ETSI TS 133 107 V12.9.0 (2015-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
3G security;
Lawful interception architecture and functions
(3GPP TS 33.107 version 12.9.0 Release 12)

Reference
RTS/TSGS-0333107vc90

Keywords
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

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

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

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

Contents

Foreword

This Technical Specification (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 specification 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 in 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 TS 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: "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] 3GPP TS 23.303: "Proximity based Services; Stage 2".

[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)".

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.

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).

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.

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 Center
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
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
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
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
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
IRI	Intercept Related Information
I-WLAN	Interworking WLAN (3GPP WLAN interworking subnetwork)
LAN	Local Area Network
LDI	Location Dependent Interception
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility

LIPA	Local IP Access
LTE	Long Term Evolution
MBMS	Multimedia Broadcast/Multicast Service
MGCF	Media Gateway Control Function
MGW	Media Gateway
ME	Mobile Entity
MIP	Mobile IP
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
RA	Routing Area
RAI	Routing Area Identity
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
TEL URI	"tel" URI, as defined in RFC 3966 [36]
TLS	Transport Layer Security
TrGW	Transit Gateway
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

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.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.

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. (eg 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 may be operated by different commercial entity than UMTS network.

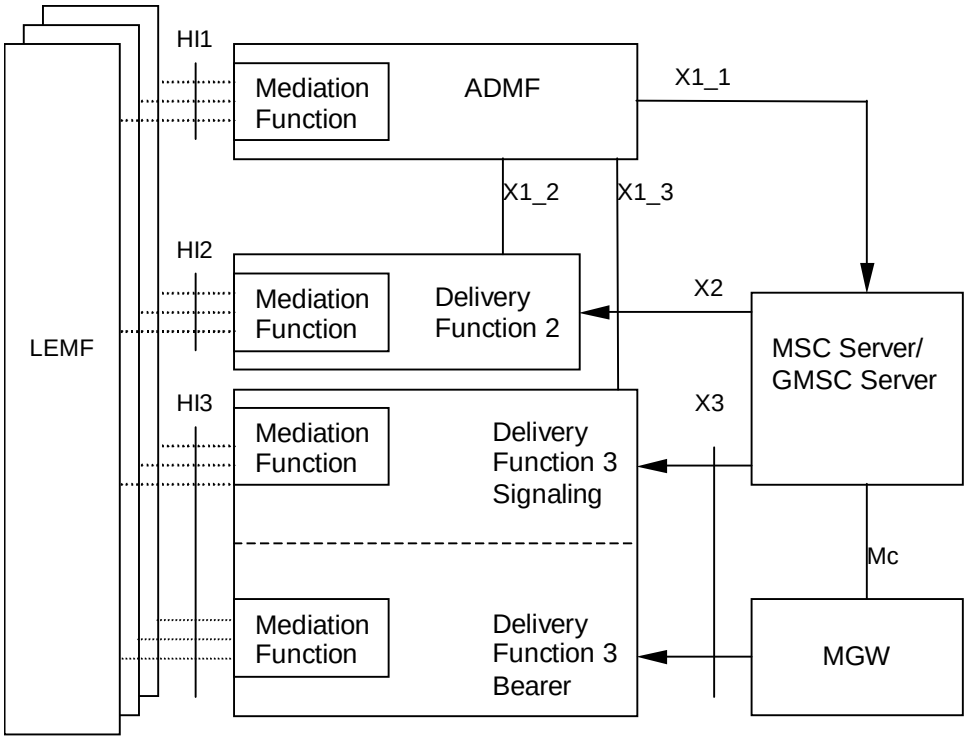


Figure 1a: Circuit switched intercept configuration

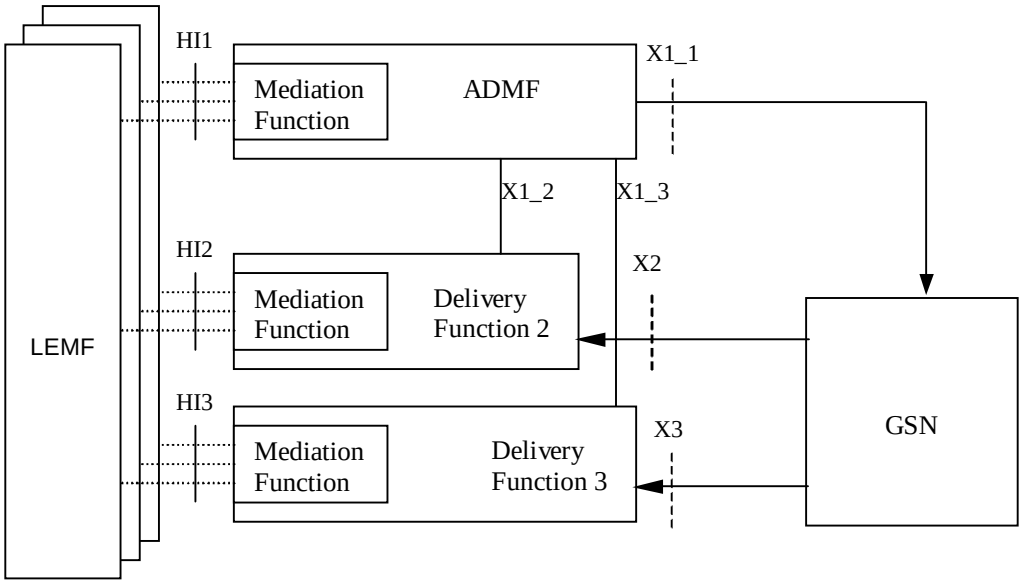


Figure 1b: Packet Switched Intercept configuration

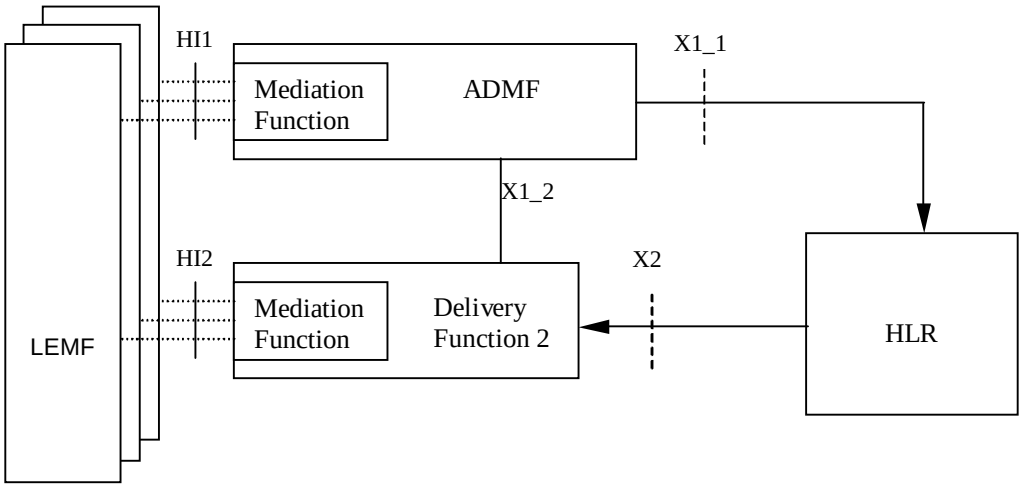


Figure 1c: HLR Intercept configuration

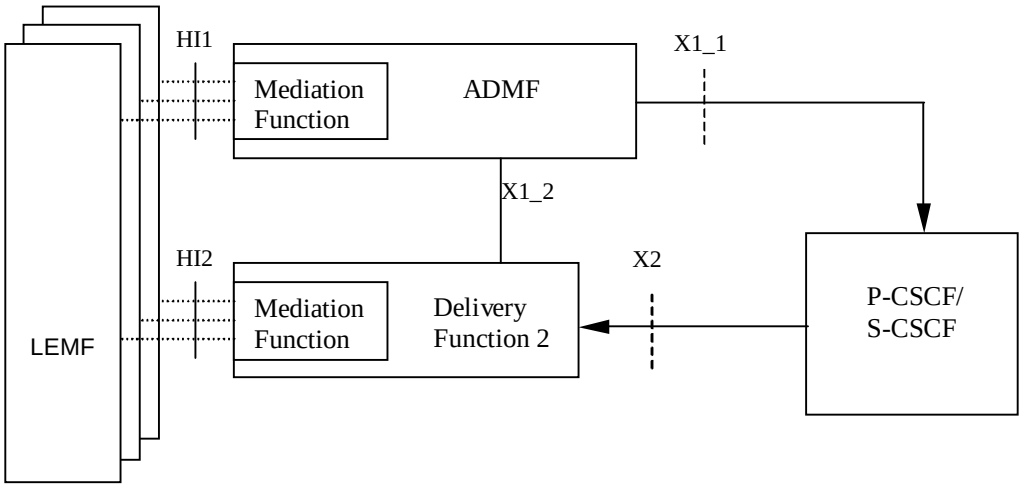


Figure 1d: IMS-CSCF Intercept configuration

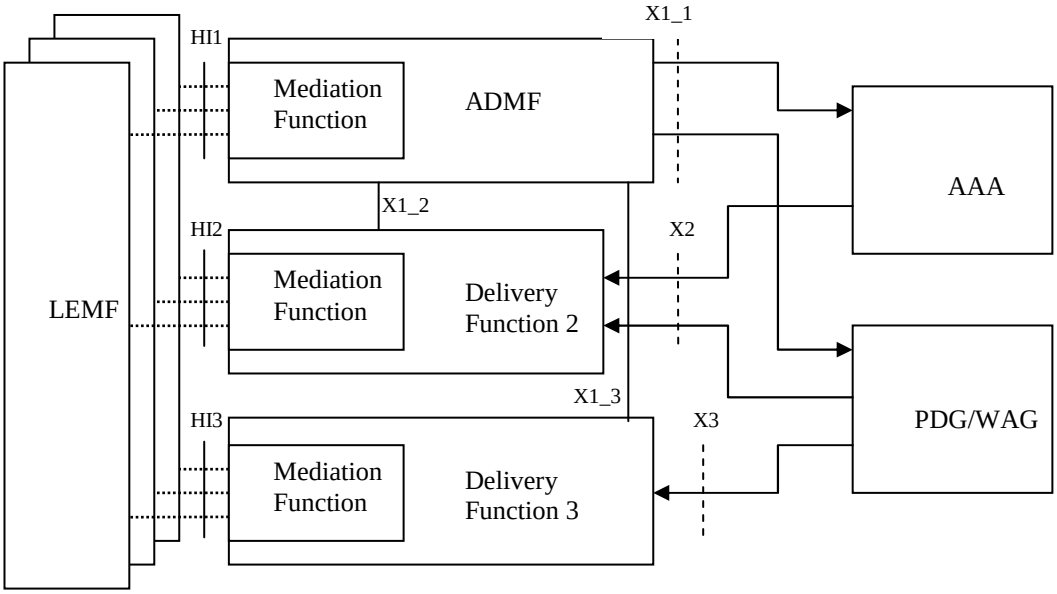


Figure 1e: WLAN Interworking Intercept configuration

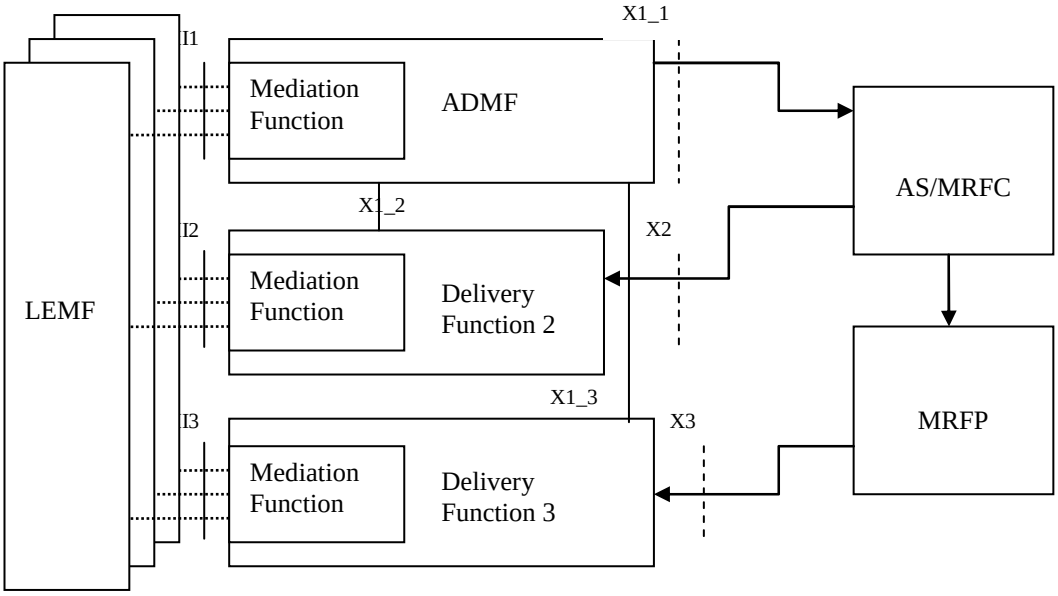


Figure 1f: IMS Conferencing Intercept configuration

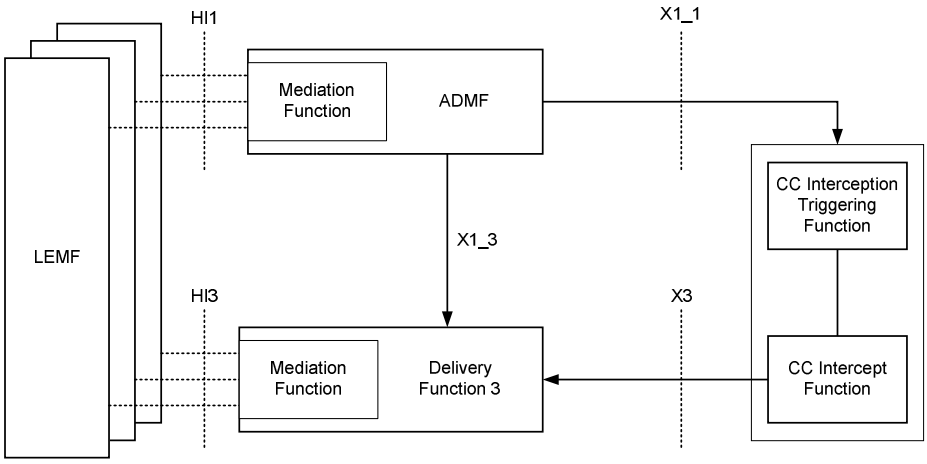


Figure 1g: VoIP CC Intercept Configuration

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 and X3 interfaces.

Interception at the Gateways is a national option. However, 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 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 and 1g, 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 and 1d 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.

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.

5 Activation, deactivation and interrogation

5.0 General

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

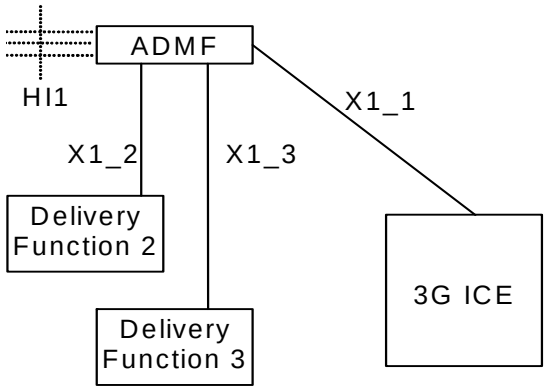


Figure 2: Functional model for Lawful Interception activation, deactivation and interrogation

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 IMEI.

NOTE 1: Some communication content during a mobility procedure may 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 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 may be a temporary ID, therefore the use of MSISDN or IMSI is recommended.

NOTE 3: Void

The target identities for 3GPP HNB interception can be IMSI, MSISDN, 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: 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: 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.

Editors' note: 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.

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.

NOTE 1: 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 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: 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: As an option, only a single DF3 is used by and known to every 3G ICE (except at the CSCFs, HLR 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: Interception at the CSCFs is based upon either 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.

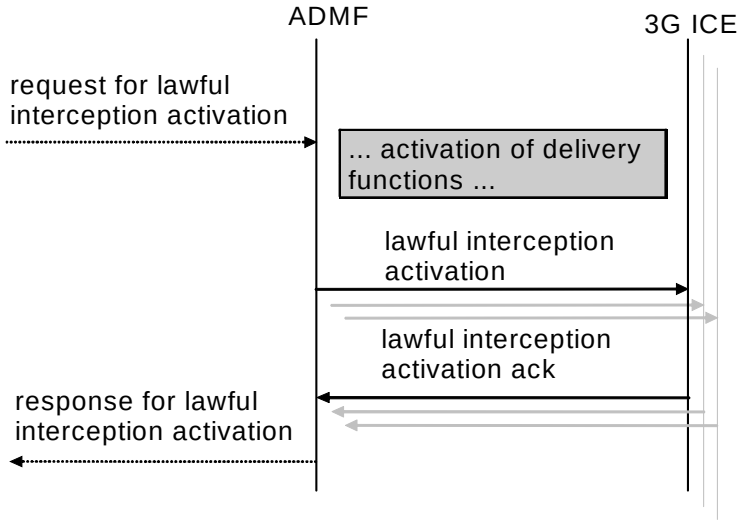


Figure 3: Information flow on X1_1-interface for Lawful Interception activation

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 for delivery of IRI (= LEMF address);
- which subset of information shall be delivered;
- 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;
- 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.

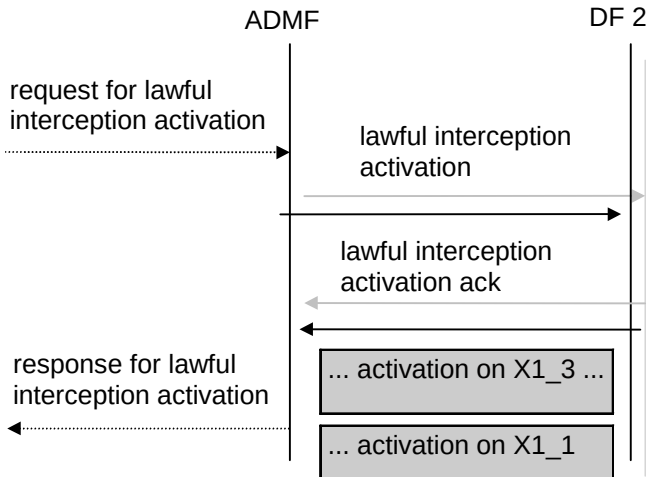


Figure 4: Information flow on X1_2-interface for Lawful Interception activation

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 of delivery for CC (= LEMF address);
- 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;
- 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.

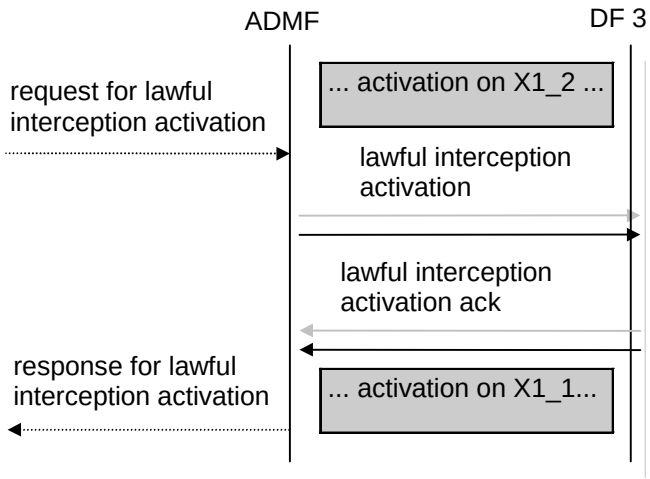


Figure 5: Information flow on X1_3-interface for Lawful Interception activation

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.

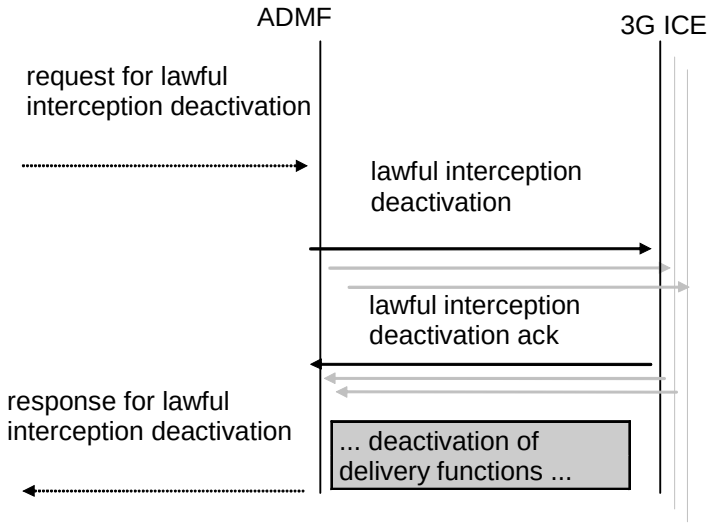


Figure 6: Information flow on X1_1-interface for Lawful Interception deactivation

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.

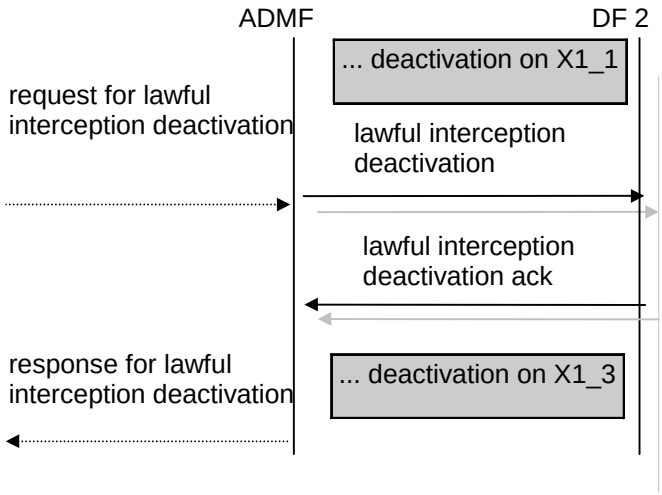


Figure 7: Information flow on X1_2-interface for Lawful Interception deactivation

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.

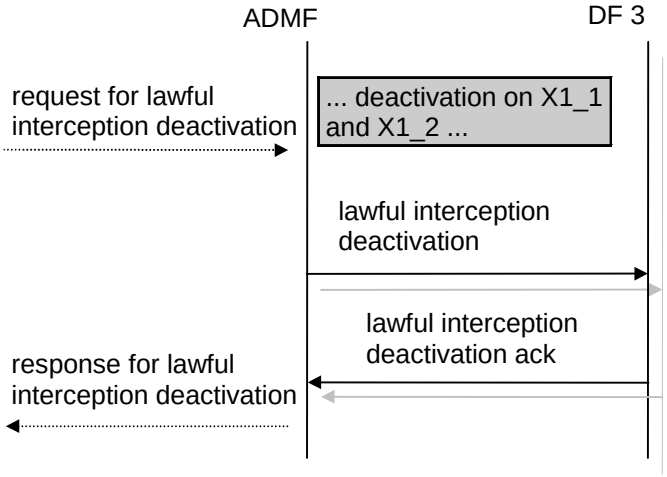


Figure 8: Information flow on X1_3-interface for Lawful Interception deactivation

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.

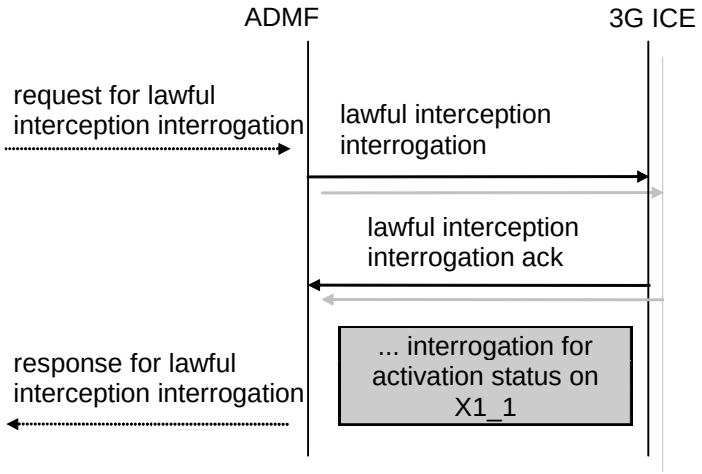


Figure 9: Interrogation of the Lawful Interception (3G ICEs)

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.

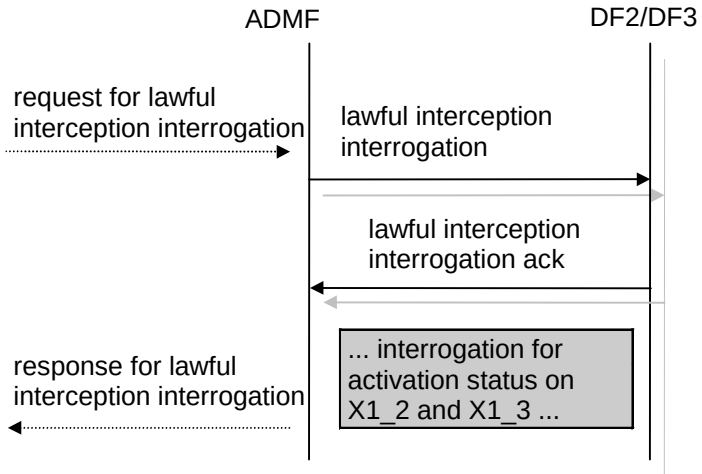


Figure 10: Interrogation of the Lawful Interception (Delivery Functions)

6 Invocation of Lawful Interception for Circuit Switched 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.

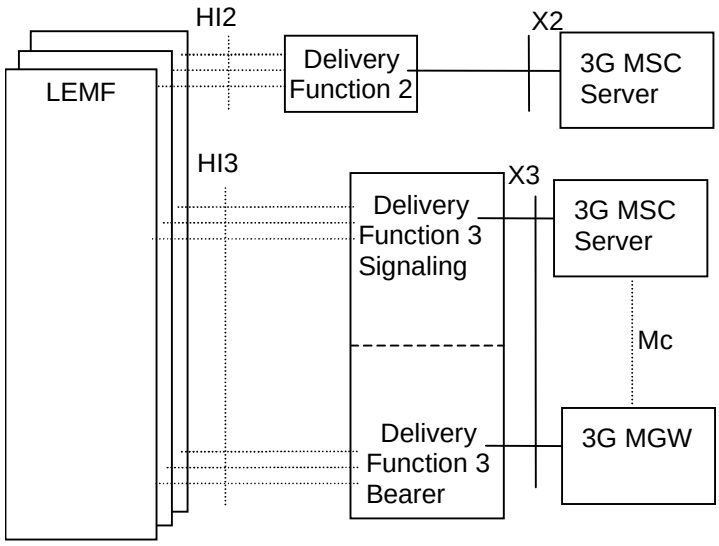


Figure 11: Functional model for Lawful Interception invocation

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 communicationsto 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: 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.

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.

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.

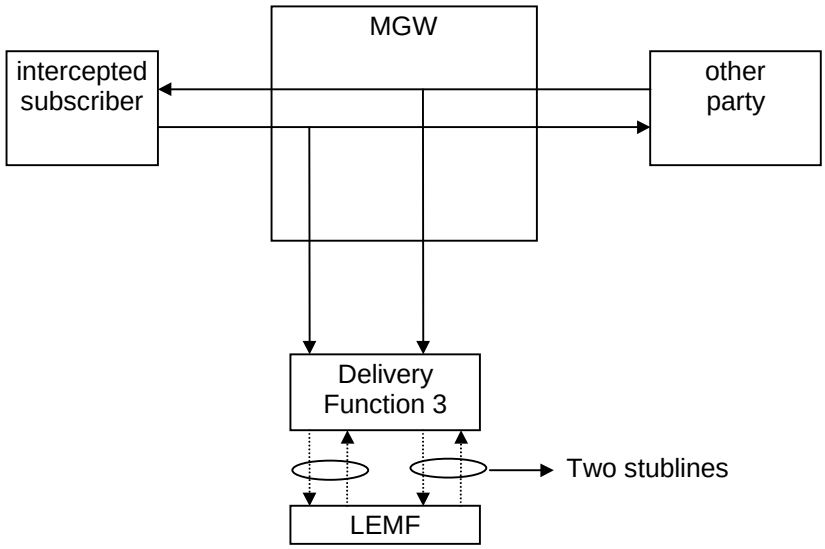


Figure 12: Delivery configuration to the LEMF for the interception of a circuit switched call

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: 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, IMSI or IMEI); note 2
- the target location (if available) or the IAs in case of location dependent interception. note 2
- correlation number (IRI <-> CC);
- direction indication - (Signal from target or signal to target).

NOTE 2: For DF3 internal use only.

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 either when the 3G MSC receives the SMS from the target MS, or when the 3G MSC receives notification that the SMS-Centre successfully received the SMS;

- for a SMS-MT. Dependent on national requirements, delivery shall occur either when the 3G MSC receives the SMS from the SMSC, or when the 3G MSC receives notification that the target MS successfully received the SMS.

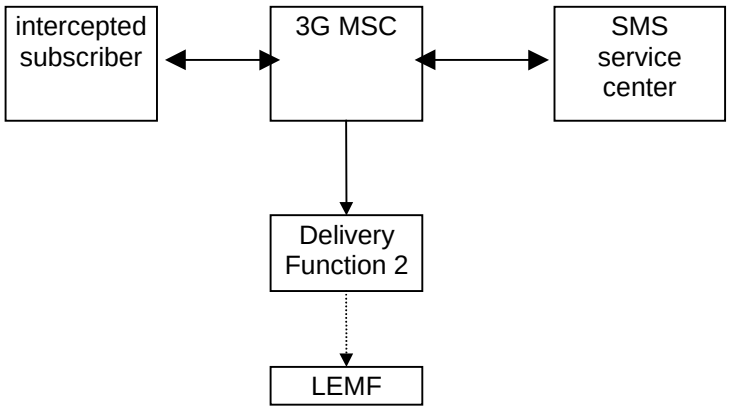


Figure 14: Provision of Content of Communication - Short Message Service

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.

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.

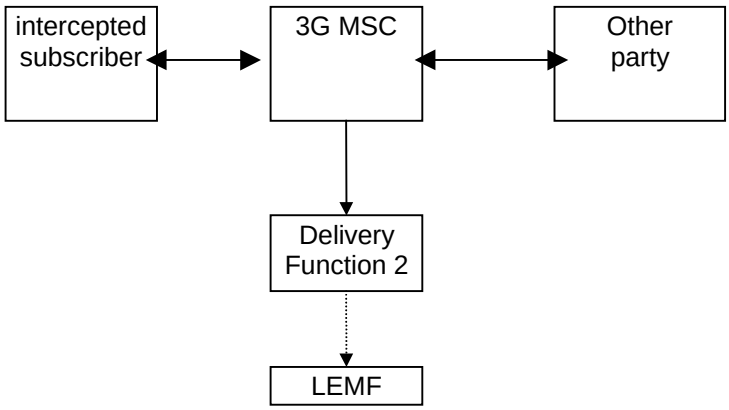


Figure 15: Provision of Intercept Related Information

6.3.1 X2-interface

The following information needs to be transferred from the 3G MSC Server 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 up to eight different call related and non-call related events. Details are described in following clause. The events for interception are configurable (if they are sent to DF2) in the 3G MSC Server and can be suppressed in the DF2. The events are listed as follows:

Call Related Events:

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

Non Call Related Events:

- SMS
- Location Update
- Subscriber Controlled Input

Table 1 below shows the set of information that can be associated with the events. The events trigger the transmission of the information from the 3G MSC Server to DF2. Available IEs from this set of information can be extended in the 3G MSC Server, 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
event type Description which type of event is delivered: Establishment, Answer, Supplementary service, Handover, Release, SMS, Location update, Subscriber controlled input
event date Date of the event generation in the 3G MSC Server
event time Time of the event generation in the 3G MSC Server
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/ terminating In or/out
Correlation number Unique number for each call sent to the DF, to help the LEA, to have a correlation between each Call 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 Server at the time of event record production. In some traffic cases the available location information can be the one received from the MME, i.e. the Tracking Area Identity (TAI) and/or the E-UTRAN Cell Global Identification (ECGI) as specified in the 3GPP TS 23.272 [30].
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

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
event type
event date
event time
dialled number
other party address
call direction
Correlation number
Redirecting number
Network Element Identifier
Location Information
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
event type
event date
event time
dialled number
other party address
Connected party
call direction
Correlation number
Redirecting number
Network Element Identifier
Location Information
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
event type
event date
event time
dialled number
other party address
call direction
Correlation number
Network Element Identifier
Location Information
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

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
event type
event date
event time
dialled number
other party address
call direction
Correlation number
Network Element Identifier
Location Information
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 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 successfully received the message. 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
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

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
SCI

6.4 Intercept cases for circuit switched supplementary services

6.4.1 Interception of Multiparty call

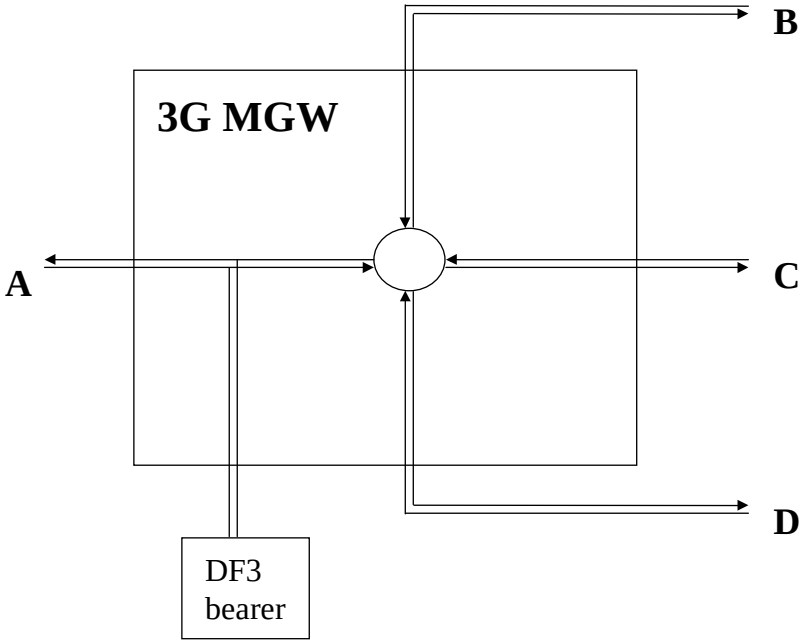


Figure 16: Interception of Multiparty for CC

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

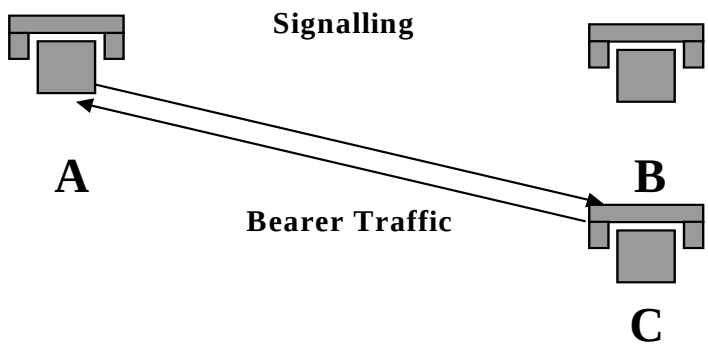


Figure 17: Interception for Call Forwarding / Deflection / ECT

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.

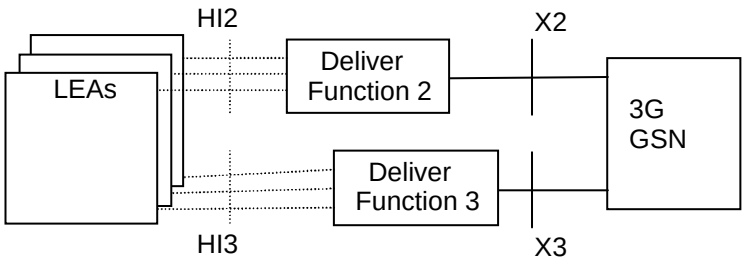


Figure 18: Functional model for Packet Data GSN Network Lawful Interception invocation

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 ([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 ([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: If interception has been activated for both parties of the Packet Data communication both CC and IRI will 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: 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.

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.

The IRI will be delivered to the LEA:

- for a SMS-MO. Dependent on national requirements, delivery shall occur either when the 3G SGSN receives the SMS from the target MS or when the 3G SGSN receives notification that the SMS-Centre successfully received the SMS;

- for a SMS-MT. Dependent on national requirements, delivery shall occur either when the 3G SGSN receives the SMS from the SMS-Centre or when the 3G SGSN receives notification that the target MS successfully received the SMS.

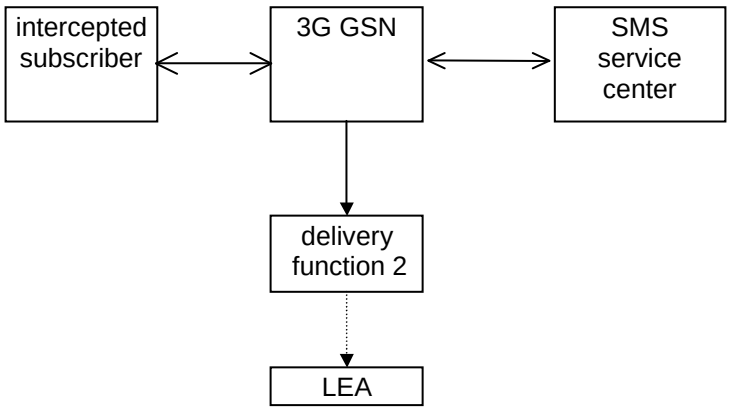


Figure 19: Provision of Intercept Product - Short Message Service

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.

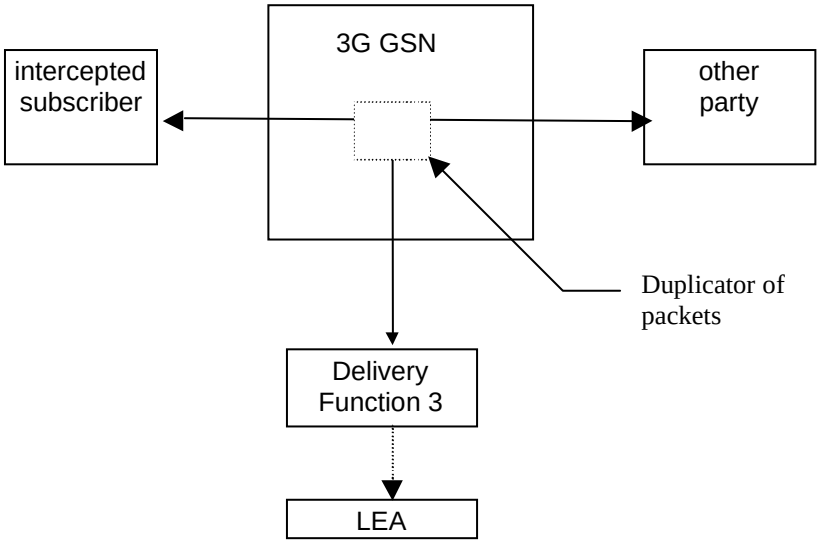


Figure 20: Configuration for interception of Packet Data GSN product data

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.

As a national option, in the case where the 3G GGSN is performing interception of the content of communications, the intercept subject 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 Header Information Reporting, and SMS events.

Serving System event reporting is a national option

Packet 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 or the Home Location Register (HLR) sends the relevant data to the DF2. For Packet 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.

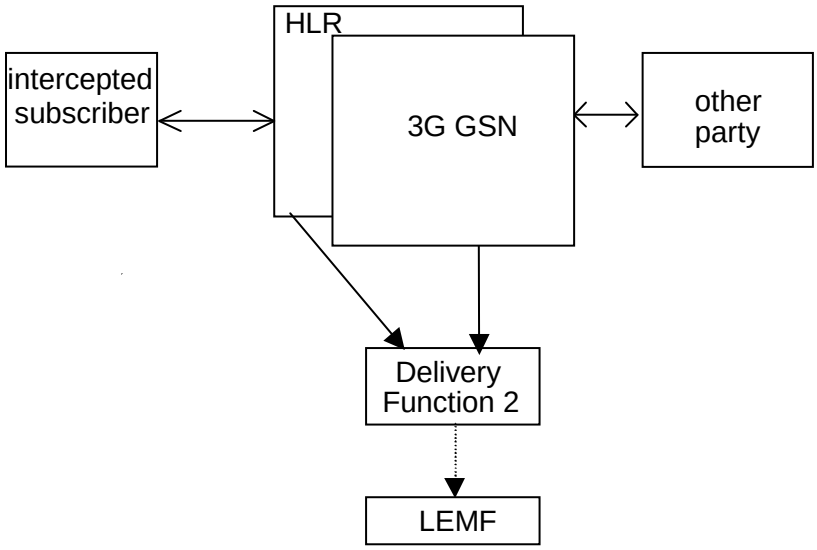


Figure 21: Provision of Intercept Related Information

7.3.1 X2-interface

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

- target identity (MSISDN, 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;

- 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 header information in the communications path but the information needed for Packet 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 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 Header Information Reporting.

NOTE: 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 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 ([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 Header Information Reporting.

The following events are applicable to the HLR:

- Serving System.

A set of elements as shown below can be associated with the events. The events trigger the transmission of the information from 3G GSN or HLR to DF2, perhaps via a MF in the case of Packet Header Information Reporting. 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 Events 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.
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.
Event date Date of the event generation in the 3G GSN or the HLR.
Event time Time of the event generation in the 3G GSN or the HLR. 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 at the time of event record production.
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.
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 3GPP 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.

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
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
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
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
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
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)
Old Location Information (only for the old SGSN)
IAs (if applicable)

NOTE: Once target moves out of the interception area, old SGSN may report the RAU event. Normally, however, 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 MO-SMS the event is generated in the 3G SGSN. Dependent on national requirements, event generation shall occur either when the 3G SGSN receives the SMS from the target MS or when the 3G SGSN receives notification that the SMS-Centre successfully receives the SMS; for MT-SMS the event is generated in the 3G SGSN. Dependent on national requirements, event generation shall occur either when the 3G SGSN receives the SMS from the SMS-Centre or when the 3G SGSN receives notification that the target MS successfully received the message. 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
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
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 intercept subject 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
IAs (if applicable)

7.4.11 Packet Header Information Reporting

7.4.11.0 Introduction

Packet 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 subject 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.

7.5 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 [25] IMS Media Plane Security options. If an ICE, in TSP IMS network using Security options [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. 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. 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.

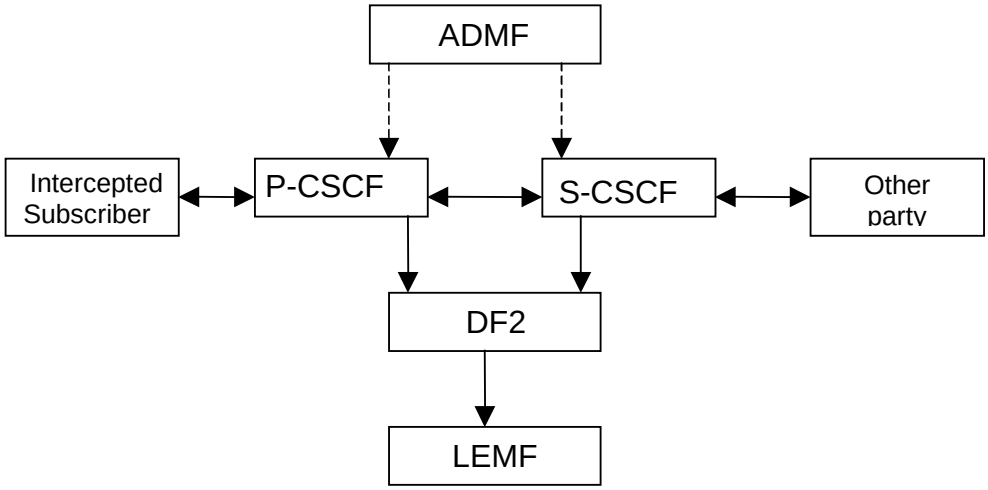


Figure 22: Provision of Intercept Related Information for multi-media

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 3GPP 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: 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: Report of events related to target"s XCAP data and resources access by non XCAP protocol are for further studies.

7A.3 Multi-media events

7A.3.0 General

- All SIP messages to or from a targeted subscriber, and all SIP messages executed on behalf of a targeted subscriber 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 (eg IMPI/IMPU changes or due to call forwarding etc) and the new identity is the subject of interception, 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 (eg IMPI/IMPU changes or due to call forwarding etc) and the new identity is not the subject of interception, 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.

- 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

  - Event Time and Date

  - Network element identifier

  - SIP Message Header

  - SIP Message Payload

NOTE: The Observed IMEI is obtained from the +sip.instance.id of the intercepted SIP message (as defined in 3GPP TS 24.229 [49]).- All IMS XCAP messages to or from a targeted subscriber 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.

Editor"s note: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 (3GPP TS 24 141, OMA Presence SIMPLE specification and IETF RFC 4827), have to be reported through the DF2. However, these are points for further studies: 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: The interpretation of XCAP messages, such as HTTP request through the Ut interface between the targets"s UE and related XCAP server may sometime be insufficient to let the LEA to understand what was modified as directed by the UE a later HTTP response is needed to understand the success or failure of the request.

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

NOTE: 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.

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 done according the definitions in clause 7A.3. Interception of CC is available with the current implementations in the GSNs.

7A.6 SMS over IMS

SMS over IMS shall be intercepted in accordance with normal IMS interception as described in 7A.3. 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 [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.

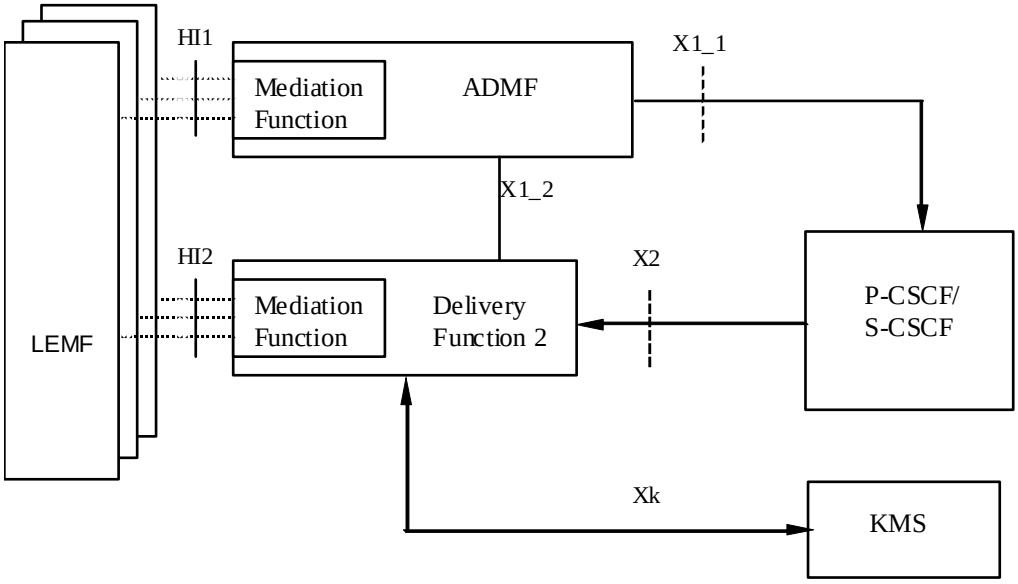


Figure 7A.7.1: KMS Intercept configuration

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 signaling 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 [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 [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.

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, 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 Server, 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, CSCF 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, 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. 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, 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 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 Server, 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 shall be capable of performing a periodic consistency check to ensure that the target list of target identities in all involved 3G MSC Servers, 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 for 3GPP WLAN Interworking Services

9.0 General

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.

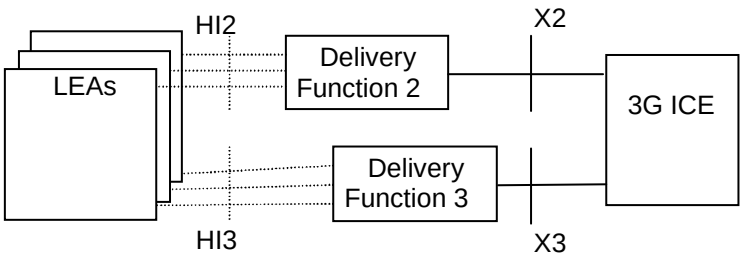


Figure 23: Functional model for invocation of Lawful Interception for 3GPP WLAN Interworking Services

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.

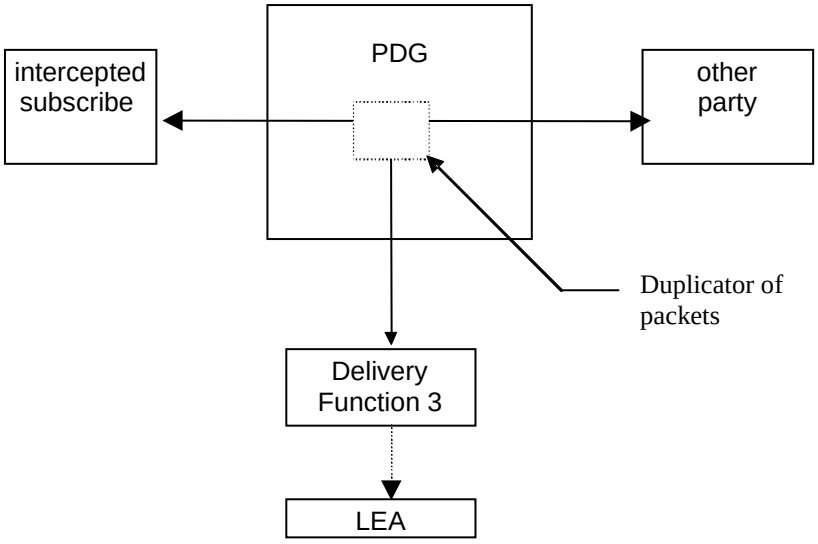


Figure 24: Configuration for interception of 3GPP WLAN Interworking product data

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 Header Information Reporting is a national option. For Packet 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.

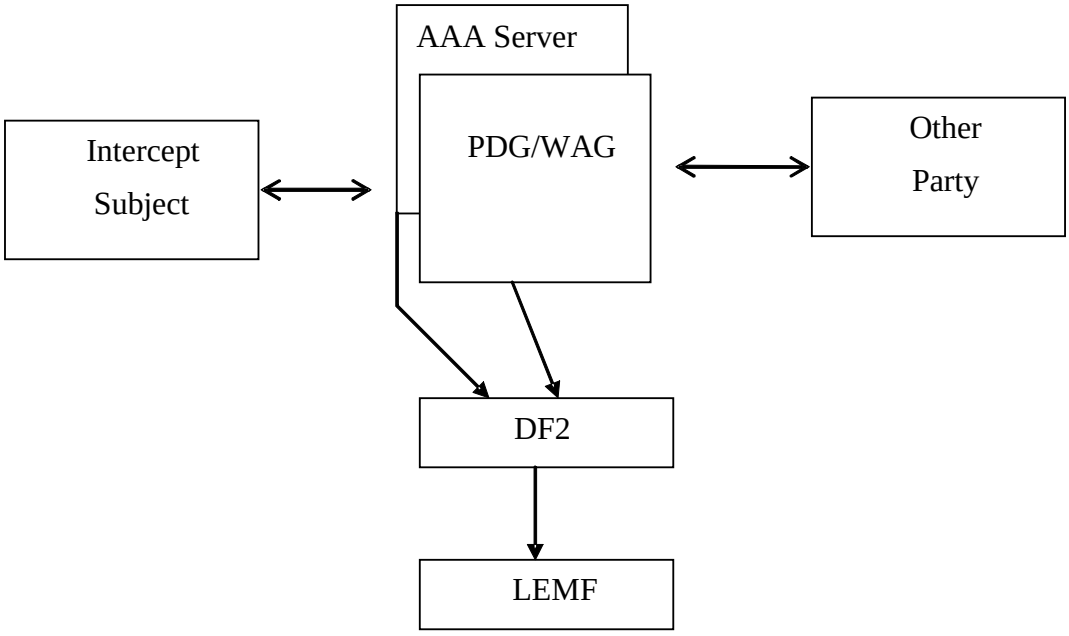


Figure 25: Provision of Intercept Related Information

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 header information in the communications path but the information needed for Packet 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 Header Information Reporting.

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: 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 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	Available, see TS 29.234
Observed NAI NAI of the target.	Not available	Available, see TS 29.234
Observed IMSI IMSI of the target.	Available, see TS 24.234	Available, see TS 29.234
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 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 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
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, 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	Not available
WLAN Access Point Name The W-APN of the access point.	Available, see TS 24.234	Available, see TS 29.234
WLAN Operator Name The name of the WLAN operator name serving the target.	Not available	Available, see TS 29.234
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
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
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

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
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
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
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 23.234 Annex F; defined 29.060 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 3GPP TS 29.234
Observed IMSI IMSI of the target.	Available, see 3GPP TS 29.234
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 addess of observed party. The WLAN UE IP address field contains the IPv4/IPv6 address (specified by 3GPP TS 29.234) of the WLAN UE tunnel endpoint as seen by the WAG. Note that this address might be dynamic.	Available, see 3GPP TS 29.234
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 3GPP TS 29.234) as seen by the WAG. Note that this address might be dynamic.	Available, see 3GPP TS 29.234
WLAN Access Point Name The W-APN of the access point.	Available, see 3GPP TS 29.234
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 3GPP TS 29.234
Tunnel Protocol The Tunnel Protocol as defined in the Routing-Policy AVP in 3GPP TS 29.234.	Available, see 3GPP TS 29.234
Source Ports The list or range of source ports as specified in the Routing-Policy AVP provided by the AAA server in 3GPP TS 29.234.	Available, see 3GPP TS 29.234
Destination Ports The list or range of destination ports as specified in the Routing-Policy AVP provided by the AAA server in 3GPP TS 29.234.	Available, see 3GPP TS 29.234
Session Alive Time The amount of time in seconds during which the target can be registered for WLAN access.	Available, see 3GPP TS 29.234
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	Available from ICE

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)	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 Header Information Reporting

9.4.6.0 Introduction

Packet 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 Header Information Reporting - 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 Header Information Reporting – 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 subject 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 Header Summary Reporting - 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 Header Summary Reporting – 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.

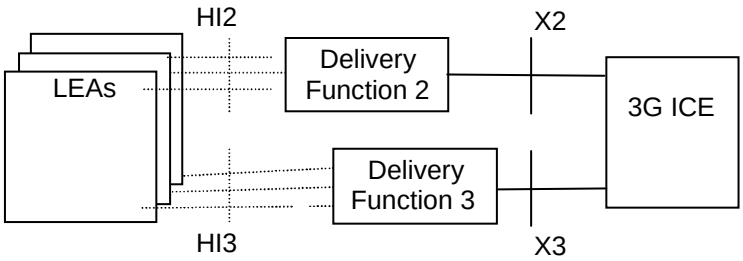


Figure 10.1: Functional model for invocation of Lawful Interception for MBMS Services

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.

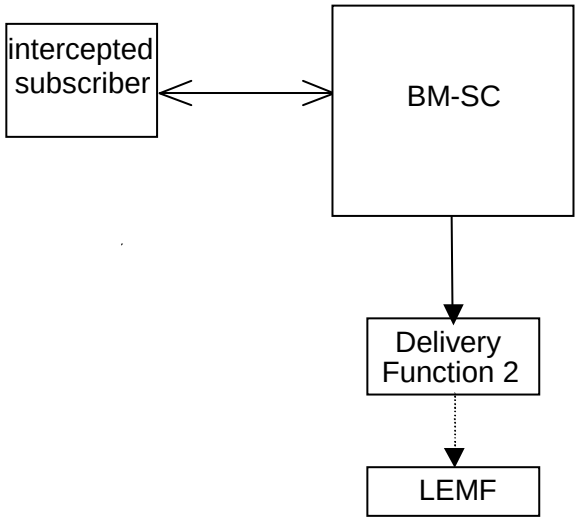


Figure 10.2: Provision of Intercept Related Information

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 subject of interception. This may be where the intercept subject 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 intercept subject.

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 intercept subject 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.

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: 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 could be passed over the X3 interface (Y conferees means 1 content stream). With the separated delivery approach, each conferee"s connection to the conference would need to be intercepted and passed over the X3 interface (Y conferees, means Y pairs of bi-directional content streams).

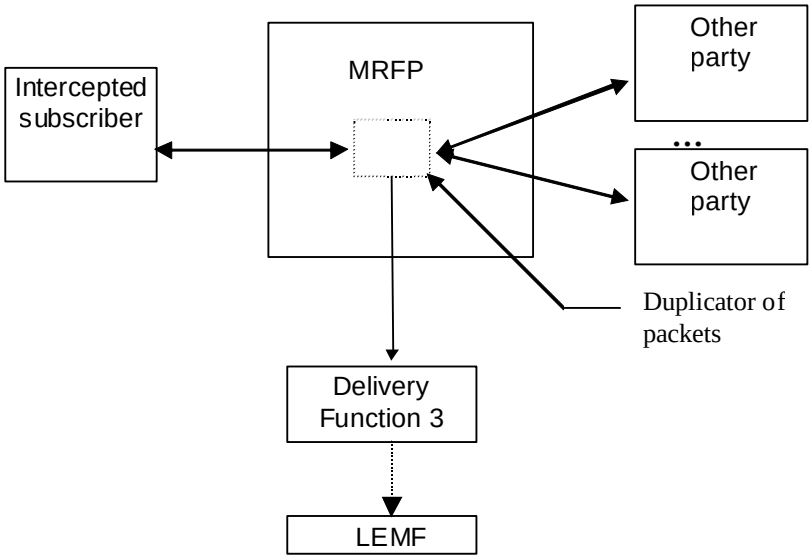


Figure 11.1: Configuration for interception of IMS Conference Services CC

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: Information passed between the MRFC and MRFP for correlation has to 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 may 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.

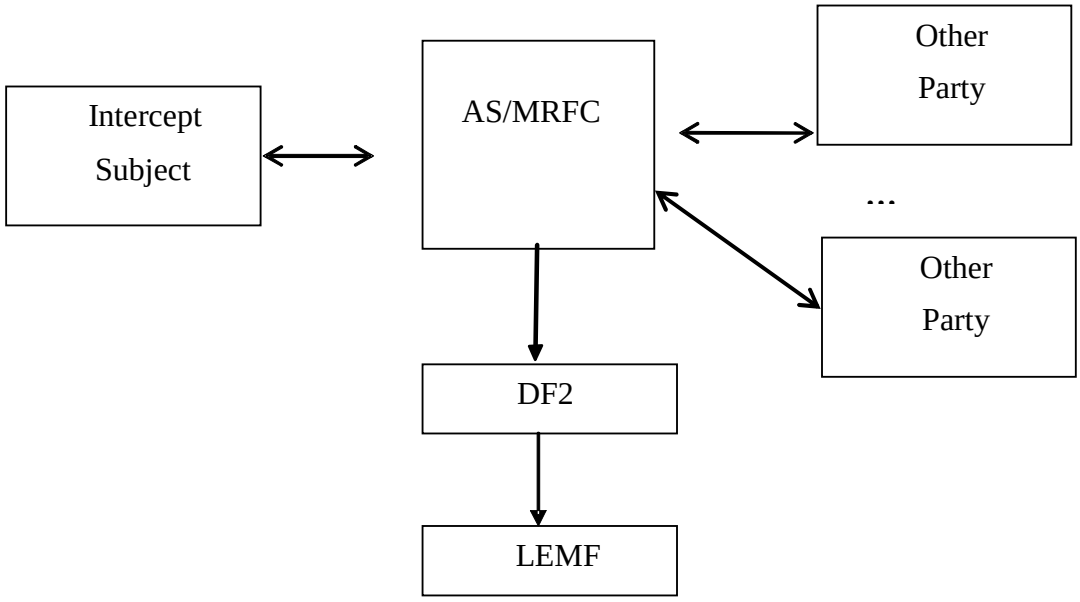


Figure 11.2: Provision of Intercept Related Information for IMS Conferencing

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.).

Editor"s Note: We should consider whether H.248 Context Identifier should be added to help correlate CII and CC

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 onference 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 ([22], [23]):

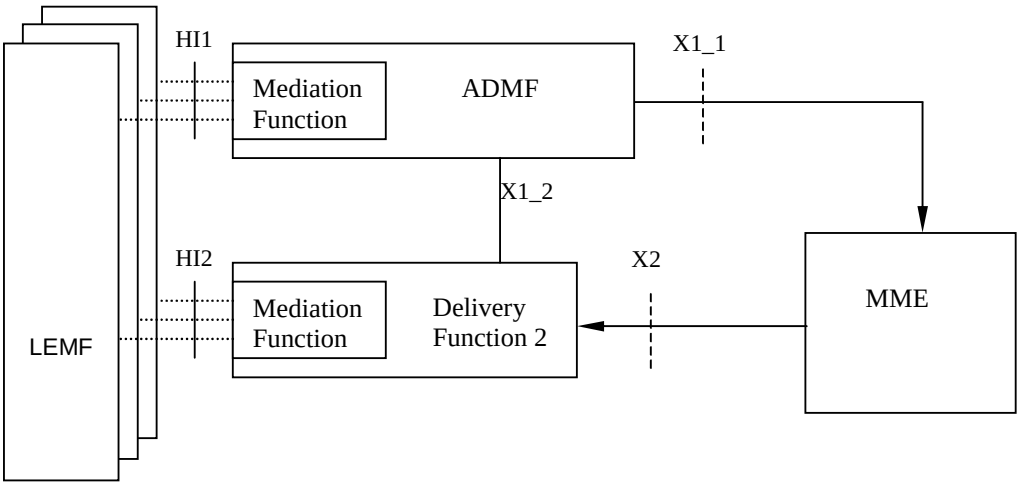


Figure 12.1.1: MME Intercept configuration

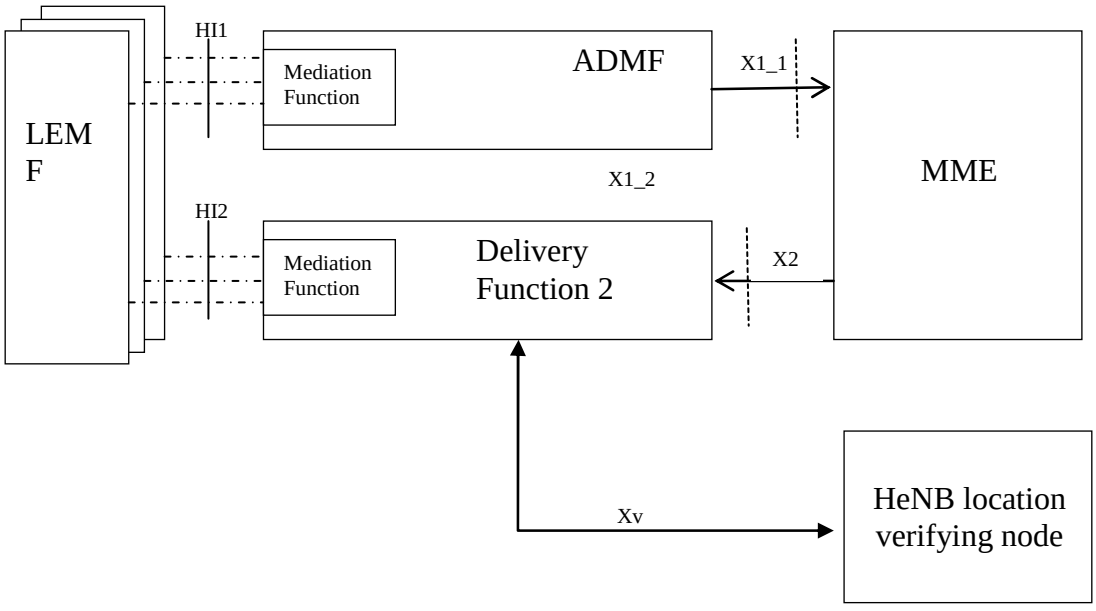


Figure 12.1.1a: Configuration for Intercept of HeNB

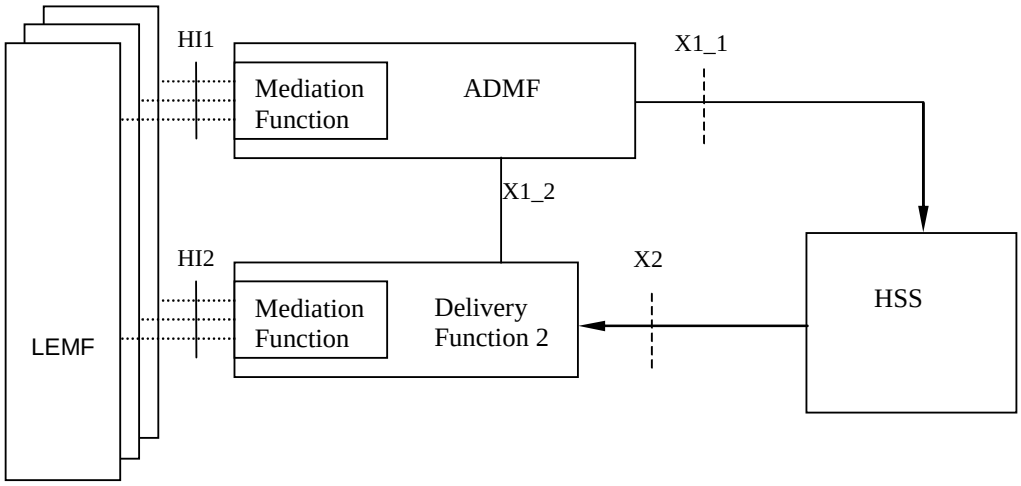


Figure 12.1.2: HSS Intercept configuration

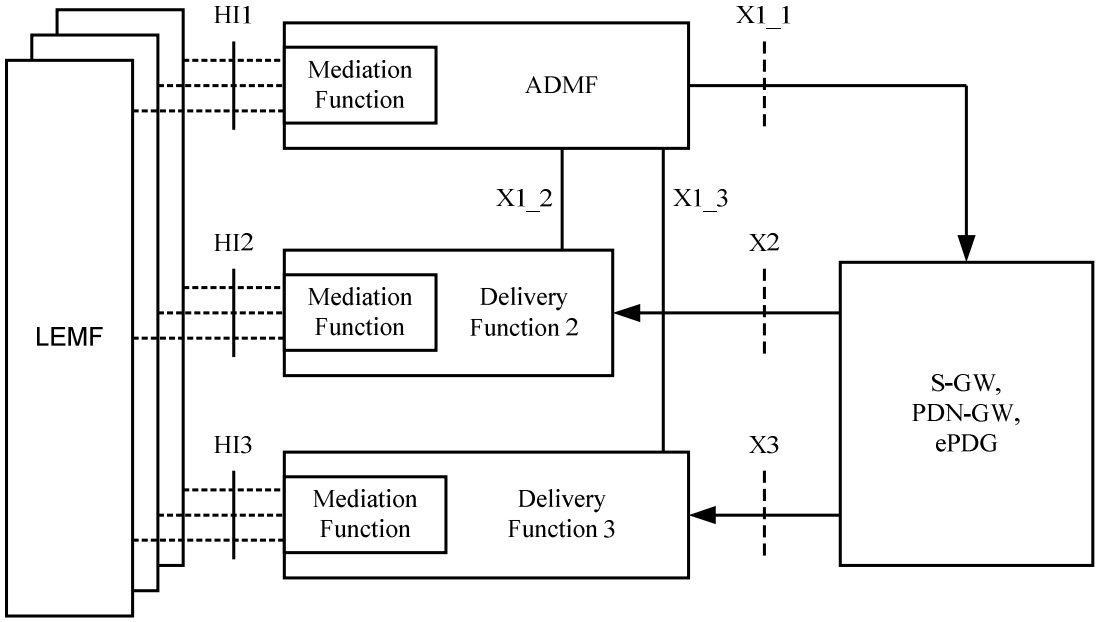


Figure 12.1.3: S-GW, PDN-GW, ePDG Intercept configuration

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 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.

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 X.

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 and PDN-GW are IMSI, MSISDN and ME (Mobile Equipment) Identity.

NOTE 1: 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 [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: If interception has been activated for both parties of the Packet Data communication both CC and IRI will be delivered for each party as separate intercept activity.

Location Dependent Interception for EPC is FFS.

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 Update, 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 event reporting is a national option.

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 clause 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;
- 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 [22].

The following events are applicable to the MME:

- Attach;
- Detach;
- Tracking Area 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.

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 Header Information Reporting shall also be performed at the PDN GW and not at the Serving GW.

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.
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.
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 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.
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.

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 3GPP 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.

Editor"s note: Identification of which HeNB IP Address is reported is needed.

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.

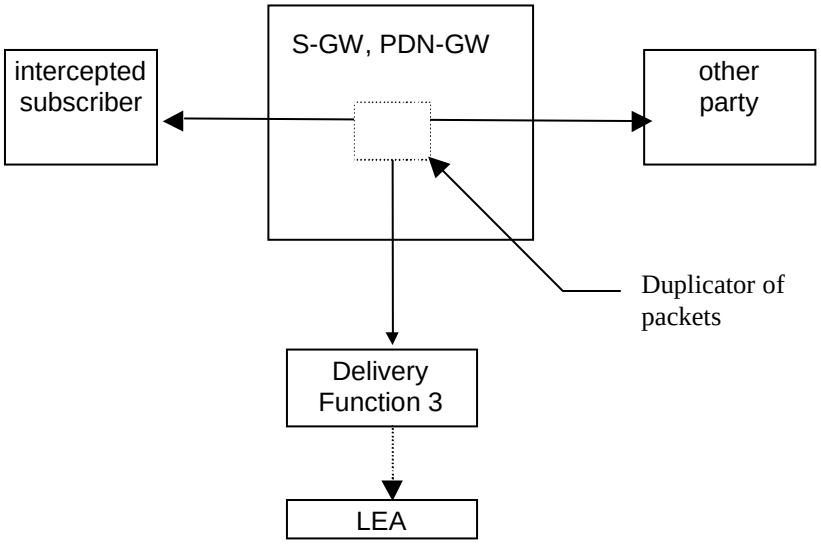


Figure 12.2.2.1: Configuration for interception of S-GW/PDN-GW product data

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.

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
Location Information
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
Location Information
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
Location Information
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

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.

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
Location Information
IAs (if applicable)
EPS bearer id
Initiator
Procedure Transaction Identifier
Bearer deactivation Cause (note)
ULI 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
Location Information
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

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 Update

For each TA update an update-event with the elements about the new location is generated. 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
Event Type
Event Time
Event Date
Network Element Identifier
Location Information (only for the new MME)
Old Location Information (only for the old MME)
IAs (if applicable)
Failure reason
HeNB Identity*
HeNB IP Address*
HeNB Location*

* These elements are applicable for HeNB interception only.

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 intercept subject has roamed. The elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME
Event Type
Event Time
Event Date
Network Element Identifier
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 ([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
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
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 ([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
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
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 [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
Event Type
Event Time
Event Date
Network Element Identifier
Location Information
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
Location Information
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 Header Information Reporting

12.2.3.14.0 Introduction

Packet 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
Location Information
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 subject 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
Location Information
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.

12.3 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 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 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: If interception has been activated for both parties of the Packet Data communication both CC and IRI will 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.

Serving Evolved Packet System 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)
- 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 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.

12.3.1.2 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 and can be suppressed in the DF2. The network procedures for which the events are generated are defined in [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.
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.
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, location information of the target.
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.

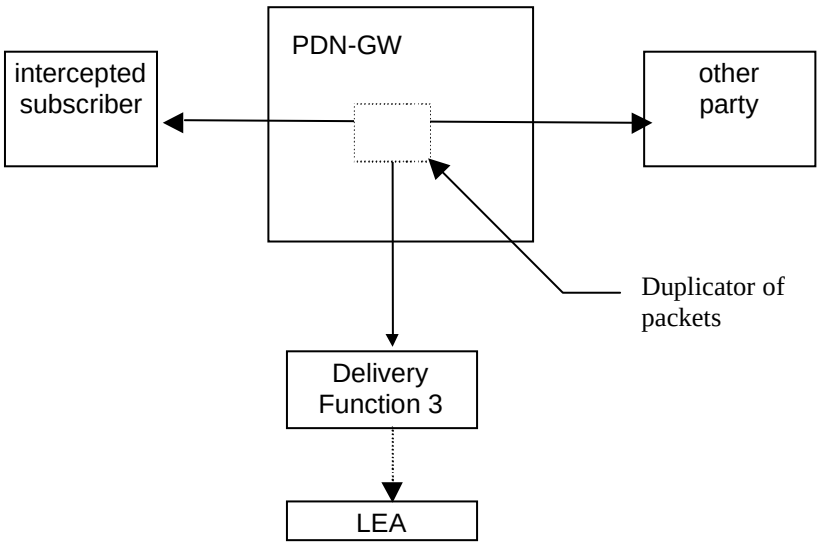


Figure 12.3.2.1: Configuration for interception of PDN-GW product data

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.

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
Lifetime
Failed attach reason
Access Technology Type
Handover Indicator
APN
UE Address Info
Additional Parameters
Serving Network
DHCPv4 Address Allocation Indication
Location information

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
Correlation number
APN
Additional Parameters
Failed reason
Location information

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 then 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
Correlation number
PDN Address(es)
Revocation trigger
Location information

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
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Failed reason
Serving Network
Handover indicator
DHCPv4 Address Allocation Indication
Location information

12.3.3.7 Packet Header Information Reporting

12.3.3.7.0 Introduction

Packet 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
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Serving Network
Handover indicator
DHCPv4 Address Allocation Indication
Location information
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 subject 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
Correlation number
Lifetime
UE Address Info
Access Technology Type
Additional Parameters
Serving Network
Handover indicator
DHCPv4 Address Allocation Indication
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)
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.

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: 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: If interception has been activated for both parties of the Packet Data communication both CC and IRI will 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)
- 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 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 3GPP TS 23.402 [23].

The following event is applicable to the HSS:

- Serving Evolved Packet System.

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 Header Information Reporting shall also be performed at the PDN GW and not at the Serving GW.

Observed MN NAI The Network Access Identifier of the Mobile Node (target identity).
Observed IMSI The IMSI 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, 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, 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.
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 [24]
Location Information Location information of the target, e.g. 3GPP2-BSID [26]. Provided if available from the PCRF.
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.

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.

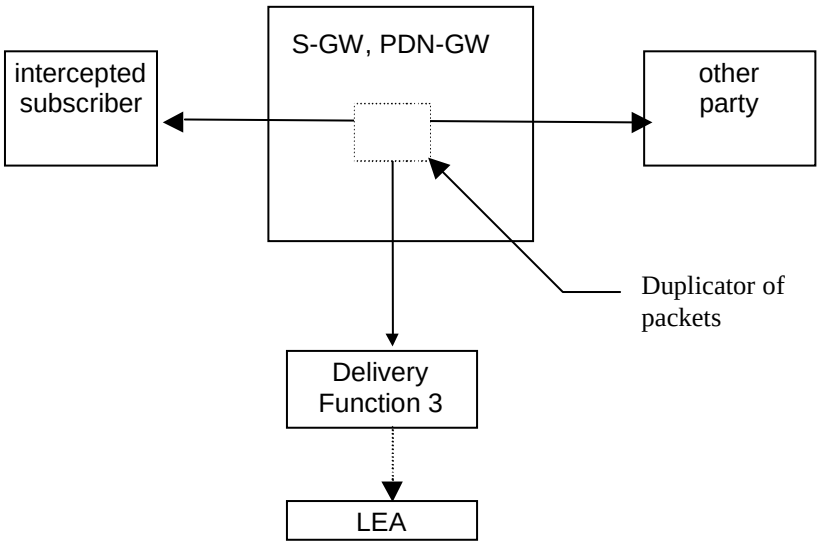


Figure 12.4.2.1: Configuration for interception of S-GW/PDN-GW product data

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.

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
Lifetime
Failed attach reason
Access Technology Type
Handover Indicator
APN
UE Address Info
Additional Parameters
Location Information

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
Lifetime
Failed attach reason
Home Address
Care of Address
Home Agent Address
APN

NOTE: 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
Lifetime
Requested IPv6 home prefix
IHome 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
APN
Initiator
Location Information

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
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
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
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
Revocation trigger
UE address info
Correlation number
Location Information

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
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 intercept subject has roamed. The elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Identity
Event Type
Event Time
Event Date
Network Element Identifier
Visited Network Identifier

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
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

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
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 Header Information Reporting

12.4.3.17.0 Introduction

Packet 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
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)
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 subject 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
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 Functional requirements for LI in case of untrusted non-3GPP IP access

12.5.0 Introduction

This section specifies functional requirements applicable to the PDN-GW and HSS. In addition, this section specifies requirements applicable to the ePDG in case this node is using a GTPv2 based protocol over s2b interface as specified in 3GPP 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.

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: 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.

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.

Serving Evolved Packet System reporting is a national option.

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)
- 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 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 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 is applicable to the HSS:

- Serving Evolved Packet System

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.

Observed MN NAI The Network Access Identifier of the Mobile Node (target identity).
Observed IMSI The IMSI of 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.
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.
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 [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.

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.

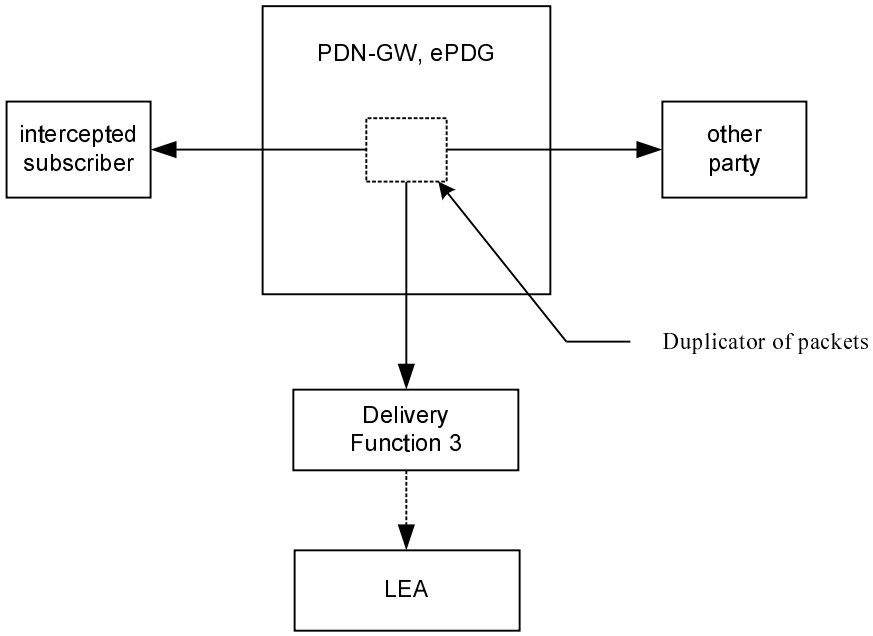


Figure 12.5.2.1: Configuration for interception of PDN-GW, ePDG product data

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.

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.

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
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.

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
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.

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
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
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 intercept subject has roamed. The elements will be delivered to the DF2 if available:

Observed MSISDN
Observed IMSI
Observed ME Identity
Event Type
Event Time
Event Date
Network Element Identifier
Visited Network Identifier

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
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
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.

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
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.

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
Lifetime
Session failure modification reason
Home address
Care of Address
APN
Requested IPv6 Home Prefix

12.5.3.11 Packet Header Information Reporting

12.5.3.11.0 General

Packet 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
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 subject 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
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.

12.6 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 [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 [10] and [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.

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);
- 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.

13.3 3GPP 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.
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

Editor"s note: Identification of which HNB IP Address is reported is needed.

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.

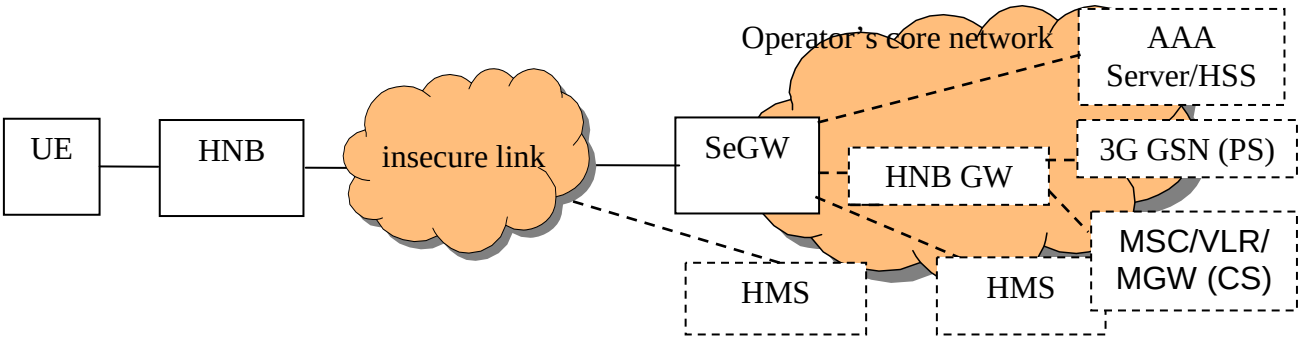


Figure 13-1: 3GPP UMTS HNB Architecture Basis for Lawful Interception

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.

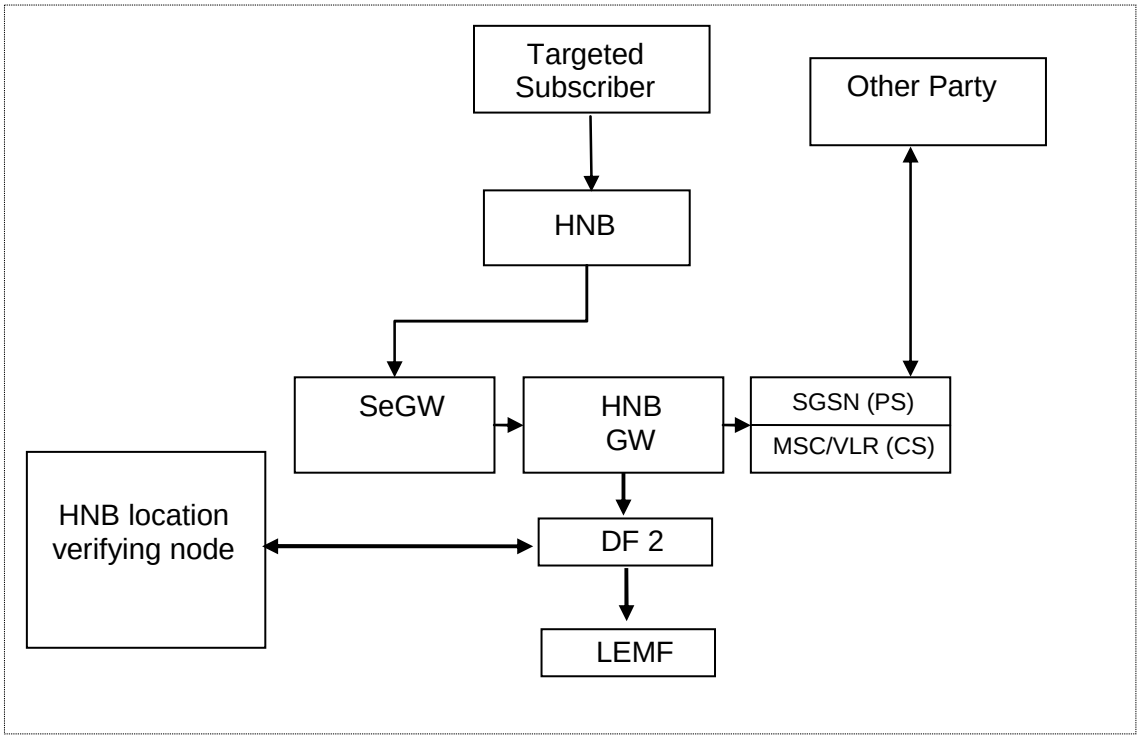


Figure 13-2: Provision of Intercept Related Information for 3GPP UMTS HNB

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);
- 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 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 1: 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
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
IAs (if applicable)

Note 1: 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.

The reporting of a soft handover between HNBs that are directly connected and the HNB GW is not involved is FFS.

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.

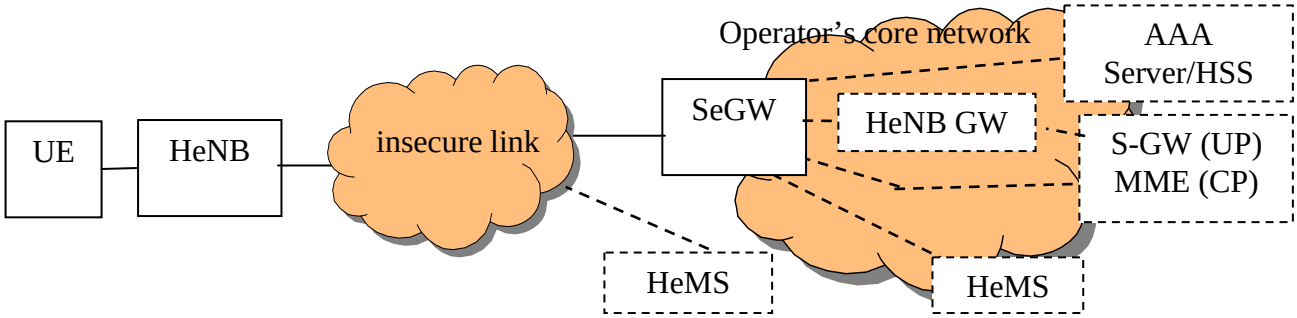


Figure 13-3: 3GPP HeNBs Architecture Basis for Lawful Interception

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 3GPP 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.

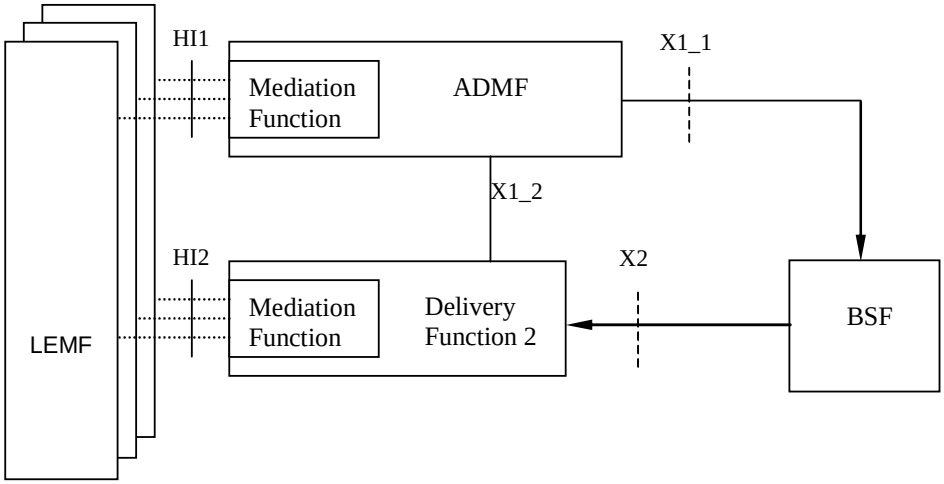


Figure 14.1: GBA Intercept Configuration

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.

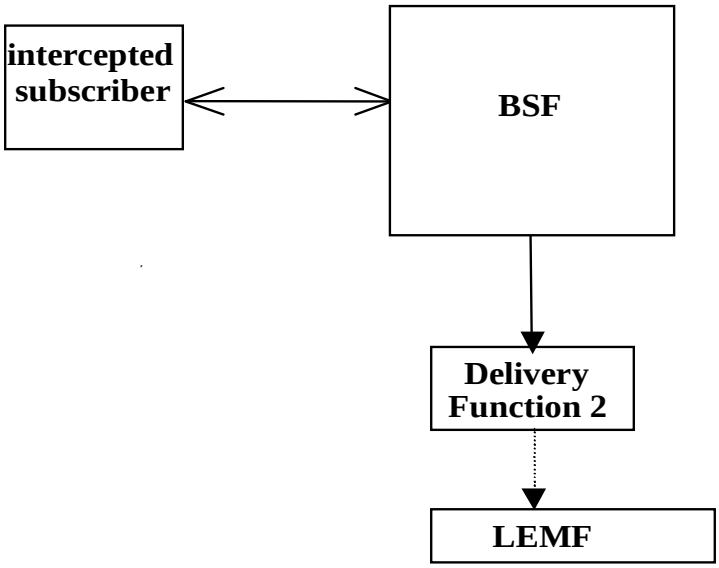


Figure 14.2: Provision of Intercept Related Information

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.

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 1: Lawful interception of VoIP as it applies SR-VCC (see 23.237 [46]) 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

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 are 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 (the mechanics of correlation is for further study);
- Media Identifier

Editor"s Note: The re-use of the existing reference point or whether to use a new reference point is for further study.

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.

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;
- time stamp (optional);
- direction (indicates media is from or to the target) – optional;

Editor"s Note: The use of the target identity for the information passed to the Delivery Function 3 requires further study.

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 15.1.

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.

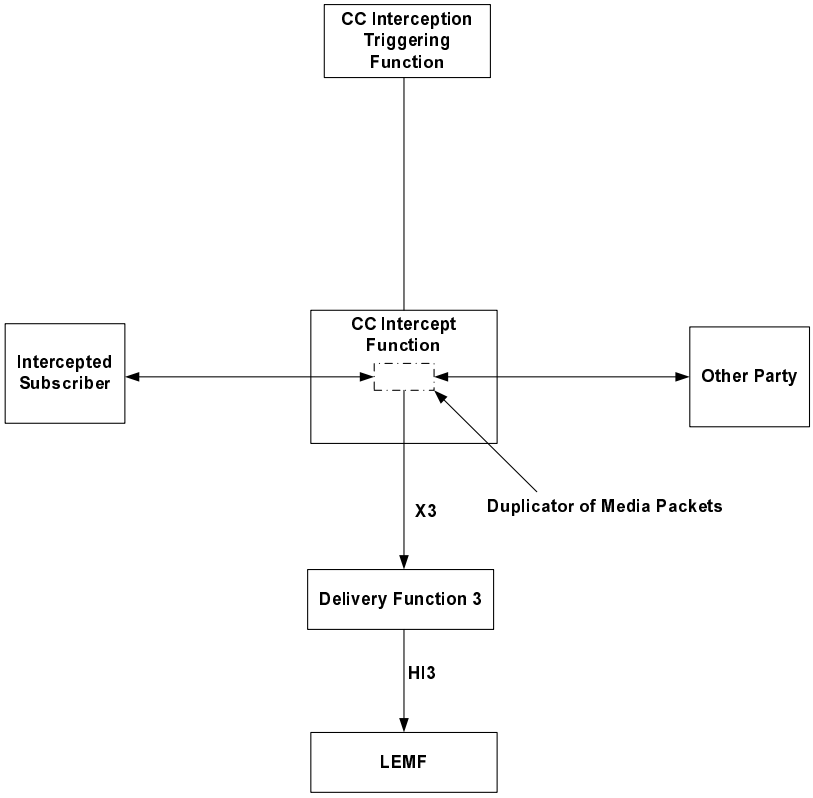


Figure 15.1: VoIP CC Interception for basic calls

In figure 15.1, the Intercepted Subscriber 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 Intercepted Subscriber (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.

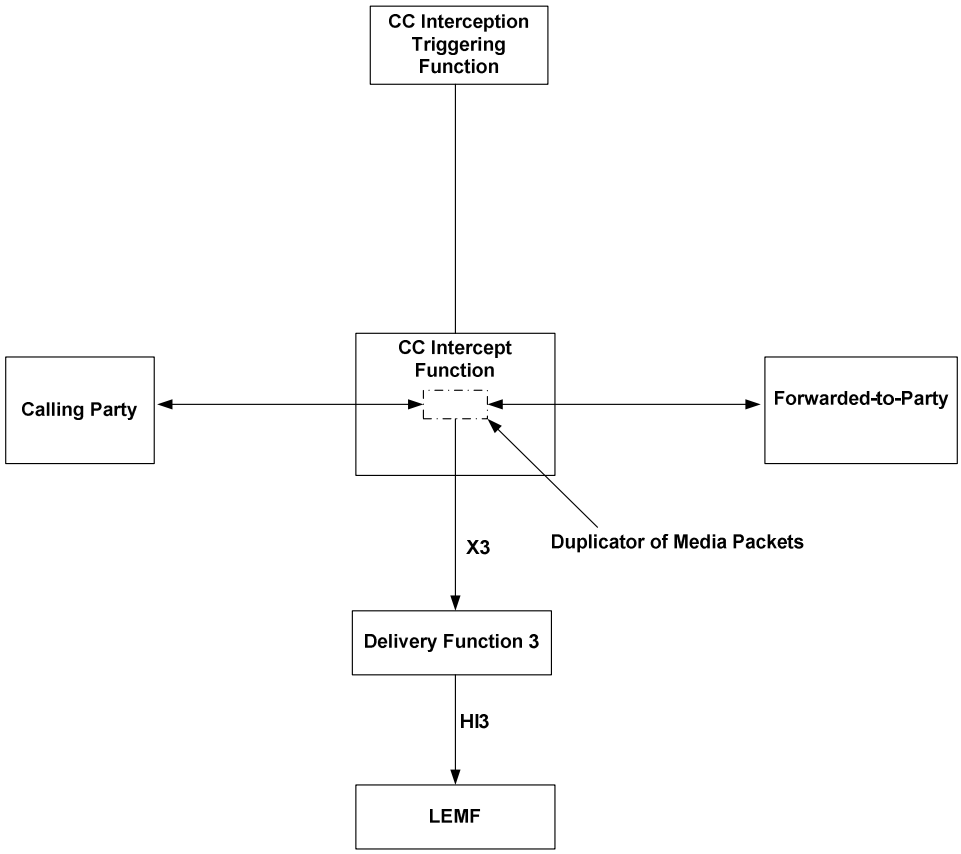


Figure 15.2: VoIP CC Interception for forwarded calls

The CC Interception Triggering Function sends the CC intercept trigger to the CC Intercept Function according 15.1.1.1. 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 15.1.1.2.

Editor"s Note: Exact use of figures 15.1 and 15.2 in call forwarding scenarios needs to be clarified.

15.3 Provision of Intercept Related Information for VoIP

See clause 7.A.

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.

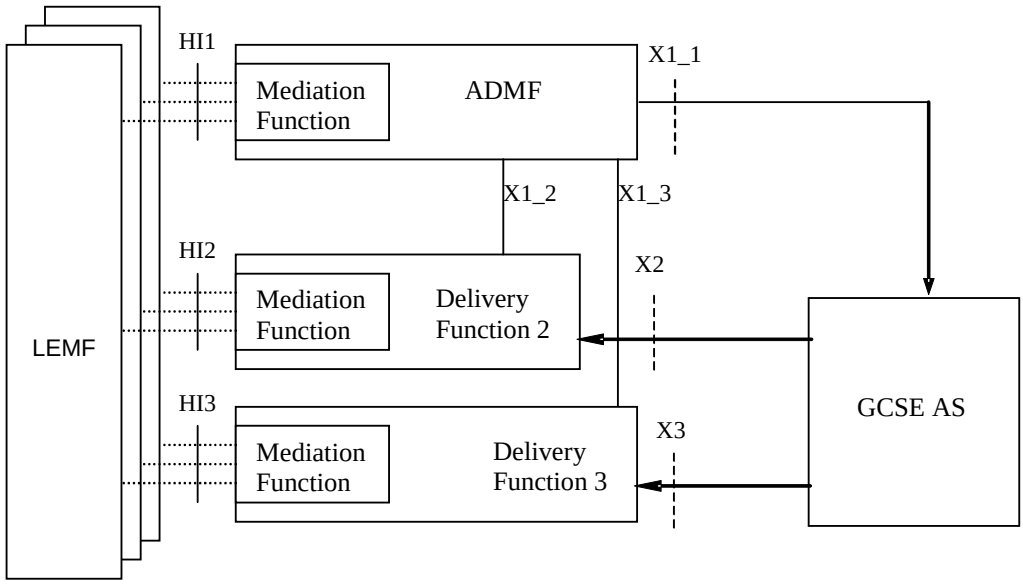


Figure 16.1: GCSE AS Intercept configuration

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.

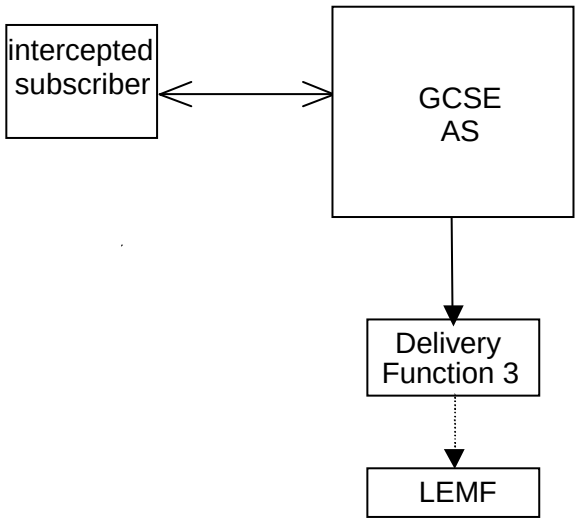


Figure 16.2: Provision of Intercept Product from GCSE AS

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 [51]);

- 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.

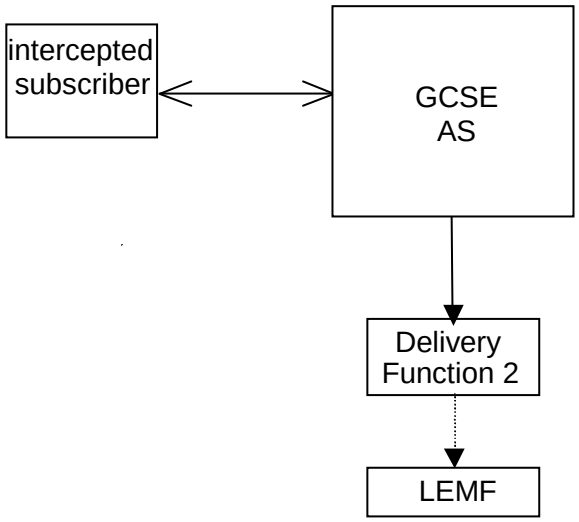


Figure 16.3: Provision of Intercept Related Information

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 X.1.2.2 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.

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

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

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

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

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 [54]. 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.

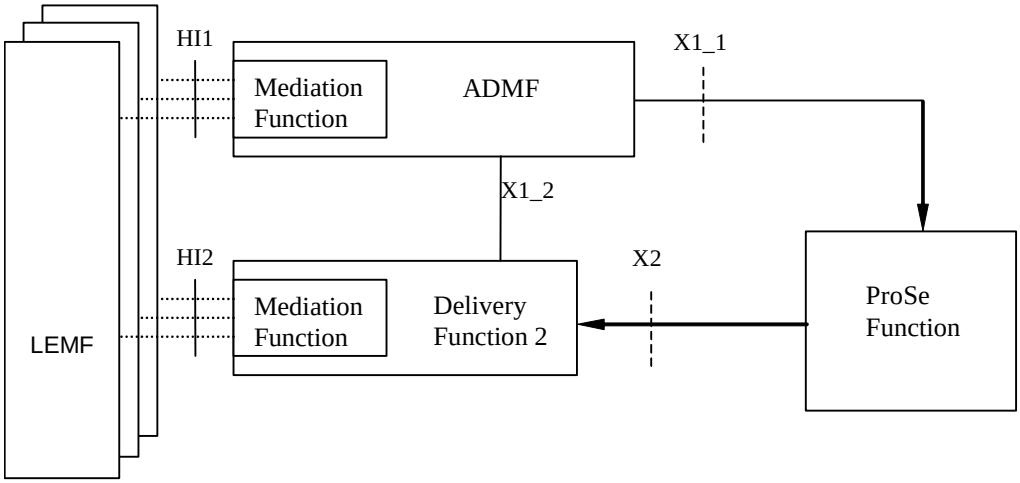


Figure 17.1-1: ProSe Direct Discovery Intercept configuration

Figure 17.1-1 shows the CC 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 Discovert 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 an intercepted subscriber 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.

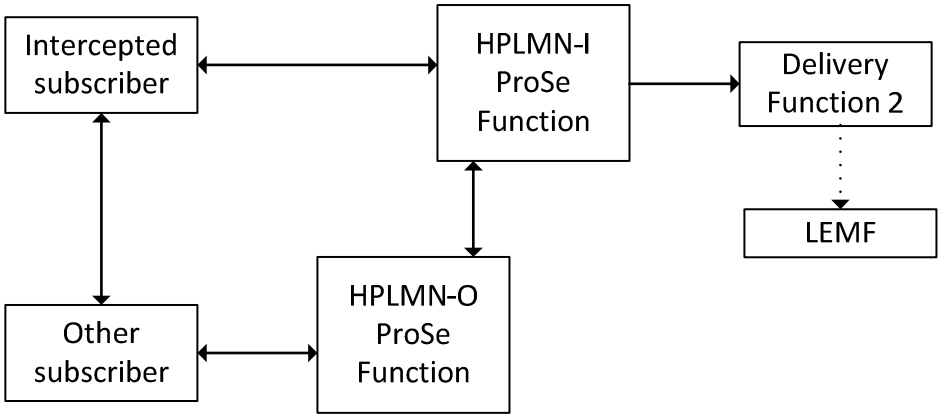


Figure 17.1.3.1-1: Provision of Intercept Related Information for discovery

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 LI subject 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 LI subject	
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 LI subject	
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 – In Network

17.2.1 General

Proximity Service (ProSe) are specified in TS 23.303 [54]. This includes one to many communications among ProSe UEs while in network coverage. Such communication may occur while the UEs are in proximity.

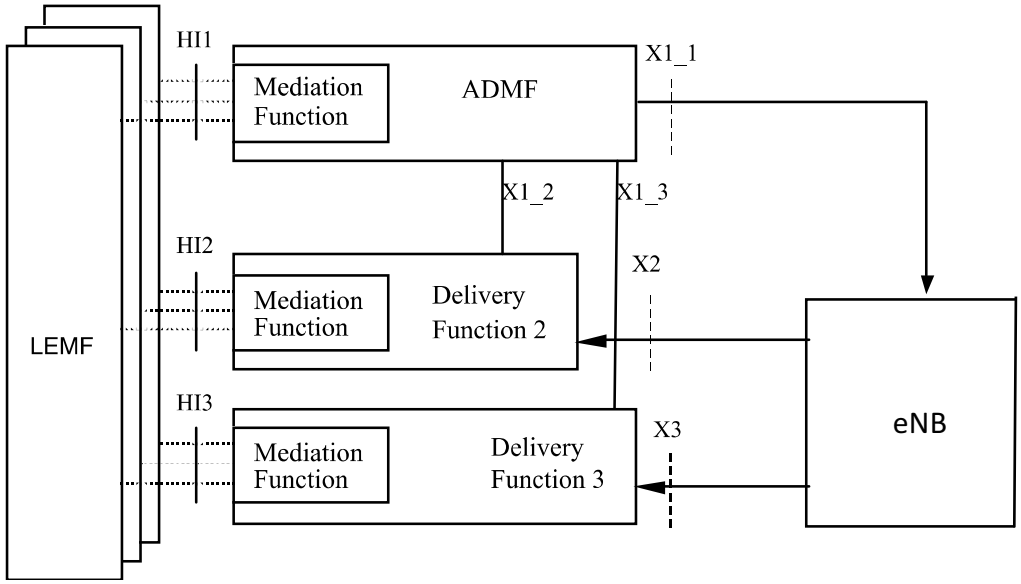


Figure 17.2-1: ProSe One To Many Communications (In Network Coverage) Intercept configuration

Figure 17.2-1 shows the IRI and CC interception configuration for ProSe one to many communications while in network coverage. 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.

While the target ProSe UE is in network coverage, the eNB providing the coverage shall perform interception of ProSe one to many communications.

The target identity for ProSe one to many communications interception is the ProSe UE ID and the ProSe Layer 2 Group ID. 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 one to many communications from the eNB to the DF2 and to the LEMF. If a one to many communications is detected a One-To-Many event, which contains the content and header of the communications, 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 One-To-Many event shall contain only one to many communications header, or both the header and content.

If an event involving an intercepted subscriber occurs, the eNB shall send the relevant data to the DF2. This is based on interception of communications containing the target ProSe UE ID or the corresponding target ProSe Layer-2 Group ID. The eNB shall send the intercept product to the DF2 for formatting and delivery to the LEMF.

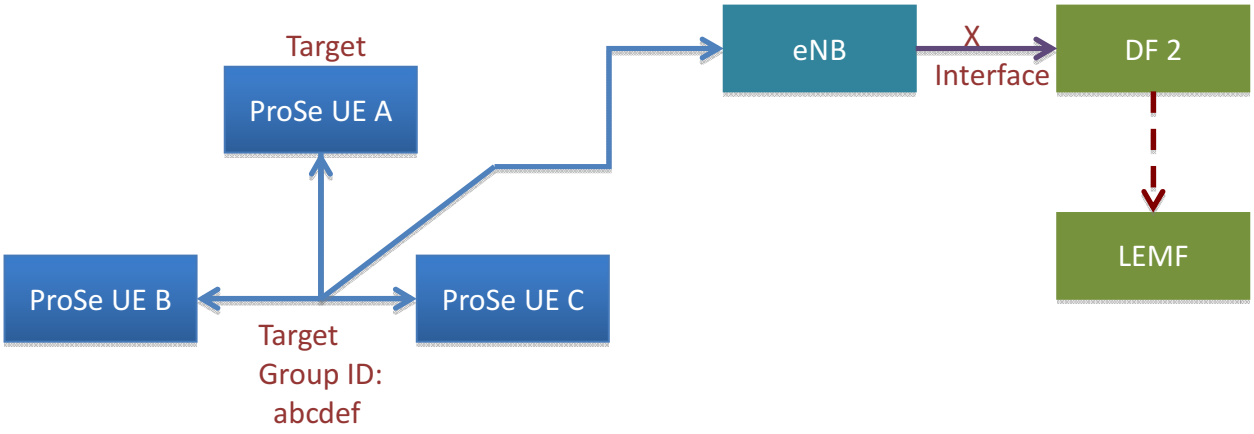


Figure 17.2.2.1-1: Provision of Intercept Product – One-To-Many Communications

17.2.2.2 X2-interface

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

- target identity (ProSe UE ID and ProSe Layer-2 Group ID);
- 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 while in network coverage:

- Target sent One-To-Many communications.

Interception of these events is mandatory in the eNB of the PLMN that is used for network coverage.

17.2.3.3.2 Structure of ProSe LI One-To-Many Event Information

A set of possible elements as shown below is used to generate the events.

Table 17.2.3.3.2.1: Information Events for One-To-Many Communications Event Records

Element
Observed ProSe UE ID ProSe UE ID of the target.
Observed ProSe Layer-2 Group ID ProSe Layer-2 Group ID of the target.
Event date Date of the event generation in the eNB.
Event time Time of the event generation in the eNB. Timestamp shall be generated relative to the eNB internal clock.
Sender ID Identifies the sender of the One-To-Many Communications.
Destination ID Identifies the destination of the One-To-Many Communications.
One-To-Many Communications Includes a copy of the actual One-To-Many Communications; applicable only when CC delivery is authorized.
GCSE Communications Group Participants List of all users that are participating in the GCSE communications group.
Network Identifier Operator ID plus unique identifier for the element reporting the ICE.
Location information Location information of the target.
IAs The observed Interception Areas.

17.2.2.3.3 ProSe LI One-To-Many Events

For One-To-Many communications a One-To-Many-Comms-event is generated. These elements will be delivered to the DF2 if available:

Table 17.2.2.3.3.1 One-To-Many-Comms event

Observed ProSe UE ID
Observed ProSe Layer-2 Group ID
Event type
Event Time
Event Date
Network Identifier (including network element identifier)
Location Information
Sender Identity
Destination Identity
One-To-Many Communications (NOTE)
IAs (if applicable)

NOTE: The CC part of the One-To-Many Communications shall be included if delivery of CC is authorized.

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.

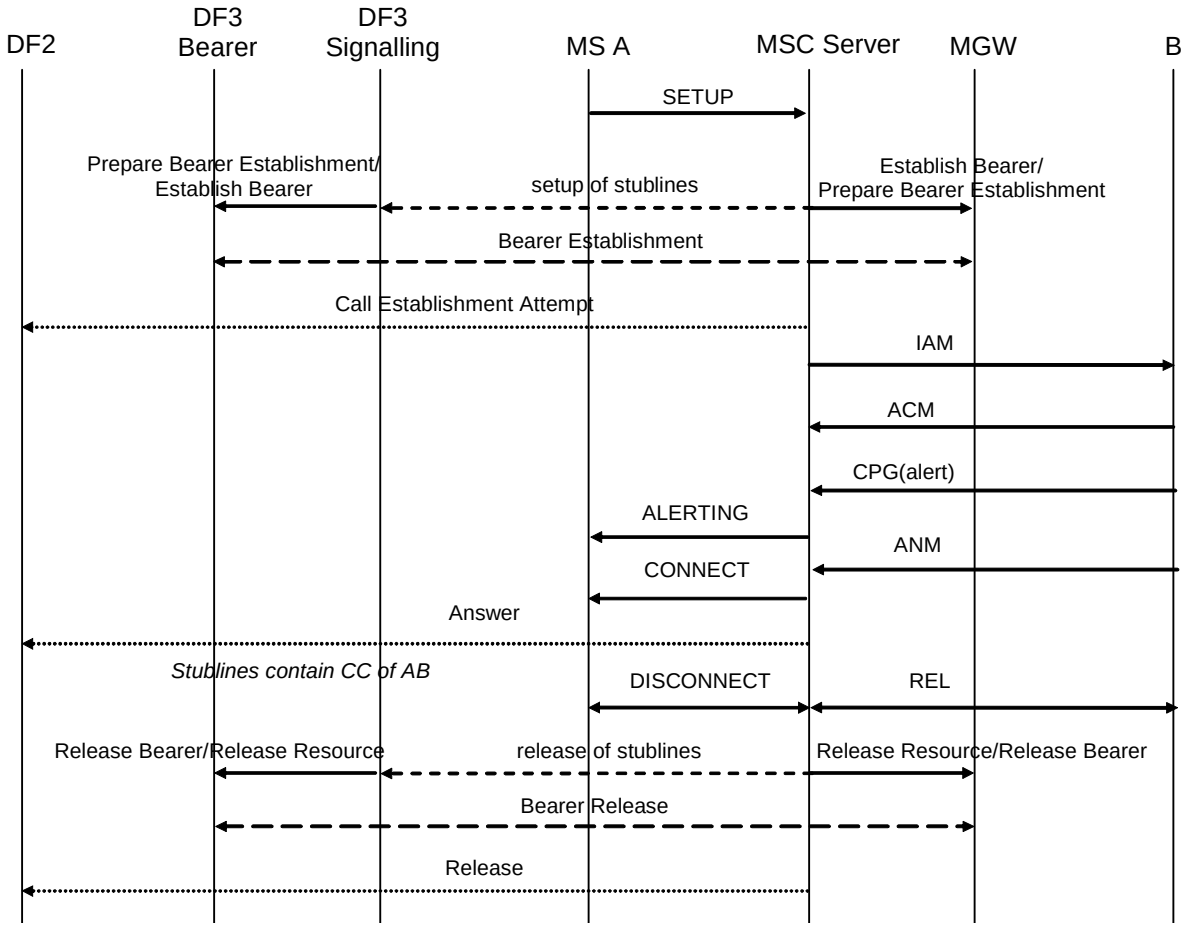


Figure A.1: Interception of mobile originated circuit switched calls

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.

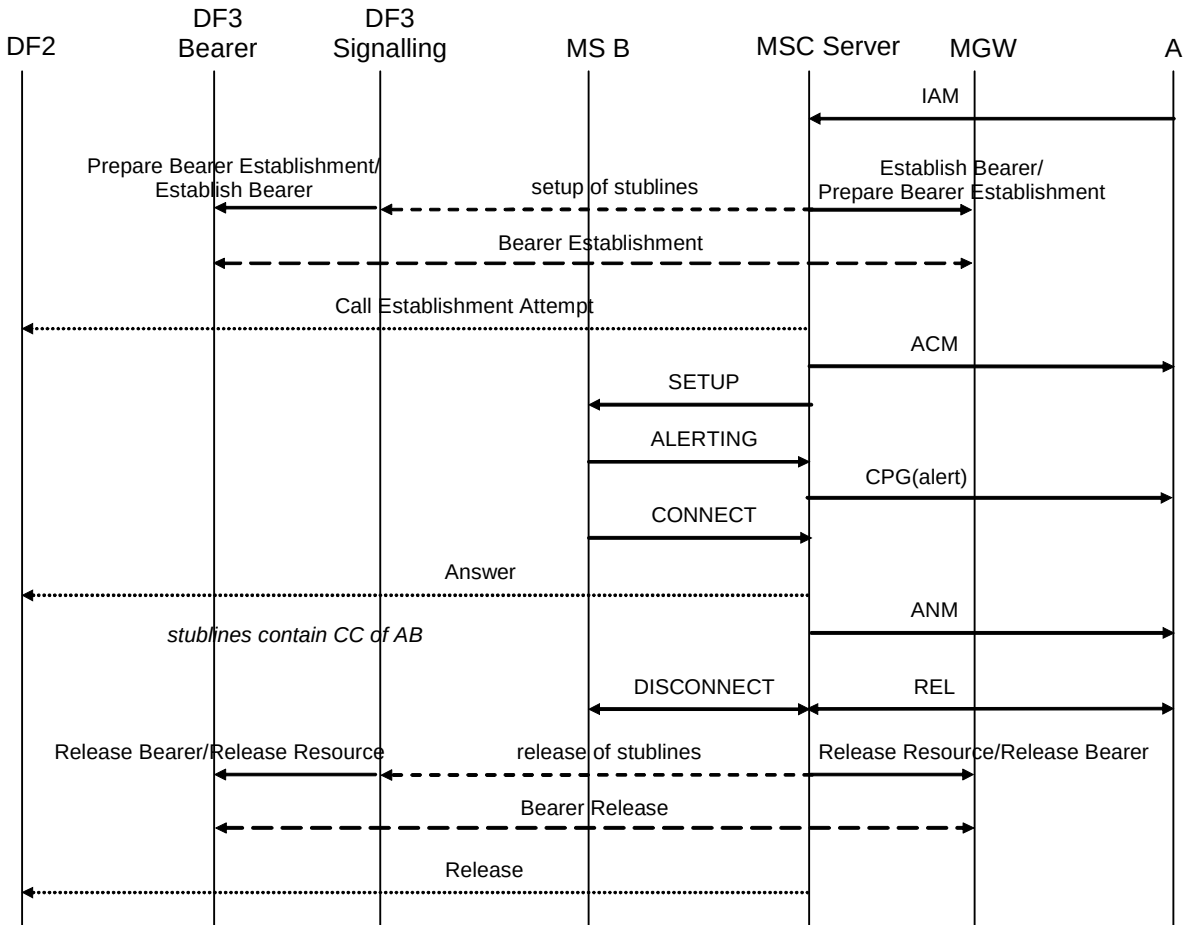


Figure A.2: Interception of mobile terminated circuit switched calls

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.

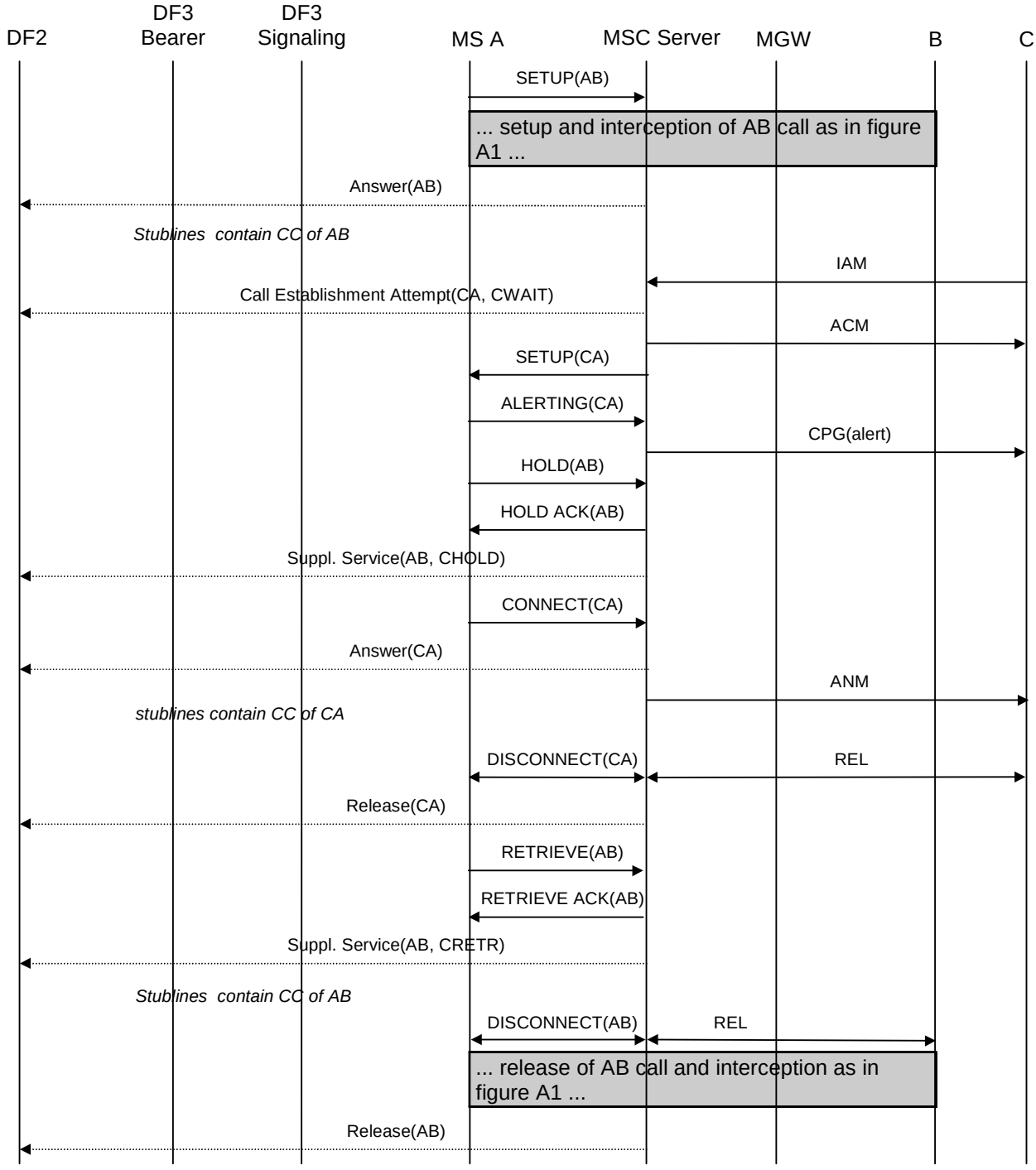


Figure A.3: Interception of call hold / call waiting - stublines per target

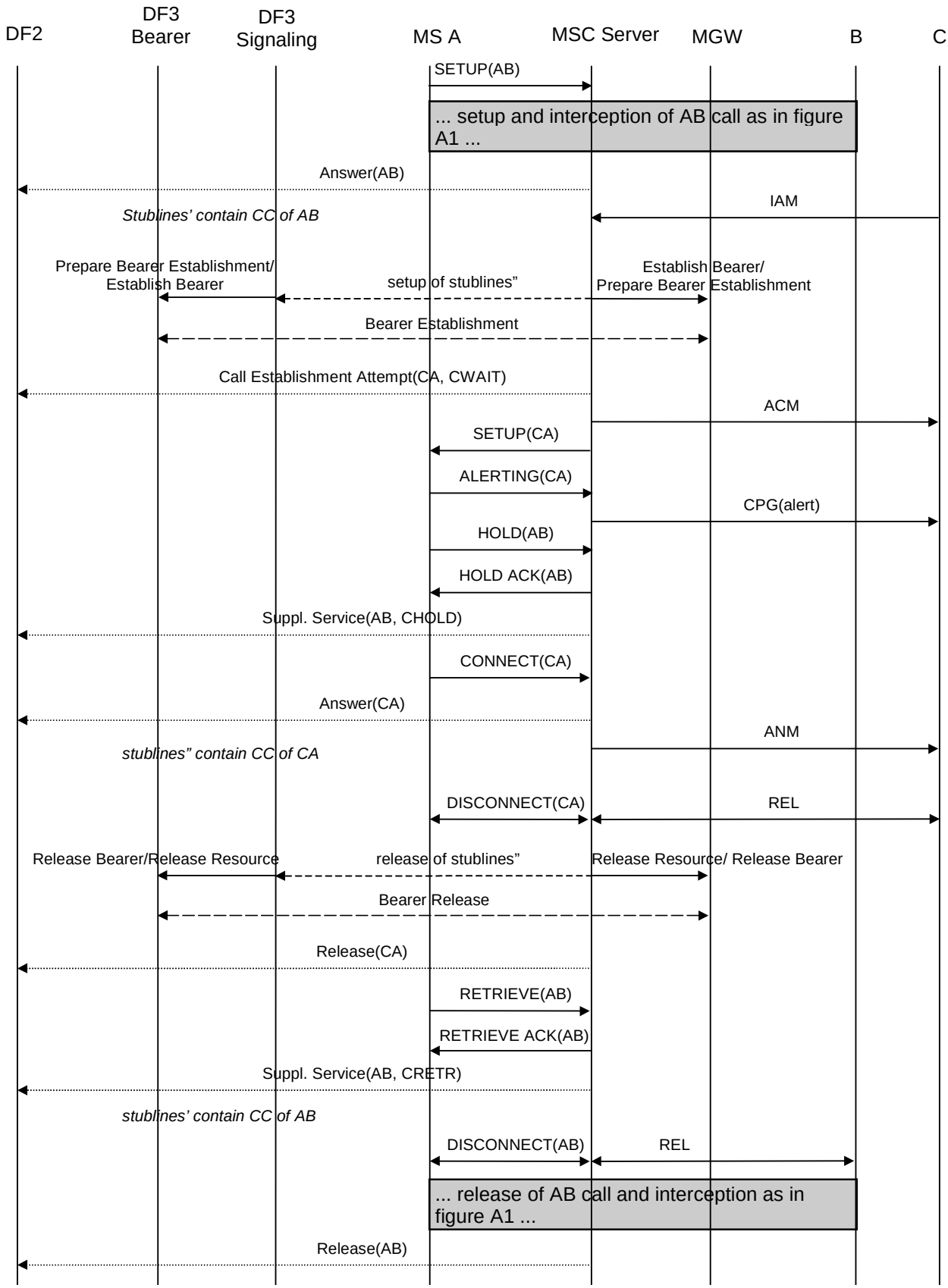


Figure A.4: Interception of call hold / call waiting - stublines per target call

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.

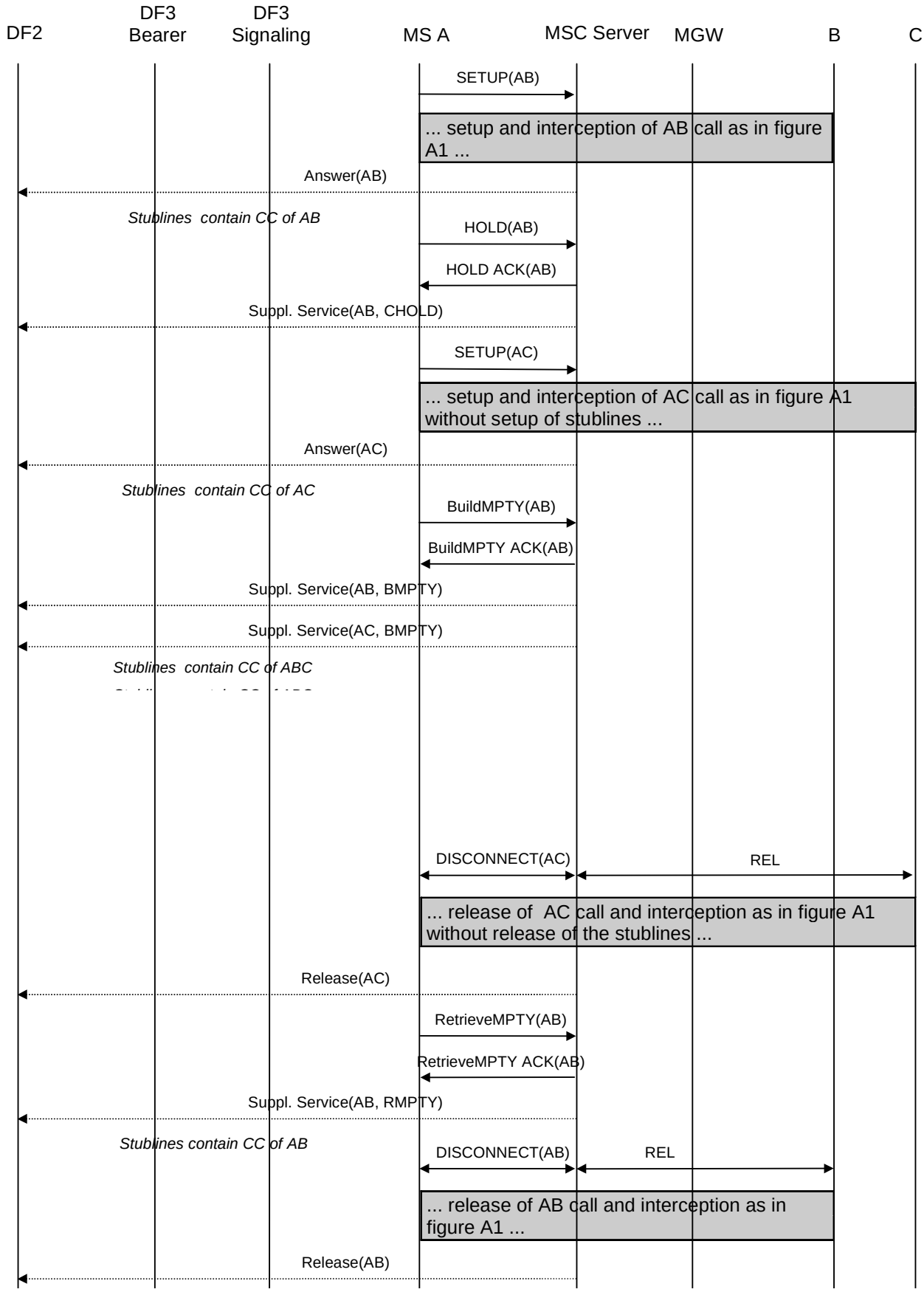


Figure A.5: Interception of multiparty calls - stublines per target

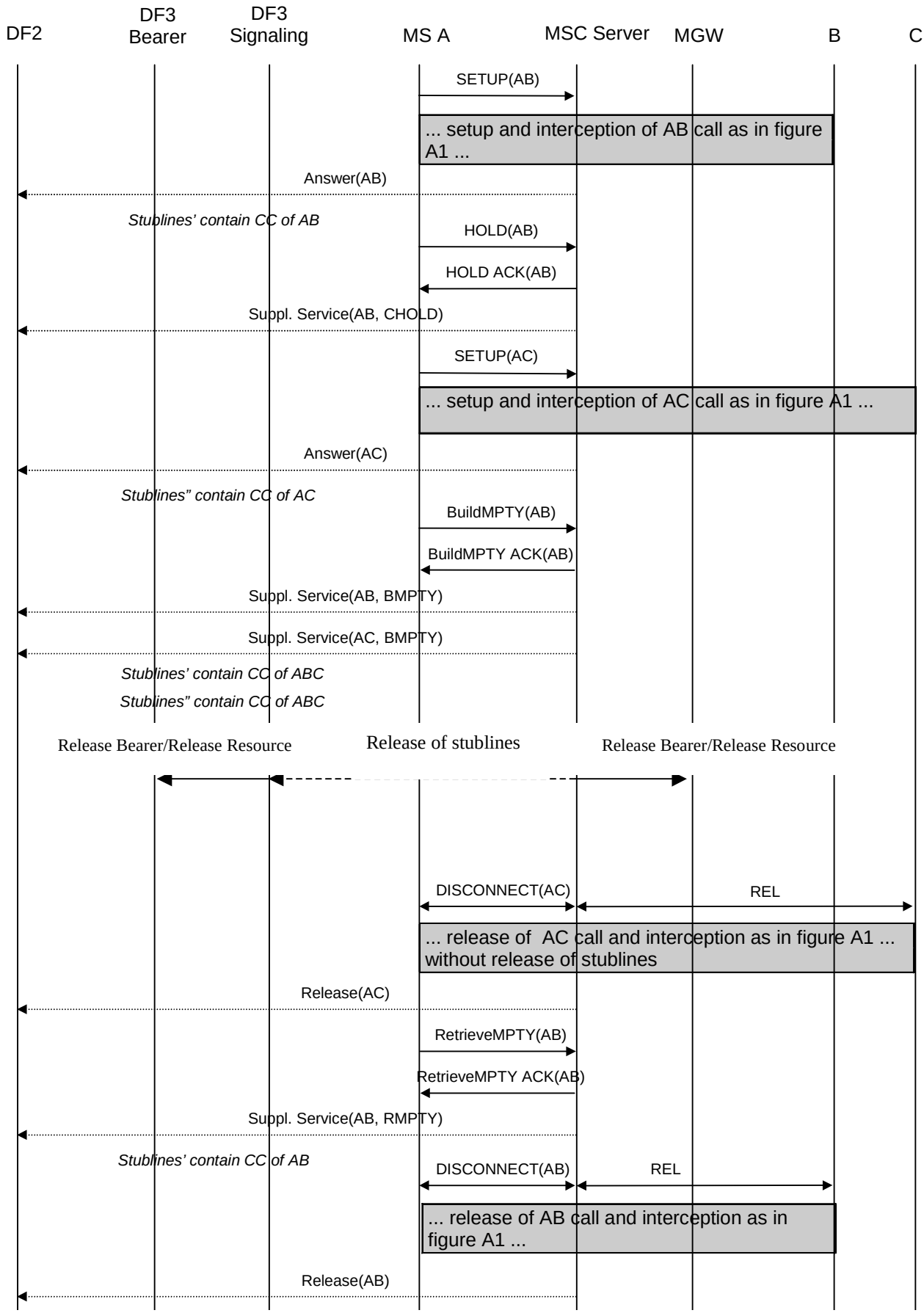


Figure A.6: Interception of multiparty calls - stublines per target call

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.

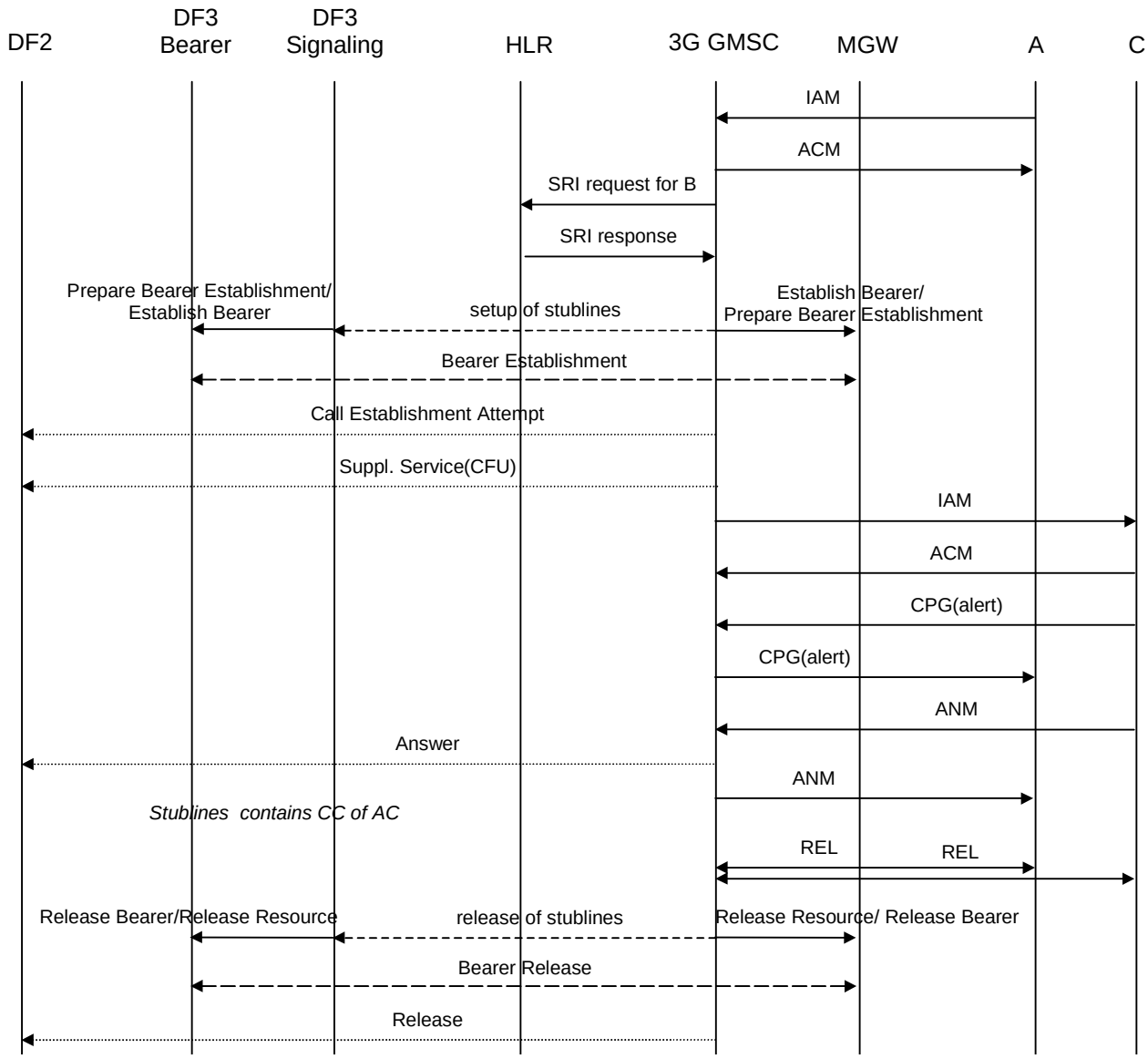


Figure A.7: Interception of unconditional call forwarding

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.

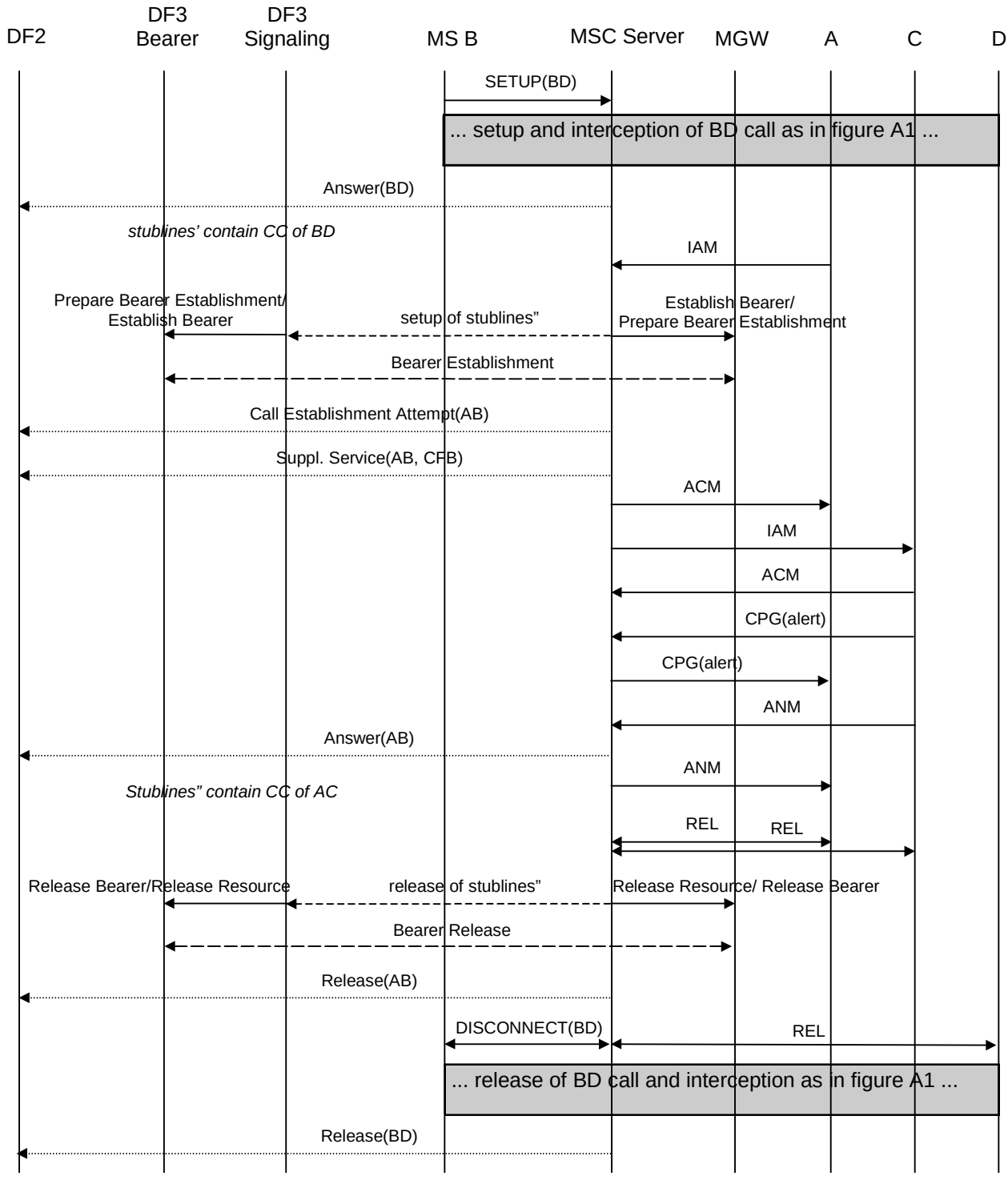


Figure A.8: Interception of call forwarding on busy (network determined)

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.

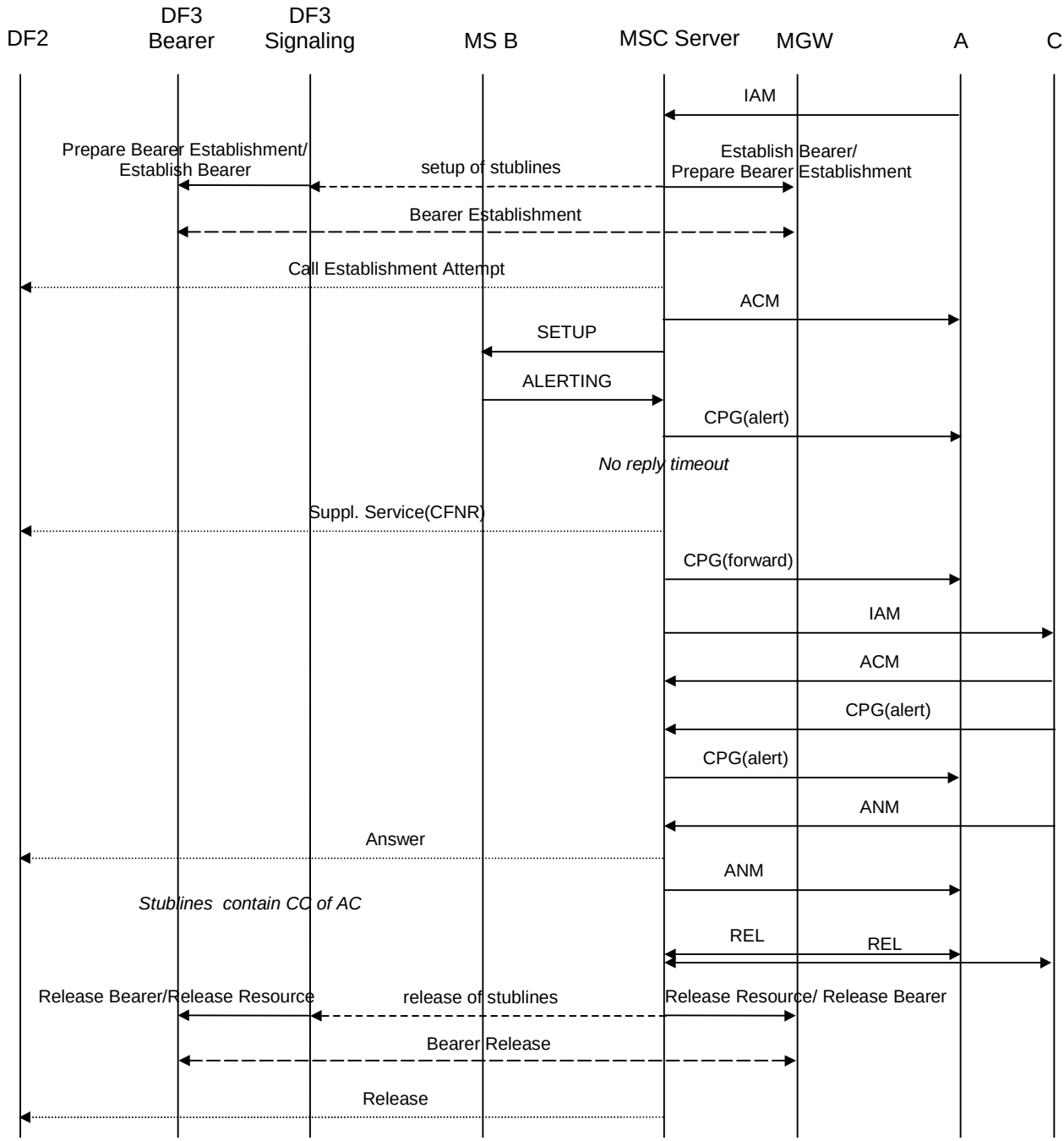


Figure A.9: Interception of call forwarding on no reply

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.

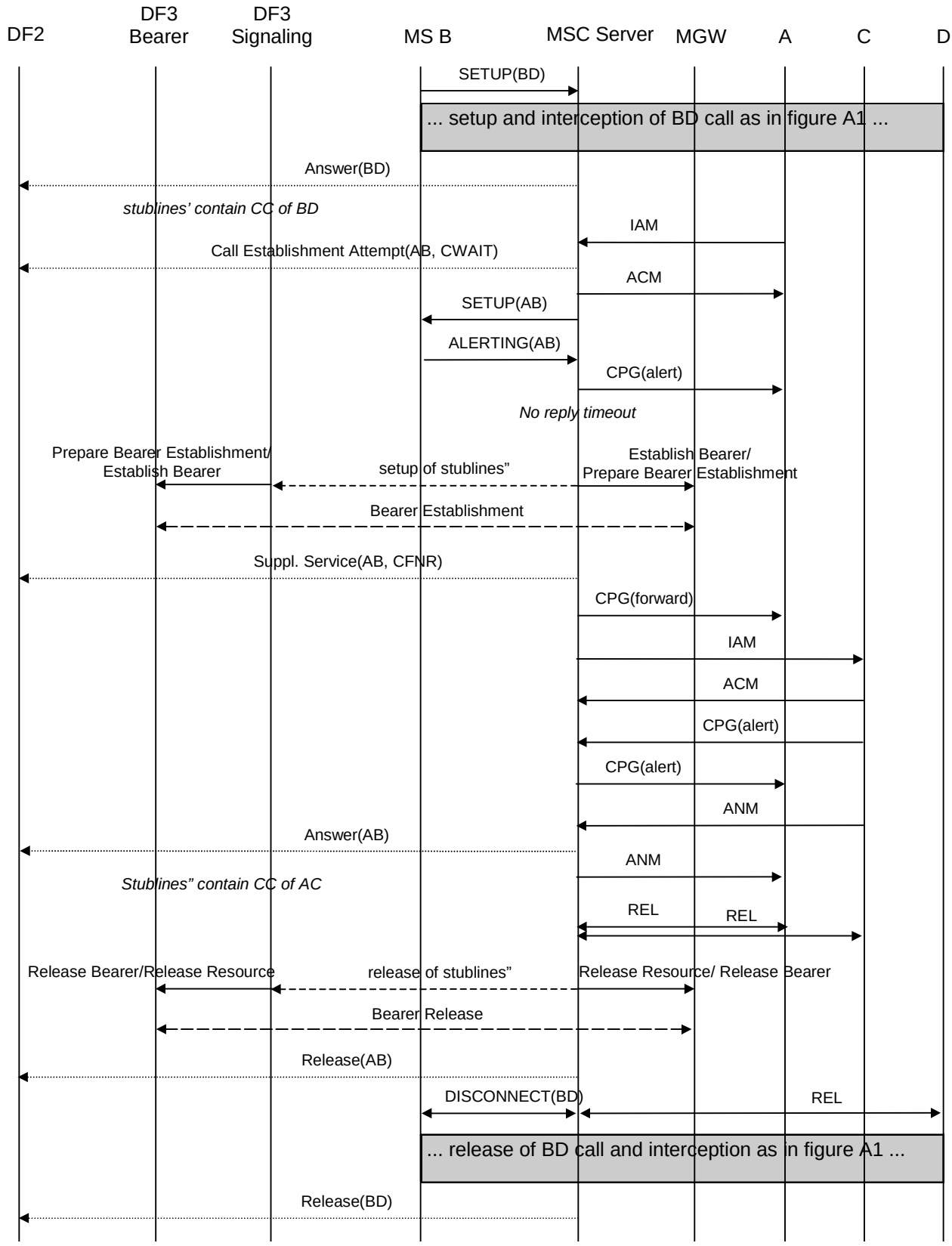


Figure A.10: Interception of call waiting / call forwarding on no reply - stublines per target

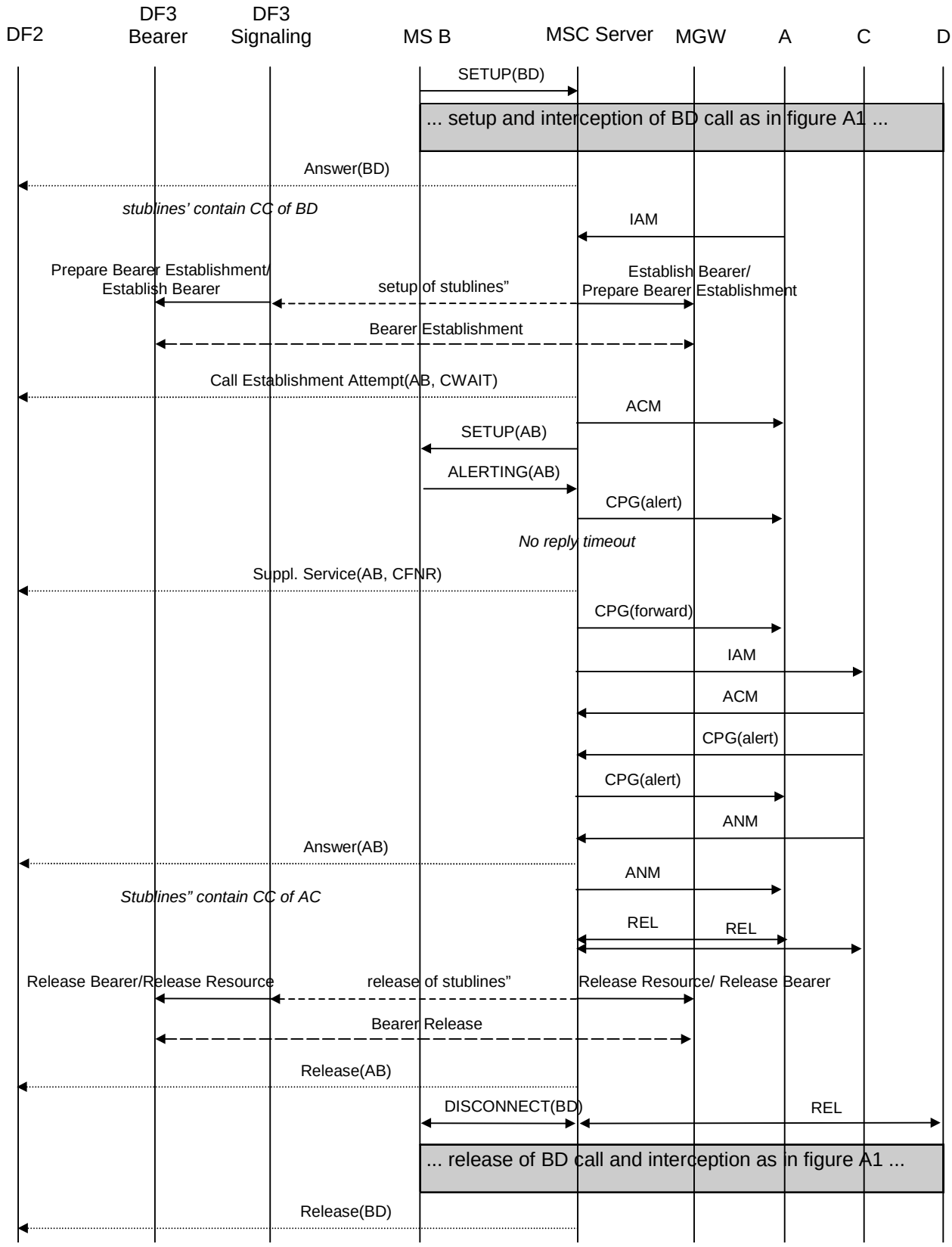


Figure A.11: Interception of call waiting / call forwarding on no reply - stublines per target call

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.

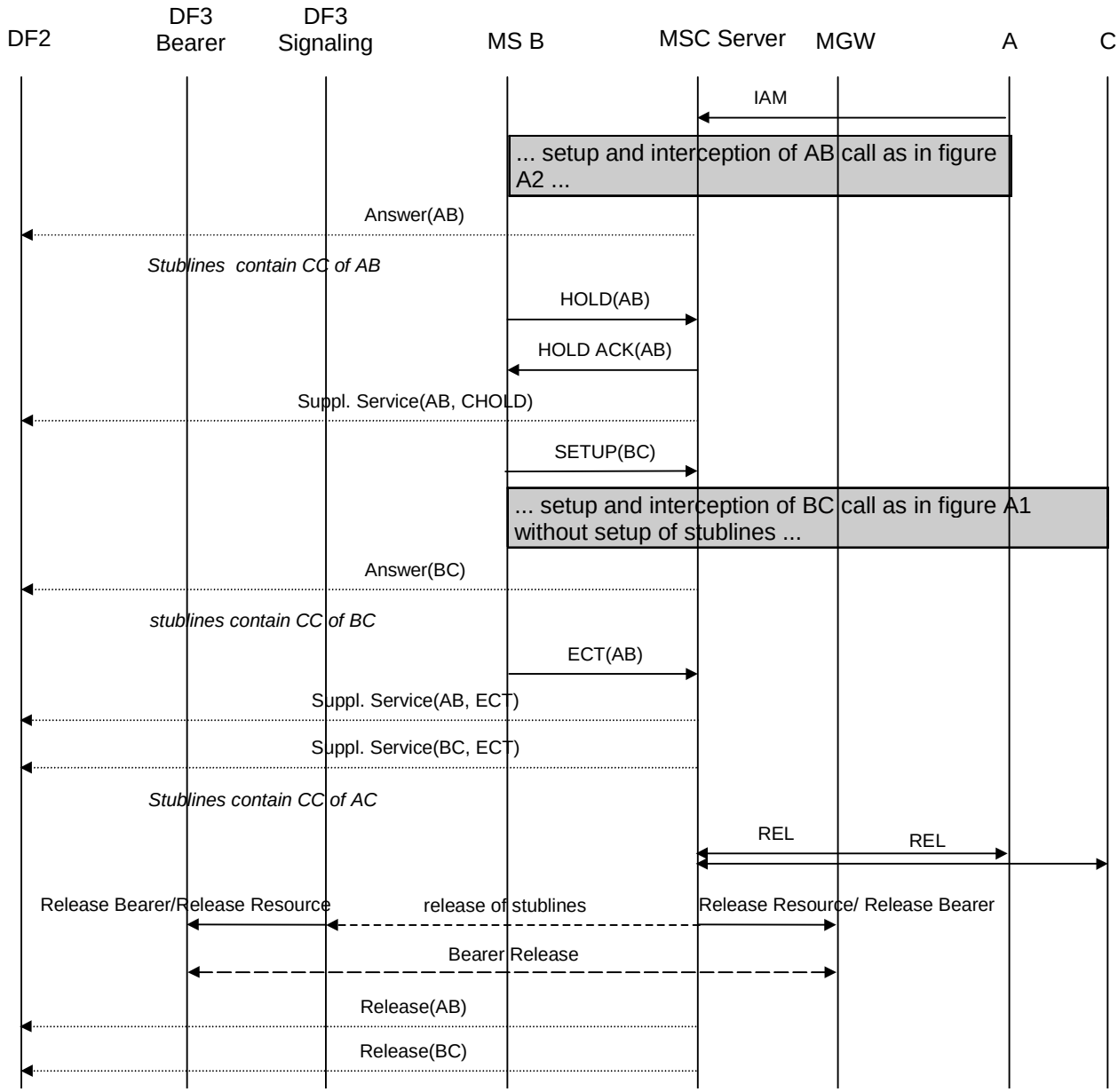


Figure A.12: Interception of explicit call transfer - stublines per target

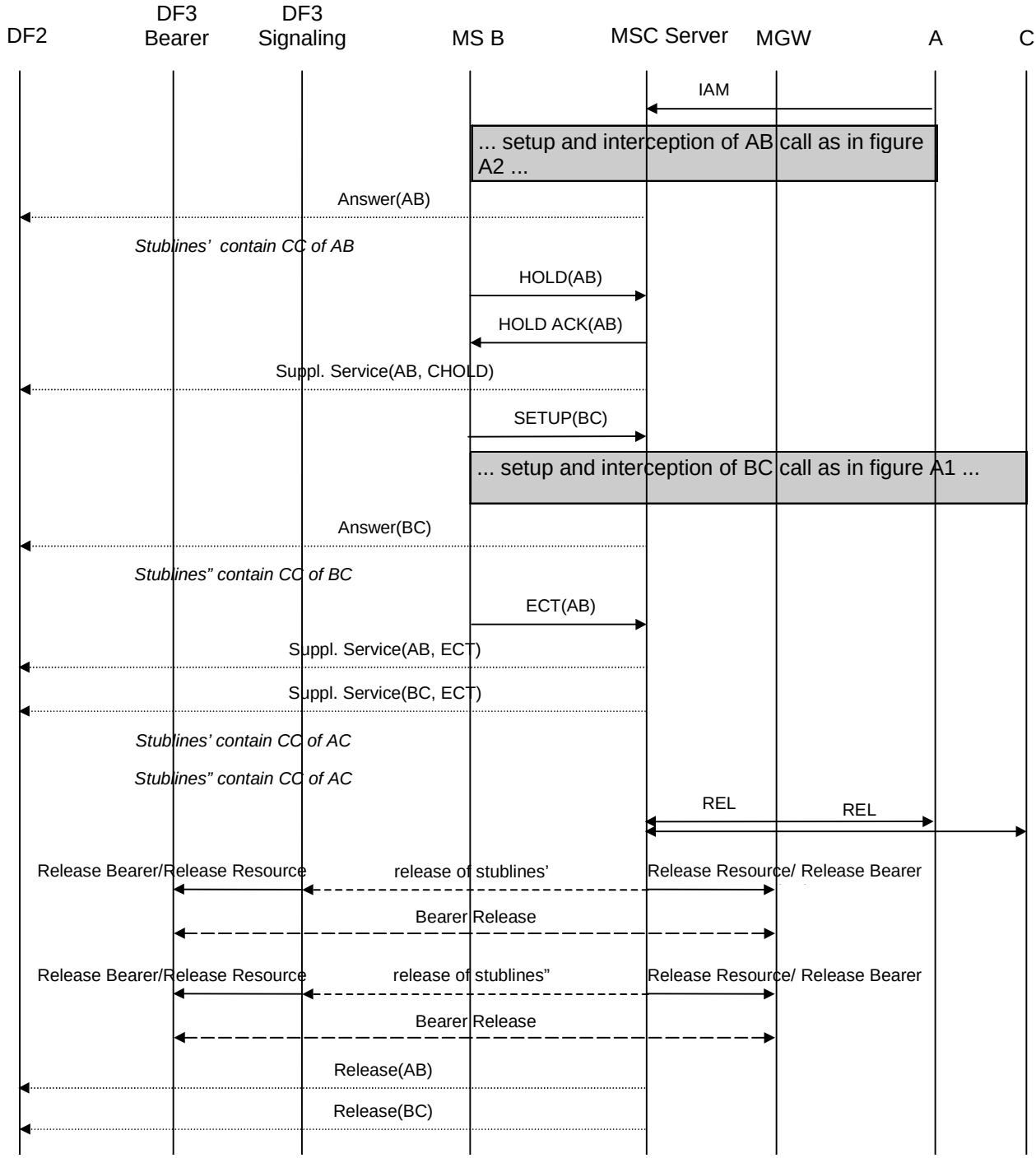


Figure A.13: Interception of explicit call transfer - stublines per target call

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.

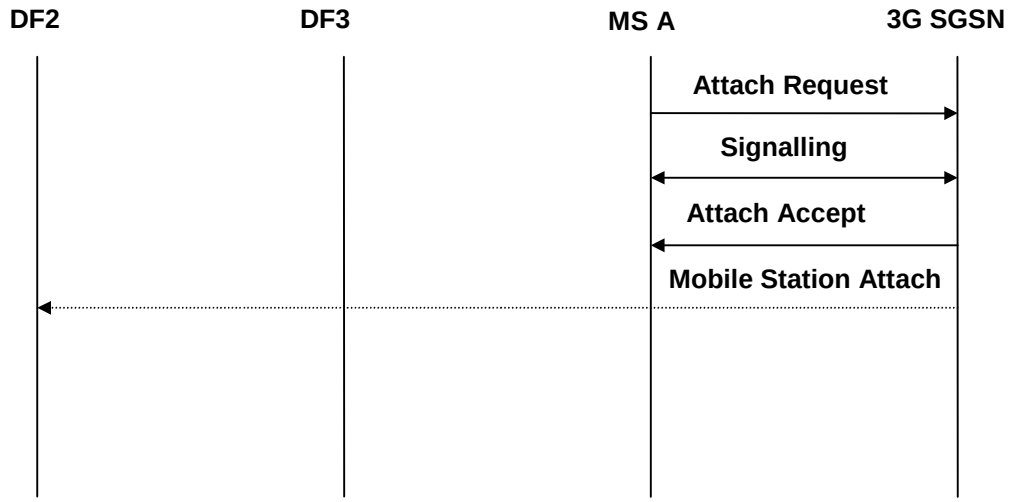


Figure B.1: Interception of mobile originated Mobile Station Attachment

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.

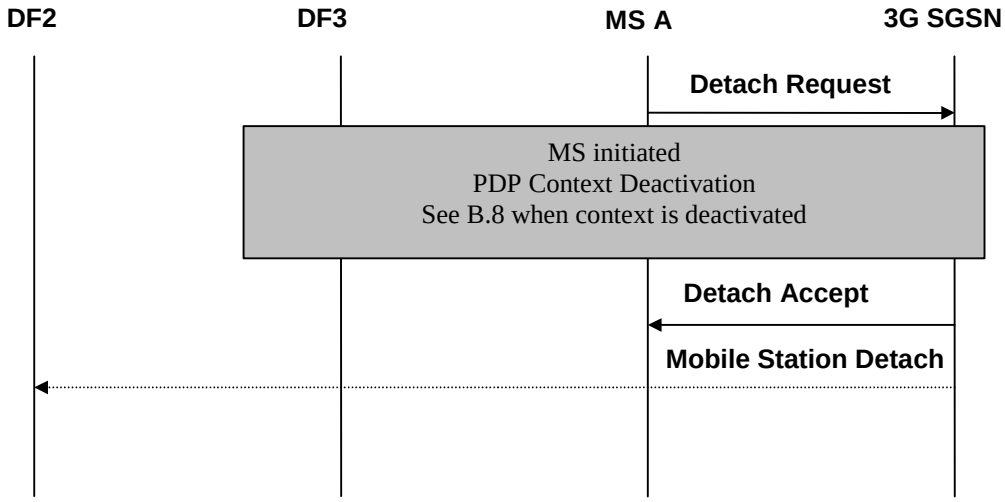
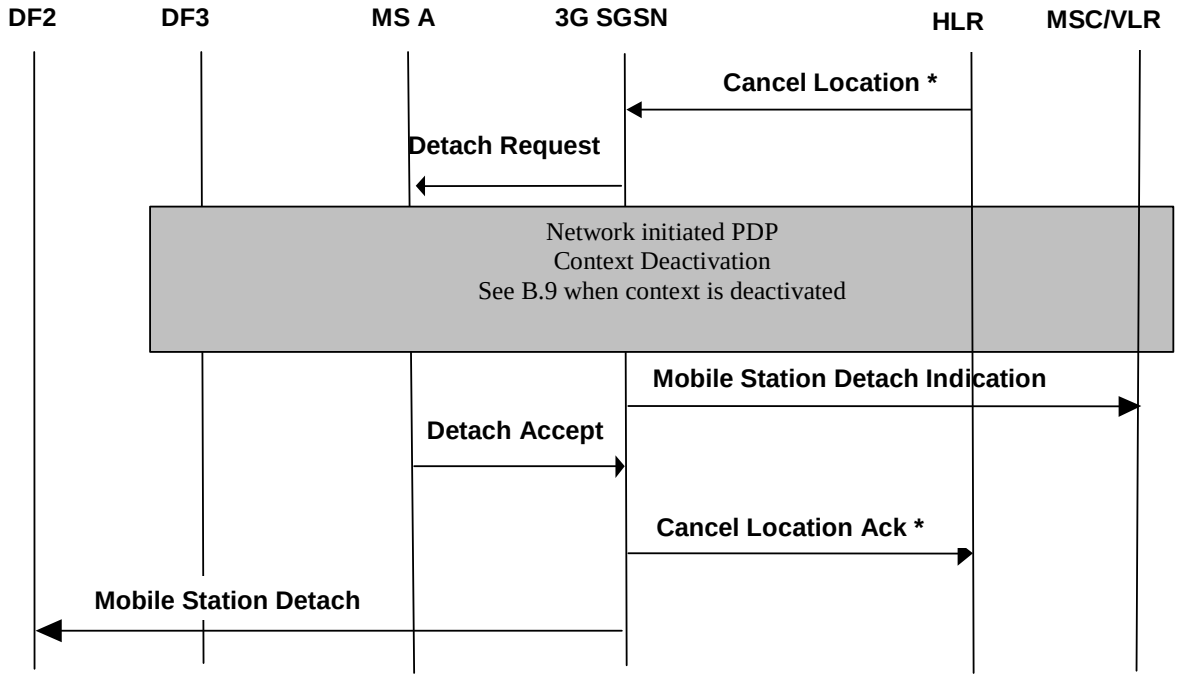


Figure B.2: Interception of mobile originated Mobile Station Detachment

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.

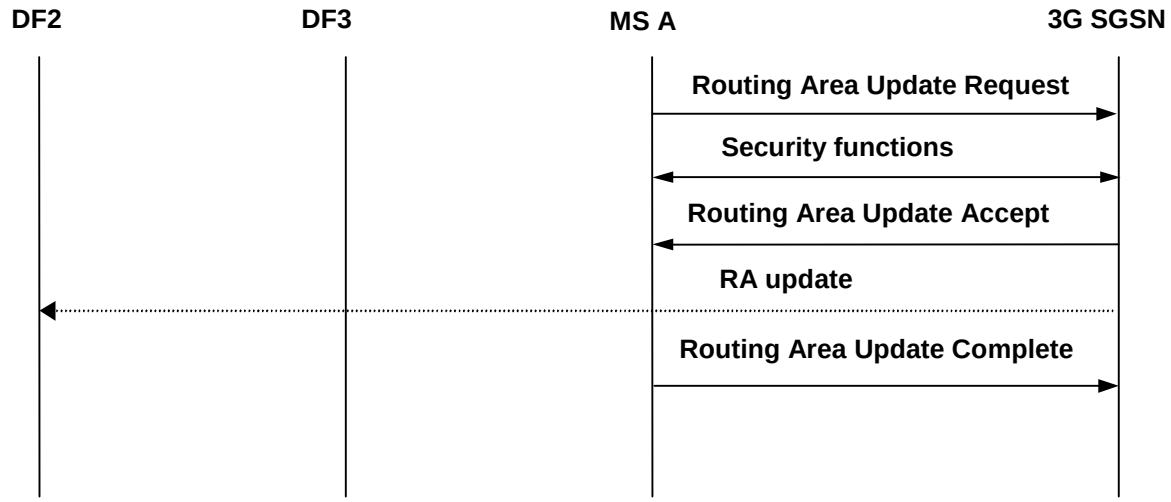


Figure B.4: Interception of an Intra Routing Area Update

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.

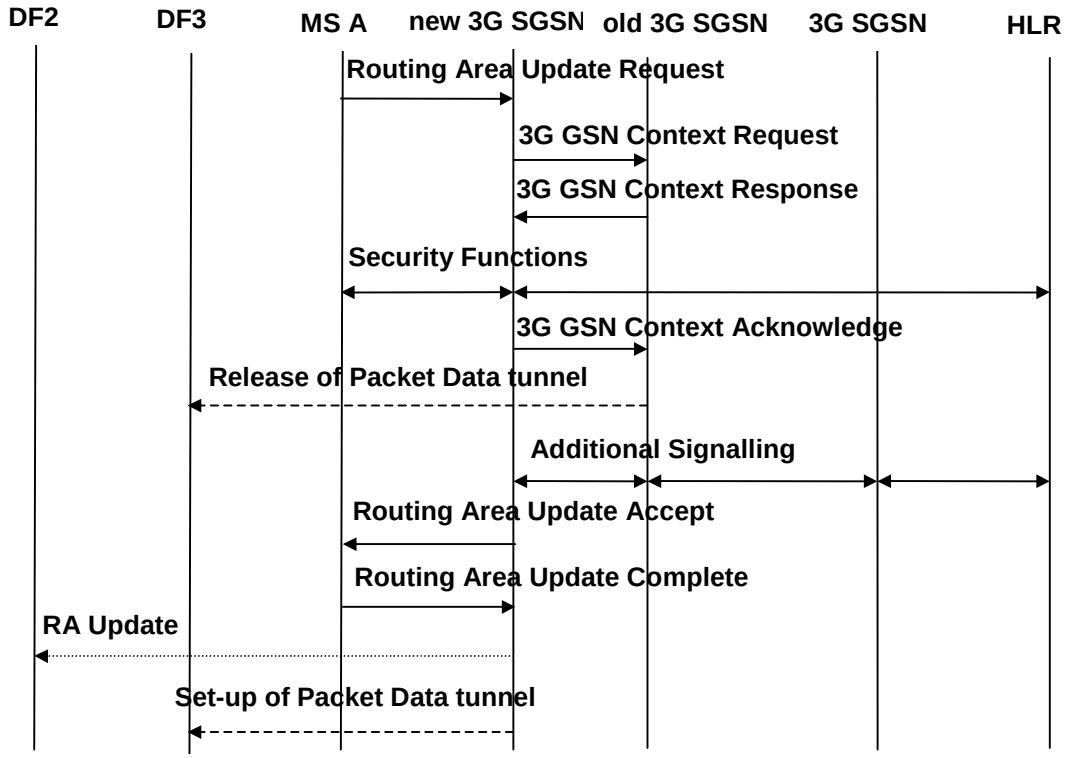


Figure B.5: Interception of an Inter Routing Area Update

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.

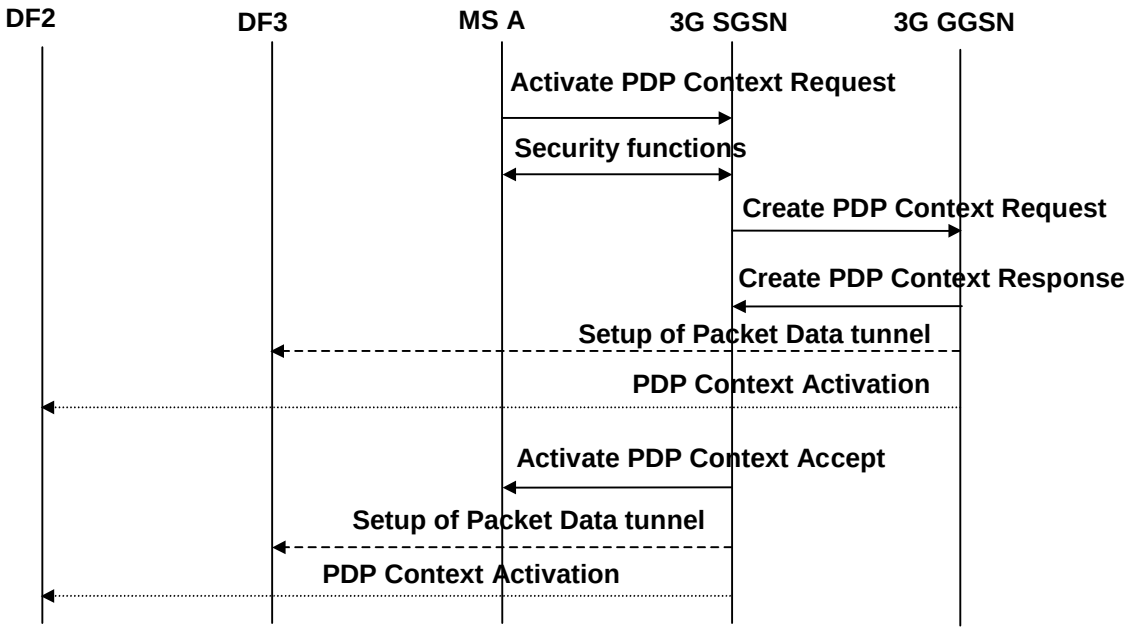


Figure B.6: Interception of a PDP Context Activation

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.

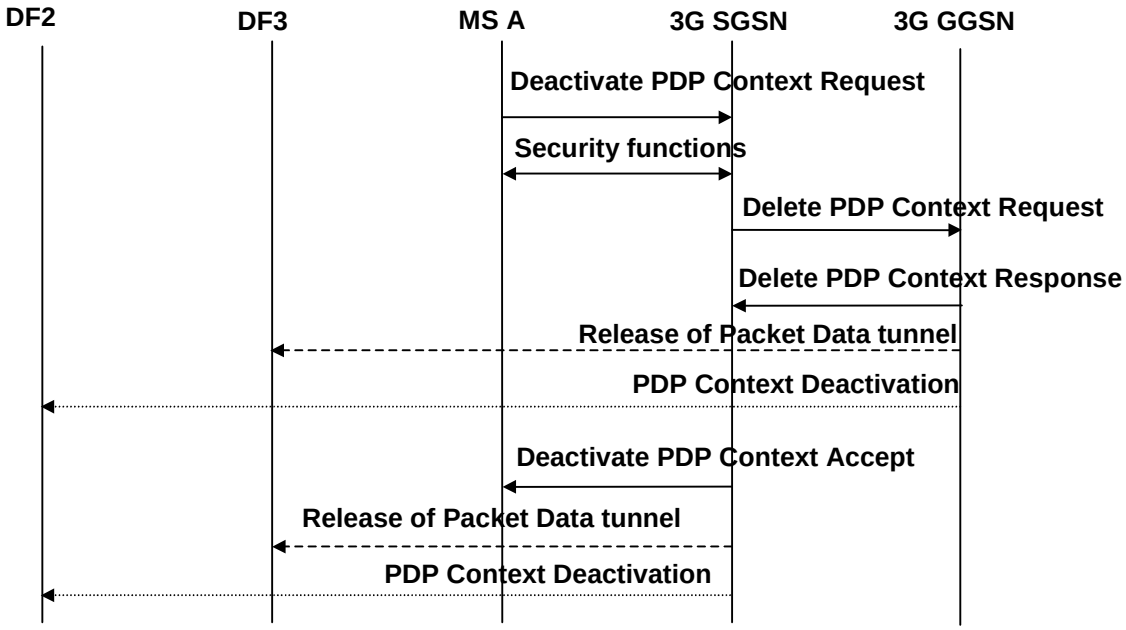


Figure B.7: Interception of a PDP Context Deactivation

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).

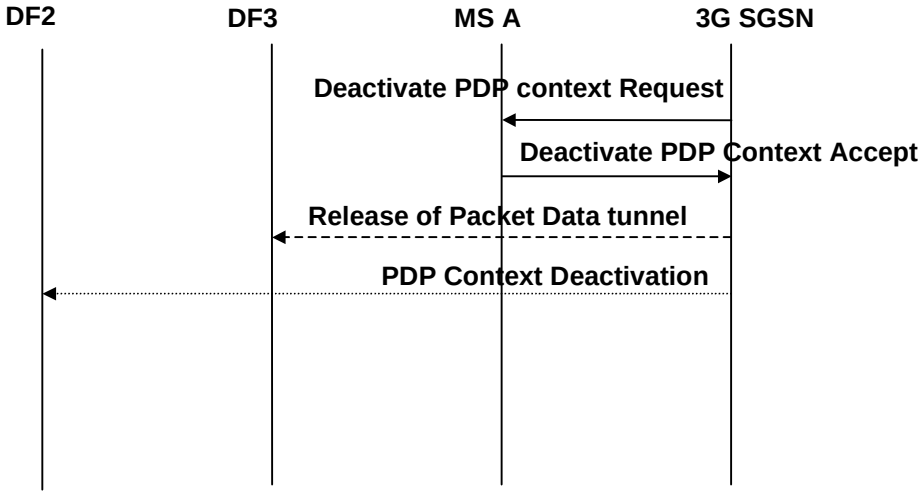


Figure B.8: Interception of a Network initiated PDP Context Deactivation

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.

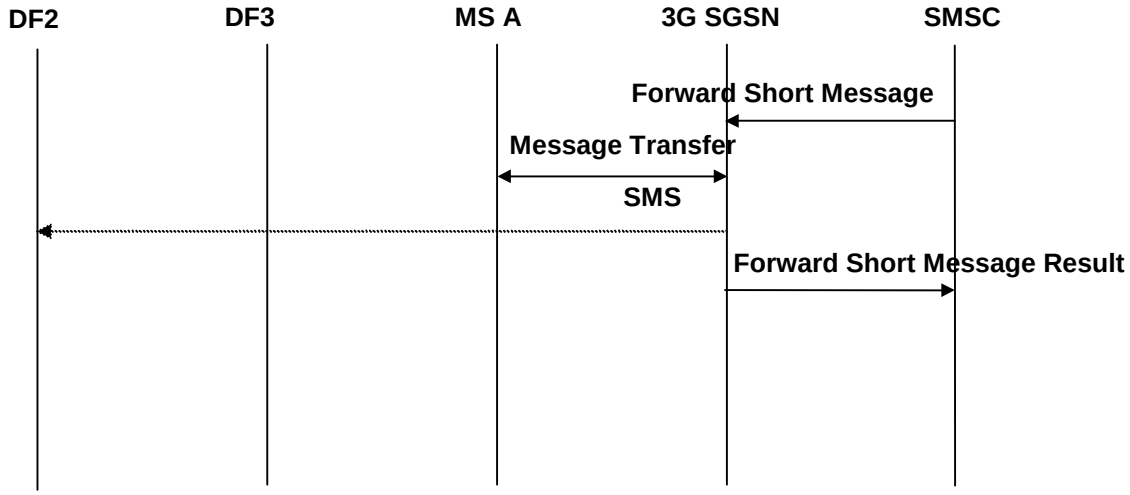


Figure B.9a: MT-SMS interception after 3G SGSN receives notification of SMS delivery to MS(A)

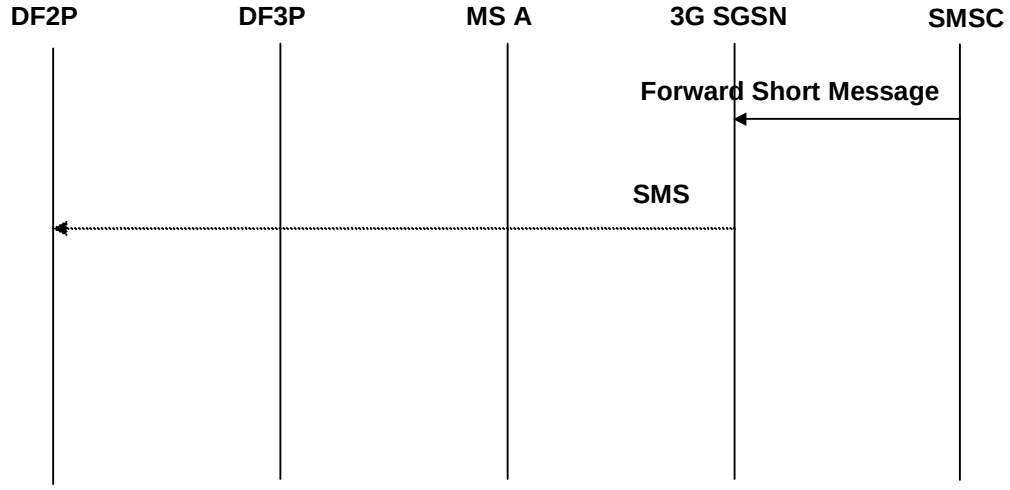


Figure B.9b: MT-SMS interception after 3G SGSN receives SMS from SMSC

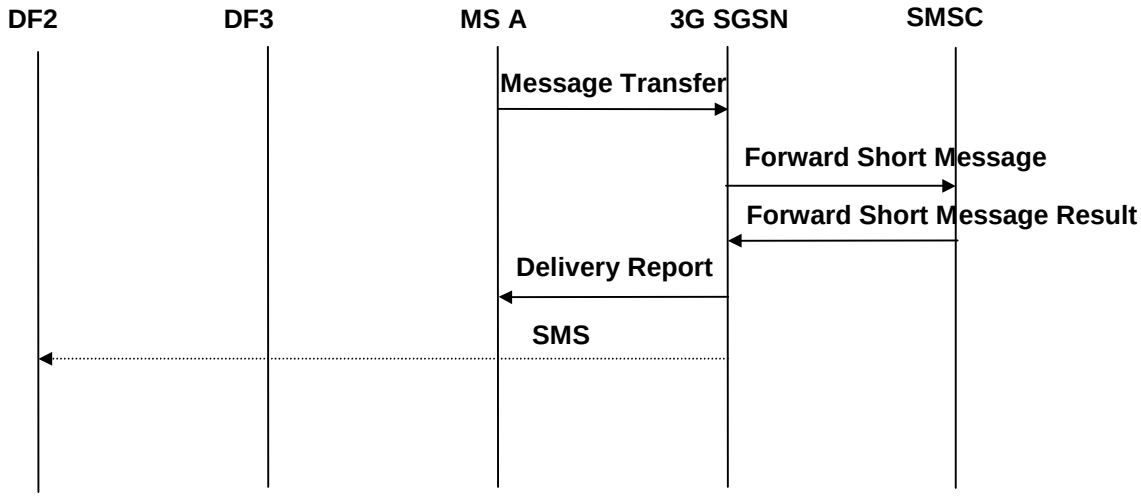


Figure B.10a: MO-SMS interception after 3G SGSN receives notification of SMS delivery from SMSC

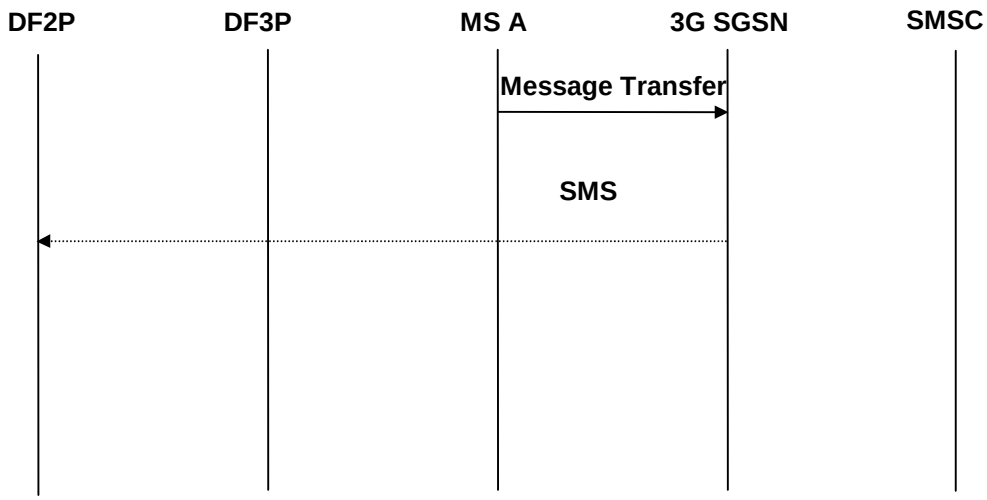


Figure B.10b: MO-SMS interception after 3G SGSN receives SMS from MS(A)

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

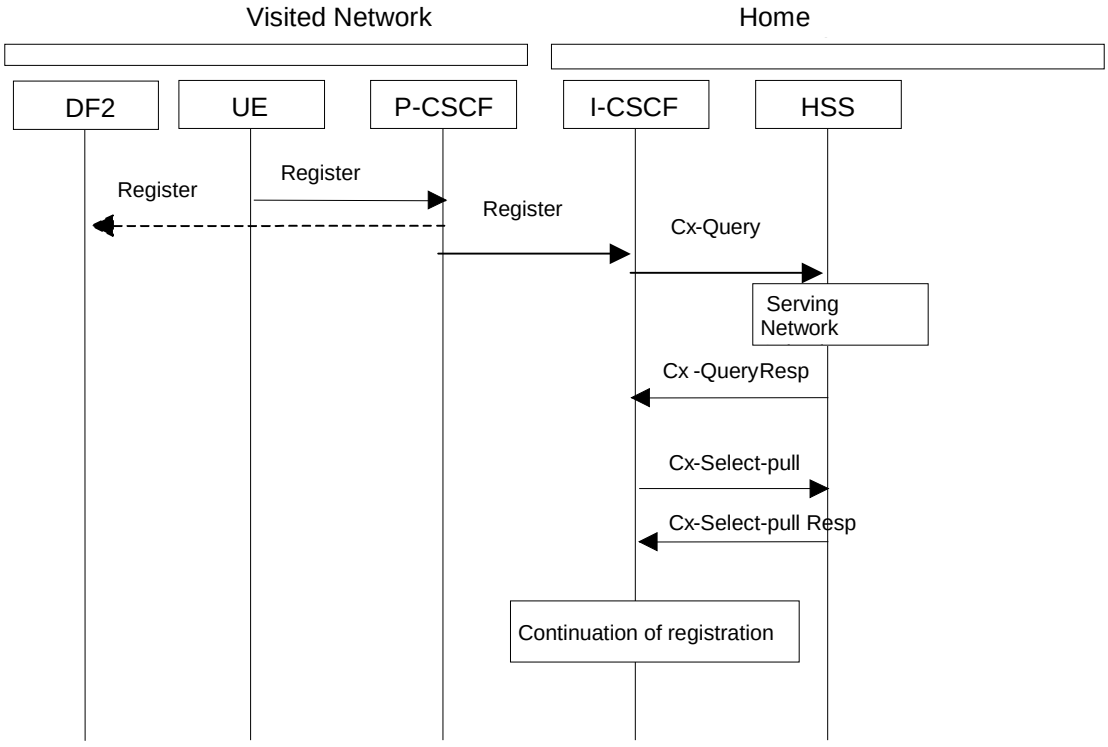
C.0 General

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 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 clauses 5.3.2.4 and 5.3.2.5).

Figure C.1.1: Intercept of Start of Multimedia Registration

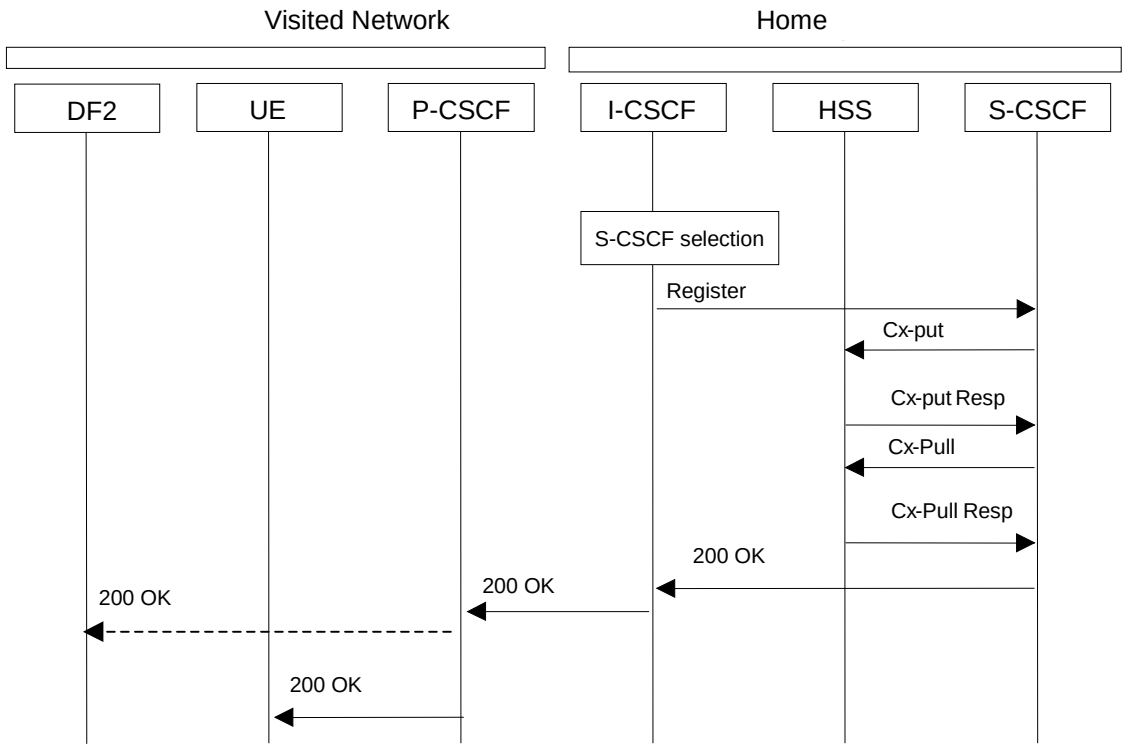


Figure C.1.2: Intercept of Continuation of Multimedia Registration

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 3G TS 23.228, clause 5.7.1).

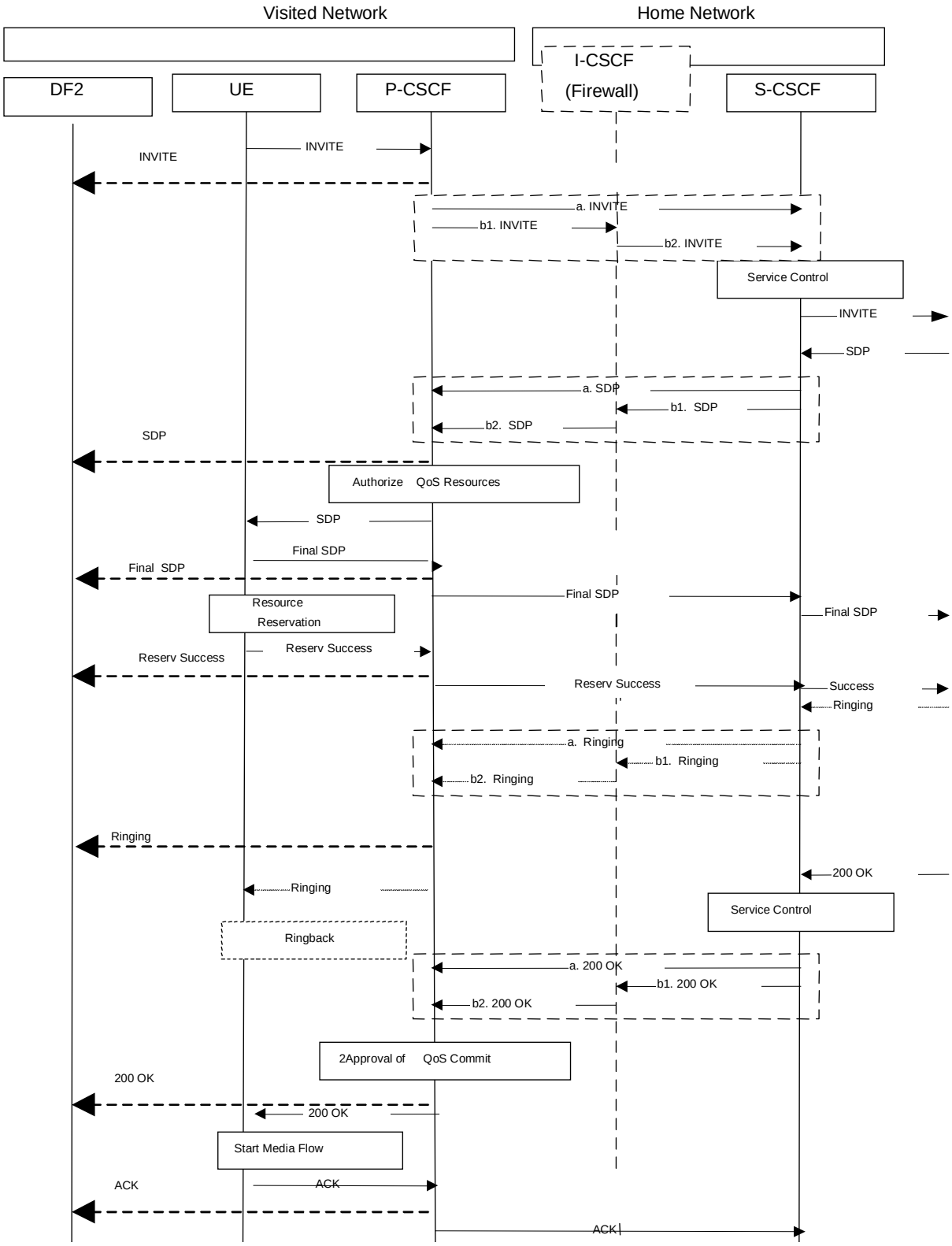


Figure C.2 Intercept of Multimedia Establishment and Answer at Visiting Network

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 (3G TS 23.228, clause C.2.1 reference available).

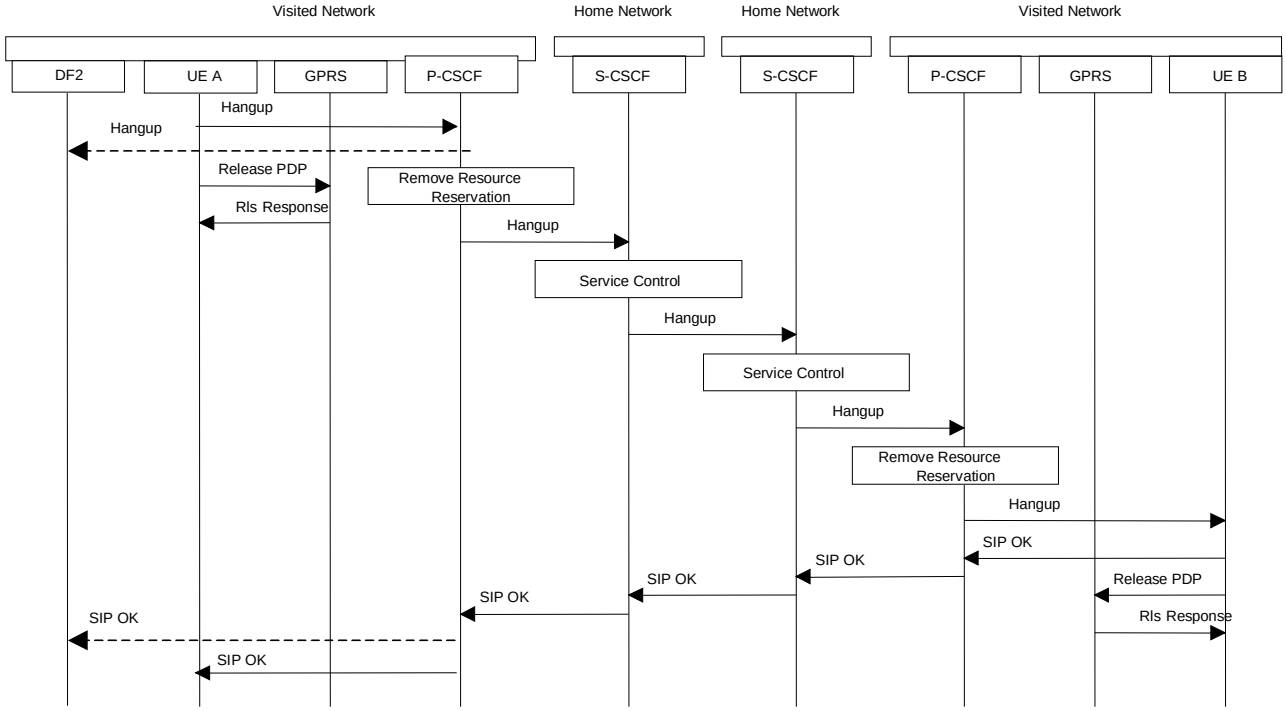


Figure C.3 Intercept of Multimedia Release at Visiting Network

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.

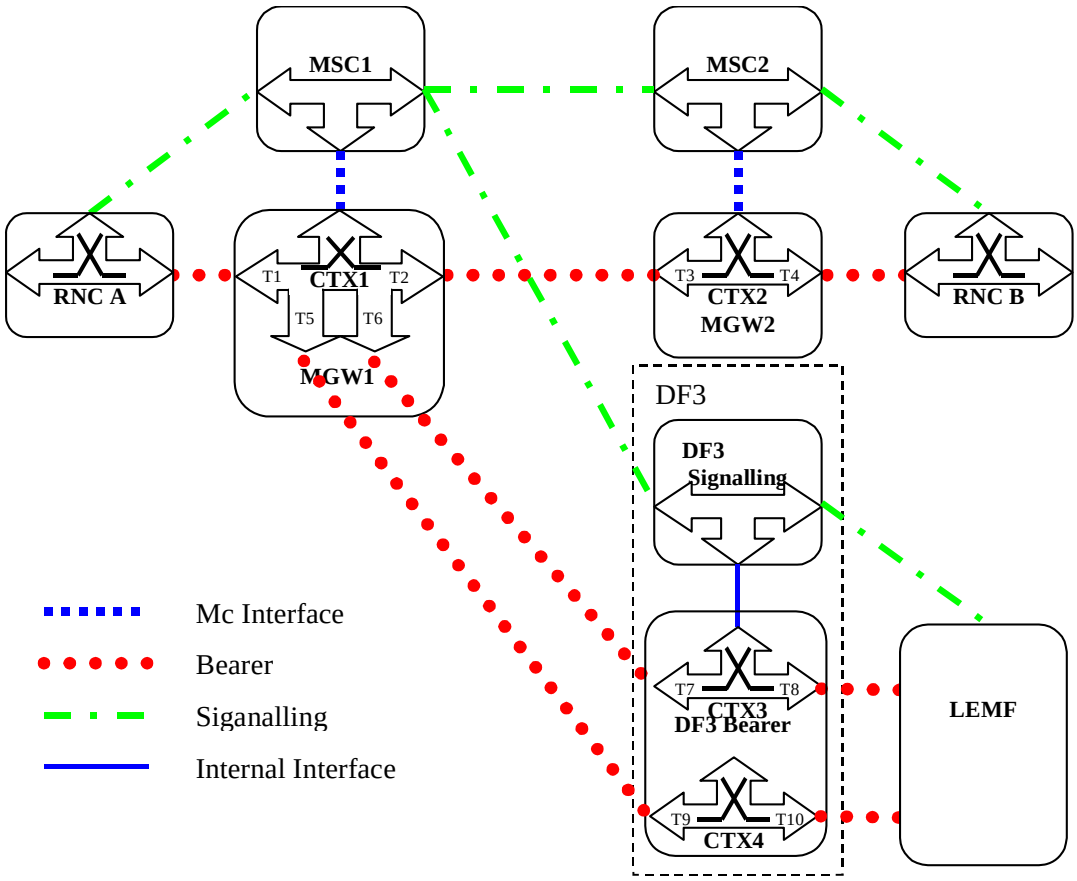


Figure D.1: Mobile to Mobile call originating side is target (network model)

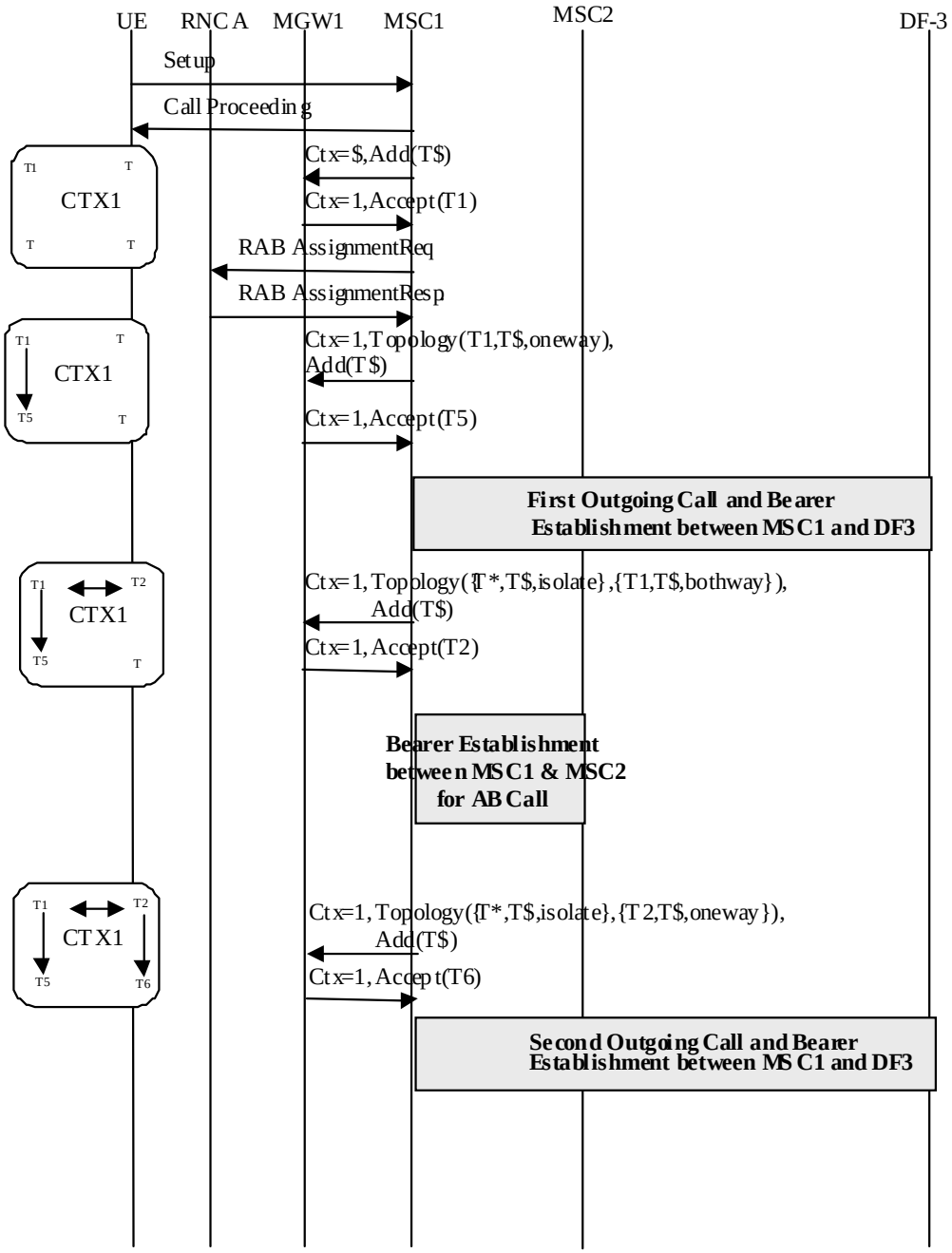


Figure D.2: Mobile to Mobile call originating side is target

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 3GPP 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 3GPP TS 29.334 [42]) or a PDN-GW (see 3GPP TS 23.401 [22] and 3GPP TS 402 [23]) or a GGSN (UMTS network).

Note 1: Even with the EPS-based access network, the media may 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 3GPP 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:

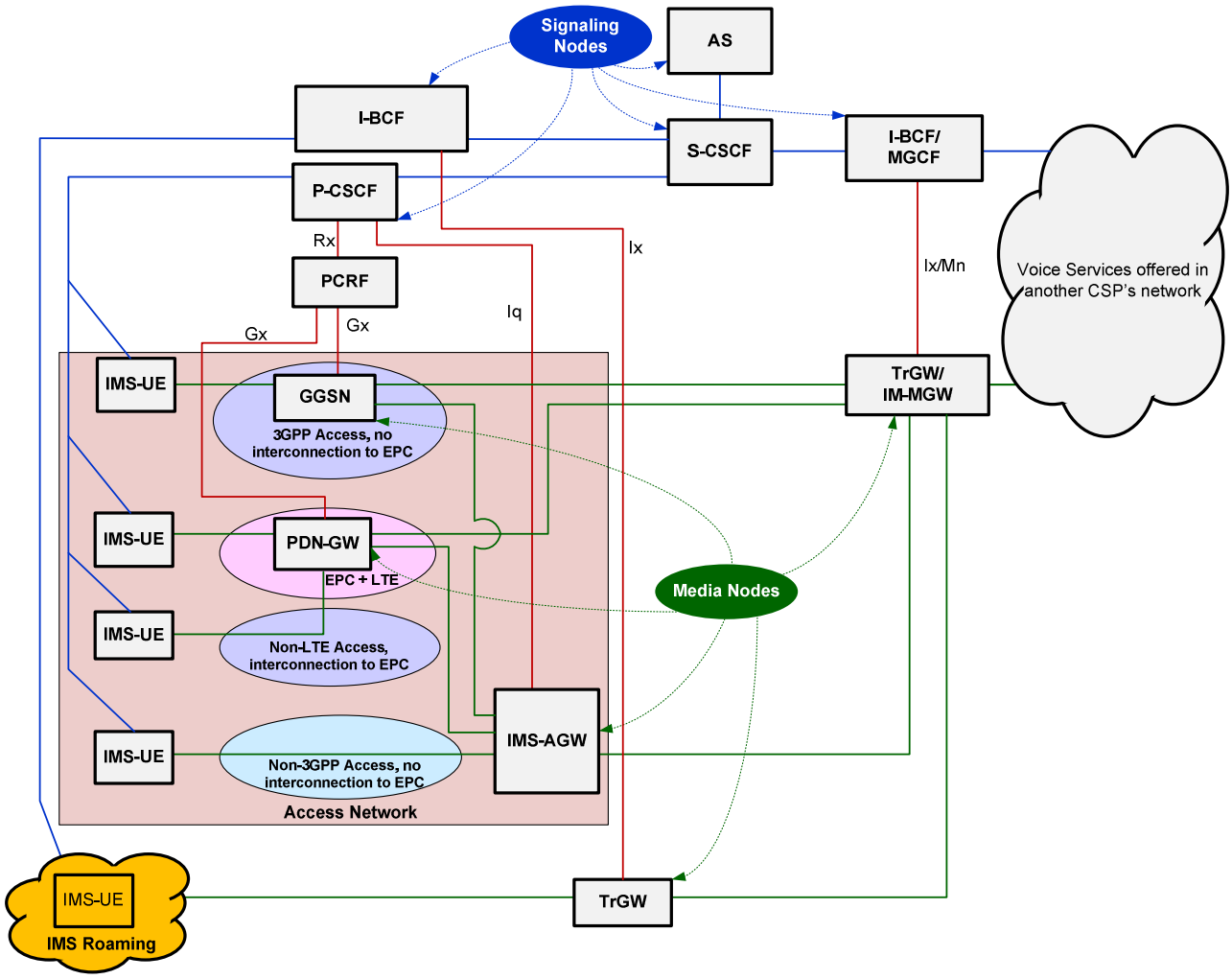


Figure E.1: IMS-based VoIP Configuration

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: In the remaining part of this informative annex, the PDN-GW/GGSN are shown in one box and should 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

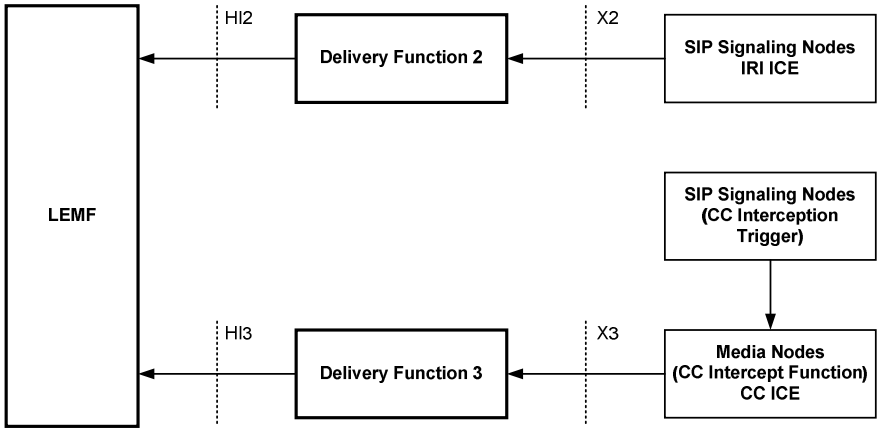


Figure E.2: General Principles of VoIP Interception

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.

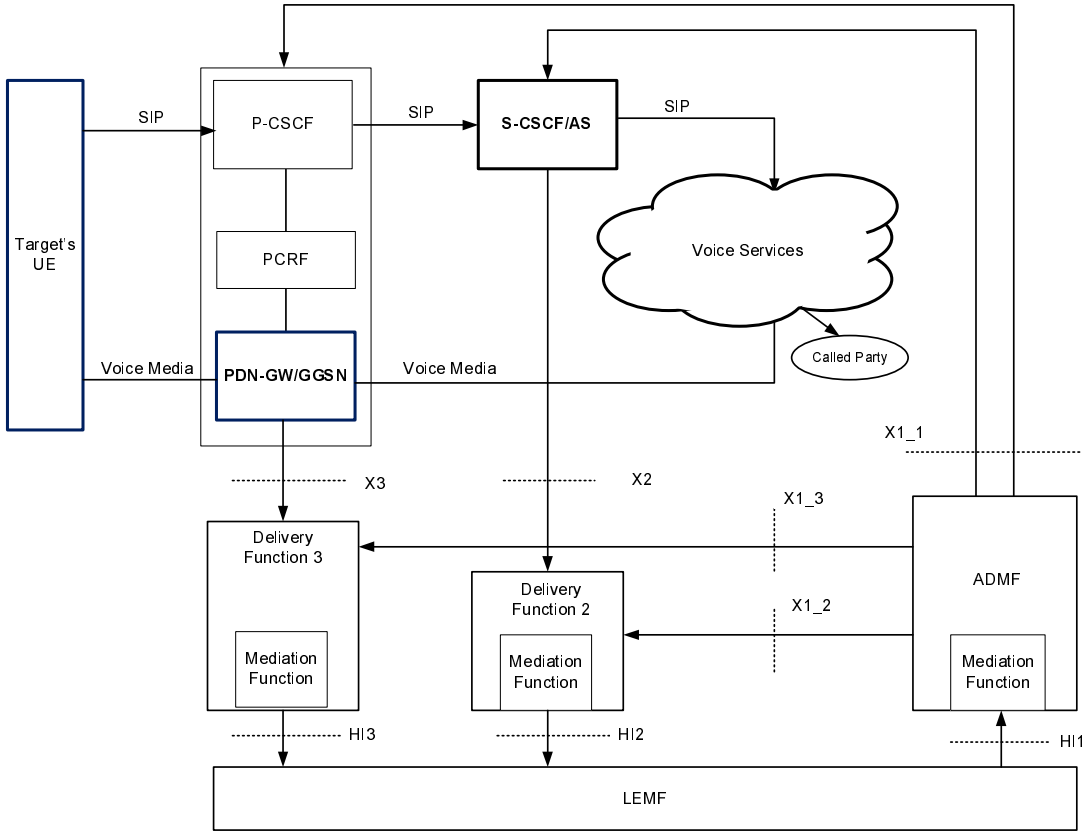


Figure E.3: VoIP lawful interception for an originating call with CC interception at the PDN-GW/GGSN

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 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 3GPP 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.

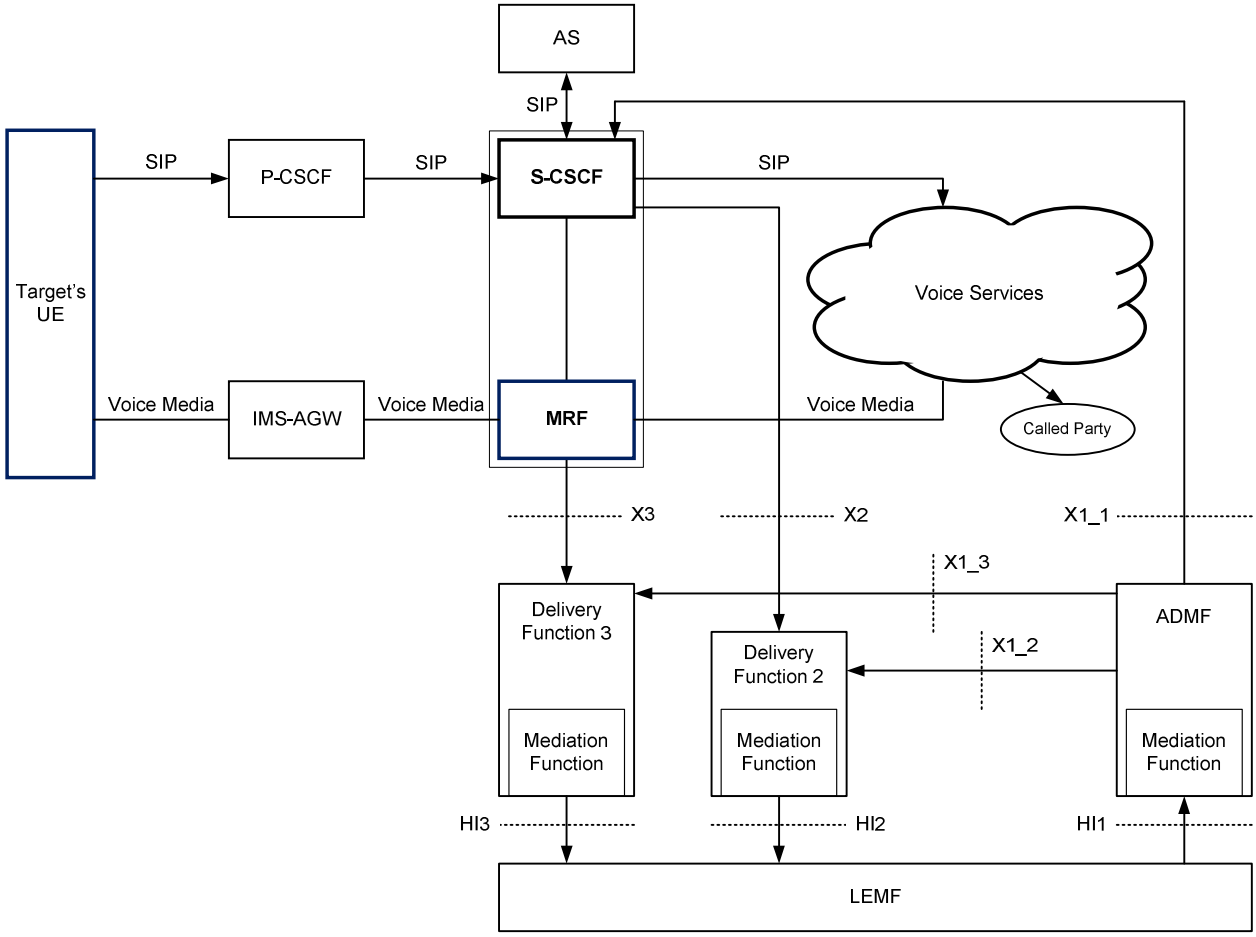


Figure E.3.1: VoIP lawful interception for an originating call with CC interception at the MRF

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 3GPP 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.

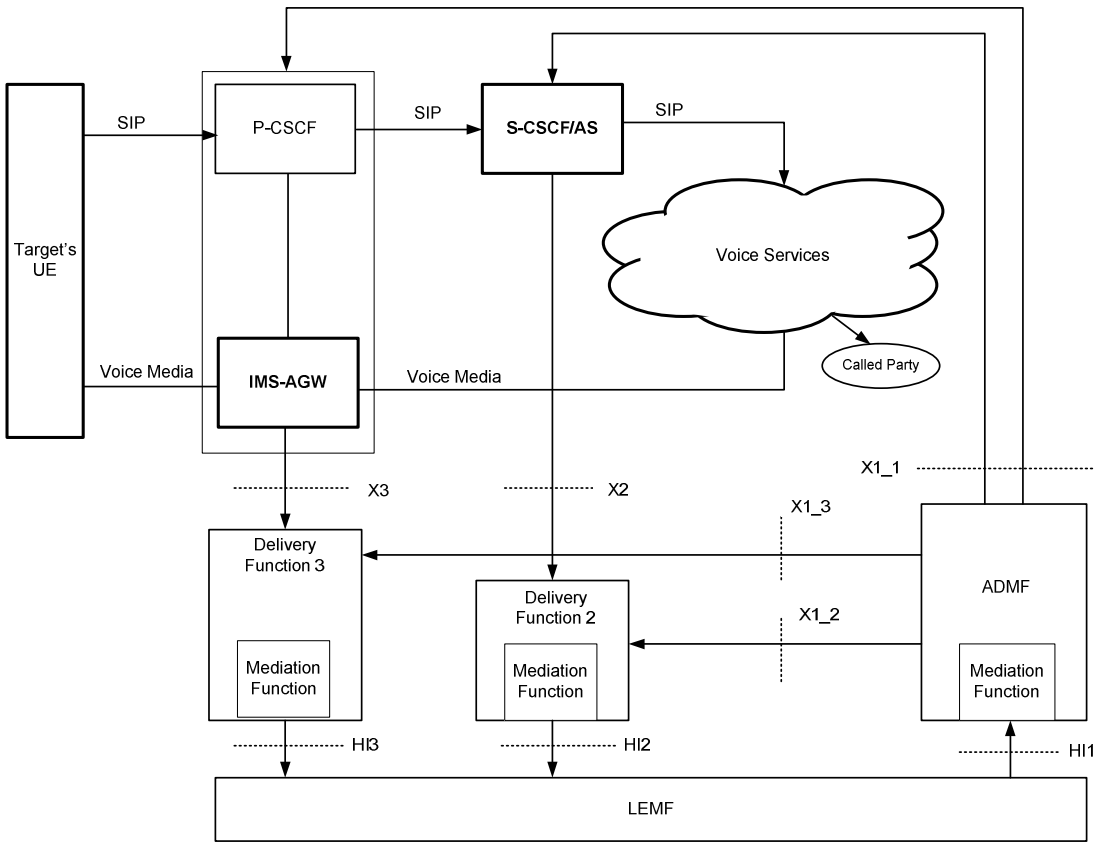


Figure E.4: VoIP lawful interception for an originating call with CC interception at the IMS-AGW

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 Z.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.

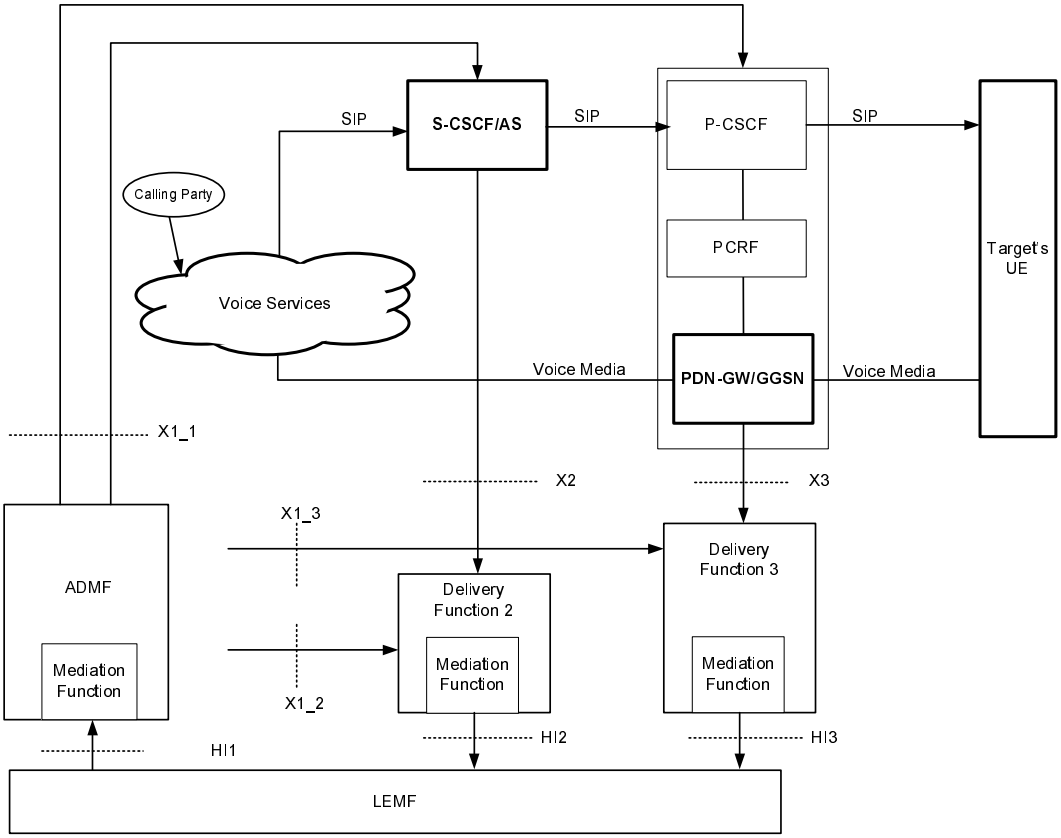


Figure E.5: VoIP lawful interception for a terminating call with CC interception at the PDN-GW/GGSN

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.

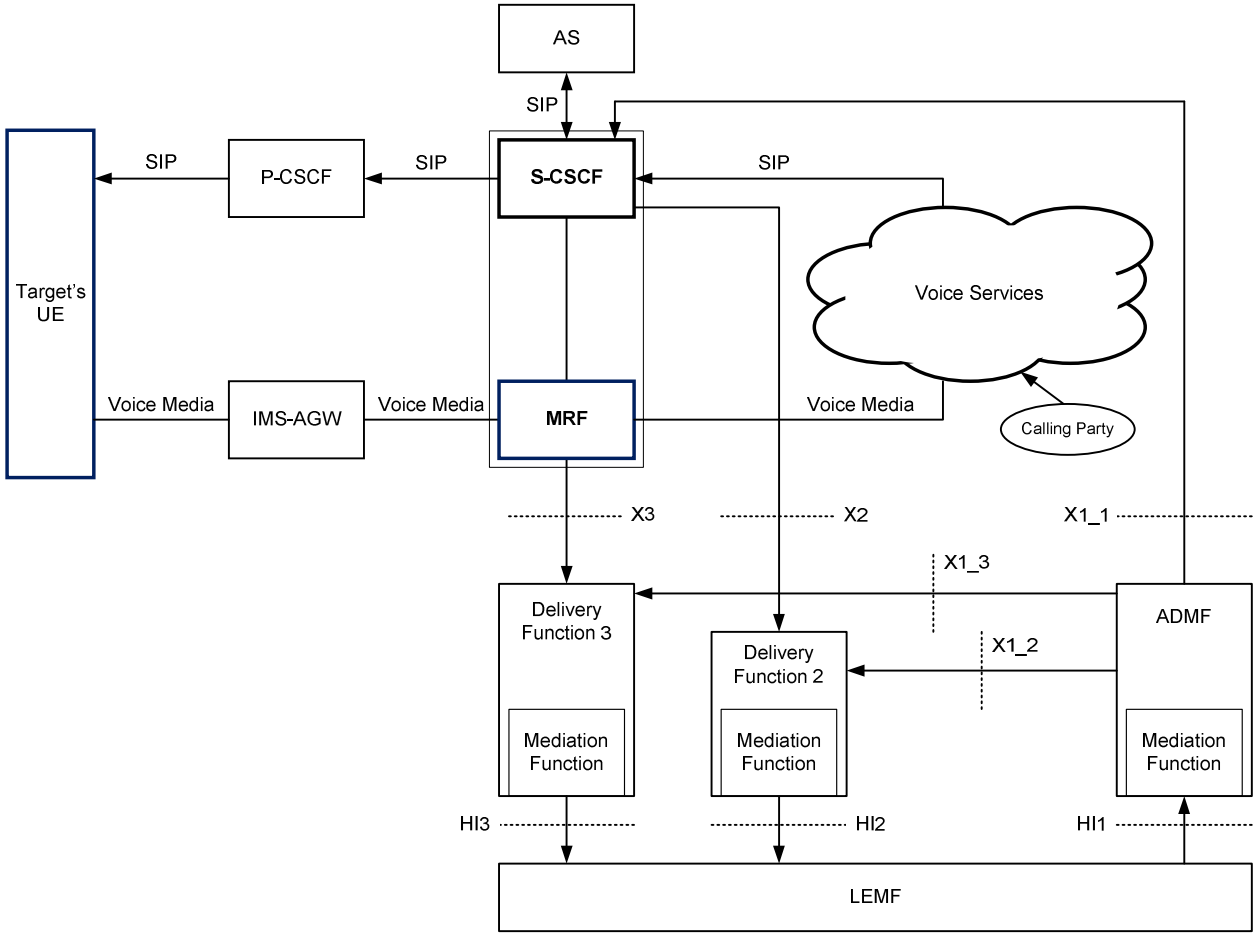


Figure E.5.1: VoIP lawful interception for a terminating call with CC interception at the MRF

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.

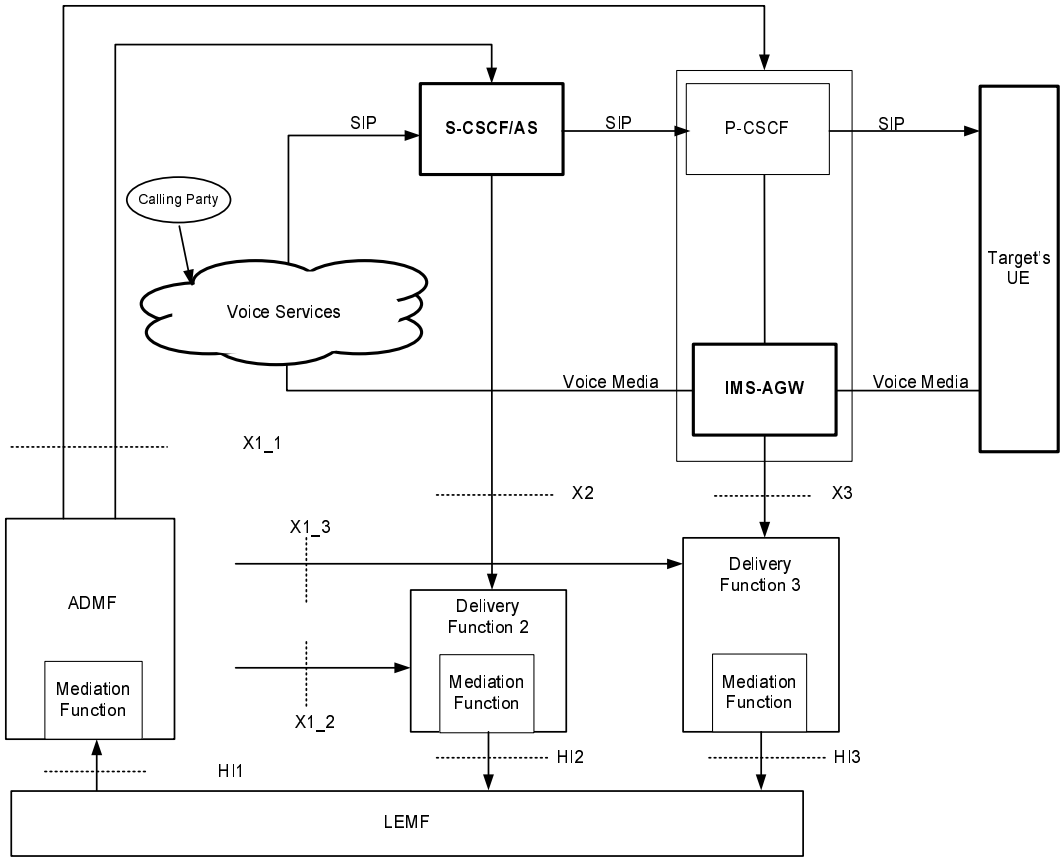


Figure E.6: VoIP lawful interception for a terminating call with CC interception at the IMS-AGW

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.

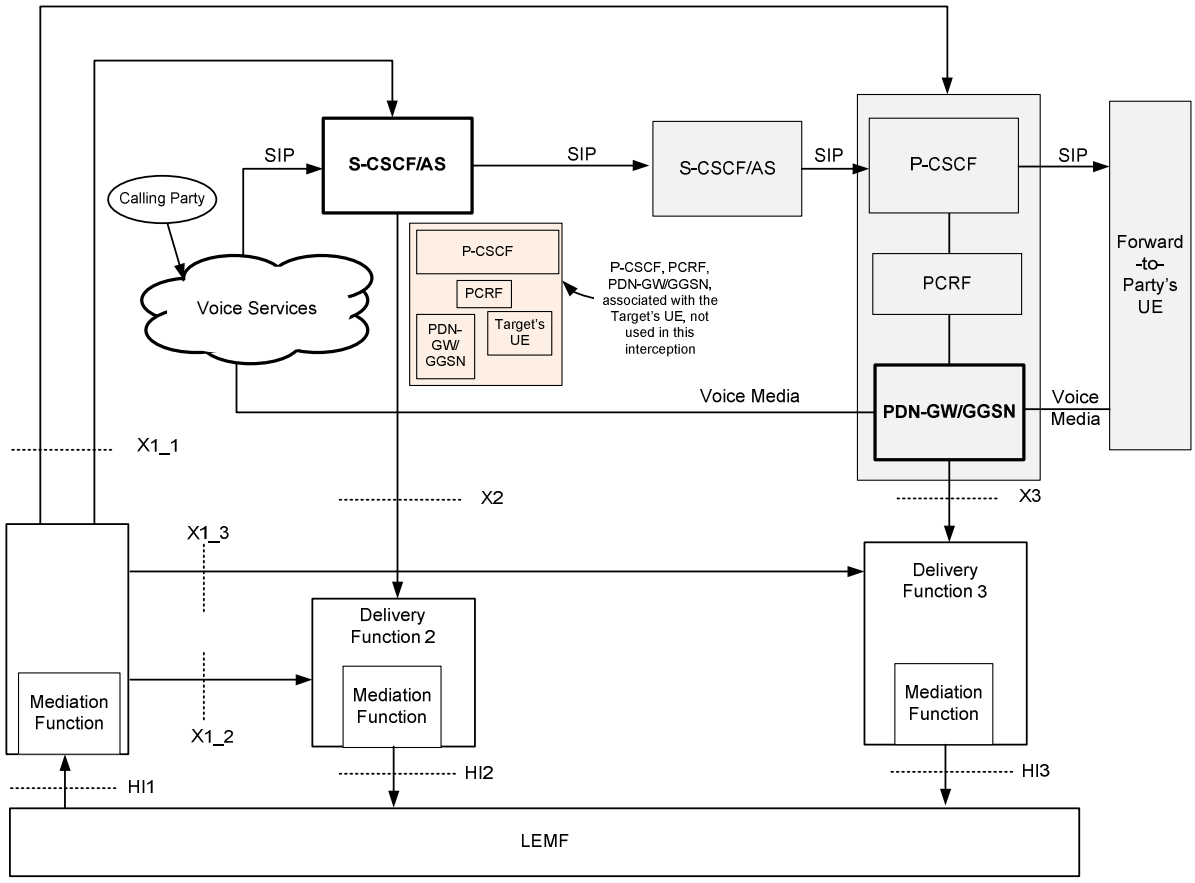


Figure E.7: VoIP lawful interception for an intra-CSP forwarded call with CC interception at the PDN-GW/GGSN

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.

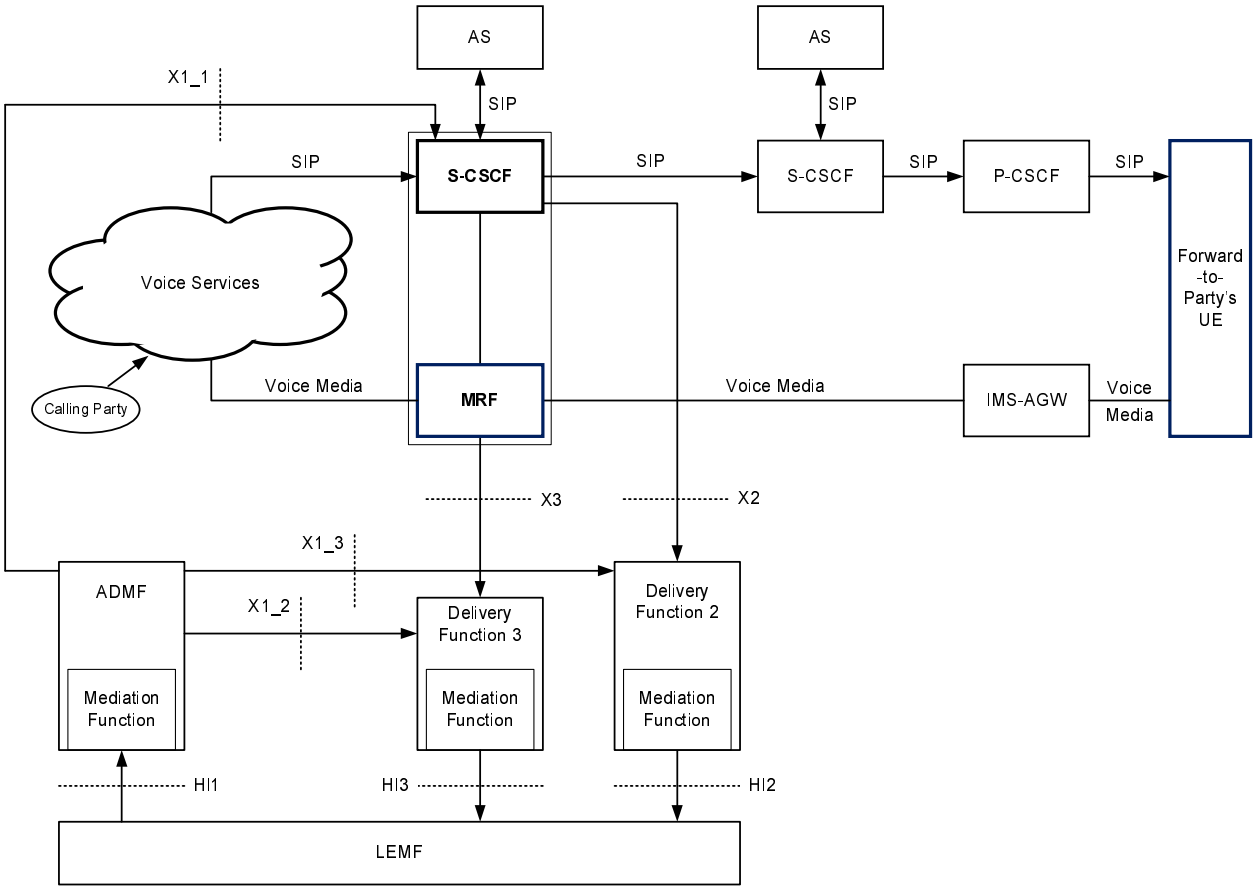


Figure E.7.1: VoIP lawful interception for an intra-CSP forwarded call with CC interception at the MRF

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.

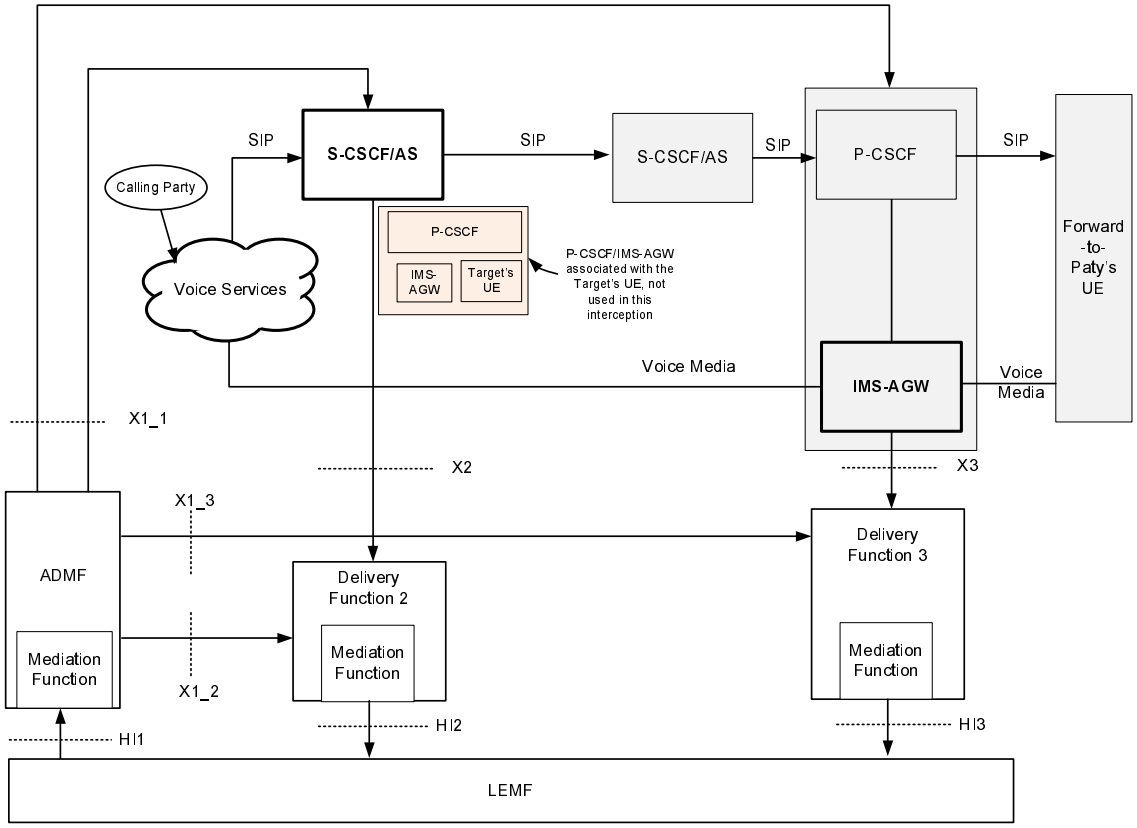


Figure E.8: VoIP lawful interception for an intra-CSP forwarded call with CC interception at the IMS-AGW

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.

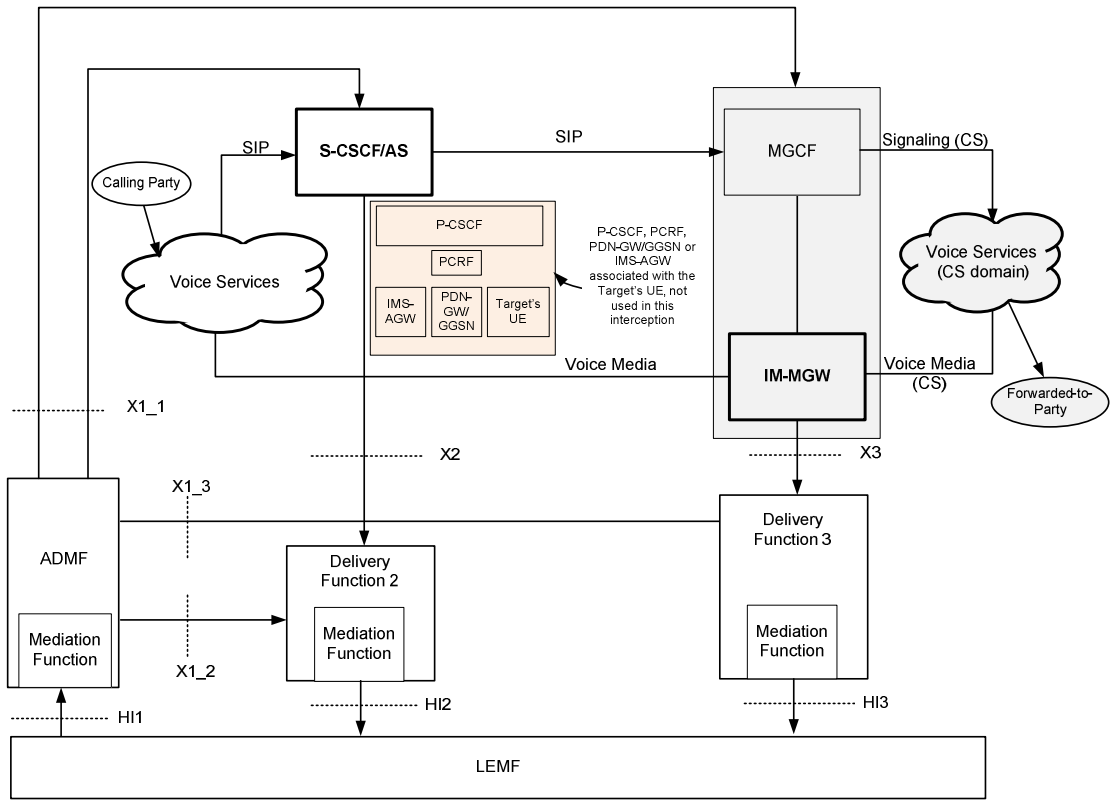


Figure E.9: VoIP lawful interception for an inter-CSP forwarded call to a CS Domain

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.

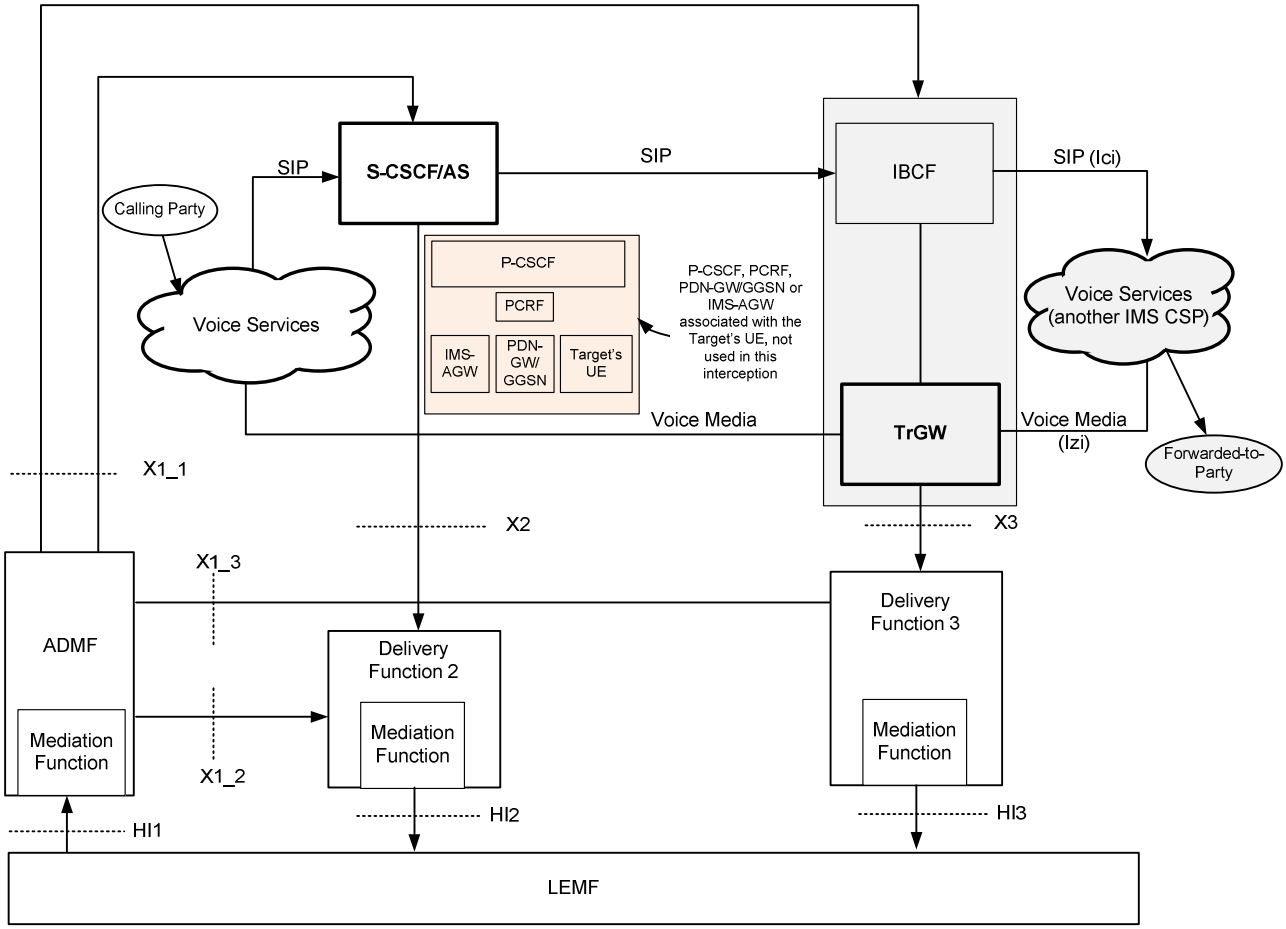


Figure E.10: VoIP lawful interception for an inter-CSP forwarded call to an IMS Domain

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.

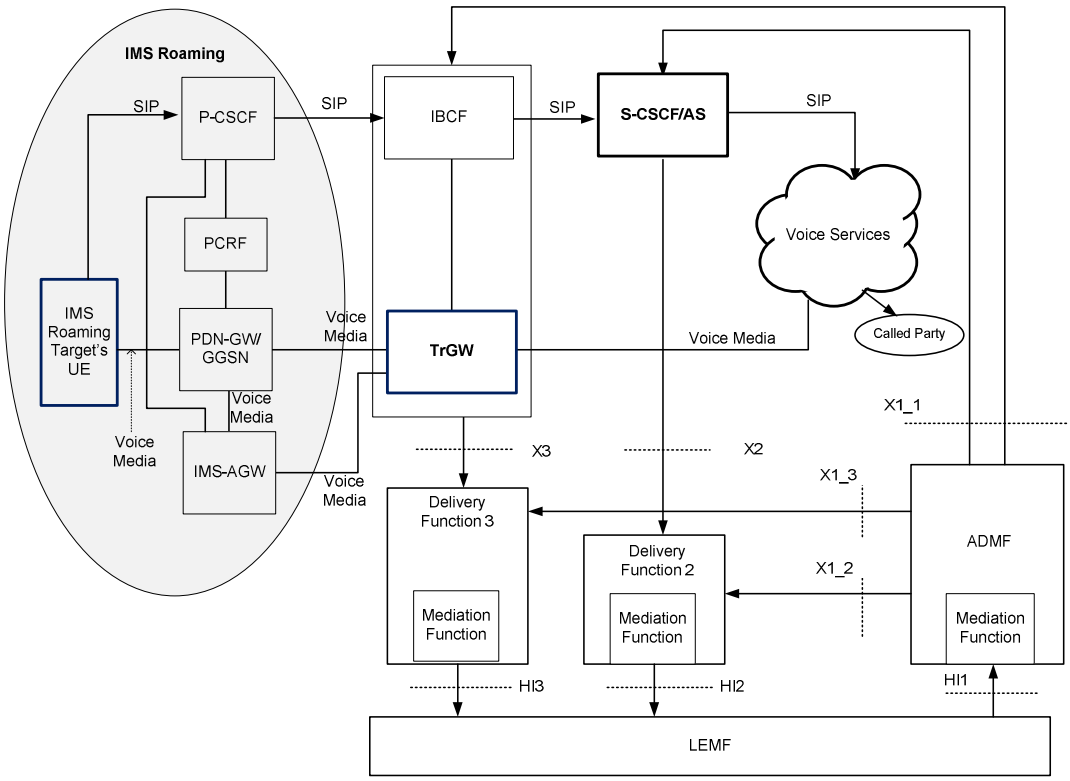


Figure E.11: VoIP lawful interception for an originating call with IMS Roaming

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).

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.

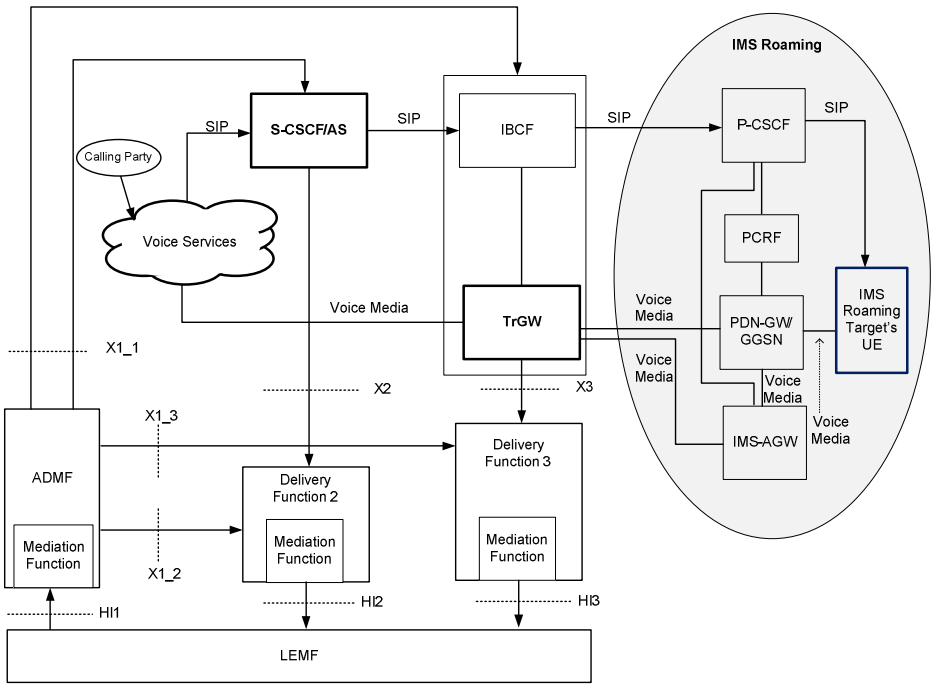


Figure E.12: VoIP lawful interception for a terminating call with IMS Roaming

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 subscriber may or may not be IMS roaming.

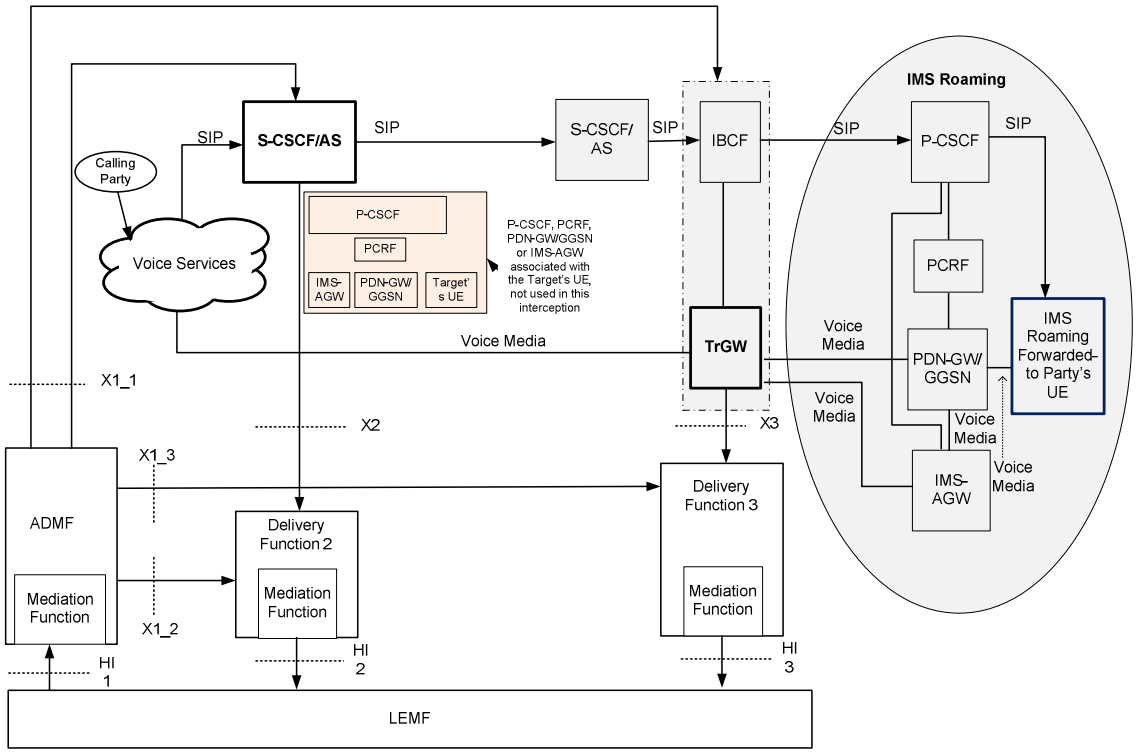


Figure E.13: VoIP lawful interception for a intra-CSP forwarded call with IMS Roaming

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: 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).

Annex F (Informative) Examples of IMS-based VoIP Lawful Interception 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

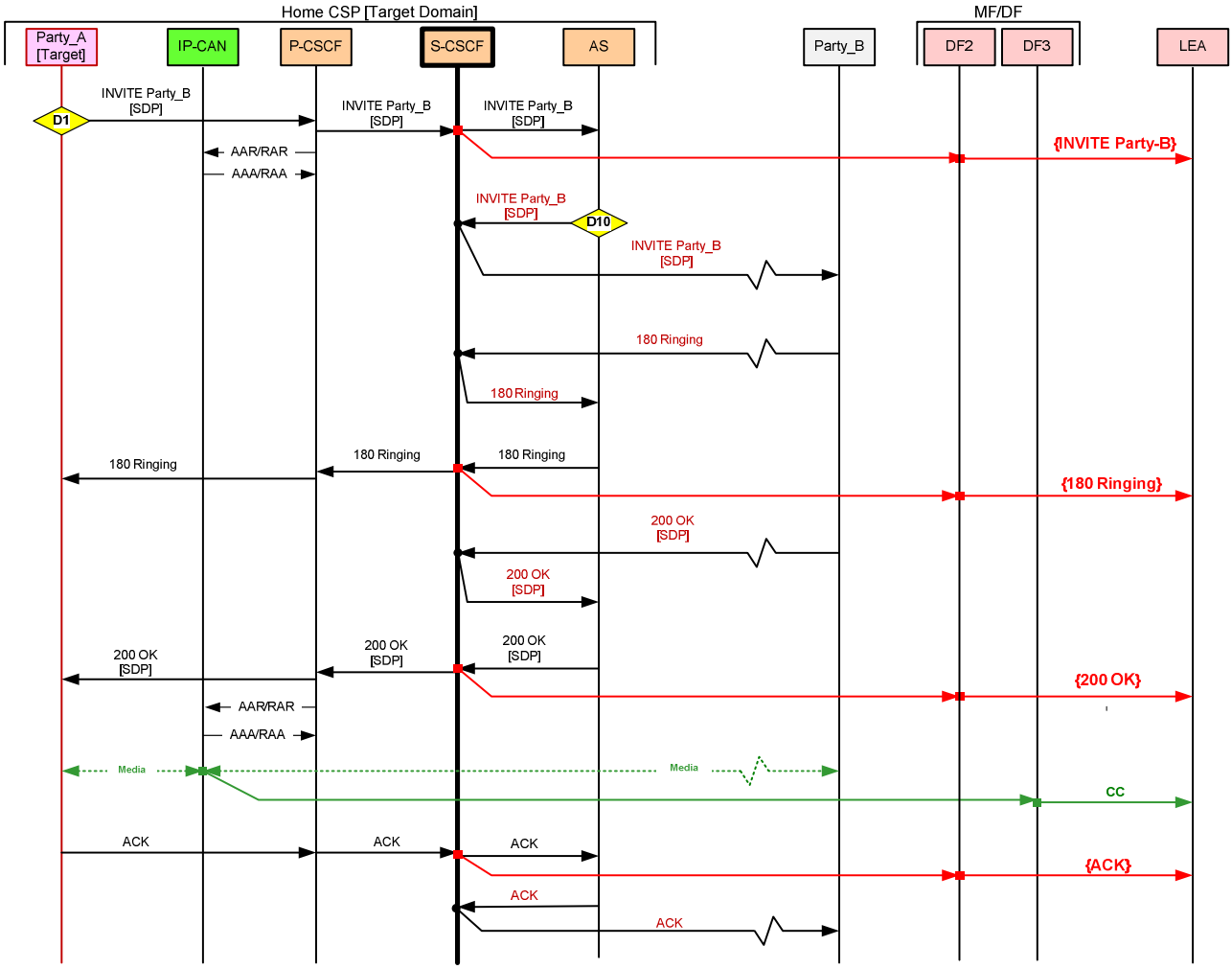


Figure F.1: Target originated call – target calls Party_B

F.2.2 Target Originated Call – Target (Party_A) dials a Special Number

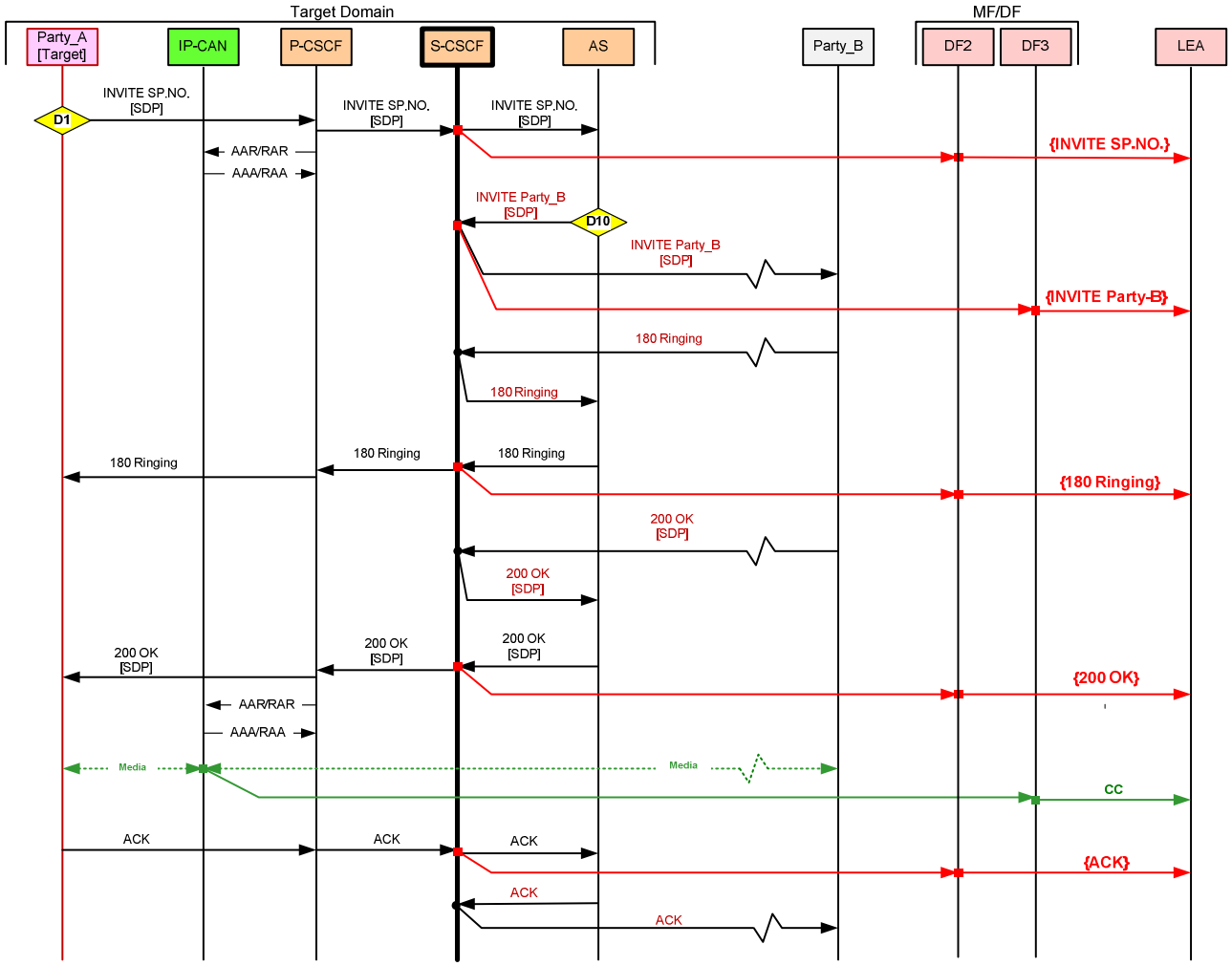


Figure F.2: Target originated call – target dials a special number

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).

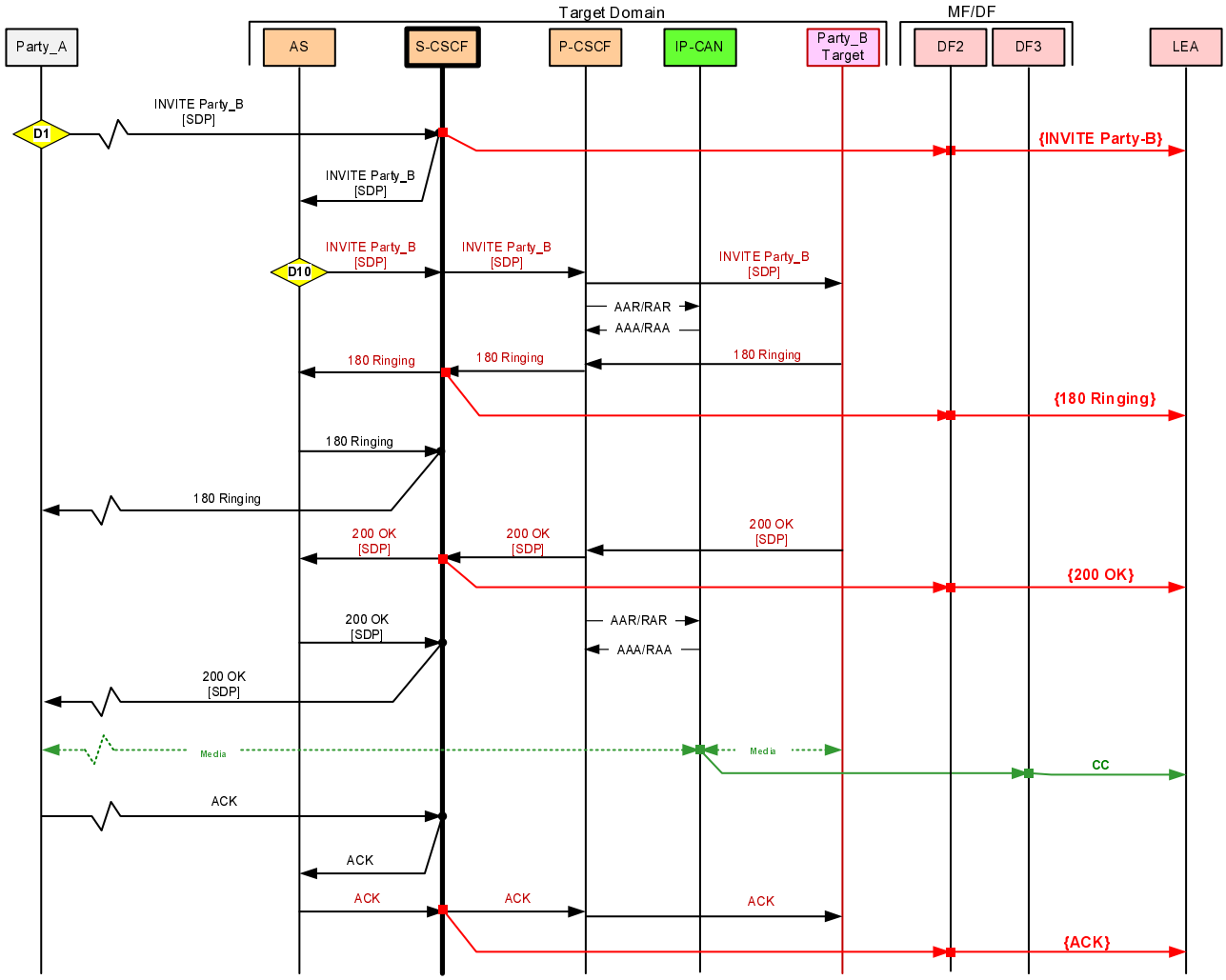


Figure F.3: Target receives an incoming call.

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

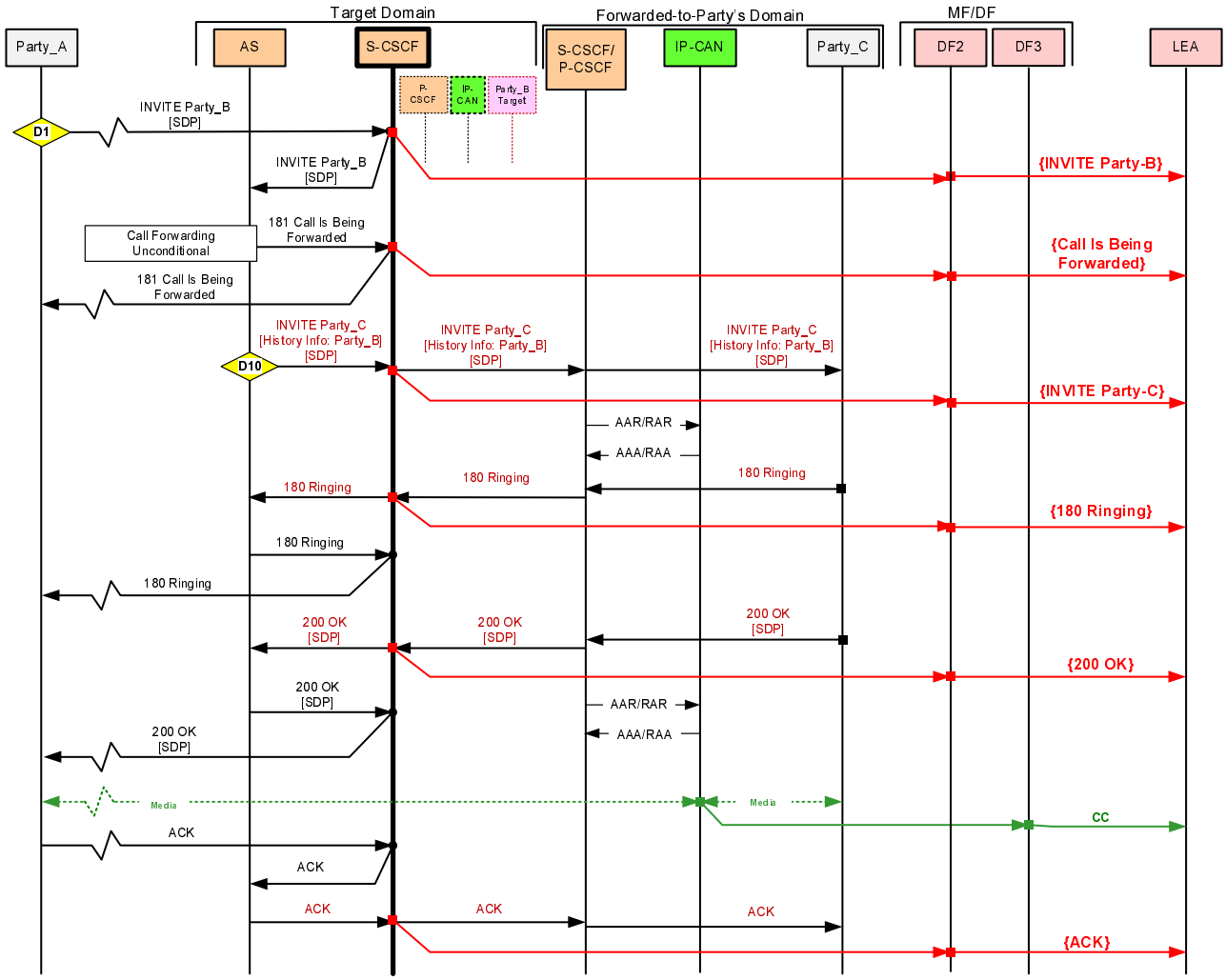


Figure F.4: Incoming call to target is forwarded within the CSP

F.4.2 Intra-CSP Call Forwarding No Answer

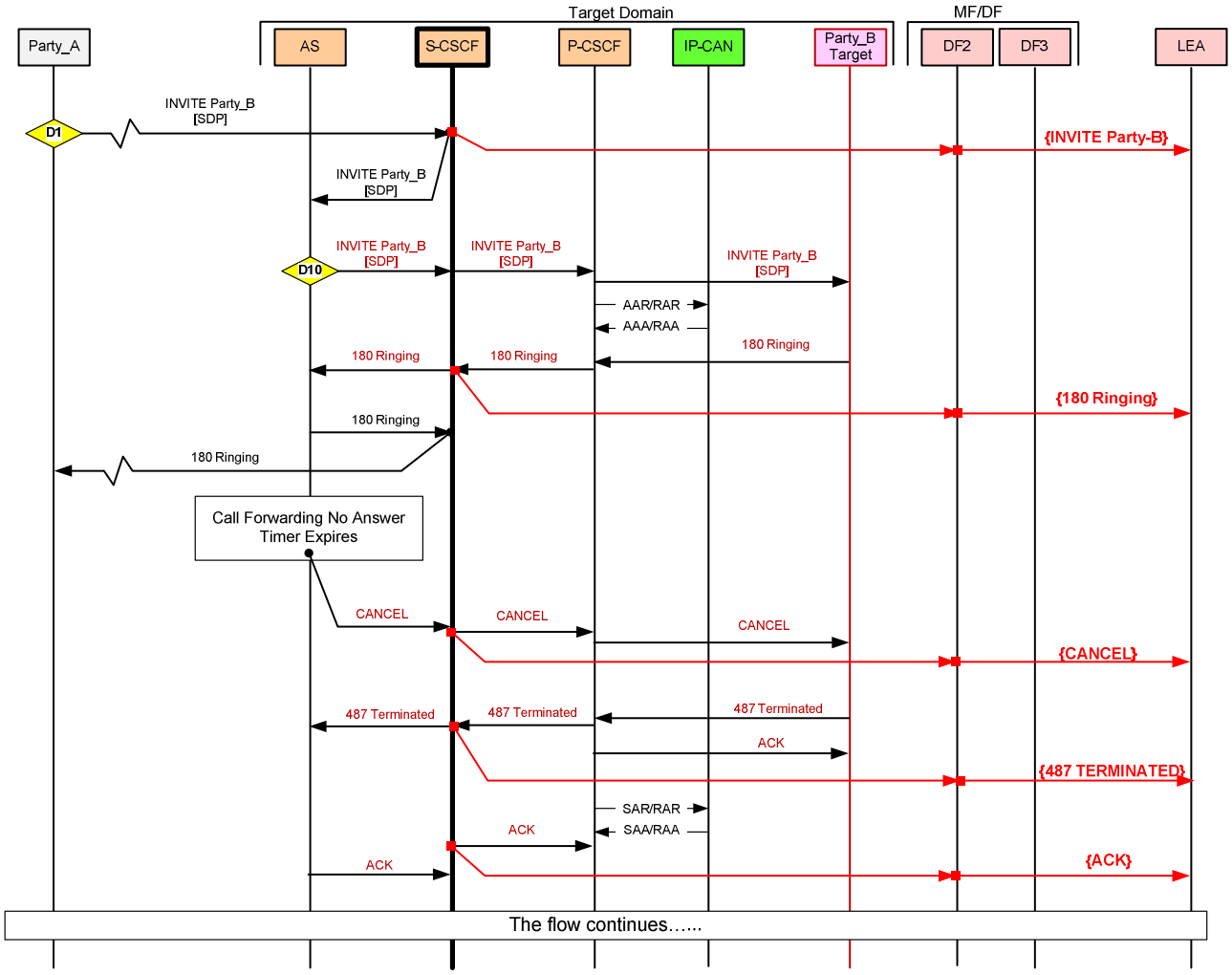


Figure F.5: Incoming call to target is forwarded due to call forwarding no answer within the CSP (flow 1 of 2)

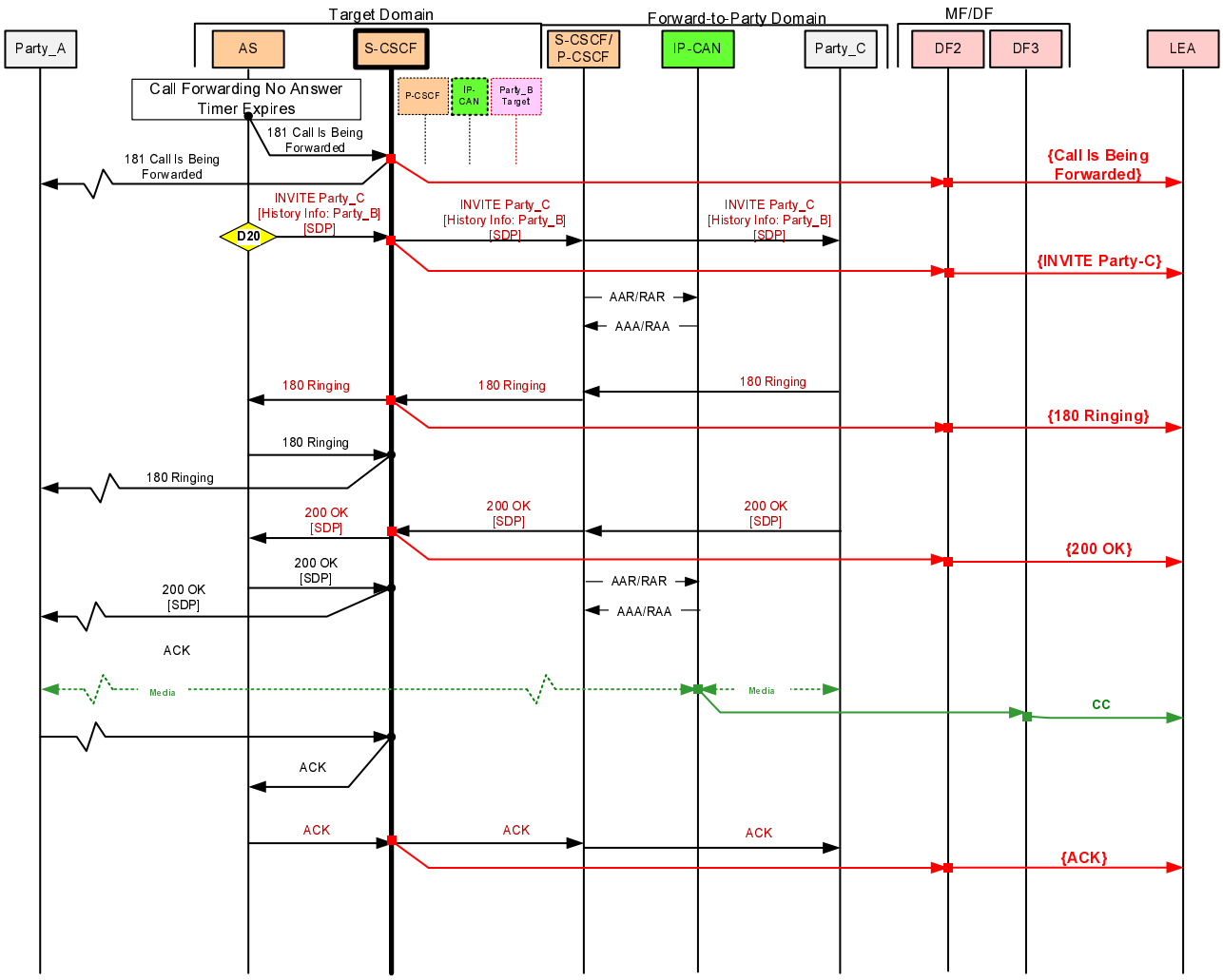


Figure F.6: Incoming call to target is forwarded due to call forwarding no answer within the CSP (flow 2 of 2)

F.4.3 Inter-CSP Call Forwarding Unconditional

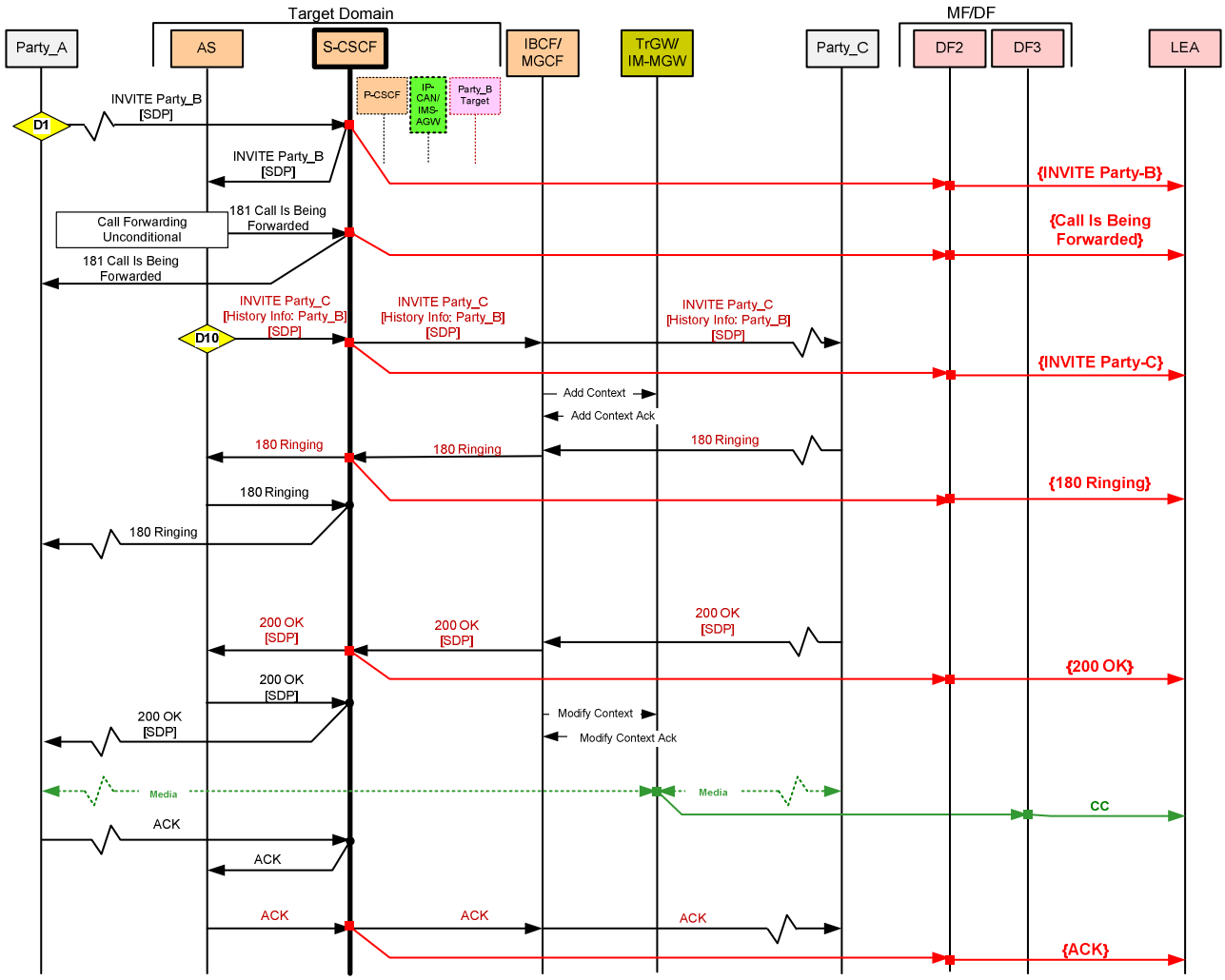


Figure F.7: Incoming call to target is forwarded outside the CSP

F.5 IMS Roaming

F.5.0 General

This clause gives 2 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.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

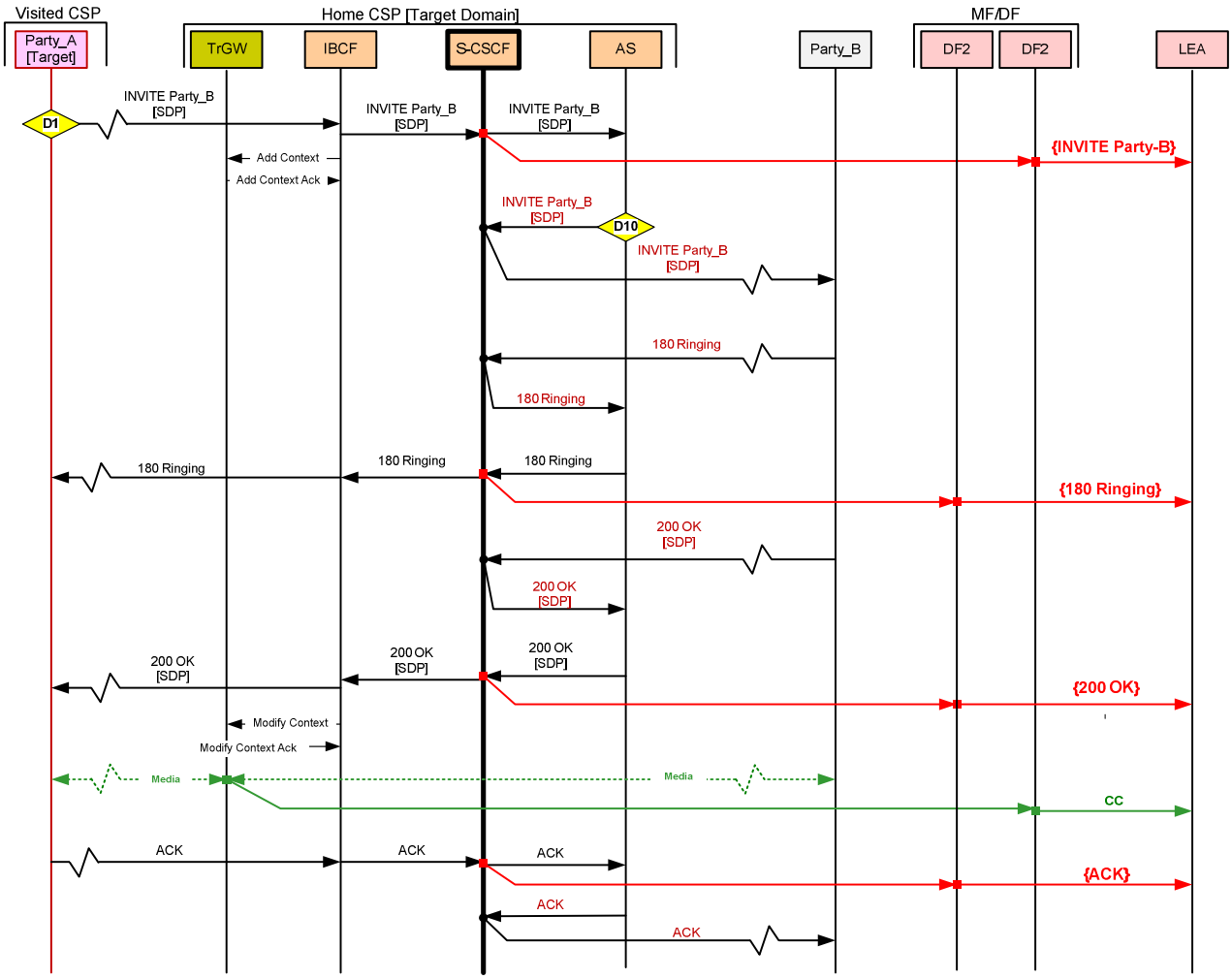


Figure F.8: Roaming target originates a call

F.5.2 Call Termination to a Roaming Target

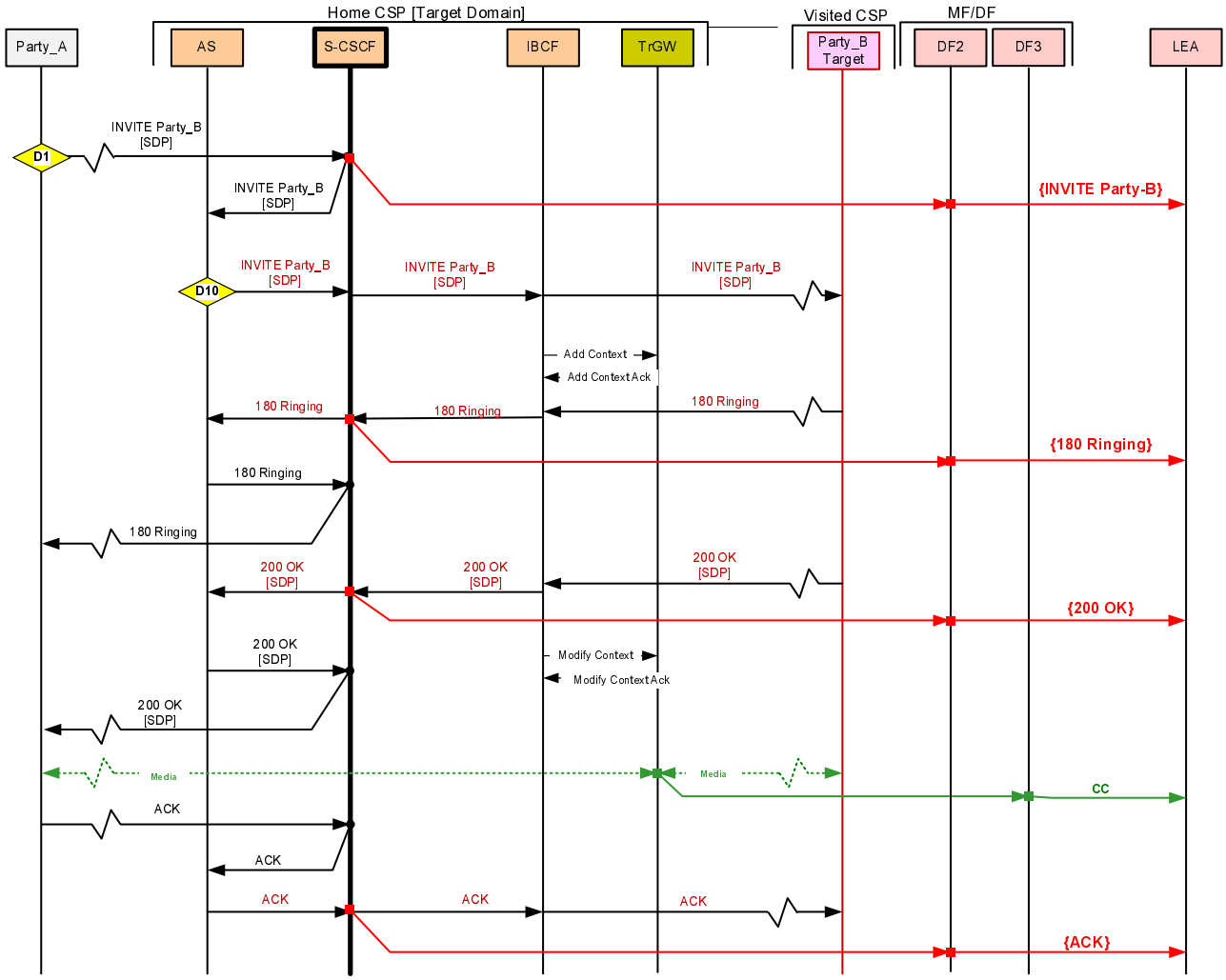


Figure F.9: Roaming target receives an incoming call.

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

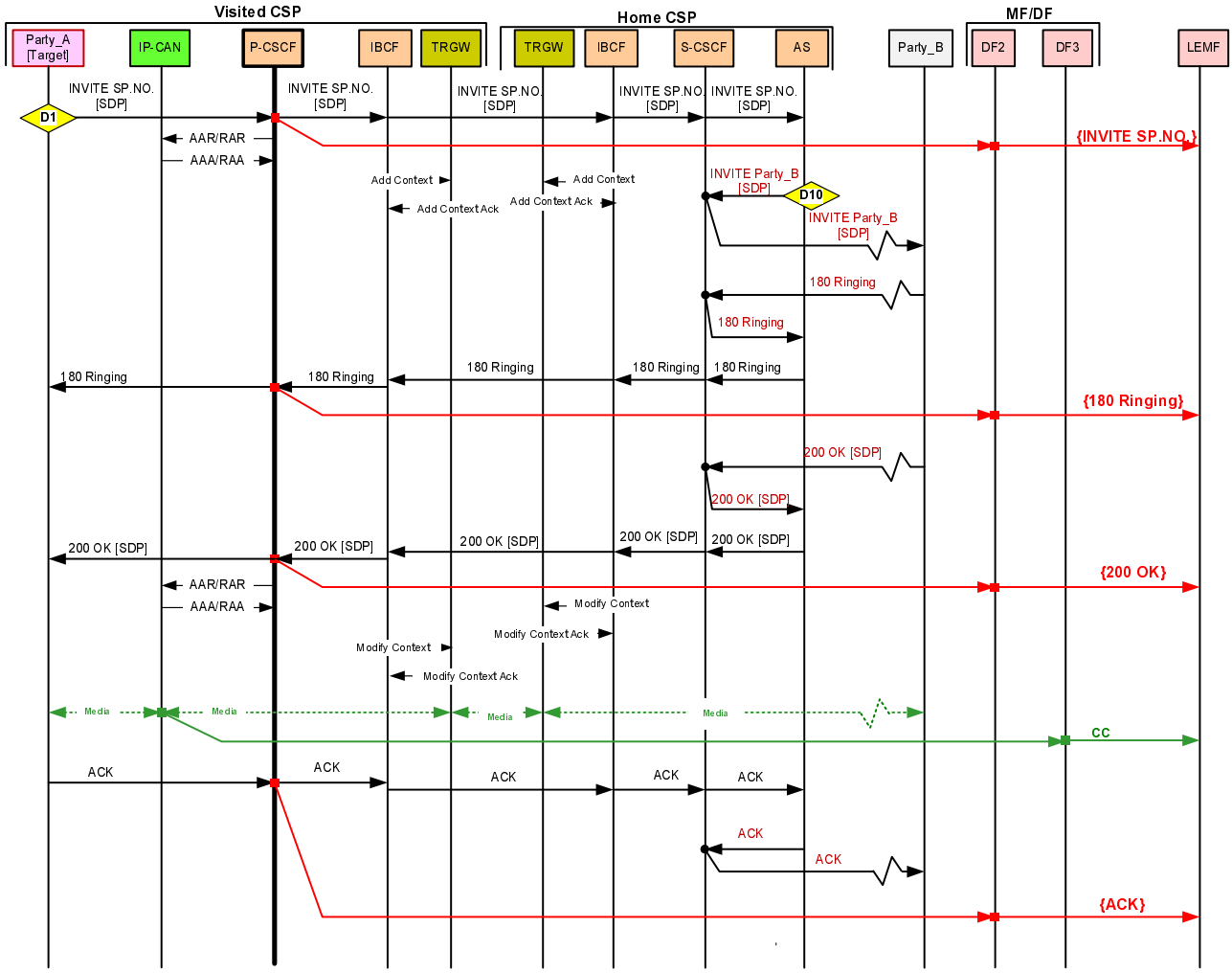


Figure F.10: Roaming target originates a call – interception in the visited CSP

F.6.2 Interception in Visited CSP – Target Terminating Calls.

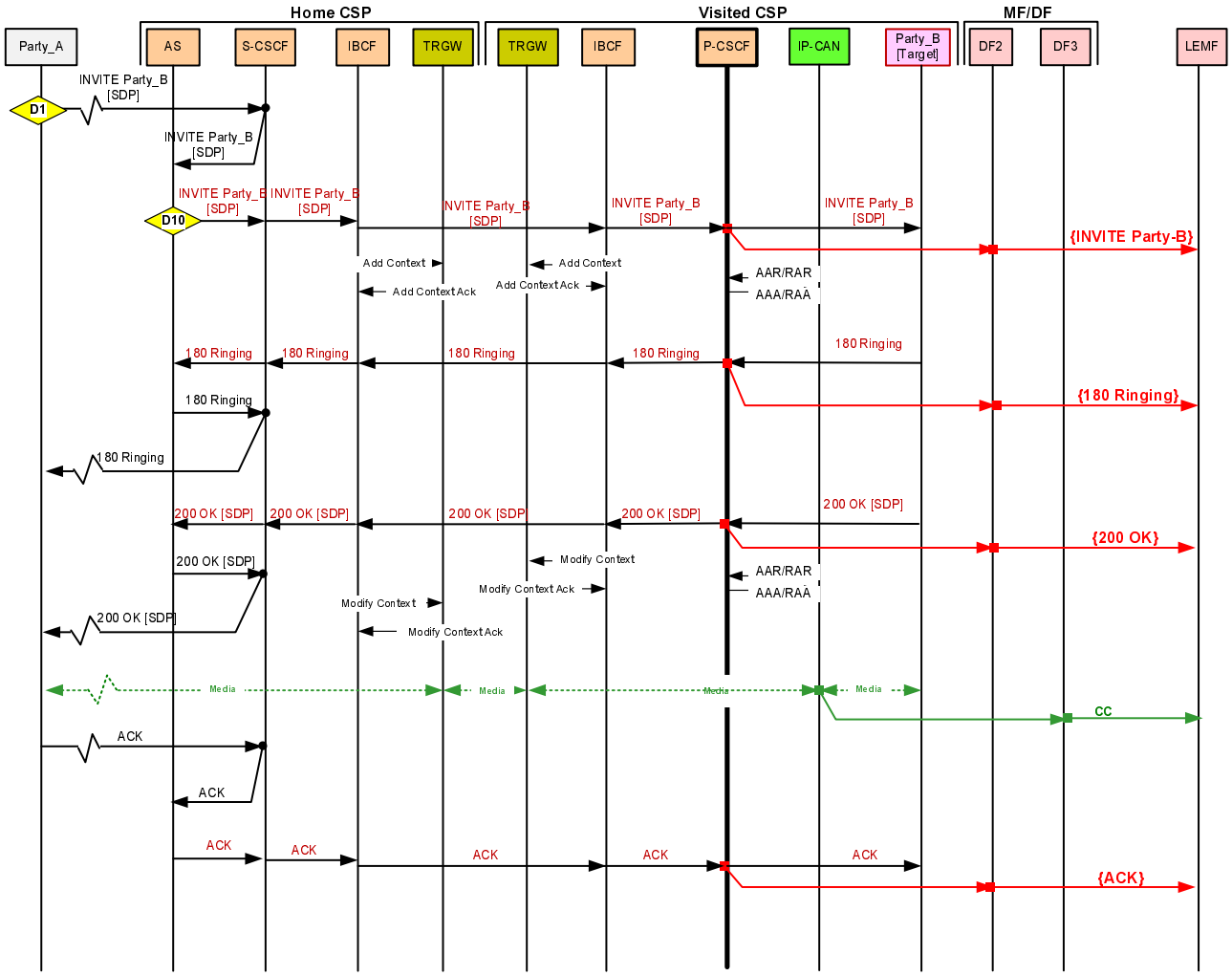


Figure F.11: Roaming target receives a call – interception in the visited CSP.

F.6.3 Incoming Call to Roaming Target is forwarded due to Call Forwarding No Answer

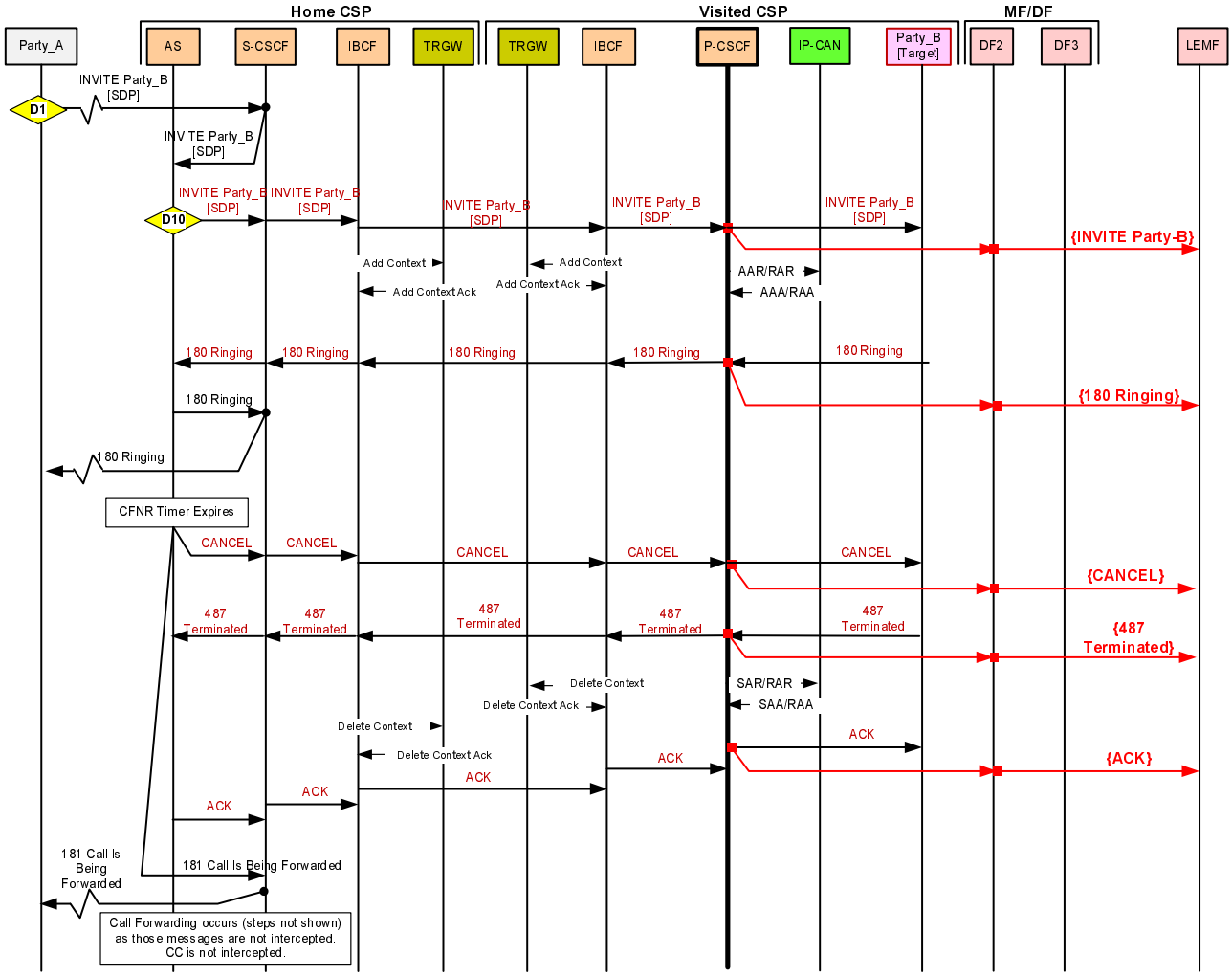


Figure F.12: Incoming call to target is forwarded in the home CSP due to Call Forwarding No Answer – interception in visited CSP.

Annex G (informative): Change history

Change history									
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New	WI
	SA_03			-		Approved at SA#6 and placed under TSG SA Change Control	1.0.0	3.0.0	
	SA_10	SP-000625	0001	-		Addition of parameters to the X3-Interface	3.0.0	3.1.0	Security
2000-03	SP-11	SP-010137	0002	-		Correction of Location information parameters in interception event records	3.1.0	3.2.0	Security
2000-03	SP-11	SP-010146	0003	-		Update of TS 33.107 for Release 4 - Inclusion of PS LI requirements	3.1.0	4.0.0	Security
2000-06	SP-12	SP-010374	0004	1	B	Update of TS 33.107 for Release 5	4.0.0	5.0.0	SEC1-LI
2001-12	SP-14	SP-010612	0010	-	A	Start of secondary interception of an active PDP context	4.1.0	5.1.0	SEC1-LI
2001-12	SP-14	SP-010613	0011	-	C	Alignment of TS 33.107 for Release 5 Network Architecture	4.1.0	5.1.0	SEC1-LI
2001-12	SP-14	SP-010614	0014	-	A	Correct the MO-SMS and MT-SMS events	4.1.0	5.1.0	SEC1-LI
2001-12	SP-14	SP-010615	0016	-	A	Source of PDP context initiation	4.1.0	5.1.0	SEC1-LI
2002-03	SP-15	SP-020109	0017	-	B	PDP context Deactivation cause	5.1.0	5.2.0	SEC1-LI
2002-03	SP-15	SP-020110	0018	-	B	The use of H.248 in setting up a bearer intercept point at the MGW	5.1.0	5.2.0	SEC1-LI
2002-03	SP-15	SP-020111	0021	-	B	Inter-SGSN RA update with active PDP context	5.1.0	5.2.0	SEC1-LI
2002-03	SP-15	SP-020112	0022	-	B	Addition of PDP context modification Event and Transferring the QoS information element across the X2 interface	5.1.0	5.2.0	SEC1-LI
	-	-	-	-	-	Change History new version corrected for SP-15 CRs	5.2.0	5.2.1	SEC1-LI
2002-06	SP-16	SP-020345	0023	-	B	Changes to 33.107 to support interception at a GGSN	5.2.1	5.3.0	SEC1-LI
2002-06	SP-16	SP-020345	0024	-	B	Addition of SMS type information	5.2.1	5.3.0	SEC1-LI
2002-06	SP-16	SP-020345	0025	-	C	Inclusion of Serving System IRI in TS 33.107	5.2.1	5.3.0	SEC1-LI
2002-09	SP-17	SP-020511	0026	-	F	Essential clarification to the Timestamp IE	5.3.0	5.4.0	SEC1-LI
2002-09	SP-17	SP-020511	0027	-	F	Additional X3-interface parameters	5.3.0	5.4.0	SEC1-LI
2002-12	SP-18	SP-020702	0028	-	F	Event Time	5.4.0	5.5.0	SEC1-LI
2002-12	SP-18	SP-020704	0029	-	F	Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active	5.4.0	5.5.0	SEC1-LI
2002-12	SP-18	SP-020703	0030	-	F	Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active	5.4.0	5.5.0	SEC1-LI
2002-12	SP-18	SP-030478	0031	-	F	Missing QoS Parameter in IRI	5.5.0	5.6.0	SEC1-LI
2003-09	SP-21	SP-030479	0032	-	B	TEL URL for IMS interception identity (Release 6)	5.5.0	6.0.0	SEC1-LI
2003-09	SP-21	SP-030479	0032	-	D	Stereo delivery to LEMF	5.5.0	6.0.0	SEC1-LI
2003-12	SP-22	SP-030590	0034	-	F	MSISDN/IMEI clarification for GPRS interception	6.0.0	6.1.0	SEC1-LI
2003-12	SP-22	SP-030591	0035	-	F	Reporting TEL URL	6.0.0	6.1.0	SEC1-LI
2004-06	SP-24	SP-040397	0036	-	F	Correction on Network initiated Mobile Station Detach signalling flow	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040398	0037	-	F	TEL-URL missing in activation of LI in the CSCFs	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040399	0038	-	F	Correction on the use of session initiator parameter	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040400	0039	-	F	Correction to HLR interception event name	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040401	0040	-	B	Clarification for Push to talk over Cellular	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040402	0041	-	F	Adding an encryption parameter to IRI across X2 interface	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040403	0042	-	F	References	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040404	0043	-	F	Enhancements for the Functional Architecture chapter	6.1.0	6.2.0	SEC1-LI
2004-09	SP-25	SP-040693	0044	-	F	Correction on the use of session initiator parameter	6.2.0	6.3.0	SEC1-LI
2004-09	SP-25	SP-040693	0045	-	F	ICE (Intercepting Control Elements), INE (Intercepting Network Elements) definition	6.2.0	6.3.0	SEC1-LI
2004-09	SP-25	SP-040693	0046	-	F	Clarification to SMS interception	6.2.0	6.3.0	SEC1-LI
2004-09	SP-25	SP-040693	0047	-	F	Replace SIP URL with SIP URI	6.2.0	6.3.0	SEC1-LI
2004-12	SP-26	SP-040850	0048	-	B	Lawful Interception for WLAN Interworking	6.3.0	6.4.0	SEC1-LI
2004-12	SP-26	SP-040850	0049	-	F	33.107 Cleanup	6.3.0	6.4.0	SEC1-LI
2004-12	SP-26	SP-040850	0050	-	B	Clarification on MMS interception	6.3.0	6.4.0	SEC1-LI
2005-06	SP-28	SP-050256	0052	-	F	Correction on the use of identities for I-WLAN lawful interception	6.4.0	6.5.0	SEC1-LI
2005-06	SP-28	SP-050257	0051	1	F	Clarifications for the usage of the notion of a service in distributed IP networks	6.4.0	7.0.0	SEC-LI
2005-06	SP-28	SP-050257	0053	-	C	Correlation for IMS intercption	6.4.0	7.0.0	SEC1-LI
2005-09	SP-29	SP-050570	0054	-	F	Clarifications to the RAU event	7.0.0	7.1.0	SEC1-LI
2005-09	SP-29	SP-050570	0055	-	C	Simplifications to LDI handling	7.0.0	7.1.0	SEC1-LI
2005-12	SP-30	SP-050779	0054	-	B	Start of interception for already attached UE	7.1.0	7.2.0	LI-7A

2005-12	SP-30	SP-050763	0056	-	A	Availability of IMSI at PDG	7.1.0	7.2.0	IMS2 (SEC1-LI)
2006-03	SP-31	SP-060064	0057	-	F	WLAN Interworking - Additional Details for TS 33.107	7.2.0	7.3.0	LI-7A
2006-09	SP-33	SP-060659	0058	1	F	Editorial Update by Rapporteur	7.3.0	7.4.0	LI-7A
2007-03	SP-35		0060	-	B	Stage 2 MBMS Interception	7.4.0	7.5.0	LI-7A
2007-03	SP-35	SP-070156	0061	1	F	SMS IRI Reporting for WLAN Interworking	7.4.0	7.5.0	LI-7A
2007-06	SP-36	SP-070331	0063	-	B	Direct Tunnel LI	7.5.0	7.6.0	LI-7A
2007-06	SP-36	SP-070332	0062	-	B	NSAPI (Network layer Service Access Point Identifier) optional in IRI	7.6.0	8.0.0	LI8
2007-09	SP-37	SP-070601	0065	-	B	WLAN IRI at AAA for re-authentication	8.0.0	8.1.0	LI8
2007-09	SP-37	SP-070599	0064	-	A	Stage 2 MBMS Interception	8.0.0	8.1.0	LI-7A
2007-12	SP-38	SP-070788	0066	-	C	P-CSCF IMS LI Optional	8.1.0	8.2.0	LI8
2007-12	SP-38	SP-070788	0067	-	C	MBMS IRI Registration	8.1.0	8.2.0	LI8
2008-03	SP-39	SP-080172	0068	1	D	CR on P-CSCF IMS LI Optional	8.2.0	8.3.0	LI8
2008-03	SP-39	SP-080172	0069	1	D	Removing "P" suffix from references	8.2.0	8.3.0	LI8
2008-03	SP-39	SP-080172	0070	1	B	Changes for Interception of IRI and CC at a WAG	8.2.0	8.3.0	LI8
2008-06	SP-40	SP-080262	0071	-	F	CSCF SIP Event reporting	8.3.0	8.4.0	LI8
2008-06	SP-40	SP-080262	0072	-	B	Conference Event Reporting	8.3.0	8.4.0	LI8
2008-06	SP-40	SP-080262	0073	-	D	Editorial corrections	8.3.0	8.4.0	LI8
2008-09	SP-41	SP-080514	0074	-	B	Updates to TS 33.107 to support LI for EPSs	8.4.0	8.5.0	LI8
2008-12	SP-42	SP-080762	0077	-	F	Editorial corrections to 33.107	8.5.0	8.6.0	LI8
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.	8.5.0	8.6.0	LI8
2008-12	SP-42	SP-080762	0076	-	F	Clarification on 3G DT with the GGSN	8.5.0	8.6.0	LI8
2009-03	SP-43	SP-090133	0078	-	F	Alignment with SAE stage 2 specifications approved by TSG SA#42	8.6.0	8.7.0	LI8
2009-04						Editorial correction to cover page	8.7.0	8.7.1	
2009-06	SP-44	SP-090272	0079	-	F	Correction on UE requested bearer resource modification - Alignment with SAE stage 2 specification	8.7.1	8.8.0	LI8
2009-06	SP-44	SP-090272	0080	-	F	Clarification on parameter APN	8.7.1	8.8.0	LI8
2009-06	SP-44	SP-090272	0081	-	F	Clarification on the handover between 2G/3G access and E-UTRAN with Gn/Gp	8.7.1	8.8.0	LI8
2009-06	SP-44	SP-090272	0082	-	F	Clarification on parameter PDN type	8.7.1	8.8.0	LI8
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	8.8.0	8.9.0	LI8
2009-09	SP-45	SP-090522	0084	-	F	Correction on Serving Evolved Packet System event	8.8.0	8.9.0	LI8
2009-10	--	--	--	--	--	Correction of misimplementation of CR0084	8.9.0	8.9.1	
2009-12	SP-46	SP-090817	86	-	F	Correction on events names	8.9.1	8.10.0	LI8
2009-12	SP-46	SP-090817	87	-	F	Restoring section header 9.4.5	8.9.1	8.10.0	LI8
2009-12	SP-46	SP-090817	88	-	F	Correction on PDP context modification event	8.9.1	8.10.0	LI8
2009-12	SP-46	SP-090817	85	-	F	Correction on LI correlation for S4-SGSN	8.9.1	8.10.0	LI8
2009-12	-	-	-	-	-	Update to Rel-9 version (MCC)	8.10.0	9.0.0	-
2010-06	SP-48	SP-100364	89	-	F	Correction in IMS Conference text	9.0.0	9.1.0	LI9
2010-06	SP-48	SP-100253	90	-	F	Reporting of Dual Stack PDP address from the SGSN	9.1.0	10.0.0	LI10
2010-10	SP-49	SP-100570	92	-	A	Correction in IMS Conference Service X2 interface	10.0.0	10.1.0	TEI9
2010-10	SP-49	SP-100570	93	-	A	IMS Conference Service configuration for CC interception	10.0.0	10.1.0	TEI9
2010-10	SP-49	SP-100481	91	-	F	Unsuccessful bearer modificatio	10.0.0	10.1.0	LI10
2010-10	SP-49	SP-100481	94	-	B	LI architecture and functions for KMS based IMS Media Security	10.0.0	10.1.0	LI10
2010-10	--	--	--	--	--	ToC update	10.1.0	10.1.1	--
2010-12	SP-50	SP-100845	97	1	A	IMSI based activation	10.1.1	10.2.0	LI10
2010-12	SP-50	SP-100865	98	1	B	MME start of interception with bearer active	10.1.1	10.2.0	LI8
2010-12	SP-50	SP-100865	103	1	C	Corrections and Alignment for IMS Conferencing	10.1.1	10.2.0	LI8
2011-03	SP-51	SP-110023	104	-	B	Location information from trusted non-3GPP access	10.2.0	10.3.0	LI10
2011-03	SP-51	SP-110023	106	-	C	Security requirements for LI in KMS based IMS media security	10.2.0	10.3.0	LI10
2011-03	SP-51	SP-110023	111	-	F	Initiator parameter definition	10.2.0	10.3.0	LI10
2011-03	SP-51	SP-110021	109	-	A	IMS Conf LI 33.107	10.2.0	10.3.0	LI8
2011-06	SP-52	SP-110260	112	-	C	TLS and IPsec profiling for Xk interface	10.3.0	10.4.0	LI10
2011-09	SP-53	SP-110511	113	-	B	Reporting of PMIP and DSMIP session modification	10.4.0	11.0.0	LI11
2012-03	SP-55	SP-12-0034	114		F	Correction on MIP specific parameters provided over the X2 interface.	11.0.0	11.1.0	LI11
2012-06	SP-56	SP-120336	114a	1	C	IMSI in untrusted non-3GPP access	11.1.0	11.2.0	LI11
2012-06	SP-56	SP-120336	115	1	C	SGs received location transfer over the X2 interface	11.1.0	11.2.0	LI11
2012-06	SP-56	SP-120336	116	2	F	UE IP Address at X2 interface	11.1.0	11.2.0	LI11
2012-06	SP-56	SP-120336	117	1	F	Handover indication at X2 interface	11.1.0	11.2.0	LI11
2012-06	SP-56	SP-120336	118	1	F	IMS Conference Services	11.1.0	11.2.0	LI11
2012-06	SP-56	SP-120336	119	1	F	IMS Provison of CC	11.1.0	11.2.0	LI11
2012-09	SP-57	SP-120627	120	1	F	Reference list correction to align with the corrected TS 29.212 title	11.2.0	11.3.0	TEI11
2012-09	SP-57	SP-120600	121	-	B	H(e)NB Support in TS 33.107	11.3.0	12.0.0	LI12

2012-12	SP-58	SP-120854	122	-	B	LI events for trusted non-3GPP access on GTP S2a, Rel12	12.0.0	12.1.0	LI12
2012-12	SP-58	SP-120854	123	-	F	Removal of LTE	12.0.0	12.1.0	LI12
2013-03	SP-59	SP-130034	124	-	B	Start of interception for an already established IMS media secured session	12.1.0	12.2.0	LI12
			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	12.2.0	12.3.0	LI12
			127	-	B	Mid Session Interception for IMS			
2013-09			128	-	B	Addition of LI to GBA			
	SP-61	SP-130401	129	-	F	Adding version to non 3GPP references	12.3.0	12.4.0	LI12
			130	-	F	Updating Tel URL to Tel URI			
2013-12	SP-62	SP-130661	131	-	B	ULI timestamp reporting	12.4.0	12.5.0	LI12
			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	12.5.0	12.6.0	LI12
			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			
			142	-	F	Editorial clean-up of target & monitored subscriber	12.6.0	12.7.0	LI12
			143	-	F	Editorial clean-up of incorrect paragraph numbering			
			144	-	A	IMS IMEI Interception			
2014-06	SP-64	SP-140310	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			
			150	-	B	LI functionalities for GTP based s2b interfaces			
			151	-	D	Editorial Corrections			
			152	-	F	Clarification on interception of VoIP CC for targeted calls			
2014-09	SP-65	SP-140586	153	-	C	Change of 'Decryption for IMS Media Plane Security' clause: making it more specific regarding E2E/E2AE modes	12.7.0	12.8.0	
			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			LI12
			159	-	B	Adding the interception feature of any XCAP usages			
			160	-	F	Editorial Correction to Stage 2 call flows (VoIP)			
			161	-	C	Group Communications LI with GSC AS outside the intercepting CSP"s network			
2014-12	SP-66	SP-140821	162	-	B	Adding the Mask parameter to the interception of ProSe direct discovery	12.8.0	12.9.0	
			163	-	C	Alignment of LI for GCSE with HI2 & HI3			
			164	-	B	LI for ProSe One to Many Communications – In Network Coverage			

History

Document history		
V12.8.0	October 2014	Publication
V12.9.0	January 2015	Publication