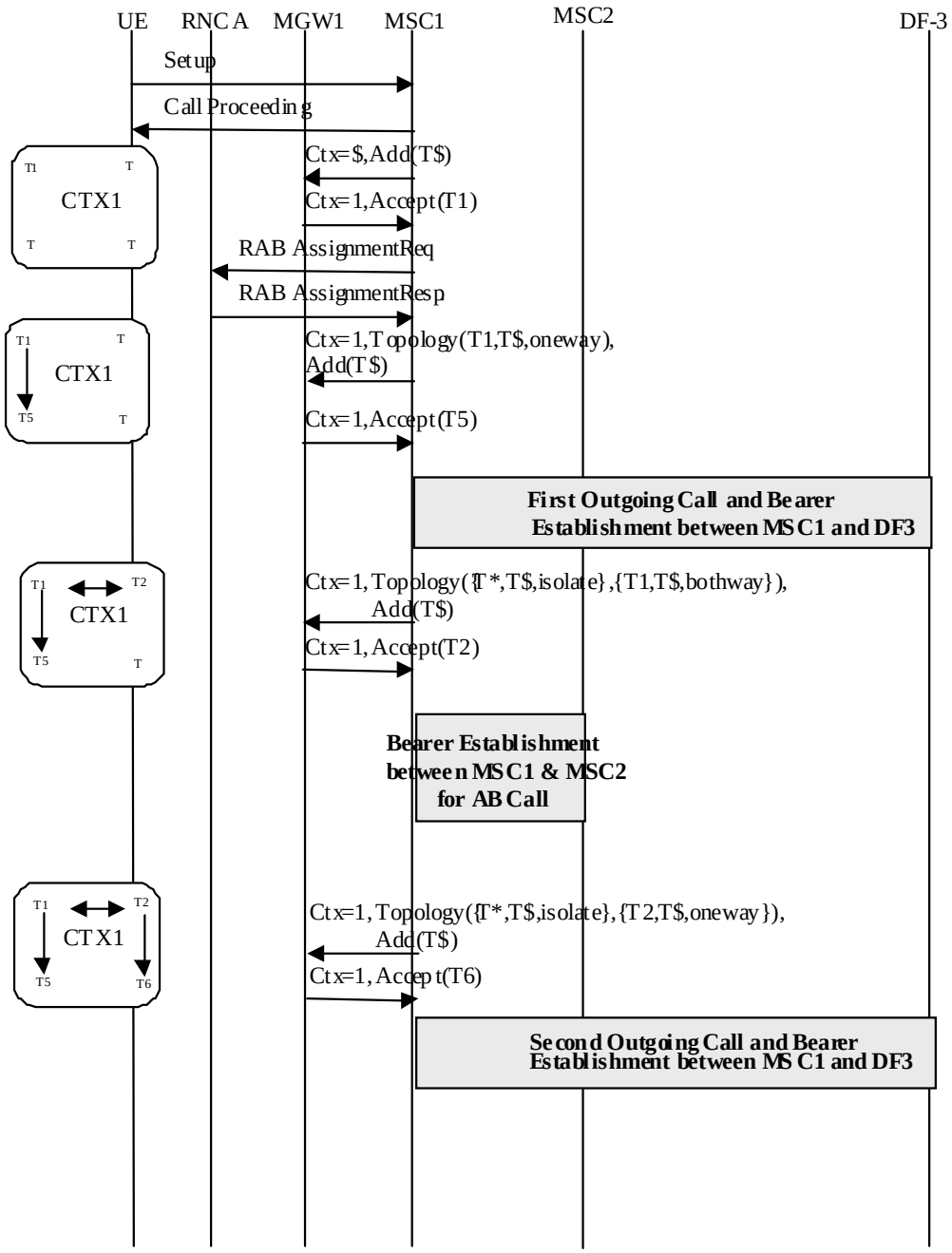


Figure D.2: Mobile to Mobile call originating side is target

Annex E (Informative): IMS-based VoIP Lawful Interception call scenarios

E.1 Overview

This informative annex provides the examples of call scenarios that illustrate the interception and delivery of CC interception for an IMS-based VoIP call.

E.2 Background

One of the use-cases of IMS-based VoIP service is VoLTE. The term "VoLTE" is used to refer to an IMS-based VoIP service when EPS (see TS 23.401 [22]) happens to be the access network. When EPS is not the access network, the lawful interception capabilities defined in this informative annex applies for any IMS-based VoIP service with the presumption that in those cases the media on the target's access goes through an IMS-AGW (see TS 29.334 [42]) or a PDN-GW (see TS 23.401 [22] and TS 23.402 [23]) or a GGSN (UMTS network).

NOTE 1: Void.

Even with the EPS-based access network, the media might still go through the IMS-AGW. And, in this case, a VoLTE shall be treated very similar to any other VoIP service.

Furthermore, it is presumed that an inter-CSP call enters or leaves an IMS network via an IBCF/TrGW or an MGCF/IM-MGW depending on whether the inter-working CSP network is an IMS-based network or a CS-based network (see TS 23.228 [43]). Also, for an IMS roaming scenario, it is presumed that the signalling and media enters or leaves the home CSP through the IBCF/TrGW.

The figure E.1 illustrates the VoIP configuration considered for the lawful interception capabilities defined in this clause:

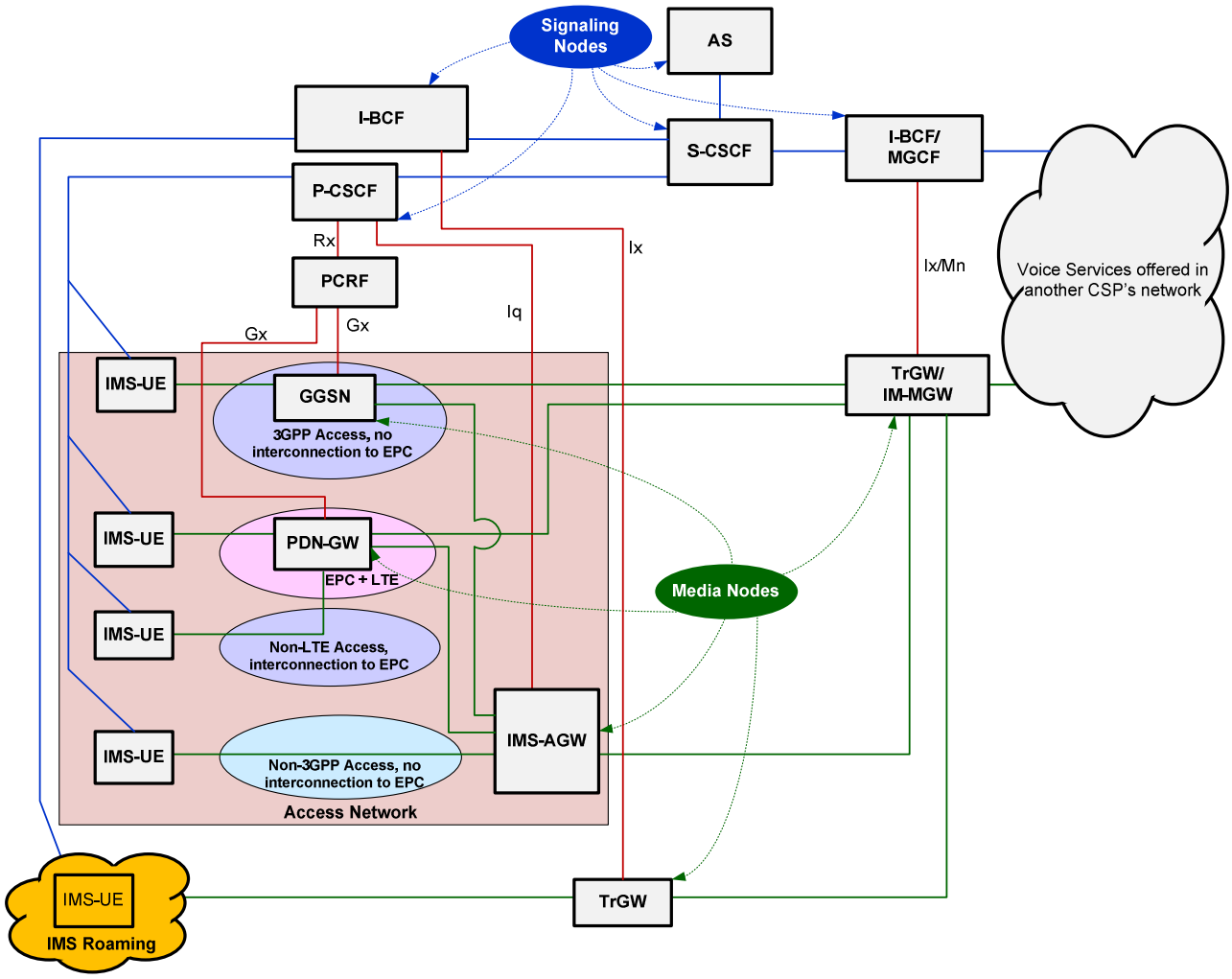


Figure E.1: IMS-based VoIP Configuration

NOTE 2: The configuration scenario where the media does not go through the GGSN, or PDN-GW or the IMS-AGW is outside the scope of this document.

NOTE 3: Void.

In the remaining part of this informative annex, the PDN-GW/GGSN are shown in one box and is to be read as either the GGSN (UMTS) or the PDN-GW (EPS).

In figure E.1, the term "media node" is used to denote the network node present on media path and the term "signalling node" is used to denote the network node present on the signalling path.

The general concepts of VoIP LI is shown in figure E.2

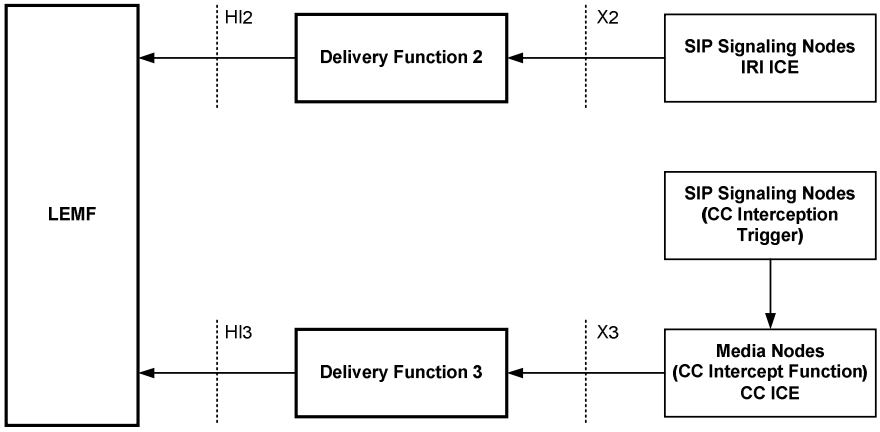


Figure E.2: General Principles of VoIP Interception

In clause 15, the SIP signalling nodes provide signalling information to the CC Interception Triggering Function. The CC Interception Triggering Function triggers the CC interception at a media node that implements the CC Intercept Function.

The following functional elements provide the CC Intercept Function in the example call scenarios:

- PDN-GW/GGSN;
- IMS-AGW;
- TrGW;
- IM-MGW
- MRF.

The following functional elements provide the signalling to the CC Intercept Triggering Function:

- P-CSCF for PDN-GW/GGSN and IMS-AGW;
- IBCF for TrGW;
- MGCF for IM-MGW
- S-CSCF for MRF.

At any given time, for a specific target and for any given call, only one functional element is required to provide the CC interception. The functional element that provides the CC interception may vary, primarily, based on the CSP network implementation and the call scenario.

E.3 Originating Call from the Target with CC Interception at the PDN-GW/GGSN

E.3.0 General

Figure E.3 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target originates a call with PDN-GW (or GGSN) providing the CC interception.

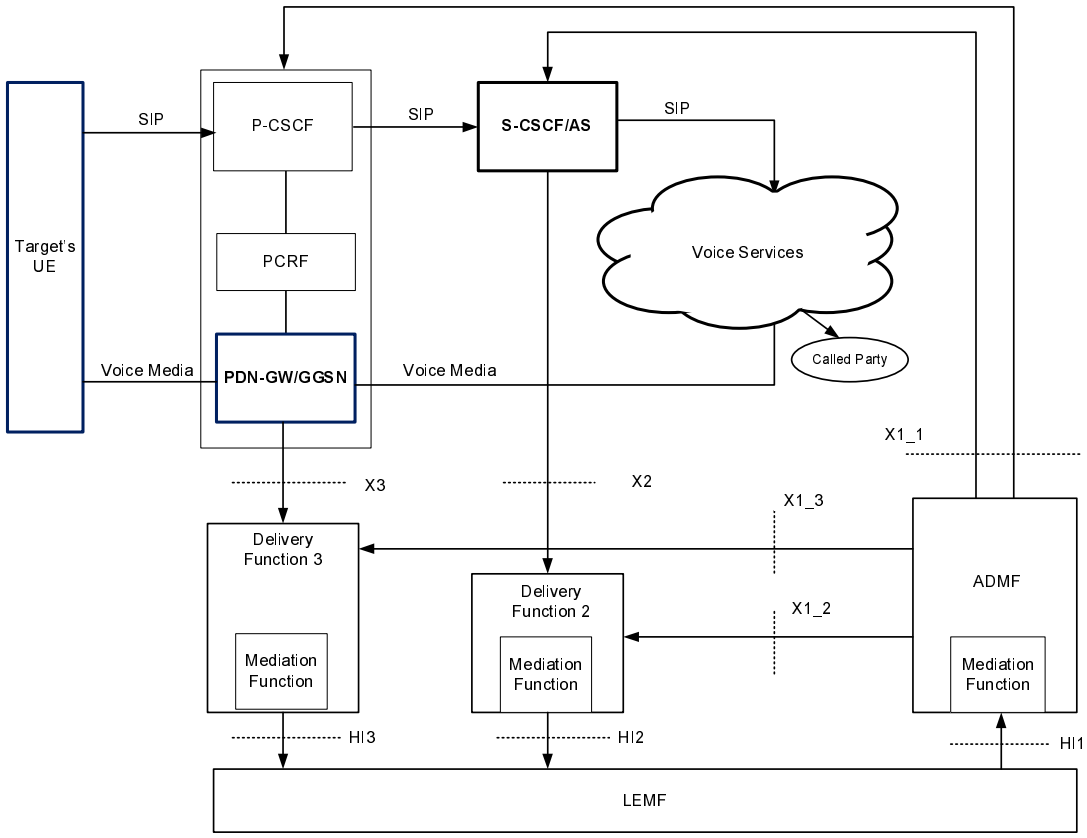


Figure E.3: VoIP lawful interception for an originating call with CC interception at the PDN-GW/GGSN

The cloud shown with the label "voice services" is to indicate that the target is making a voice call and the called party can be within the same CSP's network or in another CSP's network.

Figure E.3 shows that the IRI interception is done at S-CSCF or AS. However, as specified in clause 7A, the IRI interception can also be done at the P-CSCF (not shown in figure E.3). The CC interception is done at the PDN-GW/GGSN. The P-CSCF sends the CC intercept trigger to the PDN-GW/GGSN.

NOTE 4: PCRF is defined in TS 23.203 [44].

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI, TEL URI or IMEI).

E.3.1 Originating Call from the Target with CC Interception at the MRF

Figure E.3.1 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC when a target originates a call with an MRF providing the CC interception. The S-CSCF provides the CC Interception Triggering Function for the MRF.

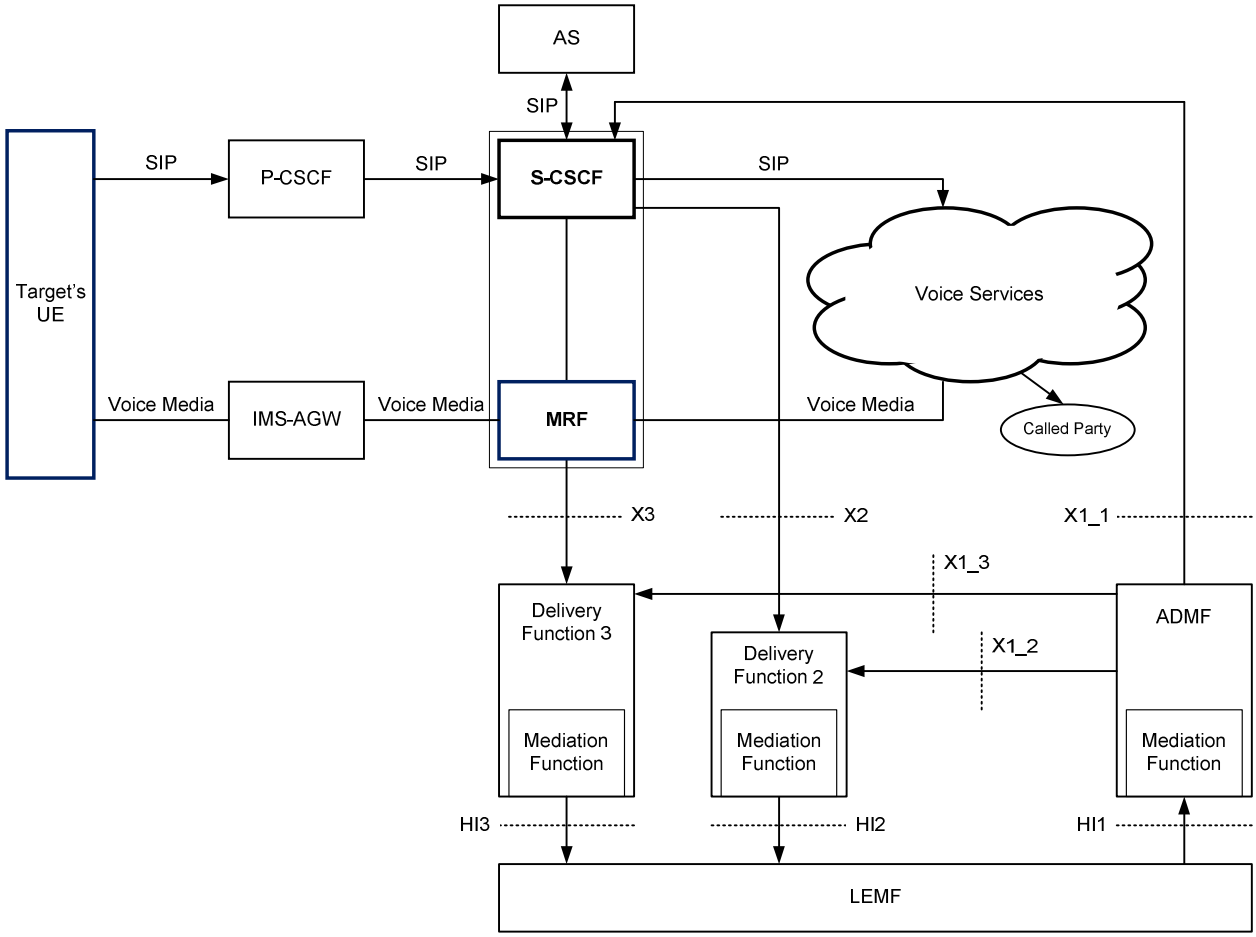


Figure E.3.1: VoIP lawful interception for an originating call with CC interception at the MRF

The cloud shown with the label "voice services" indicates that the target is making a voice call and the called party can be within the same CSP's network or in another CSP's network.

IRI interception is done at the S-CSCF. The CC interception is done at an MRF that functions as the CC ICE.

The MRF is deployed in a network configuration with an IP border access controller that serves to hide the presence of the MRF. The IP access border controller supports IP-level topology hiding for any voice media streams. Specifically, the border gateway supports NAT functionality; always presents its own IP address to the user; prevents ICMP Ping & ICMP Traceroute requests from being forwarded across the gateway; and, resets TTL field in the IP header.

NOTE 3.1: MRF is defined in TS 23.228 [43].

The ADF activates interception at the S-CSCF for IRI interception and CC interception using the same target identity (SIP URI, TEL URI or IMEI). The S-CSCF dynamically triggers CC interception at the MRF for the call.

E.4 Originating Call from the Target with CC Interception at the IMS-AGW

Figure E.4 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target originates a call with IMS-AGW providing the CC interception.

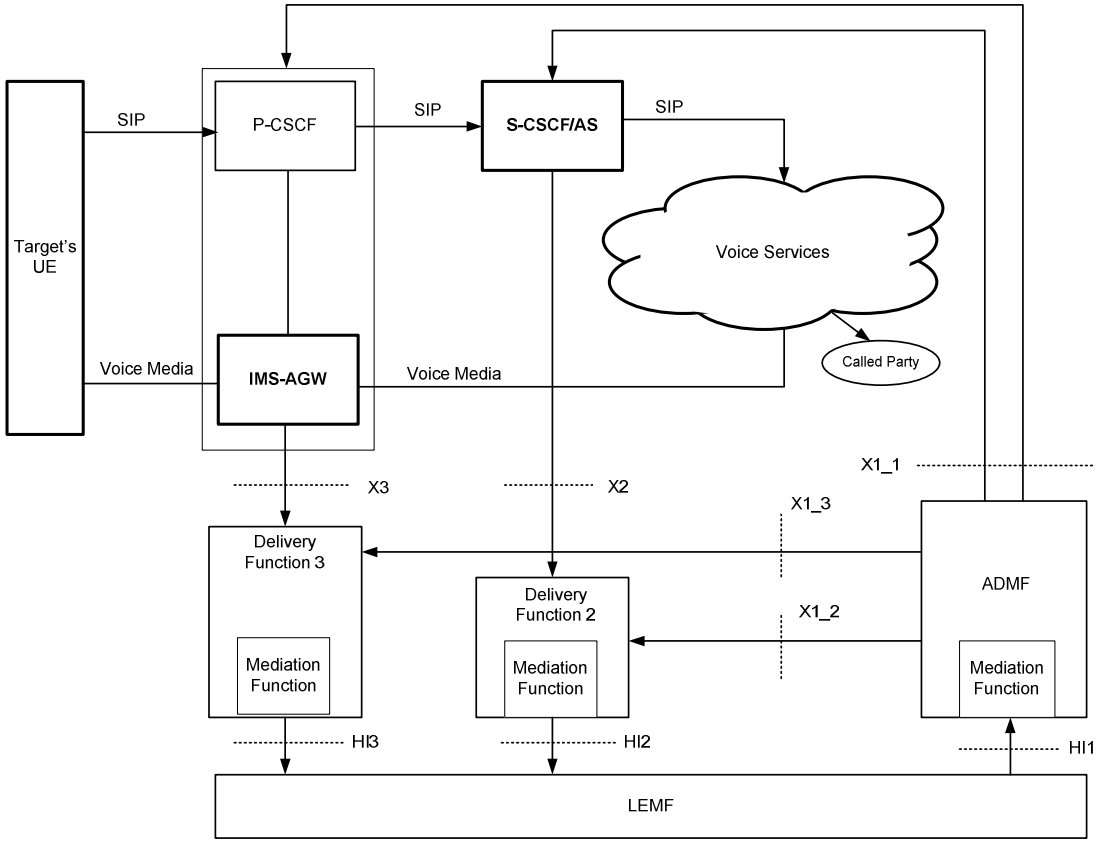


Figure E.4: VoIP lawful interception for an originating call with CC interception at the IMS-AGW

The cloud shown with the label "voice services" is to indicate that the target is making a voice call and the called party can be within the same CSP's network or in another CSP's network.

Figure E.4 shows that the IRI interception is done at S-CSCF or AS. However, as specified in 7A, the IRI interception can also be done at the P-CSCF (not shown in figure E.4). The CC interception is done at the IMS-AGW. The P-CSCF sends the CC intercept trigger to the IMS-AGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI, TEL URI or IMEI).

E.5 Terminating Call to the Target with CC Interception at the PDN-GW/GGSN

E.5.0 General

Figure E.5 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target receives an incoming call with PDN-GW/GGSN providing the CC interception.

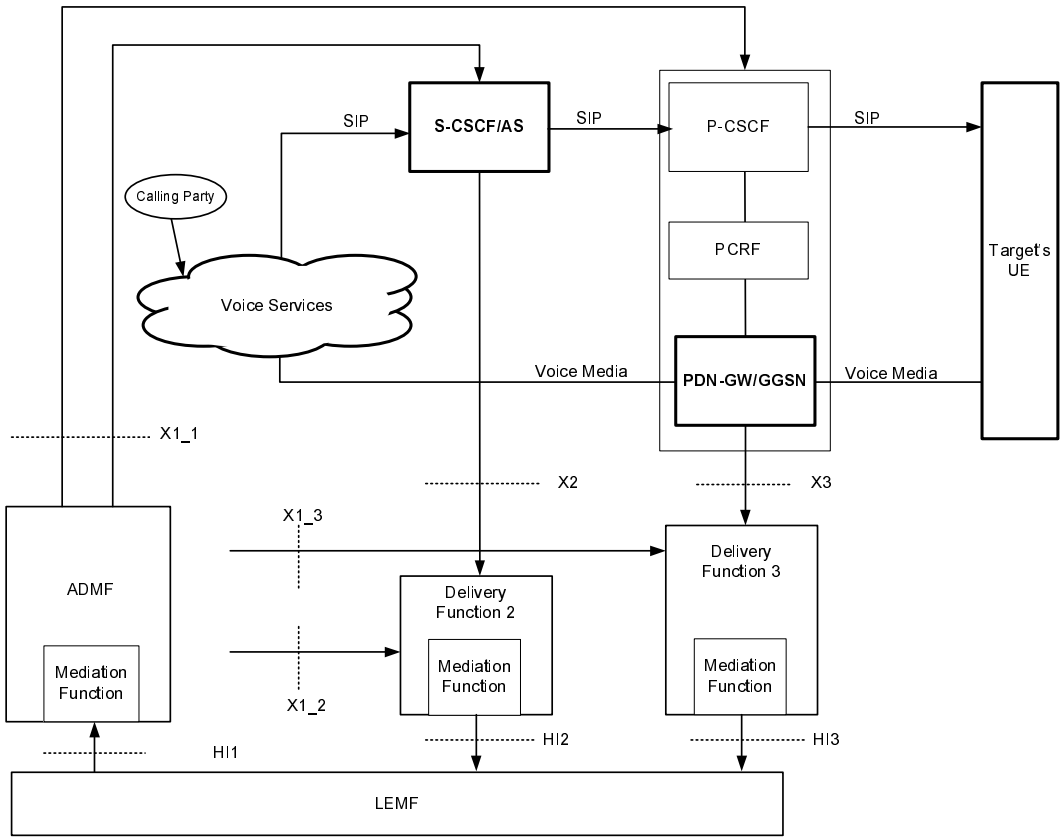


Figure E.5: VoIP lawful interception for a terminating call with CC interception at the PDN-GW/GGSN

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target are not shown for simplification of the drawing.

Figure E.5 shows that the IRI interception is done at S-CSCF or AS. However, as specified in 7A, the IRI interception can also be done at the P-CSCF (not shown in figure Z.5). The CC interception is done at the PDN-GW/GGSN. The P-CSCF sends the CC intercept trigger to the PDN-GW/GGSN.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI, TEL URI or IMEI).

E.5.1 Terminating Call to the Target with CC Interception at the MRF

Figure E.5.1 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC when the target receives an incoming call with an MRF providing the CC interception. The S-CSCF provides the CC Interception Triggering Function for the MRF.

The MRF is deployed in a network configuration with an IP border access controller that serves to hide the presence of the MRF. The IP access border controller supports IP-level topology hiding for any voice media streams. Specifically,

the border gateway supports NAT functionality; always presents its own IP address to the user; prevents ICMP Ping & ICMP Traceroute requests from being forwarded across the gateway; and, resets TTL field in the IP header.

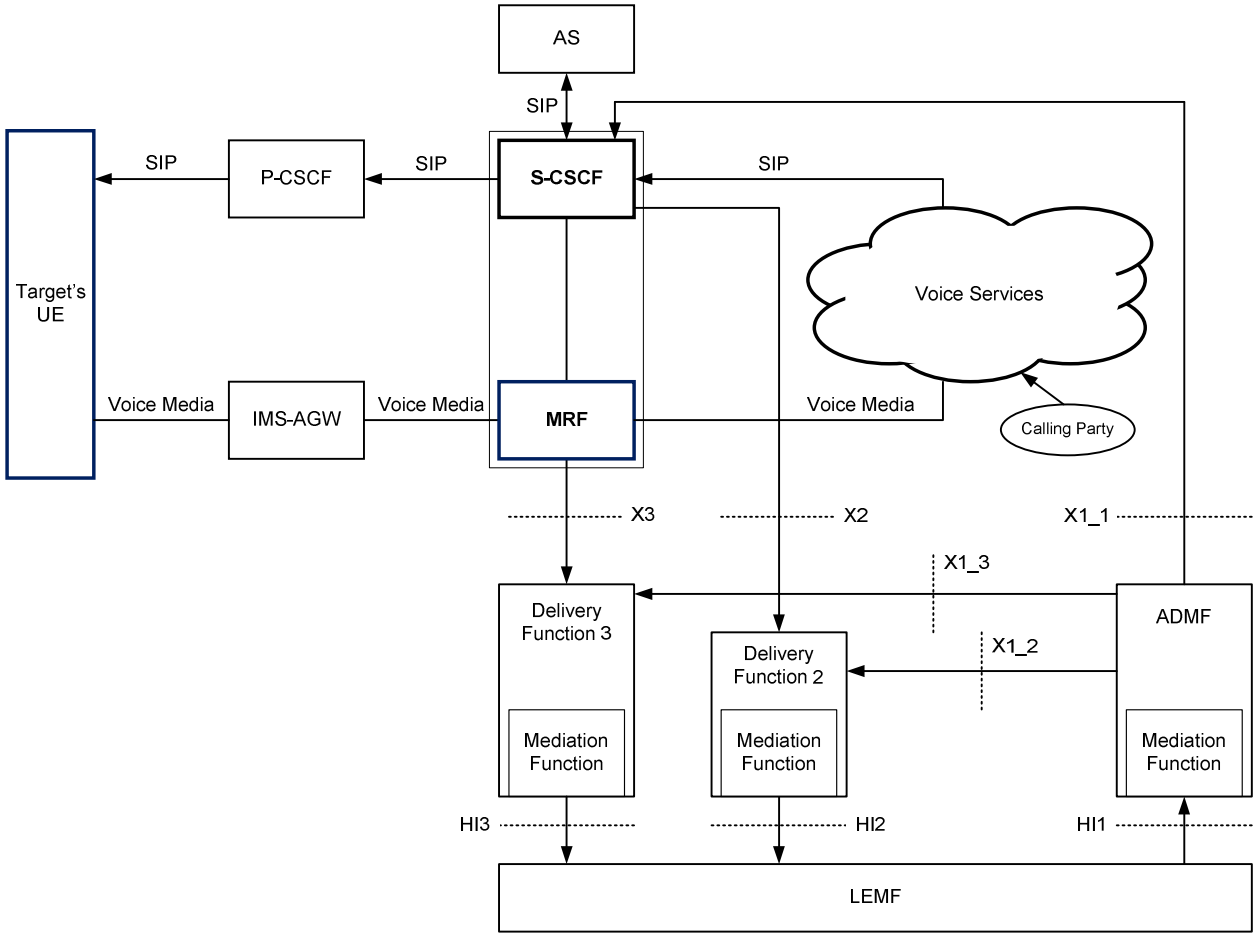


Figure E.5.1: VoIP lawful interception for a terminating call with CC interception at the MRF

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target are not shown for simplification of the figure.

IRI interception is done at the S-CSCF. The CC interception is done at an MRF that functions as the CC ICE.

The ADMF activates interception at the S-CSCF for IRI interception and CC interception using the same target identity (SIP URI, TEL URI or IMEI). The S-CSCF dynamically triggers CC interception at the MRF for the call.

E.6 Terminating Call to the Target with CC Interception at the IMS-AGW

Figure E.6 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target receives an incoming call with IMS-AGW providing the CC interception.

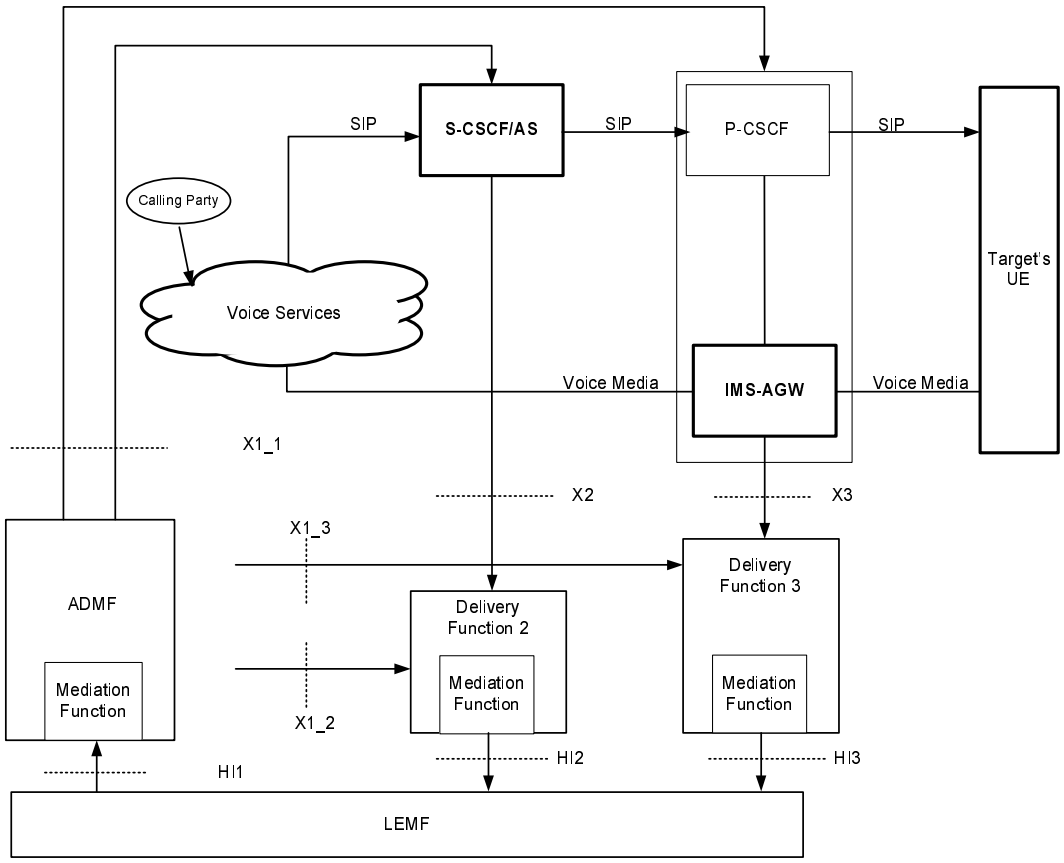


Figure E.6: VoIP lawful interception for a terminating call with CC interception at the IMS-AGW

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target are not shown for simplification of the drawing.

Figure E.6 shows that the IRI interception is done at S-CSCF or AS. However, as specified in 7A, the IRI interception can also be done at the P-CSCF (not shown in figure E.6). The CC interception is done at the IMS-AGW. The P-CSCF sends the CC intercept trigger to the IMS-AGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI, TEL URI or IMEI).

E.7 Intra-CSP Forwarded Call with CC Interception at the PDN-GW/GGSN

E.7.0 General

Figure E.7 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target receives an incoming call with PDN-GW/GGSN providing the CC interception and the call is forwarded to another IMS subscriber within the CSP's network.

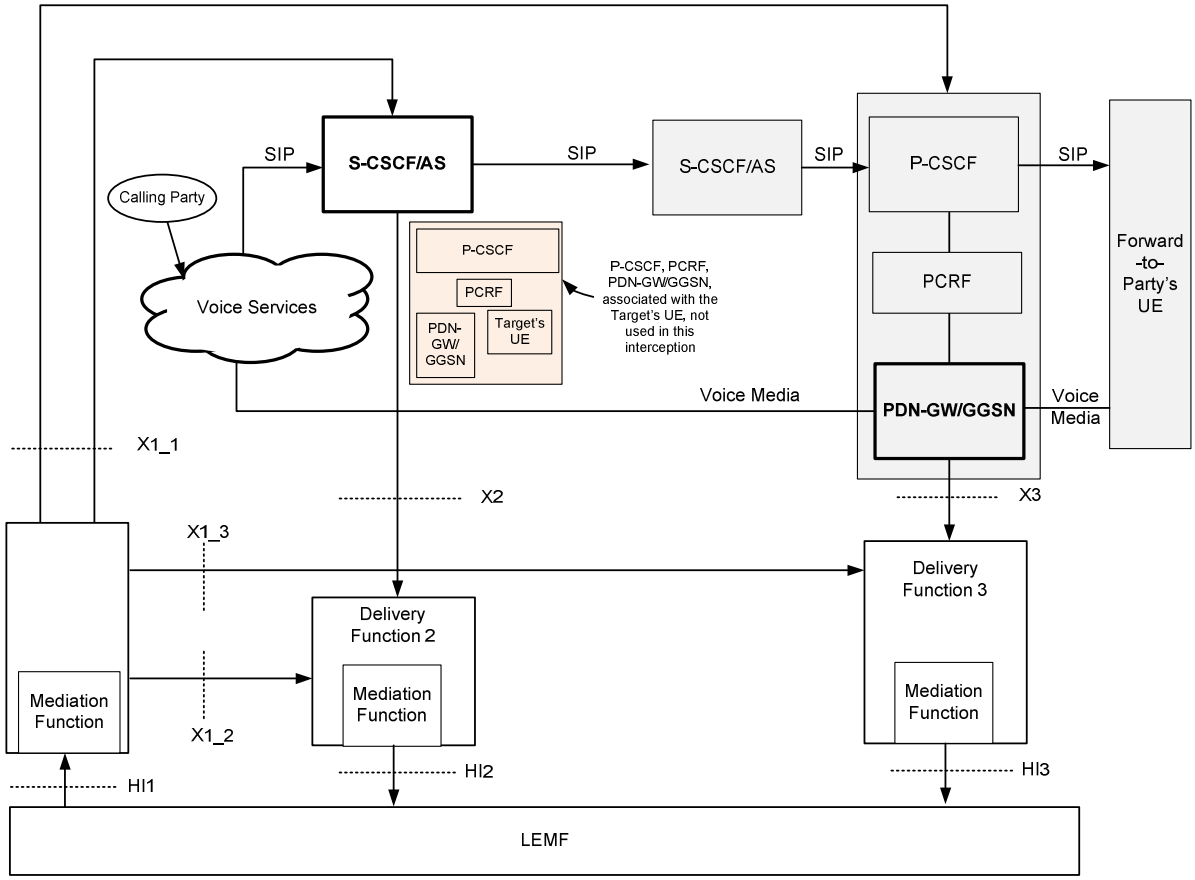


Figure E.7: VoIP lawful interception for an intra-CSP forwarded call with CC interception at the PDN-GW/GGSN

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target and to the forwarded-to-party are not shown for simplification of the drawing.

Figure E.7 shows that the IRI interception is done at S-CSCF or AS. In this scenario, the IRI interception cannot occur in the P-CSCF since the P-CSCF that provides the proxy functions to the target is not on the signalling path. The CC interception is done at the PDN-GW/GGSN. The P-CSCF (that provides the proxy functions to the forwarded-to-party) sends the CC intercept trigger to the PDN-GW/GGSN.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

E.7.1 Intra-CSP Forwarded Call with CC Interception at the MRF

Figure E.7.1 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target receives an incoming call with the MRF providing the CC interception and the call is forwarded to another IMS subscriber within the CSP's network. The S-CSCF provides the CC Interception Triggering Function for the MRF.

The MRF is deployed in a network configuration with an IP border access controller that serves to hide the presence of the MRF. The IP access border controller supports IP-level topology hiding for any voice media streams. Specifically, the border gateway supports NAT functionality; always presents its own IP address to the user; prevents ICMP Ping & ICMP Traceroute requests from being forwarded across the gateway; and, resets TTL field in the IP header.

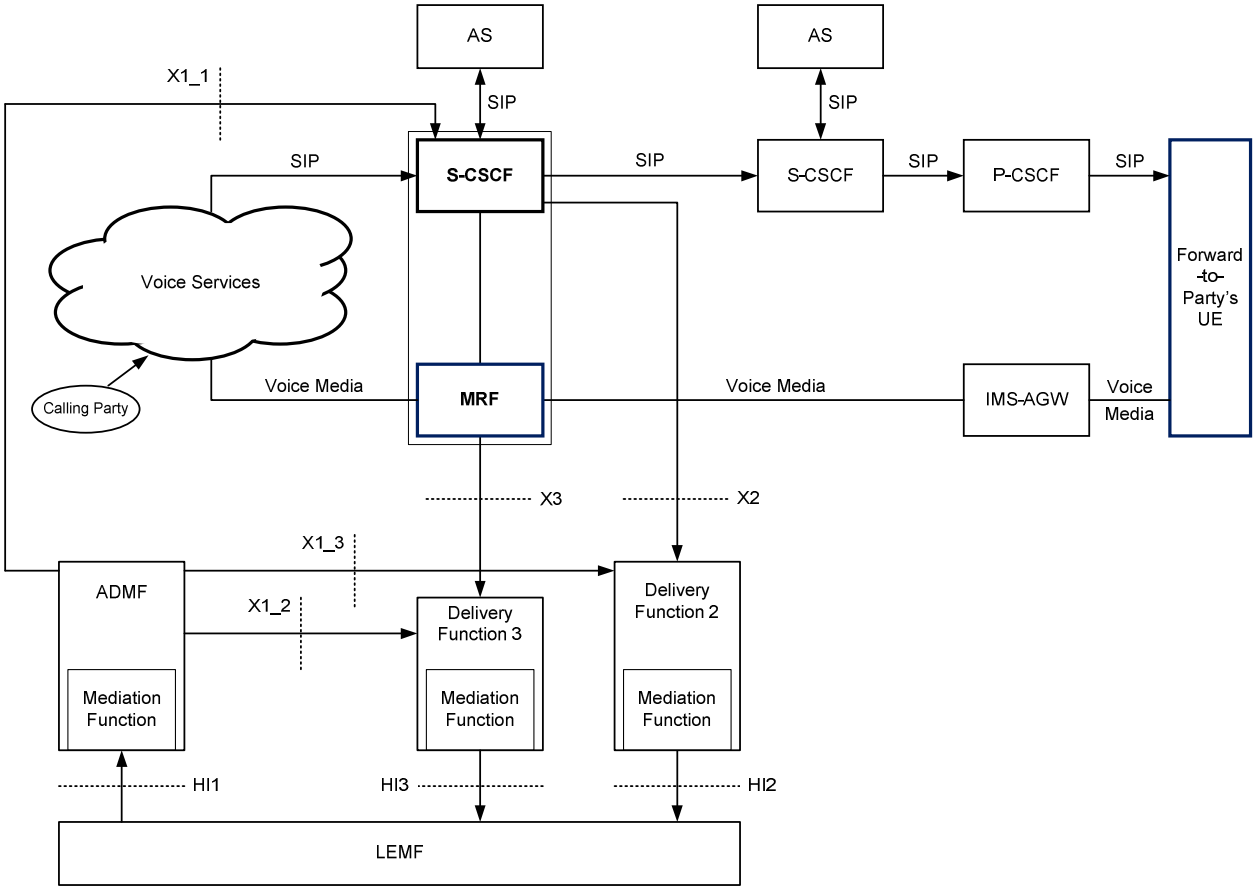


Figure E.7.1: VoIP lawful interception for an intra-CSP forwarded call with CC interception at the MRF

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as P-CSCF, IMS-AGW, HSS involved in the handling of an incoming call to the target and to the forwarded-to-party are not shown for simplification of the drawing.

Figure E.7.1 shows that the IRI interception is done at S-CSCF. The CC interception is done at the MRF that functions as the CC ICE.

The ADMF activates interception at the S-CSCF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI). The S-CSCF dynamically activates CC interception at the MRF.

E.8 Intra-CSP Forwarded Call with CC Interception at the IMS-AGW

Figure E.8 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target receives an incoming call with IMS-AGW providing the CC interception and the call is forwarded to another IMS subscriber within the CSP's network.

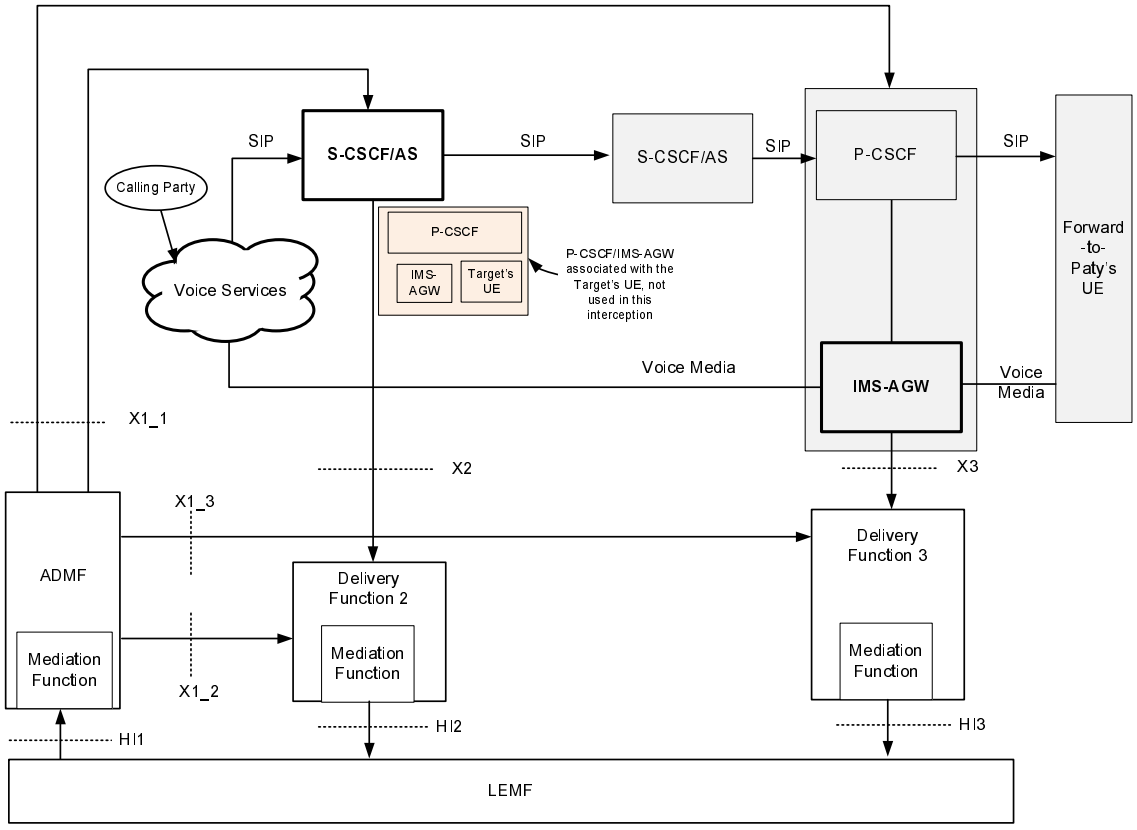


Figure E.8: VoIP lawful interception for an intra-CSP forwarded call with CC interception at the IMS-AGW

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target and to the forwarded-to-party are not shown for simplification of the drawing.

Figure E.8 shows that the IRI interception is done at S-CSCF or AS. In this scenario, the IRI interception cannot occur in the P-CSCF since the P-CSCF that provides the proxy functions to the target is not on the signalling path. The CC interception is done at the IMS-AGW. The P-CSCF (that provides the proxy functions to the forwarded-to-party) sends the CC intercept trigger to the IMS-AGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

E.9 Inter-CSP Forwarded Call to a CS Domain

Figure E.9 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target receives an incoming call and the call is forwarded to a subscriber on the CS domain of another CSP's network.

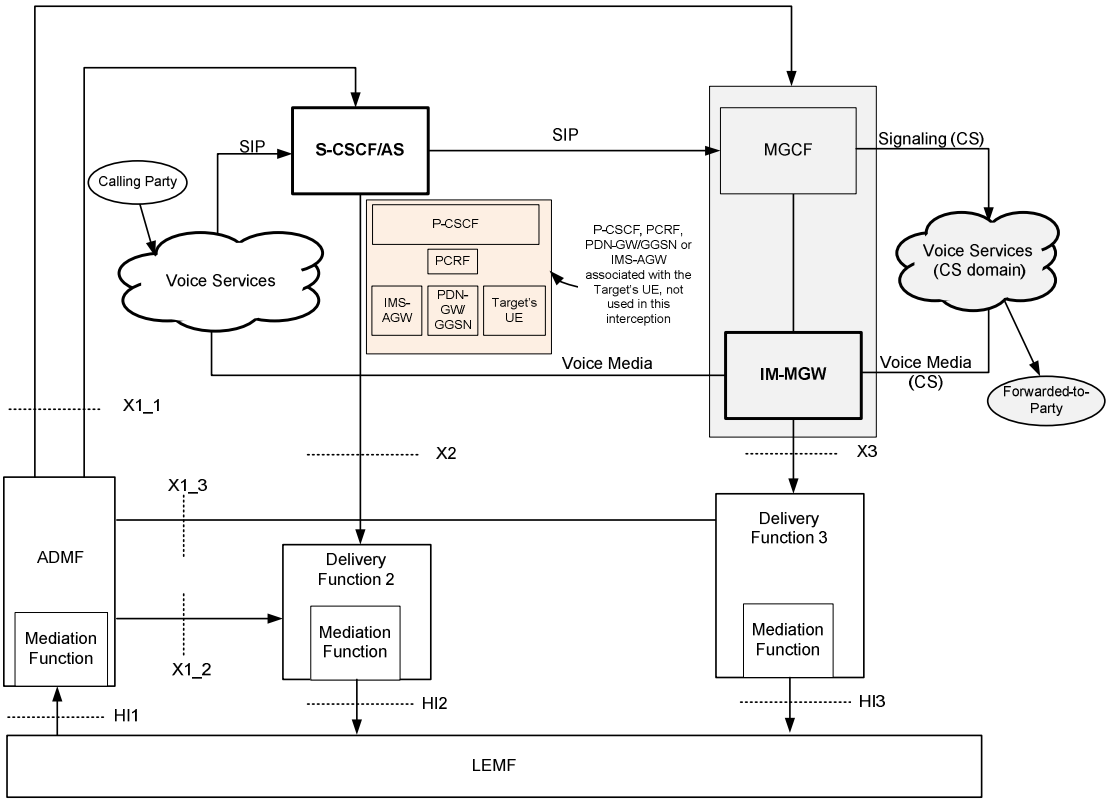


Figure E.9: VoIP lawful interception for an inter-CSP forwarded call to a CS Domain

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target are not shown for simplification of the drawing.

Figure E.9 shows that the IRI interception is done at S-CSCF or AS. In this scenario, the IRI interception cannot occur in the P-CSCF since the P-CSCF that provides the proxy functions to the target is not on the signalling path. The CC interception is done at the IM-MGW. The MGCF sends the CC intercept trigger to the IM-MGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

E.10 Inter-CSP Forwarded Call to an IMS Domain

Figure E.10 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target receives an incoming call and the call is forwarded to a subscriber on the IMS domain of another CSP's network.

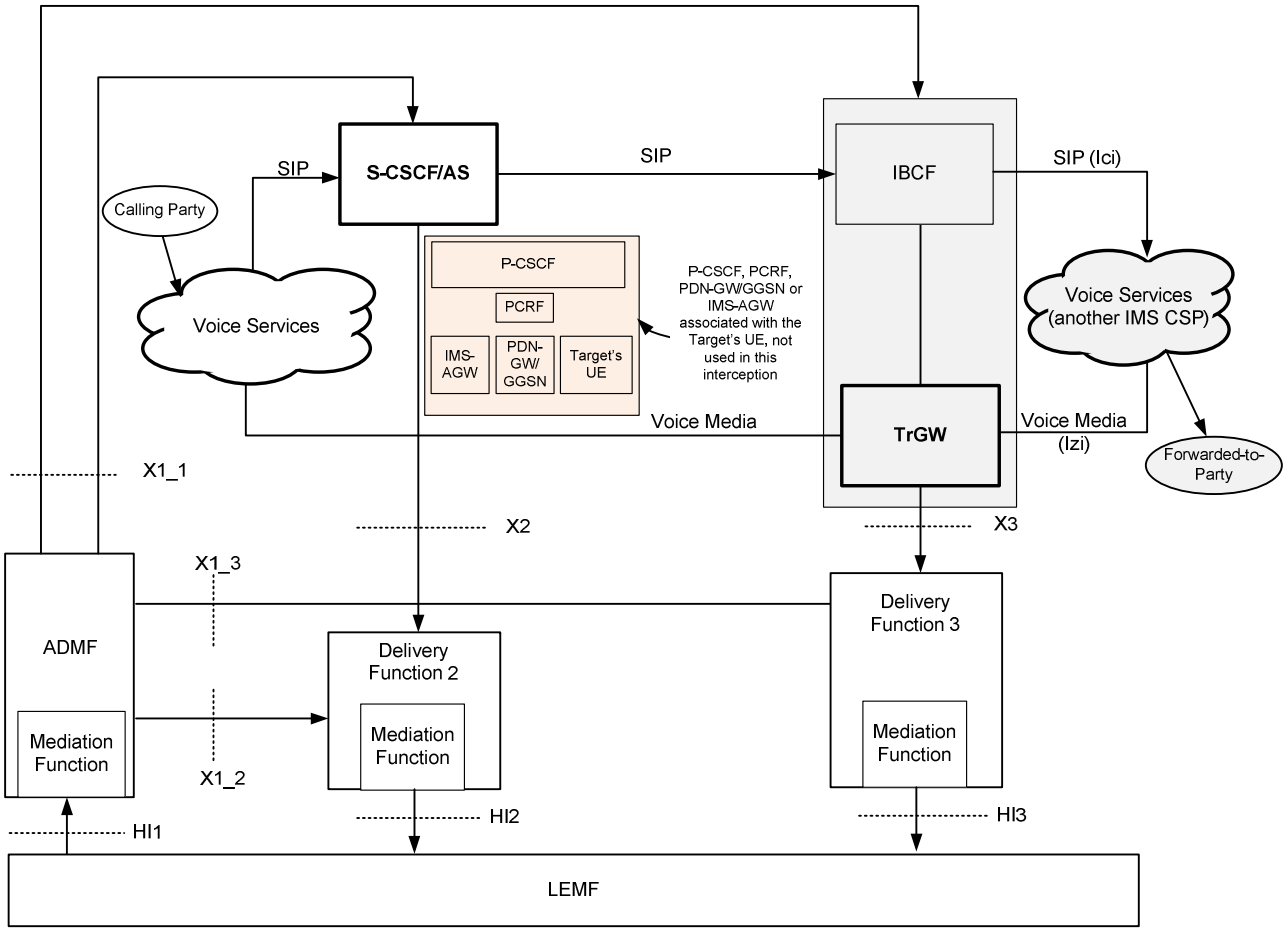


Figure E.10: VoIP lawful interception for an inter-CSP forwarded call to an IMS Domain

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target are not shown for simplification of the drawing.

Figure E.10 shows that the IRI interception is done at S-CSCF or AS. In this scenario, the IRI interception cannot occur in the P-CSCF since the P-CSCF that provides the proxy functions to the target is not on the signalling path. The CC interception is done at the TrGW. IBCF sends the CC intercept trigger to the TrGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

E.11 Originating Call from the Target with IMS Roaming

Figure E.11 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target originates a call with IMS roaming.

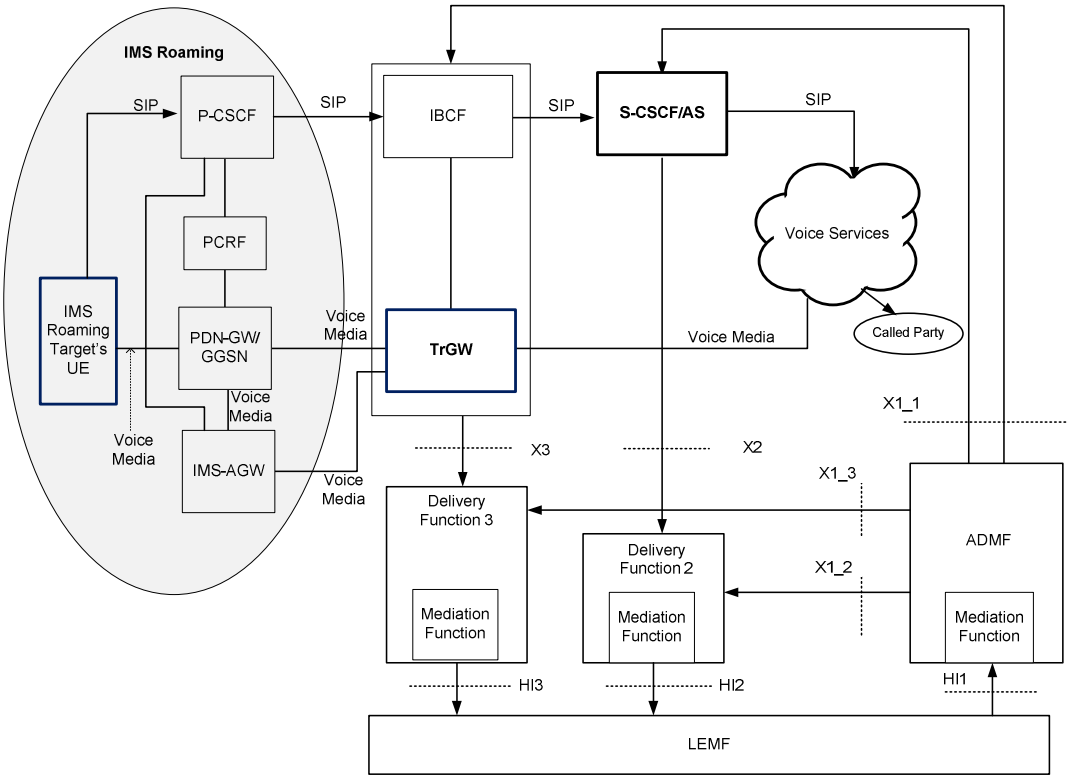


Figure E.11: VoIP lawful interception for an originating call with IMS Roaming

The cloud shown with the label "voice services" is to indicate that the target is making a voice call and the called party can be within the same CSP's network or in another CSP's network.

Figure E.11 shows that the IRI interception is done at S-CSCF or AS. The IRI interception at the P-CSCF does not apply to this configuration due to the fact that the P-CSCF resides at the visited CSP as a result of IMS roaming. The CC interception is done at the TrGW. The I-BCF sends the CC intercept trigger to the TrGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI, TEL URI or IMEI).

NOTE: The above is the case where optimal media routing is not employed. In the case where the optimal media routing is employed, the CC does not come to the TrGW.

E.12 Terminating Call to the Target with IMS Roaming

Figure E.12 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when a target with IMS roaming receives an incoming call.

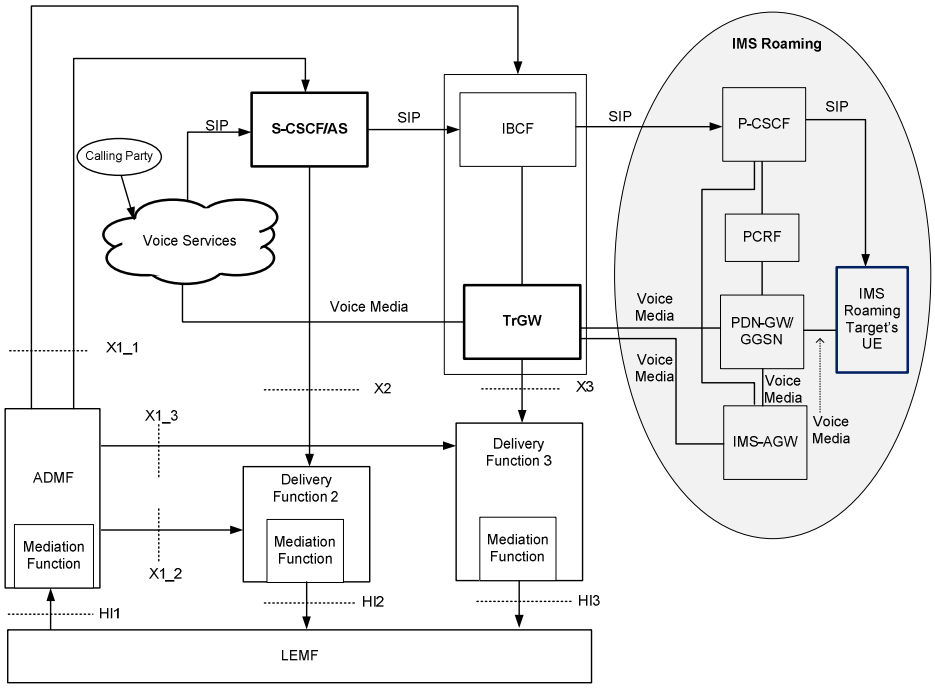


Figure E.12: VoIP lawful interception for a terminating call with IMS Roaming

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target are not shown for simplification of the drawing.

Figure E.12 shows that the IRI interception is done at S-CSCF or AS. The IRI interception at the P-CSCF does not apply to this configuration due to the fact that the P-CSCF resides at the visited CSP as a result of IMS roaming. The CC interception is done at the TrGW. The I-BCF sends the CC intercept trigger to the TrGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI, or TEL URI or IMEI).

E.13 Intra-CSP Forwarded Call with IMS Roaming

Figure E.13 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC, when an incoming call to a target gets forwarded to another subscriber who is IMS roaming. The target may or may not be IMS roaming.

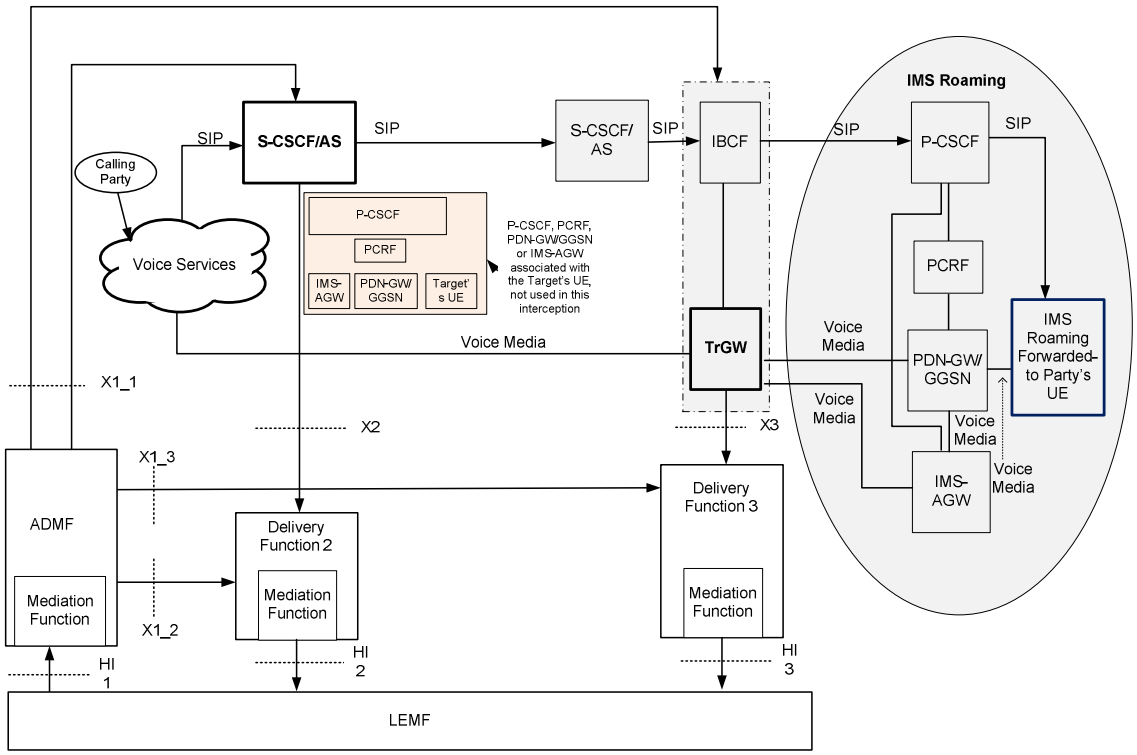


Figure E.13: VoIP lawful interception for a intra-CSP forwarded call with IMS Roaming

The cloud shown with the label "voice services" is to indicate that the target is receiving an incoming voice call and the calling party can be within the same CSP's network or in another CSP's network. The network nodes such as I-CSCF, HSS involved in the handling of an incoming call to the target are not shown for simplification of the drawing.

Figure E.13 shows that the IRI interception is done at S-CSCF or AS of the target. In this scenario, the IRI interception cannot occur in the P-CSCF since the P-CSCF that provides the proxy functions to the target is not on the signalling path. Since the forwarded-to-party is IMS roaming, the CC interception is done at the TrGW. IBCF sends the CC intercept trigger to the TrGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

NOTE 5: Void.

If the target is IMS roaming, but not the forwarded-to-party, then the CC interception for an intra-CSP forwarded call is done at the PDN-GW/GGSN (as illustrated in Z.9) or IMS-AGW (as illustrated in Z.8).

E.14 Lawful interception in the VPLMN with IMS roaming

E.14.1 Local Breakout (LBO) with P-CSCF in VPLMN

E.14.1.1 General

This clause illustrates a few scenarios of lawful interception functions in the VPLMN for inbound roaming targets. The LI functions described address the IMS roaming scenarios. Local Breakout (LBO), roaming architecture used for VoLTE, is an example of IMS roaming.

E.14.1.2 Originating call from an Inbound Roaming Target with CC Interception at the PDN-GW/GGSN

Figure E.14 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC in the VPLMN, when an inbound roaming target originates a call with PDN-GW (or GGSN) providing the CC interception.

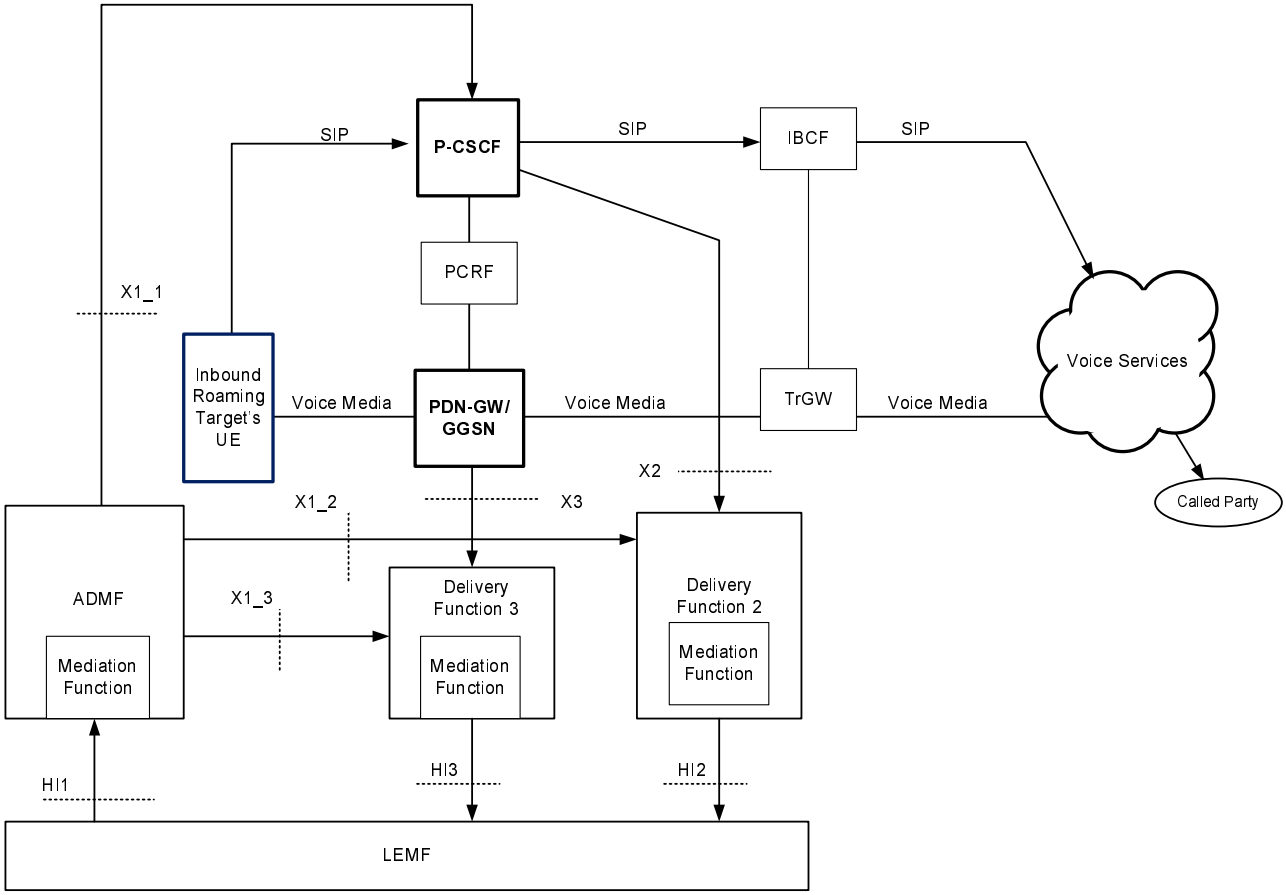


Figure E.14:VoIP lawful interception in VPLMN for an originating call with IMS Roaming with CC interception at the PDN-GW/GGSN

The routing of call to the called party can vary based on the CSP policy and the network that serves the called party. The cloud shown with the label "voice services" is to indicate that the inbound roaming target is making a voice call and the called party can be within the same VPLMN, or at the HPLMN or served by another CSP's network. At the Egress point, an IBCF/TrGW is shown. There can be other scenarios where different network nodes (e.g., TRF, MGCF, IM-MGW) can be present. However, lawful interception of an inbound roaming target in the VPLMN is independent of topology that involves such network nodes.

Figure E.14 shows that the IRI interception is done at P-CSCF. The CC interception is done at the PDN-GW/GGSN. The P-CSCF sends the CC intercept trigger to the PDN-GW/GGSN.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

Local Breakout (LBO) as a roaming architecture used for VoLTE is one of the examples of IMS roaming. Several call routing scenarios can happen with LBO. However, the lawful interception in the VPLMN is independent of all those call scenarios.

E.14.1.3 Originating Call from an Inbound Roaming Target with CC Interception at the IMS-AGW

Figure E.15 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC in the VPLMN, when an inbound roaming target originates a call with IMS-AGW providing the CC interception.

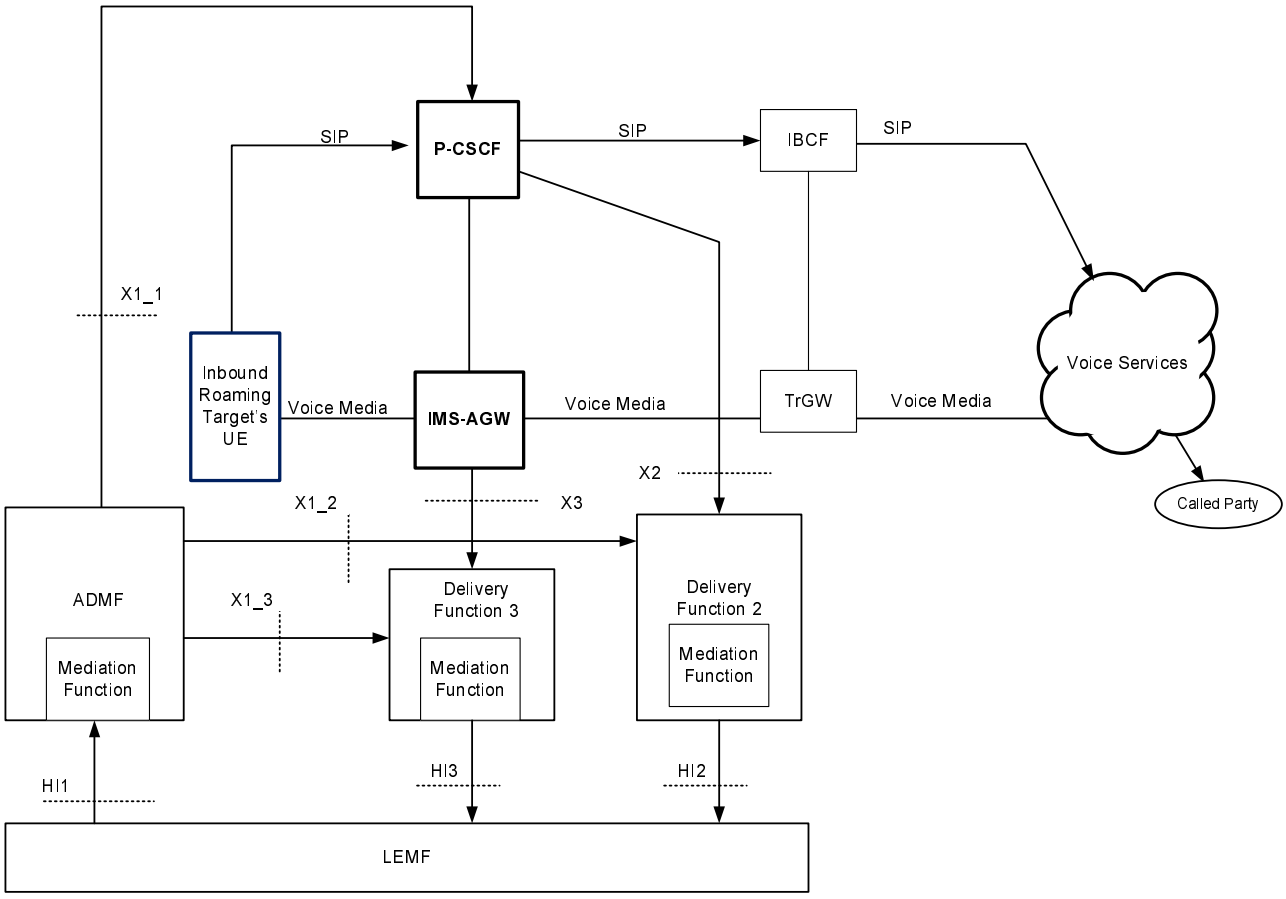


Figure E.15: VoIP lawful interception in VPLMN for an originating call with IMS Roaming with CC interception at the IMS-AGW

The routing of call to the called party can vary based on the CSP policy and the network that serves the called party. The cloud shown with the label "voice services" is to indicate that the inbound roaming target is making a voice call and the called party can be within the same VPLMN, or at the HPLMN or served by another CSP's network. At the Egress point, an IBCF/TrGW is shown. There can be other scenarios where different network nodes (e.g., TRF, MGCF, IM-MGW) can be present. However, lawful interception of an inbound roaming target in the VPLMN is independent of topology that involves such network nodes.

Figure E.15 shows that the IRI interception is done at P-CSCF. The CC interception is done at the IMS-AGW. The P-CSCF sends the CC intercept trigger to the IMS-AGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

Local Breakout (LBO) as a roaming architecture used for VoLTE is one of the examples of IMS roaming. Several call routing scenarios can happen with LBO. However, the lawful interception in the VPLMN is independent of all those call scenarios.

E.14.1.4 Terminating Call to an Inbound Roaming Target with the CC Interception at the PDN-GW/GGSN

Figure E.16 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC in the VPLMN, when an inbound target receives an incoming call with PDN-GW (or GGSN) providing the CC interception.

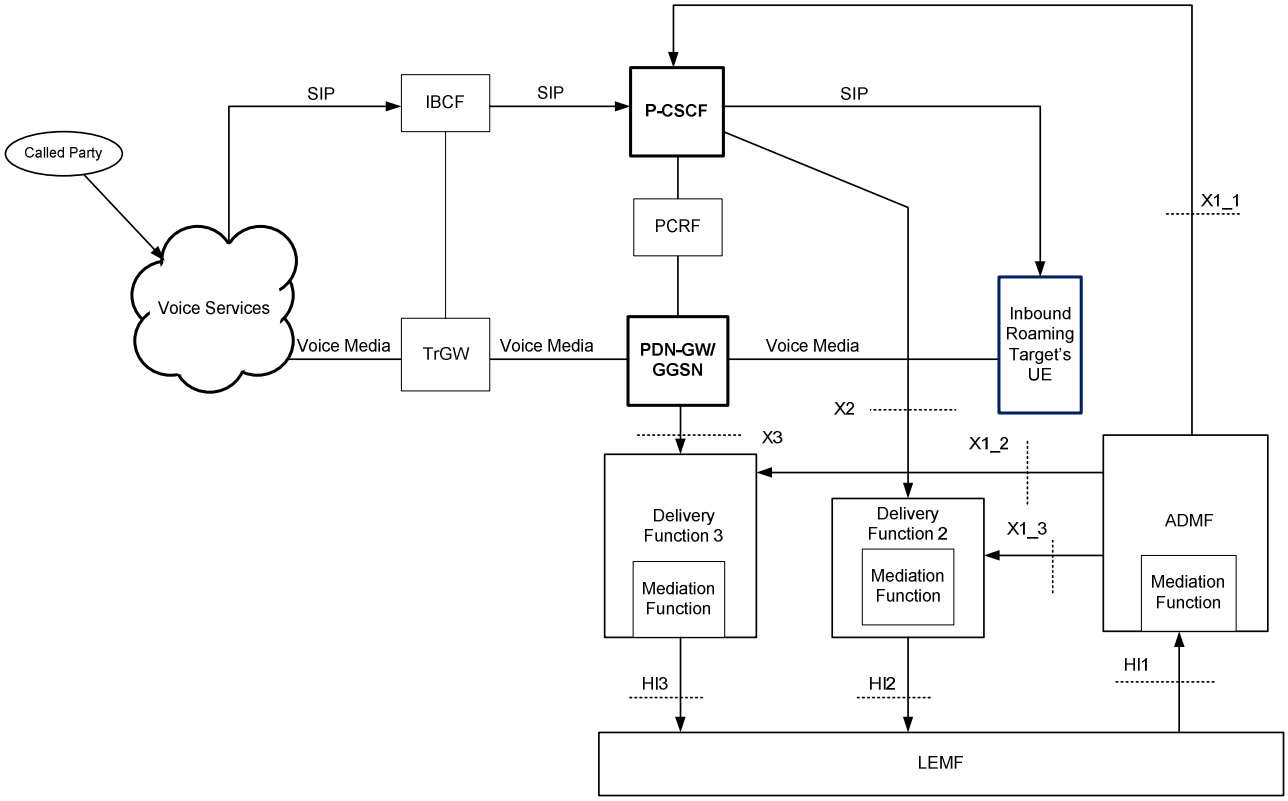


Figure E.16: VoIP lawful interception in the VPLMN for a terminating call with IMS Roaming with CC interception at the PDN-GW/GGSN

A terminating call is always routed to the VPLMN via the HPLMN of the target. The cloud shown with the label "voice services" is to indicate the calling party can be within the same VPLMN, or in the HPLMN of the target, or in another CSP's network. At the Ingress point, an IBCF/TrGW is shown. Independent of where the call has originated from, a terminating call always enters the VPLMN through the IBCF/TrGW from the HPLMN.

Figure E.16-1 shows that the IRI interception is done at P-CSCF. The CC interception is done at the PDN-GW/GGSN. The P-CSCF sends the CC intercept trigger to the PDN-GW/GGSN.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

Local Breakout (LBO) as a roaming architecture used for VoLTE is one of the examples of IMS roaming.

E.14.1.5 Terminating Call to an Inbound Roaming Target with CC Interception at the IMS-AGW

Figure E.17 provides the lawful interception architecture to illustrate the interception and delivery of IRI and CC in the VPLMN, when an inbound target receives an incoming call with IMS-AGW providing the CC interception.

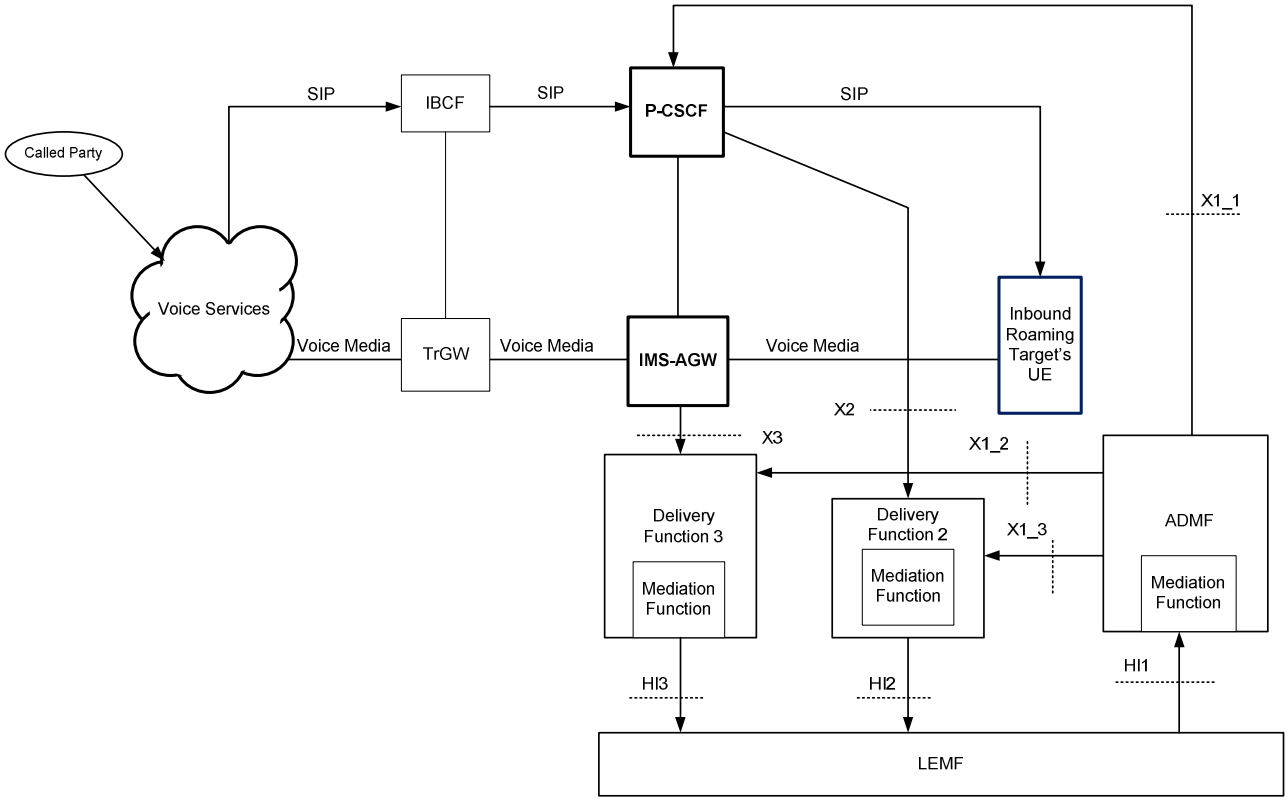


Figure E.17: VoIP lawful interception in the VPLMN for a terminating call with IMS Roaming with CC interception at the IMS-AGW

A terminating call is always routed to the VPLMN via the HPLMN of the target. The loud shown with the label "voice services" is to indicate the calling party can be within the same VPLMN, or in the HPLMN of the target, or in another CSP's network. At the Ingress point, an IBCF/TrGW is shown. Independent of where the call has originated from, a terminating call always enters the VPLMN through the IBCF/TrGW from the HPLMN.

Figure E.17 shows that the IRI interception is done at P-CSCF. The CC interception is done at the IMS-AGW. The P-CSCF sends the CC intercept trigger to the IMS-AGW.

The activation of intercept is done by the ADMF for IRI interception and CC interception using the same target identity (SIP URI or TEL URI).

Local Breakout (LBO) as a roaming architecture used for VoLTE is one of the examples of IMS roaming.

Annex F (informative): Examples of IMS-based VoIP Lawful Interception (LI) call flows

F.1 General remarks

All the call flows illustrate that the CC delivery begins once the SDP offer and answer is completed (i.e., when the media bearer is setup). In all the call flows, the first reliable response is SIP 200 OK.

In all the call flows, the originating end of the call sends the SDP offer and terminating end gives the SDP answer. Since, the first reliable response is SIP 200 OK, the SDP answer is always given in the SIP 200 OK message.

The call flows assume that per clause 7.A, the IRI for VoIP is nothing but the delivery encapsulated SIP messages. The call flows do not show the method used for correlating the IRI with IRI and IRI with CC. It is presumed that those are stage 3 details.

All the call flows assume the presence of a Voice Application Server (shown as AS) that provides the voice services like digit translation, invoking the call forwarding, etc.

IRI in the visited CSP is intercepted by the P-CSCF and IRI in the home CSP is intercepted by the S-CSCF.

The call flows show that CC interception is done at the IP-CAN (and it should be interpreted to mean that the interception is done in the PDN-GW or GGSN depending on the packet core network), or at the TrGW or at the IM-MGW. The other possible CC interception options (e.g., IMS-AGW) are not shown.

Not all the functional elements are shown in the call flows. For example, the call flows do not show I-CSCF, HSS, PCRF.

All the call flows show a summary of SIP messages that are delivered to the LEA (not all SIP messages are shown). The term LEMF, used in some call flows, means it is an equivalent of LEA.

For each call flow, references are required to identify MMTEL service that it illustrates (for further study).

F.2 Call Originations from Target in Home CSP

F.2.0 Introduction

This clause gives 2 call flows to illustrate the call origination scenarios.

Figure F.1 illustrates the case where the Party_A (target) calls Party_B.

Figure F.2 illustrates the case where the Party_A (target) dials a special number (e.g., a speed call number or an 800-number), which is translated to Party_B by the AS.

F.2.1 Target Originated Call - Target (Party_A) Calls Party_B

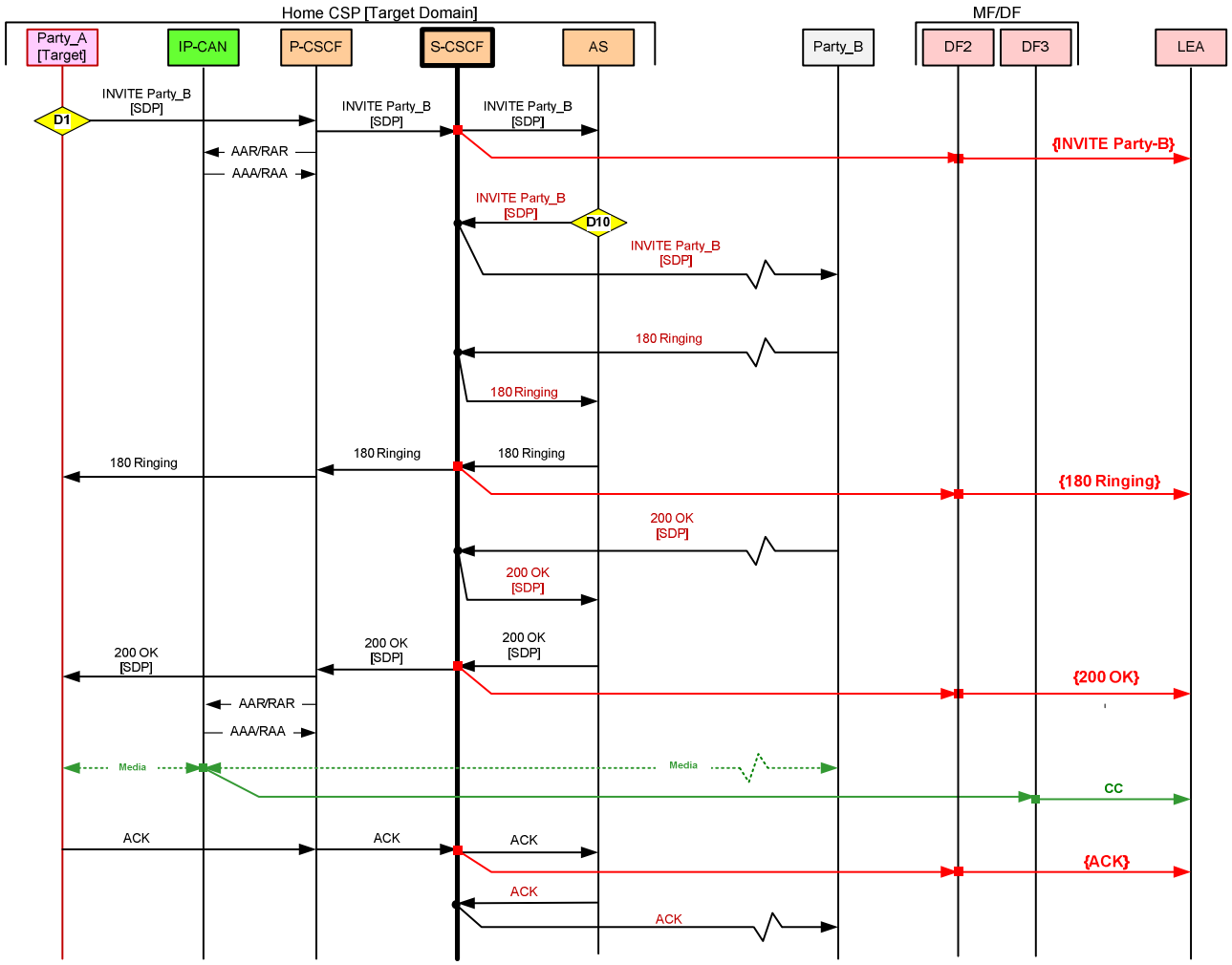


Figure F.1: Target originated call - target calls Party_B

F.2.2 Target Originated Call - Target (Party_A) dials a Special Number

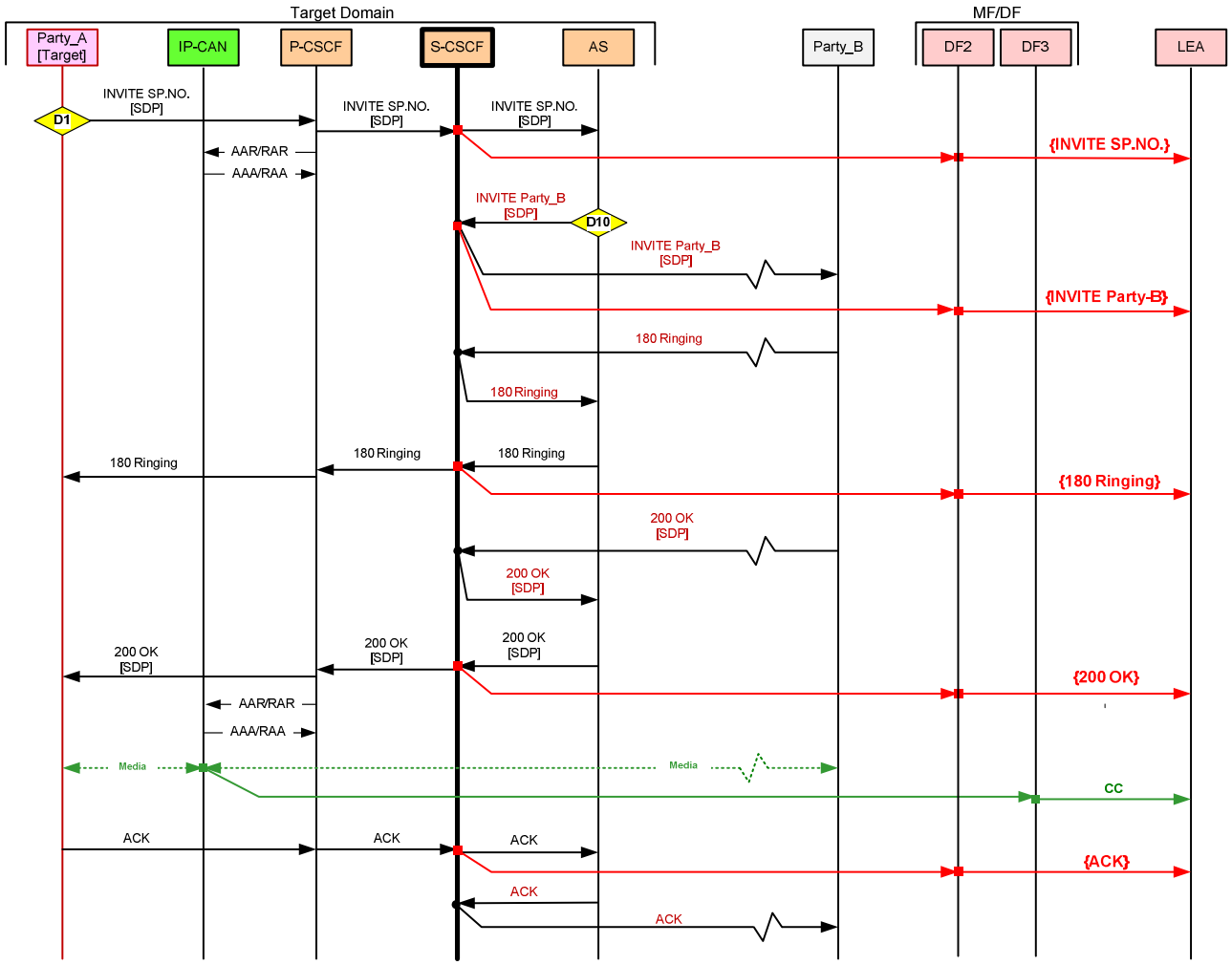


Figure F.2: Target originated call - target dials a special number

F.3 Call Terminations to Target - Home CSP

F.3.0 Introduction

This clause gives 1 call flow to illustrate the call termination scenario.

Figure F.3 illustrates the case where the Party_A calls target (Party_B).

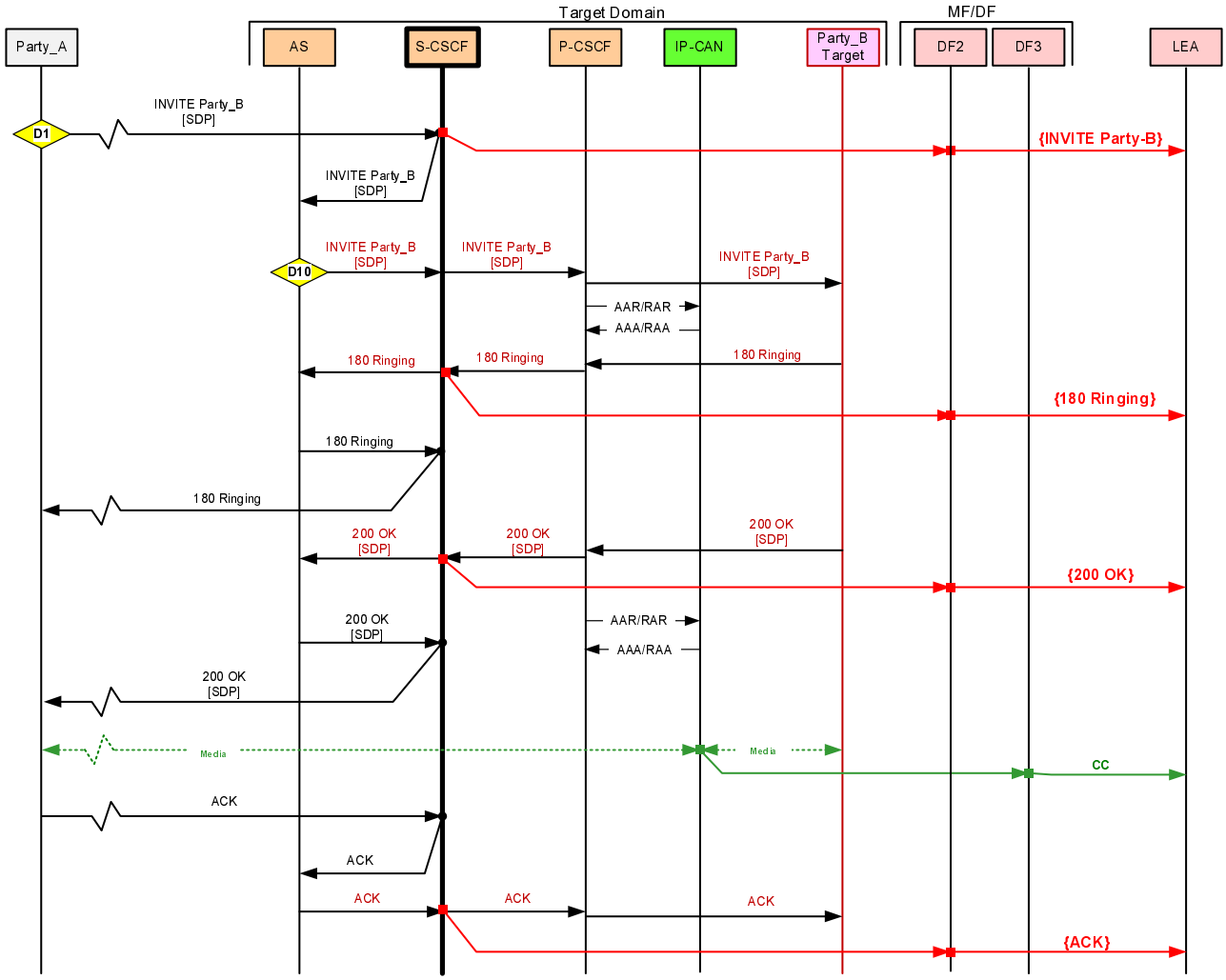


Figure F.3: Target receives an incoming call

F.4 Call Forwarding - Non Roaming

F.4.0 Introduction

This clause gives 4 call flows to illustrate call forwarding scenarios.

Figure F.4 illustrates the case of an intra-CSP call forwarding unconditional. Here, the Party_A calls target (Party_B). The AS determines that all incoming calls to the target have to be forwarded to Party_C served by the same CSP.

Figure F.5 illustrates the case first part of an intra-CSP call forwarding no answer. Figure F.6 illustrate the second part of an intra-CSP call forwarding no answer. Here, the Party_A calls target (Party_B). . The target does not answer and the AS determines that target has a call forwarding no answer enabled to Party_C served by the same CSP.

Figure F.7 illustrates the case of inter-CSP call forwarding unconditional. Here, the Party_A calls target (Party_B). The AS determines that all incoming calls to the target have to be forwarded to Party_C served by a different CSP.

F.4.1 Intra-CSP Call Forwarding Unconditional

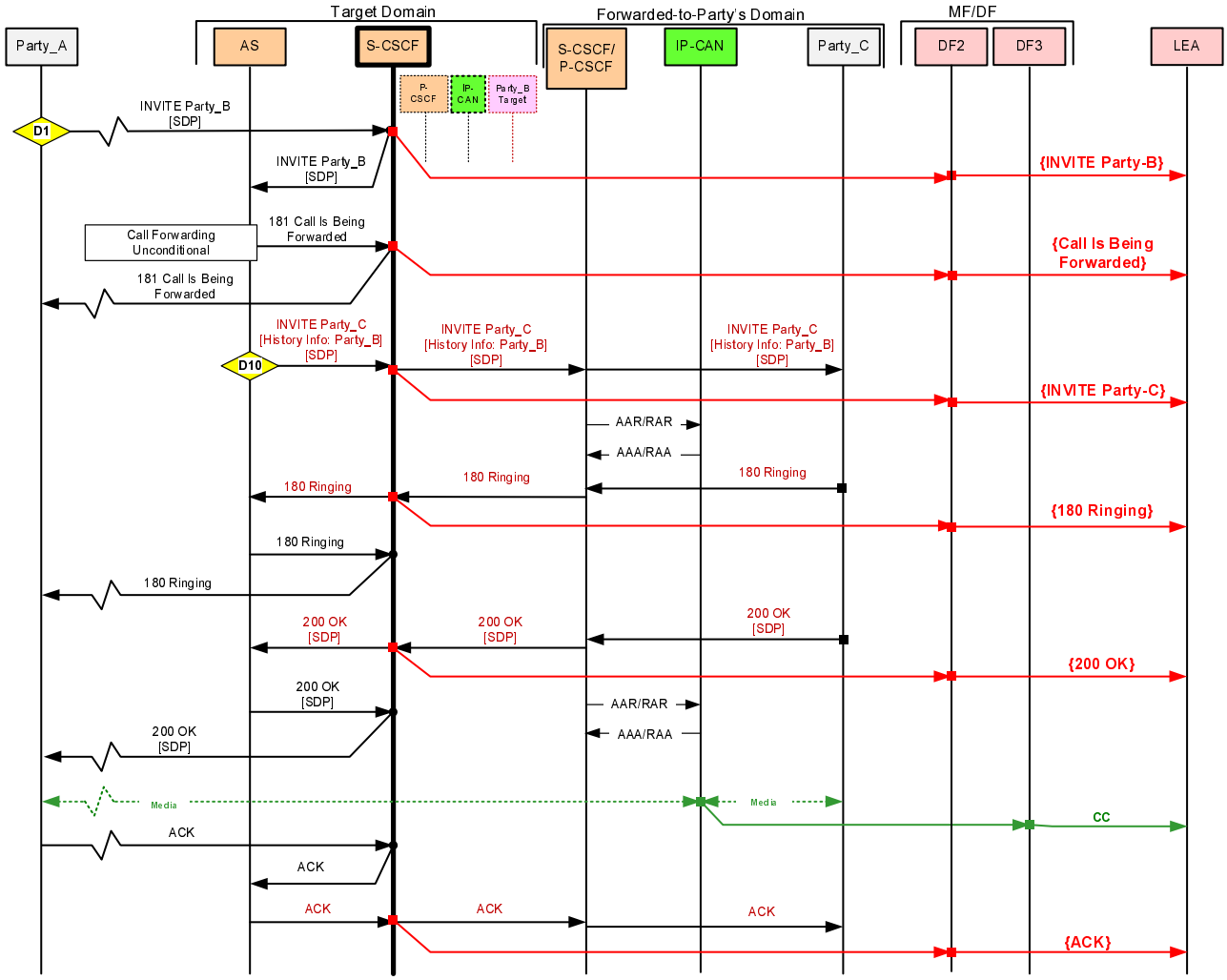


Figure F.4: Incoming call to target is forwarded within the CSP

F.4.2 Intra-CSP Call Forwarding No Answer

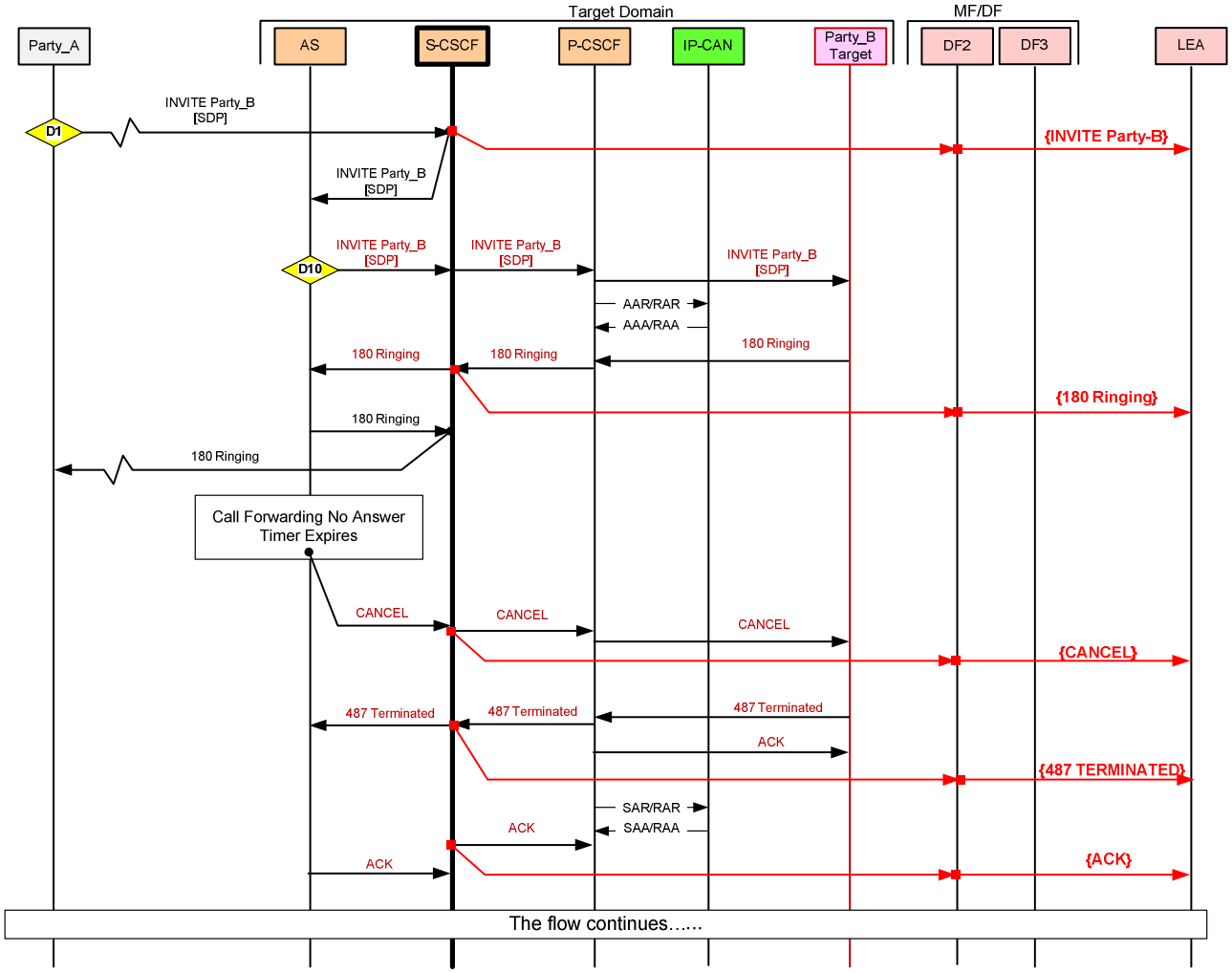


Figure F.5: Incoming call to target is forwarded due to call forwarding no answer within the CSP (flow 1 of 2)

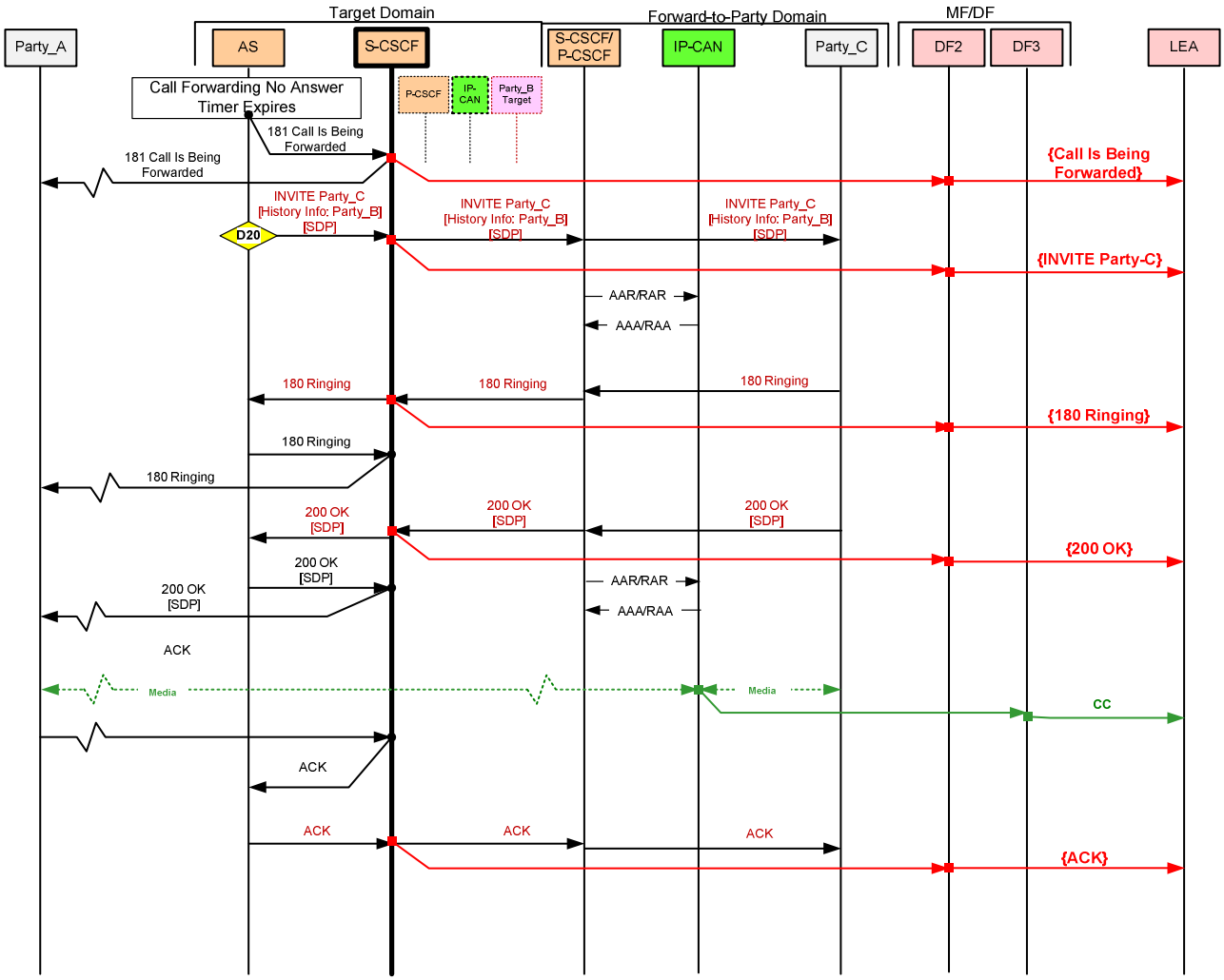


Figure F.6: Incoming call to target is forwarded due to call forwarding no answer within the CSP (flow 2 of 2)

F.4.3 Inter-CSP Call Forwarding Unconditional

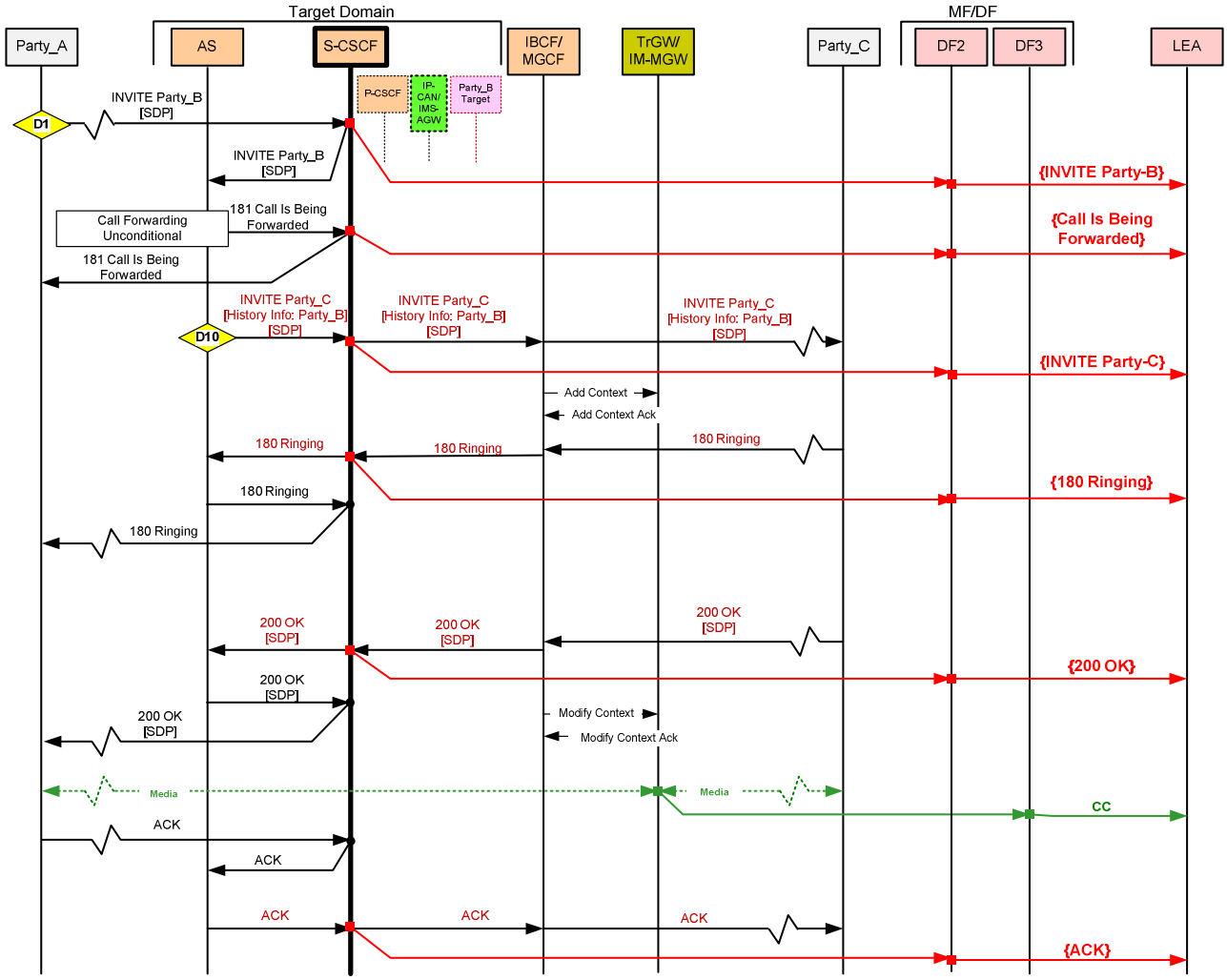


Figure F.7: Incoming call to target is forwarded outside the CSP

F.5 IMS Roaming

F.5.0 General

This clause gives 3 call flows to illustrate the case of IMS roaming.

Figure F.8 illustrate the case where the roaming target originates a call. Here, roaming target (Party_A) calls Party_B who is served by the same CSP as that of target. Party_B is not roaming.

Figure F.8A illustrates the case where a roaming target originates a call with local breakout approach is used for roaming. In this case, home CSP of Party-B happens to be visited CSP where the target is roaming and hence, the media does not enter the HPLMN of target (i.e., Home CSP of target). A Home CSP reports the CC unavailability to the LEMF with "roaming" as the reason for CC unavailability.

Figure F.9 illustrates the case where a roaming target receives an incoming call. Here, non-roaming Party_A, who is served by the same CSP as that of target, calls the target (Party_B).

F.5.1 Roaming Target Originates a Call

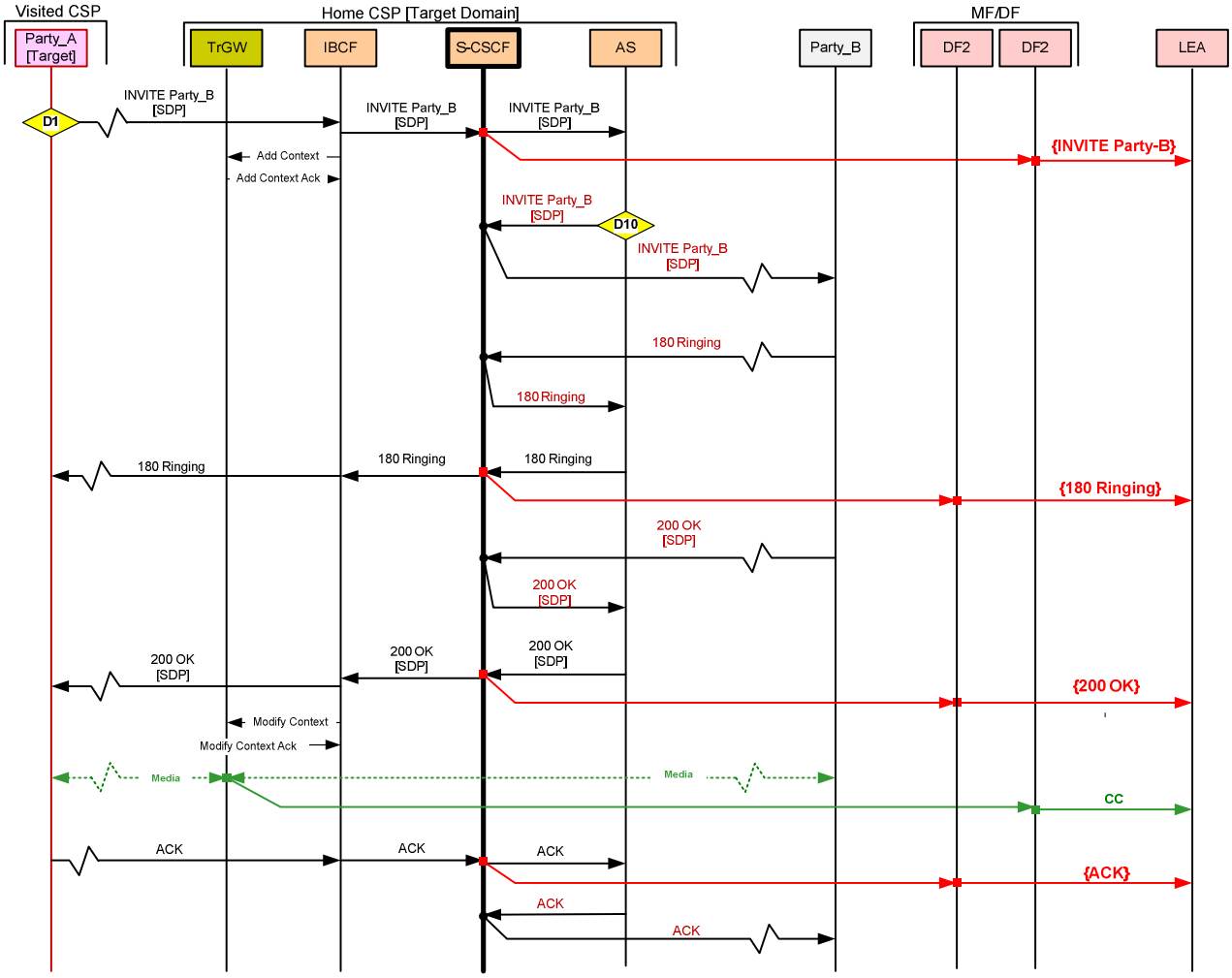


Figure F.8: Roaming target originates a call

NOTE: The above call flow is the case where optimal media routing is not employed. In the case where the optimal media routing is employed, the CC does not come to the TrGW.

F.5.1A CC Unvailable in Home CSP due to Optimal Media Routing

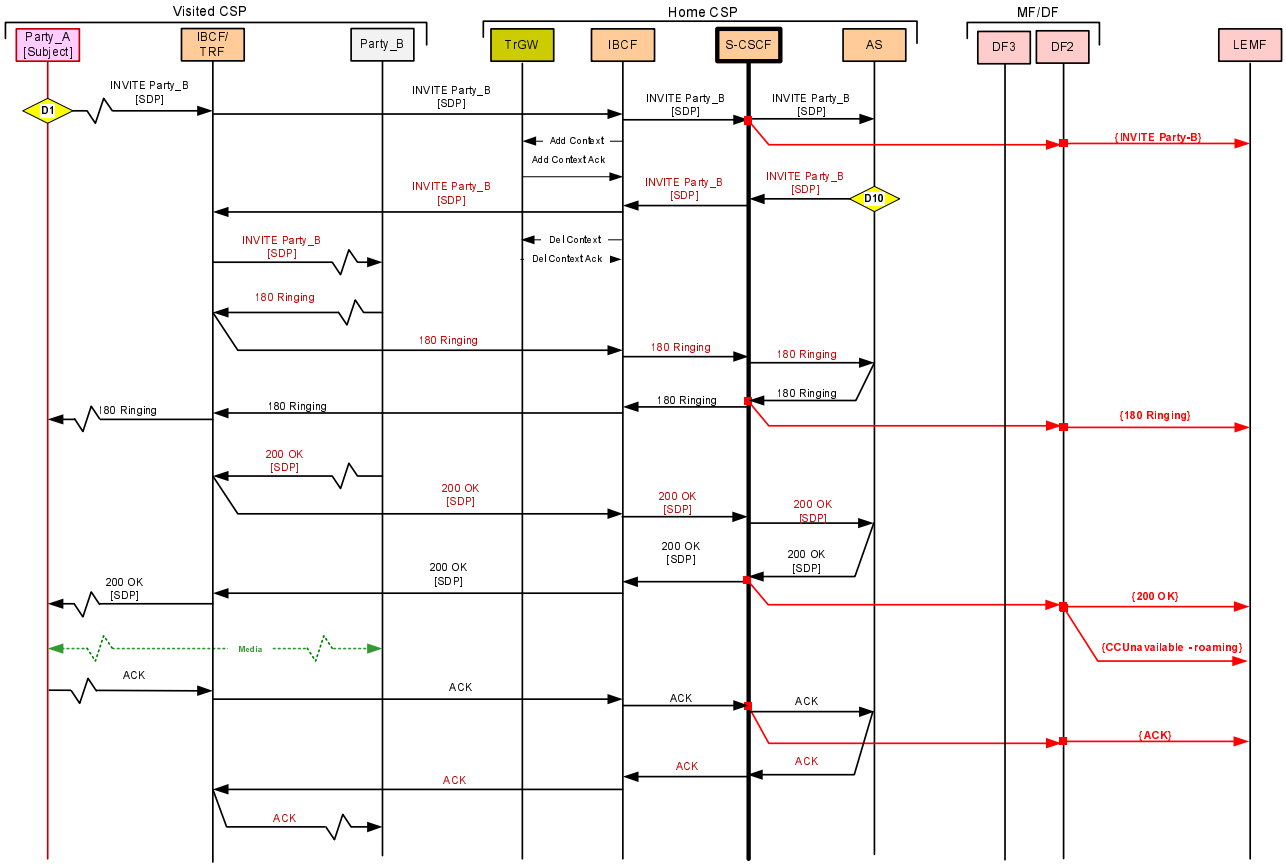


Figure F.8A: Roaming target originates a call and optimal media routing is applied

NOTE: Many different call scenarios exist that employ optimal media routing. In this particular example, the called party (Party_B) happens to be served by the same CSP where the target is currently roaming (i.e., HPLMN of Party_B is the visited CSP of Party_A).

F.5.2 Call Termination to a Roaming Target

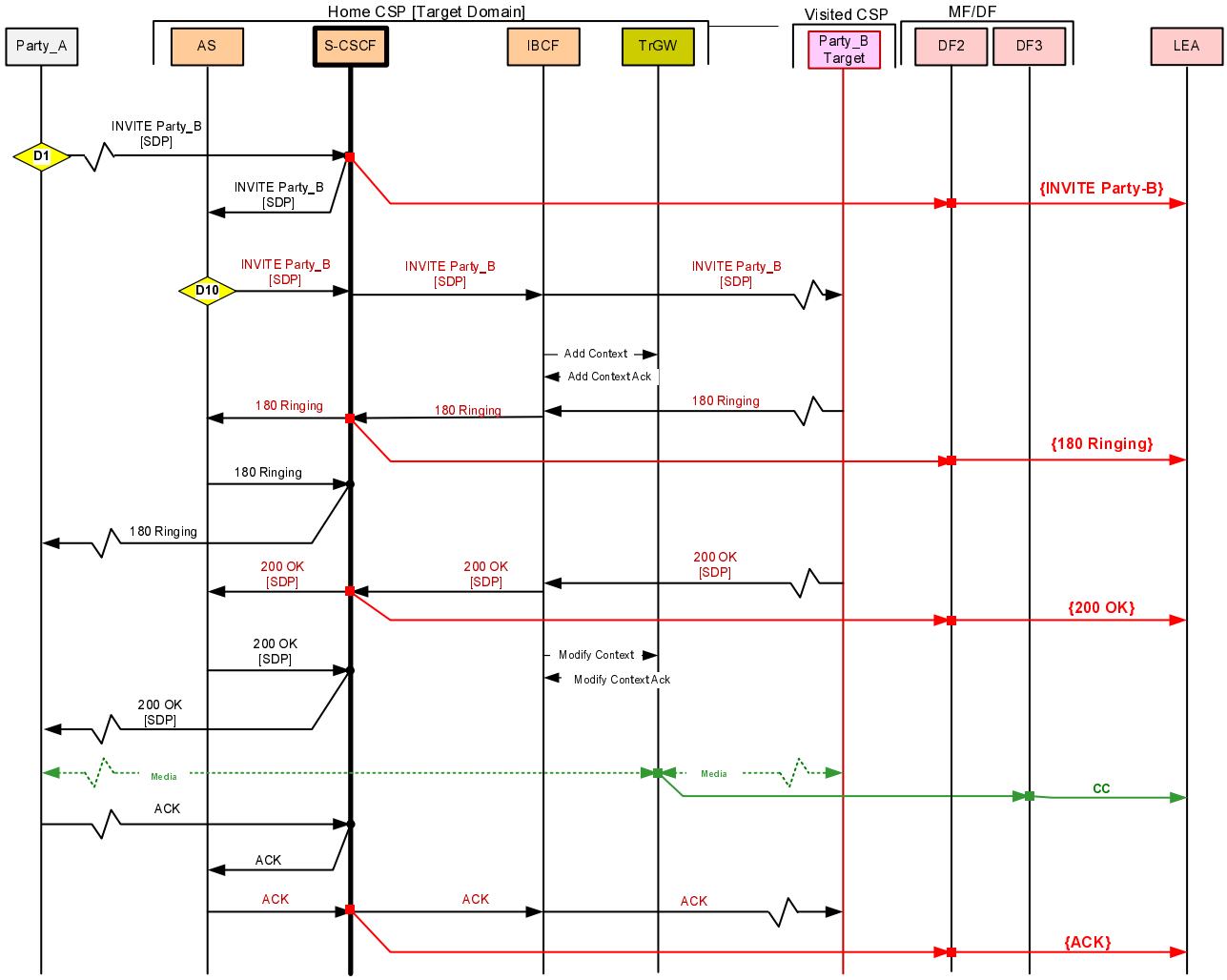


Figure F.9: Roaming target receives an incoming call

F.6 Interception in Visited CSP

F.6.0 General

This clause gives 3 call flows to illustrate the case of interception in the visited CSP. In all these flows, the IRI interception happens at the P-CSCF. Both IRI and CC interception happen in the visited CSP.

Figure F.10 illustrates the case where the target (Party_A) in the visited CSP originates a call dialing a special number. The special number is translated into Party_B in the home CSP. The flow also assumes that the interception is done only in the visited CSP.

Figure F.11 illustrates the case where the target (Party_B) in the visited CSP receives an incoming call from Party_A served by the same Home CSP. The flow assumes that the interception is done only in the visited CSP.

Figure F.12 illustrates the case where an incoming call to the target (Party_B) gets forwarded in the Home CSP due to call forwarding no answer. The flow also assumes that the interception is done only in the visited CSP.

F.6.1 Interception in Visited CSP - Target Originated Call

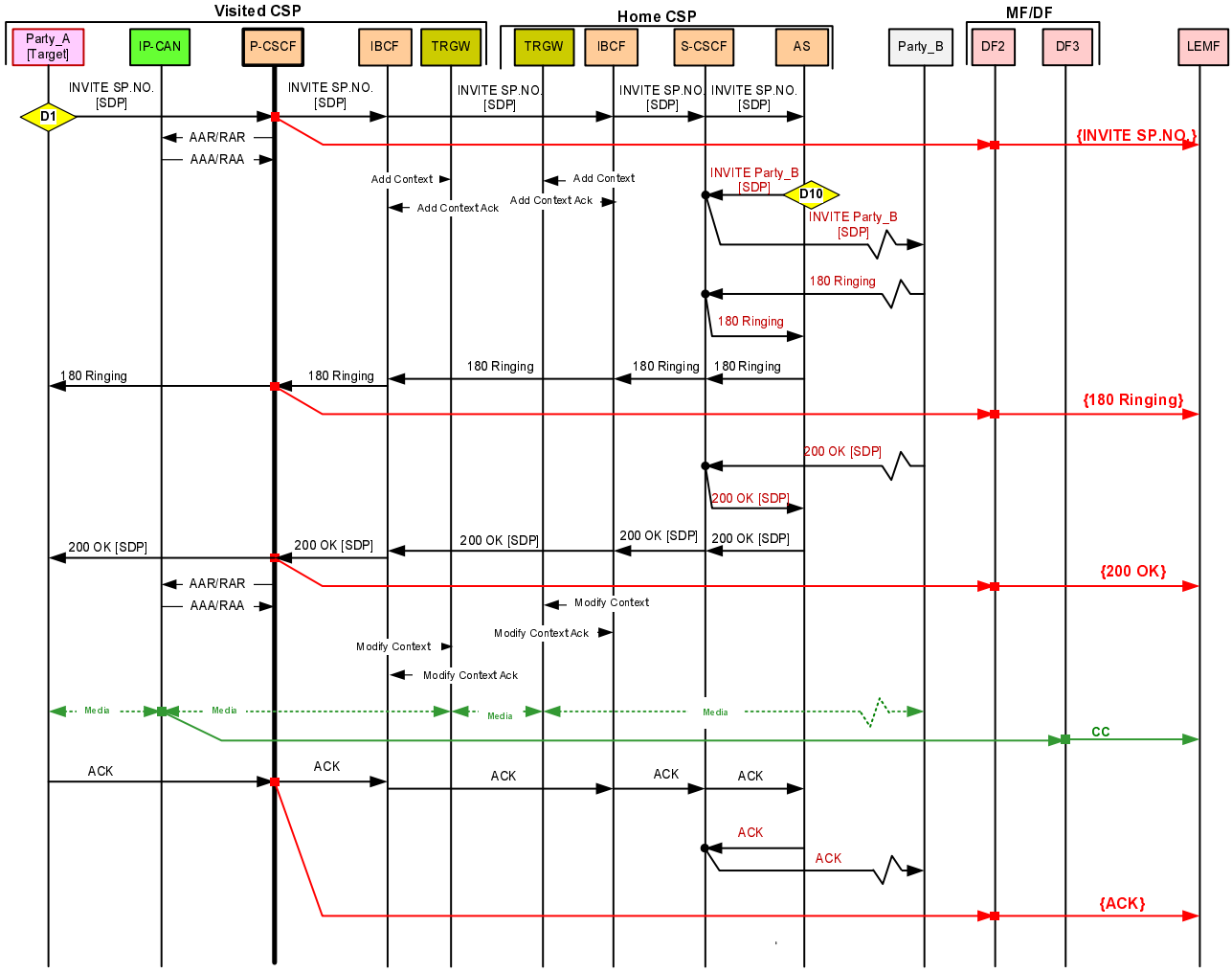


Figure F.10: Roaming target originates a call - interception in the visited CSP

F.6.2 Interception in Visited CSP - Target Terminating Calls.

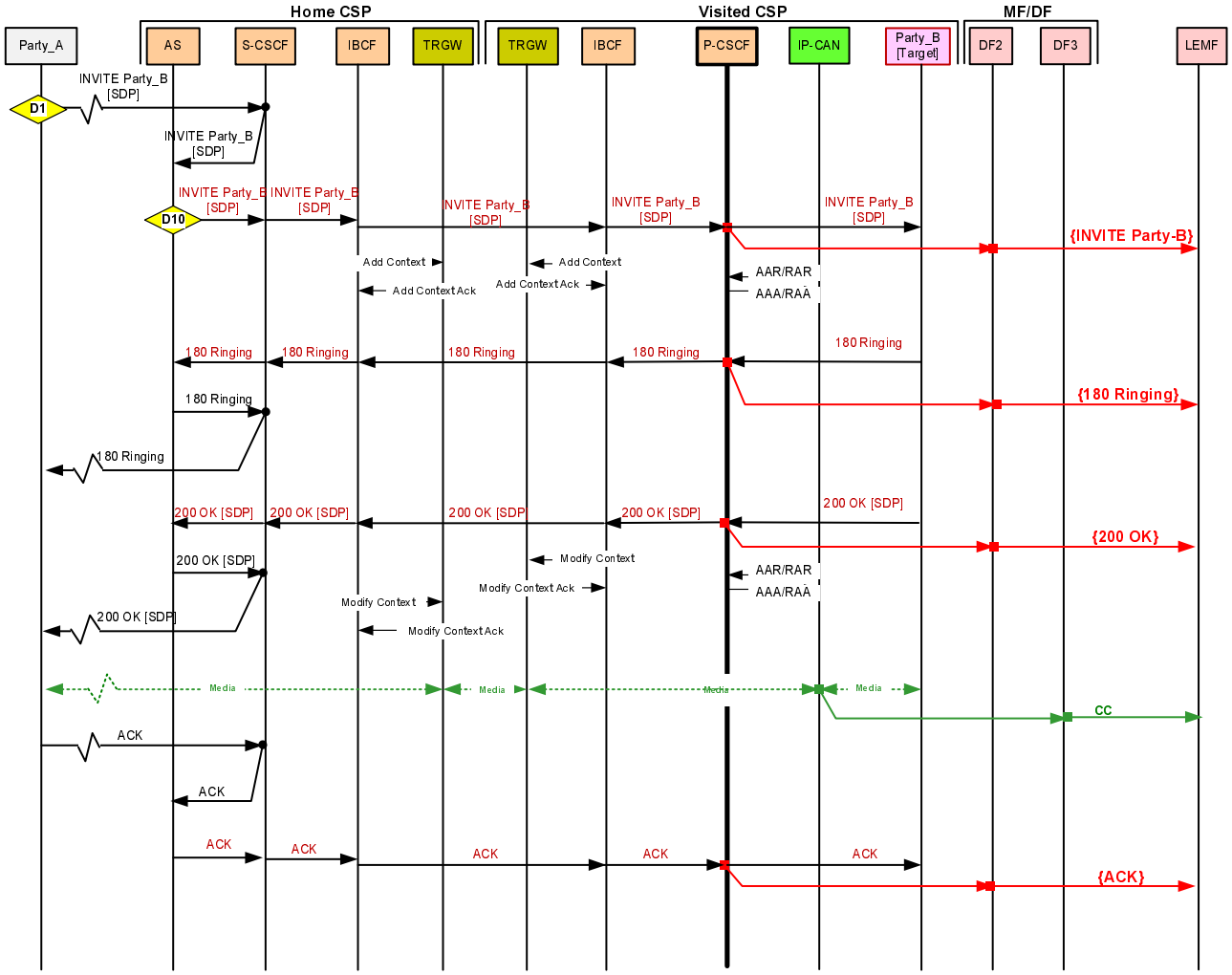


Figure F.11: Roaming target receives a call - interception in the visited CSP

F.6.3 Incoming Call to Roaming Target is forwarded due to Call Forwarding No Answer

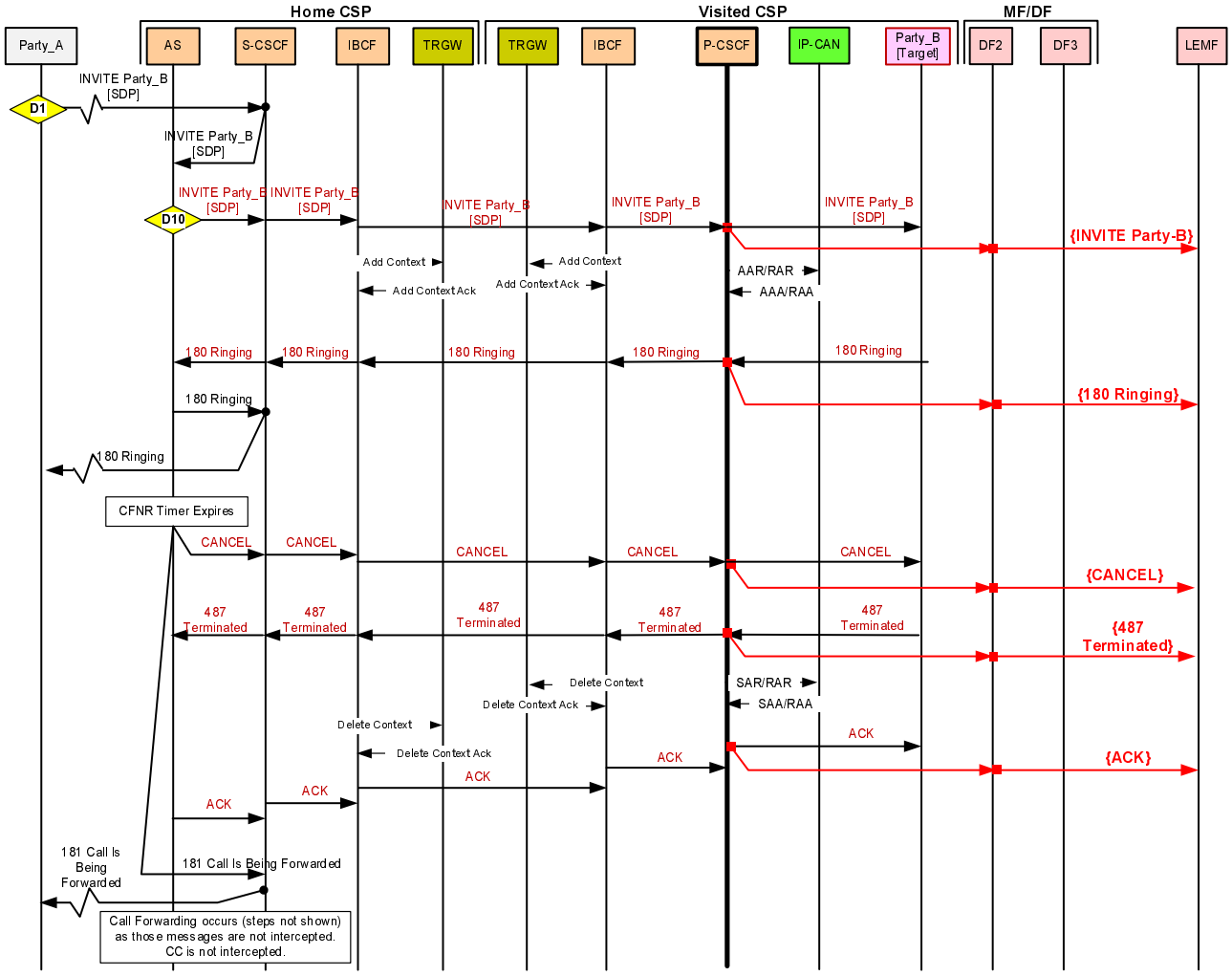


Figure F.12: Incoming call to target is forwarded in the home CSP due to Call Forwarding No Answer - interception in visited CSP

F.7 Ad-Hoc Conference Calls established by the Target

F.7.0 Introduction

This clause gives 9 call flows to illustrate the steps related to ad-hoc conference calling established by the target. The flows assume that the Party_A (target) has already made two calls, one to Party_B and one to Party_C, and placed both calls on hold so as to merge the two calls into a conference.

Figure F.7.1 illustrates the case where the Party_A (target) creates the conference.

Figure F.7.2 and Figure F.7.3 illustrate the case where the Party_A (target) brings the Party_C into the conference.

Figure F.7.4 and F.7.5 illustrate the case where the Party_A (target) brings the Party_B into the conference.

Figure F.7.6 illustrates the case where Party_C drops out of the conference call.

Figure F.7.7 illustrates the case where the call between two parties (Party_A (target) and Party_B) is converted back to a normal 2-party call.

Figure F.7.8 illustrates the case where Party_A (target) places the conference on hold.

Figure F.7.9 illustrates the case where Party_A (target) retrieves the held conference from hold.

Some of the steps may be executed by the target's UE automatically (in other words, no action is required by the target). For example, when the target tries to merge the call, the target's UE may execute the steps shown in Figure F.7.1, Figure F.7.2, Figure F.7.3, Figure F.7.4, Figure F.7.5 automatically in a serial fashion. The same way, the steps shown in Figure F.7.7 may be executed automatically after the steps shown in Figure F.7.6 when one of the conferees drop out of the conference.

The Figure F.7.8 and Figure F.7.9 are not really part of the conferencing steps, however, included here to show how the content of a held conference call (a requirement in some countries) is delivered to the LEAs.

F.7.1 Party_A (target) creates the conference

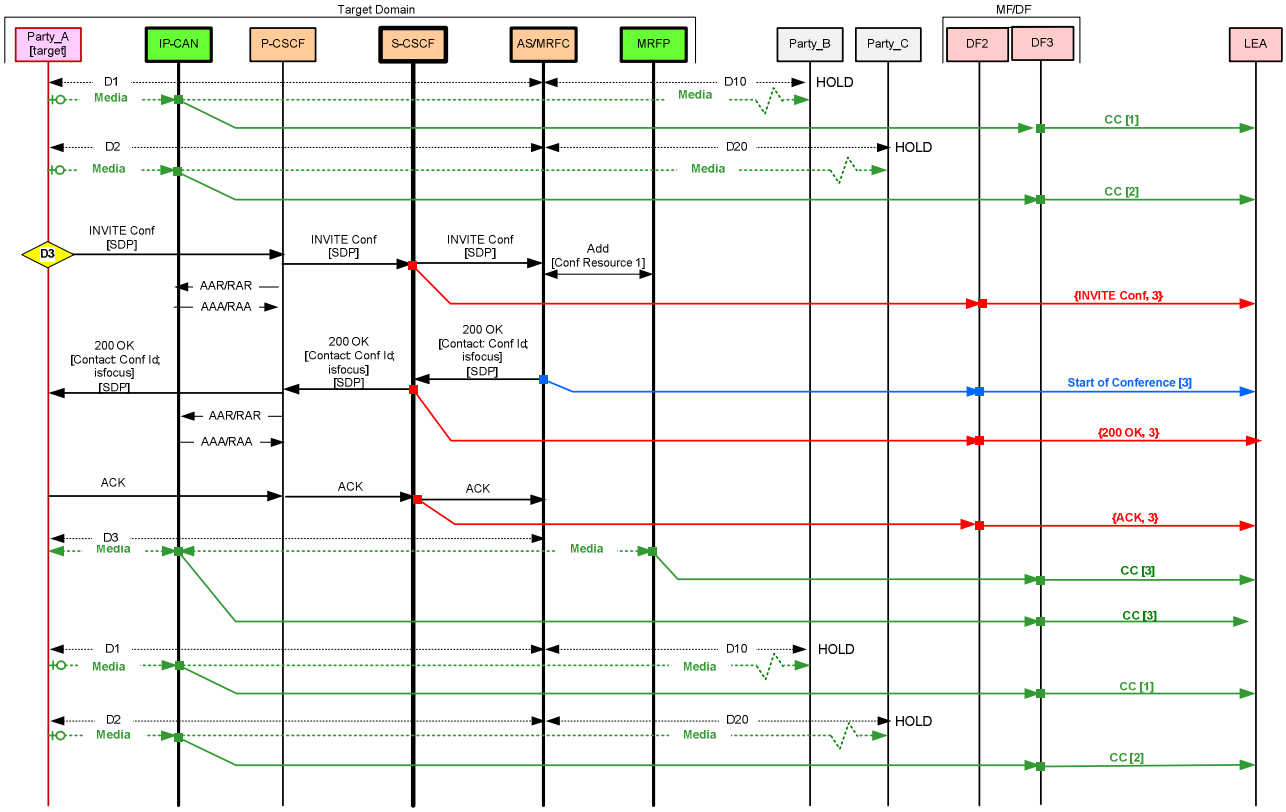


Figure F.7.1: Party_A (target) creates the conference

D1 and D10 represent the dialogue of the original call between the Party_A (target) and the Party_B. D2 and D20 represent the original the dialogue of the original call between Party_A (target) and the Party_C. D3 represents the new dialogue of call between Party_A and the conference.

The IRI/CC delivered for D1 and D10 use the Correlation Number 1. The IRI/CC delivered for D2 and D20 use the Correlation Number 2. The IRI/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3.

F.7.2 Party_C joins the conference

This flow is illustrated in two figures: Figure F.7.2 and Figure F.7.3.

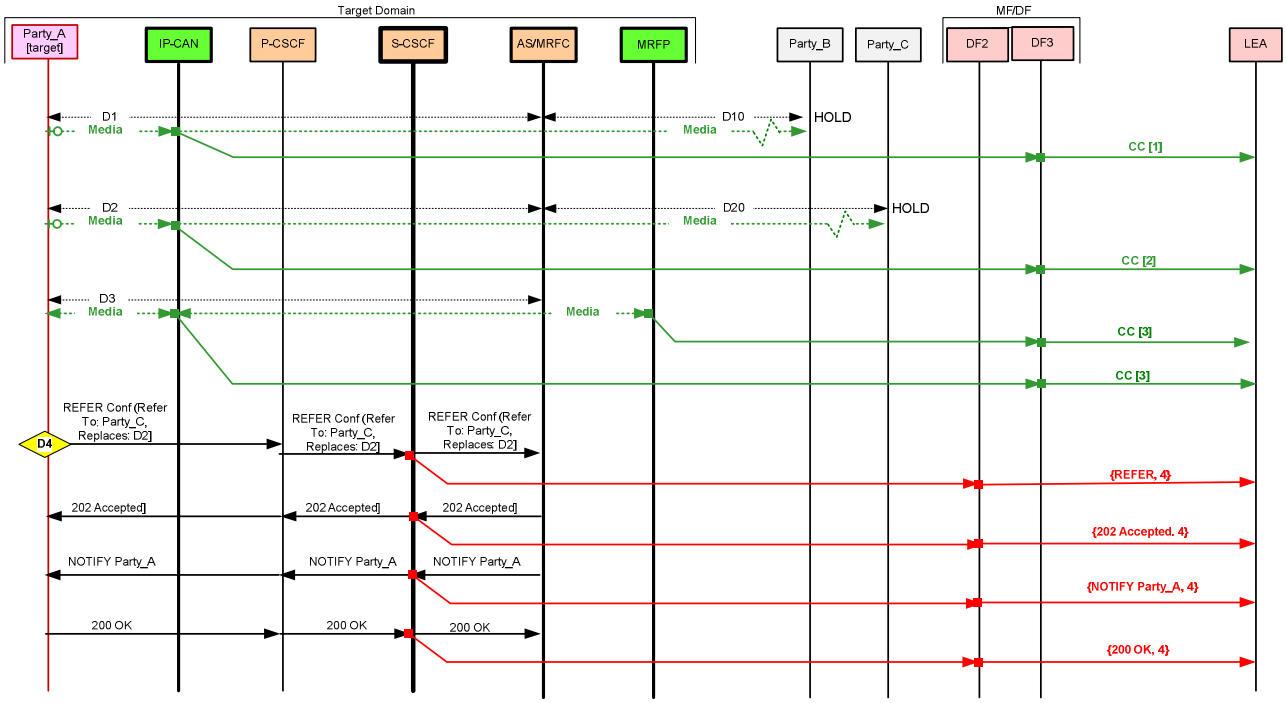


Figure F.7.2: Party_C joins the conference (flow 1 of 2)

D1 and D10 represent the dialogue of the original call between the Party_A (target) and the Party_B. D2 and D20 represent the original the dialogue of the original call between Party_A (target) and the Party_C. D3 represents the dialogue of the call between Party_A and the conference. D4 represents the dialogue that the Party_A (target) uses to refer Party_C to the conference.

NOTE: Here, REFER is sent by Party_A outside of any existing dialogues. Sending of REFER inside a dialogue is also possible.

The IRI/CC delivered for D1 and D10 use the Correlation Number 1. The IRI/CC delivered for D2 and D20 use the Correlation Number 2. The IRI/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3. The IRI for D4 uses the Correlation Number 4.

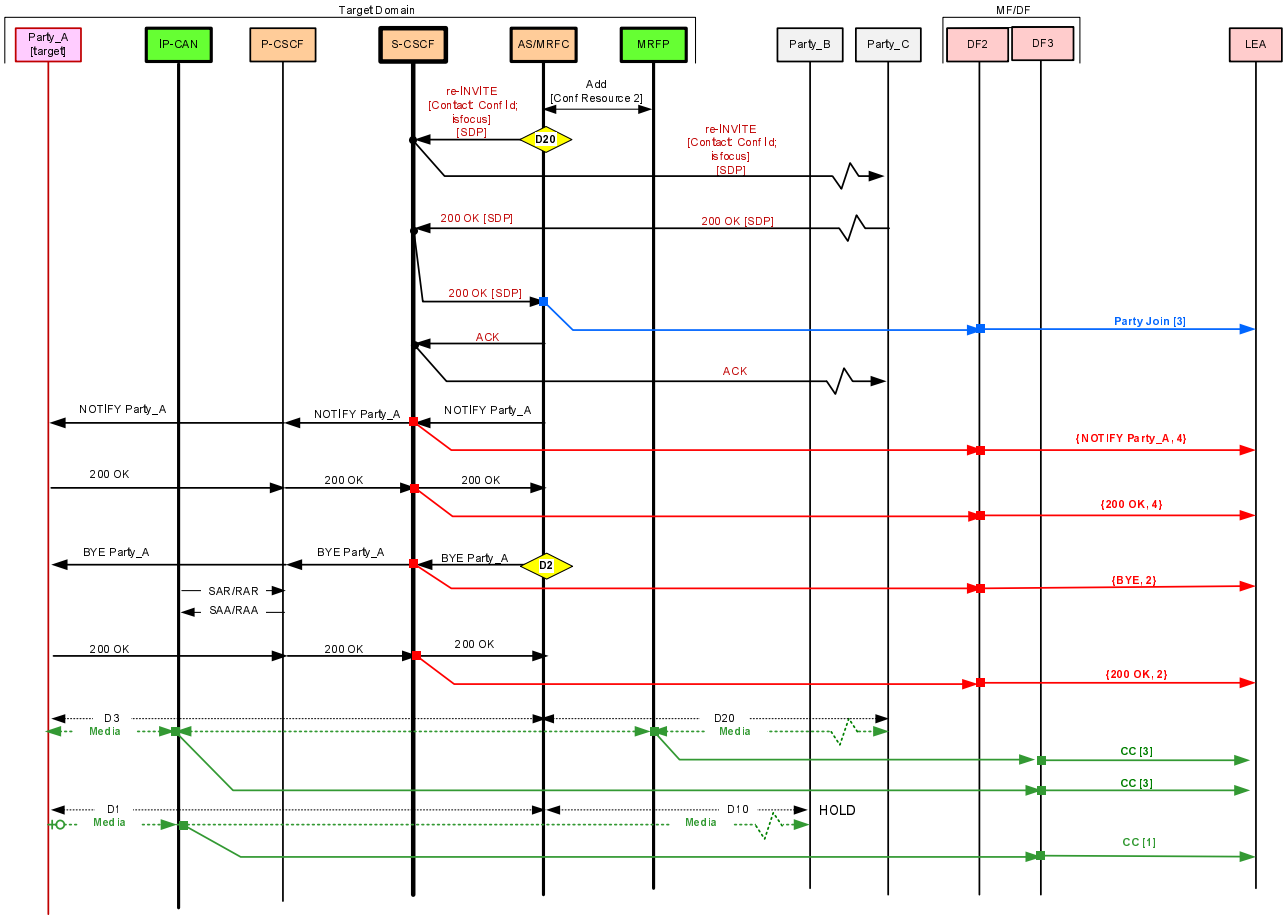


Figure F.7.3: Party_C joins the conference (flow 2 of 2)

At the end of this flow, the Party_A (target) and Party_C are connected via the conference. Party_C is still on hold. Part of the original call between Party_A (target) and Party_C (D2) is released with D20 now representing the call between the Party_C and the conference.

F.7.3 Party_B joins the conference

This flow is illustrated in two figures: Figure F.7.4 and Figure F.7.5.

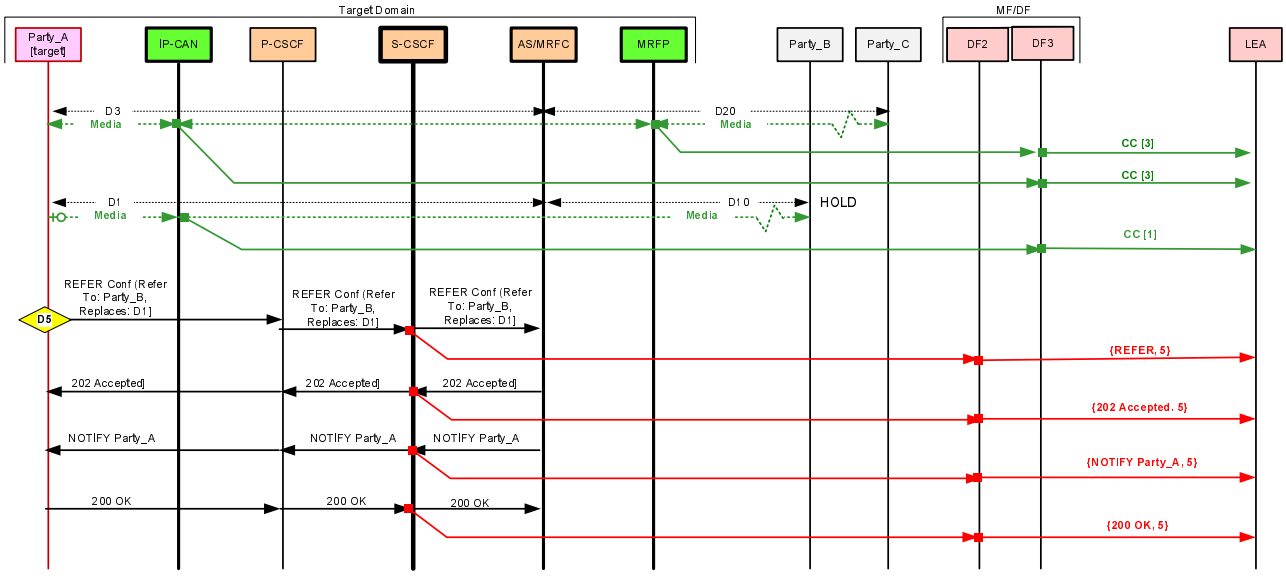


Figure F.7.4: Party_B joins the conference (flow 1 of 2)

D3 represents the dialogue of the call between the Party_A (target) and the conference. D20 represents the dialogue between the Party_C and the conference. D1 and D10 represent the original the dialogue of the original call between Party_A (target) and the Party_B. D5 represents the dialogue that the Party_A (target) uses to refer Party_B to the conference.

NOTE: Here, REFER is sent by Party_A outside of any existing dialogues. Sending of REFER inside a dialogue is also possible.

The IRI/CC delivered for D1 and D10 use the Correlation Number 1. The IRI/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3. The IRI for D5 uses the Correlation Number 5.

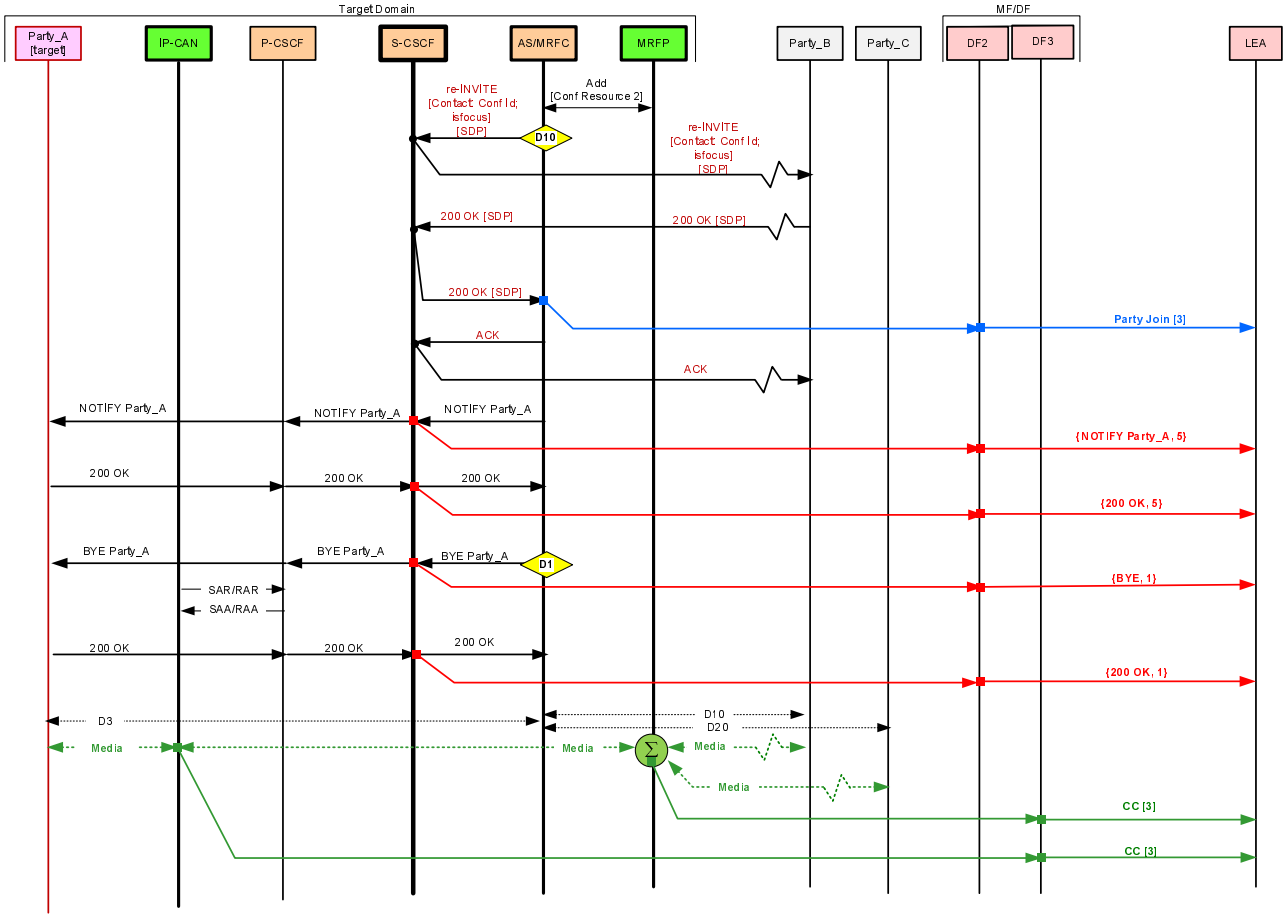


Figure F.7.5: Party_B joins the conference (flow 2 of 2)

At the end of this flow, the Party_A (target), Party_B and Party_C are connected via the conference. Part of the original call between Party_A (target) and Party_B (D1) is released with D10 now representing the call between the Party_B and the conference.

F.7.4 Party_C drops out of the conference

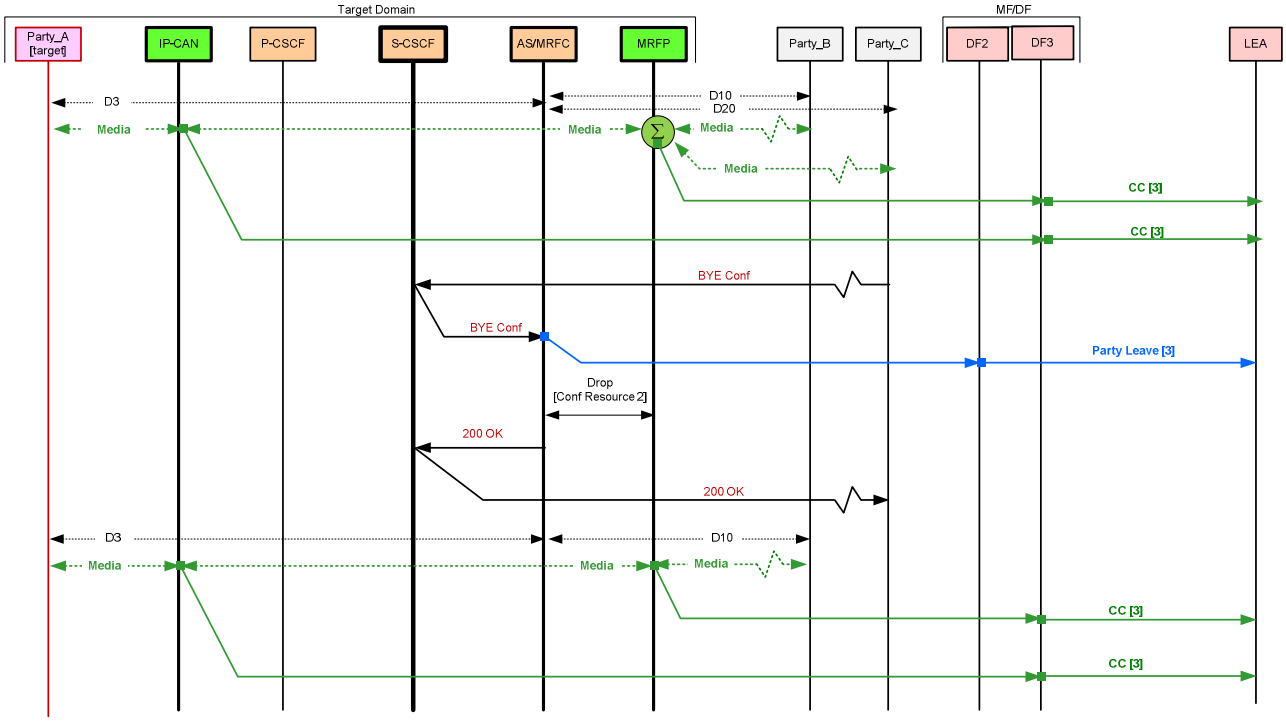


Figure F.7.6: Party_C drops out of the conference

D3 represents the dialogue of the call between the Party_A (target) and the conference. D20 represents the dialogue between the Party_C and the conference. D10 represents the dialogue between the Party_B and the conference.

The IRI/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3.

At the end of this flow, Party_A (target) and Party_B are connected through the conference.

F.7.5 Reconfiguration from Conference to two-party call

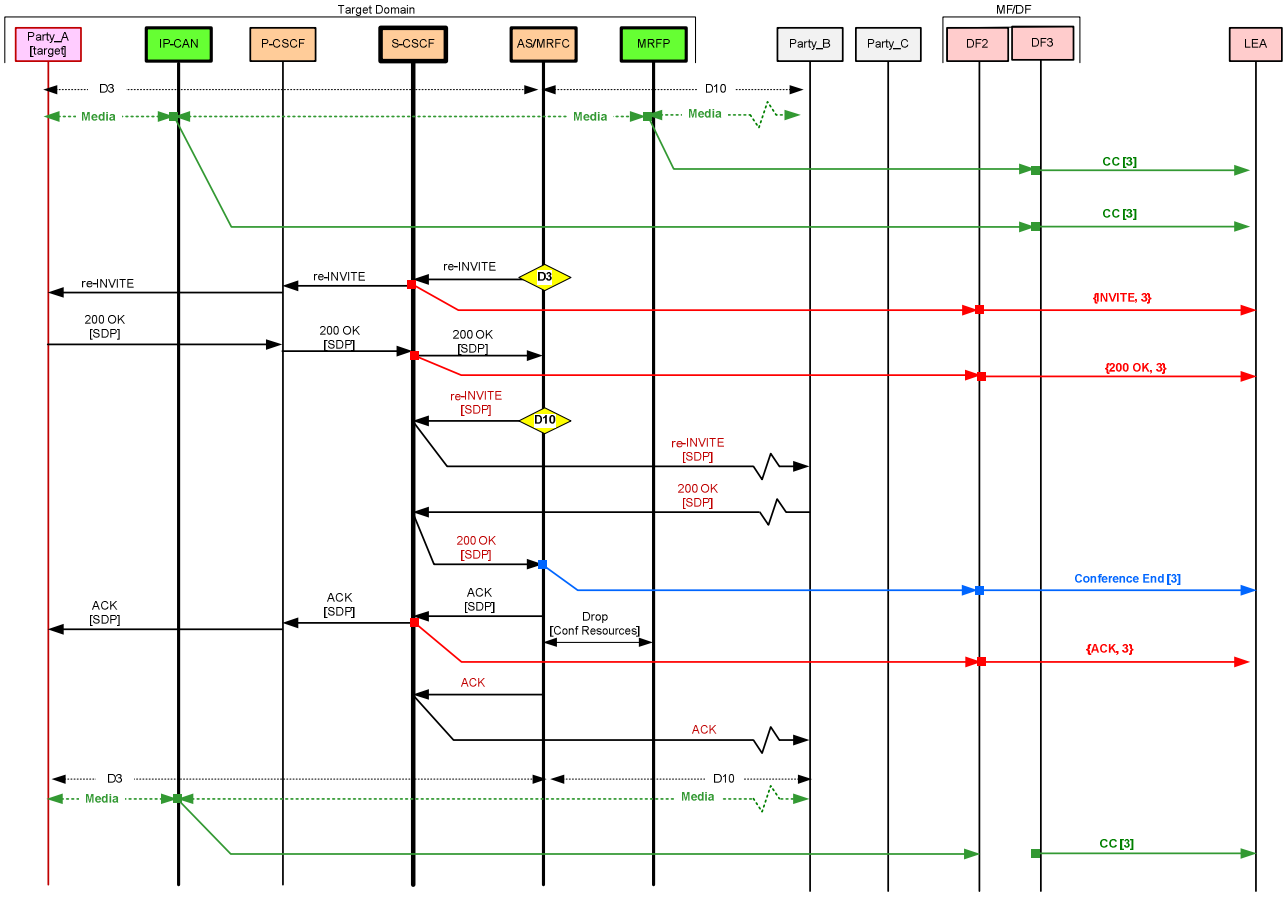


Figure F.7.7: Conference is reconfigured to a two-party call

D3 represents the dialogue of the call between the Party_A (target) and the conference. D10 represents the dialogue between the Party_B and the conference.

The IRI/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3.

At the end of this flow, Party_A (target) and Party_B are connected directly (without the conference). The IRI/CC delivered for this call between Party_A (target) and Party_B (D3 and D10) uses the Correlation Number 3.

NOTE: Reconfiguration may done using other ways (e.g., AS/MRFC sending a REFER to Party_A (target) to invite Party_C). The sequence of steps and the Correlation Number used can be different with such a flow.

F.7.6 Party_A (target) places Conference on hold

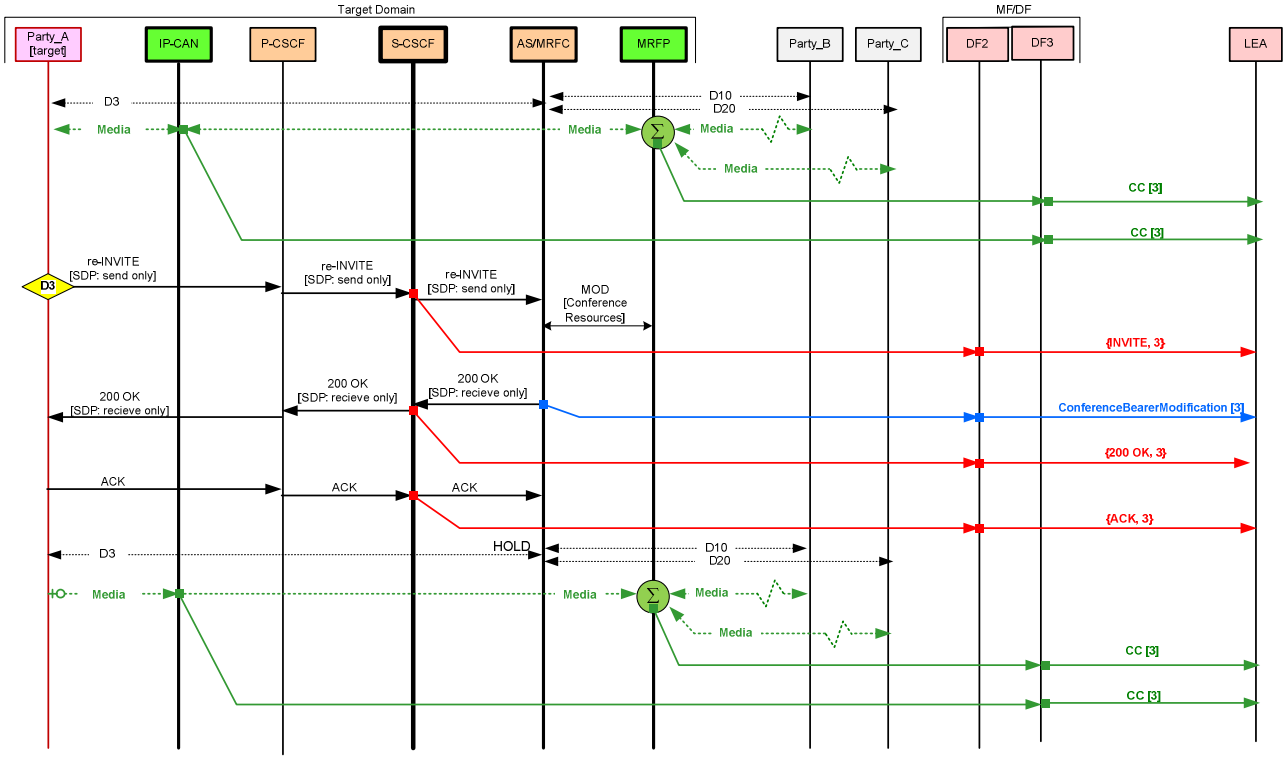


Figure F.7.8: Party_A (target) retrieves conference on hold

D3 represents the dialogue of the call between the Party_A (target) and the conference. D20 represents the dialogue between the Party_C and the conference. D10 represents the dialogue between the Party_B and the conference.

The IRI/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3.

At the end of this flow, Party_B and Party_C can still communicate via the conference, but without the Party_A. The CC delivered from the MRFP contains the communication content of that conversation.

NOTE: Similar steps as shown here are used when Party_A (target) retrieves a two-party call from hold.

F.7.7 Party_A (target) retrieves Conference from hold

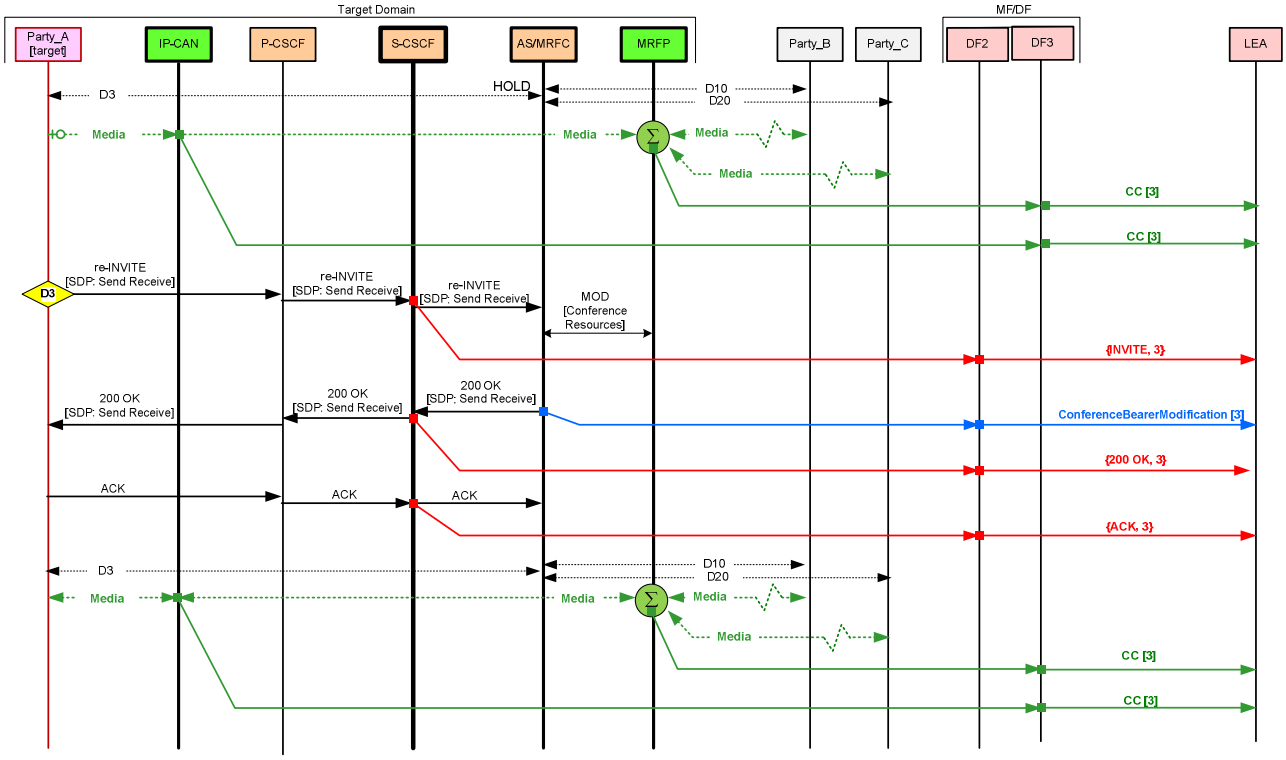


Figure F.7.9: Party_A (target) retrieves conference from hold

D3 represents the dialogue of the call between the Party_A (target) and the conference. D20 represents the dialogue between the Party_C and the conference. D10 represents the dialogue between the Party_B and the conference.

The IRI/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3.

At the end of this flow, Party_A (targt), Party_B and Party_C are communicating via the conference.

NOTE: Similar steps as shown here are used when Party_A (target) retrieves a two-party call from hold.

Annex G (informative): Examples of CC interception for transcoded media

G.1 Introduction

This annex provides some illustrative examples of media transcoding scenarios and its implication on the CC interception.

In some situations, the media information known to the S-CSCF can be different from the media information associated with the CC delivered to the LEMF. For example, when transcoding is involved in the media path, the media information (e.g., codec used) can change at the time transcoding is done and the S-CSCF that normally provides the media information to the DF2 may not have the knowledge of media information associated with the CC delivered to the LEMF.

In a particular implementation, the CC interception point may be chosen in such a way that information associated with the intercepted CC always matches to the information known to the IRI ICE (e.g., S-CSCF). But, there may some deployment situations and/or regulations that may require having a need to perform the CC interception at the other points with the information known to S-CSCF not being aligned with the information associated with the intercepted CC.

G.2 CC Interception of transcoded media

The Figure G.2-1 illustrates a case where the media is transcoded at the IMS-AGW. In this example, the media is not encrypted.

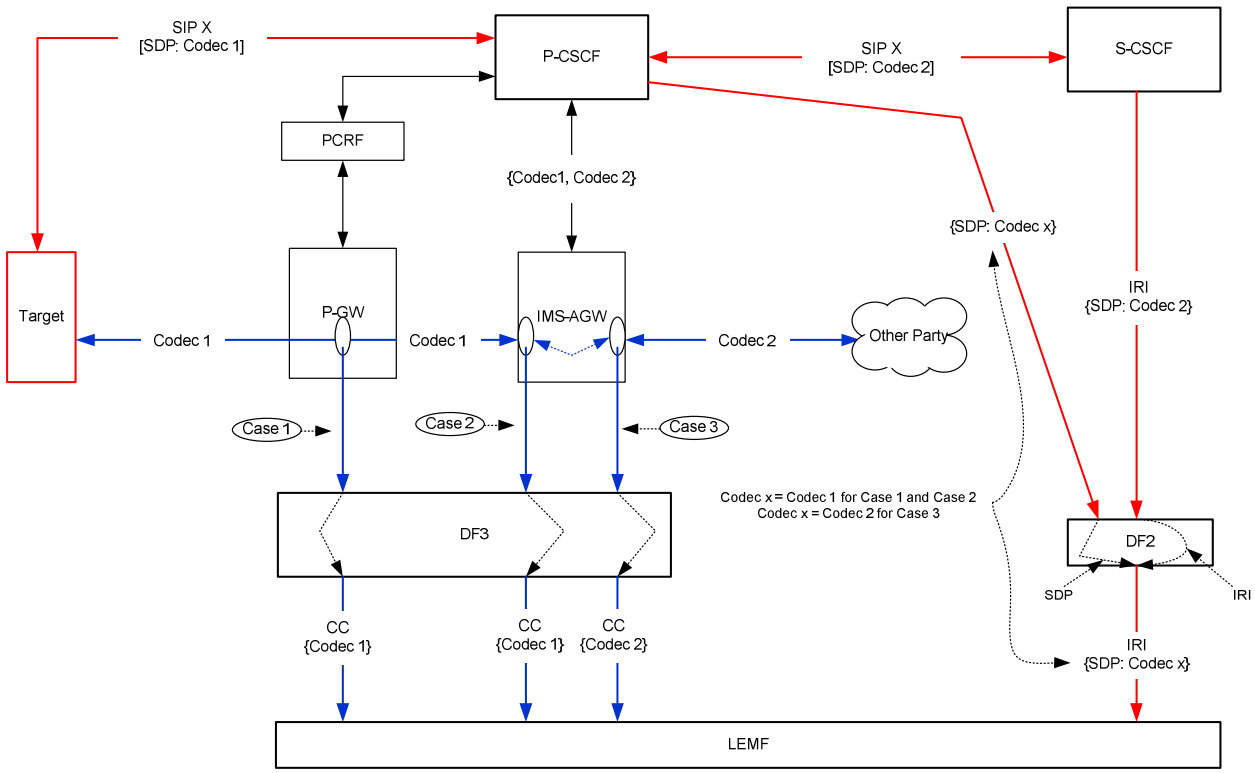


Figure G.2-1: Transcoded Media

The Figure G.2-1 shows three different cases of CC interception points. In the illustrated example, Codec 1 is associated with the media from the Target to the Ingress point of IMS-AGW and Codec 2 is used from the Egress point of IMS-AGW and beyond. Therefore, Codec 1 is associated with the CC delivered to the LEMF when that CC is intercepted at the PDN-GW or at the Ingress point of IMS-AGW, and Codec 2 is associated with the media delivered to the LEMF when that CC is intercepted at the Egress point of IMS-AGW.

The Codec 2 is included within the SDP of SIP messages handled at the S-CSCF and therefore, if S-CSCF provides the codec information to the DF2 in all cases, then there would be a misalignment with the codec information delivered over the HI2 and codec information associated with the CC delivered over HI3 for Case 1 and Case 2.

Depending on which case is used for the CC interception, the P-CSCF can send either Codec 1 or Codec 2 to the DF2. With the DF2 using the codec information received from the P-CSCF for reporting purposes, the codec information reported in the HI2 and HI3 are now aligned. For case 3, the codec information would be aligned irrespective of who sends that information to the DF2. Therefore, for Case 3, P-CSCF sending the codec 2 information to the DF2 can be an implementation alternative.

In a scenario like this, an implementation can also be such that the CC interception is always done at the Egress point of IMS-AGW (i.e., only Case 3), but because of some deployment situations and regulations, there may also be a need to perform the CC interception at the Ingress point of IMS-AGW (Case 2) or at the PDN-GW (Case 1).

G.3 CC Interception of transcoded media with e2ae encryption

The Figure G.3-1 illustrates a case where the media is transcoded at IMS-AGW with e2ae encryption. In this example, media is encrypted e2ae (i.e. between the Target and the Ingress point of IMS-AGW). The CC is delivered to the LEMF in a decrypted form.

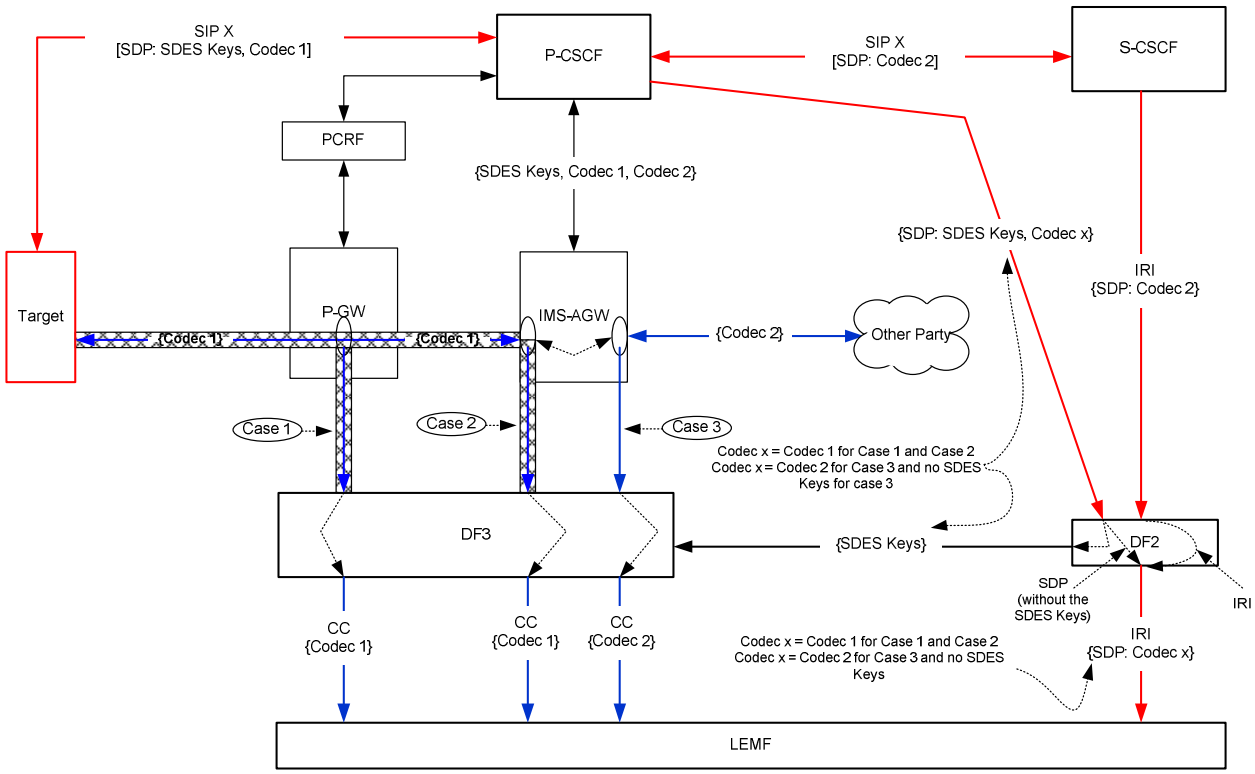


Figure G.3-1: Transcoded Media with e2ae encryption

The Figure G.3-1 shows three different cases of CC interception points. In this example, Codec 1 is associated with the media from the Target to the Ingress point of IMS-AGW and Codec 2 is used from the Egress point of IMS-AGW and beyond. Therefore, Codec 1 is associated with the CC delivered to the LEMF when that CC is intercepted at the PDN-GW or at the Ingress point of IMS-AGW, and Codec 2 is associated with the media delivered to the LEMF when that CC is intercepted at the Egress point of IMS-AGW. The Codec 2 is included within the SDP of SIP messages handled at the S-CSCF and therefore, if S-CSCF provides the codec information to the DF2 in all cases, then there would be a misalignment with the codec information delivered over the HI2 and codec information associated with the CC delivered over HI3 for Case 1 and Case 2.

Depending on which case is used for the CC interception, the P-CSCF can send either Codec 1 or Codec 2 to the DF2. With the DF2 using the codec information received from the P-CSCF for reporting purposes, the codec information reported in the HI2 and HI3 are now aligned. For case 3, the codec information would be aligned irrespective of who

sends that information to the DF2. Therefore, for Case 3, P-CSCF sending the codec 2 information to the DF2 can be an implementation alternative.

In this example, media is encrypted (with SDES keys in SDP) from Target to the Ingress point of IMS-AGW and not encrypted from the Egress point of IMS-AGW and beyond. Therefore, for Case 1 and Case 2, the DF2 has to provide the SDES keys to the DF3 (see clause 7A.1.A) to perform the decryption. The S-CSCF does not receive the SDES keys within the SDP of SIP messages. Therefore, P-CSCF shall send the SDES Keys to the DF2 and the DF2 shall use that for its handling (i.e., sending to the DF3). P-CSCF does not send any SDES Keys to the DF2 for Case 3 since the CC is intercepted in the Egress point of IMS-AGW in a decrypted form.

In a scenario like this, an implementation can also be such that the CC interception is always done at the Egress point of IMS-AGW (i.e., only Case 3), but because of some deployment situations and regulations, there may also be a need to perform the CC interception at the Ingress point of IMS-AGW (Case 2) or at the PDN-GW (Case 1).

G.4 CC Interception of transcoded media with e2e hop-by-hop encryption

The Figure G.4-1 illustrates a case where the media is transcoded at IMS-AGW with e2e hop-by-hop encryption. Different SDES keys are for the encryption.

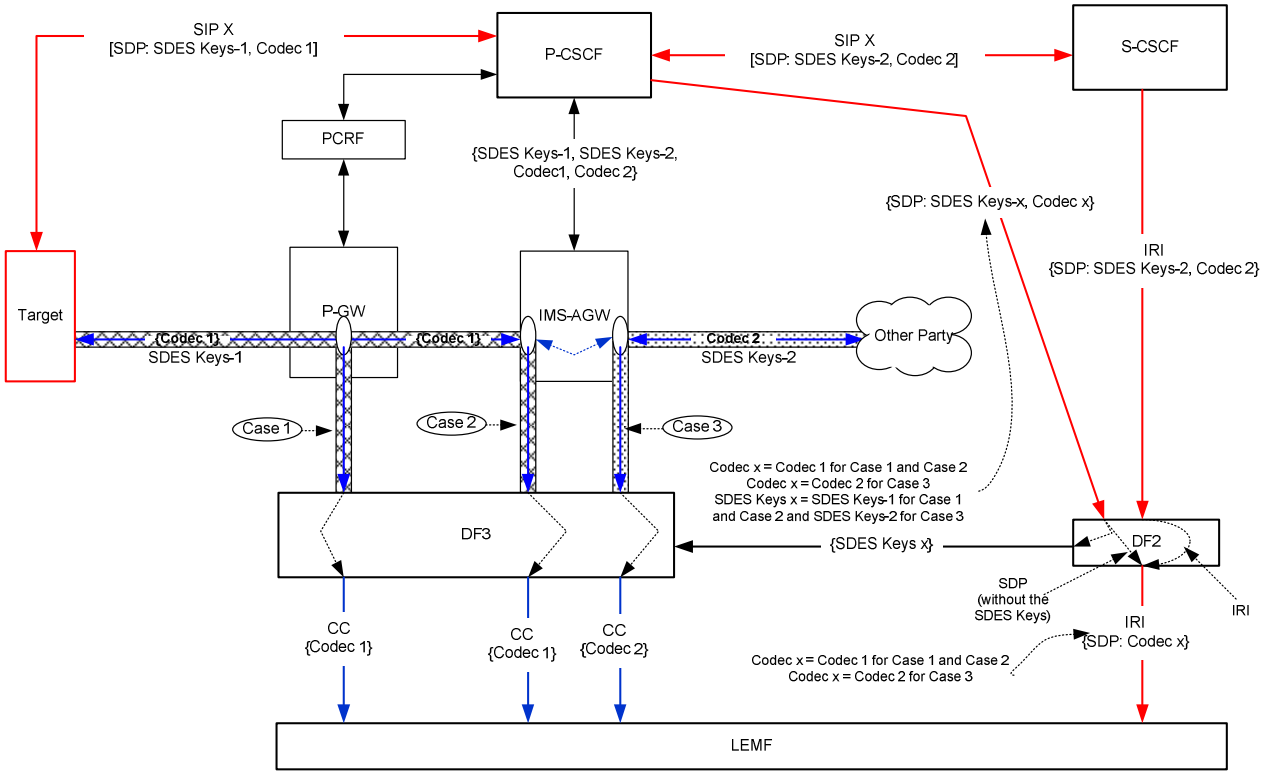


Figure G.4-1: Transcoded Media with e2e encryption

The Figure G.4-1 shows three different cases of CC interception points. In this example, Codec 1 is associated with the media from the Target to the Ingress point of IMS-AGW and Codec 2 is used from Egress point of IMS-AGW and beyond. Therefore, Codec 1 is associated with the CC delivered to the LEMF when that CC is intercepted at the PDN-GW or at the Ingress point of IMS-AGW, and Codec 2 is associated with the media delivered to the LEMF when that CC is intercepted at the Egress point of IMS-AGW. The Codec 2 is included within the SDP of SIP messages handled at the S-CSCF and therefore, if S-CSCF provides the codec information to the DF2 in all cases, then there would be a misalignment with the codec information delivered over the HI2 and codec information associated with the CC delivered over HI3 for Case 1 and Case 2.

Depending on which case is used for the CC interception, the P-CSCF can send either Codec 1 or Codec 2 to the DF2. With the DF2 using the codec information received from the P-CSCF for reporting purposes, the codec information reported in the HI2 and HI3 are now aligned. For case 3, the codec information would be aligned irrespective of who

sends that information to the DF2. Therefore, for Case 3, P-CSCF sending the codec 2 information to the DF2 can be an implementation alternative.

The media is encrypted (with SDES keys in SDP) from Target to the Ingress point of IMS-AGW with SDES keyes-1 as the encryption keys and encrypted from Egress point of IMS-AGW to the other end using SDES keys-2 as the encryption keys. The S-CSCF is aware of only the SDES keys-2 as it sees that in the SDP of the SIP messages. For Case 1 and Case 2, the P-CSCF shall provide the SDES keys to the DF2. For Case 3, either of the two, S-CSCF or the P-CSCF, can send the SDES keys to the DF2. DF2 has to use the SDES keys received from the P-CSCF for its handling (i.e., sending it to DF3) to perform the decryption. For Case 3, if the P-CSCF does not send the SDES Keys to the DF2, then the DF2 will use the SDES keys received from the S-CSCF for its handling.

In a scenario like this, an implementation can also be such that the CC interception is always done at the Egress point of IMS-AGW (i.e., only Case 3), but because of some deployment situations and regulations, there may also be a need to perform the CC interception at the Ingress point of IMS-AGW (Case 2) or at the PDN-GW (Case 1).

G.5 CC Interception of transcoded media at the TrGW

The Figure G.5-1 illustrates a case where the media is transcoded at TrGW. In this example, the TrGW provides the transcoding. This scenario can be see when an incoming call to the Target is forwarded (illustration assumes) or when Target is IMS roaming.

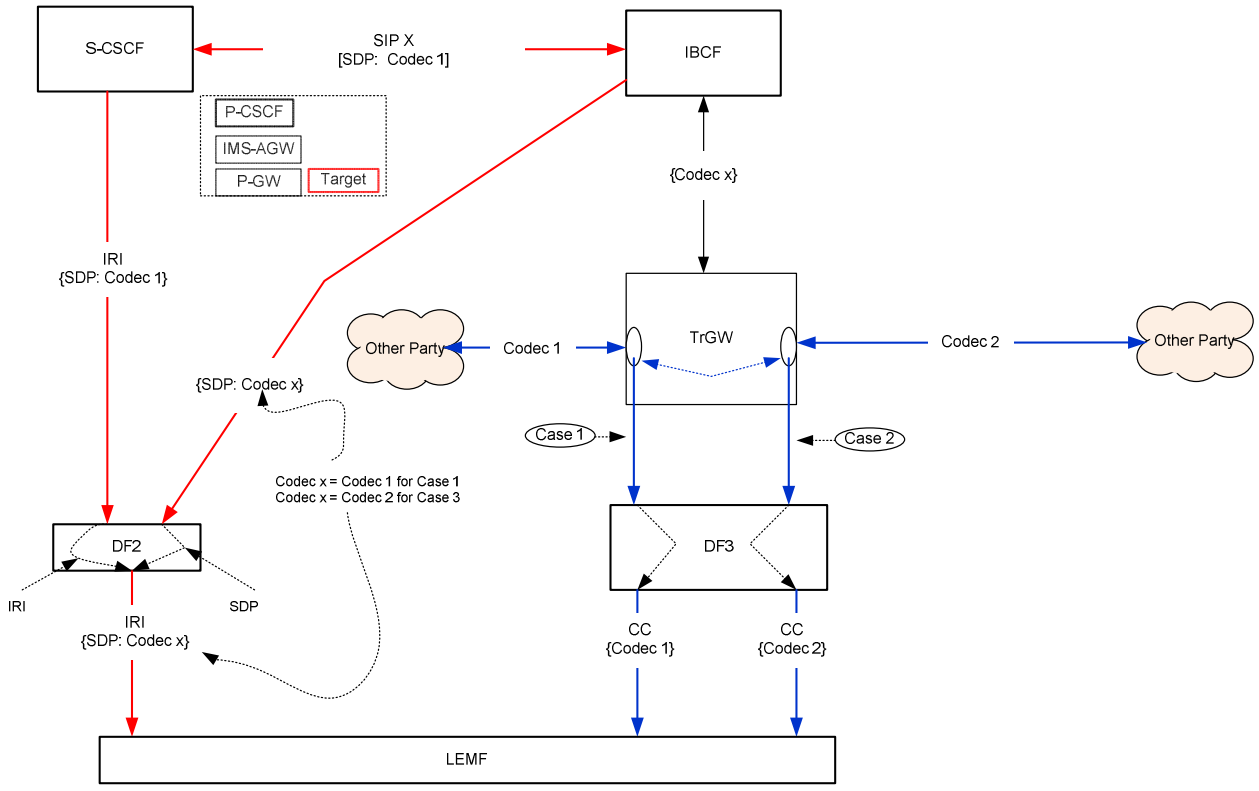


Figure G.5-1: TrGW Transcoded Media

The Figure G.5-1 shows two different cases of CC interception points. In this example, Codec 1 is associated with the media from the first Other Party (e.g., calling party) to the Ingress point of TrGW and Codec 2 is used from Egress point of TrGW to the second Other Party (e.g., forwarded-to-party). Therefore, Codec 1 is associated with the CC delivered to the LEMF when that CC is intercepted at Ingress point of TrGW and Codec 2 is associated with the media delivered to the LEMF when that CC is intercepted at the Egress point of TrGW. The Codec 1 is included within the SDP of SIP messages handled at the S-CSCF and therefore, if S-CSCF provides that to the DF2 in both cases, there would be a misalignment with the codec information delivered over the HI2 and codec information associated with the CC delivered over HI3 for Case 2.

Depending on which case is used for the CC interception, the IBCF can send either Codec 1 or Codec 2 to the DF2. With the DF2 using the codec information received from the IBCF for reporting purposes, the codec information reported in the HI2 and HI3 are now aligned. For Case 1 the codec information would be aligned irrespective of who

sends that information to the DF2. Therefore, for Case 1, IBCF sending the codec 1 information to the DF2 can be an implementation alternative.

In a scenario like this, an implementation can also be such that the CC interception is always done at the Ingress point of TrGW (i.e., only Case 1), but because of some deployment situations and/or regulations, there may also be a need to perform the CC interception at the Egress point of TrGW as well.

Annex H (informative): Location only warrant

H.1 General

The following describes the information that is delivered for authorization in those countries that allow authorized Lawful Interception (LI) for location scenarios.

H.2 Location only warrant

The ADMF provides the network and/ or LI LCS Client to collect location IRI against a target with a specified periodicity. The target may have several interception invocations with multiple LEAs. For an Authorization for location reporting, all other IRI's not associated with Location is filtered. For example if a target places a voice call, new location information is now available to be sent to the LEA with a location authorization, that location data, and only the location value can be sent to the LEA, any record of the event (call start and other associated event information) is not be sent. Other LEAs may have a warrant for the Voice Services, and they will get the associated IRI. The invocations of elements to be captured can be sent to the DF and/ or the MF can filter events not required for the Location Authorization

H.3 Immediate Location warrant

The ADMF provides the network and/ or LI LCS Client to collect the immediate location of a target. The target may have several interception invocations with multiple LEAs. For an Authorization for Immediate location, all other IRI's not associated with Location is filtered.

Annex I (informative): Interception of Targets with Non-Local IDs

I.1 Introduction

This annex provides some informative illustrations on the interception of targets with Non-Local IDs. A target with a Non-Local ID means that the identity used for the target may not belong to the network that is providing the interception. However, in a roaming scenario, that subscriber with a Non-Local ID could as well be in the network where the interception is provided. For the lawful interception purpose, a target with a Non-Local ID is distinctly identified as a Non-Local target along with the nature of the interception that is required to be performed on that target.

This clause covers only the IRI aspects of interception capabilities since the capabilities to perform the CC interception do not change.

I.2 Interception of outgoing calls

I.2.1 General

In order to perform the interception of outgoing calls to a particular destination (identified as target with Non-Local ID for outgoing calls), called party information of the outgoing message is checked.

In the CS domain, this could be the Called Party Information present in the IAM message (as an example) that is sent from the switch that performs the interception.

In the case of IMS-based VoIP calls, this can be any of the SIP headers used to identify the called party information present in the outgoing SIP message. The examples are: Request URI and To headers. The interception functions may be provided by the S-CSCF or P-CSCF (optional in a non-roaming case, and mandatory in the roaming case when LBO approach is used as the roaming architecture). Alternatively, in another implementation, the interception functions may also be provided by the Egress IBCF or Egress MGCF for a non-roaming case. Of the two approaches S-CSCF/P-CSCF Vs IBCF/MGCF used for non-roaming case, only one approach is required to be supported within a CSP's network.

I.2.2 Interception at S-CSCF or P-CSCF

The Figure I.1 shows an example where the interception is done at the S-CSCF. The Figure I.2 shows an example where the interception is done at the P-CSCF in a roaming case with LBO as the roaming architecture. In both illustrations, Party-B is the target with Non-Local ID and the nature of the interception to be performed is for outgoing calls. In the call, the Request URI and To headers point to Party-B.

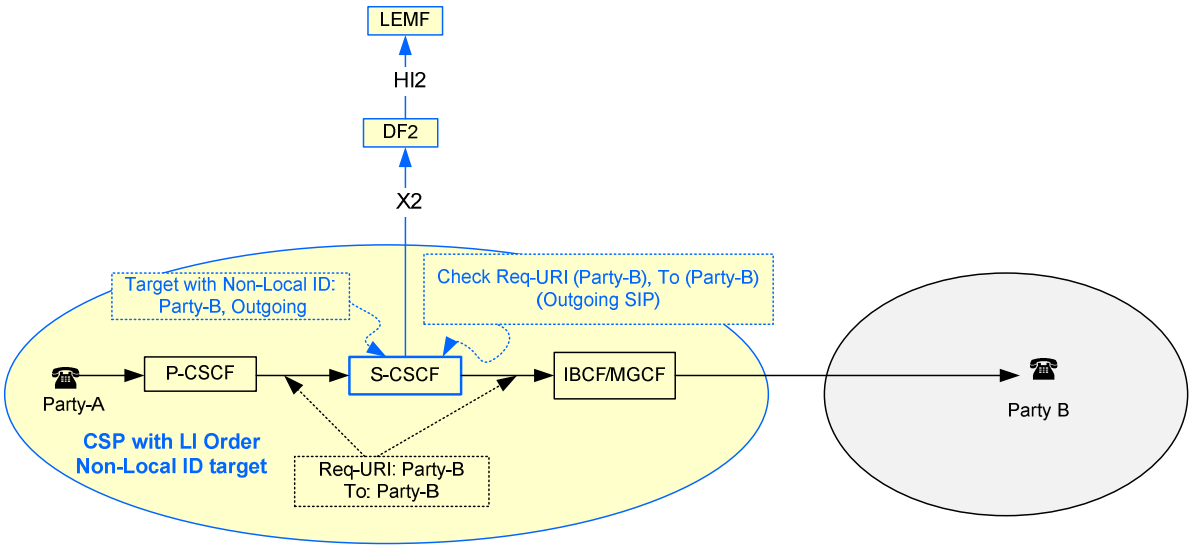


Figure I.1: IRI ICE at S-CSCF - interception of a target with Non-Local ID for outgoing calls

Figure I.1 shows the case where S-CSCF is the IRI ICE and hence, the S-CSCF checks the Request URI and To headers of SIP message that it sends out toward IBCF/MGCF. Since a match is found, S-CSCF would perform the interception.

In the event, multiple S-CSCF are involved in the signalling path (due to call forwarding case), all S-CSCF are expected to do the same check and the S-CSCF closer to the Egress IBCF/MGCF will find a match. It is important to note that the S-CSCF checks the headers from the SIP message it sends out because the Request URI of the SIP message it receives will be pointing to the local ID (which may have the call forwarding activated).

As in the case of interception of target with Local ID, a P-CSCF may optionally provide the IRI ICE functions in a non-roaming case. However, in a roaming case with LBO as the roaming architecture, P-CSCF provides the IRI ICE functions.

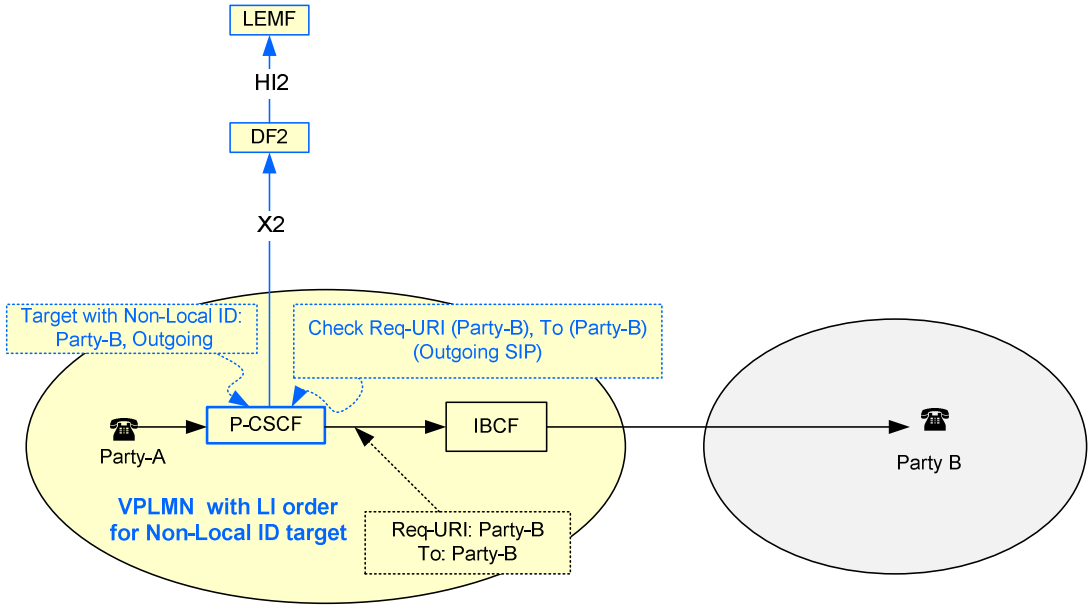


Figure I.2: IRI ICE at P-CSCF (roaming) - interception of a target with Non-Local ID for outgoing calls

In Figure I.2, the P-CSCF in the VPLMN checks the Request URI and To headers of SIP message that it sends out toward IBCF. Since a match is found, P-CSCF would perform the interception.

I.2.3 Interception at the IBCF/MGCF

The Figure I.3 shows an example where the interception is done at the IBCF or MGCF in a non-roaming case. In the illustration, Party-B is the target with Non-Local ID and the nature of the interception to be performed is for outgoing calls. In the call, the Request URI and To headers point to Party-B.

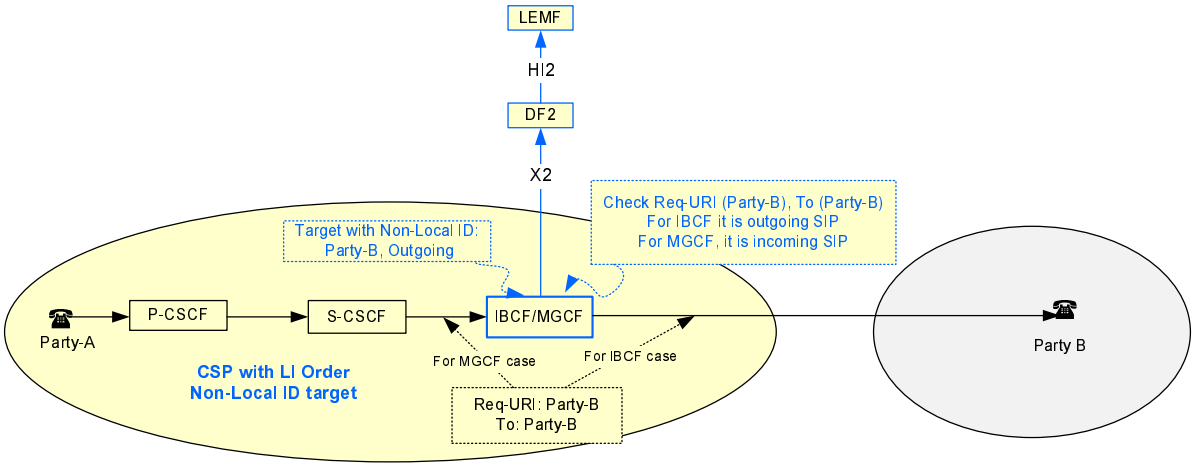


Figure I.3: IRI ICE at BCF - interception of a target with Non-Local ID for outgoing calls

Figure I.3 shows the case where the Egress IBCF or MGCF is the IRI ICE for intercepting when the target is identified with a Non-Local ID. Accordingly, the IBCF or MGCF checks the Request URI and To headers of SIP message. Since MGCF is providing signalling conversion (e.g., SIP to ISUP and Vice-Versa), the MGCF checks the headers of the SIP message it receives. IBCF could check the headers from either of the SIP messages (they have to be the same anyway). Alternatively, the MGCF could also check the Called Party Information present in the IAM it sends out.

I.3 Interception of incoming calls

I.3.1 General

In order to perform the interception of incoming calls from a particular origination point (identified as target with Non-Local ID for incoming calls), calling party information and redirecting party information of the incoming message are checked. The redirecting information is checked because the call may have encountered a call forwarding before arriving at the CSP where the interception for Non-Local ID is performed.

In the CS domain, this could be the Calling Party Information and Redirecting Party Information present in the IAM message (as an example) that is received at the switch where the interception is performed.

In the case of IMS-based VoIP calls, this can be any of the SIP headers used to identify the calling party information and redirecting party information present in the incoming SIP message. The examples are: P-Asserted Id, From headers and History-Info, Diversion headers. The interception functions may be provided by the S-CSCF or P-CSCF (optional in a non-roaming case and mandatory in the roaming case when LBO approach is used as the roaming architecture). Alternatively, in another implementation, the interception functions may also be provided by the Ingress IBCF or Ingress MGCF for non-roaming case. Of the two approaches S-CSCF/P-CSCF Vs IBCF/MGCF used for non-roaming case, only one approach is required to be supported within a CSP's network.

I.3.2 Interception at S-CSCF or P-CSCF

The Figure I.4 shows an example where the interception is done at the S-CSCF. The Figure I.5 shows an example where the interception is done at the P-CSCF in a roaming case with LBO as the roaming architecture. In both illustrations, Party-A is the target with Non-Local ID and the nature of the interception to be performed is for incoming calls. In the call, the P-Asserted-Id, From headers point to Party-A. There are no History-Info or Diversion headers in the examples.

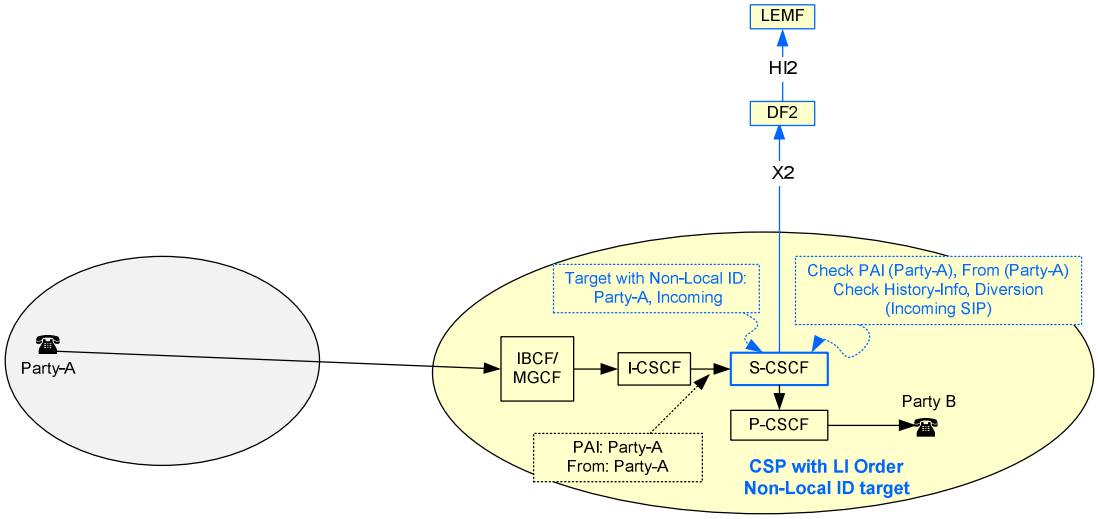


Figure I.4: IRI ICE at S-CSCF - interception of a target with Non-Local ID for incoming calls

Figure I.4 shows the case where S-CSCF is the IRI ICE and hence, the S-CSCF checks the P-Asserted-Id and From headers of SIP message that it receives from the I-CSCF. Since a match is found, S-CSCF would perform the interception. In the event, multiple S-CSCF are involved in the signalling path (due to call forwarding case), all S-CSCFs may to do the same check and all S-CSCFs may end up finding a match to the target's Non-Local ID. Special care will have to be taken to suppress the duplicate interception of one LI request. When a call forwarding is involved, the subsequent S-CSCF may see History-Info or Diversion headers present, however, none of those are expected to match the Non-Local ID of the target. As in the case of interception of target with Local ID, a P-CSCF may optionally

provide the IRI ICE functions in a non-roaming case. However, in a roaming case with LBO as the roaming architecture, P-CSCF provides the IRI ICE functions.

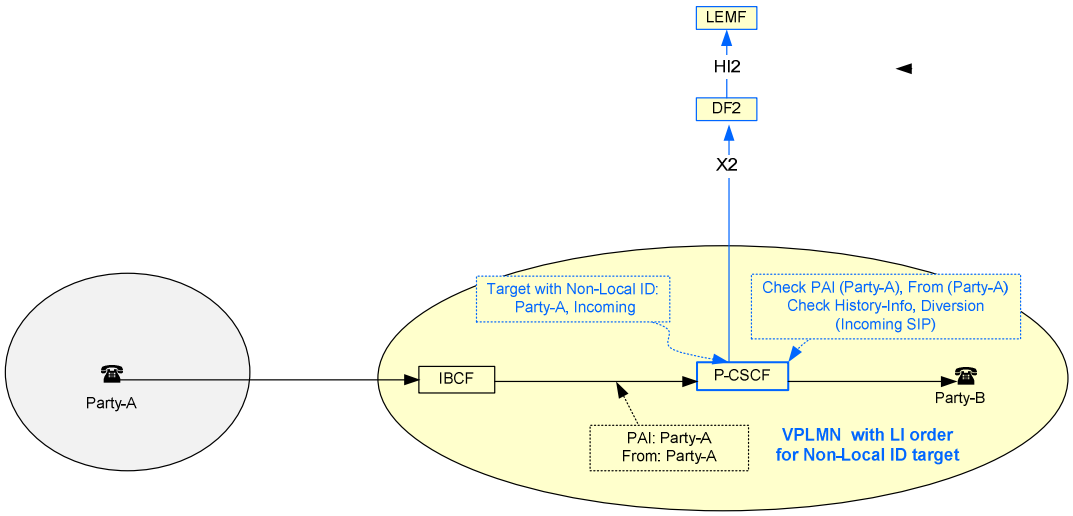


Figure I.5: IRI ICE at P-CSCF (roaming) - interception of a target with Non-Local ID for incoming calls

In Figure I.5, the P-CSCF in the VPLMN checks the P-Asserted-Id, From headers and History-Info and Diversion headers of the SIP message that it receives. Since a match is found for P-Asserted-Id and From header values, P-CSCF would perform the interception.

I.3.3 Interception at the IBCF/MGCF

The Figure I.6 shows an example where the interception is done at the IBCF or MGCF in a non-roaming case. In the illustration, Party-A is the target with Non-Local ID and the nature of the interception to be performed is for incoming calls. In the call, the P-Asserted-Id and From headers point to Party-A. There are no History-Info or Diversion headers in the example.

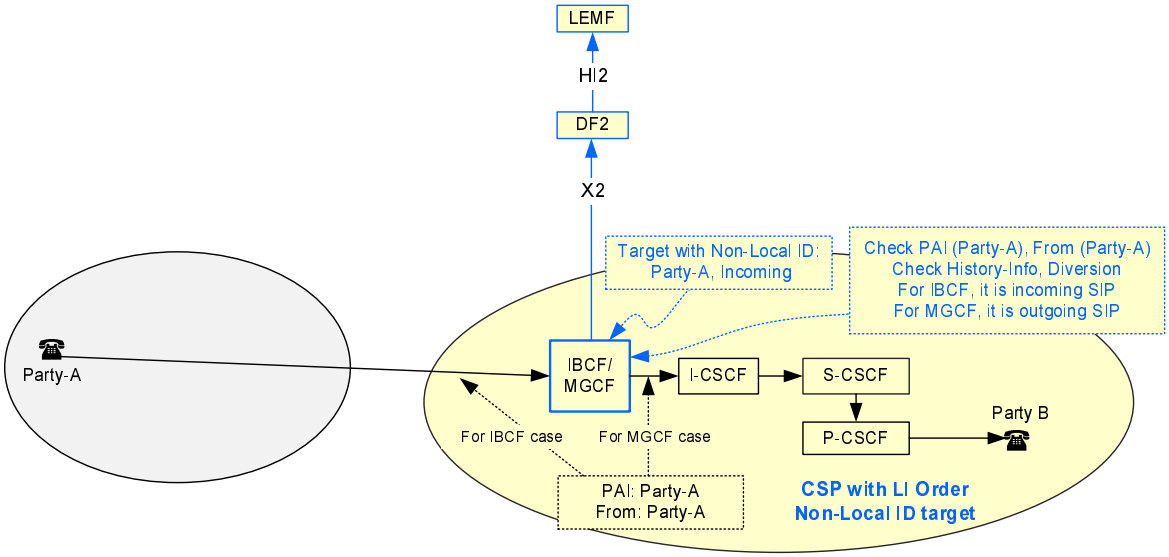


Figure I.6: IRI ICE at BCF - interception of a target with Non-Local ID for incoming calls

Figure I.6 shows the case where the Ingress IBCF or MGCF is the IRI ICE for intercepting when the target is identified with a Non-Local ID. Accordingly, the IBCF or MGCF checks the P-Asserted-Id, From headers, and History-Info, Diversion headers of SIP message. Since MGCF is providing signalling conversion (e.g., ISUP to SIP and Vice-Versa), the MGCF checks the headers of the SIP message it sends out. IBCF could check the headers from either of the SIP messages (they have to be the same anyway). Alternatively, the MGCF could also check the Calling Party Information and Redirecting Information present in the IAM message that it receives.

Annex J (informative): Lawful Interception Illustrations in VPLMN with S8HR

J.1 Overview

This informative annex illustrates the process of performing lawful interception in the VPLMN for voice services involving the inbound roaming targets when S8HR approach is used as the roaming architecture.

When S8HR approach is used as the roaming architecture for VoLTE, all of the IMS nodes reside in the HPLMN. Even the PDN-GW resides in the HPLMN. In this case, the lawful interception of voice services involving the inbound roaming targets requires new capabilities in the VPLMN since the VPLMN does not have any IMS nodes. New LI-specific functions are introduced to examine the packets that flow through the VPLMN packet core network nodes to generate IRI and CC when the communication involves an inbound roaming target. The LI architecture diagram shown in figure 1j is expanded in figure J.1 that shows an overview of S8HR roaming architecture as well.

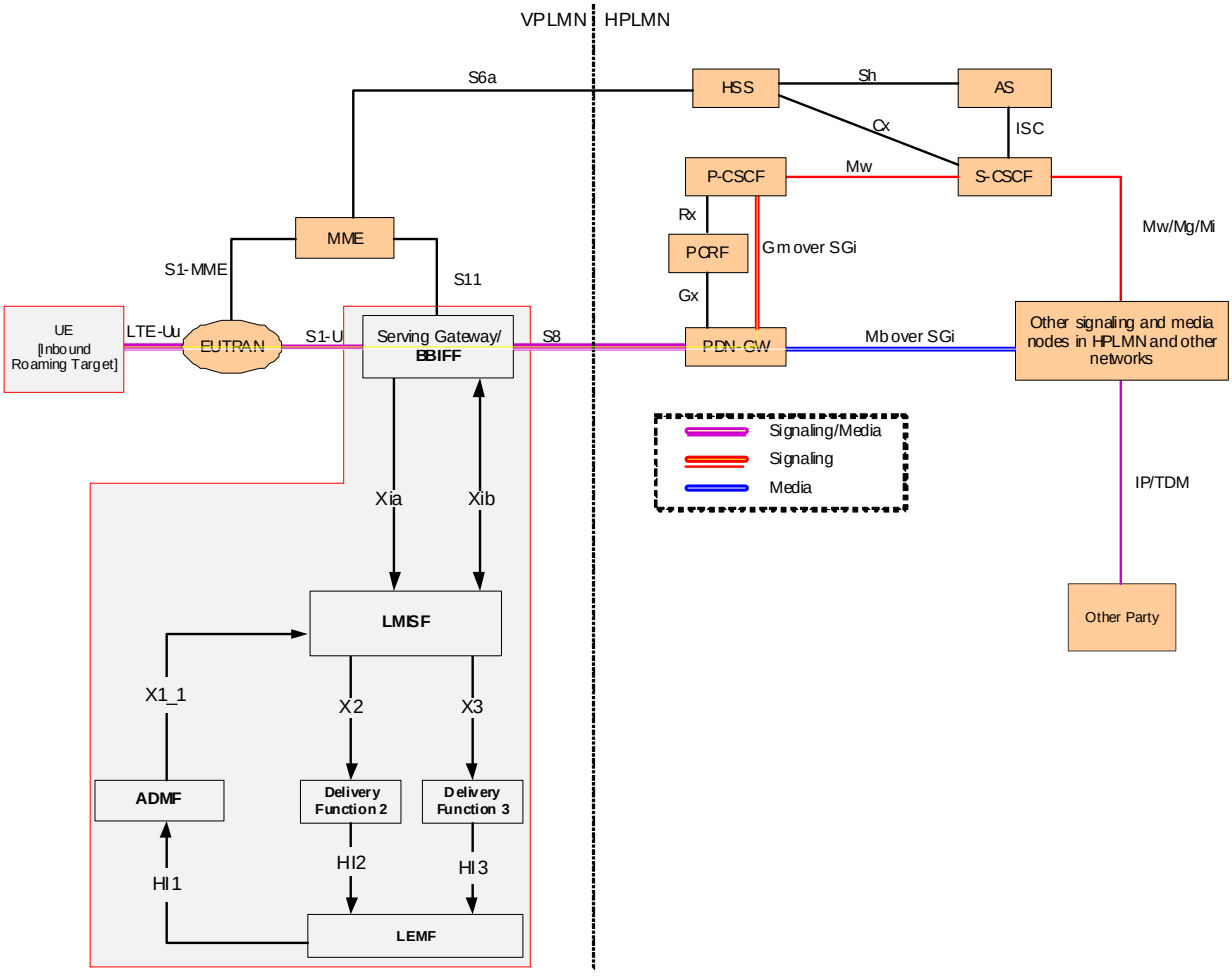


Figure J.1 Lawful interception of voice services in VPLMN for S8HR

As shown in figure J.1, the SIP signalling messages are exchanged between the UE and P-CSCF over the Gm reference point. Within the VPLMN with S8HR, the IMS signalling messages are carried over the GTP tunnel that corresponds to the IMS Signalling Bearer and the media packets are carried over the GTP tunnel that corresponds to the Media Bearer (i.e., dedicated EPS Bearer used to carry the media packets). The present document assumes that the EPS Bearer ID of the IMS Signalling Bearer is always linked to the dedicated EPS Bearer used as a Media Bearer.

J.2 Process Flow

The basic concept is LMISF instructs the S-GW/BBIFF over the Xib reference point to deliver packets from the GTP tunnels associated with IMS signalling bearer of all inbound roamers with S8HR as the roaming architecture. S-GW/BBIFF extracts the packets from those GTP tunnels and delivers the same to the LMISF. The LMISF extracts the SIP messages from those packets and provides an IMS call state function similar to the way P-CSCF provides the IMS call state function. In addition, the LMISF provisioned with the target identity by ADMF examines the SIP messages to determine whether the IMS session needs to be intercepted. When the IMS session needs to be intercepted, the LMISF generates IRI from the SIP messages and deliver the same to the Delivery Function 2 over X2 reference point. In addition to the generation and delivery of IRI, when CC interception is required, the LMISF also informs the S-GW/BBIFF that the IMS session is being intercepted and instructs the S-GW/BBIFF over Xib reference point to start delivering the packets from the Media Bearer l associated with the intercepted IMS Signalling Bearer. The S-GW/BBIFF extracts the packets from that GTP tunnel used for Media Bearer associated with the intercepted IMS Signalling Bearer and delivers the same to the LMISF. The LMISF constructs the CC from those packets and delivers the same to the Delivery Function 3 over X3 reference point.

Figure J.2 shows the steps to illustrate the process flow:

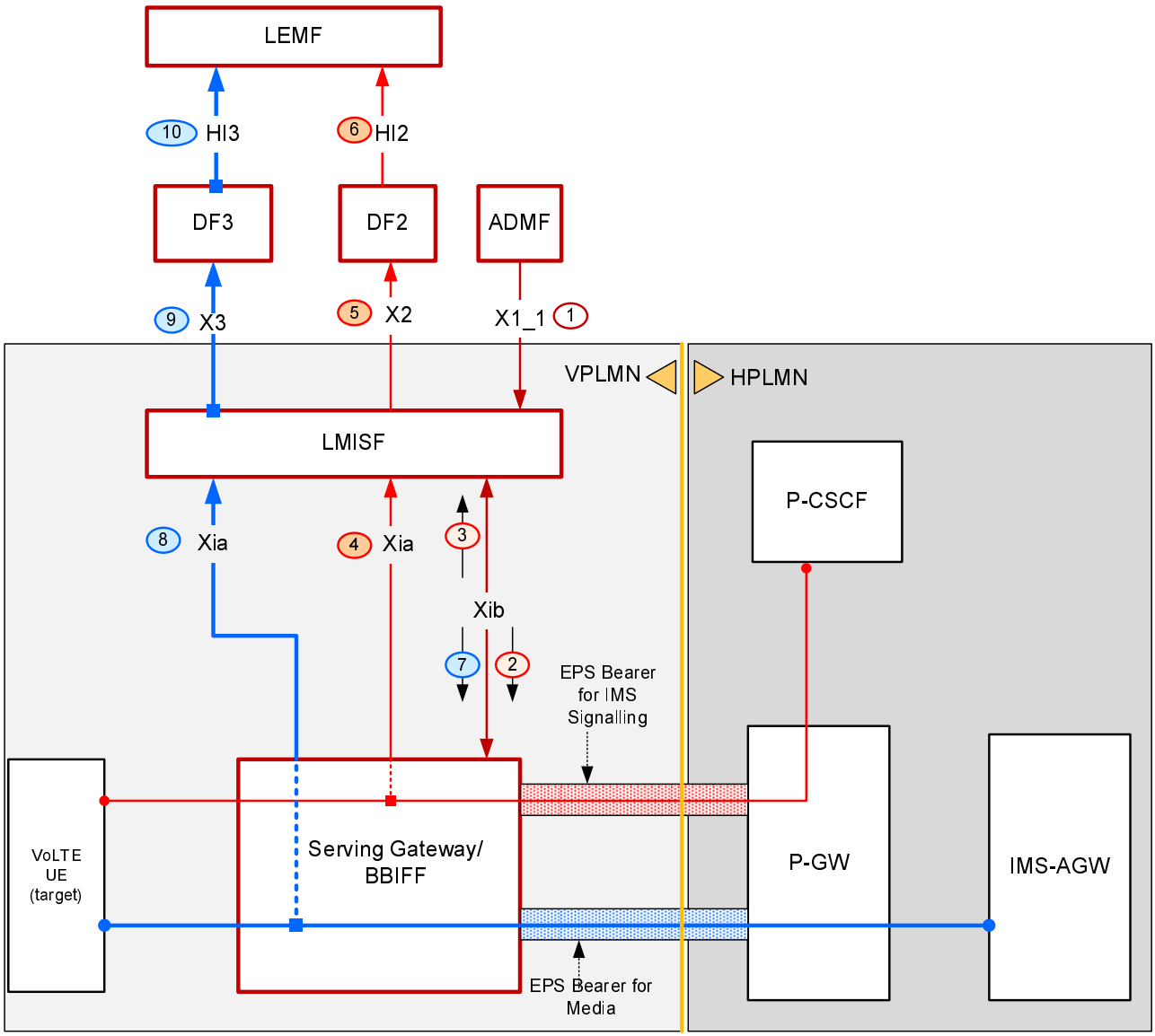


Figure J.2: Process Flow of S8HR LI

1. LMISF is provisioned with target information (for Voice Services, it can be SIP URI, TEL URI or IMEI) from the ADMF.

2. LMISF instructs the S-GW/BBIFF to notify (to LMISF), based on the GTP-C event, whenever an IMS Signalling Bearer or the Media Bearer for S8HR APN is created, modified, or deleted, and to deliver the packets (to LMISF) of all IMS Signalling Bearers established for S8HR APNs (Access Point Names). Here, the LMISF may supply the S8HR APNs to the S-GW/BBIFF.

NOTE1: This step is independent of target specific LI service operation such as Step 1.

3 S-GW/BBIFF to notifies the LMISF, based on the GTP-C event, whenever the IMS Signalling Bearer for S8HR APN is created, modified, or deleted. S-GW/BBIFF also notifies the LMISF, based on the GTP-C event, whenever the IMS Media Bearer is created, modified, or deleted.

NOTE2: The S-GW/BBIFF includes the IMSI value associated with the inbound roamer's UE when notifies (to the LMISF) creation, modification or deletion of IMS Signalling Bearer and IMS Media Bearer for S8HR APN. In such notifications, the S-GW/BBIFF also includes the UE location that it receives from the MME. This step is also independent of target specific LI service operation such as Step 1.

4. S-GW/BBIFF delivers the packets of those IMS Signalling Bearers to the LMISF. As such, S-GW/BBIFF has no idea whether the packets of an IMS Signalling Bearer are related to a target or not. It simply delivers all packets.

5. The LMISF looks for the SIP message within those packets delivered by the S-GW/BBIFF and examines the SIP headers that carry the calling party identity or called party identity (depending on the call direction) to verify whether any of those match with the target identity stored locally. If the SIP message corresponds to a target, then the LMISF delivers the SIP message to the DF2 over the X2 reference point. If required, the LMISF includes the UE location previously received from the S-GW/BBIFF while delivering the SIP messages to the DF2.

6. The DF2 will generate and deliver the IRI to the LEMF as per TS 33.108 [11].

The following steps are performed only if CC interception is required.

7. The LMISF then informs the S--GW/BBIFF about the IMS Signalling Bearer that corresponds to intercepted IMS session and instructs the S-GW/BBIFF to start delivering (to LMISF) the packets of the Media Bearers associated with that IMS Signalling Bearer.

NOTE 3: Step 7 is executed in parallel to step 5.

8. S-GW/BBIFF delivers the media packets to the LMISF. The S-GW/BBIFF knows that the media packets are related to an IMS Signalling Bearer, but does not know which media packet is related to which IMS session in the event target is involved in multiple sessions. The S-GW/BBIFF need not know that association.

9. LMISF looks at the media packets that it receives and examines the IP address and the port number associated with the RTP stream. Then LMISF will determine the associated IMS session comparing the IP address/port number of the RTP stream with the similar information from the IMS session. LMISF delivers the media packets to DF3 along with the Correlation Number it has used while delivering the SIP messages to DF2.

10. DF3 generates and delivers the CC as per TS 33.108 [11] to the LEMF.

Figure J.3 below illustrates the above steps in a flow diagram format.

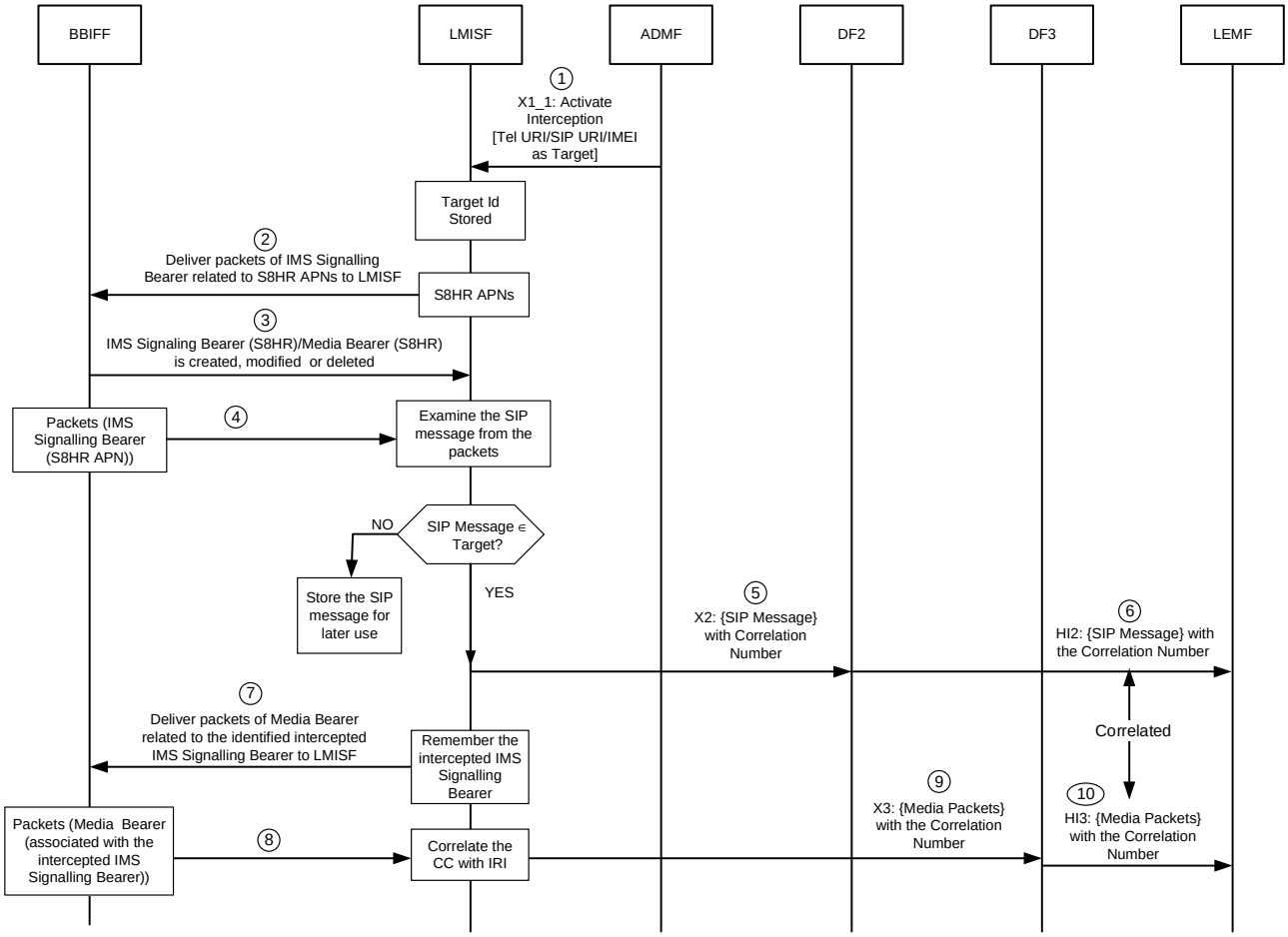


Figure J.3: Flow diagram illustrating the process steps for S8HR LI

The LMISF will be able to correlate the CC with the IRI since it receives both media packets and the IMS signalling packets.

Figure J.4 shows the steps when an intercept is deactivated during a VoLTE session.

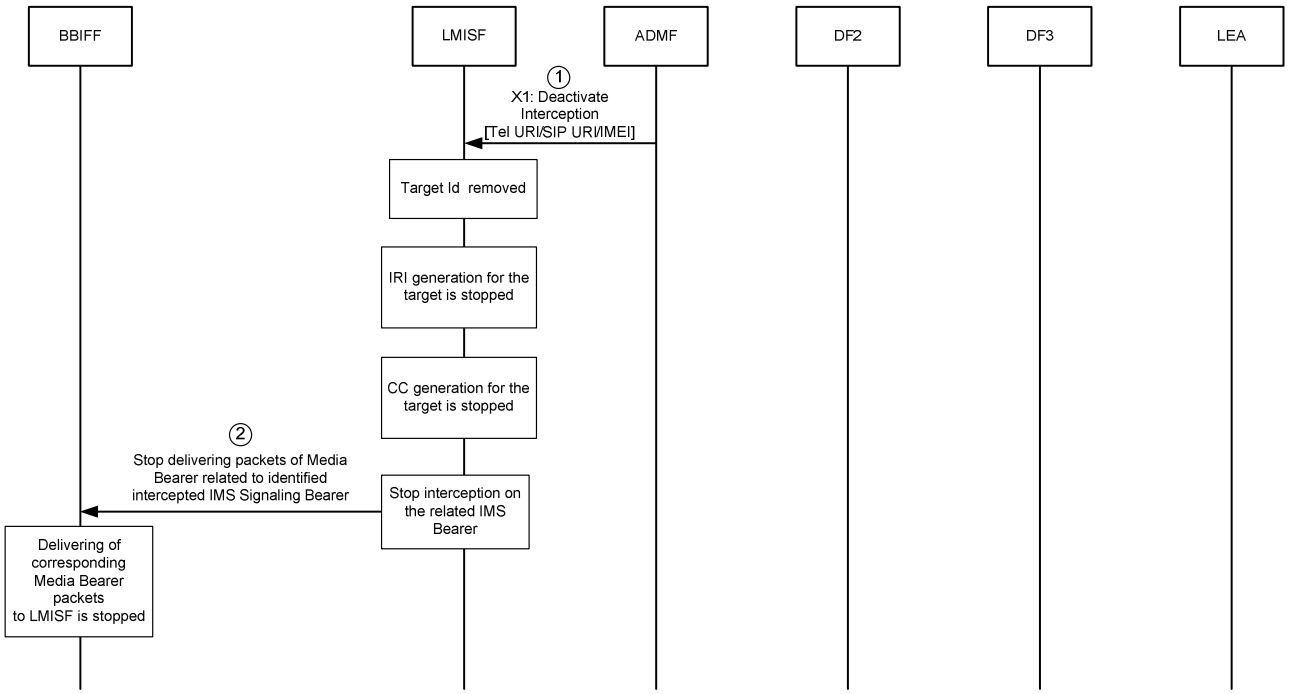


Figure J.4**: Flow diagram illustrating the process steps during intercept stop procedures for S8HR LI**

1. LMISF is provisioned to deactivate the lawful interception on the target (for Voice Services, it can be SIP URI, TEL URI or IMEI from the ADMF.

The LMISF will stop generation of IRI and CC immediately after it detects that the interception is deactivated.

The following steps may be required if CC interception is applicable.

2. The LMISF informs the S-GW/BBIFF about the identity of the IMS Signalling Bearer on which the interception is stopped and instructs the S-GW/BBIFF to stop delivering the packets of the Media Bearers associated to that IMS Signalling Bearer to LMISF.

The S-GW/BBIFF will stop delivering the media packets associated with the intercepted IMS Signalling Bearer to the LMISF.

J.3 Call Flows

J.3.1 General

Four call flows are presented in this clause:

- Inbound roaming target originates a voice call. The CC interception is required.
- A voice call is terminated to an inbound roaming target. The CC interception is required.
- An interception is activated while an inbound roaming user is active on a call.
- An inbound roaming user originates a voice call. The CC interception is not required.

In all the call flows, the target identity is the SIP URL or TEL URL. All the call flows assume that the SIP messages and the media are not encrypted at S-GW/BBIFF (one of the requirements for performing the lawful interception in the VPLMN for S8HR).

Independently of the active intercept on a target, the S-GW/BBIFF notifies the LMISF whenever an IMS Signalling Bearer or Media Bearer for S8HR APNs is created, modified or deleted. Such notifications include the up-to-date UE location information that S-GW receives from the MME. The LMISF includes the latest UE location information in the SIP messages that it reports to the DF2 for active intercepts.

J.3.2 Originating call

Figure J.5 below illustrates a call flow where an inbound roaming target originates a voice call. In the flow, Party_A (target) calls Party_B. The flow shows that Party_B is also an IMS user (SIP messages are shown), however, Party_B can also be a non-IMS user served by CS domain.

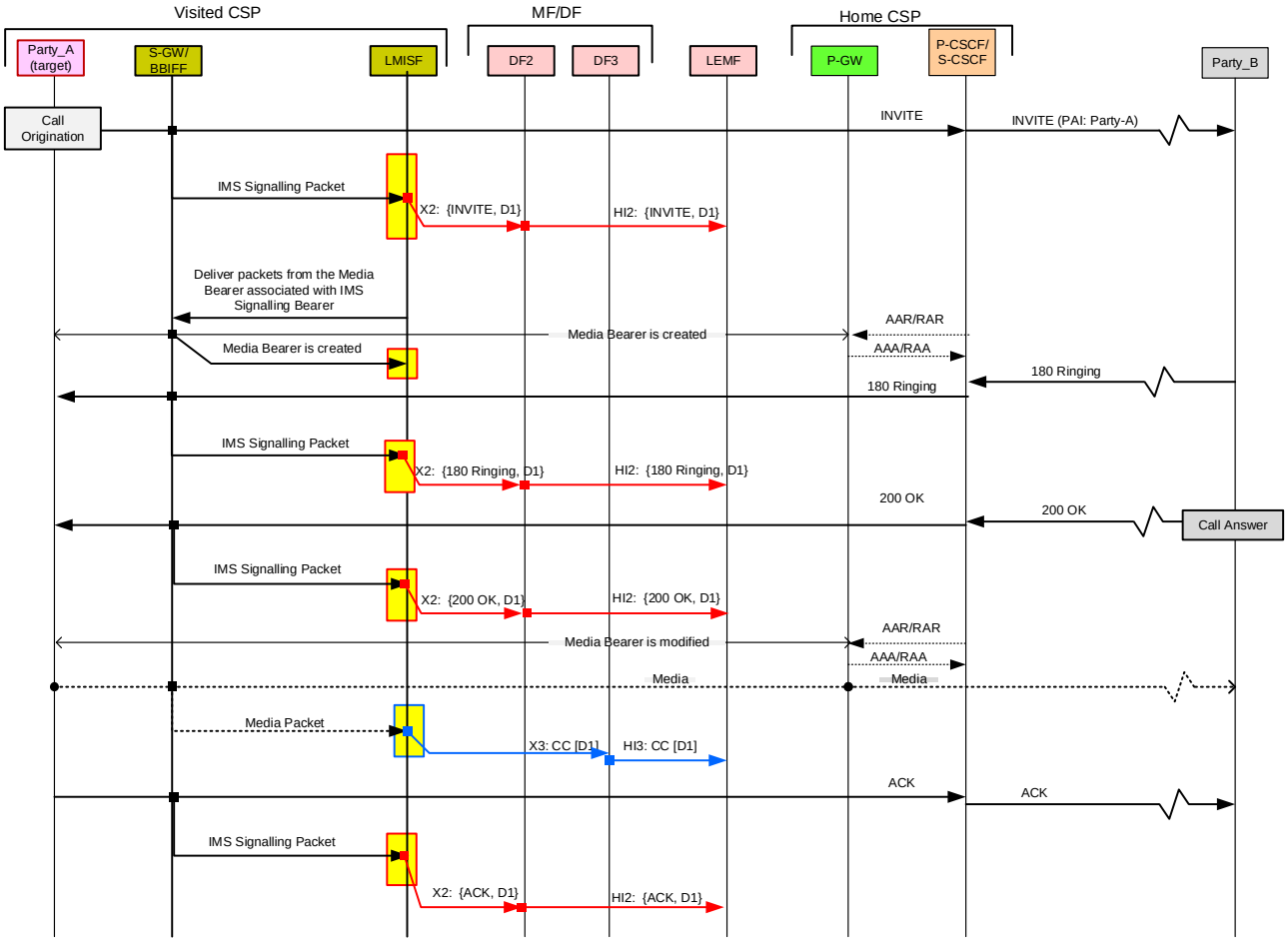


Figure J.5: Call Origination from an inbound roaming target with S8HR

The S-GW/BBIFF delivers the IMS signalling packets to the LMISF. The LMISF examines the SIP message to verify whether the SIP headers pointing to the calling party (e.g. P-preferred-Identity, From) is a target. In this illustration, that is the case, and therefore, the LMISF forwards the IRI message containing the SIP INVITE to the DF2 with correlation number D1. The DF2 forwards the IRI to the LEMF.

Since CC interception is required, the LMISF notifies S-GW/BBIFF with the IMS Signalling Bearer information associated with the intercepted IMS session. Once the dedicated EPS Bearer to be used as the Media Bearer linked to the EPS Bearer ID of the IMS Signalling Bearer is created, S-GW/BBIFF delivers the media packets flowing through the GTP tunnel used for that Media Bearer to the LMISF. The LMISF delivers the media packets as the CC along with the correlation number D1 to the DF3. The DF3 delivers the CC to the LEMF.

The LMISF delivers the subsequent SIP messages (in the call flow: 180 Ringing, 200 OK and ACK) received from the S-GW/BBIFF as IRI to the DF2 which in turn the deliver the same to the LEMF.

J.3.3 Terminating call

Figure J.6 below illustrates a call flow where an inbound roaming target receives a voice call. In the flow, Party_A calls Party_B (target). The flow shows that Party_A is also an IMS user (SIP messages are shown), however, Party_A can also be a non-IMS user served by CS domain.

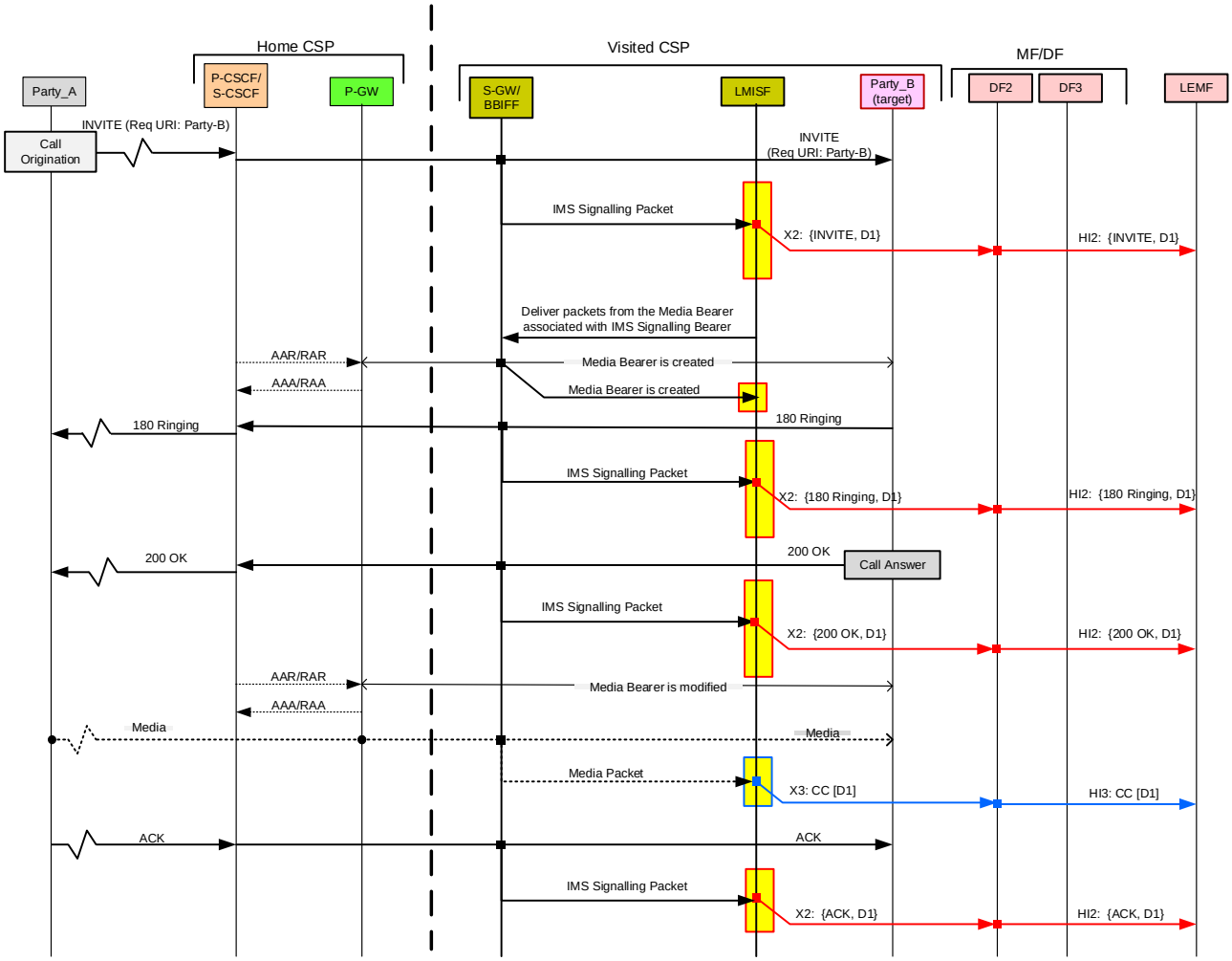


Figure J.6: Call Termination to an inbound roaming target with S8HR

The S-GW/BBIFF delivers the IMS signalling packets to the LMISF. The LMISF examines the SIP message to verify whether the SIP headers pointing to the called party (e.g. Request URI, P-Called-Party-Id, To) is a target. In this illustration, that is the case, and therefore, the LMISF forwards the IRI message containing the SIP INVITE to the DF2 with correlation number D1. The DF2 forwards the IRI to the LEMF.

Since CC interception is required, the LMISF notifies S-GW/BBIFF with the IMS Signalling Bearer information associated with the intercepted IMS session.

Once the EPS Bearer to be used as the Media Bearer linked to the EPS Bearer ID of the IMS Signalling Bearer is created, S-GW/BBIFF delivers the media packets flowing through the GTP tunnel used for that Media Bearer to the LMISF. The LMISF delivers the media packets as the CC along with the correlation number D1 to the DF3. The DF3 delivers the CC to the LEMF.

The LMISF delivers the subsequent SIP messages (in the call flow: 180 Ringing, 200 OK and ACK) received from the S-GW/BBIFF as IRI to the DF2 which in turn the deliver the same to the LEMF.

J.3.4 Mid-Call Interception

Figure J.7 below illustrates a call flow where a lawful interception is activated while an inbound roaming user is active on a voice call. In the flow, Party_A (target) calls Party_B. The flow shows that Party_B is also an IMS user (SIP messages are shown), however, Party_B can also be a non-IMS user served by CS domain.

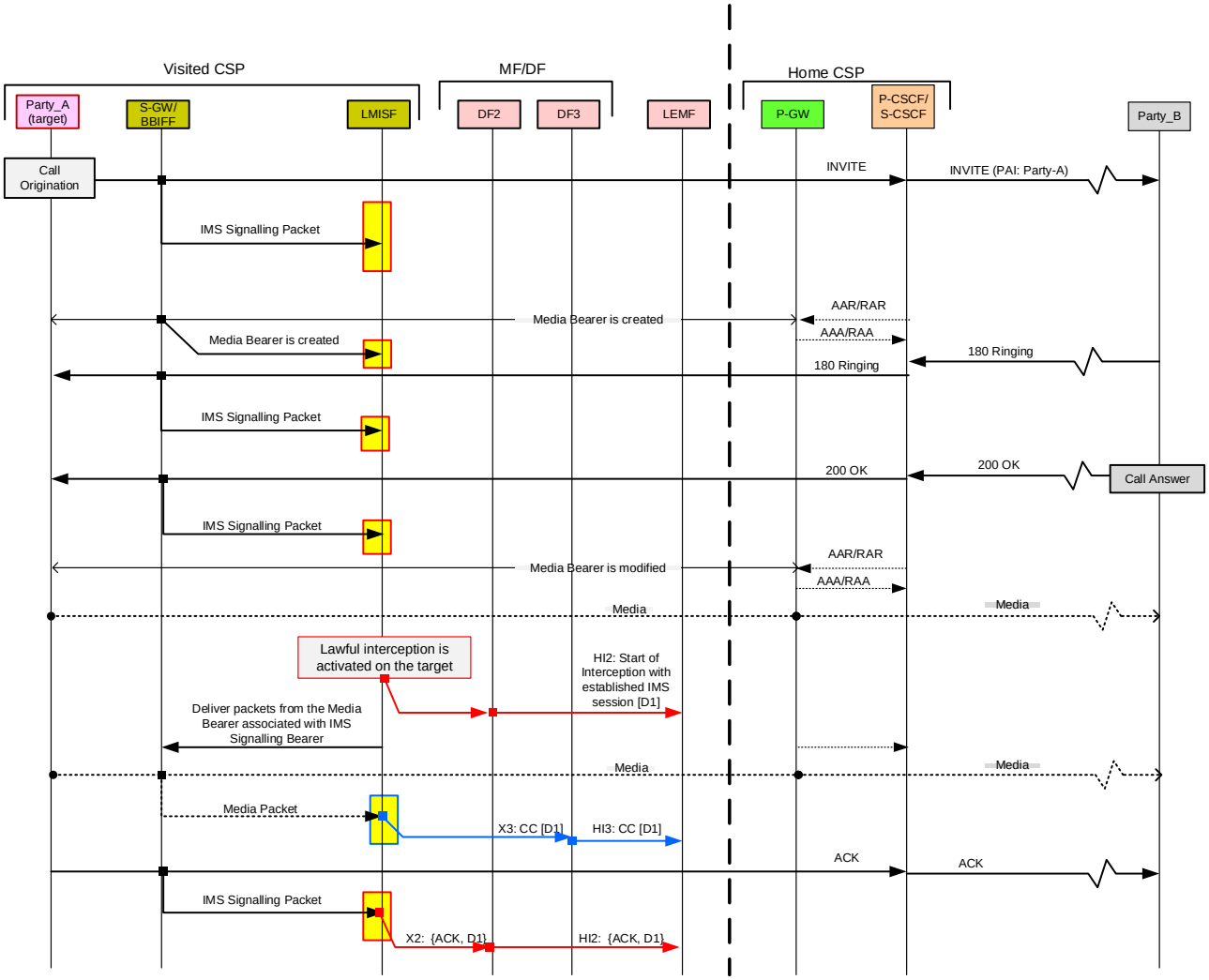


Figure J.7: Mid Call Interception

The S-GW/BBIFF delivers the IMS signalling packets to the LMISF. The LMISF examines the SIP message to verify whether the SIP headers pointing to the calling party (e.g. P-preferred-Identity, From) is a target. In this illustration, that is not the case, and therefore, the LMISF does not generate any IRI messages. However, the LMISF stores this SIP message and the subsequent SIP messages. The LMISF also maintains the IMS call state for the inbound roaming user.

In this illustration, a lawful interception is activated on the inbound roaming user right after the called party (Party_B) answers the call, but before the Party_A (target) has a chance to send the ACK message. Since the SDP offer and SDP answer are already completed, the LMISF generates the *Start Interception for established IMS session* with the Correlation Number D1 to the DF2 over X2 reference point. The DF2 forwards the same to the LEMF over the HI2 reference point.

NOTE: This flow assumes that there was no other lawful intercepts active on the target.

Since the just activated lawful interception requires CC interception, the LMISF notifies S-GW/BBIFF with the IMS Signalling Bearer information associated with the IMS session on which the lawful interception is activated.

The S-GW/BBIFF delivers the media packets from the GTP tunnel used for the Media Bearer linked to the EPS Bearer ID of the IMS Signalling Bearer to the LMISF. The LMISF delivers the media packets as the CC along with the correlation number D1 to the DF3. The DF3 delivers the CC to the LEMF over HI3 reference point.

The LMISF delivers the subsequent SIP messages (in the call flow: ACK) received from the S-GW/BBIFF as IRI to the DF2 which in turn the deliver the same to the LEMF.

J.3.5 Lawful Interception without CC

Figure J.8 below illustrates a call flow where an inbound roaming target originates a voice call. The lawful interception does not require CC interception. In the flow, Party_A (target) calls Party_B. The flow shows that Party_B is also an IMS user (SIP messages are shown), however, Party_B can also be a non-IMS user served by CS domain.

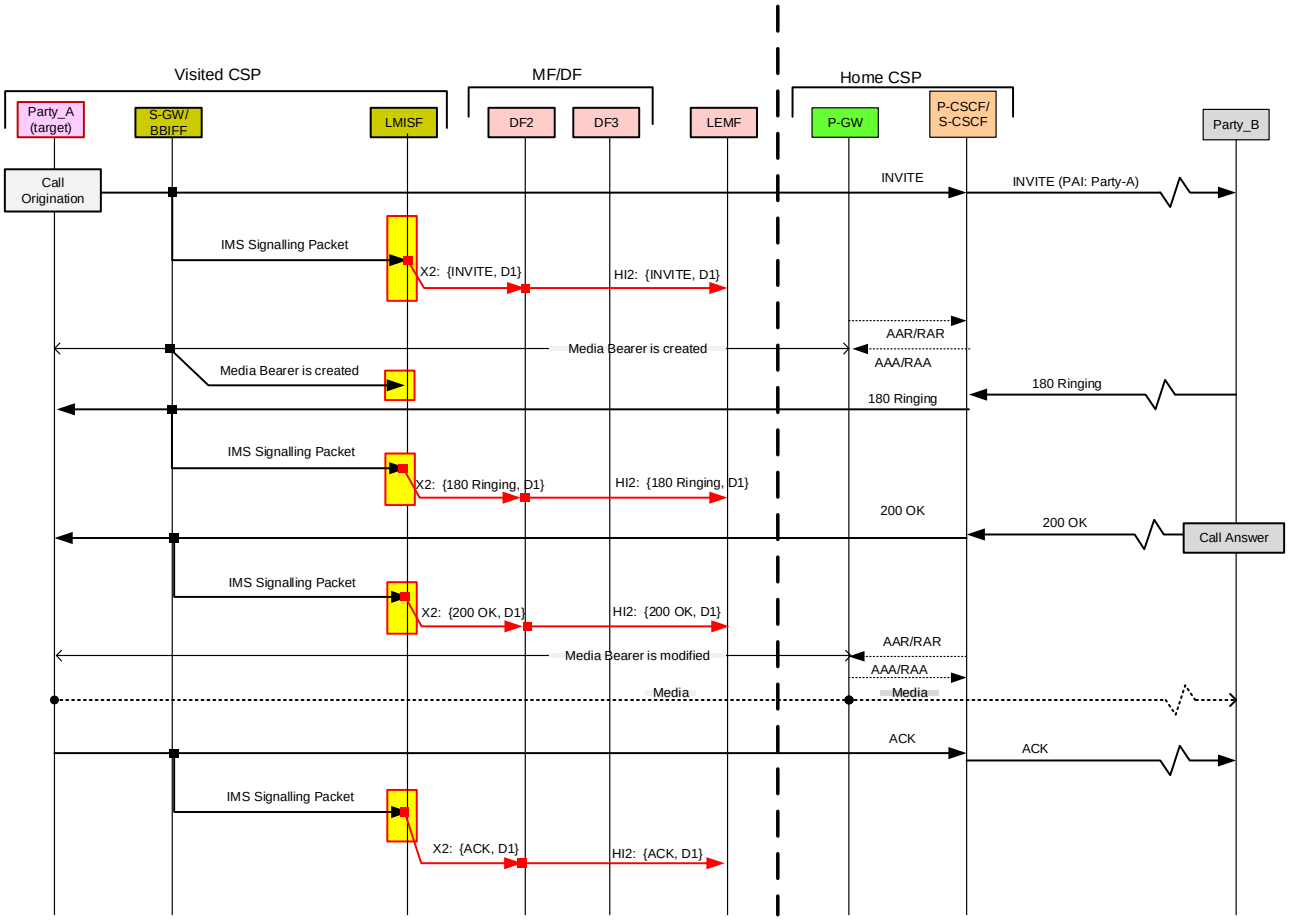


Figure J.8: Call Origination from an inbound roaming target with S8HR; CC is not required

The S-GW/BBIFF delivers the IMS signalling packets to the LMISF. The LMISF examines the SIP message to verify whether the SIP headers pointing to the calling party (e.g. P-preferred-Identity, From) is a target. In this illustration, that is the case, and therefore, the LMISF forwards the IRI message containing the SIP INVITE to the DF2 with correlation number D1. The DF2 forwards the IRI to the LEMF.

Since CC interception is not required, the LMISF does not notify the S-GW/BBIFF with the IMS Signalling Bearer information associated with the intercepted IMS session.

S-GW/BBIFF does not deliver the media packets flowing through the GTP tunnel of Media Bearer to the LMISF. As a matter of fact, the S-GW/BBIFF does not know that the call involves a target.

The LMISF delivers the subsequent SIP messages (in the call flow: 180 Ringing, 200 OK and ACK) received from the S-GW/BBIFF as IRI to the DF2 which in turn the deliver the same to the LEMF.

J.3.6 S-GW Relocation

Figure J.9 below illustrates a call flow where a a S-GW relocation occurs while an inbound roaming user is active on a voice call. In the flow, Party_A (target) calls Party_B. The flow shows that Party_B is also an IMS user (SIP messages are shown), however, Party_B can also be a non-IMS user served by CS domain.

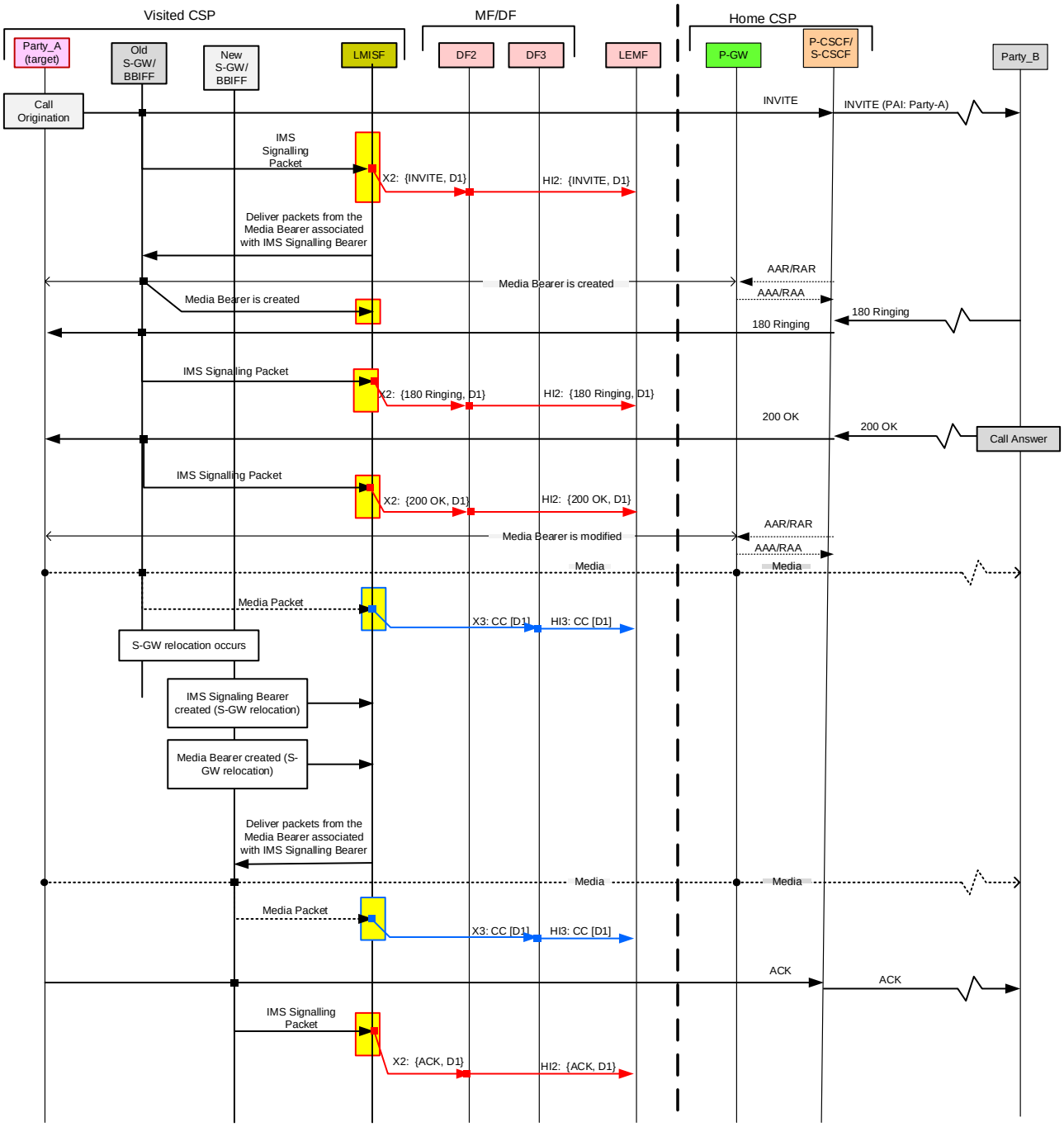


Figure J.9: S8HR LI with S-GW Relocation

The old S-GW/BBIFF delivers the IMS signalling packets to the LMISF. The LMISF examines the SIP message to verify whether the SIP headers pointing to the calling party (e.g. P-preferred-Identity, From) is a target. In this illustration, that is the case, and therefore, the LMISF forwards the IRI message containing the SIP INVITE to the DF2 with correlation number D1. The DF2 forwards the IRI to the LEMF.

Since CC interception is required, the LMISF notifies old S-GW/BBIFF with the IMS Signalling Bearer information associated with the intercepted IMS session.

Once the dedicated EPS Bearer to be used as the Media Bearer linked to the EPS Bearer ID of the IMS Signalling Bearer is created, old S-GW/BBIFF delivers the media packets flowing through the GTP tunnel used for that Media Bearer to the LMISF. The LMISF delivers the media packets as the CC along with the correlation number D1 to the DF3. The DF3 delivers the CC to the LEMF.

The LMISF delivers the subsequent SIP messages (in the call flow: 180 Ringing, 200 OK) received from the old S-GW/BBIFF as IRI to the DF2 which in turn the deliver the same to the LEMF.

In this illustration, a S-GW relocation happens right after the called party (Party_B) answers the call, but before the Party_A (target) has a chance to send the ACK message. When the IMS Signalling Bearer is created, the new S-GW/BBIFF notifies the LMISF along with the IMSI value with an indication that a S-GW relocation has occurred. The LMISF examines to see whether the IMS Signalling Bearer is associated with an intercepted IMS session. In this illustration since the CCinterception is required, the LMISF notifies the S-GW/BBIFF with the IMS Signalling Bearer information associated with the intercepted IMS session.

Once the dedicated EPS Bearer to be used as the Media Bearer linked to the EPS Bearer ID of the IMS Signalling Bearer is created, new S-GW/BBIFF delivers the media packets flowing through the GTP tunnel used for that Media Bearer to the LMISF. The LMISF delivers the media packets as the CC along with the correlation number D1 to the DF3. The DF3 delivers the CC to the LEMF.

The LMISF delivers the subsequent SIP messages (in the call flow: ACK) received from the new S-GW/BBIFF as IRI to the DF2 which in turn the deliver the same to the LEMF.

J.4 Correlation of CC and IRI

A target is identified using SIP URI, TEL URI or IMEI. Not all SIP messages carry these identities. The LMISF by maintaining the IMS call state is able to determine the subsequent SIP messages that correspond to the same target. When a target is involved in multiple IMS sessions, the LMISF will have the logic to associate and correlate the SIP messages that are related to an IMS session. For example, the SIP messages that have the same Call Identity value can be treated as the SIP messages of a particular IMS session and hence, when reported to the LEMF (via DF2) can have the same Correlation Number.

LMISF will also examine the SIP messages that carry the SDP offer and SDP answer to determine the media information related to an IMS session.

When an IMS session is established, the media information is exchanged between the two end points of the media stream (e.g. target's UE and IMS-AGW in HPLMN) through the SDP offer and answer process. The combination of IP address of the end point (e.g. UE and IMS AGW) and UDP port numbers used to transport the RTP and RTCP are part of this SDP offer and answer along with other things like Codec information. The media packets (i.e. RTP streams) exchanged between the two end points of the media use those IP addresses and the port numbers (assigned for RTP).

One method that can be used to establish the correlation is to use the IP addresses and the UDP port numbers exchanged within the SDP offer and answer process and compare them with the IP addresses and UDP port numbers of the media packets to establish an association between the IMS session and the media.

In other words, the IP address and UDP port numbers associated with a media packet when compared with the IP address and UDP port numbers exchanged in the SDP offer and answer, one can determine to which IMS session a media packet corresponds to. Once that determination is made, these parameters may be used to establish a correlation.

When S-GW/BBIFF is asked to deliver the packets from the IMS Signalling Bearers to LMISF, it delivers everything above the GTP-U layer. S-GW/BBIFF does not look into the IMS packets above the GTP-U layer. Similarly, when the S-GW/BBIFF is asked to deliver the packets from the Media Bearer to the LMISF, it delivers everything above the GTP-U layer. It does not look into the Media packets above the GTP-U layer. However, the BBIFF knows that the Media Bearer and the IMS Signalling Bearer are related through the GTP protocol concepts defined in TS 29.274 [38].

The LMISF will generate a Correlation Number and include that Correlation Number while delivering the SIP messages to the DF2. When the media packets are received, LMISF will examine the Media packets to determine which IMS session, the Media packets are related to. Once determined, the LMISF will deliver the Media packets to the DF3 along with the Correlation Number previously stored against the IMS session.

J.5 UE Location Reporting

Within the EPC, the MME sends the UE location to the S-GW within the Create Session Request and Create Bearer Response messages that it sends to the S-GW. The Create Session Request is sent from the MME to the S-GW when the default bearer is created. The Create Bearer Response is sent from the MME to the S-GW when a dedicated bearer used as Media Bearer is created.

In addition, the MME sends the UE location to the S-GW when a Bearer is modified (Modify Bearer Request and Update Bearer Response) or deleted (Delete Session Request and Delete Bearer Response).

The details of the above messages (i.e. Create Session Request etc.) are specified in 3GPP TS 29.274 [38].

For the S8HR LI, the S-GW/BBIFF notifies the LMISF whenever the IMS signalling bearer (i.e. default bearer) or Media Bearer (i.e. dedicated bearer linked to the IMS Signalling Bearer) is created, modified, or deleted. The S-GW/BBIFF includes the UE Location that it receives from the MME when it notifies the IMS signalling bearer creation and Media Bearer creation events to the LMISF.

The LMISF should store the UE location as it stores the IMSI value (currently specified in TS 33.107), and include the same in the appropriate IRI events sent to the DF2 over the X2 reference point.

The DF2 delivers the UE Location to the LEMF (when required) as it is done for the non-roaming scenario or in a roaming with LBO scenario.

Annex L (informative): IP-based Handover Interface for CC of CS Intercepts

L.1 Background

Figure L.1 shows an overview of the architecture that shows using IP-based handover interface for CC of CS intercepts:

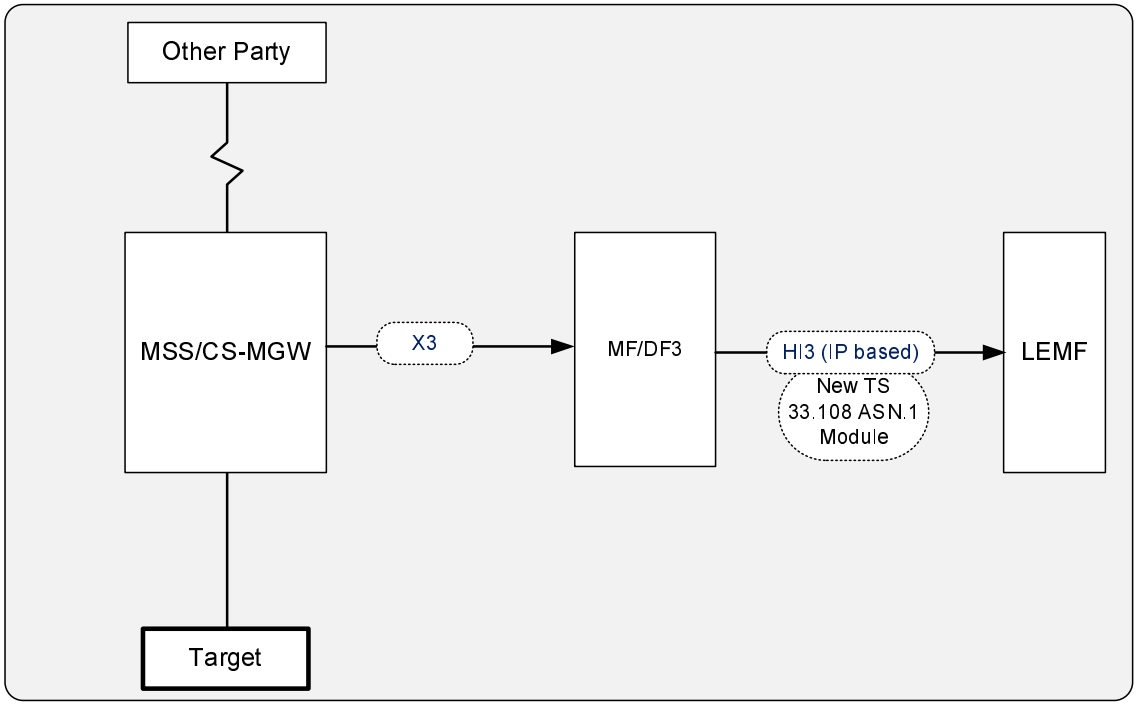


Figure L.1: General Concepts of IP-based Handover Interface using an ASN.1 module for HI3

The call content (CC) from CS-MGW is delivered to the MF/DF3 over X3 reference point. In some implementations, the MSS may also have to be part of the CC interception to provide the signalling aspects of the CC-related call setup. The X3 reference point is not standardized in the present document.

L.2 Options for X3

This sub-clause provides a few options for realizing the X3 reference to support an IP-based handover interface. Figure L.2 shows three different possible options:

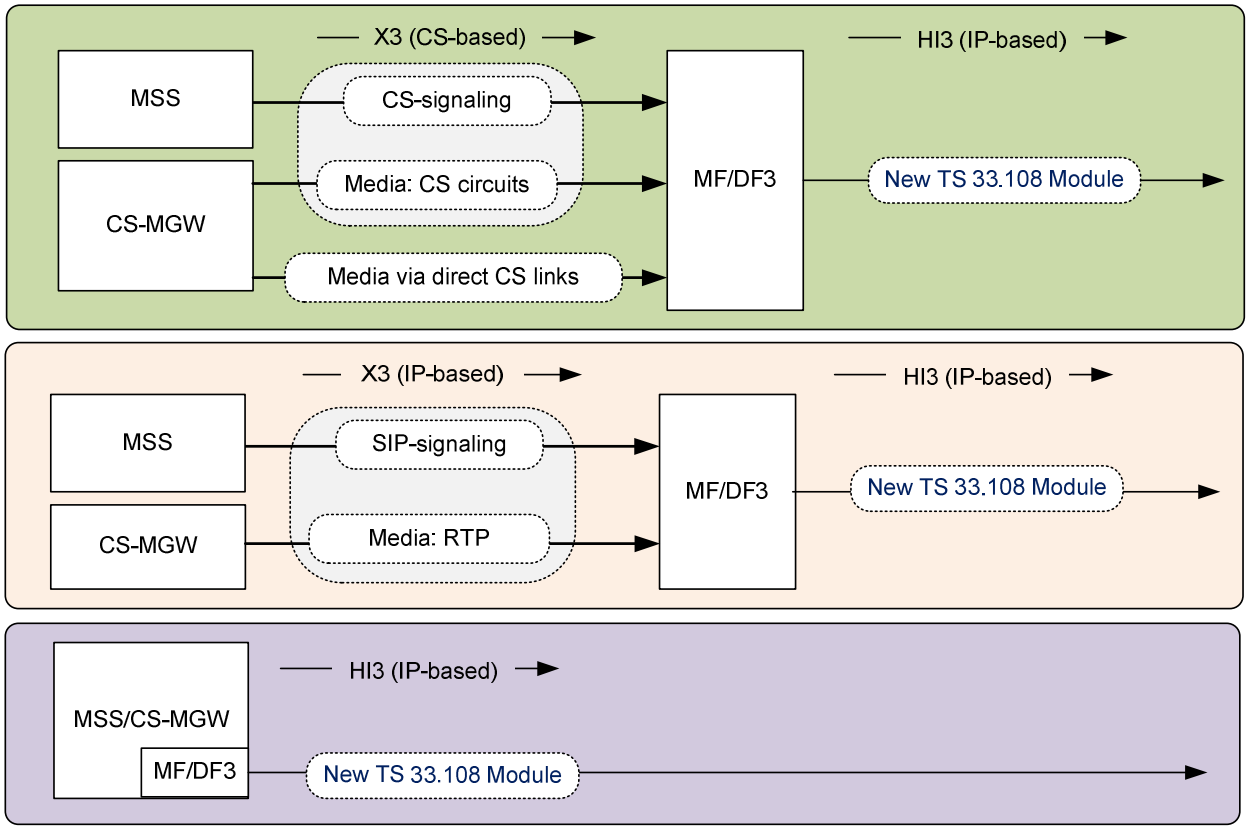


Figure L.2: Three options for X3 reference point

The X3 reference point can be CS based in which case the MF/DF3 will have to convert the CS-based CC into RTP (RFC 3550 [86]) streams and then deliver the same over the HI3 reference point using the new ASN.1 object module (see TS 33.108 [11]) to the LEMF. The CS circuits that carry the content of intercepted call can be based on the dedicated direct links between the CS-MGW and the MF/DF3, or dynamic links setup via CS-based signalling (e.g. ISUP or ISDN).

The X3 reference point can also be a SIP-based in which case MSS will have to set up the SIP session and CS-MGW will have to deliver the CC in the form of RTP. The SIP-based signalling may use either SIP (RFC 3261 [88]) or SIP-I (RFC 3998 [87]). The MF/DF3 would have to deliver the received RTP streams to the LEMF using the the new ASN.1 object module (see TS 33.108 [11]) to the LEMF.

In another option, the MF/DF3 function can be integrated into the MSS/CS-GW and in this case, that integrated MF/DF3 will have to deliver the CC using the new ASN.1 object module (see TS 33.108 [11]) to the LEMF. However, realization of this approach can be complex since it will require the MSS/CS-MGW to have the capability to support the generation of RTP streams and then ASN.1 module based handover interface.

L.3 Information delivered along with the CC

The CC delivered using the IP-based delivery interface should carry the following information at the minimum:

- Correlation information: to correlate the CC with the IRI messages
- Payload description: to decode the RTP streams
- Media direction: to indicate whether the payload belongs to target transmit or target receive or in a combined form.

The method used by the MF/DF3 in determining the above information is outside the scope of the present document. For example, the DF2 may pass the correlation information to the MF/DF3 or MSS may pass the correlation information to the MF/DF3. Since the RTP payload is constructed at the MF/DF3, the MF/DF3 may be able to derive the payload description on its own. The intercepted voice media stream may be delivered to the LEAs in a combined form (i.e. target transmit and receive as one stream) or in separated form (target transmit and target receive). The media direction may be provided by the MSS to the MF/DF3 or the MF/DF3 may derive the media direction using the other means.

Annex M (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
	SA_03			-		Approved at SA#6 and placed under TSG SA Change Control	3.0.0
	SA_10	SP-000625	0001	-		Addition of parameters to the X3-Interface	3.1.0
2000-03	SP-11	SP-010137	0002	-		Correction of Location information parameters in interception event records	3.2.0
2000-03	SP-11	SP-010146	0003	-		Update of TS 33.107 for Release 4 - Inclusion of PS LI requirements	4.0.0
2000-06	SP-12	SP-010374	0004	1	B	Update of TS 33.107 for Release 5	5.0.0
2001-12	SP-14	SP-010612	0010	-	A	Start of secondary interception of an active PDP context	5.1.0
2001-12	SP-14	SP-010613	0011	-	C	Alignment of TS 33.107 for Release 5 Network Architecture	5.1.0
2001-12	SP-14	SP-010614	0014	-	A	Correct the MO-SMS and MT-SMS events	5.1.0
2001-12	SP-14	SP-010615	0016	-	A	Source of PDP context initiation	5.1.0
2002-03	SP-15	SP-020109	0017	-	B	PDP context Deactivation cause	5.2.0
2002-03	SP-15	SP-020110	0018	-	B	The use of H.248 in setting up a bearer intercept point at the MGW	5.2.0
2002-03	SP-15	SP-020111	0021	-	B	Inter-SGSN RA update with active PDP context	5.2.0
2002-03	SP-15	SP-020112	0022	-	B	Addition of PDP context modification Event and Transferring the QoS information element across the X2 interface	5.2.0
	-	-	-	-	-	Change History new version corrected for SP-15 CRs	5.2.1
2002-06	SP-16	SP-020345	0023	-	B	Changes to 33.107 to support interception at a GGSN	5.3.0
2002-06	SP-16	SP-020345	0024	-	B	Addition of SMS type information	5.3.0
2002-06	SP-16	SP-020345	0025	-	C	Inclusion of Serving System IRI in TS 33.107	5.3.0
2002-09	SP-17	SP-020511	0026	-	F	Essential clarification to the Timestamp IE	5.4.0
2002-09	SP-17	SP-020511	0027	-	F	Additional X3-interface parameters	5.4.0
2002-12	SP-18	SP-020702	0028	-	F	Event Time	5.5.0
2002-12	SP-18	SP-020704	0029	-	F	Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active	5.5.0
2002-12	SP-18	SP-020703	0030	-	F	Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active	5.5.0
2002-12	SP-18	SP-030478	0031	-	F	Missing QoS Parameter in IRI	5.6.0
2003-09	SP-21	SP-030479	0032	-	B	TEL URL for IMS interception identity (Release 6)	6.0.0
2003-09	SP-21	SP-030479	0032	-	D	Stereo delivery to LEMF	6.0.0
2003-12	SP-22	SP-030590	0034	-	F	MSISDN/IMEI clarification for GPRS interception	6.1.0
2003-12	SP-22	SP-030591	0035	-	F	Reporting TEL URL	6.1.0
2004-06	SP-24	SP-040397	0036	-	F	Correction on Network initiated Mobile Station Detach signalling flow	6.2.0
2004-06	SP-24	SP-040398	0037	-	F	TEL-URL missing in activation of LI in the CSCFs	6.2.0
2004-06	SP-24	SP-040399	0038	-	F	Correction on the use of session initiator parameter	6.2.0
2004-06	SP-24	SP-040400	0039	-	F	Correction to HLR interception event name	6.2.0
2004-06	SP-24	SP-040401	0040	-	B	Clarification for Push to talk over Cellular	6.2.0
2004-06	SP-24	SP-040402	0041	-	F	Adding an encryption parameter to IRI across X2 interface	6.2.0
2004-06	SP-24	SP-040403	0042	-	F	References	6.2.0
2004-06	SP-24	SP-040404	0043	-	F	Enhancements for the Functional Architecture chapter	6.2.0
2004-09	SP-25	SP-040693	0044	-	F	Correction on the use of session initiator parameter	6.3.0
2004-09	SP-25	SP-040693	0045	-	F	ICE (Intercepting Control Elements), INE (Intercepting Network Elements) definition	6.3.0
2004-09	SP-25	SP-040693	0046	-	F	Clarification to SMS interception	6.3.0
2004-09	SP-25	SP-040693	0047	-	F	Replace SIP URL with SIP URI	6.3.0
2004-12	SP-26	SP-040850	0048	-	B	Lawful Interception for WLAN Interworking	6.4.0
2004-12	SP-26	SP-040850	0049	-	F	33.107 Cleanup	6.4.0
2004-12	SP-26	SP-040850	0050	-	B	Clarification on MMS interception	6.4.0
2005-06	SP-28	SP-050256	0052	-	F	Correction on the use of identities for I-WLAN lawful interception	6.5.0
2005-06	SP-28	SP-050257	0051	1	F	Clarifications for the usage of the notion of a service in distributed IP networks	7.0.0
2005-06	SP-28	SP-050257	0053	-	C	Correlation for IMS interception	7.0.0
2005-09	SP-29	SP-050570	0054	-	F	Clarifications to the RAU event	7.1.0
2005-09	SP-29	SP-050570	0055	-	C	Simplifications to LDI handling	7.1.0
2005-12	SP-30	SP-050779	0054	-	B	Start of interception for already attached UE	7.2.0
2005-12	SP-30	SP-050763	0056	-	A	Availability of IMSI at PDG	7.2.0
2006-03	SP-31	SP-060064	0057	-	F	WLAN Interworking - Additional Details for TS 33.107	7.3.0
2006-09	SP-33	SP-060659	0058	1	F	Editorial Update by Rapporteur	7.4.0
2007-03	SP-35		0060	-	B	Stage 2 MBMS Interception	7.5.0
2007-03	SP-35	SP-070156	0061	1	F	SMS IRI Reporting for WLAN Interworking	7.5.0
2007-06	SP-36	SP-070331	0063	-	B	Direct Tunnel LI	7.6.0
2007-06	SP-36	SP-070332	0062	-	B	NSAPI (Network layer Service Access Point Identifier) optional in IRI	8.0.0
2007-09	SP-37	SP-070601	0065	-	B	WLAN IRI at AAA for re-authentication	8.1.0
2007-09	SP-37	SP-070599	0064	-	A	Stage 2 MBMS Interception	8.1.0
2007-12	SP-38	SP-070788	0066	-	C	P-CSCF IMS LI Optional	8.2.0
2007-12	SP-38	SP-070788	0067	-	C	MBMS IRI Registration	8.2.0
2008-03	SP-39	SP-080172	0068	1	D	CR on P-CSCF IMS LI Optional	8.3.0

2008-03	SP-39	SP-080172	0069	1	D	Removing "P" suffix from references	8.3.0
2008-03	SP-39	SP-080172	0070	1	B	Changes for Interception of IRI and CC at a WAG	8.3.0
2008-06	SP-40	SP-080262	0071	-	F	CSCF SIP Event reporting	8.4.0
2008-06	SP-40	SP-080262	0072	-	B	Conference Event Reporting	8.4.0
2008-06	SP-40	SP-080262	0073	-	D	Editorial corrections	8.4.0
2008-09	SP-41	SP-080514	0074	-	B	Updates to TS 33.107 to support LI for EPSs	8.5.0
2008-12	SP-42	SP-080762	0077	-	F	Editorial corrections to 33.107	8.6.0
2008-12	SP-42	SP-080762	0075	-	F	Corrections and clarifications of LI for EPS and alignment with latest version of SAE stage 2 specs.	8.6.0
2008-12	SP-42	SP-080762	0076	-	F	Clarification on 3G DT with the GGSN	8.6.0
2009-03	SP-43	SP-090133	0078	-	F	Alignment with SAE stage 2 specifications approved by TSG SA#42	8.7.0
2009-04						Editorial correction to cover page	8.7.1
2009-06	SP-44	SP-090272	0079	-	F	Correction on UE requested bearer resource modification - Alignment with SAE stage 2 specification	8.8.0
2009-06	SP-44	SP-090272	0080	-	F	Clarification on parameter APN	8.8.0
2009-06	SP-44	SP-090272	0081	-	F	Clarification on the handover between 2G/3G access and E-UTRAN with Gn/Gp	8.8.0
2009-06	SP-44	SP-090272	0082	-	F	Clarification on parameter PDN type	8.8.0
2009-09	SP-45	SP-090522	0083	-	F	Correction on identities and parameters for LI in case of E-UTRAN access and PMIP based S5/S8	8.9.0
2009-09	SP-45	SP-090522	0084	-	F	Correction on Serving Evolved Packet System event	8.9.0
2009-10	--	--	--	--	--	Correction of misimplementation of CR0084	8.9.1
2009-12	SP-46	SP-090817	86	-	F	Correction on events names	8.10.0
2009-12	SP-46	SP-090817	87	-	F	Restoring section header 9.4.5	8.10.0
2009-12	SP-46	SP-090817	88	-	F	Correction on PDP context modification event	8.10.0
2009-12	SP-46	SP-090817	85	-	F	Correction on LI correlation for S4-SGSN	8.10.0
2009-12	-	-	-	-	-	Update to Rel-9 version (MCC)	9.0.0
2010-06	SP-48	SP-100364	89	-	F	Correction in IMS Conference text	9.1.0
2010-06	SP-48	SP-100253	90	-	F	Reporting of Dual Stack PDP address from the SGSN	10.0.0
2010-10	SP-49	SP-100570	92	-	A	Correction in IMS Conference Service X2 interface	10.1.0
2010-10	SP-49	SP-100570	93	-	A	IMS Conference Service configuration for CC interception	10.1.0
2010-10	SP-49	SP-100481	91	-	F	Unsuccessful bearer modificatio	10.1.0
2010-10	SP-49	SP-100481	94	-	B	LI architecture and functions for KMS based IMS Media Security	10.1.0
2010-10	--	--	--	--	--	ToC update	10.1.1
2010-12	SP-50	SP-100845	97	1	A	IMSI based activation	10.2.0
2010-12	SP-50	SP-100865	98	1	B	MME start of interception with bearer active	10.2.0
2010-12	SP-50	SP-100865	103	1	C	Corrections and Alignment for IMS Conferencing	10.2.0
2011-03	SP-51	SP-110023	104	-	B	Location information from trusted non-3GPP access	10.3.0
2011-03	SP-51	SP-110023	106	-	C	Security requirements for LI in KMS based IMS media security	10.3.0
2011-03	SP-51	SP-110023	111	-	F	Initiator parameter definition	10.3.0
2011-03	SP-51	SP-110021	109	-	A	IMS Conf LI 33.107	10.3.0
2011-06	SP-52	SP-110260	112	-	C	TLS and IPsec profiling for Xk interface	10.4.0
2011-09	SP-53	SP-110511	113	-	B	Reporting of PMIP and DSMIP session modification	11.0.0
2012-03	SP-55	SP-12-0034	114		F	Correction on MIP specific parameters provided over the X2 interface.	11.1.0
2012-06	SP-56	SP-120336	114a	1	C	IMSI in untrusted non-3GPP access	11.2.0
2012-06	SP-56	SP-120336	115	1	C	SGs received location transfer over the X2 interface	11.2.0
2012-06	SP-56	SP-120336	116	2	F	UE IP Address at X2 interface	11.2.0
2012-06	SP-56	SP-120336	117	1	F	Handover indication at X2 interface	11.2.0
2012-06	SP-56	SP-120336	118	1	F	IMS Conference Services	11.2.0
2012-06	SP-56	SP-120336	119	1	F	IMS Provison of CC	11.2.0
2012-09	SP-57	SP-120627	120	1	F	Reference list correction to align with the corrected TS 29.212 title	11.3.0
2012-09	SP-57	SP-120600	121	-	B	H(e)NB Support in TS 33.107	12.0.0
2012-12	SP-58	SP-120854	122	-	B	LI events for trusted non-3GPP access on GTP S2a, Rel12	12.1.0
2012-12	SP-58	SP-120854	123	-	F	Removal of LTE	12.1.0
2013-03	SP-59	SP-130034	124	-	B	Start of interception for an already established IMS media secured session	12.2.0
			125	-	F	Correcting 33.107 and 33.108 differences - TFT is applicable only to dedicated bearer	
2013-06	SP-60	SP-130248	126	-	C	Provision on Unencrypted CC	12.3.0
			127	-	B	Mid Session Interception for IMS	
2013-09	SP-61	SP-130401	128	-	B	Addition of LI to GBA	12.4.0
			129	-	F	Adding version to non 3GPP references	
			130	-	F	Updating Tel URL to Tel URI	
2013-12	SP-62	SP-130661	131	-	B	ULI timestamp reporting	12.5.0
			132	-	D	Editorial Correction on header	
			133	-	B	107 UMTS IRI Packet Header Information Reporting	
			134	-	B	107 WLAN IRI Packet Header Information Reporting	
			135	-	B	107 LTE IRI Packet Header Information Reporting	
			136	-	F	Correction to I-WLAN LI location information reporting	
			137	-	D	Editorial Fix of implementation of SA3LI13_073r3	

2014-03	SP-63	SP-140020	138	-	C	Handling of unsuccessful LI procedures in getting encryption keys from the KMS	12.6.0
			139	-	B	Basic architecture to deliver location information based Civic Addresses	
			140	-	F	Clarification to EPS Interception for Trusted Non-3GPP IP Access	
			141	-	B	Addition of VoIP LI Functions	
2014-06	SP-64	SP-140310	142	-	F	Editorial clean-up of target & monitored subscriber	12.7.0
			143	-	F	Editorial clean-up of incorrect paragraph numbering	
			144	-	A	IMS IMEI Interception	
			145	-	B	LI for GCSE Group Communications	
			147	-	C	IMS-Based VoIP LI Enhancements	
			148	-	B	Adding the interception of ProSe Direct Discovery	
			149	-	B	IMS-based VoIP Stage 2 Call Flows	
2014-09	SP-65	SP-140586	150	-	B	LI functionalities for GTP based s2b interfaces	12.8.0
			151	-	D	Editorial Corrections	
			152	-	F	Clarification on interception of VoIP CC for targeted calls	
			153	-	C	Change of 'Decryption for IMS Media Plane Security' clause: making it more specific regarding E2E/E2AE modes	
			154	-	F	Intercept trigger and X3 alignment for IMS based VOIP stage 2	
			155	-	A	IMEI-based LI stage 2 description	
			157	-	C	Clarifications to IMS Interception relative to CC	
			158	-	D	Hanging paragraph repair	
2014-12	SP-66	SP-140821	159	-	B	Adding the interception feature of any XCAP usages	12.9.0
			160	-	F	Editorial Correction to Stage 2 call flows (VoIP)	
			161	-	C	Group Communications LI with GSC AS outside the intercepting CSP's network	
			162	-	B	Adding the Mask parameter to the interception of ProSe direct discovery	
			163	-	C	Alignment of LI for GCSE with HI2 & HI3	
			164	-	B	LI for ProSe One to Many Communications - In Network Coverage	
2015-03	SP-67	SP-150075	165	-	F	Correction to referenced in-house clauses	12.10.0
			166	-	F	Adding a minor note on how to understand the architecture that support the annex M of TS 33.108 on Hi1 over Hi2	
			167	-	F	Clarification on X interfaces	
			168	-	F	Adding logical function information	
			169	-	F	Uniform use of "target"	
			170	-	B	Adding the details of ProSe one-to-many communication interception	
			171	-	B	WebRTC Interworking LI Stage 2	
2015-06	SP-68	SP-150296	172	-	F	Clarification on the delivery of encryption keys and the CC delivery	12.11.0
			173	-	F	Delivery of media information to LEAs when transcoding is involved	
2015-09	SP-69	SP-150469	174	4	F	Adding WLAN interworking maintanance statement	12.12.0
		SP-150470	175	3	B	New events related to some messages to and from HSS/HLR	13.0.0
			176	2	B	Addition of Multiple Delivery Addresses for Resilience and Failover Mechanism	
			177	1	D	Introduce a clause for a hanging paragraph in clause 15.2.	
			178	4	F	Media Information Reporting	
			179	2	F	CC Interception in HPLMN in some roaming scenarios	
			180	2	B	Separate Delivery of Messaging Services - ICE-DF	
			181	1	F	Correcting the drawing errors in two figures of Annex F	
2015-12	SP-70	SP-150724	182	1	B	LI features and events with HLR for CS domain	13.1.0
			183	-	B	Reporting of UE local IP address and port	
			184	5	B	New LI events related to HSS in IMS, non 3GPP access network	
			185	3	F	Correction to have consistant event name Packet Data Header Information	
			186	1	B	Call flow to illustrate the CC Unavailable case	
			187	1	F	Insertion of call flow that was accidentally deleted	
		SP-150728	192	1	A	LTE Location Information: Cell Based IRI Reporting (MME)	
2016-03	SP-71	SP-160050	193	1	F	Editorial clean up	13.2.0
2016-03	SP-71	SP-160050	194	1	F	Removing requirements from NOTEs	13.2.0
2016-03	SP-71	SP-160050	195	3	F	Stage 2 Description of LI Functions in the VPLMN for IMS Roaming	13.2.0
2016-03	SP-71	SP-160050	196	2	B	User Location Information reporting extensions over s2b	13.2.0
2016-03	SP-71	SP-160050	197	1	B	Interception of ProSe Remote UE	13.2.0
2016-06	SA#72	SP-160384	0198	1	F	Stage 2: TWAN Location for default bearer as well	13.3.0
2016-06	SA#72	SP-160384	0215	2	B	Mega changes to allow Location Services (LCS)	13.3.0
2016-09	SA#73	SP-160564	0216	3	B	Lawful Access Location Services - Stage 2	13.4.0
2016-09	SA#73	SP-160564	0217	3	B	Non-Local ID interception CS domain and GSN/SGSN issue about SMS	13.4.0
2016-09	SA#73	SP-160564	0218	4	B	Non-Local ID interception with VoIP/IMS services and cleaning up of the security clause	13.4.0

2016-09	SA#73	SP-160564	0219	3	B	Non-Local ID interception with VoIP/IMS services with IBCF	13.4.0
2016-09	SA#73	SP-160564	0222	-	D	Correcting the editorial errors	13.4.0
2016-09	SA#73	SP-160564	0223	-	F	Acting on an Editor's Note in clause 7A.2.1	13.4.0
2016-09	SA#73	SP-160564	0225	1	C	Informative Stage 2 Call Flows to illustrate the IMS Conferencing Steps	13.4.0
2016-09	SA#73	SP-160564	0226	1	B	Informative Annex on the interception of Target with Non-Local ID	13.4.0
2016-09	SA#73	SP-160564	0227	2	B	Separate Delivery of Messaging Services	13.4.0
2016-09	SA#73	SP-160564	0228	1	B	Toggle for Roaming	13.4.0
2016-09	SA#73	SP-160564	0230	2	B	LI for ProSe UE-to-NW Relay	13.4.0
2016-12	SA#74	SP-160797	0232	2	F	Targeting of Non-Local ID in case of SMS usages: correction of existing texts	13.5.0
2016-12	SA#74	SP-160797	0233	-	F	Corrections on deregistrations events	13.5.0
2016-12	SA#74	SP-160798	0231	1	B	Proposes Stage 2 description for S8HR LI	14.0.0
2016-12	SA#74	SP-160798	0234	1	B	Separate Delivery of MMS	14.0.0
2016-12	SA#74	SP-160798	0235	1	C	VPLMN ID for IMS VoIP Events	14.0.0
2016-12	SA#74	SP-160798	0236	1	F	Adding Missing Parameters for HLR Events to Common Table	14.0.0
2017-03	SA#75	SP-170037	0237	1	B	Stage 2 description for CUPS LI	14.1.0
2017-03	SA#75	SP-170037	0238	1	C	Phase 2 of LALS development - Stage 2 description	14.1.0
2017-03	SA#75	SP-170036	0240	2	A	Location information for ProSe UE-to-NW Relay	14.1.0
2017-03	SA#75	SP-170037	0242	1	C	Separate Delivery of MMS	14.1.0
2017-03	SA#75	SP-170036	0243	-	A	SDP_info at DF3	14.1.0
2017-06	SA#76	SP-170342	0244	1	C	Changes to S8HR LI Stage 2 description to address the agreed simplifications	14.2.0
2017-06	SA#76	SP-170342	0245	1	C	S8HR LI with CUPS for S-GW	14.2.0
2017-06	SA#76	SP-170342	0248	1	C	S8HR LI - stage 2 descriptions addressing SGW Relocation with one LMISF	14.2.0
2017-06	SA#76	SP-170342	0249	1	B	Non-local ID target at the MMS level	14.2.0
2017-09	SA#77	SP-170706	0251	1	A	Incorrect usage of interception type in a ProSe Direct Discovery clause	14.3.0
2017-09	SA#77	SP-170707	0252	1	B	SMS over NAS	14.3.0
2017-09	SA#77	SP-170707	0255	1	B	Push to Talk over Cellular Service adding of functional architecture, references, definitions, and abbreviations	14.3.0
2017-09	SA#77	SP-170707	0256	1	B	Push to Talk over Cellular service addition feature Part A	14.3.0
2017-09	SA#77	SP-170707	0258	1	B	Requirement to Toggle interception for an outbound international roaming target	14.3.0
2017-09	SA#77	SP-170707	0259	1	F	CUPS to support LI	14.3.0
2017-12	SA#78	SP-170841	0265	-	F	S8HR LI - replacing the erroneous call fow	14.4.0
2017-12	SA#78	SP-170841	0266	1	F	Push to Talk over Cellular Service corrections of the functional architecture	14.4.0
2017-12	SA#78	SP-170841	0267	2	F	Push to Talk over Cellular corrections and additional events	14.4.0
2017-12	SA#78	SP-170840	0268	1	A	IP-based CC handover interface for CS intercepts (stage 2)	14.4.0
2017-12	SA#78	SP-170841	0269	1	F	Include DF3 based approach for packet data header reporting with CUPS LI	14.4.0
2017-12	SA#78	SP-170840	0271	1	A	Corrections on LI for HSS in IMS	14.4.0
2017-12	SA#78	SP-170841	0273	-	F	Move IMS VoIP text from clause 7A to clause 15	14.4.0
2017-12	SA#78	SP-170841	0274	1	F	Administrative changes	14.4.0
2017-12	SA#78	SP-170842	0272	2	B	Support for Standardised X Interfaces	15.0.0
2018-03	SA#79	SP-180035	0276	1	B	Adding of the abbreviations and Network Function Architecture for Cell site Information reporting plus Handover details	15.1.0
2018-03	SA#79	SP-180034	0283	-	A	Stage 2 Corrections to the Serving System event reported by HSS for EPS	15.1.0
2018-03	SA#79	SP-180034	0284	-	A	Stage 2 Corrections HSS Subscriber Record Change in EPS	15.1.0
2018-03	SA#79	SP-180034	0285	-	A	Stage 2 Corrections Cancel Location, Registration Termination HSS events, EPS	15.1.0
2018-03	SA#79	SP-180034	0286	-	A	Stage 2 Corrections for the Register Location event reported by for EPS	15.1.0
2018-03	SA#79	SP-180034	0287	-	A	Stage 2 Corrections Location Information Request event from HSS in EPS	15.1.0
2018-06	SA#80	SP-180290	0288	1	F	Stage 2 Corrections to the Subscriber Record Change event by HLR for CS	15.2.0
2018-06	SA#80	SP-180290	0289	1	F	Stage 2 Corrections to the Subscriber Record Change event by HLR for PS	15.2.0
2018-06	SA#80	SP-180290	0290	1	F	Stage 2 Corrections to the Subscriber Record Change event by HSS for EPS	15.2.0
2018-06	SA#80	SP-180290	0291	1	F	Errors in stage 2 text related to EPS	15.2.0
2018-06	SA#80	SP-180290	0292	1	F	Incorrect references to HSS triggered events in the SMS, MMS clauses	15.2.0
2018-06	SA#80	SP-180289	0294	1	A	Critical fix for location reporting with S8HR LI (stage 2 text)	15.2.0
2018-06	SA#80	SP-180290	0295	1	B	Interception of terminating CS calls when outbound roaming	15.2.0
2018-06	SA#80	SP-180290	0297	1	B	PTC Encryption information delivery	15.2.0
2018-06	SA#80	SP-180290	0298	1	F	PTC corrections	15.2.0
2018-09	SA#81	SP-180790	0300	1	C	Reporting Media Bearer information for S8HR	15.3.0
2018-09	SA#81	SP-180790	0301	1	C	S8HR LI: Location reporting corrections in Annex J	15.3.0

2018-12	SA#82	SP-180990	0302	3	C	Time of Location Stage 2	15.4.0
2018-12	SA#82	SP-180990	0304	1	F	PTC Stage 2 Text: Fixing few errors in the PTC clause	15.4.0

History

Document history		
V15.2.0	June 2018	Publication
V15.3.0	October 2018	Publication
V15.4.0	April 2019	Publication