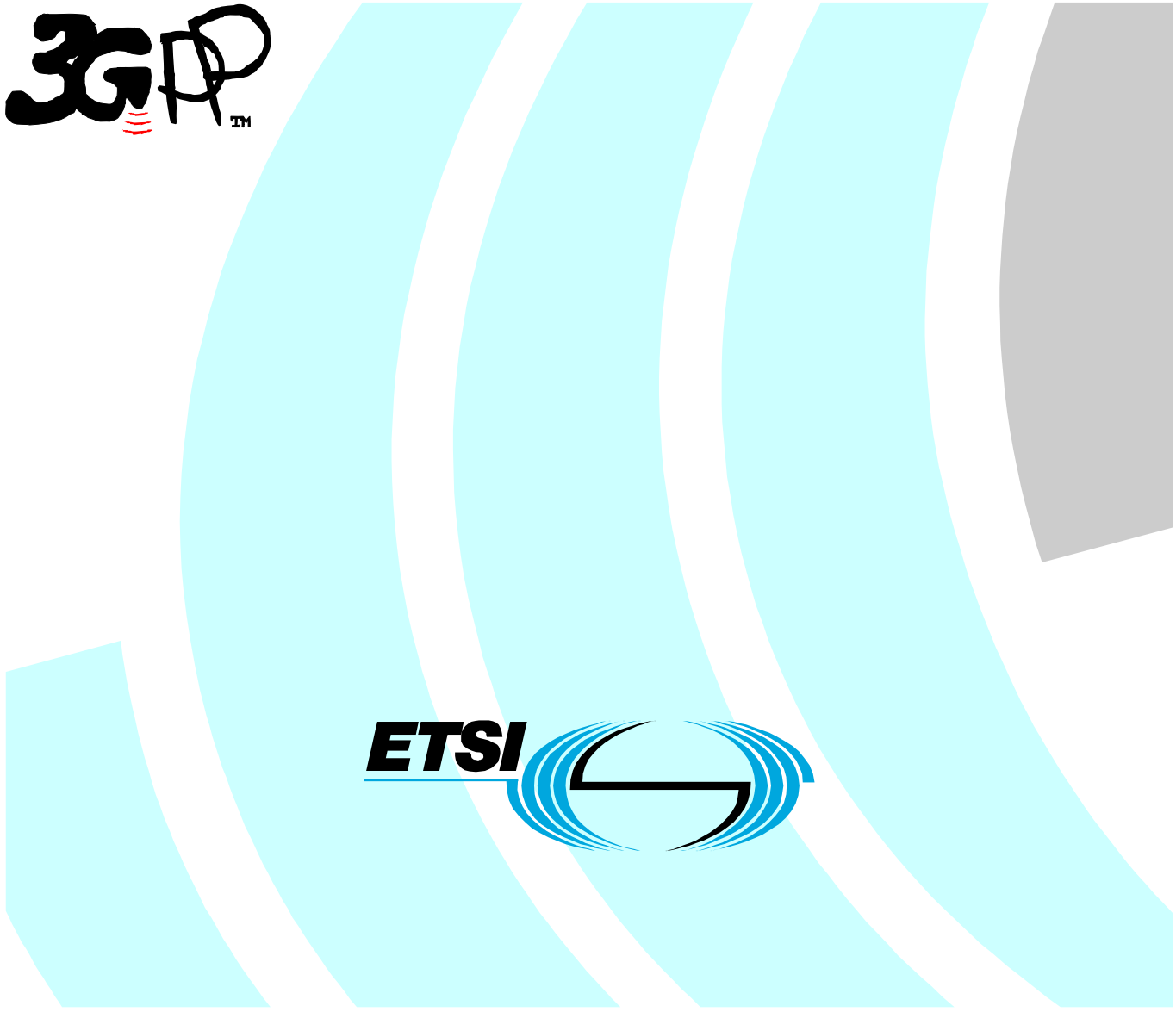
ETSI TS 133 107 V6.5.0 (2005-06)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
3G security;
Lawful interception architecture and functions
(3GPP TS 33.107 version 6.5.0 Release 6)



Reference
RTS/TSGS-0333107v650

Keywords
UMTS

ETSI

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

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

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

Intellectual Property Rights

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

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

Foreword

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

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

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

Contents

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 (3GPP MS).

The specification shows the service requirements from a Law Enforcement point of view only. The aim of this document is to define a 3GPP MS 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 for stage 3 are described in 3GPP 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] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[2] ETSI ES 201 158: "Lawful Interception; Requirements for network functions".

[3] ETSI ES 201 671: "Handover Interface for the lawful interception of telecommunications traffic".

[4] GSM 01.33: "Lawful Interception requirements for GSM".

[5] GSM 02.33: "Lawful Interception - stage 1".

[6] GSM 03.33: "Lawful Interception - stage 2".

[7] 3GPP TS 33.106: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements".

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

[9] IETF RFC 2806: "URLs for Telephone Calls ".

[10] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description".

[11] 3GPP TS 33.108: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Handover interface for Lawful Interception".

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

[13] 3GPP TS 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[14] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[15] 3GPP TS 23.008: "3rd Generation Partnership Project; Technical Specification Group Core Network; Organization of subscriber data'.

[16] 3GPP TS 29.234: "3rd Generation Partnership Project; Technical Specification Group Core Network; 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3".

[17] 3GPP TS 24.234: "3rd Generation Partnership Project; Technical Specification Group Core Network; 3GPP system to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [13] and the following apply.

Network Based Interception: Interception that is invoked at a network access point regardless of Target Identity.

Subject Based Interception: Interception that is invoked using a specific Target Identity.

Target Identity: A technical identity that uniquely identifies a target of interception. One target may have one or several identities.

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).

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [13] and the following apply:

3GPP MS	3rd Generation Mobile Communication 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
CC	Content of Communication
DF	Delivery Function
ECT	Explicit Call Transfer
GPRS	General Packet Radio Service
HI	Handover Interface
IA	Interception Area
ICEs	Intercepting Control Elements (3G MSC Server, 3G GMSC Server, P-CSCF, S-CSCF, SGSN, GGSN, HLR, AAA Server, PDG)
IMS	IP Multimedia Core Network Subsystem
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
LDI	Location Dependent Interception
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility

PDG	Packet Data Gateway
RA	Routing Area
RAI	Routing Area Identity
SAI	Service Area Identity
SIP	Session Initiation Protocol
TEL URL	"tel" URL, as defined in [9]
URI	Universal Resource Identifier
URL	Universal Resource Locator

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 various entities and interfaces are described in more detail in the succeeding clauses.

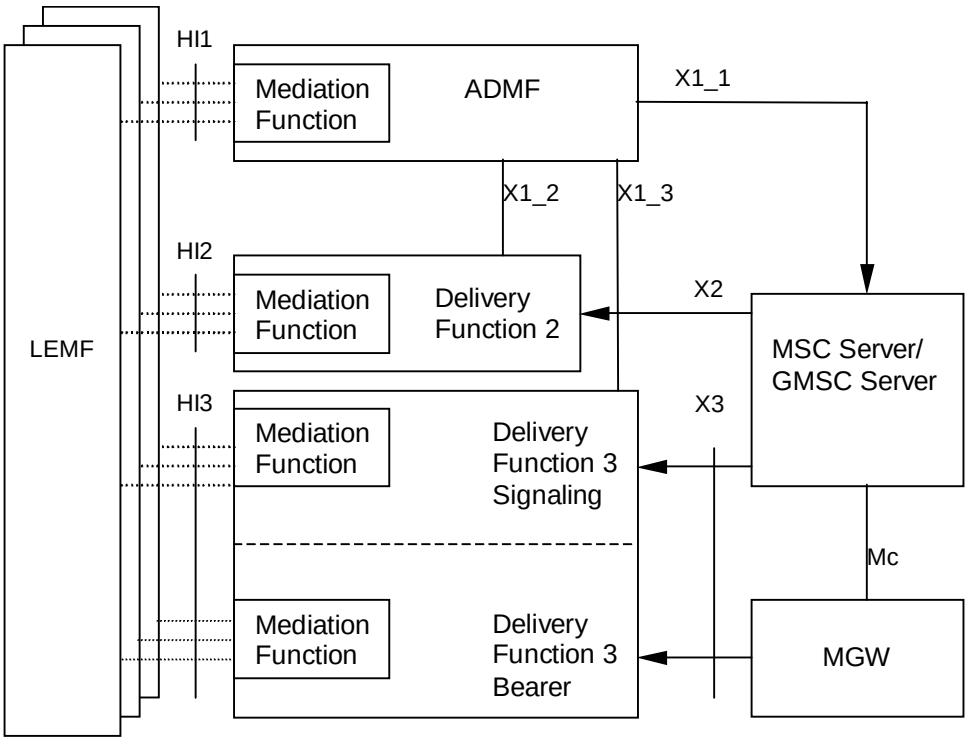


Figure 1a: Circuit switched intercept configuration

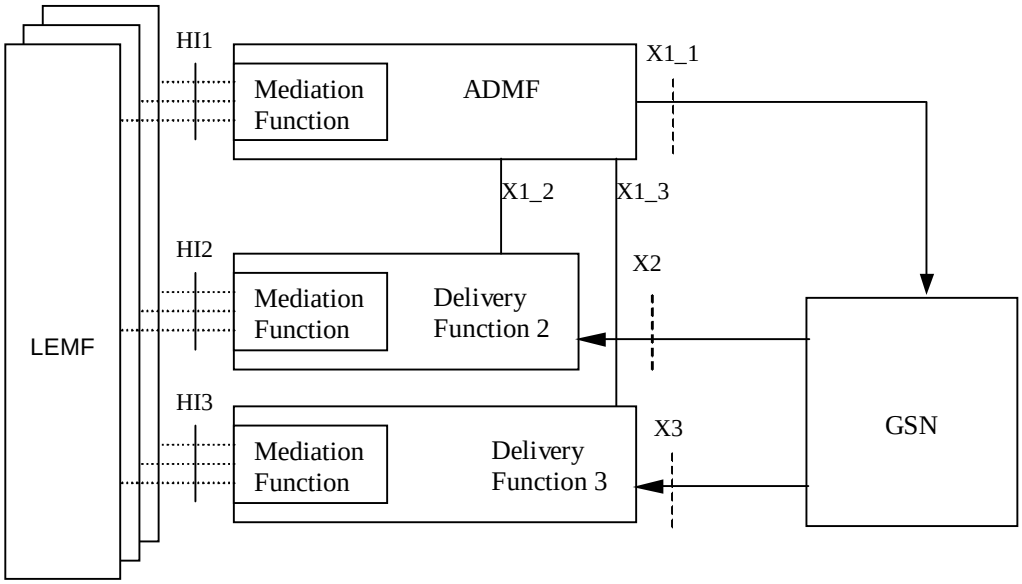


Figure 1b: Packet Switched Intercept configuration

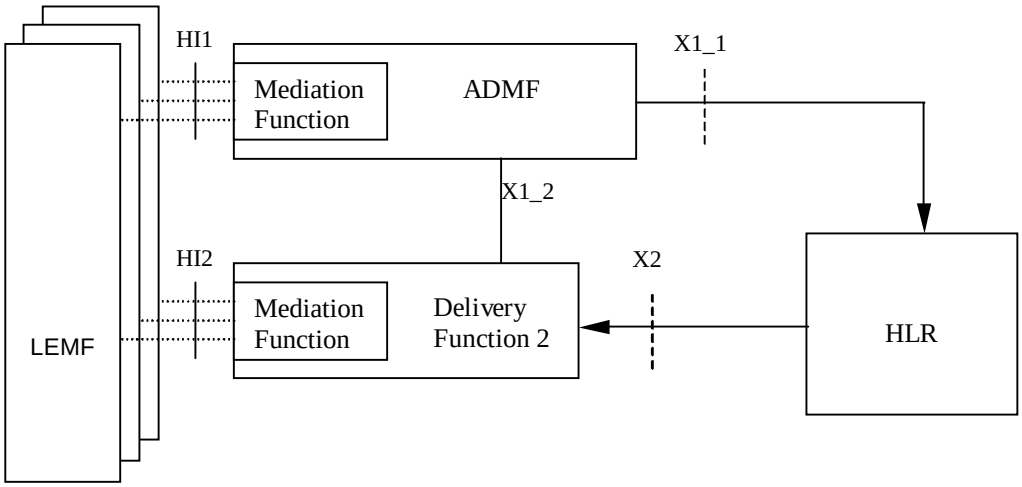


Figure 1c: HLR Intercept configuration

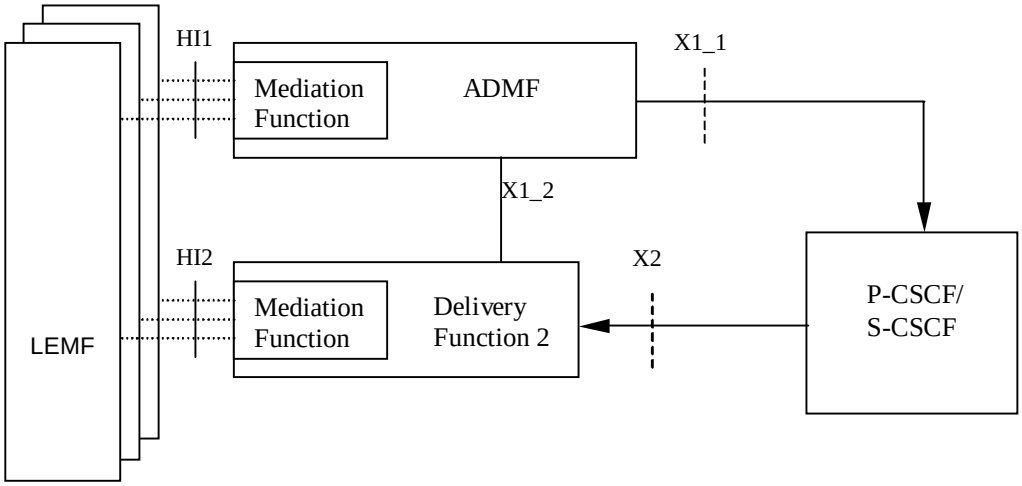


Figure 1d: IMS-CSCF Intercept configuration

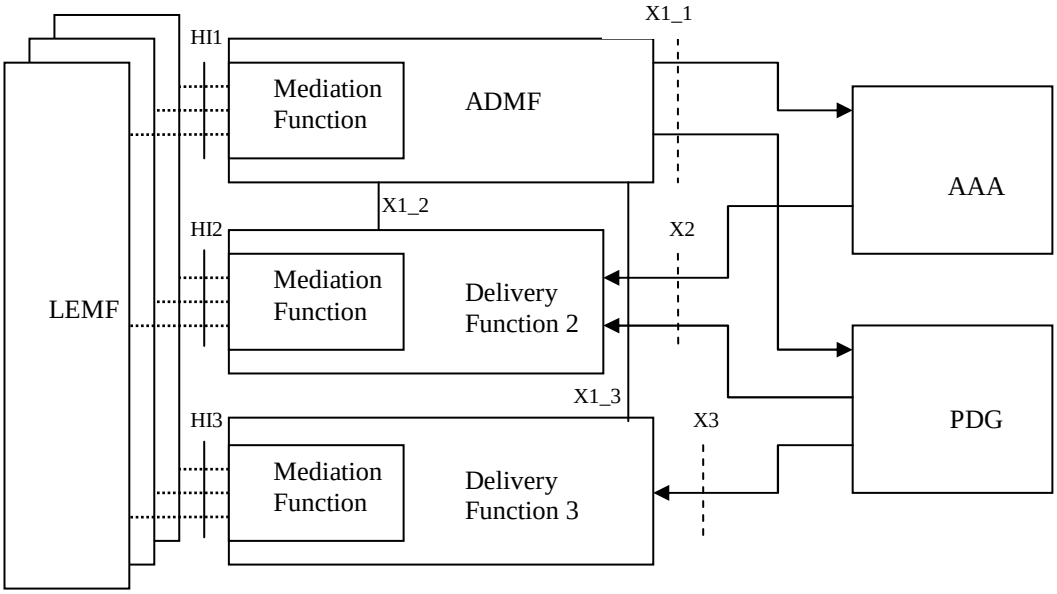


Figure 1e: WLAN Interworking Intercept configuration

The reference configuration is only a logical representation of the entities involved in lawful interception and does not mandate separate physical entities. This allows for higher levels of integration.

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 ES 201 671 [3] or 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.

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 and 1e, 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.

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

NOTE 2: 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).

5 Activation, deactivation and interrogation

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.

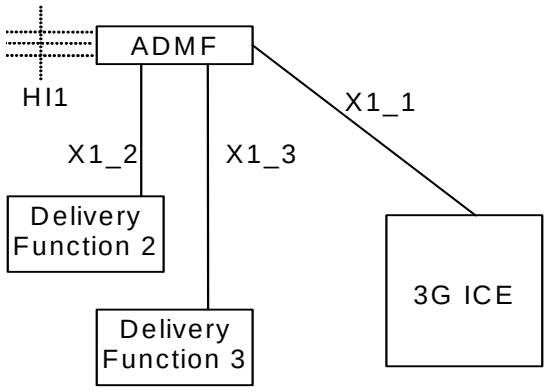


Figure 2: Functional model for Lawful Interception activation, deactivation and interrogation

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.

The target identities for 3GPP MS 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 [10].

The target identities for multi-media at the CSCF can be one or more of the following: SIP URI or TEL URL. 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), refer to [14], [15], [16] and [17].

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

NOTE 3: The IMSI may be used, however, in many cases it will not be available.

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 and SSGN 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

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 URL, NAI) (see notes 4, 5, 6 and 7);
- 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 product and/or intercept related information has to be provided can be part of the delivery functions. (Note that intercept product 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 product and related information has to be provided" for theICE. 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 or TEL URL. SIP URI and TEL URL as target identities are not supported by the other ICEs.

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

NOTE 7: As the IMSI is not available in most cases, interception based on the IMSI is not applicable at the PDG.

If after activation subsequently 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.

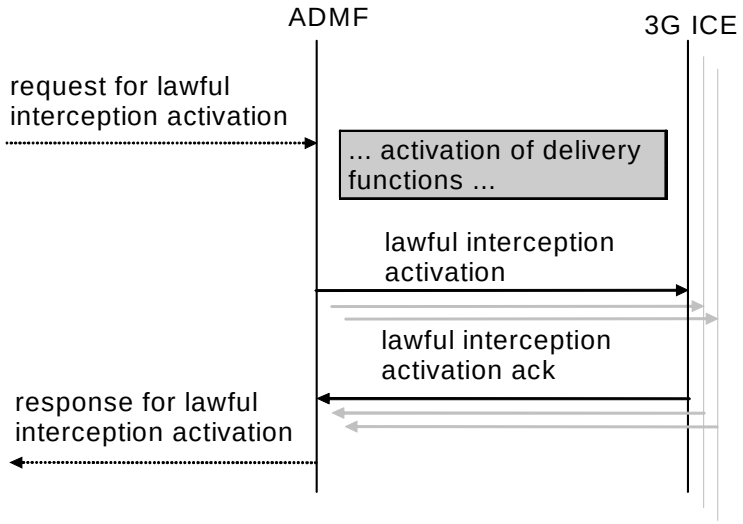


Figure 3: Information flow on X1_1-interface for Lawful Interception activation

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 then the ADMF determines that there are existing activations on the identity. In this case, the ADMF may (as an implementation option) send an additional activation message 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.

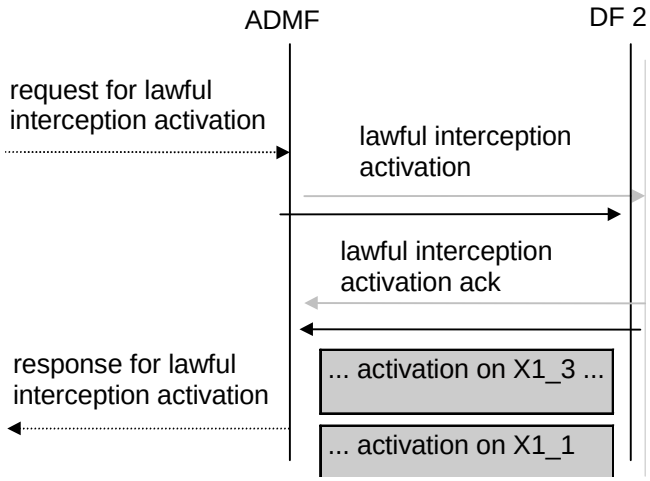


Figure 4: Information flow on X1_2-interface for Lawful Interception activation

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.

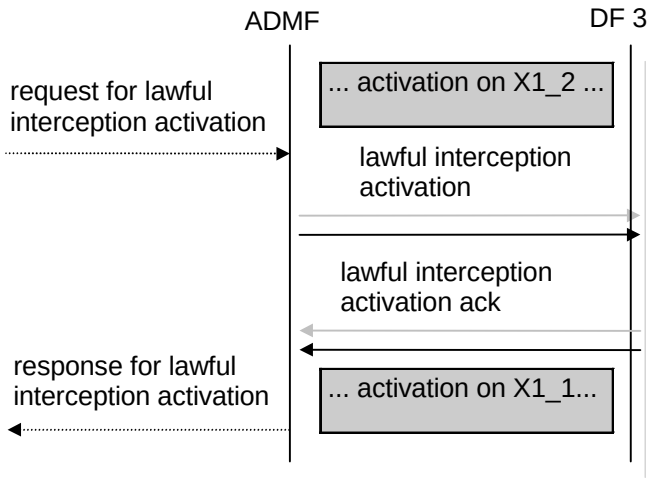


Figure 5: Information flow on X1_3-interface for Lawful Interception activation

5.2 Deactivation

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.

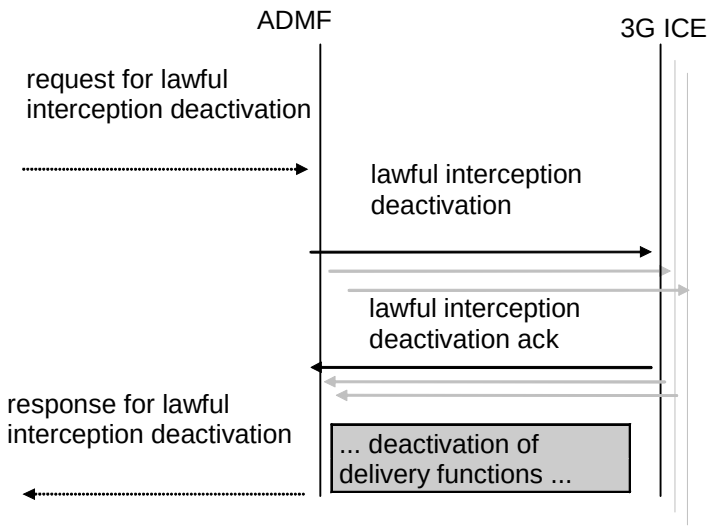


Figure 6: Information flow on X1_1-interface for Lawful Interception deactivation

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 messages sent from the ADMF to Delivery Function 2 for the deactivation of the Intercept Related Information contain:

- 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.

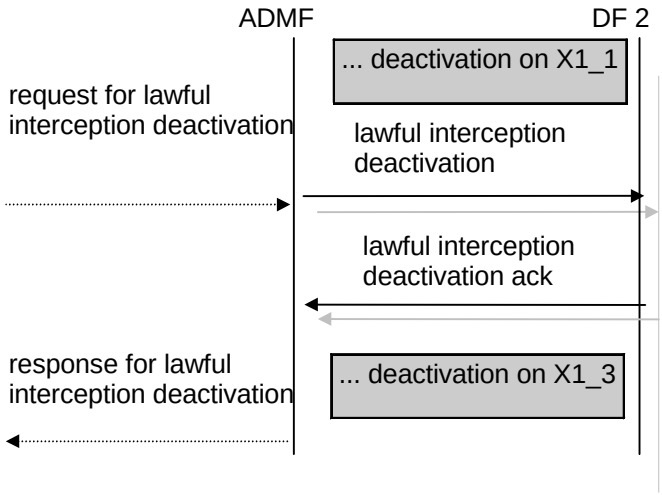


Figure 7: Information flow on X1_2-interface for Lawful Interception deactivation

5.2.3 X1_3-interface (CC)

For the deactivating the delivery of the CC the messages from the ADMF to DF3 contain:

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

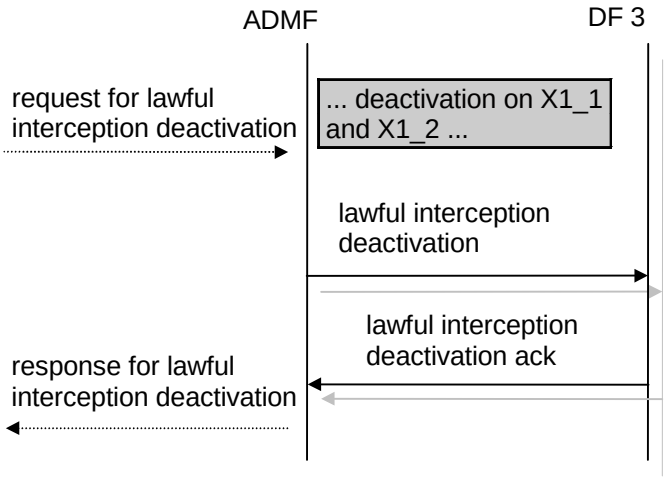


Figure 8: Information flow on X1_3-interface for Lawful Interception deactivation

5.3 Interrogation

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.

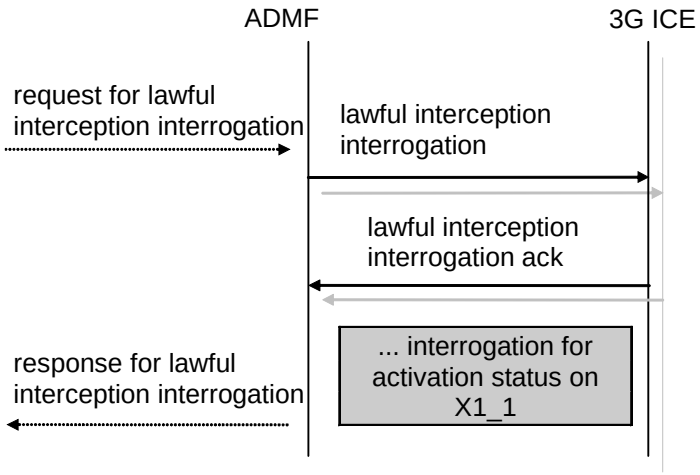


Figure 9: Interrogation of the Lawful Interception (3G ICEs)

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.

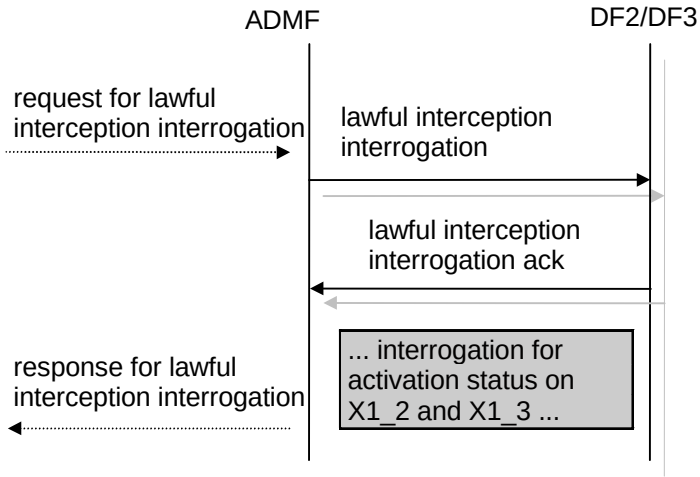


Figure 10: Interrogation of the Lawful Interception (Delivery Functions)

6 Invocation of Lawful Interception for Circuit Switched Services

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

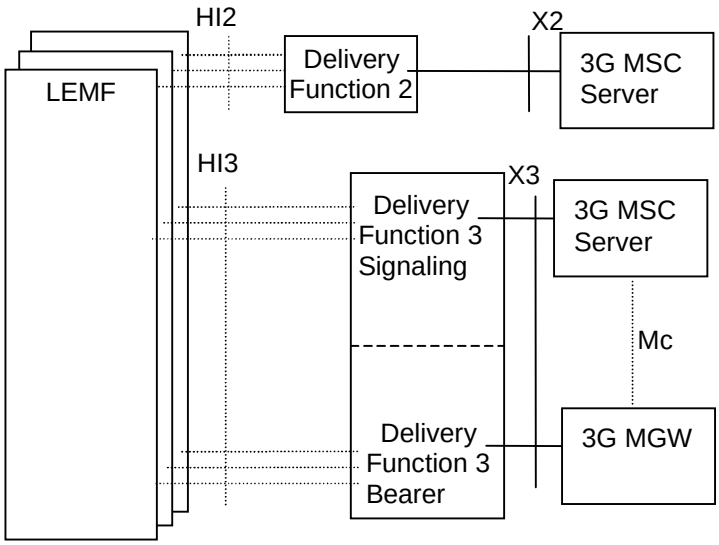


Figure 11: Functional model for Lawful Interception invocation

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 product to the relevant LEA(s) (based on IAs, if defined).

For the delivery of the CC and IRI, the 3G MSC Server provides a correlation number and target identity to the DF2 and DF3 which is used there in order 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.

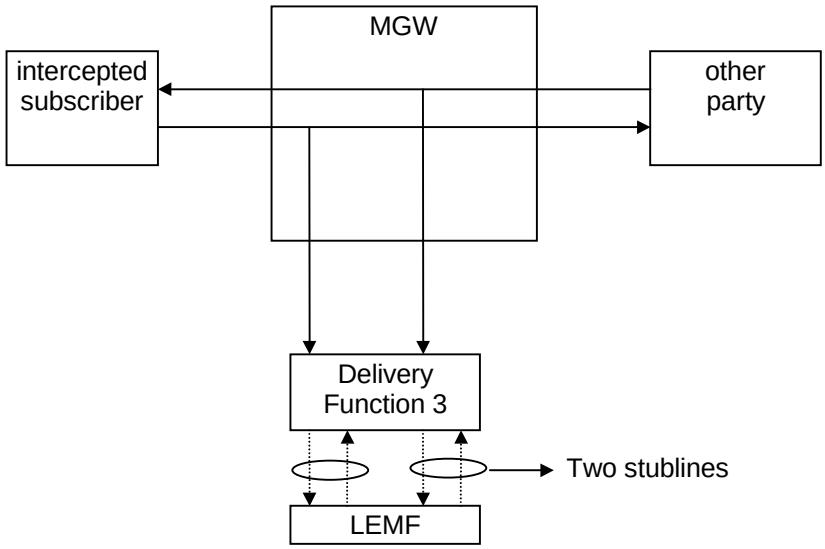


Figure 12: Delivery configuration to the LEMF for the interception of a circuit switched call

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: 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 be confirmed by SA WG3 LI group) to the DF3 in order to allow the DF3 to perform its functionality:

- target identity (MSISDN, IMSI or IMEI); note 1
- the target location (if available) or the IAs in case of location dependent interception. note 1
- correlation number (IRI <-> CC);
- direction indication - (Signal from target or signal to target).

NOTE 1: 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.

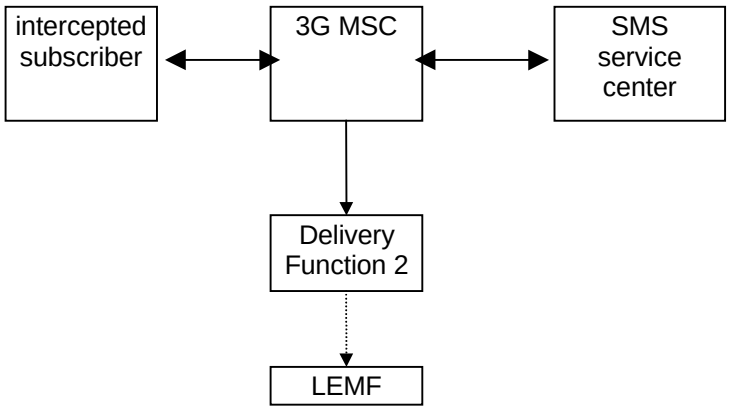


Figure 14: Provision of Content of Communication - Short Message Service

6.3 Provision of Intercept Related Information

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.

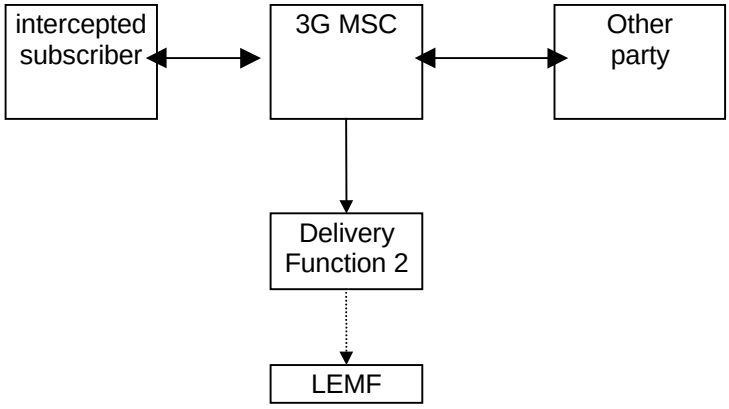


Figure 15: Provision of Intercept Related Information

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 subscriber (monitored subscriber).
Observed IMSI Target Identifier with the IMSI of the target subscriber (monitored subscriber).
Observed IMEI Target Identifier with the IMEI of the target subscriber (monitored subscriber), 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 monitored subscriber 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
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

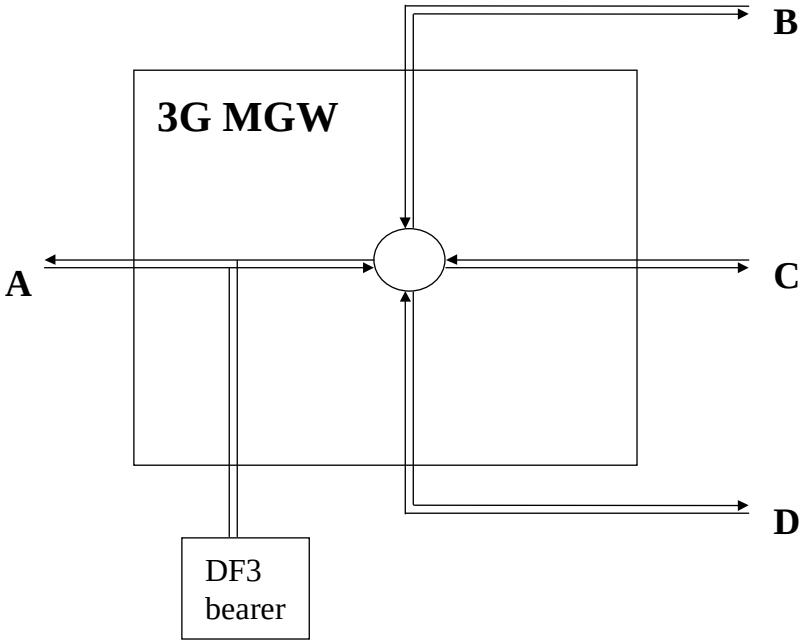


Figure 16: Interception of Multiparty for CC

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

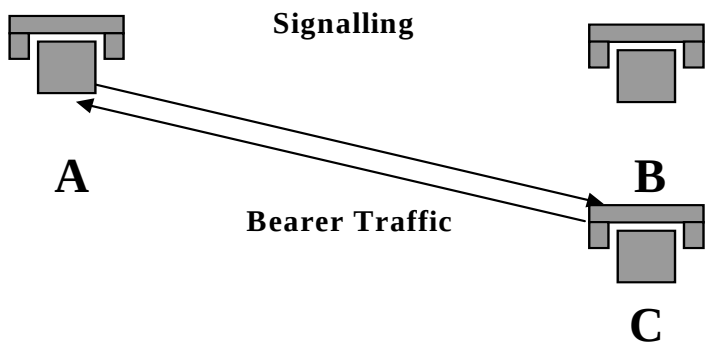


Figure 17: Interception for Call Forwarding / Deflection / ECT

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

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.

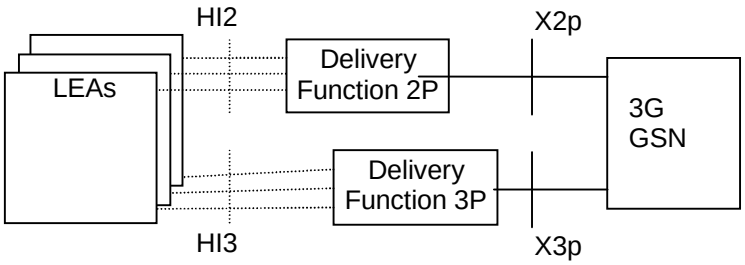


Figure 18: Functional model for Packet Data GSN Network Lawful Interception invocation

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.

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.

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, a Mobile Station Detach event is sent when changing servicing 3 G GSNs or a RA update event is sent when changing IAs inside the same servicing 3G SGSN to DF2;

- 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 3GPP TS 23.060 [10], clause 6.9.1.2.2 and 3GPP 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.

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.

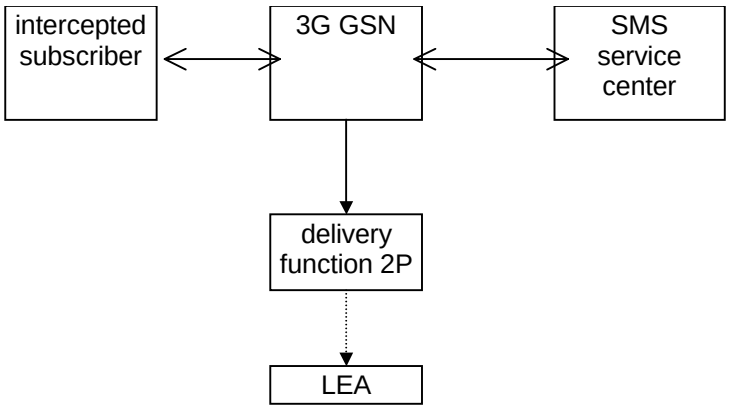


Figure 19: Provision of Intercept Product - Short Message Service

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

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 the header, as described in the following clauses, are sent to DF3 for further delivery via a tunnel.

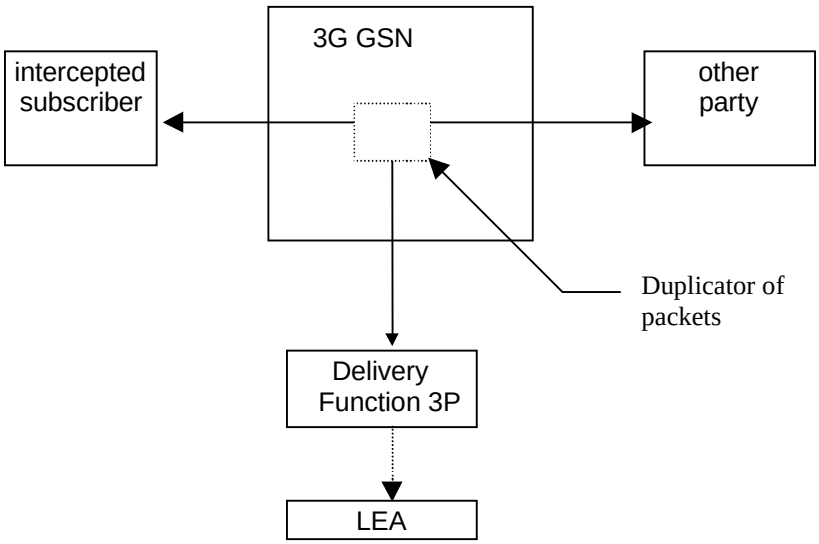


Figure 20: Configuration for interception of Packet Data GSN product data

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.

7.3 Provision of Intercept Related Information

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 and SMS events.

Serving System event 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.

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

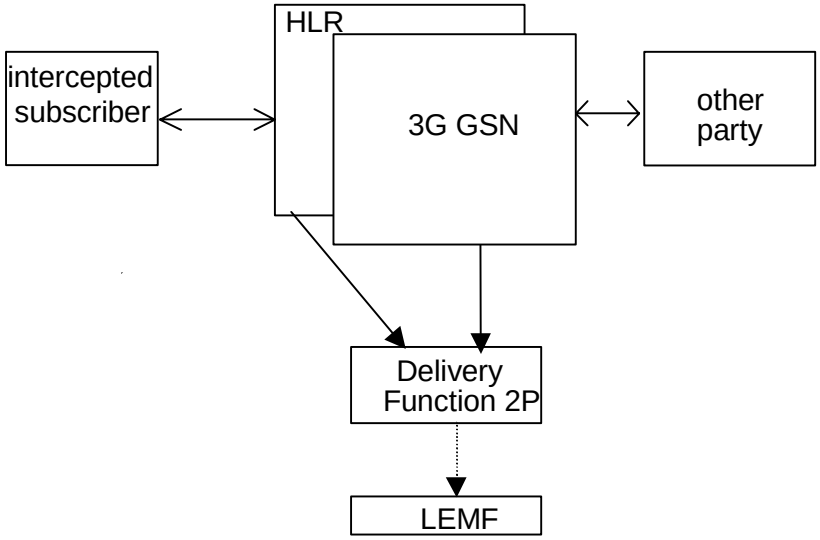


Figure 21: Provision of Intercept Related Information

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.

7.3.2 Structure of the events

There are eight 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 intercept with PDP context active;
- PDP context modification;
- PDP context deactivation;
- RA update;
- SMS.

NOTE: 3G GGSN interception is a national option. Location information may not be available in this case.

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.

The following events are applicable to the HLR:

- Serving System.

A set of fields as shown below can be associated with the events. The events trigger the transmission of the information from 3G GSN or HLR to DF2. Available IEs from this set of fields 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 subscriber (monitored subscriber).
Observed IMSI IMSI of the target subscriber (monitored subscriber).
Observed IMEI IMEI of the target subscriber (monitored subscriber),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, 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 subscriber. Note that this address might be dynamic.
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 subscriber.
Failed context activation reason Reason for failed context activation of the target subscriber.
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).

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 servicing 3G G SN this event is generated. These fields 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 fields 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

For PDP context activation a PDP context activation-event is generated. When a PDP context activation is generated from the mobile to 3G GSN this event is generated. These fields 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)

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 then one PDP context are open for each of them an event record is generated. These fields 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)

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.

7.4.5 Packet Data PDP context deactivation

At PDP context deactivation a PDP context deactivation-event is generated. These fields 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)

7.4.6 RA update

For each RA update an update-event with the fields about the new location is generated. These fields 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)

7.4.7 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 fields 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 interception for a target is started and if the target has at least one PDP context active. These fields 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 fields 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

7.5 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. No additional content of communications intercept requirements are identified. (to be confirmed pending completion of multi-media stage 2 specifications) Activation and invocation of multi-media service does not produce interception of content of communications, which must be intercepted at the GSN under a separate activation and invocation.

7A.2 Provision of IRI

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 subscriber are subject to intercept at the P CSCF and S CSCF. Based upon network configuration, the ADMF shall provision P CSCFs, or S CSCFs, or both P CSCFs and S CSCFs with SIP URI or TEL URL target identifiers. These resulting intercepted SIP messages shall be sent to DF2 for mediation prior to transmittal across the HI2 interface.

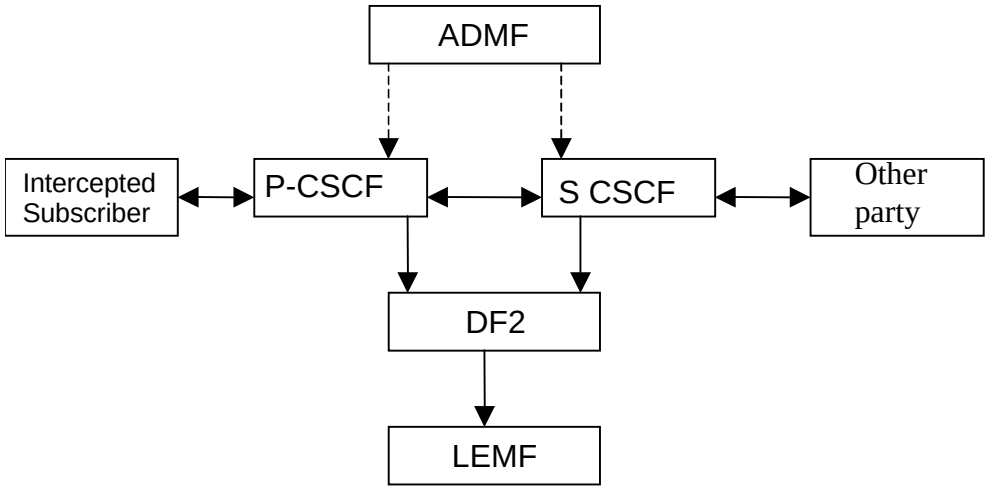


Figure 22: Provision of Intercept Related Information for multi-media

7A.3 Multi-media events

- 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 P CSCF and S CSCF and sent to DF2. The target identifier used to trigger the intercept will also be sent with the SIP message. 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.
- The use of a correlation ID for SIP to bearer correlation is not defined in this release.
- An intercepted SIP event sent to DF2 is shown below:
  - Observed SIP URI
  - Observed TEL URL
  - Event Time and Date
  - Network element identifier
  - SIP Message Header
  - SIP Message Payload

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.

8 Security

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 3GPP MS shall be capable to perform a periodic consistency check to ensure that the target list of target identities in all involved 3G MSC Servers, CSCFs, 3G GSNs in the 3GPP MS 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

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.

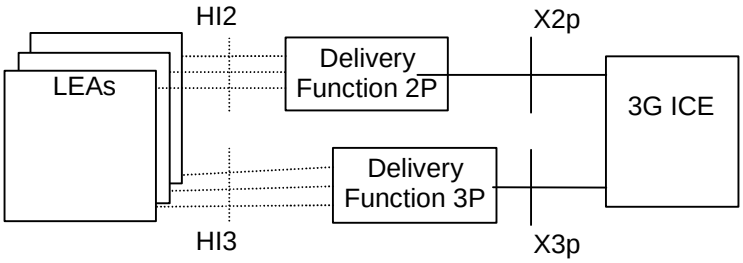


Figure 23: Functional model for invocation of Lawful Interception for 3GPP WLAN Interworking Services

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).

9.1 Provision of Intercept Product - Short Message Service

LI for SMS in the 3GPP-WLAN Interworking case is not defined in this release. However, SMS may be available at the PDG as part of the CC.

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

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

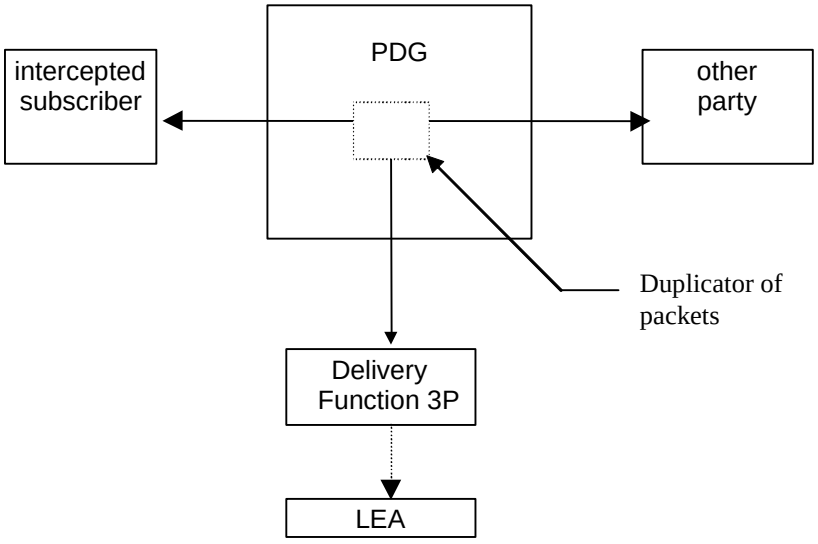


Figure 24: Configuration for interception of 3GPP WLAN Interworking product data

9.2.1 X3-interface

In addition to the intercepted content of communications, the following information needs to be transferred from the PDG 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

Figure 25 shows the transfer of intercept related information to the DF2. If an event for / from a mobile subscriber occurs, the PDG, or the AAA Server sends the relevant data to the DF2.

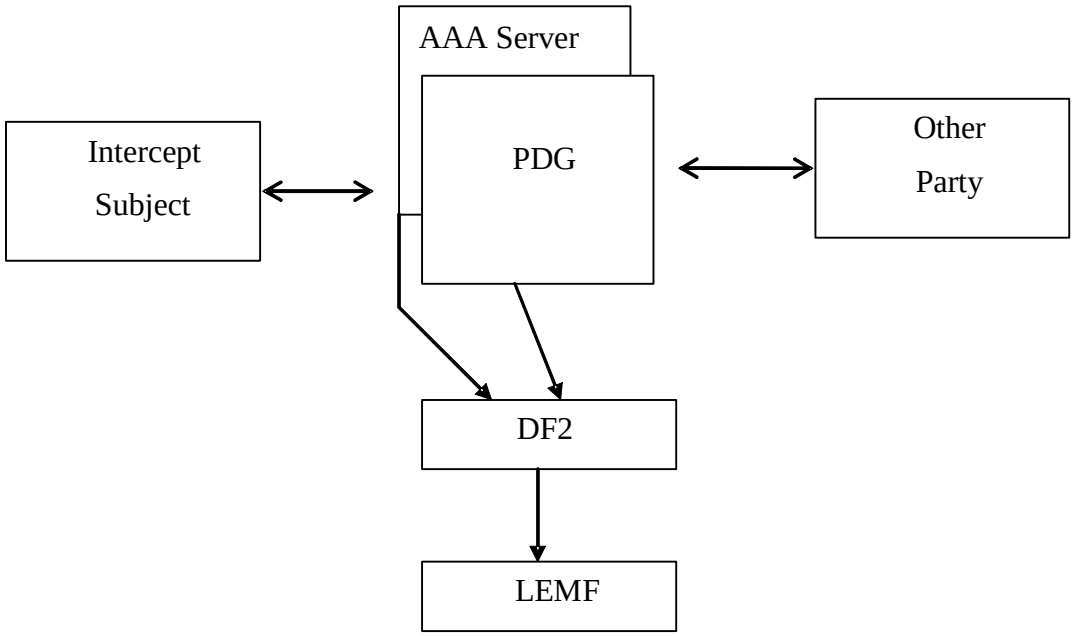


Figure 25: Provision of Intercept Related Information

9.3.1 X2-interface

The following information needs to be transferred from the PDG 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 (for PDG only);
- Quality of Service (QoS) identifier (if available).

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

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 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:

- I-WLAN Tunnel Establishment;
- I-WLAN Tunnel Disconnect;
- Start of Intercept with I-WLAN Communication Active.

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 subscriber. The bearer establishment to agency will be in parallel or immediately following the bearer establishment to the target subscriber. 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.

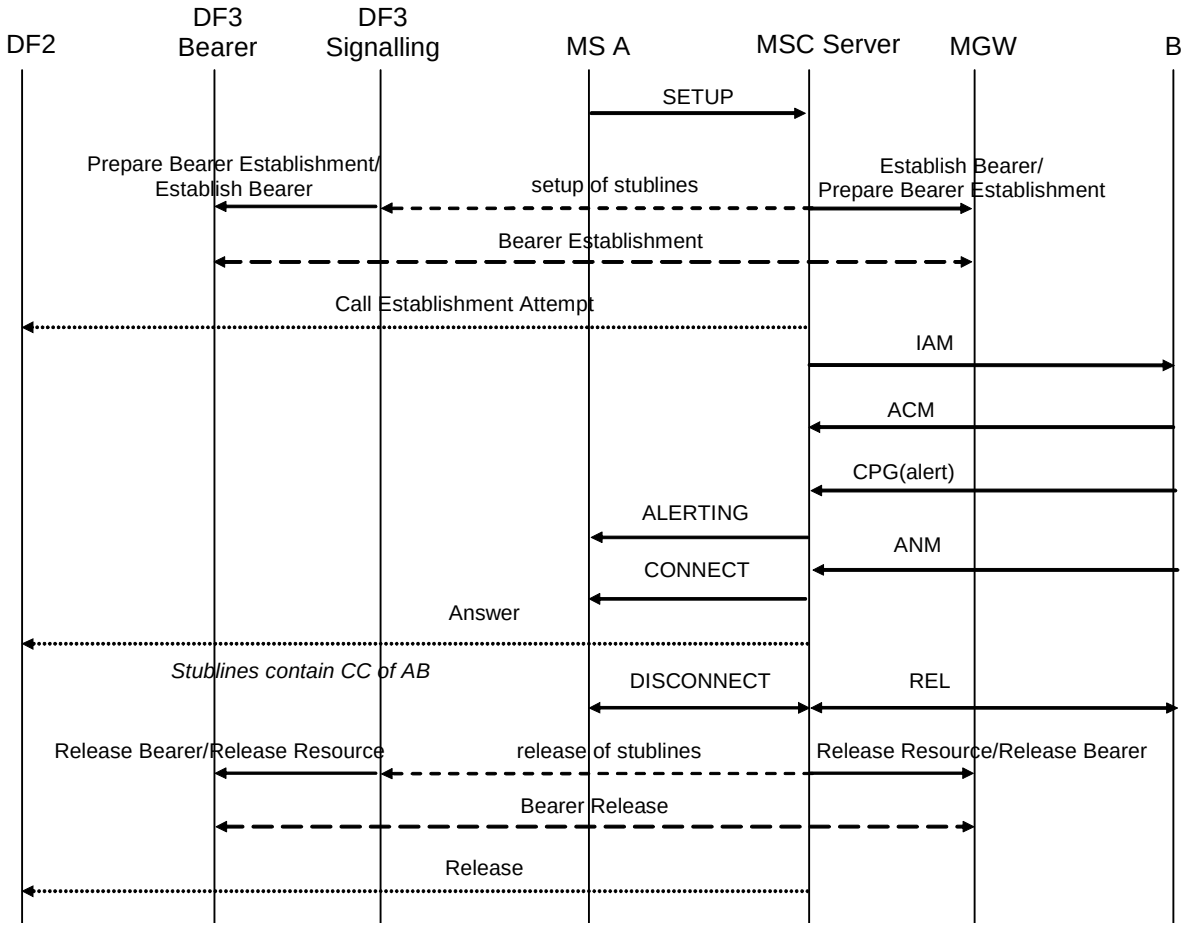


Figure A.1: Interception of mobile originated circuit switched calls

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.

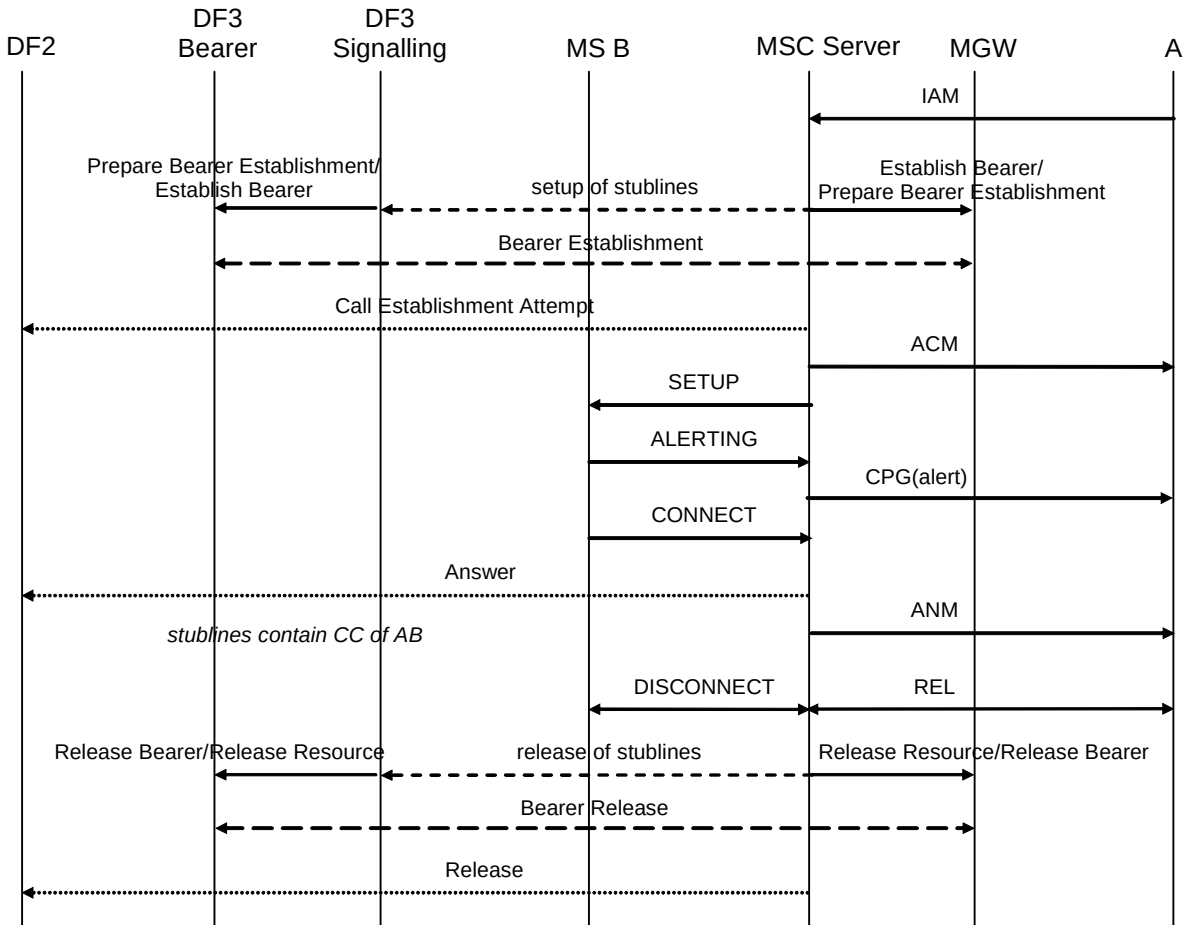


Figure A.2: Interception of mobile terminated circuit switched calls

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.

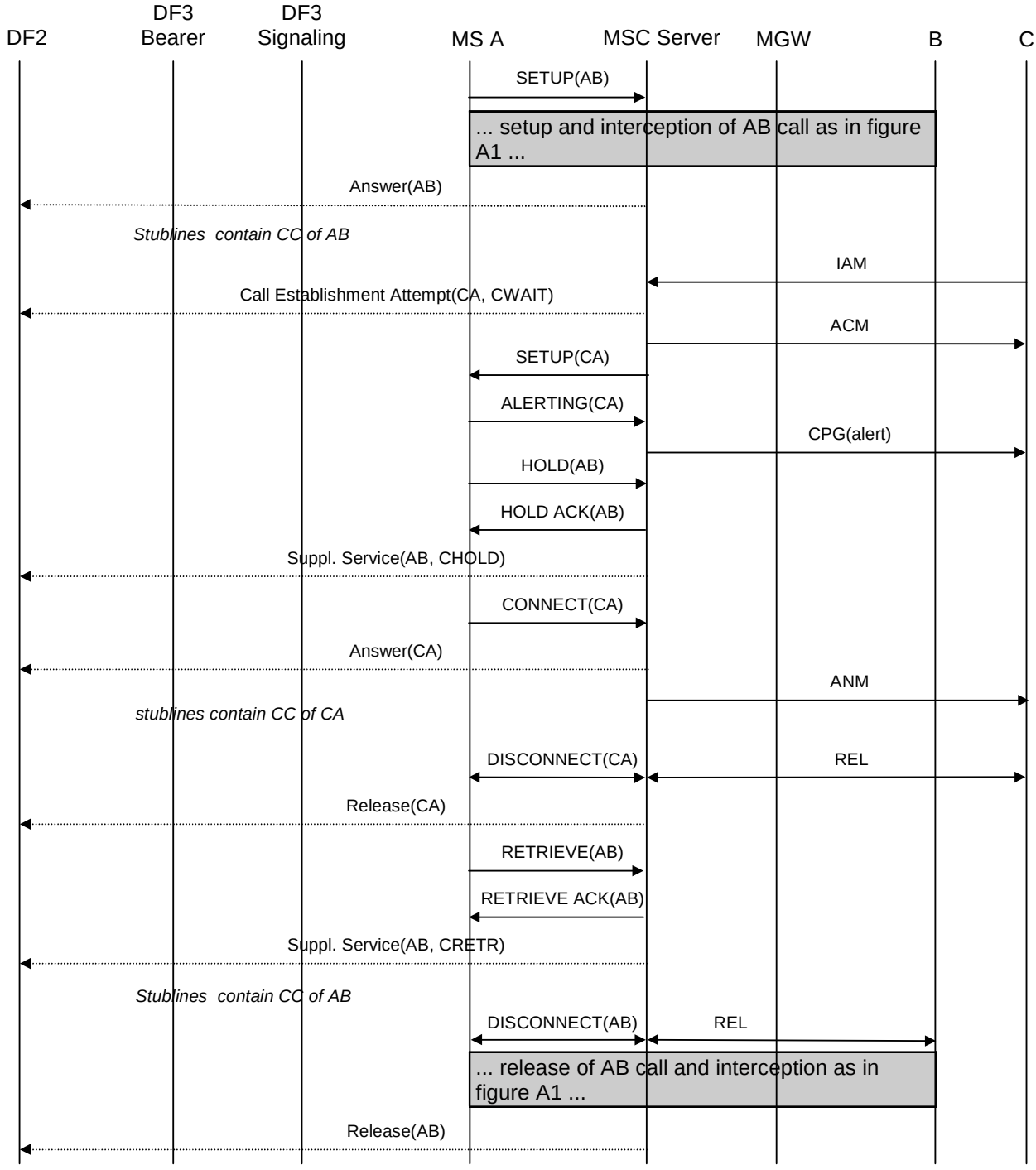


Figure A.3: Interception of call hold / call waiting - stublines per target

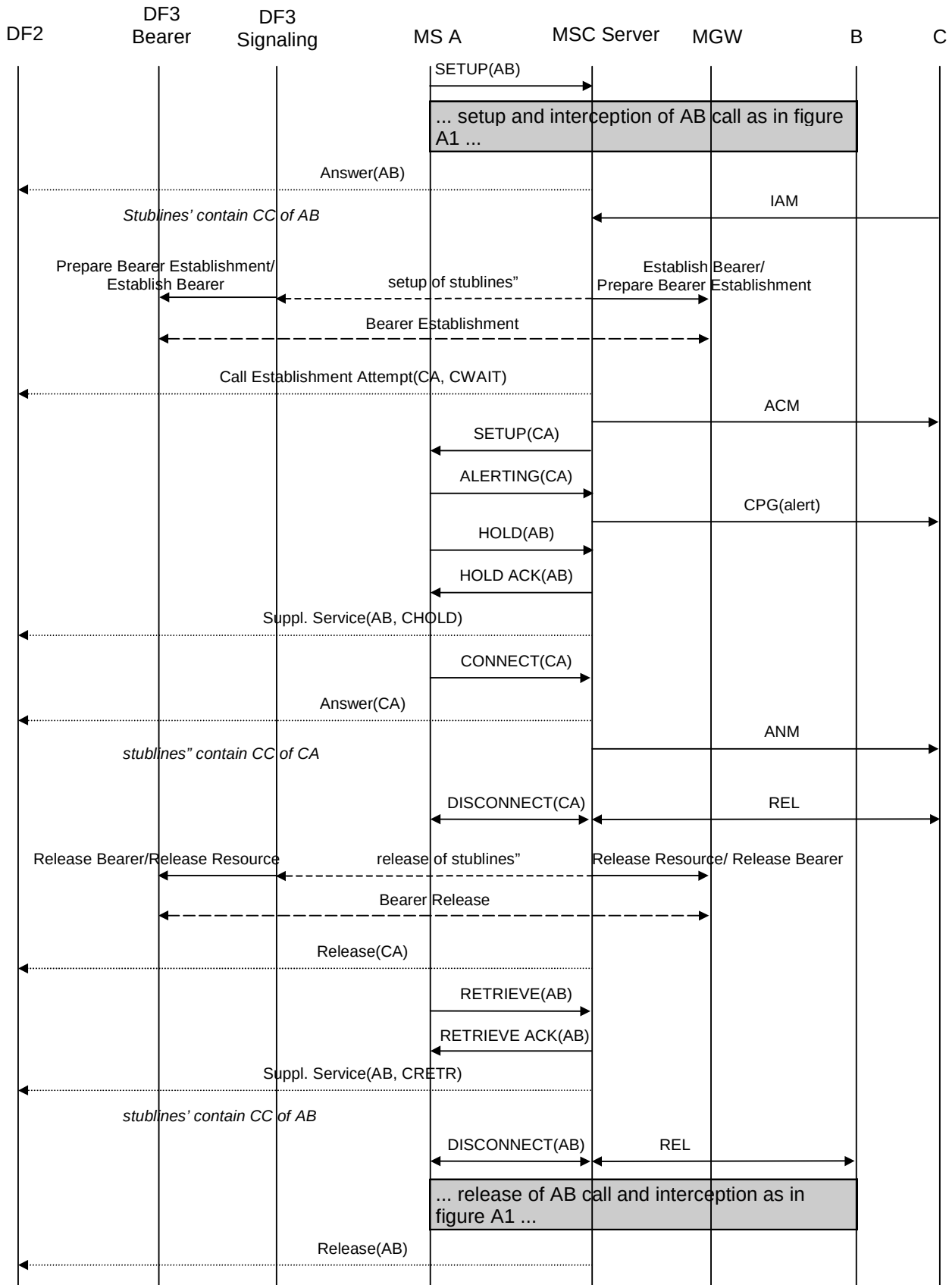


Figure A.4: Interception of call hold / call waiting - stublines per target call

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.

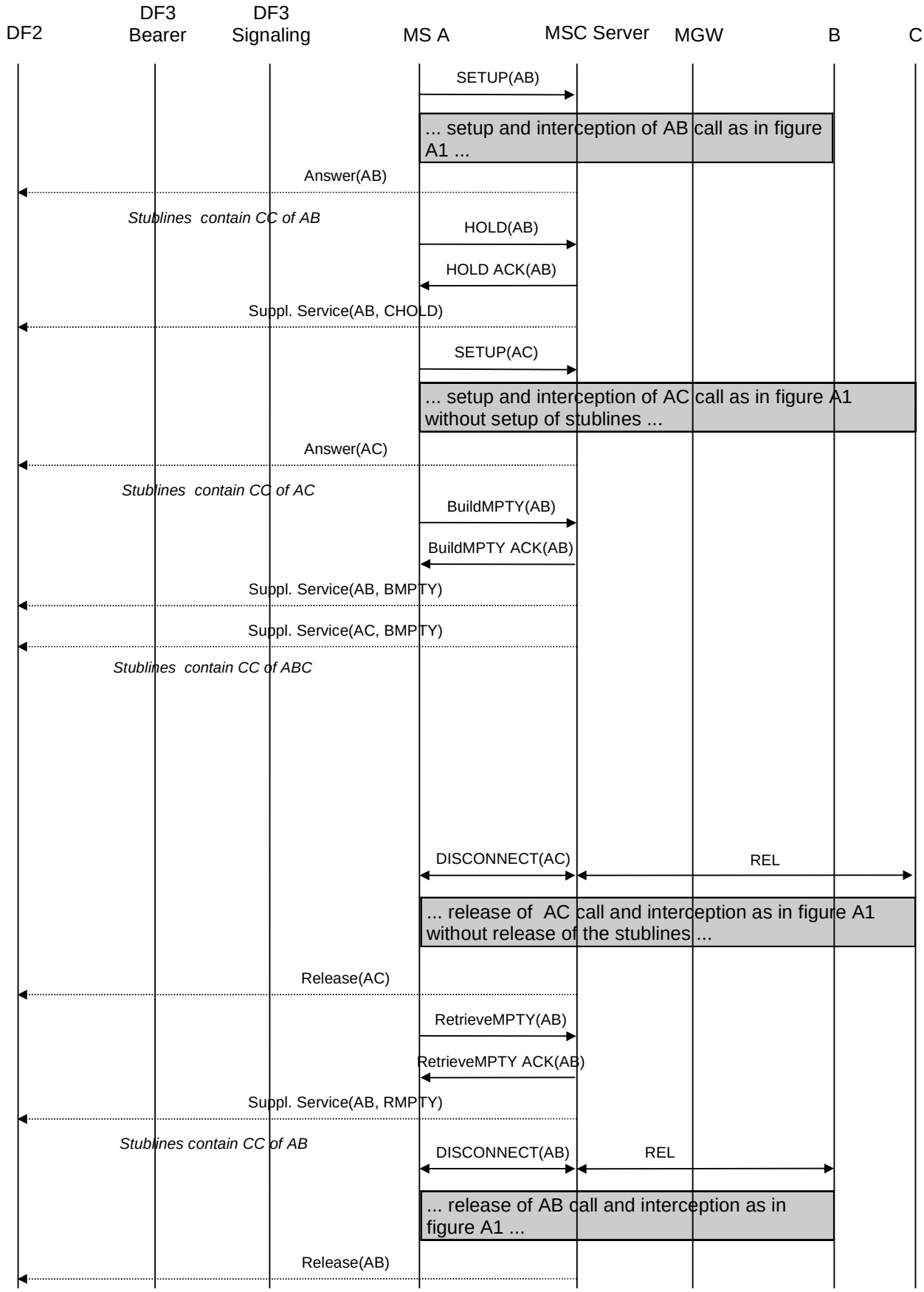


Figure A.5: Interception of multiparty calls - stublines per target

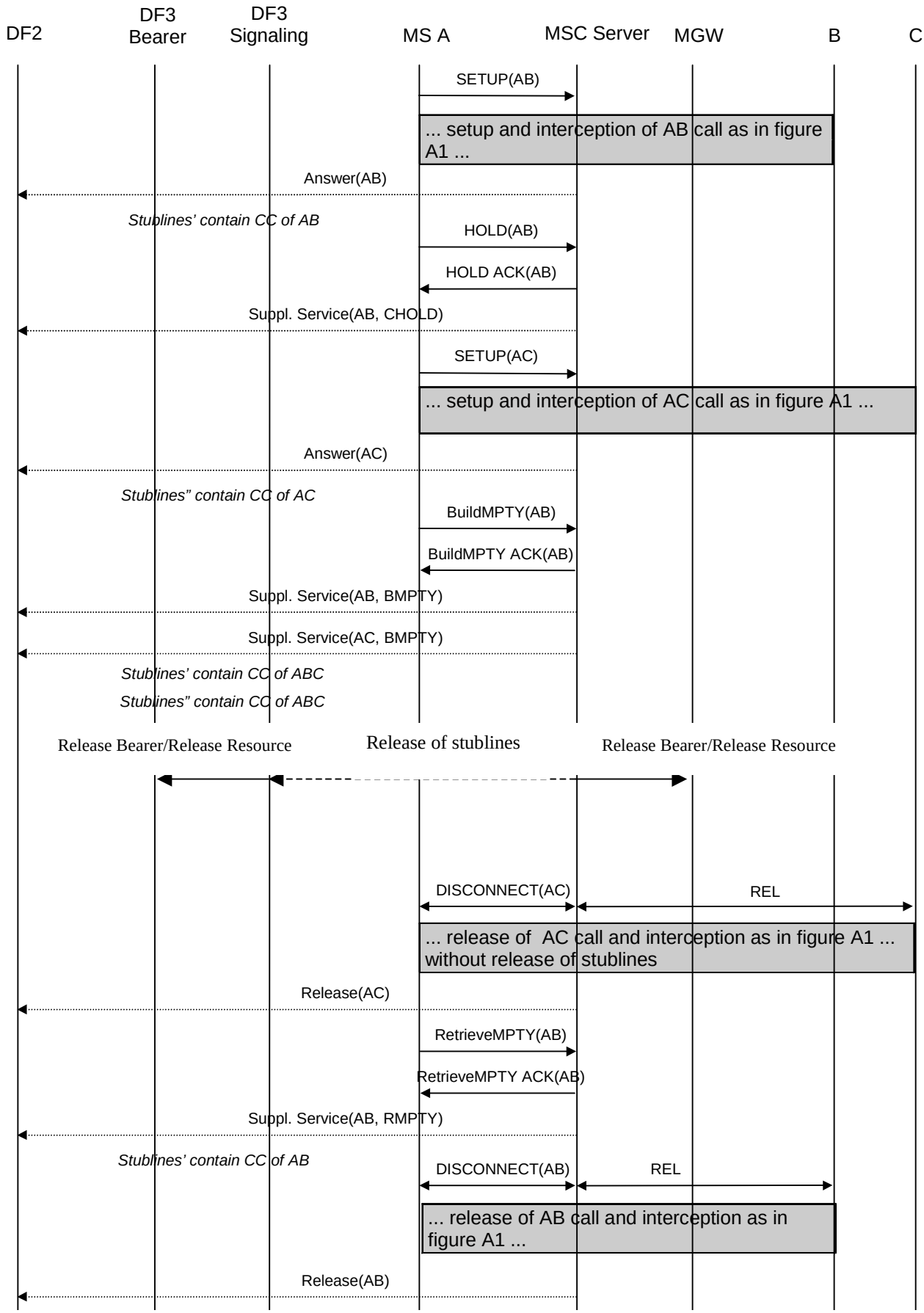


Figure A.6: Interception of multiparty calls - stublines per target call

A.5 Call forwarding / call deflection

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.

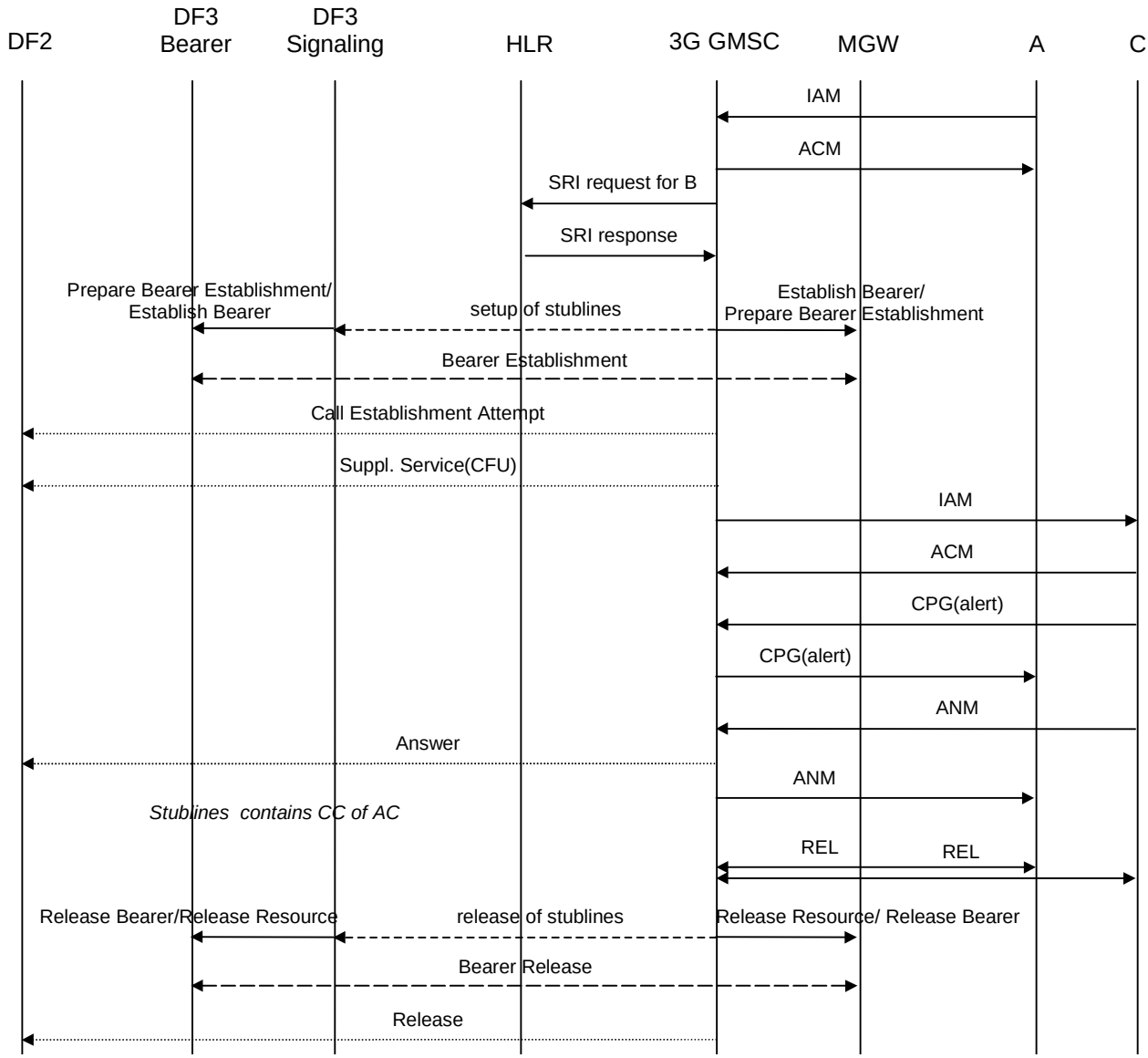


Figure A.7: Interception of unconditional call forwarding

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.

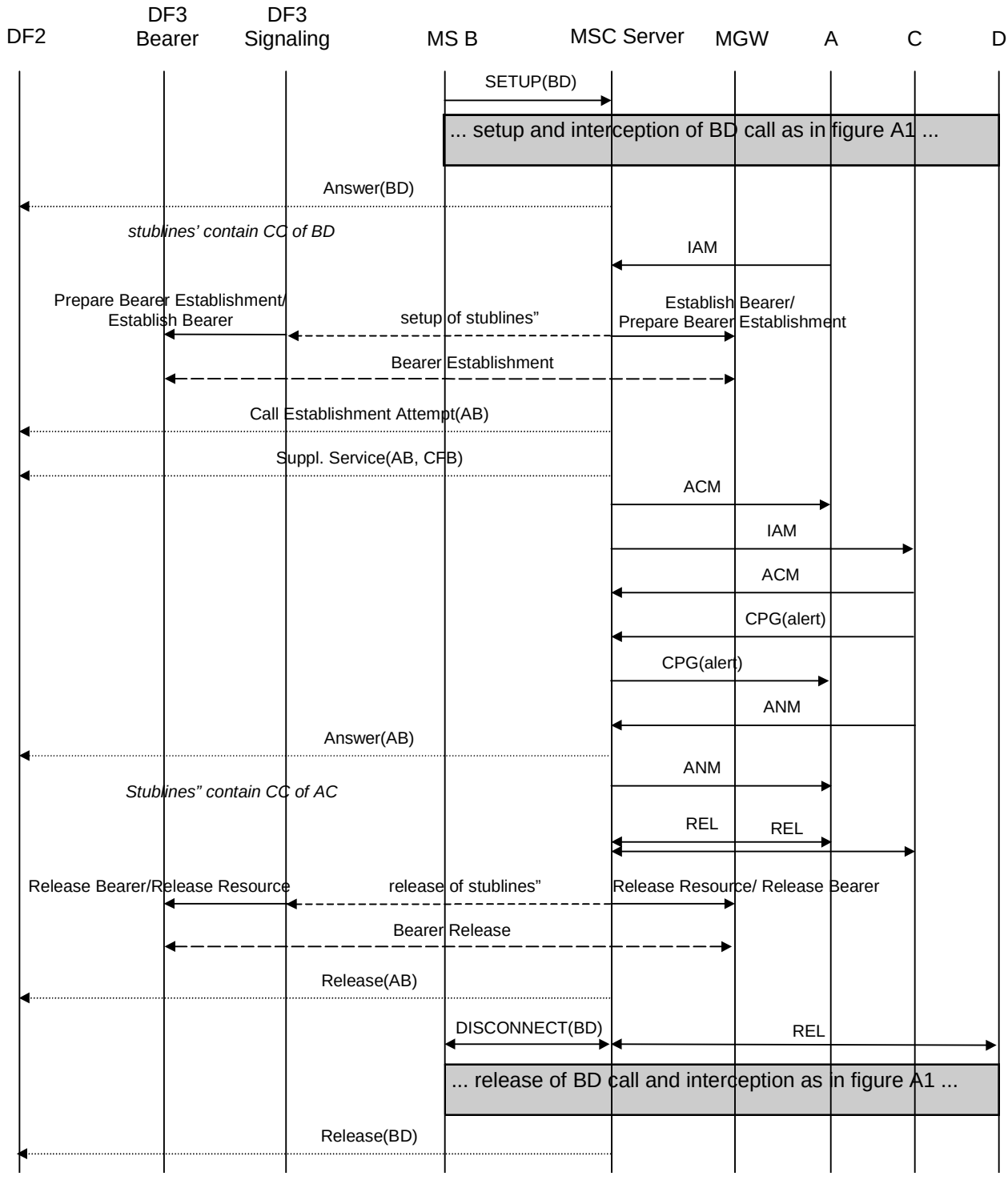


Figure A.8: Interception of call forwarding on busy (network determined)

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.

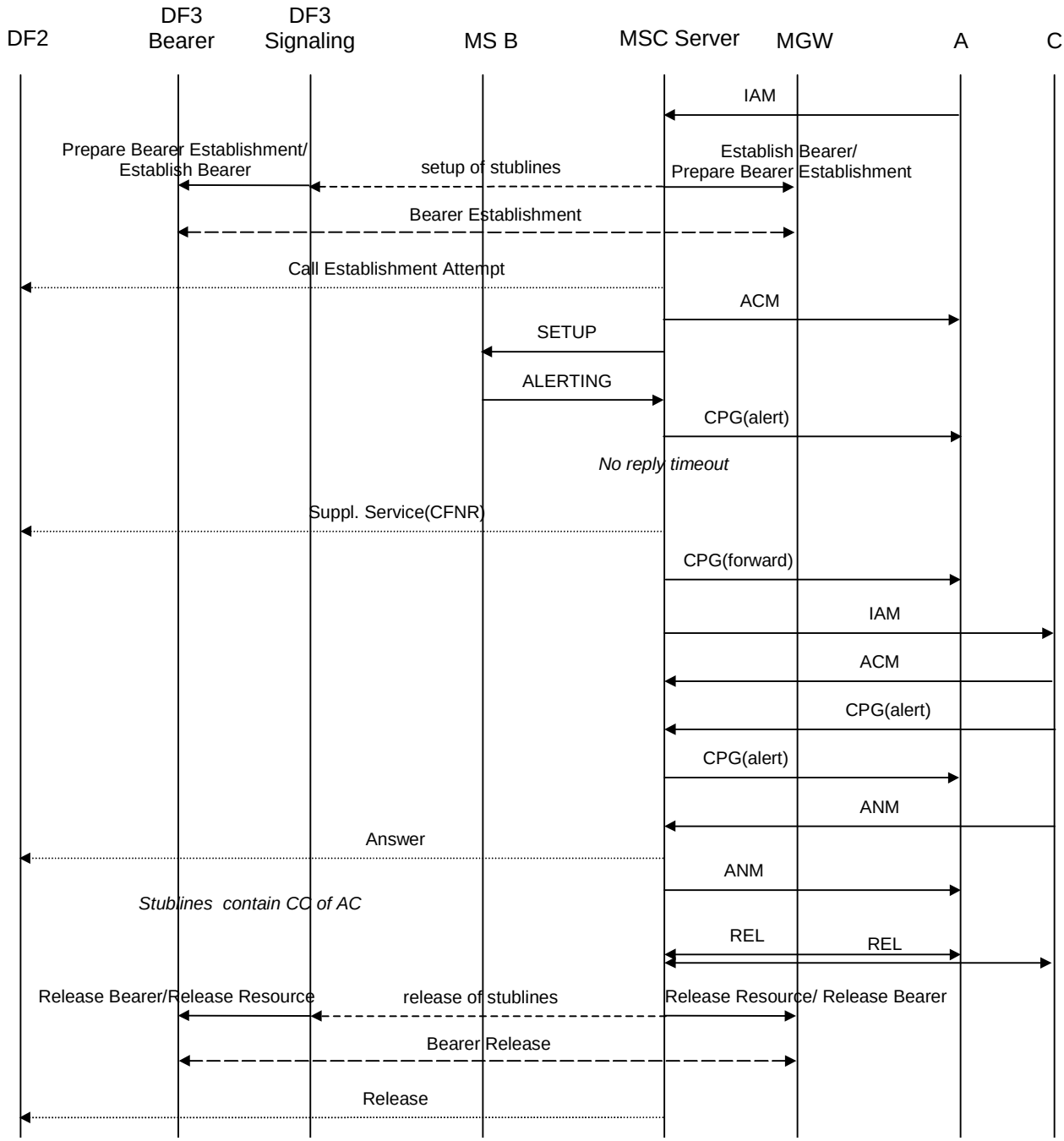


Figure A.9: Interception of call forwarding on no reply

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.

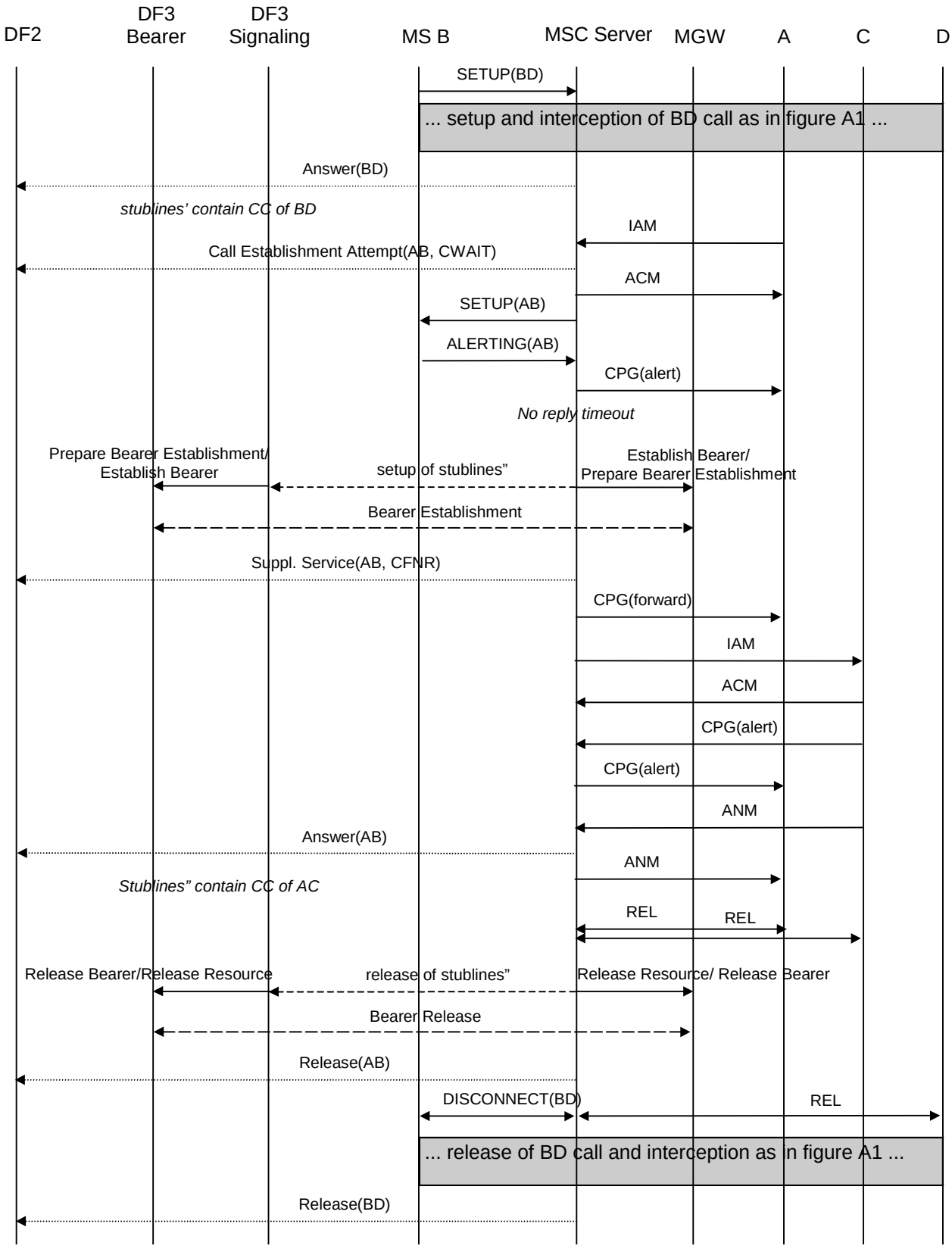


Figure A.10: Interception of call waiting / call forwarding on no reply - stublines per target

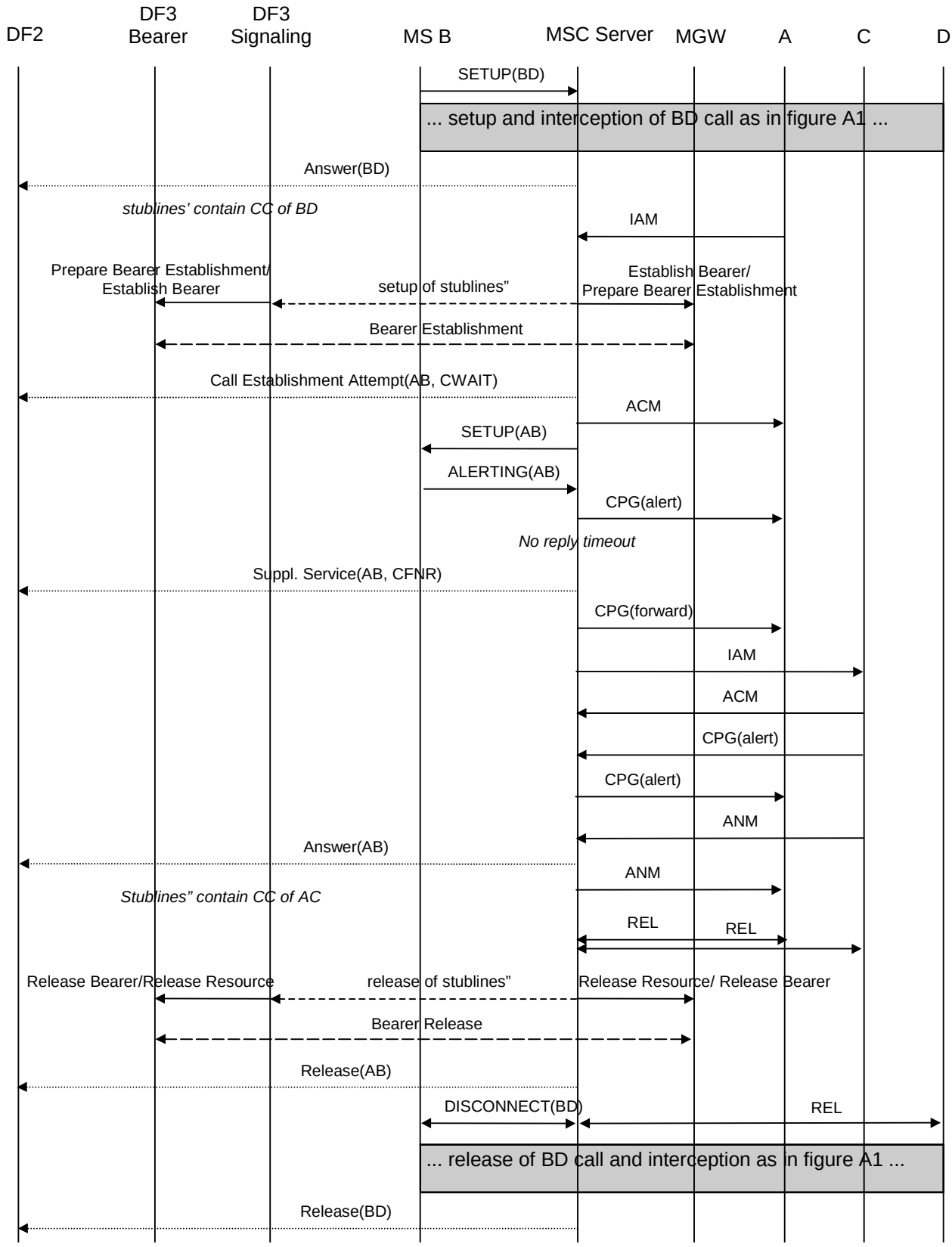


Figure A.11: Interception of call waiting / call forwarding on no reply - stublines per target call

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.

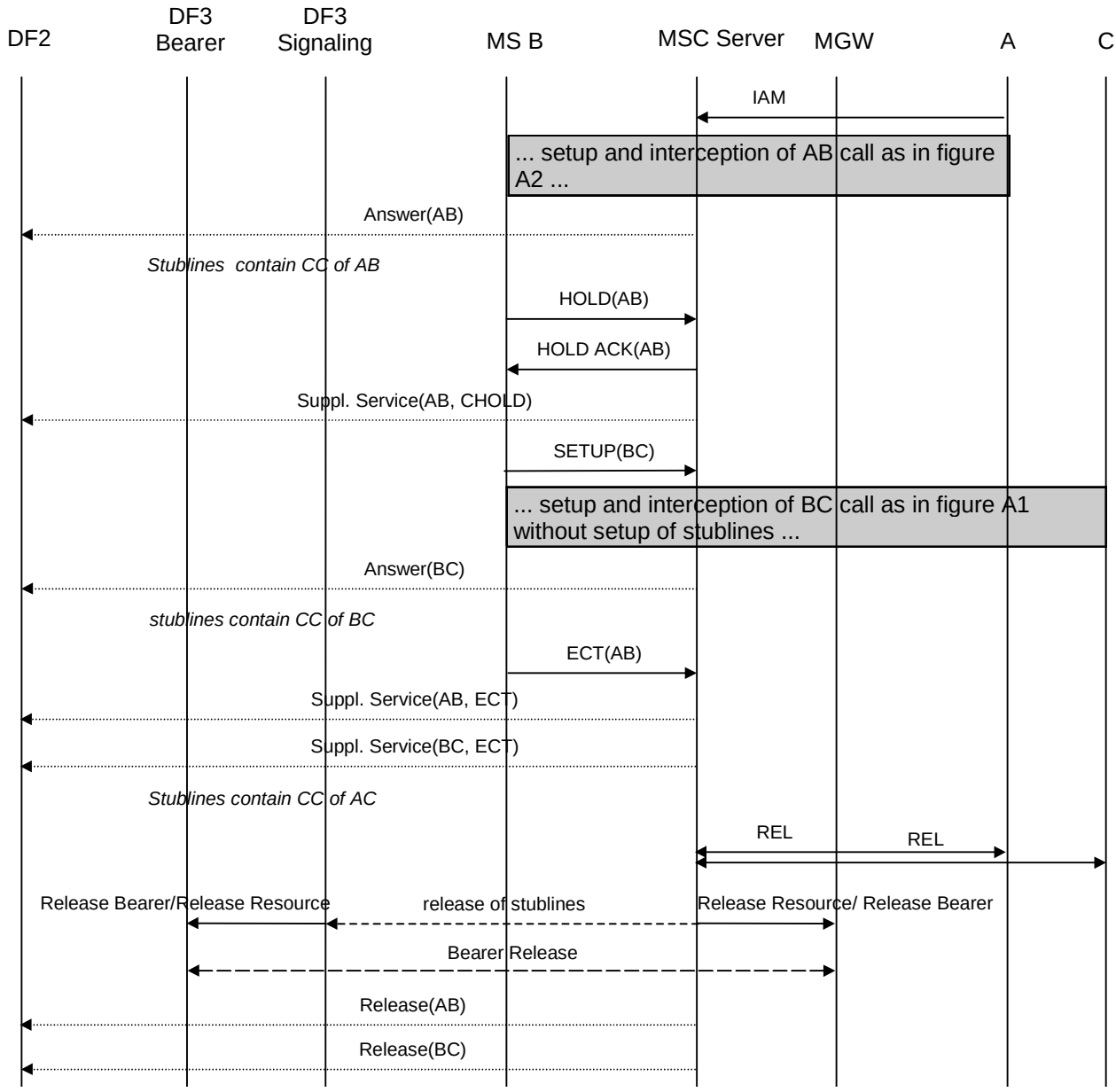


Figure A.12: Interception of explicit call transfer - stublines per target

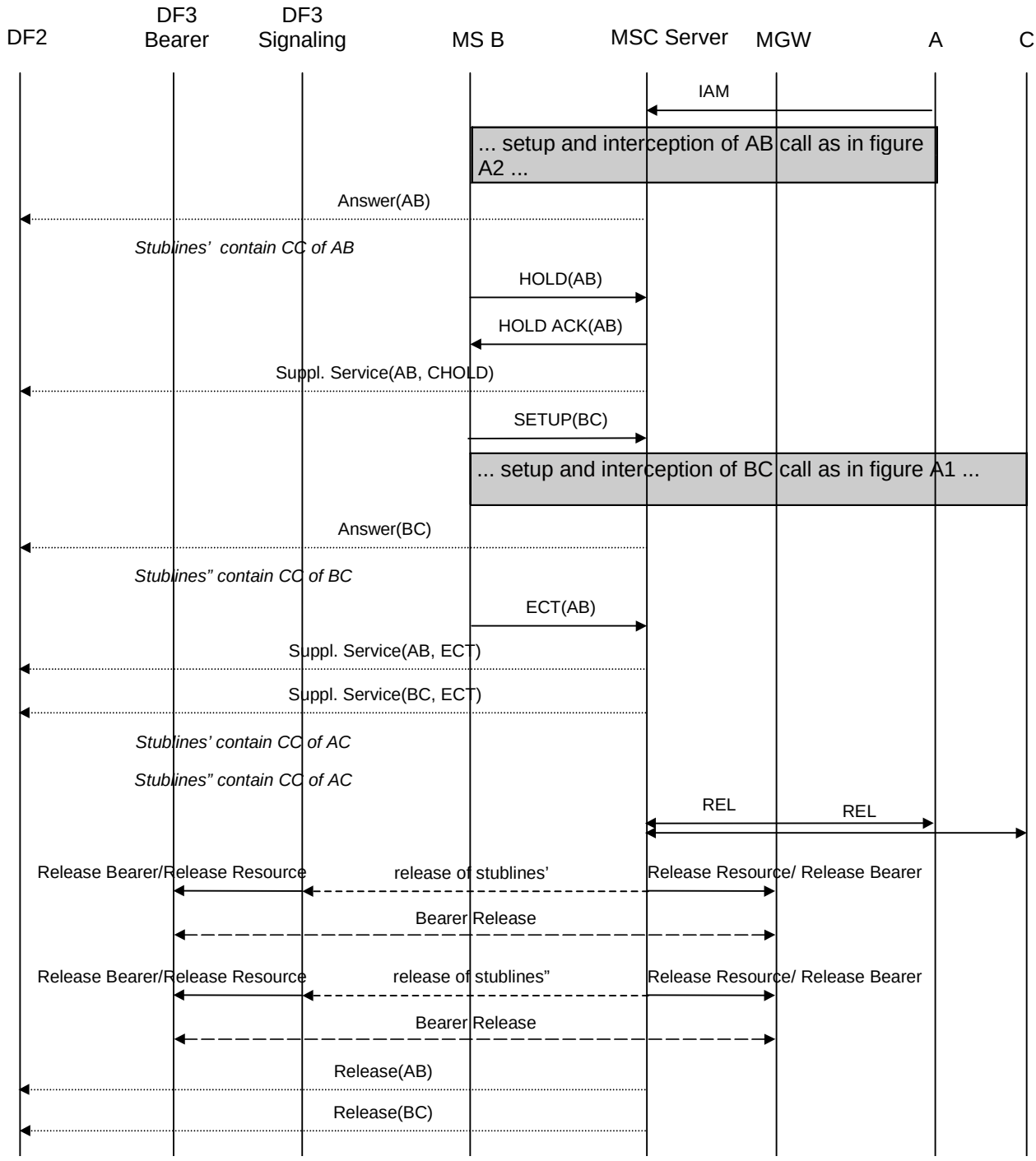


Figure A.13: Interception of explicit call transfer - stublines per target call

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

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.

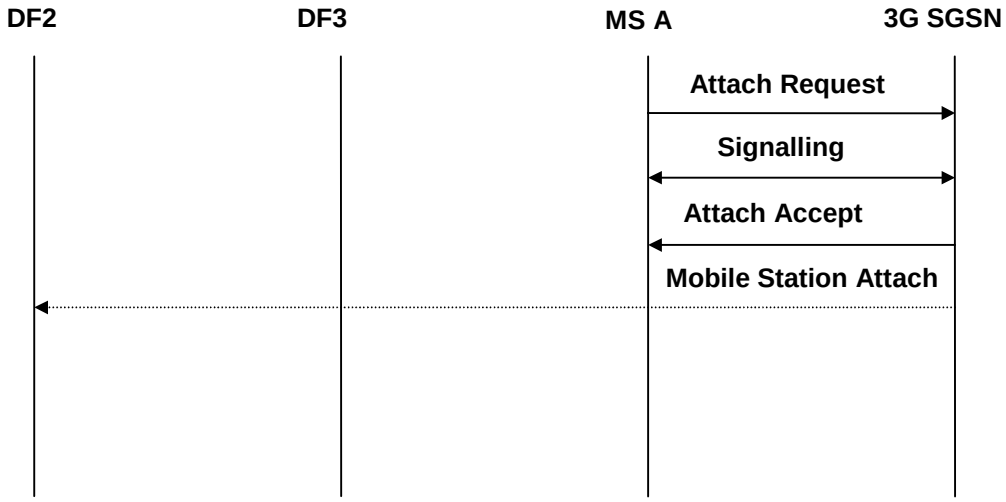


Figure B.1: Interception of mobile originated Mobile Station Attachment

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.

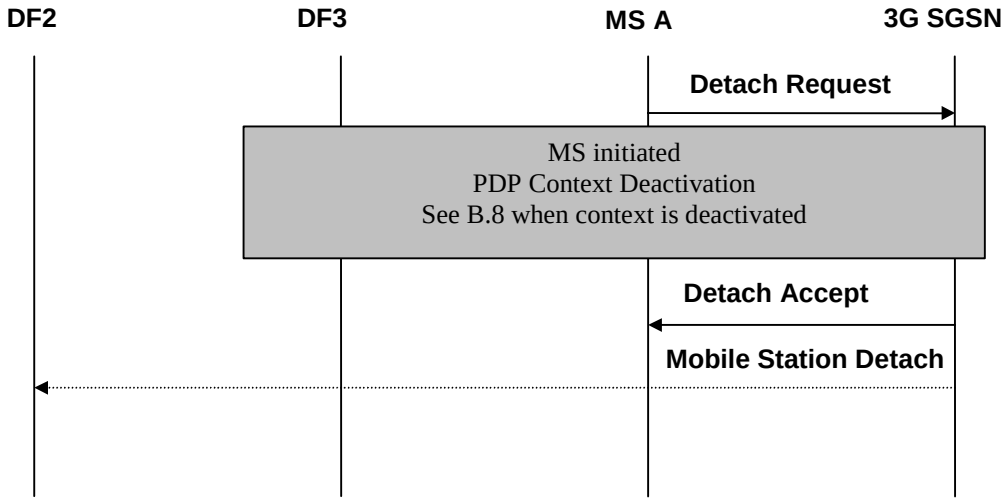
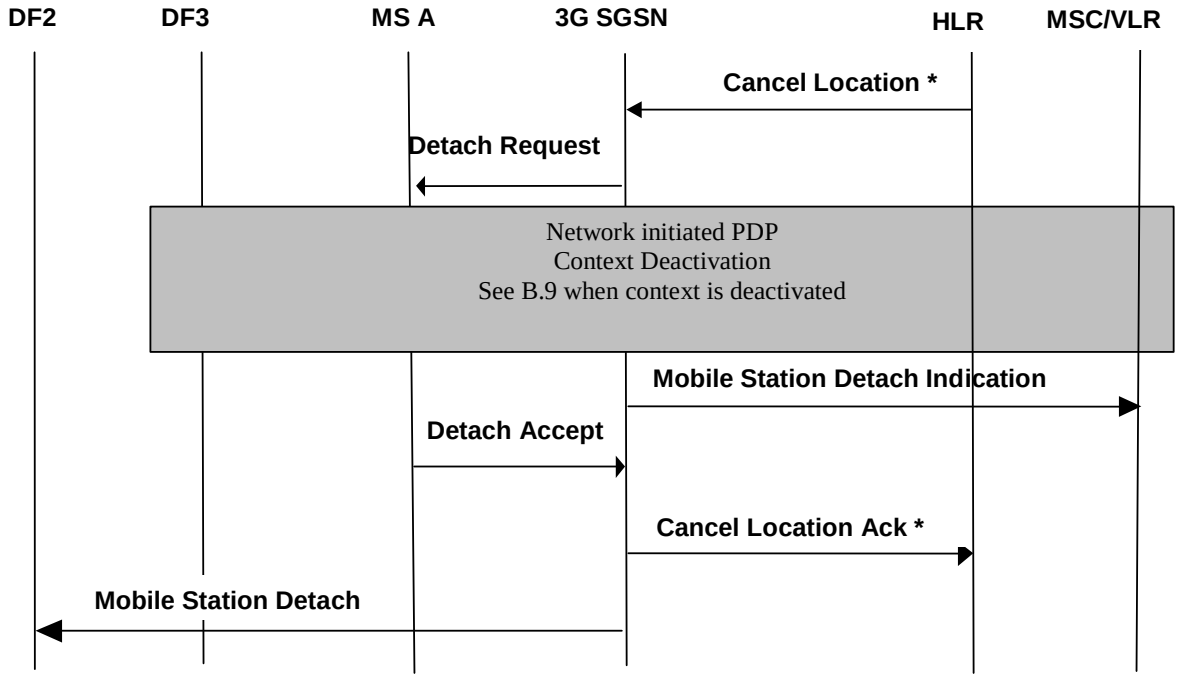


Figure B.2: Interception of mobile originated Mobile Station Detachment

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.

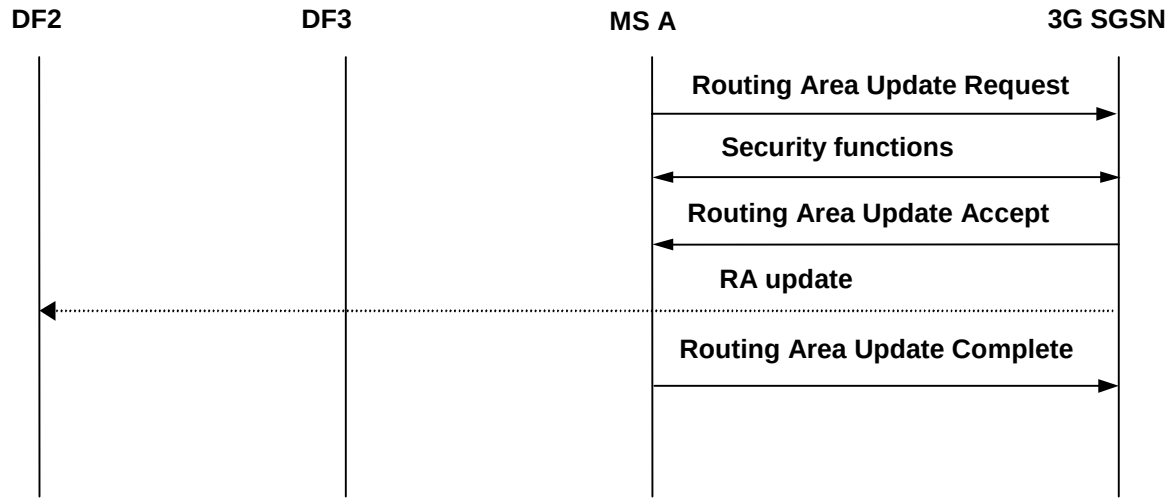


Figure B.4: Interception of an Intra Routing Area Update

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.

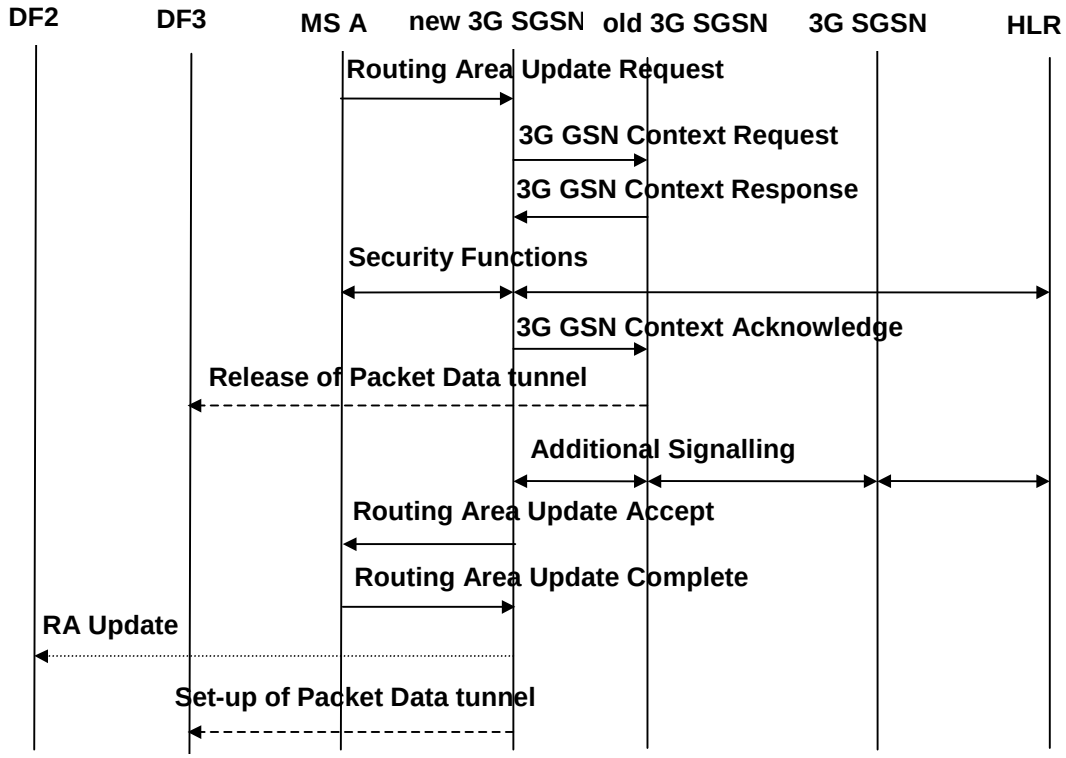


Figure B.5: Interception of an Inter Routing Area Update

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.

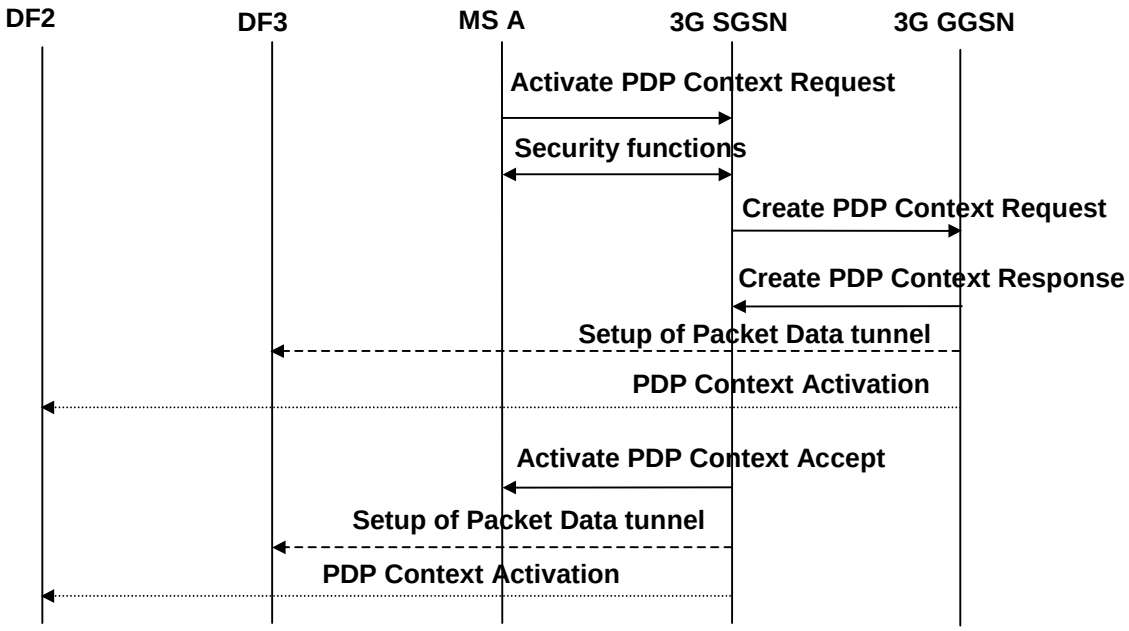


Figure B.6: Interception of a PDP Context Activation

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.

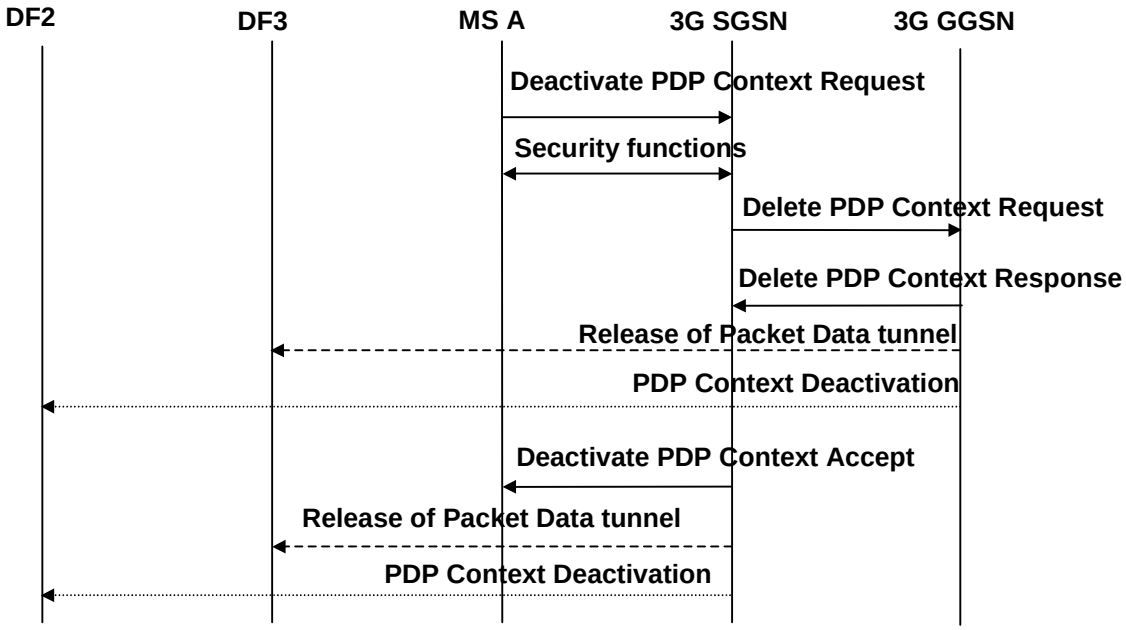


Figure B.7: Interception of a PDP Context Deactivation

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).

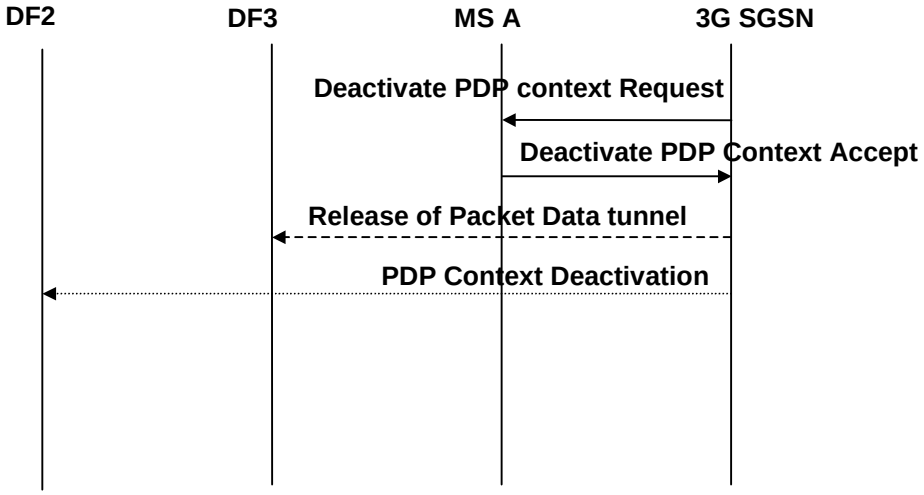


Figure B.8: Interception of a Network initiated PDP Context Deactivation

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.

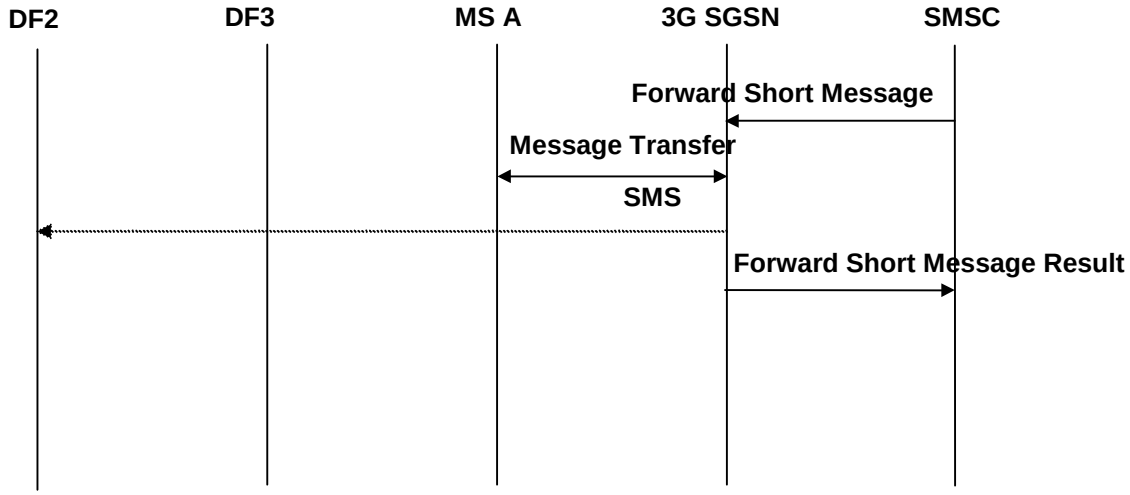


Figure B.9a: MT-SMS interception after 3G SGSN receives notification of SMS delivery to MS(A)

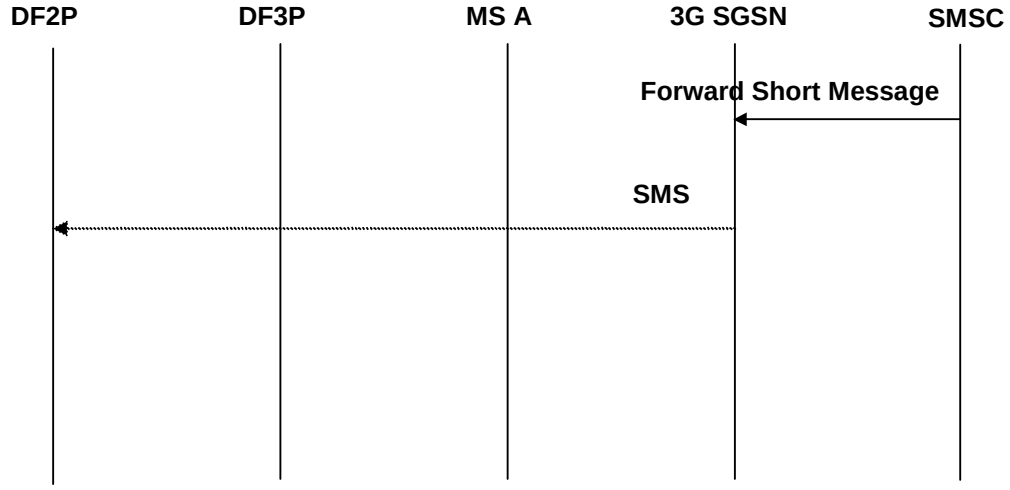


Figure B.9b: MT-SMS interception after 3G SGSN receives SMS from SMSC

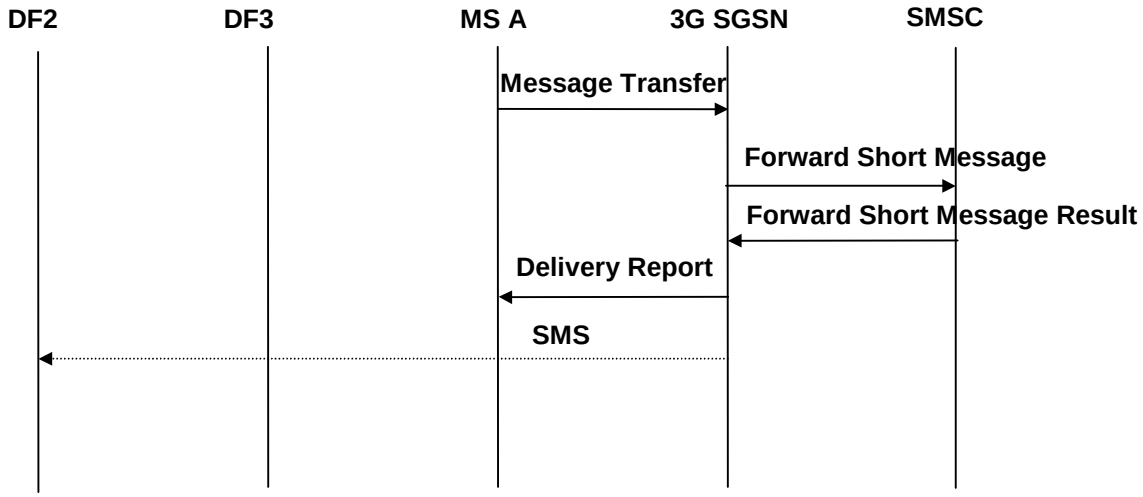


Figure B.10a: MO-SMS interception after 3G SGSN receives notification of SMS delivery from SMSC

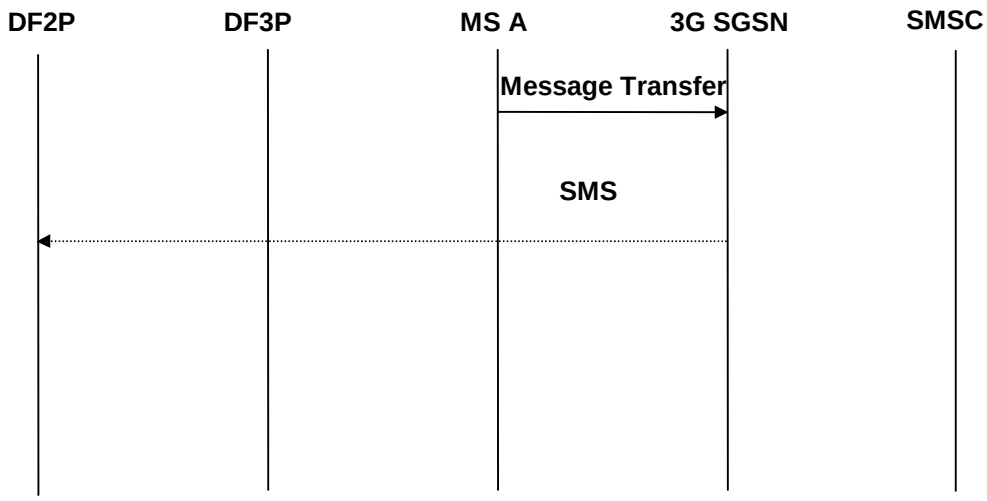


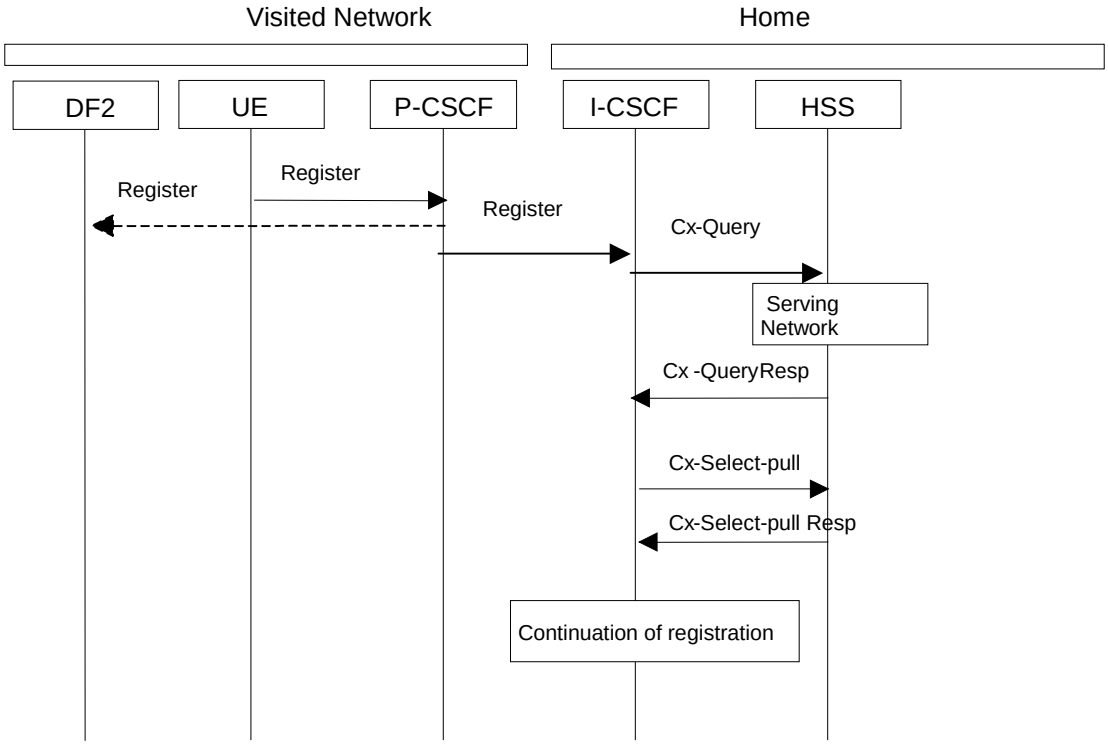
Figure B.10b: MO-SMS interception after 3G SGSN receives SMS from MS(A)

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

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.

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 3GPP 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 (refer to 3GPP TS 23.228 clauses 5.3.2.4 and 5.3.2.5).

Figure C.1.1: Intercept of Start of Multimedia Registration

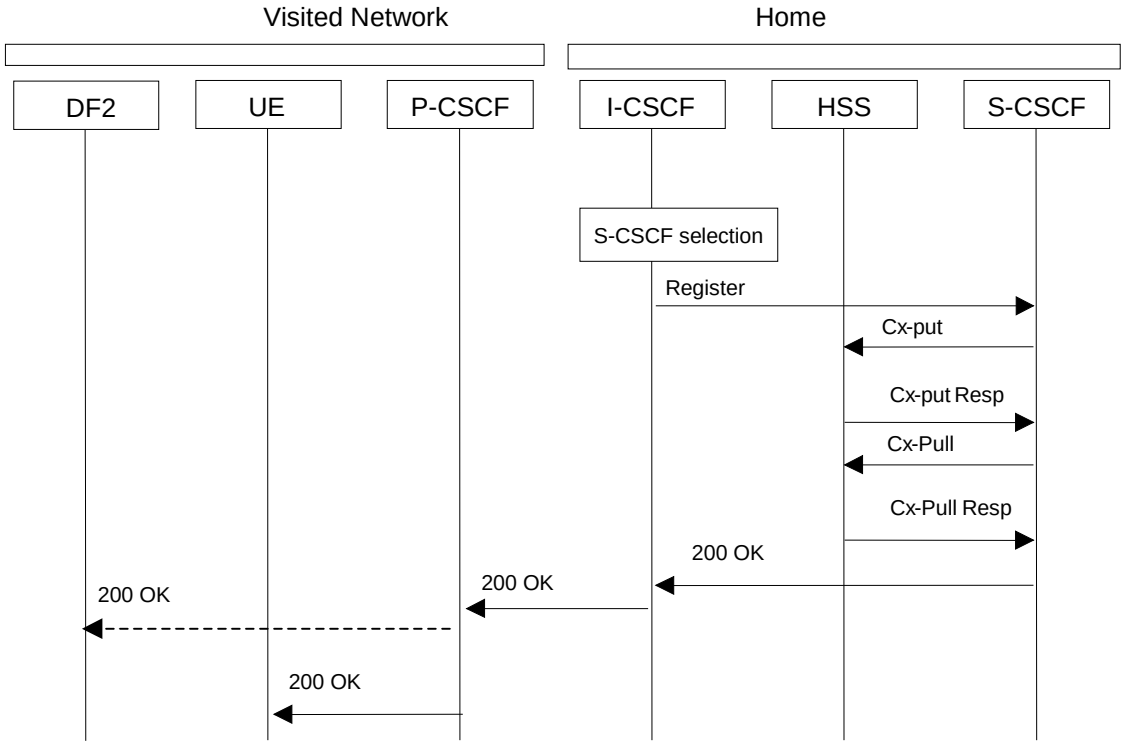


Figure C.1.2: Intercept of Continuation of Multimedia Registration

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 (refer to 3G TS 23.228, clause 5.7.1).

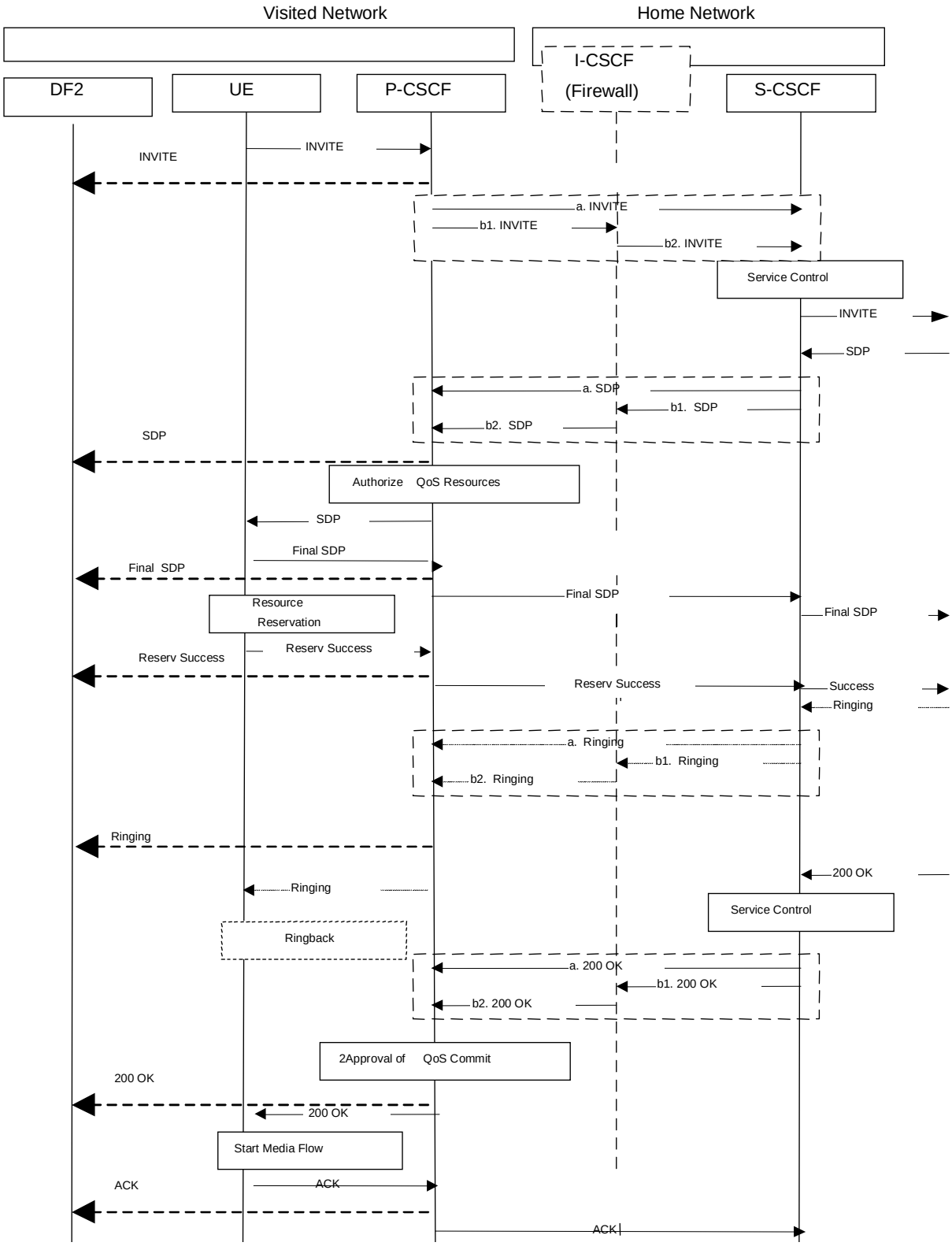


Figure C.2 Intercept of Multimedia Establishment and Answer at Visiting Network

C.3 Multimedia Release

Figure C.3 shows the intercept of the Multimedia Release in the visited network (3G TS 23.228, clause C.2.1 reference available).

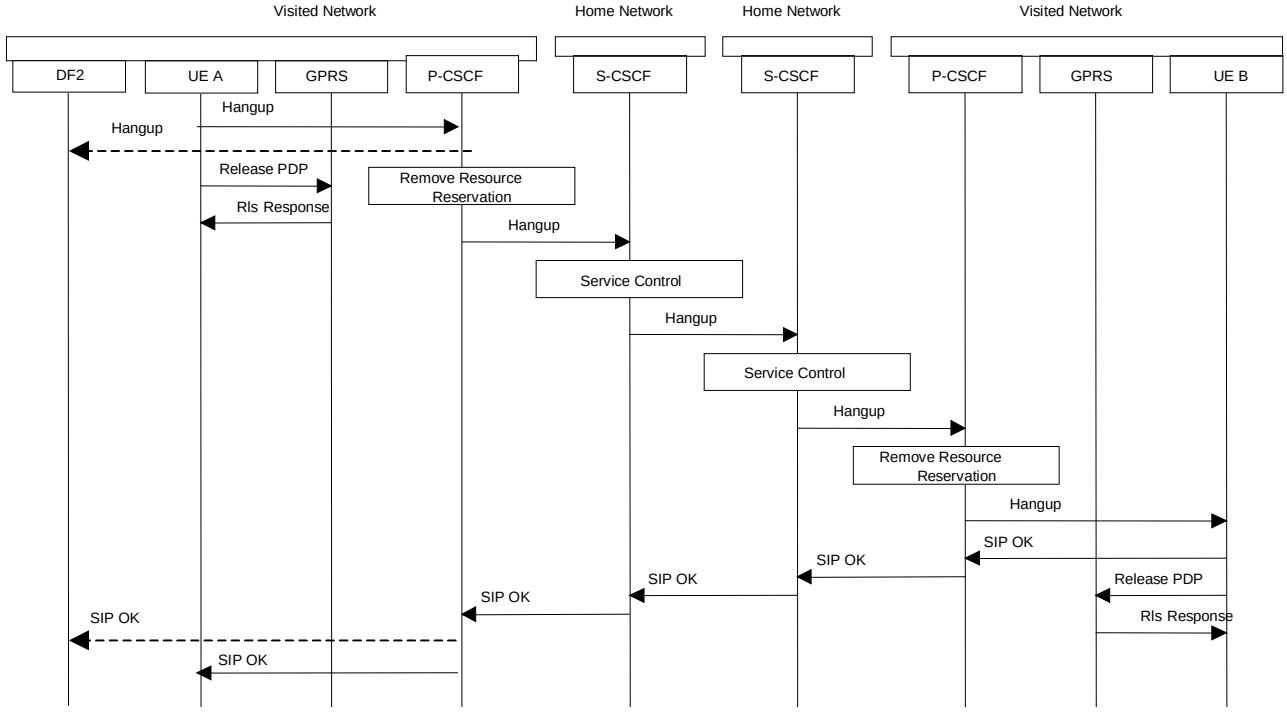


Figure C.3 Intercept of Multimedia Release at Visiting Network

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

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 3GPP TS 23.205.
It should be noted that other means exist with H.248 to achieve similar interception.

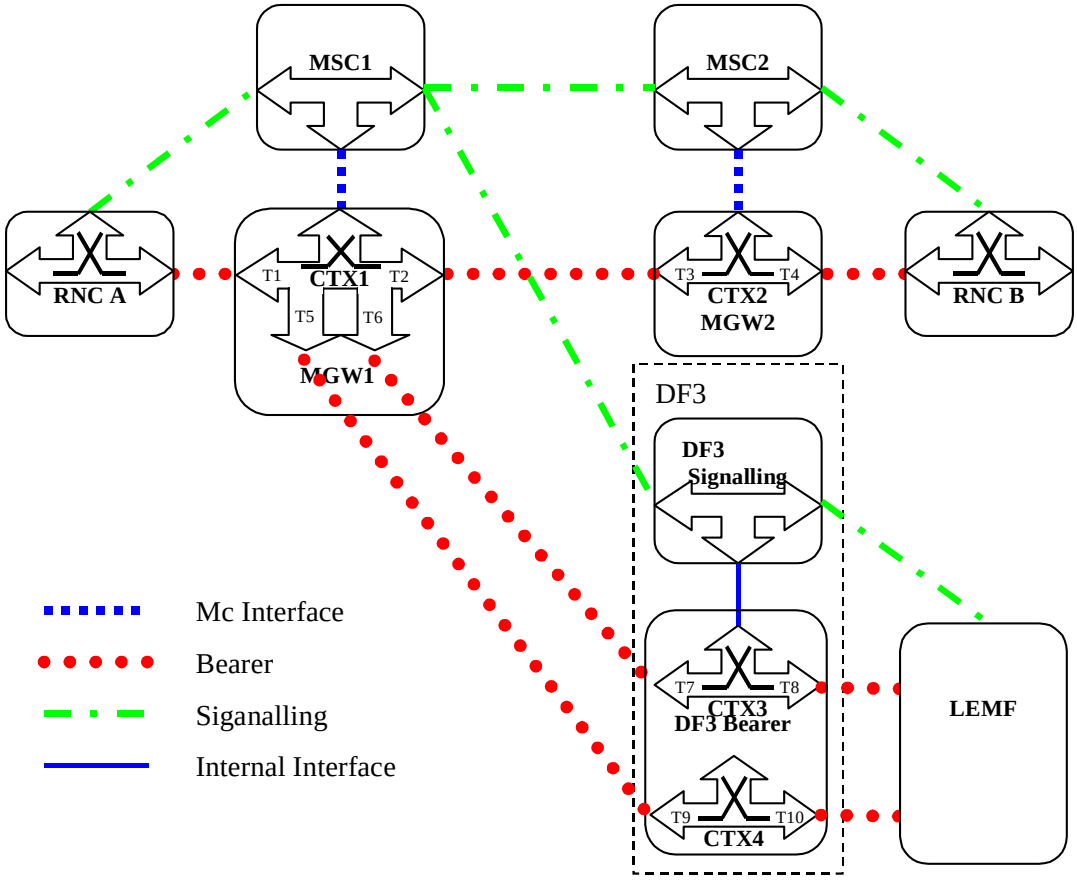


Figure D.1: Mobile to Mobile call originating side is target (network model)

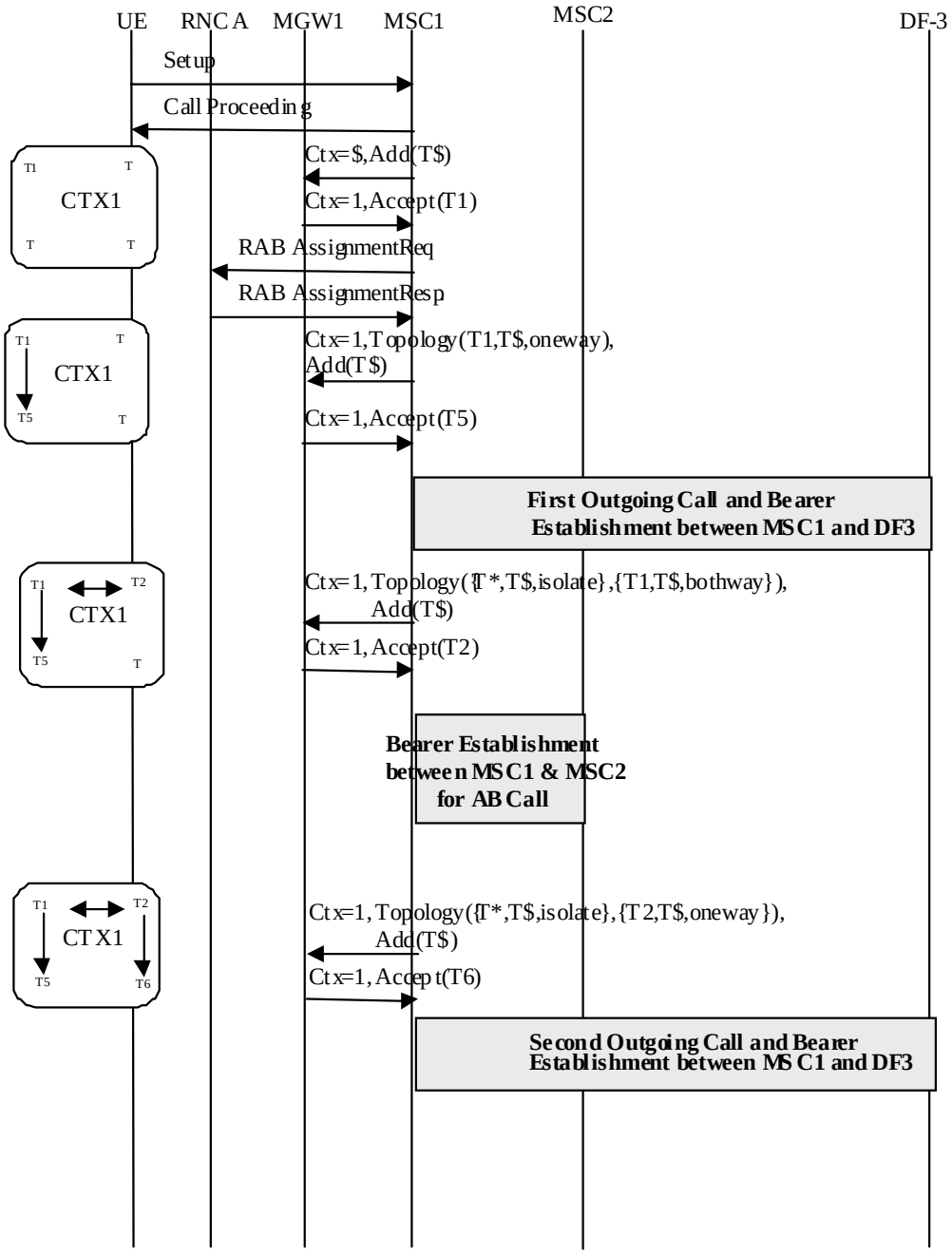


Figure D.2: Mobile to Mobile call originating side is target

Annex 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	001	-		Addition of parameters to the X3-Interface	3.0.0	3.1.0	Security
2000-03	SP-11	SP-010137	002	-		Correction of Location information parameters in interception event records	3.1.0	3.2.0	Security
2000-03	SP-11	SP-010146	003	-		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	004	1	B	Update of TS 33.107 for Release 5	4.0.0	5.0.0	SEC1-LI
2001-12	SP-14	SP-010612	010	-	A	Start of secondary interception of an active PDP context	4.1.0	5.1.0	SEC1-LI
2001-12	SP-14	SP-010613	011	-	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	014	-	A	Correct the MO-SMS and MT-SMS events	4.1.0	5.1.0	SEC1-LI
2001-12	SP-14	SP-010615	016	-	A	Source of PDP context initiation	4.1.0	5.1.0	SEC1-LI
2002-03	SP-15	SP-020109	017	-	B	PDP context Deactivation cause	5.1.0	5.2.0	SEC1-LI
2002-03	SP-15	SP-020110	018	-	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	021	-	B	Inter-SGSN RA update with active PDP context	5.1.0	5.2.0	SEC1-LI
2002-03	SP-15	SP-020112	022	-	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	023	-	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	024	-	B	Addition of SMS type information	5.2.1	5.3.0	SEC1-LI
2002-06	SP-16	SP-020345	025	-	C	Inclusion of Serving System IRI in TS 33.107	5.2.1	5.3.0	SEC1-LI
2002-09	SP-17	SP-020511	026	-	F	Essential clarification to the Timestamp IE	5.3.0	5.4.0	SEC1-LI
2002-09	SP-17	SP-020511	027	-	F	Additional X3-interface parameters	5.3.0	5.4.0	SEC1-LI
2002-12	SP-18	SP-020702	028	-	F	Event Time	5.4.0	5.5.0	SEC1-LI
2002-12	SP-18	SP-020704	029	-	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	030	-	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	031	-	F	Missing QoS Parameter in IRI	5.5.0	5.6.0	SEC1-LI
2003-09	SP-21	SP-030479	032	-	B	TEL URL for IMS interception identity (Release 6)	5.5.0	6.0.0	SEC1-LI
2003-09	SP-21	SP-030479	032	-	D	Stereo delivery to LEMF	5.5.0	6.0.0	SEC1-LI
2003-12	SP-22	SP-030590	034	-	F	MSISDN/IMEI clarification for GPRS interception	6.0.0	6.1.0	SEC1-LI
2003-12	SP-22	SP-030591	035	-	F	Reporting TEL URL	6.0.0	6.1.0	SEC1-LI
2004-06	SP-24	SP-040397	036	-	F	Correction on Network initiated Mobile Station Detach signalling flow	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040398	037	-	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	038	-	F	Correction on the use of session initiator parameter	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040400	039	-	F	Correction to HLR interception event name	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040401	040	-	B	Clarification for Push to talk over Cellular	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040402	041	-	F	Adding an encryption parameter to IRI across X2 interface	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040403	042	-	F	References	6.1.0	6.2.0	SEC1-LI
2004-06	SP-24	SP-040404	043	-	F	Enhancements for the Functional Architecture chapter	6.1.0	6.2.0	SEC1-LI
2004-09	SP-25	SP-040693	044	-	F	Correction on the use of session initiator parameter	6.2.0	6.3.0	SEC1-LI
2004-09	SP-25	SP-040693	045	-	F	ICE (Intercepting Control Elements), INE (Intercepting Network Elements) definition	6.2.0	6.3.0	SEC1-LI
2004-09	SP-25	SP-040693	046	-	F	Clarification to SMS interception	6.2.0	6.3.0	SEC1-LI

2004-09	SP-25	SP-040693	047	-	F	Replace SIP URL with SIP URI	6.2.0	6.3.0	SEC1-LI
2004-12	SP-26	SP-040850	048	-	B	Lawful Interception for WLAN Interworking	6.3.0	6.4.0	SEC1-LI
2004-12	SP-26	SP-040850	049	-	F	33.107 Cleanup	6.3.0	6.4.0	SEC1-LI
2004-12	SP-26	SP-040850	050	-	B	Clarification on MMS interception	6.3.0	6.4.0	SEC1-LI
2005-06	SP-28	SP-050256	052	-	F	Correction on the use of identities for I-WLAN lawful interception	6.4.0	6.5.0	SEC1-LI

History

Document history		
V6.4.0	December 2004	Publication
V6.5.0	June 2005	Publication