ETSI TS 101 671 V2.5.0 (2002-11)

Technical Specification

Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic

Reference

RTS/LI-00001

Keywords

data, handover, interface, security, speech

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

Important notice

Copyright Notification

Contents

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 Technical Committee Lawful Interception (LI).

1 Scope

The present document is step 3 of a three-step approach to describe a generic Handover Interface (HI) for the provision of lawful interception from a Network Operator, an Access Provider or a Service Provider (NWO/AP/SvP) to the Law Enforcement Agencies (LEAs). The provision of lawful interception is a requirement of national law, which is usually mandatory for the operation of any telecommunication service.

Step 1 contains the requirements for lawful interception from a users (LEAs) point of view and is published in TS 101 331 [1].

Step 2 describes the derived network functions and the general architecture (or functional model) and is published in ES 201 158 [2].

The present document specifies:

- the *generic flow of information* as well as the procedures and information elements, which are applicable to any future telecommunication network or service;
- the network/service specific protocols relating to the provision of lawful interception at the Handover Interface, for the following networks/services:
  - switched circuit; and
  - packet data.

The technologies covered in the present document are: GSM, TETRA, GPRS, ISDN and PSTN.

NOTE 1: Handover for TETRA is not fully developed.

NOTE 2: As new networks and/or services are developed, the present document will be expanded as the relevant standards become available.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies".

[2] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[3] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

[4] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".

[5] ETSI EN 300 403-1 (V1.2.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

[6] ETSI EN 300 061-1: "Integrated Services Digital Network (ISDN); Subaddressing (SUB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[7] ETSI EN 300 097-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[8] ETSI EN 300 138-1: "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[9] ETSI EN 300 185-1: "Integrated Services Digital Network (ISDN); Conference call, add-on (CONF) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[10] ETSI EN 300 188-1: "Integrated Services Digital Network (ISDN); Three-Party (3PTY) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[11] ETSI EN 300 286-1: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[12] ETSI EN 300 369-1 (V1.2.4): "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[13] ETSI EN 300 196-1 (V1.2.2): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[14] ETSI ETS 300 974: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Application Part (MAP) specification (GSM 09.02)".

[15] ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[16] ITU-T Recommendation X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[17] ITU-T Recommendation X.880: "Information technology - Remote Operations: Concepts, model and notation".

[18] ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".

[19] ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".

[20] ETSI EN 300 122-1: "Integrated Services Digital Network (ISDN); Generic keypad protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[21] ETSI TS 101 509: "Digital cellular telecommunications system (Phase 2+) (GSM); Lawful interception; Stage 2 (GSM 03.33)".

[22] ETSI TS 100 927: "Digital cellular telecommunications system (Phase 2+) (GSM); Numbering, addressing and identification (GSM 03.03)".

[23] ETSI TS 101 347: "Digital cellular telecommunications system (Phase 2+) (GSM); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across Gn and Gp Interface (GSM 09.60)".

[24] IETF RFC 959: "File Transfer Protocol".

[25] ITU-T Recommendation Q.763: "Signalling System No.7 - ISDN User Part formats and codes".

[26] ETSI TS 101 393: "Digital cellular telecommunications system (Phase 2+) (GSM); General Packet Radio Service (GPRS); GPRS Charging (GSM 12.15)".

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

[28] IETF RFC 793: "Transmission Control Protocol".

[29] ETSI EN 300 089: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Service description".

[30] ETSI TS 100 940: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile radio interface layer 3 specification (GSM 04.08)".

[31] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".

[32] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[33] ETSI TS 129 060: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS);General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface(3GPP TS 29.060)".

[34] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS);3G security; Handover interface for Lawful Interception (LI)(3GPP TS 33.108)".

[35] ETSI TS 125 413: "Universal Mobile Telecommunications System (UMTS);UTRAN Iu interface RANAP signalling(3GPP TS 25.413)".

[36] ITU-T Recommendation Q.731.3: "Stage 3 description for number identification supplementary services using Signalling System No. 7: Calling line identification presentation (CLIP)".

[37] ITU-T Recommendation Q.951: "Stage 3 description for number identification supplementary services using DSS 1".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access provider: provides a user of some network with access from the user's terminal to that network

NOTE: This definition applies specifically for the present document. In a particular case, the access provider and network operator may be a common commercial entity.

activation/deactivation of supplementary services: procedures for activation, which is the operation of bringing the service into the "ready for invocation" state, and deactivation, which is the complementary action

(to) buffer: temporary storing of information in case the necessary telecommunication connection to transport information to the LEMF is temporarily unavailable

call: any temporarily switched connection capable of transferring information between two or more users of a telecommunications system

NOTE: In this context a user may be a person or a machine.

Communication IDentifier (CID): See definition in clause 6 of TS 101 671.

CC link: communication channel for HI3 information between a mediation function and a LEMF

NOTE: It is used for transmission of the Content of Communication. This term refers to circuit switched only.

CC link identifier: See definition in clause A.1 of TS 101 671.

communication: information transfer according to agreed conventions

Communication Identity Number (CIN): See definition in clause 6 of TS 101 671.

Content of Communication (CC): information exchanged between two or more users of a telecommunications service, excluding intercept related information

NOTE: This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Handover Interface (HI): physical and logical interface across which the interception measures are requested from network operator/access provider/service provider, and the results of interception are delivered from a network operator/access provider/service provider to a law enforcement monitoring facility

identity: technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis

information: intelligence or knowledge capable of being represented in forms suitable for communication, storage or processing

NOTE: Information may be represented for example by signs, symbols, pictures or sounds.

Intercept Related Information (IRI): collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (including unsuccessful communication attempts), service associated information or data (e.g. service profile management by subscriber) and location information

interception: action (based on the law), performed by a network operator/access provider/service provider, of making available certain information and providing that information to a law enforcement monitoring facility

NOTE: In the present document the term interception is not used to describe the action of observing communications by a law enforcement agency.

interception configuration information: information related to the configuration of interception

interception interface: physical and logical locations within the network operator's/access provider's/service provider's telecommunications facilities where access to the Content of Communication and intercept related information is provided

NOTE: The interception interface is not necessarily a single, fixed point.

interception measure: technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations

interception subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted

Internal Intercepting Function (IIF): point within a network or network element at which the Content of Communication and the intercept related information are made available

Internal Network Interface (INI): network's internal interface between the Internal Intercepting Function and a mediation function

invocation and operation: describes the action and conditions under which the service is brought into operation

NOTE 1: In the case of a lawful interception this may only be on a particular communication. It should be noted that when lawful interception is activated, it shall be invoked on all communications (invocation takes place either subsequent to or simultaneously with activation). Operation is the procedure which occurs once a service has been invoked.

NOTE 2: The definition is based on [19], but has been adapted for the special application of lawful interception, instead of supplementary services.

Law Enforcement Agency (LEA): organization authorized by a lawful authorization based on a national law to request interception measures and to receive the results of telecommunications interceptions

Law Enforcement Monitoring Facility (LEMF): designated as the transmission destination for the results of interception relating to a particular interception subject

lawful authorization: permission granted to a LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator/access provider/service provider

NOTE: Typically this refers to a warrant or order issued by a lawfully authorized body.

Lawful Interception (LI): See interception.

Lawful Interception IDentifier (LIID): See definition in clause 6 of TS 101 671.

location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject

Mediation Function (MF): mechanism which passes information between a network operator, an access provider or service provider and a Handover Interface, and information between the internal network interface and the Handover Interface

network element: component of the network structure, such as a local exchange, higher order switch or service control processor

Network Element IDentifier (NEID): See definition in clause 6 of TS 101 671.

network identifier: See definition in clause 6 of TS 101 671.

NetWork Operator (NWO): operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means

Quality of Service (QoS): quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc.

NOTE: Quality of Service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

reliability: probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions

result of interception: information relating to a target service, including the Content of Communication and intercept related information, which is passed by a network operator, an access provider or a service provider to a law enforcement agency

NOTE: Intercept related information shall be provided whether or not call activity is taking place.

service information: information used by the telecommunications infrastructure in the establishment and operation of a network related service or services

NOTE: The information may be established by a network operator, an access provider, a service provider or a network user.

Service Provider (SvP): natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network

NOTE: A service provider needs not necessarily run his own network.

Short Message Service (SMS): gives the ability to send character messages to phones

NOTE: SMS messages can be MO (Mobile Originate) or MT (Mobile Terminate).

target identity: technical identity (e.g. the interception's subject directory number), which uniquely identifies a target of interception

NOTE: One target may have one or several target identities.

target service: telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception

NOTE: There may be more than one target service associated with a single interception subject.

telecommunications: any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3PTY	Three-PartY service
AA	Abbreviated Address
AC	Alarm Call
AOC	Advice Of Charge service
AP	Access Provider
ASE	Application Service Element
ASN.1	Abstract Syntax Notation No.1
BA	DSS1 Basic Access
BC	Bearer Capability
BER	Basic Encoding Rules
BS	Basic Service
CC	Content of Communication
CCBS	Completion of Calls to Busy Subscriber
CCLID	CC Link IDentifier
CCNR	Completion of Calls on No Reply
CD	Call Deflection
CF	Call Forwarding
CFB	Call Forwarding on Busy
CFNR	Call Forwarding on No Reply
CFU	Call Forwarding Unconditional
CH	Call Hold
CID	Communication IDentifier
CIN	Call Identity Number
CLI	Calling Line Identity (Calling Party Number)
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COL	COnnected Line identity (Connected Number)
COLP	COnnected Line identification Presentation
COLR	COnnected Line identification Restriction
CONF	CONFerence call, add-on
CUG	Closed User Group
CW	Call Waiting
DDI	Direct Dialling In
DF	Delivery Function
DIV	call DIVersion services
DN	Directory Number
DSS1	Digital Subscriber Signalling system No.1
ECT	Explicit Call Transfer
FB	FallBack procedure
FDC	Fixed Destination Call
FPH	Free PHone
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GLIC	GPRS LI Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTP	GPRS Tunnelling Protocol
HI	Handover Interface
HI1	Handover Interface Port 1 (for Administrative Information)

HI2	Handover Interface Port 2 (for Intercept Related Information)
HI3	Handover Interface Port 3 (for Content of Communication)
HLC	High Layer Compatibility
HOLD	call HOLD service
IA5	International Alphabet No.5
ICB	Incoming Call Barring
IE	Information Element
IIF	Internal Interception Function
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception IDentifier
LLC	Lower Layer Compatibility
MAP	Mobile Application Part
MCID	Malicious Call IDentification
MF	Mediation Function
MMC	Meet-Me Conference
MO	Mobile Originated
MS	Mobile Station
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
MT	Mobile Terminated
MWI	Message Wait Indication
NDUB	Network Determined User Busy
NEID	Network Element IDentifier
NID	Network IDentifier
NWO	NetWork Operator
OCB	Outgoing Call Barring
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PR	Partial Rerouting
PSTN	Public Switched Telephone Network
QoS	Quality of Service
ROSE	Remote Operation Service Element
R_x	Receive direction
SCF	Service Control Function
SCI	Subscriber Controlled Input
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SS No.7	common channel Signalling System ITU(T) No.7
SS	Supplementary Service
SSF	Service Switching Function
SUB	SUBaddressing (supplementary service)
SvP	Service Provider
TCP	Transmission Control Protocol
TETRA	TErrestrial Trunked RAdio
TMR	Transmission Medium Requirement
TP	Terminal Portability
T-PDU	Tunnelled PDU
T_x	Transmit direction
UDUB	User Determined User Busy
UUS	User-to-User Signalling

WUS	Wake-Up Service
xGSN	SGSN or GGSN

4 General requirements

The present document focuses on the Handover Interface related to the provision of information related to LI between a network operator, access provider and/or service provider and a Law Enforcement Agency (LEA).

4.1 Basic principles for the Handover Interface

The network requirements mentioned in the present document are derived, in part, from the requirements defined in ES 201 158 [2].

Lawful interception requires functions to be provided in some, or all of, the switching or routing nodes of a telecommunications network.

The specification of the Handover Interface is subdivided into three ports each optimized to the different purposes and types of information being exchanged.

The interface is extensible.

4.2 Legal requirements

It shall be possible to select elements from the Handover Interface specification to conform with:

- national requirements;
- national law;
- any law applicable to a specific LEA.

As a consequence, the present document shall define, in addition to mandatory requirements, which are always applicable, supplementary options, in order to take into account the various influences listed above. See also [1] and [3].

4.3 Functional requirements

A lawful authorization shall describe the kind of information (Content of Communication (CC) and/or Intercept Related Information (IRI)) that is required by this LEA, the interception subject, the start and stop time of LI, and the addresses of the LEAs for CC and/or IRI and further information.

A single interception subject may be the subject to interception by different LEAs. It shall be possible strictly to separate these interception measures.

If two targets are communicating with each other, each target is dealt with separately.

5 Overview of Handover Interface

The generic Handover Interface adopts a three port structure such that administrative information (HI1), intercept related information (HI2) and the Content of Communication (HI3) are logically separated.

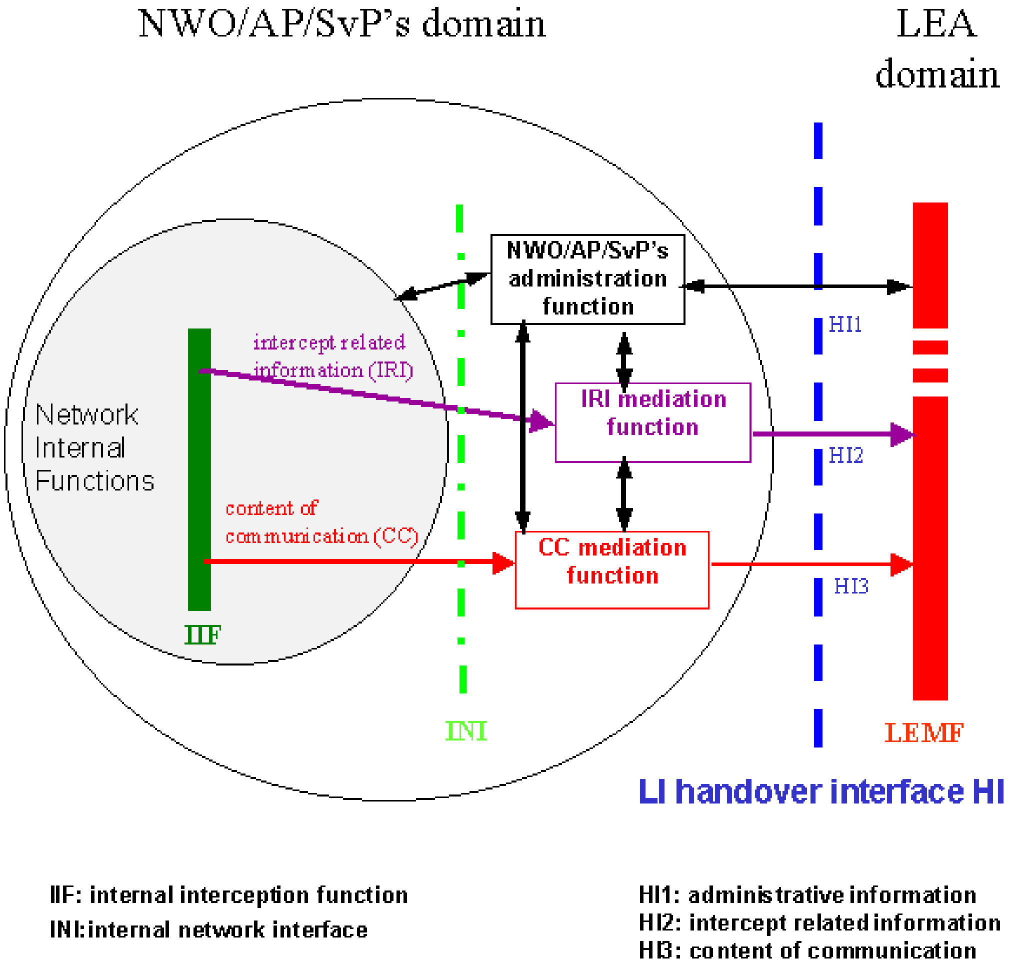
Figure 5.1 shows a block diagram with the relevant entities for Lawful Interception.

The outer circle represents the NWO/AP/SvP's domain with respect to lawful interception. It contains the network internal functions, the Internal Network Interface (INI), the administration function and the mediation functions for IRI and CC. The inner circle contains the internal functions of the network (e.g. switching, routing, handling of the communication process). Within the network internal function the results of interception (IRI, CC) are generated in the IIF.

The Internal Interception Functions (IIF) provide the Content of Communication (CC) and the Intercept Related Information (IRI), respectively, at the internal network interface INI. For both kinds of information, mediation functions may be used, which provide the final representation of the standardized Handover Interfaces at the NWO/AP/SvP's domain boundary.

Within the NWO/AP/SvP's administration centre, the LI related tasks, as received via interface HI1, are translated into man machine commands for the NWO/AP/SvP's equipment.

Depending on the type of network, there might be a need to standardize also some or all of the internal network interfaces (INI). Such standards are not in the scope of the present document.


NWO/AP/SvP's domain
LEA domain
NWO/AP/SvP's administration function
HI1
intercept related information (IRI)
IRI mediation function
HI2
Network Internal Functions
content of communication (CC)
CC mediation function
HI3
IIF
INI
LEMF
LI handover interface HI
IIF: internal interception function
INI:internal network interface
HI1: administrative information
HI2: intercept related information
HI3: content of communication

NOTE 1: Figure 5.1 shows only a reference configuration, with a logical representation of the entities involved in lawful interception and does not mandate separate physical entities.

NOTE 2: The mediation functions may be transparent.

Figure 5.1: Functional block diagram showing Handover Interface (HI)

5.1 Handover Interface port 1 (HI1)

The Handover Interface port 1 shall transport various kinds of administrative information from/to the LEA and the organization at the NWO/AP/SvP, which is responsible for LI matters. This interface may be manual or electronic.

The HI1 interface may be crossing borders between countries. This possibility is subject to corresponding international laws or agreements.

A complete separation is required between the administrative part (HI1) and the technical part (INI) of the interface. No direct access to the switching function shall be given to the LEMF. Activation, deactivation or modification of an interception in the switching function shall only be possible by the NWO/AP/SvP.

As an option, in direction to the LEA, some HI1 related information (e.g. fault reporting) may be delivered directly using the HI2 mechanism. As an additional option, in direction to the LEA, some HI1 related information may be delivered directly, for example, as part of a lawful authorization procedure.

Further description of HI1 is given in clause 7.

5.1.1 Manual interface

If the HI1 is designed as a manual interface, it will normally consist of paper documents. The request for lawful interception may be sent via letter or via fax to the administration centre of the NWO/AP/SvP. The personnel of the administration centre will take the request and activate it in the network element (activation of interception). After the interception specified in the lawful authorization is activated, the LEA will be informed, see clause 7. From this point in time on, the LEA shall be prepared to receive intercept related information (IRI) via HI2 and Content of Communication (CC) via HI3.

5.1.2 Electronic interface

An alternative solution may be the electronic transmission of the request for lawful interception.

The information content shall be such that the authorized personnel of the NWO/AP/SvP is able to map it to the information which is required to activate the interception with a minimum of manual translation. This principle reduces the probability of errors.

5.2 Handover Interface port 2 (HI2)

The Handover Interface port 2 shall transport the IRI from the NWO/AP/SvP's IIF to the LEMF.

The delivery shall be performed via data communication methods which are suitable for the network infrastructure and for the kind and volume of data to be transmitted.

The delivery can in principle be made via different types of lower communication layers, which should be standard or widely used data communication protocols.

The individual IRI parameters shall be coded using ASN.1 and the Basic Encoding Rules (BER). The format of the parameter's information content shall be based on existing telecommunication standards, where possible.

The individual IRI parameters have to be sent to the LEMF at least once (if available).

The IRI records are transmitted individually, or as an option, IRI records can be aggregated for delivery to the same LEA (i.e., in a single delivery interaction). As there are time constraints associated with the delivery of IRI, the use of this optional feature is subject to national or regional requirements. As a general principle, IRI records shall be sent immediately and shall not be held in the MF/DF in order to use the IRI record aggregation option.

The IRI records shall contain information available from normal network or service operating procedures. In addition the IRI records shall include information for identification and control purposes as specifically required by the HI2 port.

The IIF is not required to make any attempt to request explicitly extra information which has not already been supplied by a signalling system.

5.3 Handover Interface port 3 (HI3)

The appropriate form of HI3 depends upon the technology being intercepted, see clause 9.

6 Specific identifiers for LI

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different Handover Interfaces (HI1, HI2 and HI3). The identifiers, which apply to all communication technologies, are defined in the clauses below. Additional technology specific identifiers are defined in related annexes.

6.1 Lawful Interception IDentifier (LIID)

For each target identity related to an interception measure, the authorized NWO/AP/SvP operator shall assign a special Lawful Interception IDentifier (LIID), which has been agreed between the LEA and the NWO/AP/SvP. It is used within parameters of all HI interface ports.

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific interception target limited within the authorized NWO/AP/SvP operators and the handling agents at the LEA.

The Lawful Interception IDentifier LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the Handover Interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters (or digit string for sub-address option, see annex E). It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized NWO/AP/SvP shall enter for each target identity of the interception subject a unique LIID.

EXAMPLE: The interception subject has an ISDN access with three MSNs. The NWO/AP/SvP enters for each MSN an own LIID.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned, relating to each LEA.

6.2 Communication IDentifier (CID)

NOTE 1: Was called Call Identifier in Edition 1. It is renamed because of new technologies.

For each activity relating to a target identity a CID is generated by the relevant network element. The CID consists of the following two identifiers:

- Network IDentifier (NID);
- Communication Identity Number (CIN) - optional.

NOTE 2: For all non CC related records like SMS, SCI etc. no correlation to a CC could be made.

The CID distinguishes between the different activities of the target identity. It is also used for correlation between IRI records and CC connections. It is used at the interface ports HI2 and HI3.

The Communication IDentifier is specified in the clauses below. For ASN.1 coding details, see annex D.

6.2.1 Network IDentifier (NID)

The Network IDentifier is a mandatory parameter; it should be internationally unique. It consists of one or both of the following two identifiers.

1) NWO/AP/SvP- identifier (mandatory):
Unique identification of network operator, access provider or service provider.

2) Network Element Identifier NEID (optional):
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be:

- an E.164 international node number in the case of circuit switched networks, such as ISDN, PSTN, GSM;
- an X.25 address;
- an IP address.

6.2.2 Communication Identity Number (CIN) - optional

NOTE: Was called Call Identity Number in Edition 1. It is renamed because of new technologies.

This parameter is mandatory for IRI in case of reporting events for connection-oriented types of communication (e.g. circuit switched calls).

The communication identity number is a temporary identifier of an intercepted communication, relating to a specific target identity.

7 HI1: Interface port for administrative information

The interface HI1 is typically bi-directional. It is used to hand over the requests for lawful interception to the NWO/AP/SvP, such as orders for activation, deactivation and modification, and the corresponding notifications, and send other information to the LEA.

There shall be no direct control over the NWO/AP/SvP's equipment by the LEA/LEMF.

7.1 Information for the activation of lawful interception

The HI1 interface may be realized as manual or electronic processing, see clause 5.1.

If the LEA requests lawful interception, the NWO/AP/SvP needs a minimum set of information to activate lawful interception in the network.

The LEA shall provide the following information, for activation of LI:

1) Identification of the interception subject: Target identity.

2) The agreed Lawful Interception Identifier (LIID).

3) Start and end (or duration) of the interception.

4) Further specification of type of interception, i.e. kind of information to be provided (IRI, CC or both).

5) HI2 destination address of the LEMF, to which the IRI-Records shall be sent (if applicable).

6) HI3 destination address of the LEMF, to which the Content of Communication (CC) shall be sent (if applicable).

7) Other network dependent parameters (e.g. location information, delivery mechanisms used for HI2 and HI3).

8) A reference for authorization of the interception.

9) Technical contact for issues relating to set-up and execution of the interception (e.g. solution of problems with communication links to the LEMF).

10) Other information as required.

7.2 LI notifications towards the LEMF

LI management notifications to the LEMF shall be sent in the following cases:

1) After the activation of lawful interception.

2) After the deactivation of lawful interception.

3) After modification of an active lawful interception.

4) In case of certain exceptional situations.

For the definition of the information content of these LI management notifications, see clause D.4.

8 HI2: Interface port for intercept related information

The HI2 interface port shall be used to transport all Intercept Related Information (IRI), i.e. the information or data associated with the communication services of the target identity apparent to the network. It includes signalling information used to establish the telecommunication service an^^d to control its progress, time stamps, and, if available, further information such as supplementary service information or location information. Only information which is part of standard network signalling procedures shall be used within communication related IRI, see also clause 5.2; e.g. if information of the other party is not available, it need not be requested from the origin, by extra procedures, especially when such procedures are not provided by the used network protocols.

Sending of the Intercept Related Information (IRI) to the LEMF shall in general take place as soon as possible, after the relevant information is available.

In exceptional cases (e.g. data link failure), the intercept related information may be buffered for later transmission for a specified period of time.

Within this clause only definitions are made which apply in general for all network technologies. Additional technology specific HI2 definitions are specified in related annexes (e.g. for circuit switched communication technologies see clause A.3).

8.1 Data transmission protocols

The protocol used by the "LI application" for the encoding and the sending of data between the MF and the LEMF is based on already standardized data transmission protocols like ROSE or FTP, see annex C.

The specified data communication methods provide a general means of data communication between the LEA and the NWO/AP/SvP's mediation function. They are used for the delivery of:

- HI1 type of information (notifications and alarms);
- HI2 type of information (IRI records);
- HI3 data type of information in certain circumstances (UUS, SMS, etc.).

The present document specifies the use of the two possible methods for delivery: ROSE or FTP on the application layer and the BER on the presentation layer. The lower layers for data communication may be chosen in agreement with the NWO/AP/SvP and the LEA.

The delivery to the LEMF should use the internet protocol stack.

8.1.1 Application for IRI (HI2 information)

As defined in clause 5.2, the Handover Interface port 2 shall transport the intercept related information (IRI) from the NWO/AP/SvP's MF to the LEMF.

The individual IRI parameters shall be coded using ASN.1 and the basic encoding rules (BER). Where possible, the format of the information content shall be taken over from existing telecommunication standards, which are used for these parameters with the network already (e.g. the ISDN user part, DSS1, MAP and IP). Within the ASN.1 coding for IRI, such standard parameters are typically defined as octet strings.

8.2 Types of IRI records

Intercept related information shall be conveyed to the LEMF in messages, or IRI data records, respectively. Four types of IRI records are defined:

1) IRI-BEGIN record at the first event of a communication attempt, opening the IRI transaction;

2) IRI-END record at the end of a communication or communication attempt, closing the IRI transaction;

3) IRI-CONTINUE record at any time during a communication or communication attempt within the IRI transaction;

4) IRI-REPORT record used in general for non-communication related events.

For information related to an existing communication case, the record types 1 to 3 shall be used. They form an IRI transaction for each communication case or communication attempt, which corresponds directly to the communication phase (set-up, active or release).

Record type 4 is used for non-communication related subscriber action, like Subscriber Controlled Input (SCI) for service activation. For simple cases, it can also be applicable for reporting unsuccessful communication attempts.

The record type is an explicit part of the record. The 4 record types are defined independently of target communication events. The actual indication of one or several communication events, which caused the generation of an IRI record, is part of further parameters within the records, information content. Consequently, the record types of the IRI transactions are not related to specific messages of the signalling protocols of a communication case, and are therefore independent of future enhancements of the intercepted services, of network specific features, etc. Any transport level information (i.e. higher-level services) on the target communication-state or other target communication related information is contained within the information content of the IRI records.

9 HI3: Interface port for Content of Communication

The port HI3 shall transport the Content of the Communication (CC) of the intercepted telecommunication service to the LEMF. The Content of Communication shall be presented as a transparent en-clair copy of the information flow during an established, frequently bi-directional, communication of the interception subject.

As the appropriate form of HI3 depends upon the service being intercepted, HI3 is described in relevant annexes.

The HI2 and HI3 are logically different interfaces, even though in some installations the HI2 and HI3 packet streams might also be delivered via a common transmission path from a MF to a LEMF. It is possible to correlate HI2 and HI3 packet streams by having common (referencing) data fields embedded in the IRI and the CC packet streams. This may be possible e.g. for packet switched, but not for analogue circuit switched networks.

10 Performance and quality

10.1 Timing

As a general principle, within a telecommunication system, Intercept Related Information (IRI), if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of intercept related information fails, it may be buffered or lost.

10.2 Quality

The Quality of Service associated with the result of interception should be (at least) equal to the Quality of Service of the original Content of Communication.

11 Security aspects

This clause will give an informative overview of the security properties and mechanisms that can be used to meet possible security requirements for the transportation of Lawful Intercepted data.

11.1 Security properties

A secure communication channel has the following properties:

- confidentiality;
- integrity;
- authentication;
- availability.

Confidentiality means that it is impossible to interpret the data by eavesdropping on the communication link.

Integrity means that any alteration or mutilation of the transported data is immediately detected.

Authentication means that the communicating parties have verified and confirmed each other's identities.

Availability means that the communicating parties have made agreements about up- and downtimes of the systems. In case of irregularities, alarm messages should be sent through another communication channel. Because of the nature of the transported data, confidentiality can be an issue. Lawful Intercepted data can also be confidential or secret by law and appropriate measures need to be taken to prevent eavesdropping by unauthorized third parties.

Integrity can be an issue when Lawful Intercepted data is used as evidence in a criminal investigation. It must be provable that the data is unaltered and an exact representation of the intercepted communication.

In the process of Lawful Interception it is very important to know that the LEMF is receiving the data from a real MF and the MF needs to be sure that it is sending its data to a real LEMF. If this verification of identity does not take place, Lawful Intercepted data might end up in the wrong place or the LEMF is processing data that is originating from an unauthorized source.

The process of Lawful Interception takes place during well-defined periods of time. In case of any irregularities, appropriate actions need to be taken. Irregularities can be a sign of a breach of security, loss of data or detection of interception.

11.2 Security mechanisms

This clause will give an overview of possible mechanisms to achieve the properties as described above. Technical details are to be decided during the process of implementation.

Confidentiality can be achieved by using encryption. A common technique is to use a symmetric encryption algorithm. A symmetric algorithm is an algorithm where both communicating parties use the same key for encryption and decryption. This key must be exchanged in a secure way.

Integrity can be achieved using hashing algorithms. These algorithms generate a unique fingerprint of the transported data. When the transported data is altered, the fingerprint does not match anymore and appropriate actions can be undertaken (like retransmission of data).

Authentication can be achieved using cryptographic techniques. A common technique is to use asymmetric encryption. In this technique, both parties have two keys: A public key and a private key. Data encrypted with one key can only be deciphered with the other. If party X encrypts something using the public key of party Y then party Y is the only one able to decrypt this data using his private key. If party X encrypts something using his private key then this data can only be deciphered using his public key. By combining these properties, both parties can make sure that they are communicating with the right party.

12 Quantitative aspects

See ES 201 158 [2]. The number of targets based on a percentage of subscribers should be provided at a national level together with an indication as to the expected usage.

Annex A (normative): Circuit switched network handover

This annex is applicable to 64 kbit/s based circuit switched networks.

A.1 Specific identifiers for LI

In this clause, additional identifiers, which are needed in circuit switched networks are described here. See clause 6.

A communication is a call in a circuit switched network.

A.1.1 CC Link Identifier (CCLID)

This identifier is only used at the interface ports HI2 and HI3 in case of the reuse of CC links (option B, see clause A.5.4.2).

For each CC link, which is set up by the mediation function towards the LEMF, a CC Link Identifier (CCLID) is transmitted in the HI2 records and HI3 setup message in addition to CIN and NID. For the correct correlation of multiparty calls this identity number indicates in the IRI records of each multiparty call, which CC link is used for the transmission of the CC.

The CCLID may use the same format as the CIN; in this case, it need not be transmitted explicitly during set up of the CC links, as part of HI3. The CIN may also implicitly represent the CCLID.

A.1.2 Circuit switched LI correlation between CC and IRI

To assure correlation between the independently transmitted Content of Communication (CC) and Intercept Related Information (IRI) of an intercepted call the following parameters are used:

- Lawful Interception IDentifier (LIID), see clause 6.1;
- Communication IDentifier (CID), see clause 6.2;
- CC Link IDentifier (CCLID), see clause A.1.1.

These parameters are transferred from the MF to the LEMF in:

- HI2: see clause A.3.2.1;
- HI3: see clause A.4.2.

A.1.3 Usage of identifiers

The identifiers are exchanged between the mediation function and the LEMF via the interfaces HI1, HI2 and HI3. There exist several interface options for the exchange of information. Tables A.1.1 and A.1.2 define the usage of numbers and identifiers depending on these options.

NOTE: X in tables A.1.1 and A.1.2: Identifier used within parameters of the interface.

Table A.1.1: Usage of identifiers, IRI and CC transmitted; options A, B (see clause A.5.4)

Identifier	IRI and CC transmitted (option A)			IRI and CC transmitted (option B)		
	HI1	HI2	HI3	HI1	HI2	HI3
LIID	X	X	X	X	X	X
NID		X	X		X	X
CIN		X	X		X	X (see note 1)
CCLID					X	X (see note 2)
NOTE 1: The CIN of the 1st call for which this CC link has been set-up. NOTE 2: The CCLID may be omitted, see clause A.1.1.						

Table A.1.2: Usage of identifiers, only IRI or only CC transmitted

Identifier	Only IRI transmitted		Only CC transmitted	
	HI1	HI2	HI1	HI3
LIID	X	X	X	X
NID		X		X
CIN		X		X
CCLID				

A.2 HI1: interface port for administrative state

There are no additions beyond clause 7.

A.3 HI2: interface port for IRI

A.3.1 Definition of Intercept Related Information

Intercept Related Information will in principle be available in the following phases of a call (successful or not):

1) At call initiation when the target identity becomes active, at which time call destination information may or may not be available (set up phase of a call, target may be the originating or terminating party, or be involved indirectly by a supplementary service).

2) At the end of a call, when the target identity becomes inactive (release phase of call).

3) At certain times between the above phases, when relevant information becomes available (active phase of call).

In addition, information on non-call related actions of a target constitutes IRI and is sent via HI2, e.g. information on subscriber controlled input.

The Intercept Related Information (IRI) may be subdivided into the following categories:

1) Control information for HI2 (e.g. correlation information).

2) Basic call information, for standard calls between two parties.

3) Information related to supplementary services, which have been invoked during a call.

4) Information on non-call related target actions.

A.3.2 Structure of IRI records

Each IRI-record contains several parameters. In the clauses below, the usage of these parameters is explained in more detail.

Mandatory parameters are indicated as HI2 control information. Optional parameters are provided depending on the availability at the MF. For the internal structure of the IRI records, the ASN.1 description, with the application of the basic encoding rules (BER) is used. This ASN.1 specification is enclosed in annex D.

A.3.2.1 Control information for HI2

The main purpose of this information is the unique identification of records related to a target identity, including their unique mapping to the links carrying the Content of Communication. In general, parameters of this category are mandatory, i.e. they have to be provided in any record.

The following items are identified (in brackets: ASN.1 name and reference to the ASN.1 definition or clause D.5):

1) Record type (*IRIContent*, see clause D.5)
IRI-BEGIN, IRI-CONTINUE, IRI-END, IRI-REPORT-record types.

2) Version indication (*iRIversion*, see clause D.5)
Identification of the particular version of the HI2 interface specification.

3) Communication Identifier (*CommunicationIdentifier,* see clauses 6.2 and D.5).

4) Lawful Interception Identifier (*LawfulInterceptionIdentifier,* see clauses 6.1 and D.5).

5) Date & time (*TimeStamp*, see clause D.5)
Date & time of record trigger condition.
The parameter shall have the capability to indicate whether the time information is given as Local time without time zone, GMT with time zone, or UTC. Normally, the NWO/AP/SvP shall define these options.

6) CC Link Identifier (*CC-Link-Identifier*, see clause A.1.2 for definition and clause D.5 for ASN.1 definition).

Table A.3.1 summarizes the items of HI2 control information. It is mandatory information, except the CID - it may be omitted for non-call related IRI records - and the CCLID. Their format and coding definition is LI specific, i.e. not based on other signalling standards.

Table A.3.1: Parameters for LI control information in IRI records (HI2 interface port)

IRI parameters: LI control information	
IRI parameter name	**ASN.1 name (used in annex D)**
Type of record	IRIContent
Version indication	IRIversion
Lawful Interception IDentifier (LIID)	LawfulInterceptionIdentifier
Communication IDentifier (CID) - Communication Identity Number (CIN) - Network IDentifier (NID)	CommunicationIdentifier
Date & time	TimeStamp
CC Link IDentifier (CCLID) (only used in case of option B)	CC-Link-Identifier

A.3.2.2 Basic call information

This clause defines parameters within IRI records for basic calls, i.e. calls, for which during their progress no supplementary services have been invoked. In general, the parameters are related to either the originating or terminating party of a call; consequently, ASN.1 containers are defined for the originating/terminating types of parties, which allow to include the relevant, party-related information. The structure of these containers and the representation of individual items are defined in clause D.5.

NOTE: A third type of party information is defined for the forwarded-to-party (see clause A.3.2.3 on calls with supplementary services being invoked).

The items below are to be included, when they become available for the first time during a call in progress. If the same item appears identically several times during a call, it needs only to be transmitted once, e.g. in an IRI-BEGIN record. The ASN.1 name of the respective parameters, as defined in clause D.5, is indicated in brackets.

1) Direction of call (*intercepted-Call-Direct*)
Indication, whether the target identity is originating or terminating Party.

2) Address of originating and terminating parties (*CallingPartyNumber* or *CalledPartyNumber*)
If e.g. in case of call originated by the target at transmission of the IRI-BEGIN record only a partial terminating address is available, it shall be transmitted, the complete address shall follow, when available.

3) Basic Service, LLC (*Services-Information*)
Parameters as received from signalling protocol (e.g. BC, HLC, TMR, LLC).

4) Cause (*ISUP-parameters* or *DSS1-parameters-codeset-0*)
Reason for release of intercepted call. Cause value as received from signalling protocol. It is transmitted with the ASN.1 container of the party, which initiated the release; in case of a network-initiated release, it may be either one.

5) Additional network parameters
E.g. location information (*Location*).

Parameters defined within tables A.3.2 and A.3.3 shall be used for existing services, in the given ETSI format. National extensions may be possible using the ASN.1 parameter *National-Parameters*.

A.3.2.3 Information on supplementary services, related to a call in progress

The general principle is to transmit service related information within IRI records, when the corresponding event/information, which needs to be conveyed to the LEMF, is received from the signalling protocol. Where possible, the coding of the related information shall use the same formats as defined by standard signalling protocols.

The selection, which types of events or information elements are relevant for transmission to the LEAs is conforming to the requirements defined in [1] and [2].

A dedicated ASN.1 parameter is defined for supplementary services related to forwarding or re-routing calls (*forwarded-to-Party* information), due to the major relevance of these kinds of services with respect to LI. For the various cases of forwarded calls, the information related to forwarding is included in the *originatingParty*/*terminatingParty*/*forwarded-to-Party* information:

1) If a call to the target has been previously forwarded, available parameters relating to the redirecting party(ies) are encapsulated within the *originatingPartyInformation* parameter.

2) If the call is forwarded at the target's access (conditional or unconditional forwarding towards the forwarded-to-party), the parameters which are related to the redirecting party (target) are encapsulated within the *terminatingPartyInformation* parameter.

3) All parameters related to the forwarded-to-party or beyond the forwarded-to-party are encapsulated within the *forwarded-to-Party* ASN.1 coded parameter. In addition, this parameter includes the *supplementary-Services-Information*, containing the forwarded-to address, and the redirection information parameter, with the reason of the call forwarding, the number of redirection, etc.).

For the detailed specification of supplementary services related procedures see clause A.5.

Parameters defined within tables A.3.2 and A.3.3 shall be used for existing services, in the given ETSI format. National extensions may be possible using the ASN.1 parameter National-Parameters.

A.3.2.4 Information on non-call related supplementary services

The general principle is to transmit non-call related service information as received from the signalling protocol.

A typical user action to be reported is Subscriber Controlled Input (SCI).

For the detailed specification of the related procedures see clause A.5.

A.3.3 Selection of parameters for IRI records

Relevant information on a call is taken from the call handling process, using wherever possible the coding specifications of the standardized ISDN protocols, or other standard network protocols. The protocol-defined information content is copied transparently into the information elements of the IRI records. This principle enables to reuse of internationally agreed standardization results; it allows reuse of existing functions within the NWO/AP/SvP equipment and in the terminal area (LEMF).

Consequently, the present document needs for a large number of IRI-relevant items only to refer to other, existing standards, instead of including separate definitions in its scope. By this principle, also consistency issues and dependencies on the ongoing enhancements of the various protocols are minimized.

The relevant parameters are listed in tables A.3.2 and A.3.3.

For other signalling systems, which are not included in table A.3.2, the parameters shall be interpreted on a functional level, for defining their applicability in an IRI record; e.g. in case of a local call between analogue users, the *called party number* may only exist in an internal format of the switching system. Within the IRI records, such parameters shall also use the standardized coding. Existing interworking specifications, like [7] shall be used for the conversion to the standard format. If the signalling system provides less information than defined by the standards in table A.3.2, spare or default values may be used instead.

This method avoids the need to analyse for all situations, especially in the area of supplementary services, each detail of the service procedures, with specification of which parameter shall be sent in which state or situation. Instead, only a reference to the applicable standards is made. As soon as a parameter defined in one of the parameter tables appears within the target call protocol, it shall be transmitted within an IRI record.

In addition to parameters taken from the call handling process, further, lawful interception specific parameters are needed, like the control information for LI.

Three types of origins for the specification of HI2 parameters in IRI records can be differentiated:

1) Parameters for LI control information; they are specific for the LI HI2 interface, and are specified in the present document (see table A.3.1).

2) Parameters used to convey information to the LEMF, which is retrieved from the target's call or service signalling protocol information (see table A.3.2). Within the IRI a standardized protocol coding is used.

   The relevant protocol specifications are the ISDN user part, as a generic protocol, used by several types of networks, and dedicated network protocols, e.g. DSS1 or GSM standards. For a common implementation in different countries and to guarantee the possibility of an interception measure across borders only parameters defined in ETSI standards shall be used.

3) Parameters used to convey information from events relating to the target call, but with no equivalent parameters being available in protocol standards. Such parameters shall be specified in the present document (see table A.3.3).

The LI control information is a mandatory part of each IRI record (exception: CID), the information defined in table A.3.3 is included in IRI records, if the according parameter or event is detected during processing a call or a target identity related action.

Table A.3.2: List of parameters from standard protocols, which may be contained in IRI records

IRI parameters: target call information, based on standard protocols			
IRI parameter name	**Name of ASN.1 parameter (of annex D)**	**Related standard**	**Ref.**
Three party conference invoke/result components (see note 2)	PartyInformation/supplementary-Services-Information	DSS1	[10]
Add on conference invoke/result components (see note 2)	PartyInformation/supplementary-Services-Information	DSS1	[9]
Bearer capability	PartyInformation/services-Information	DSS1	[5]
Call diversion information	PartyInformation/supplementary-Services-Info	ISUP/DSS1	[4], [5]
Call transfer number	PartyInformation/supplementary-Services-Info	ISUP	[4]
Called party number	PartyInformation/calledPartyNumber	ISUP/DSS1/MAP	[4], [5], [14]
Called party subaddress	PartyInformation/supplementary-Services-Info	DSS1	[6]
Calling party number	PartyInformation/callingPartyNumber	ISUP/DSS1	[4], [5]
Calling party subaddress	PartyInformation/supplementary-Services-Info	DSS1	[6]
Cause indicator	Release-Reason-Of-Intercepted-Call CallContentLinkCharacteristics	ISUP/DSS1	[4], [5]
Cell id	Location	MAP/ISUP	[14], [4]
Closed user group interlock code	PartyInformation/supplementary-Services-Info	ISUP	[8]
Connected number	PartyInformation/supplementary-Services-Info	ISUP/DSS1	[4], [5]
Connected subaddress	PartyInformation/supplementary-Services-Info	DSS1	[6]
Explicit Call Transfer invoke/result components (see note 2)	PartyInformation/supplementary-Services-Information	DSS1	[12]
Facility (see note 3)	PartyInformation/supplementary-Services-Info	DSS1	[13]
Generic notification indicator	PartyInformation/supplementary-Services-Info	ISUP	[4]
Generic number	PartyInformation/supplementary-Services-Info	ISUP	[4]
High layer compatibility	PartyInformation/services-Information	DSS1	[5]
IMEI	PartyInformation/imei	MAP	[14]
IMSI	PartyInformation/imsi	MAP	[14]
Keypad facility	PartyInformation/supplementary-Services-Info	DSS1	[13]
Location number	Location	ISUP/MAP	[4], [14]
Low layer compatibility	PartyInformation/services-Information	DSS1	[5]
MCID response indicator	PartyInformation/services-Information	ISUP	[4]
MSISDN	PartyIdentity/msISDN	MAP	[14]
Original called number	PartyInformation/supplementary-Services-Info	ISUP/DSS1	[4], [5]
Redirecting number	PartyInformation/supplementary-Services-Info	ISUP/DSS1	[4], [5]
Redirection information	PartyInformation/supplementary-Services-Info	ISUP/DSS1	[4], [5]
Redirection number	PartyInformation/supplementary-Services-Info	ISUP/DSS1	[4], [5]
Subaddress Transfer	PartyInformation/supplementary-Services-Info	DSS1	[12]
Transmission Medium Reqmt	PartyInformation/services-Information	ISUP	[4]
NOTE 1: Column "Related standard" indicates the ETSI standard, which specifies the format and coding of the parameter. NOTE 2: Refers to several ASN.1 encoded elements, which are in the DSS1 protocol embedded in a facility information element. NOTE 3: The facility IE is only included, if it contains one or more of the parameters, which are parts of this table.			

Table A.3.3: List of LI specific parameters, which may be contained in IRI

IRI parameters: Target call information, LI specific definition	
IRI parameter name	**ASN.1 name (used in annex D)**
Direction of call	Intercept-Call-Direct
Call event (e.g.: answer indication call waiting indication hold indication retrieve indication suspend indication resume indication	SimpleIndication
Ringing duration	RingingDuration
Conversation duration	ConversationDuration
CC link information	CallContentLinkInformation
Subscriber controlled input data	DSS1-parameters-codeset-0, or sciData
NOTE: Format and coding details see annex D.	

The general principle is that, if parameters included in table A.3.2 are available, they shall be included in an IRI record, and be sent to the LEMF. Parameters of table A.3.3, which are not part of standard protocols, shall be included, when the according event or parameter, which needs to be reported to the LEMF is detected.

Parameters of table A.3.1 are present in all IRI records, except the Communication Identifier: it may be missing in IRI-REPORT records; if no target call is related to it.

The list can be adapted to the requirements and feature specifications of an NWO/AP/SvP, and the laws and regulations of a country. That is, tables A.3.2 and A.3.3 may be extended nationally, or by a NWO/AP/SvP. Further in the present document, such extensions are referred to as national extensions or national parameters.

The IIF for IRI parameter generation may be seen as a kind of screening function, which watches the signalling information flow related to a target, and copies those information elements, which match with an element type in the screening lists, defined by tables A.3.2 and A.3.3.

The NWO/AP/SvP is not required to filter information out of the IRI.

An instance of the IIF for IRI generation needs in general not to store the information it has sent, or other information on a call, for the purpose to be aware of the status or context of a call. Each IRI parameter is independent from previous or future parameters. Exceptions from this general principle can exist, e.g. in order to avoid multiple transmission of the same information. In such a case identical parameters do not have to be repeated in succeeding records, unless their content or value has changed.

As it is indicated in table A.3.2, for a given logical parameter different format types may be used, depending on the type of network, and the call configuration. If a parameter is specified in the ISDN user part, and also identically in other standards, only the ISDN user part is referenced.

A.3.4 Coding of parameters in IRI records

The parameters shall be included in the IRI records in a structured way. The structure is defined using ASN.1, the individual parameters are in terms of the ASN.1 notation octet strings, which are taken over from the applicable standards. The ASN.1 detailed coding specification is described in annex D.

In case of the delivery of the IRI records to a LEA, when network specific extensions are used, the network specific parameters are transmitted as defined by the sending network.

A.3.5 Information content of the IRI record types

In principle, no restriction is made on which parameters shall or may be present in which IRI record type, except for the mandatory parameters, which are needed in all records. However, the logical information flow of calls implies that certain parameters will normally not appear in specific records; e.g. a called party number parameter is not included in an IRI-END record, because it has already been transmitted earlier.

A.4 HI3: interface port for Content of Communication

The port HI3 shall transport the Content of the Communication (CC) of the intercepted telecommunication service to the LEMF. The Content of Communication shall be presented as a transparent en-clair copy of the information flow during an established, frequently bi-directional, communication of the interception subject. It may contain voice or data. A target call has two directions of transmission associated with it, to the target, and from the target. Two communication channels to the LEMF are needed for transmission of the Content of Communication (stereo transmission).

The network does not record or store the Content of Communication.

A.4.1 Delivery of Content of Communication

The transmission media used to support the HI3 port shall be standard ISDN calls, based on 64 kbit/s circuit switched bearer connections. The CC links are set up on demand to the LEMF. The LEMF constitutes an ISDN DSS1 user function, with an ISDN DSS1 basic or primary rate access. It may be locally connected to the target switching node, or it may be located somewhere in the target network or in another network, with or without a transit network in between. For network signalling, the standard ISDN user part shall be used. No modifications of the existing ISDN protocols shall be required. Any information needed for LI, like to enable correlation with the IRI records of a call, can be inserted in the existing messages and parameters, without the need to extend the ETSI standard protocols for the LI application.

For each LI activation, a fixed LEMF address is assigned; this address is, within the present document, not used for any identification purposes; identification and correlation of the CC links is performed by separate, LI specific information, see clauses 6 and A.1.

The functions defined in the ISDN user part standard, Version 1 (ETSI ISUP V1) are required as a minimum within the target network and, if applicable, the destination and transit networks, especially for the support of:

- Correlation of HI3 information to the other HI port's information, using the supplementary service user-to-user signalling 1 implicit (UUS1).
- Access verification of the delivery call (see clause A.4.5).

The bearer capability used for the CC links is 64 kbit/s unrestricted digital information; this type guarantees that the information is passed transparently to the LEMF. No specific HLC parameter value is required.

The CC communication channel is a one-way connection, from the NWO/AP/SvP's IIF to the LEMF, the opposite direction is not switched through in the switching node of the target.

The scenario for delivery of the Content of Communication is as follows:

1) At call attempt initiation, for one 64 kbit/s bi-directional target call, two ISDN delivery calls are established from the MF to the LEMF. One call offers the Content of Communication towards the target identity (CC Rx call/channel), the other call offers the Content of Communication from the target identity (CC Tx call/channel). See figure A.4.1.
2) During the establishment of each of these calls, appropriate checks are made (see clause A.4.5).
3) The MF passes during call set up, within the signalling protocol elements of the CC link the LIID and the CID to the LEMF. The LEMF uses this information to identify the target identity and to correlate between the IRI and CC (see clause A.4.2).
4) At the end of a call attempt, each delivery call associated with that call attempt shall be released by the MF.

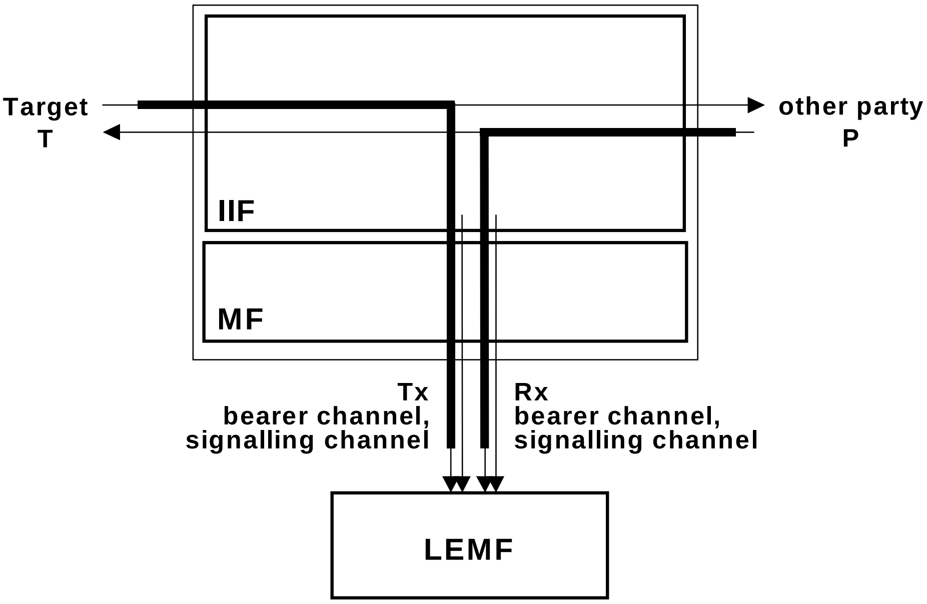


Figure A.4.1: Content of Communication transmission from MF to LEMF

A.4.2 Delivery of packetized Content of Communication (general)

The operation for transmission of UUS and SMS may use the same mechanisms as used for HI2, or a dedicated link may be used. The ROSE operations for the transmission of the Content of Communication (HI3 data interface) shall follow the same rules as the one defined for the HI2 interface in clause 8.1.

A differentiation is made between:

1) bearer related or bearer unrelated end user information; and

2) packet data services.

NOTE: Exceptionally, for the GSM SMS service, this information may be passed via HI2.

The physical or logical links supporting the Handover Interface traffic should be dimensioned to handle the bandwidth of the expected CC.

A.4.3 Control information for circuit switched Content of Communication

The delivery calls shall use unmodified standard ISDN protocols (DSS1, ISDN user part). Table A.4.1 summarizes specific settings of parameters for the CC links. The User-to-User service 1 parameter is used during call set up (within the ISUP Initial Address Message [4] or DSS1 Set Up Message [5], respectively) to transmit LI-specific control information. This information is carried transparently and delivered to the specific LEMF remote user.

To identify the delivered information, including correlating the delivery calls with the IRI records, parameters 1 to 3 and 5 shall be included in the call set up. Parameters 6 to 9 specify settings of further relevant information. Other parameters of the ISDN protocols shall correspond to normal basic calls.

Table A.4.1: Definition of HI3 specific signalling information; UUS1 coding details (see clause D.8)

No.	Used information element of CC link signalling protocol	Information	Purpose
1	CLI-Parameter with attribute "network provided"	See clause A.4.5	LEMF can check identity of origin of call.
2	UUS1-parameter	Lawful Interception IDentifier (LIID); see clause 6	Identifier, identifying target identity
3	UUS1-parameter	Communication IDentifier (CID), see clause 6	Identifier, identifying specific call of target identity
4	UUS1-parameter	CC Link IDentifier (CCLID), if required; see clause A.1	Identifier, used for correlation CC link-IRI records
5	UUS1-parameter	Direction indication (communication from/towards target/combined (mono))	Signal from (Tx)/towards (Rx) target identity or combined
6	UUS1-parameter	Bearer capability of target call	Indication to the LEMF of the basic service in use by the target
7	Closed user group interlock code	Closed user group interlock code	Supplementary Service CUG Security measure at set up of the CC link
8	Basic Service (BS)	Basic Service (BS) of CC link: 64 kbit/s unrestricted	Guarantee transparent transmission of CC copy from MF to LEMF
9	ISDN user part forward call indicators parameter	ISDN user part preference indicator: "ISDN user part required all the way"	Guarantee transparent transmission of UUS1 and other supplementary services information
10	ISDN user part optional forward call indicators parameter	Connected line identity request parameter: requested	Sending of the connected number by the destination network

Parameters 2, 3 and 4 are also present in the IRI records, for correlation with the CC links. Parameter 5 indicates in case of separate transmission of each communication direction, which part is carried by a CC link. Parameter 6, the basic service of the target call, can be used by the LEMF for processing of the CC signal, e.g. to apply compression methods for speech signals, in order to save storage space. Parameter 7 contains the CUG of the LEA. It is optionally used at set up the CC link to the LEA. Parameter 8, the basic service of the CC link, is set to "64 kbit/s unrestricted": All information of the Rx, Tx channels can be transmitted fully transparently to the LEA. The setting of the ISDN user part indicator guarantees, that the services supporting the LI CC link delivery are available for the complete CC link connection.

The MF uses en-bloc dialling, i.e. there exists only one message in forward direction to the LEA.

NOTE: The LEMF should at reception of the set up message not use the alerting state, it should connect immediately, to minimize time delay until switching through the CC links. Not all networks will support such a transition. Exceptionally, it may be necessary to send an alerting message before the connected message.

The maximum length of the user information parameter can be more than the minimum length of 35 octets (national option, see [4]), i.e. the network transmitting the CC links shall support the standard maximum size of 131 octets for the UUS1 parameter.

The User-to-User service 1 parameter cannot be discarded by the ETSI ISUP procedures: the only reason, which would allow the ISUP procedures to discard it would be, if the maximum length of the message carrying UUS1 would be exceeded. With the specified amount of services used for the CC links, this cannot happen.

The signalling messages of the two CC channels (stereo mode) carry the same parameter values, except for the direction indication.

See clause D.8 for the ASN.1 definition of the UUS1 LI specific content of the UUS1 parameter.

A.4.4 Exception handling

A.4.4.1 Failure of CC links

If a CC link cannot be set up, a certain number of repeat attempts during a certain period of time shall be made.

NOTE: Typical values are three tries during 10 s.

In case of a delay or total failure to transmit the Content of Communication, the target call is handled fully independent of the CC link, the CC information gets lost.

A.4.4.2 Fault reporting

For several events the target switching function sends messages to the NWO/AP/SvP administration centre. Some example events are given in table A.4.2.

Alternatively, all or some of these events may be transmitted directly to the LEMF. In this case, they are part of the LI management notification type of information.

Delivery to the NWO/AP/SvP administration centre is not part of the HI.

Table A.4.2: Typical events causing messages

Event type	Event causing message with LI alarm information
CC link failure	No answer from LEA
	LEA is busy
	CC link failed due to a COLP error
	CC link failed due to a CUG error
	CC link set up failure within the network
	CC link failed due to a lack of system resources
	General CC link set up failure

A.4.5 Security requirements at the interface port HI3

The process of access verification and additional (optional) authentication between the MF and the LEMF shall not delay the set up of the CC.

For the protection and access verification of the Content of Communication delivery call the ISDN supplementary services CLIP, COLP and CUG shall be used when available in the network involved.

Generally any authentication shall be processed before the set-up of the CC links between the MF and the LEMF is completed. If this is technically not feasible the authentication may be processed after completion of the CC connection in parallel to the existing connection.

A.4.5.1 LI access verification

The supplementary service CLIP shall be used to check for the correct origin of the delivery call.

NOTE: When using CLIP, the supplementary service CLIR must not be used.

The supplementary service COLP shall be used to ensure that only the intended terminal on the LEA's side accepts incoming calls from the Handover Interface (HI).

To ensure access verification the following two checks shall be performed:

- check of Calling-Line Identification Presentation (CLIP) at the LEMF; and

- check of COnnected-Line identification Presentation (COLP) at the Handover Interface (HI) (due to the fact that the connected number will not always be transported by the networks involved, there shall be the possibility for deactivating the COLP check for a given interception measure. In addition, the COLP check shall accept two different numbers as correct numbers, i.e. the user provided number and the network provided number. Usually, the user provided number contains a DDI extension).

A.4.5.2 Access protection

In order to prevent faulty connections to the LEA, the CC links may be set up as CUG calls.

In this case, the following settings of the CUG parameters should be used:

- Incoming access:	not allowed;
- Outgoing access:	not allowed;
- Incoming calls barred within a CUG:	no;
- Outgoing calls barred within a CUG:	yes.

A.4.5.3 Authentication

In addition to the minimum access verification mechanisms described above, optional authentication mechanisms according to the standard series ISO 9798 "Information technology - Entity authentication - parts 1 to 5" may be used.

These mechanisms shall only be used in addition to the access verification and protection mechanisms.

A.5 LI procedures for circuit switched supplementary services

A.5.1 General

In general, LI shall be possible for all connections and activities in which the target is involved. The target shall not be able to distinguish alterations in the offered service. It shall also not be possible to prevent interception by invoking supplementary services. Consequently, from a supplementary services viewpoint, the status of interactions with LI is "no impact", i.e. the behaviour of supplementary services shall not be influenced by interception.

Depending on the type of supplementary service, additional CC links to the LEA may be required, in addition to already existing CC links.

Within the IRI records, the transmission of additional, supplementary service specific data may be required.

Supplementary services, which have an impact on LI, with respect to CC links or IRI record content, are shown in table A.5.1. The table is based on ISDN services (DSS1 protocol specifications), it considers the services which have been standardized at the time of finalizing the present document. Future services should be treated following the same principles.

NOTE 1: Co-ordination of handling of new services should be performed via ETSI TC LI. If required, additions will be included in a subsequent version of the present document.

Services defined for other signalling protocols, which can be related to the services in the table shall be treated in the same manner (see also below). Other protocols are e.g.:

- Analogue user signalling; in general, no ETSI standards are available for supplementary services.
- Mobile user protocols of the GSM, defined within the MAP [14].

The question of Lawful Interception with Intelligent Networks is not covered in the present document (see note 2).

NOTE 2: The general principle is, that LI takes place on the basis of a technical identity, i.e. a directory number. Only numbers which are known to the NWO/AP/SvP, and for which LI has been activated in the standard way, can be intercepted. No standardized functions are available yet which would enable an SCF to request from the SSF the invocation of LI for a call.

Additional CC links are only required, if the target is the served user. IRI Records may also carry data from other parties being served users.

Clause A.6 specifies details for relevant services:

- The procedures for CC links, depending on the call scenario of the target.
- Related to the IRI records, the point in time of sending and supplementary service specific information.
- Additional remarks for services with "no impact" on LI.

The specifications for supplementary services interactions are kept as far as possible independent of the details of the used signalling protocols; service related events are therefore described in more general terms, rather than using protocol dependent messages or parameters.

Interactions with services of the same family, like call diversion services, are commonly specified, if the individual services behaviour is identical, with respect to LI.

With respect to the IRI records, clause A.6 specifies typical cases; the general rules for data which shall be included in IRI records are defined in clause 8, specifically in clauses A.3.3 and A.5.3.

Services, which are not part of table A.5.1, do not require the generation of LI information: No CC links are generated or modified, and no specific information on the service is present in the IRI records. That is, these services have "no impact" on LI, no special functions for LI are required. However, within the IIF, functions may be required to realize the principle, that the service behaviour shall not be influenced by LI.

"No impact" is not automatically applicable for new services. Each new service has to be checked for its impact on LI. Additionally, also services using other than the DSS1 protocols, which cannot be related to one of the DSS1 based services, may have impact on LI.

The present document does not intend to give a complete description of all possible cases and access types of interactions with supplementary services.

Table A.5.1: Supplementary Services with impact on LI CC links or IRI records content; see also clause A.6

Suppl. Service	Abbr.	CC links: additional calls, impact	IRI items related to service
Call Waiting	CW	CC links for active or all calls (option A/B)	Target: call waiting indication, calling party address other party: generic notification indicator
Call Hold	HOLD	CC links for active or all calls (option A/B)	Target: call hold indication other party: generic notification indicator
Call Retrieve	RETRIEVE	CC links for active or all calls (option A/B)	Target: call retrieve indication other party: generic notification indicator
Explicit Call Transfer	ECT	Before transfer: see HOLD After transfer: LI may or may not be stopped	Target: components of Facility IE other party: generic notification indicator
Terminal Portability	TP	No impact on CC links	Target: call suspend/resume indications other party: generic notification indicator
Subaddressing	SUB	No impact on CC links	Subaddress IE, as available (calling, called, etc.)
Calling Line Identification Presentation	CLIP	No impact on CC links	CLI parameter: part of originating-Party information
Calling Line Identification Restriction	CLIR	No impact on CC links	Restriction indicator is part of CLI parameter
Connected Line Identification Presentation	COLP	No impact on CC links	COL parameter: part of terminating-Party information
Connected Line Identification Restriction	COLR	No impact on CC links	Restriction indicator is part of COL parameter
Closed User Group	CUG	No impact on CC links	CUG interlock code
Add On Conference	CONF	T_X: signal from target; Rx call sum signal CC links depending on option A/B	Target: components of Facility IE other party: generic notification indicator
Three Party Conference	3PTY	Initially: held and active calls see HOLD Conf.: see CONF	Target: components of Facility IE other party: generic notification indicator
Call Forwarding Unconditional; (see note)	CFU	One CC link for each call, which is forwarded by the target Forwarding by other parties: no impact	Target: see clause A.3.2.3, point 2, 3; if redirecting no. = target DN: not included Other party (call to target is a forwarded call): See clause A.3.2.3, point 1 Other party (call from target gets forwarded): See clause A.3.2.3, point 3
Call Forwarding No Reply; (see note)	CFNR	1) basic call with standards CC links, released after time-out (incl. CC links) 2) forwarding: same as CFU	1) basic call, released after time-out, standard IRI 2) forwarding: same parameters as for CFU
Call Forwarding Busy; see note	CFB	Network determined user busy: see CFU User determined user busy: see CFNR	Network determined user busy: see CFU user determined user busy: see CFNR
Call Deflection	CD	See CFNR	See CFNR
Partial Rerouting	PR	See CFNR	See CFNR
Malicious Call Identification	MCID	No impact on CC links	MCID response indicator sent at invocation
User-to-User Signalling 1, 2, 3	UUS	No impact on CC links	User-to-user information, more data IE (part of HI3 information, see clause D.6)
Fallback procedure (not a supplementary service)	FB	No impact on CC links	Target or other party: new basic service IE
NOTE: Other variants of Call Forwarding, like forwarding to fixed numbers, to information services, etc. are assumed to be covered by the listed services.			

A.5.2 CC link impact

The column "CC links: additional calls, impact" (see table A.5.1) defines, whether:

- for the related service CC links shall be set up, in addition to the CC links for a basic call;
- already existing calls are impacted, for example by disconnecting their information flow.

The CC link impact relates always to actions of a target being the served user. Services invoked by other parties have no CC link impact.

A.5.3 IRI Impact, general principle for sending IRI records

The column "IRI items related to service" (see table A.5.1) specifies, which parameters may be transmitted to the LEA within the IRI records. For several services, it is differentiated, whether the target or the other party is the served user.

The table specifies, which parameters are applicable in principle. That is, these parameters are normally sent to the LEA, immediately when they are available from the protocol procedures of the service. In many cases, additional IRI-CONTINUE records, compared to a basic call, will be generated. However, not each service related signalling event needs to be sent immediately within an individual record. Exceptions may exist, where several events are included in one record, even if this would result in some delay of reporting an event (this may be implementation dependent). Each record shall contain all information, which is required by the LEA to enable the interpretation of an action; example: the indication of call forwarding by the target shall include the forwarded-to number and the indication of the type of forwarding within the same record.

The complete set of parameters, which are applicable for IRI, is specified in clause A.3.3 (see tables A.3.2 and A.3.3).

If during procedures involving supplementary services protocol parameters, which are listed in tables A.3.2 and A.3.3 become available, they shall be included in IRI records. This rule is directly applicable for parameters received via ISUP and DSS1 signalling protocols. Regarding all other protocols, e.g. of analogue users, the mapping to the ISDN protocols, as defined in clause A.3.3 is assumed, before discriminating, which (mapped) parameters are copied to the IRI records.

IRI data are not stored by the IIF or MF for the purpose of keeping information on call context or call configuration, including complex multiparty calls. The LEMF (electronically) or the LEA's agent (manually) shall always be able, to find out the relevant history on the call configuration, to the extent, which is given by the available signalling protocol based information, within the telecommunication network.

Service invocations, which result in invoke and return result components (as defined in table A.3.2) need only be reported in case of successful invocations. One IRI record, containing the invoke component, possibly including additional parameters from the return result component, is sufficient. Instead of the DSS1 functional protocol components, for specific networks other ETSI-standardized components may be used, e.g. of the MAP [14].

With respect to the inclusion of LI specific parameters, see also the parameter specifications and example scenarios in clause E.3 for more details.

Details of e.g. the definition of the used record type, their content, the exact points in time of sending etc. follow from the according service specifications; in some cases, they are specified explicitly in clauses A.6 and E.3.

A.5.4 Multi party calls - general principles, options A, B

Each network must adopt option A or B according to local circumstances.

With respect to IRI, each call or call leg owns a separate IRI transaction sequence, independent of whether it is actually active or not.

With respect to the CC links, two options (A, B) exist, which depend on laws and regulations, see below. Active call or call leg means in this context, that the target is actually in communication with the other party of that call or call leg; this definition differs from the definition in [5].

A.5.4.1 CC links for active and non-active calls (option A)

For each call, active or not, separate CC links shall be provided. This guarantees, that:

- changes in the call configuration of the target are reflected immediately, with no delay, at the LEMF;
- the signal from held parties can still be intercepted.

It is a network option, whether the communication direction of a non-active call, which still carries a signal from the other party, is switched through to the LEMF, or switched off.

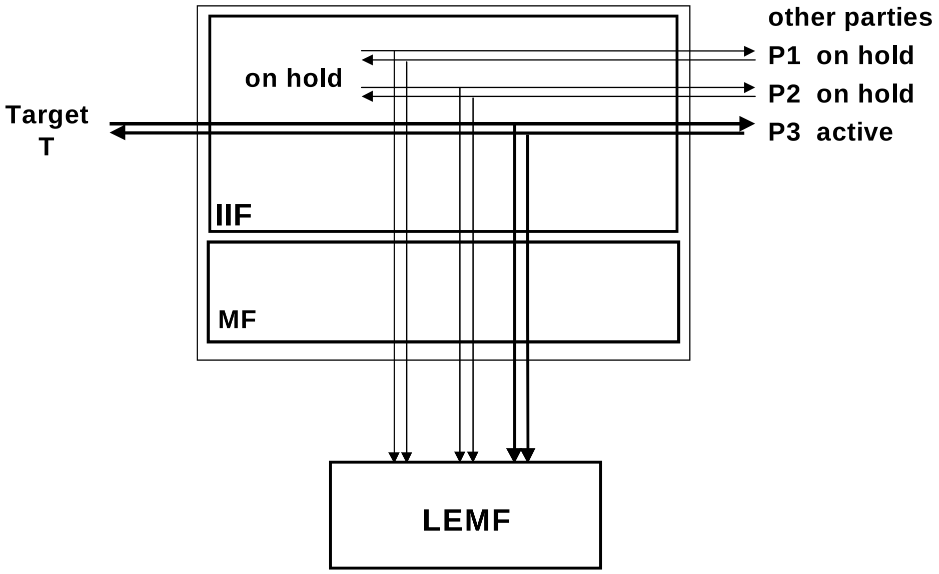


Figure A.5.1: CC link option A (example for call hold supplementary service)

A.5.4.2 Reuse of CC links for active calls (option B)

CC links are only used for calls active in their communication phase. Changes in the call configuration may not be reflected at the LEMF immediately, because switching in the IIF/MF is required, and the signal from the held party is not available.

Each time, another target call leg uses an existing CC link, an IRI-CONTINUE record with the correct CID and CCLID shall be sent.

NOTE: Even when option B is used, more than one CC link may be required simultaneously.

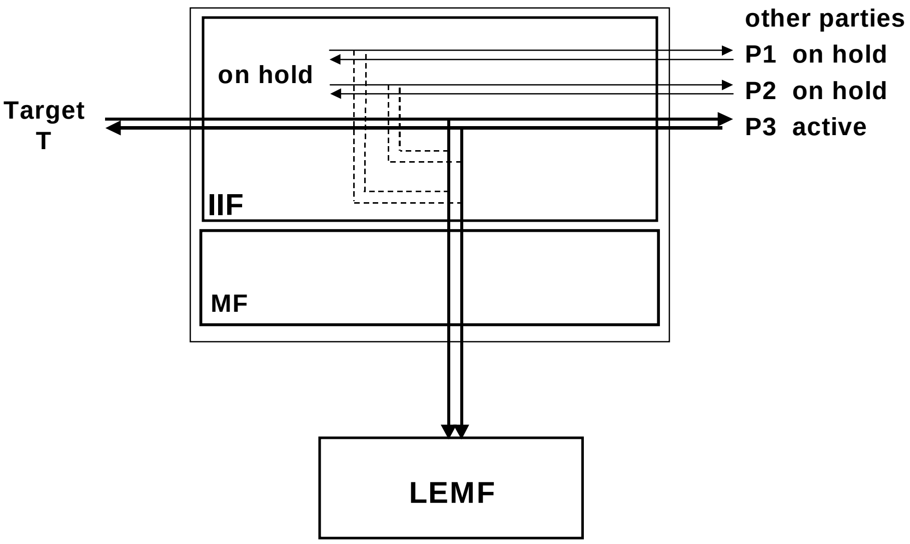


Figure A.5.2: CC link option B (example for call hold supplementary service)

A.5.5 Subscriber Controlled Input (SCI): Activation/Deactivation/Interrogation of services

For user procedures for control of Supplementary Services (Activation/Deactivation/Interrogation), a special IRI record type (IRI-REPORT record) is defined to transmit the required information.

If the DSS1 Functional Protocol [13] is used by the target, the functional information elements, usually ASN.1 encoded, are copied to the IRI-REPORT record as received by the target exchange. In case of analogue targets or use of the ISDN keypad protocol [20] (digits or IA5-characters), other appropriate parameters identifying the services are used. They may consist of the string sent by the user, or system-specific parameters, which identify the service sufficiently.

The IRI-REPORT record shall contain an indicator, whether the request of the target has been processed successfully or not.

At the exchange, where the subscriber data of a target shall be modified via a remote control procedure, an IRI-REPORT record shall be generated as if the control procedure had taken place locally.

A.6 Detailed procedures for circuit switched supplementary services

A.6.1 Advice Of Charge services (AOC)

No impact.

Advice Of Charge information is not included in IRI records.

A.6.2 Call Waiting (CW)

A.6.2.1 Call Waiting at target: CC links

In case of option A "CC links for all calls", a CC link is set up for the waiting call, using the standard procedures for terminating calls. In case of option B "CC links for active calls", no CC link is set up for the waiting call, it is treated like a held call.

With respect to CC links, the same configurations as for Call Hold apply.

Procedure, when the target accepts the waiting call: see retrieve of a held call (see clause A.6.3).

A.6.2.2 Call Waiting: IRI records

A.6.2.2.1 Target is served user

If Call Waiting is invoked at the target access by another (calling) party: the IRI-BEGIN record or a following IRI-CONTINUE record for the waiting call shall contain the LI specific parameter *call waiting indication*.

A.6.2.2.2 Other party is served user

If Call Waiting is invoked at the other (called) party's access: if a *CW notification* is received by the target's switching node, it shall be included in an IRI-CONTINUE record; it may be a separate record, or the next record of the basic call sequence.

A.6.3 Call Hold/Retrieve

A.6.3.1 CC links for active and non-active calls (option A)

If an active call is put on hold, its CC links shall stay intact; as an option, the signal from the held party is not switched through to the LEMF.

If the target sets up a new call, while one call is on hold, this call is treated like a normal originating call, i.e. a new LI configuration (CC links, IRI records) is established.

A.6.3.2 Reuse of CC links for active calls (option B)

If an active call is put on hold, its CC links shall not immediately be disconnected; as an option, the signal from the held party is not switched through to the LEMF.

If the target sets up a new call, or retrieves a previously held call, while one target call, which still owns CC links, is on hold, these CC links shall be used for the signals of the new active call.

A.6.3.3 IRI records

A.6.3.3.1 Invocation of Call Hold or Retrieve by target

An IRI-CONTINUE record with the LI specific parameter hold indication or retrieve indication, respectively, shall be sent.

A.6.3.3.2 Invocation of Hold or Retrieve by other parties

An IRI-CONTINUE record with a call hold or retrieve notification shall be sent if it has been received by the signalling protocol entity of the target call.

A.6.4 Explicit Call Transfer (ECT)

A.6.4.1 Explicit Call Transfer, CC link

During the preparation phase of a transfer, the procedures for Call Hold/Retrieve are applicable.

If the served (transferring) user is the target, its original call is released. This terminates also the CC link, and causes an IRI-END record to be sent.

After transfer, two options exist:

1) for the transferred call, CC links (and IRI records) shall be generated, in principle like for a forwarded call (similar to procedures in clause A.6.16.1, case b));

2) the transferred call shall not be intercepted.

A.6.4.2 Explicit Call Transfer, IRI records

In addition to the basic or hold/retrieve/waiting call related records and parameters, during the reconfiguration of the call, ECT-specific information at the target's access is sent to the LEMF within IRI-CONTINUE records.

When the target leaves the call after transfer, an IRI-END record is sent, and the LI transaction is terminated. Options for the new call, after transfer: see clause A.6.4.1.

A.6.5 Calling Line Identification Presentation (CLIP) (IRI Records)

A.6.5.1 Call originated by target (target is served user)

The standard CLI parameter of an originating target is included as a supplementary service parameter in the IRI records.

If for the access (BRI or PRI) of the target a special arrangement according to EN 300 089 [29] exists, whereby the user provides a user provided, not screened number, this number is included in the IRI-BEGIN record (originating-Party information), as a generic number parameter. The network provided default number of the access is, as without this arrangement, also included in the IRI record.

A.6.5.2 Call terminated at target (other party is served user)

The CLI sent from the other party is included in the IRI-BEGIN record (*originating-Party* information), irrespective of a restriction indication. An eventually received second number (case two number delivery option) is included in the IRI record as supplementary services information (Generic Number parameter).

A.6.6 Calling Line Identification Restriction (CLIR)

For use by LI, the restriction is ignored, but copied within the CLI parameter to the IRI record.

A.6.7 COnnected Line identification Presentation (COLP)

A.6.7.1 Call terminated at target (target is served user)

A connected number parameter received from the target shall be included in an IRI record (terminating-Party information). In cases where a special arrangement applies, the user provided and the network provided default number of the access is included in the IRI record.

A.6.7.2 Call originated by target (other party is served user)

If available, a connected number parameter as received from the other (terminating) party shall be included in an IRI record (terminating-Party information). Any additional number, e.g. a Generic Number, shall also be included in the IRI record.

A.6.8 COnnected Line identification Restriction (COLR)

For use by LI, the restriction is ignored, but copied within the COL parameter to the IRI record.

A.6.9 Closed User Group (CUG)

In case of a CUG call, the closed user group interlock code shall be included in an IRI.

A.6.10 Completion of Call to Busy Subscriber (CCBS)

No impact.

The first call, which meets a (terminating) busy subscriber, and is released subsequently, is treated like a standard busy call, with no CCBS related IRI information.

The procedures for CCBS, until starting a new call attempt from the served user to the terminating user, including the CCBS recall, are not subject of LI.

A.6.11 CONFerence call, add-On (CONF)

A.6.11.1 CONFerence calls, add On: CC links

The CC links carry the same bit stream as sent to/received from the target, that is, the Rx call contains the sum signal of the conference, the Tx call contains the signal from the target.

The general rules for multi party calls (see clause A.5.4) apply also for the various possible states during a conference (isolate, split, etc.). The call to the conference device as such is treated like a standard call. In case of a n-party conference, there exist n + 1 CC links in case of option "CC link for all calls", or just one CC link, in case of option "CC link for active calls".

A.6.11.2 Conference calls: IRI records

In addition to the basic or hold/retrieve/waiting call related records and parameters, during the set up and eventual reconfigurations of a conference, CONF-specific information is sent to the LEMF within IRI records.

A.6.12 Three Party Service (Conference)

A.6.12.1 CC links

a) Target is conference controller:
The 3PTY conference originates from a configuration with two single calls (one active, one held). When joining the calls to a conference, the CC links, which have carried the signals of the active target call are used to transmit the conference signals; that is, the Rx call contains the sum signal of the conference, the Tx call contains the signal from the target.

   The second CC link set, for the previously held call stays intact. If the conference is released, and the initial state (1 held, 1 active call) is re-established, the required CC links are still available.

b) Target is passive party of conference:
No impact on CC links.

A.6.12.2 Three Party Service, IRI records

For the events indicating the start and the end of the 3PTY conference, IRI records are generated.

A.6.13 Meet-Me Conference (MMC)

No impact; calls to a MMC are treated as standard calls; the MMC device is not required to be subject of LI.

A.6.14 Direct Dialling In (DDI)

LI may be applied to a PABX access DN or to a DDI extension number according to national laws and requirements.

A.6.15 Multiple Subscriber Number (MSN)

LI shall be activated individually per MSN.

If LI has to be activated for a whole ISDN BA, activation commands shall be input by the LI administrator for each number; administrative procedure shall ensure, that all numbers are covered. If during a surveillance a MSN is added or removed, a LI administrative message shall be generated, see clause 7.2.

A.6.16 Diversion Services (DIV)

Calls to a target, with a called party number equal to the intercepted target DN(s), but forwarded, are intercepted, i.e. CC links are set up, and IRI records are sent to the LEA. This applies for all kinds of call forwarding.

For calls forwarded by the other party (calling or called), the available diversion-related information is sent to the LEA.

A.6.16.1 Call diversion by target

A.6.16.1.1 Call diversion by target, CC links

In order to handle call diversion services by applying, as far as possible, common procedures, the following two cases are differentiated:

a) Call Forwarding Unconditional (CFU), Call Forwarding Busy (NDUB):
In these cases, forwarding is determined, before seizing the target access. CC links are set up, immediately, for the forwarded call.

   Other variants of Call Forwarding with immediate forwarding, i.e. without first seizing the target access, are handled in the same way (e.g. unconditional Selective Call Forwarding).

b) Call Forwarding No Reply, Call Forwarding Busy (UDUB), Call Deflection, Partial Rerouting:
Initially, the target call is set up, and the call is intercepted like a basic call.

   When forwarding takes place (e.g. after expiry of the CFNR timer), the original call is released; this may cause also a release of the CC links. In such case two optional IRI record handling may apply:

   1) For the original call an IRI-END record is sent. For the forwarded call a new set up procedure, including new LI transaction may take place with new set of IRI records (starting with IRI-BEGIN record sent to the LEA).

   2) For the forwarded call the IRI-CONTINUE record is generated and sent to a LEA, indicating the CFNR invocation.

Other variants of Call Forwarding with forwarding after first seizing the target access, are handled in the same way.

In case of multiple forwarding, one call may be intercepted several times, if several parties are targets. Considering the maximum number of diversions for one call of 5 (ITU recommended limit), one call can be intercepted 7 times, from the same or different LEAs. In principle, these procedures are independent of each other.

A.6.16.1.2 Call diversion by target, IRI records

See clause A.3.2.3, case 2, related to the target's information, and case 3, related to the forwarded-to-party information.

As above for the CC links, the diversion types a) and b1, 2) are differentiated: For case a) and b2) diversions, the IRI is part of one transaction, IRI-BEGIN, -CONTINUE, -END, for case b1) diversions, a first transaction informs about the call section, until diversion is invoked (corresponding to a basic, prematurely released call), a second transaction informs about the call section, when diversion is invoked (corresponding to case a)).

A.6.16.2 Forwarded call terminated at target

The CC link is handled in the standard way. The IRI-BEGIN record contains the available call diversion information, see clause A.3.2.3 case 1.

A.6.16.3 Call from target forwarded

The CC link is handled in the standard way. The IRI-BEGIN and possibly IRI-CONTINUE records contain the available call diversion related information, see clause A.3.2.3 case 3.

A.6.17 Variants of call diversion services

Variants of the above "standard" diversion services are treated in the same way as the corresponding "standard" diversion service.

A.6.18 Void

A.6.19 Malicious Call IDentification (MCID)

CC links: no impact.

IRI records: If a terminating target or other party invokes MCID, the MCID response indicator parameter shall be included in a dedicated or the next regular IRI record.

A.6.20 SUBaddressing (SUB)

The different types of subaddress information elements are part of the IRI records, in all basic and supplementary services cases, where they are present.

A.6.21 Terminal Portability (TP)

A.6.21.1 CC links

No impact.

A.6.21.2 IRI records

A.6.21.2.1 Invocation of terminal portability by target

Sending of the LI parameters suspend indication or resume indication in an IRI-CONTINUE record.

A.6.21.2.2 Invocation of terminal portability by other parties

Sending of the generic notification indicator, values user suspended or user resumed in an IRI-CONTINUE record.

A.6.22 User-to-User Signalling (UUS)

User-to-User parameters of services UUS1, UUS2 and UUS3 shall be reported as HI3, see clause A.4.

If User-User information is not delivered from a target to the other party (e.g. due to overload in the SS No.7 network), no notification is sent to the LEA.

A.6.23 Abbreviated Address (AA)

No impact. The service access code and abbreviated number (user input) is not included in IRI records.

A.6.24 Fixed Destination Call (FDC)

No impact. The service access code (if applicable) is not included in IRI records.

A.6.25 Alarm Call (AC)/Wake-up Service (WUS)

No impact. A Wake-up call is intercepted in the standard way; the identity of the originating party may be missing.

A.6.26 Incoming Call Barring (ICB)

No impact.

a) **Case terminating call to a target with ICB active:**
In general, the barring condition of a target is detected before the target access is determined, consequently, an IRI-REPORT records is generated.
If the access would be determined, a standard IRI-END record is generated, with the applicable cause value.

b) **Case target calls a party with ICB active:**
In general, an IRI-BEGIN record has been sent already, and CC links have been set up. Consequently, a standard IRI-END record is generated, with the applicable cause value.

A.6.27 Outgoing Call Barring (OCB)

No impact.

For a barred call, a standard record may be generated; its type and content are depending on the point in the call, where the call was released due to OCB restrictions.

A.6.28 Completion of Calls on No Reply (CCNR)

No impact. See remarks to service CCBS.

A.6.29 Reverse charging

No impact.

A.6.30 Line hunting

All accesses of the group shall get the interception profile, independently of each other, if the whole group has to be intercepted (responsibility of the LI operator).

A.6.31 Message Wait Indication (MWI)

No impact. The information, that a message is waiting, is not sent to the LEA.

A.6.32 Name display

No impact. Name strings are not included in IRI records.

A.6.33 Tones, announcements

No impact.

If the normal procedures, depending on the call state, result in sending the tone or announcement signal on the Rx CC link channel, this shall be transmitted as CC.

A.7 Fixed network technologies annex

Not covered in the present document.

A.8 GSM circuit switched technology annex

A.8.1 Functional architecture

The following picture contains the reference configuration for the lawful interception (see [21]).

There is one Administration Function (ADMF) in the network. Together with the delivery functions it is used to hide from the MSC/VLR and GMSC that there might be multiple activations by different Law Enforcement Agencies (LEAs) on the same target.

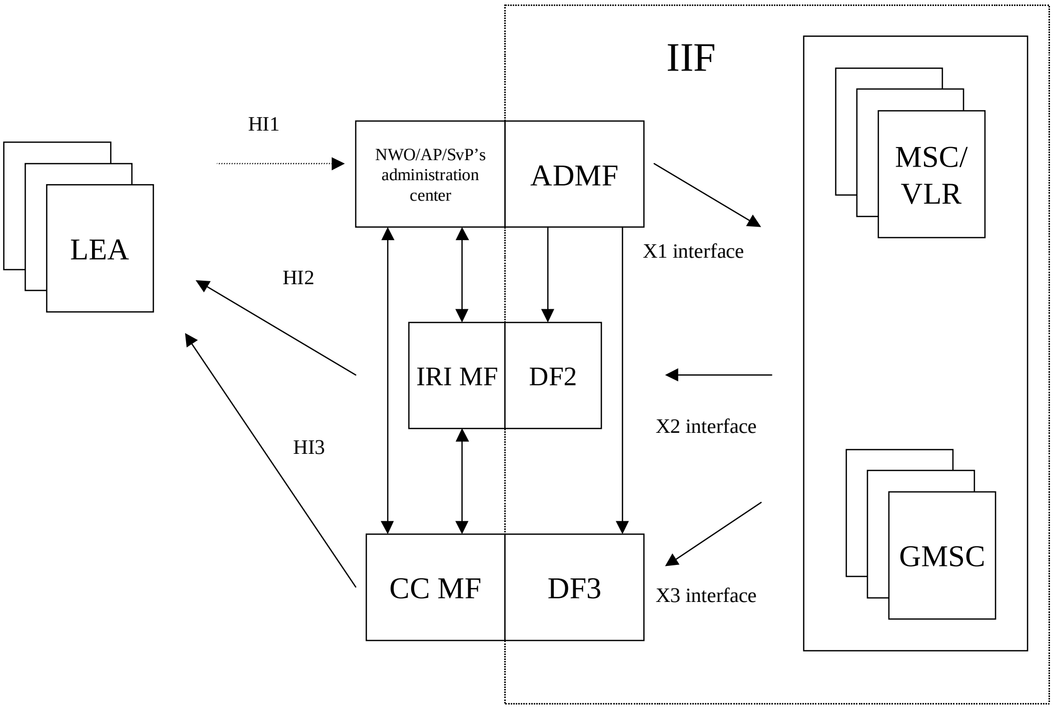


Figure A.8.1: Reference configuration for GSM Circuit switched

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.

A call could be intercepted based on several identities (MSISDN, IMSI, IMEI) of the same target.

Interception based on IMEI could lead to a delay in start of interception at the beginning of a call and interception of non-call related events is not possible.

For the delivery of the IP(CC) and IRI(CD) the MSC/VLR or GMSC 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 to.

A.8.2 Correlation of CC and IRI (see clause 6)

Correlation of the present document ID's to TS 101 509 [21] ID's.

The ID Lawful Interception Identifier (LIID) out of the present document is supported at the IIF (GSM) with warrant reference number.

Parameters out of the present document, see clause 6.2:

Communication Identifier (CID)

For each call or other activity relating to a target identity a CID is generated by the relevant network element. The CID consists of the following two identifiers:

- Network IDentifier (NID);
- Communication Identity Number (CIN).

Intercepting Node ID is used for the NID in the GSM system.

The correlation number is used for the CIN.

For the Communication IDentifier (CID) in the GSM system we use the combination of Interception Node ID and the correlation number.

A.8.3 HI3 (delivery of CC)

CC will be delivered as described in clause D.8 and as an option annex E.

Exceptionally, SMS will be delivered via HI2.

A.8.4 HI2 (delivery of IRI)

The events defined in [21] are used to generate Records for the delivery via HI2.

There are eight different events type received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

It is an implementation option if the redundant information will be sent for each further event.

Table A.8.1: Structure of the records for GSM (CS)

Event	IRI record type
Call establishment	BEGIN
Answer	CONTINUE
Supplementary service	CONTINUE
Handover	CONTINUE
Release	END
Location update	REPORT
Subscriber controlled input	REPORT
SMS	REPORT

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in MSC/VLR or GMSC or DF2/MF, if this is necessary in a specific country. Table A.8.2 gives the mapping between information received per event and information sent in records.

Table A.8.2: Description of parameters

Parameter	Definition	ASN.1 parameter
observed MSISDN	Target Identifier with the MSISDN of the target subscriber (monitored subscriber)	PartyInformation/msISDN
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber)	PartyInformation/imsi
observed IMEI	Target Identifier with the IMEI of the target subscriber (monitored subscriber), it must be checked for each call over the radio interface	PartyInformation/imei
event type	Description which type of event is delivered: Establishment, Answer, Supplementary service, Handover, Release, SMS, Location update, Subscriber controlled input	There is no one-to-one mapping for this information. Parameters presence on HI2 indicates the event type (e.g. sMS or sciData parameter presence)
event date	Date of the event generation in the MSC/VLR or GMSC	timestamp
event time	Time of the event generation in the MSC/VLR or GMSC	
dialled number	Dialled number before digit modification, IN-modification, etc.	PartyInformation (= originating)/DSS1-parameters/calledpartynumber
connected number	Number of the answering party	PartyInformation/supplementary-Services-Info
other party address	Directory number of the other party for originating calls Calling party for terminating calls	PartyInformation (= terminating)/calledpartynumber PartyInformation/callingpartynumber
call direction	Information if the monitored subscriber is calling or called e.g. MOC/MTC or originating/terminating in or/out	intercepted-Call-Direct
CID	Unique number for each call sent to the DF, to help the LEA, to have a correlation between each call and the IRI (combination of Interception Node ID and the correlation number)	communicationIdentifier
lawful interception identifier	Unique number for each surveillance lawful authorization	LawfulInterceptionIdentifier
cell id	Cell number of the target; for the location information	locationOfTheTarget
location area code	Location-area-code of the target defines the Location Area in a PLMN	
basic service	Information about Tele service or bearer service	PartyInformation/DSS1-parameters-codeset-0
supplementary service	Supplementary services used by the target e.g. CF, CW, ECT	PartyInformation/Supplementary-Services
forwarded to number	Forwarded to number at CF	PartyInformation/calledPartyNumber (party-Qualifier indicating forwarded-to-party)
call release reason	Call release reason of the target call	Release-Reason-Of-intercepted-Call
SMS	The SMS content with header which is sent with the SMS-service	SMS
SCI	Non-call related Subscriber Controlled Input (SCI) which the MSC/VLR receives from the ME	PartyInformation/sciData
NOTE: LIID parameter must be present in each record sent to the LEMF.		

A.9 TETRA technology annex

Not covered in the present document.

Annex B (normative): Packet switched network handover

B.1 Specific identifiers for LI

Beyond clause 6, at present the correlation number as specific LI identifier for packet switched networks is defined.

The correlation number is unique per PDP context and is used for the following purposes:

- correlate CC with IRI;
- correlate different IRI records within one PDP context.

As an example, in the GSM GPRS system, the correlation number may be the combination of GGSN address and charging ID.

B.2 HI1: interface port for administrative state

There are no additions beyond clause 7.

B.3 HI2: interface port for IRI

B.3.1 Definition of Interception Related Information for packet switched

Intercept related information will in principle be available in the following phases of a data transmission:

1) At connection attempt when the target identity becomes active, at which time packet transmission may or may not occur (set up of a data context, target may be the originating or terminating party).

2) At the end of a connection, when the target identity becomes inactive (removal of a data context).

3) At certain times when relevant information are available.

In addition, information on non-transmission related actions of a target constitute IRI and is sent via HI2, e.g. information on subscriber controlled input.

The Intercept Related Information (IRI) may be subdivided into the following categories:

4) Control information for HI2 (e.g. correlation information).

5) Basic data context information, for standard data transmission between two parties.

B.3.2 Exception handling

Not covered in the present document.

B.3.3 Security aspects

Not covered in the present document.

B.4 HI3: interface port for Content of Communication

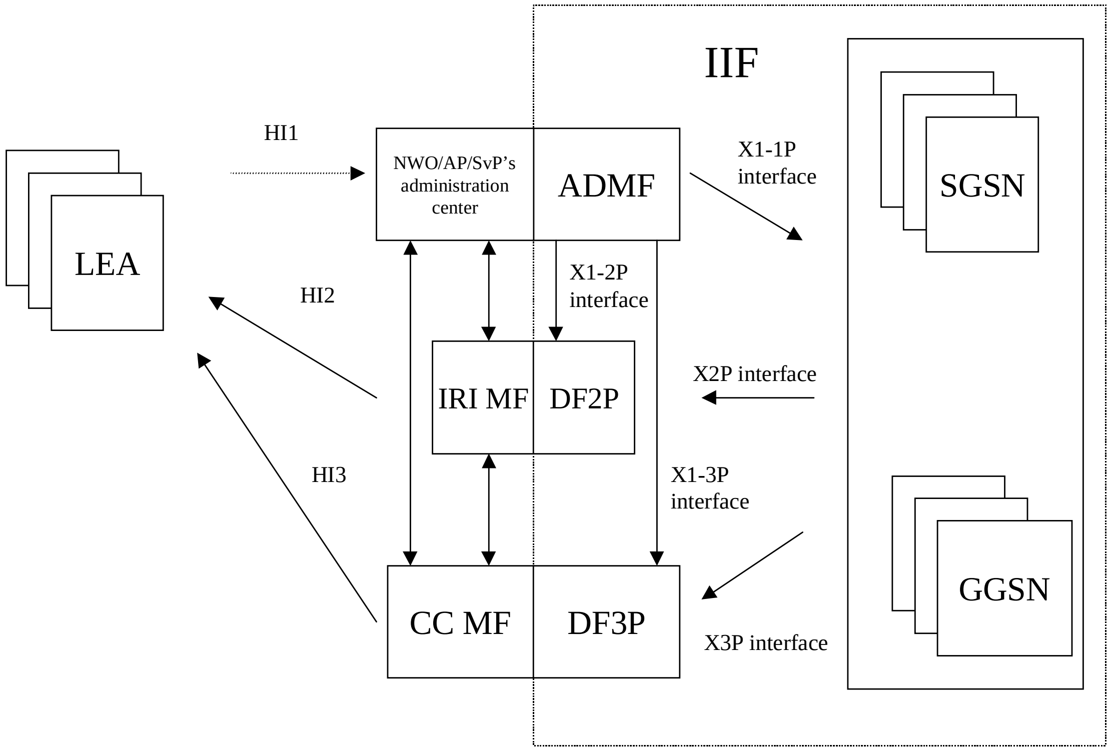
Not covered in the present document.

B.5 GPRS technology annex

B.5.1 Functional architecture

Figure B.5.1 contains the reference configuration for the lawful interception (see [21]).

There is one Administration Function (ADMF) in the network. Together with the delivery functions it is used to hide from the xGSN that there might be multiple activations by different Law Enforcement Agencies (LEAs) on the same target identity.



NOTE: GGSN interception is a national option.

Figure B.5.1: Reference 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.

A communication could be intercepted based on several identities (MSISDN, IMSI, IMEI) of the same target.

For the delivery of the IP(CC) and IRI(CD) the xGSN provides a correlation number and target identity to the DF2P and DF3P which is used there to select the different LEAs where the CC/CD shall be delivered to.

B.5.2 Correlation

B.5.2.1 Correlation of the present document ID's to GSM ID's

The ID Lawful Interception Identifier (LIID) out of the present document is supported at the IIF (GSM) with warrant reference number.

Parameters from the present document, see clause 6.2.

Communication IDentifier (CID)

For each communication or other activity relating to a target identity a CID is generated by the relevant network element. The CID consists of the following two identifiers:

- Network IDentifier (NID);
- Communication Identity Number (CIN).

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

B.5.2.2 GPRS LI correlation between CC and IRI

For the delivery of CC and IRI, the SGSN or GGSN provides correlation numbers and target identities to the HI2 and HI3. The correlation number is unique per PDP context and is used to correlate CC with IRI and the different IRIs of one PDP context.

B.5.3 HI2 (Delivery of IRI)

The events defined in [22] are used to generate records for the delivery via HI2.

There are eight different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. Table gives B.5.1 the mapping between event type received at DF2 level and record type sent to the LEMF.

Table B.5.1: Mapping between GPRS events and HI2 records type

Event	IRI record type
GPRS attach	REPORT
GPRS detach	REPORT
PDP context activation (successful)	BEGIN
PDP context activation (unsuccessful)	REPORT
Start of intercept with PDP context active	BEGIN
PDP context deactivation	END
Cell and/or RA update	REPORT if no PDP context is active CONTINUE if, at least, one PDP context is active
SMS	REPORT

For some packet oriented data services such as GPRS, the first event of a communication attempt shall be the PDP context activation or a similar event and an IRI-BEGIN record shall be issued. The end of the communication attempt shall be the PDP context deactivation or a similar event and an IRI-END record shall be issued. While a PDP context is active, IRI-CONTINUE records shall be used for CC relevant IRI data records, IRI-REPORT records otherwise.

For some packet oriented data services such as GPRS, if LI is being activated during an already established PDP context or similar, an IRI-BEGIN record will mark the start of the interception. If LI is being deactivated during an established PDP context or similar, no IRI-END record will be transmitted. The end of interception can be communicated to the LEA by other means (HI1).

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in xGSN or DF2P/MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

Table B.5.2: Mapping between events information and IRI information

Parameter	Description	HI2 ASN.1 parameter
observed MSISDN	Target Identifier with the MSISDN of the target subscriber (monitored subscriber)	PartyInformation/msISDN
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber)	PartyInformation/imsi
observed IMEI	Target Identifier with the IMEI of the target subscriber (monitored subscriber)	PartyInformation/imei
observed PDP address	PDP address used by the target	PartyInformation/pDP-address-allocated-to-the-target
event type	Description which type of event is delivered: PDP Context Activation, PDP Context Deactivation, GPRS Attach, etc.	gPRSevent
event date	Date of the event generation in the xGSN	timestamp
event time	Time of the event generation in the xGSN	
Access point name	The APN of the access point	PartyInformation/aPN
PDP type	This field describes the PDP type as defined in TS 101 347 [23], TS 100 940 [30], ETS 300 974 [14]	PartyInformation/pDP-type
Correlation number	Unique number for each PDP context delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context and the IRI	gPRSCorrelationNumber
lawful interception identifier	Unique number for each lawful authorization	LawfulInterceptionIdentifier
CGI (Cell Global ID)	Cell number of the target; for the location information	locationOfTheTarget/globalCellId
routing area code	Routing-area-code of the target defines the Routing Area in a GPRS-PLMN	locationOfTheTarget/rAId
SMS	The SMS content with header which is sent with the SMS-service	SMS
failed context activation reason	This field gives information about the reason(s) for failed context(s) activation of the target subscriber	gPRSOperationErrorCode
failed attach reason	This field gives information about the reason(s) for failed attach attempts of the target subscriber	gPRSOperationErrorCode
NOTE: LIID parameter must be present in each record sent to the LEMF.		

B.5.4 HI3 (Delivery of CC)

For a GPRS HI3 interface port for Content of Communication see annex F.

Annex C (normative): HI2 Delivery mechanisms and procedures

There are two possible methods for delivery of IRI to the LEMF:

a) ROSE (see clause C.1);

b) FTP (see clause C.2).

According to national requirements at least one of these methods shall be provided.

C.1 ROSE

C.1.1 Architecture

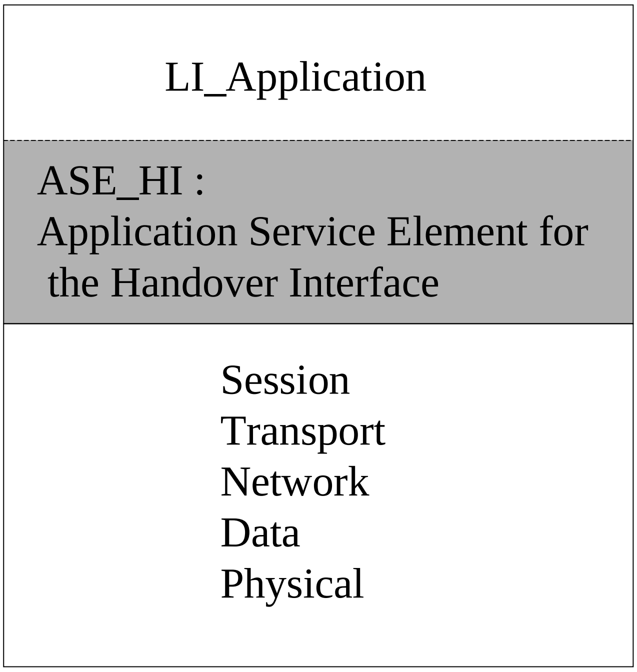


Figure C.1.1: Architecture

The ASE_HI manages the data link, the coding/decoding of the ROSE operations and the sending/receiving of the ROSE operations.

C.1.2 ASE_HI procedures

C.1.2.1 Sending part

To request the sending of data to a peer entity, the LI_Application provides the ASE_HI, the address of the peer entity, the nature of the data and the data.

On receiving a request of the LI_Application:

- If the data link toward the peer entity address is active, the ASE_HI, from the nature of the data provided, encapsulates this data in the relevant RO-Invoke operation.

- If the data link toward the peer entity address is not active, the ASE_HI establishes this data link (see clause C.1.2.3). Then, depending on the nature of the data provided, the ASE_HI encapsulates this data in the relevant RO-Invoke operation.

Depending on the natures of the data provided by the LI_Application, the ASE_HI encapsulates this data within the relevant ROSE operation:

- LI management notification: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation "Sending_of_HI1_Notification". The ASN.1 format is described in clauses D.2 and D.4 (HI1 interface).

- IRI: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation *Sending_of_IRI*. The ASN.1 format is described in clauses D.2 and D.5 (HI2 interface).

- SMS: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation *Sending-of-IRI*. The ASN.1 format is described in clauses D.2 and D.5 (HI2 interface).

- User packet data transfer (used for data which can be exchanged via ISUP/DSS1/MAP signalling: e.g. UUS): in this case the data provided by the application are encoded:

  - either within the class 2 RO-Invoke operation "Circuit-Call-related-services" in case of data associated to a circuit call (for e.g. UUS 1 to 3) The ASN.1 format is described in clauses D.2 and D.6 (HI3 interface);

  - either within the class 2 RO-Invoke operation "No-Circuit-Call-related-services" in case of data not associated with a circuit call (for e.g. UUS 4.) The ASN.1 format is described in annex A, clauses D.2 and D.6 (HI3 interface).

- TETRA data transfer: in this case all the information provided by the application are encoded within the class 2 RO-Invoke operation "Sending-of-TETRA-Data". The ASN.1 format is described in clauses D.2 and D.7.

Depending on the class of the operation, the ASE-HI may have to wait for an answer. In this case a timer, depending on the operation, is started on the sending of the operation and stopped on the receipt of an answer (RO_Result, RO_Error, RO_Reject).

On timeout of the timer, the ASE_HI indicates to the LI_Application that no answer has been received. It is under the LI_Application responsibility to send again the data or to inform the administrator of the problem.

On receipt of an answer component (after verification that the component is not erroneous), the ASE_HI stop the relevant timer and acts depending on the type of component:

- On receipt of a RO_Result, the ASE_HI provide the relevant LI_Application an indication that the data has been received by the peer LI-application and the possible parameters contained in the RO_Result.

- On receipt of a RO_Error, the ASE_HI provide the relevant LI_Application an indication that the data has not been received by the peer LI-application and the possible "Error cause". The error causes are defined for each operation in the relevant ASN.1 script. It is under the LI_Application responsibility to generate or not an alarm message toward an operator or administrator.

- On receipt of a RO_Reject_U/P, the ASE_HI provide the relevant LI_Application an indication that the data has not been received by the peer LI-application and the "Problem cause". The "problem causes" are defined in [17] to [19]. It is under the LI_Application responsibility to send again the data or to inform the operator/administrator of the error.

On receipt of an erroneous component, the ASE_HI acts as described in [17] to [19].

C.1.2.2 Receiving part

On receipt of a ROSE operation from the lower layers:

- When receiving operations from the peer entity, the ASE_HI verifies the syntax of the component and transmits the parameters to the LI-Application. If no error/problem is detected, in accordance with the [17] to [19] standard result (only Class2 operation are defined), the ASE_HI sends back a RO_Result which coding is determined by the relevant operation ASN.1 script. The different operations which can be received are:
    - RO-Invoke operation "Sending-of-HI1-Notification" (HI1 interface);
    - RO-Invoke operation "Sending-of-IRI" (HI2 interface);
    - RO-Invoke operation "Circuit-Call-Related-Services" (HI3 interface);
    - RO-Invoke operation "No-Circuit-Call-Related-Services" (HI3 interface);
    - RO-Invoke operation "Sending-of-TETRA-Data" (HI3 interface).

In case of error, the ASE_HI acts depending on the reason of the error or problem:

- In accordance with the rules defined by [17] to [19], a RO_Error is sent in case of unsuccessfully operation at the application level. The Error cause provided is one among those defined by the ASN.1 script of the relevant operation.
- In accordance with the rules defined in [17] to [19], a RO_Reject_U/P is sent in case of erroneous component. On receipt of an erroneous component, the ASE_HI acts as described in [17] to [19].

C.1.2.3 Data link management

This function is used to establish or release a data link between two peer LI_Applications entities (MF and LEMF).

Depending on a per destination address configuration data, the data link establishment may be required either by the LEMF LI_Application or by the MF LI_Application.

C.1.2.3.1 Data link establishment

To request the establishment of a data link toward a peer entity, the LI_Application provides, among others, the destination address of the peer entity (implicitly, this address defined the protocol layers immediately under the ASE_HI: TCP/IP, X25, …). On receipt of this request, the ASE_HI request the establishment of the data link with respect of the rules of the under layers protocol.

As soon as the data link is established, the requesting LI_Application initiates an authentication procedure:

- The origin LI_Application requests the ASE_HI to send the class 2 RO-Invoke operation "Sending_of_Password" which includes the "origin password" provided by the LI_Application.
- The peer LI-Application, on receipt of the "origin password" and after acceptance, requests to its ASE_HI to send back a RO-Result. In addition, this destination application requests the ASE_HI to send the class 2 RO-Invoke operation "Sending-of-Password" which includes the "destination password" provided by the LI_Application.
- The origin LI-Application, on receipt of the "destination password" and after acceptance, requests to its ASE_HI to send back a RO-Result. This application is allowed to send data.
- After receipt of the RO_Result, this application is allowed to send data.

In case of erroneous password, the data link is immediately released and a "password error indication" is sent toward the operator.

Optionally a *Data link test* procedure may be used to verify periodically the data link:

- When no data have been exchanged during a network dependent period of time toward an address, (may vary from 1 min to 30 min) the LI_Application requests the ASE_HI to send the class 2 RO-Invoke operation *Data-Link-Test*.
- The peer LI-Application, on receipt of this operation, requests to its ASE_HI to send back a RO-Result.
- On receipt of the Result the test is considered valid by the LI_Application.
- If no Result is received or if a Reject/Error message is received, the LI_Application requests the ASE_LI to release the data link and send an error message toward the operator.

C.1.2.3.2 Data link release

- The end of the connection toward the peer LI_Application is under responsibility of the LI_Application. E.g. the end of the connection may be requested in the following cases:
  - When all the data (IRI, etc.) has been sent. To prevent unnecessary release, the datalink may be released only when no LI_Application data have been exchanged during a network dependent period of time.
  - The data link is established when a call is intercepted and released when the intercepted call is released (and all the relevant data have been sent).
  - For security purposes.
  - For changing of password or address of the LEMF/IIF.
  - Etc.
- To end the connection a LI_Application requests the ASE_HI to send the class 2 RO-Invoke operation "End-Of-Connection".
- The peer LI-Application, on receipt of this operation, requests to its ASE_HI to send back a RO_Result.
- On receipt of the Result the LI_Application requests the ASE_LI to release the data link.
- If no Result is received after a network dependent period of time, or if a Reject/Error message is received, the LI_Application requests the ASE_LI to release the data link and to send an error message toward the operator/administrator.

C.1.2.4 Handling of unrecognized fields and parameters

See annex G.

C.1.3 Profiles

Not covered in the present document.

C.2 FTP

C.2.1 Introduction

At HI2 interface FTP is used over internet protocol stack for the delivery of the IRI. The FTP is defined in [24]. The IP is defined in [27]. The TCP is defined in [28].

FTP supports reliable delivery of data. The data may be temporarily buffered in the Mediation Function (MF) in case of link failure. FTP is independent of the payload data it carries.

C.2.2 Usage of the FTP

The MF acts as the FTP client and the LEMF acts as the FTP server. The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The MF may buffer files.

Several records may be gathered to bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing/file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms;
- frequency of transfer, based on volume trigger, e.g. X octets.

Every file shall contain only complete IRI records. The single IRI record shall not be divided into several files.

There are two possible ways how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (ref: "File naming method A)"). The other way is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (ref: "File naming method B)").

File naming:

The names for the files transferred to a LEA are formed according to one of the two available formats, depending on the delivery file strategy chosen (e.g. due to national convention or operator preference).

Either each file contains data of only one observed target (as in method A) or several targets' data is put to files common to all observed target traffic through MF (as in method B).

The maximum set of allowed characters in interception file names are "a"…"z", "A"…"Z", "-", "_", ".", and decimals "0"…"9".

File naming method A):

<LIID>_<seq>.<ext>

where:

LIID = as defined in the present document clause "Lawful Interception Identifier (LIID)". This field has a character string (or digit string for sub-address option) value, e.g. "ABCD123456". This is a unique interception request identifier allocated by the ADMF. It will be given by the ADMF to the LEA via the HI1 interface after the ADMF has been authorized to command the start of the interception of a specific target. The possible network operator identifier part used should be agreed with (and allocated by) the regulatory organization administrating the local telecommunication practises.

seq = integer ranging between [0..2^64-1], in ASCII form (not exceeding 20 ASCII digits), identifying the sequence number for file transfer from this node per a specific target.

ext = ASCII integer ranging between ["1".."7".] (in hex: 31H…37H), identifying the file type. The possible file type coding for IRI is shown in table C.2.1.

Table C.2.1: Possible file types

File types that the LEA may get	Intercepted data types
"1" (in binary: 0011 0001)	IRI

This alternative A is used when each target's IRI is gathered per observed target to dedicated delivery files. This method provides the result of interception in a very refined form to the LEAs, but requires somewhat more resources in the MF than alternative B. With this method, the data sorting and interpretation tasks of the LEMF are considerably easier to facilitate in near real time than in alternative B.

File naming method B):

The other choice is to use monolithic fixed format file names (with no trailing file type part in the file name):

<filenamestring> of the format ABXYyymmddhhmmsseeeet

where:

AB = Two letter ASCII Operator ID (as agreed with the national telecom regulators).
XY = Two letter ASCII identification of the MF node (as assigned by the operator).
yy = Two digits ASCII integer ranging between ["00"..."99"], identifying the last to digits of the year.
mm = Two digits ASCII integer ranging between ["01"..."12"], identifying the month.
dd = Two digits ASCII integer ranging between ["01"..."31"], identifying the day.
hh = Two digits ASCII integer ranging between ["00"..."23"], identifying the hour.
mm = Two digits ASCII integer ranging between ["00"..."59"], identifying the minute.
ss = Two digits ASCII integer ranging between ["00"..."59"], identifying the second.
eeee = Alphanumeric extension made up of four characters chosen at the discretion of the Operator and/or the MF to avoid file name clashes within the MF. Each of the position shall be out of 'A'....'Z', '0'....'9'.
t = ASCII integer is ["1"] (in hex: 31H), identifying the file type. The possible file type codings for intercepted data are shown in table C.2.1.

EXAMPLE:

<filenamestring> (e.g. ABXY00041014084400001)

Where:

ABXY = Source node identifier part, used for all files by the mobile network operator "AB" from this MF node named "XY".
00 = year 2000
04 = month April
10 = day 10
14 = hour
08 = minutes
44 = seconds
0000 = extension
1 = file type. The type "1" is reserved for IRI data files.
(Codings "2" = CC(MO), "4" = CC(MT), "6" = CC(MO&MT) are reserved for HI3).

This alternative B is used when several targets' intercepted data is gathered to common delivery files. This method does not provide the result of interception in as refined form to the LEAs as the alternative A, but it is faster in performance for the MF point of view. With this method, the MF does not need to keep many files open like in alternative A.

C.2.3 Profiles

NOTE: This clause is informative only.

As there are several ways (usage profiles) how data transfer can be arranged by using the FTP, this clause contains practical considerations how the communications can be set up. Guidance is given for client-server arrangements, session establishments, time outs, the handling of the files (in RAM or disk). Example batch file is described for the case that the sending FTP client uses files. If instead (logical) files are sent directly from the client's RAM memory, then the procedure can be in principle similar though no script file would then be needed.

At the LEMF side, FTP server process is run, and at MF, FTP client. No FTP server (which could be accessed from outside the operator network) shall run in the MF. The FTP client can be implemented in many ways, and here the FTP usage is presented with an example only. The FTP client can be implemented by a batch file or a file sender program that uses FTP via an API. The login needs to occur only once per e.g. <destaddr> & <leauser> **-** pair. Once the login is done, the files can then be transferred just by repeating "mput" command and checking the transfer status (e.g. from the API routine return value). To prevent inactivity timer triggering, a dummy command (e.g. "pwd") can be sent every T seconds (T should be less than L, the actual idle time limit). If the number of FTP connections is wanted to be as minimized as possible, the FTP file transfer method "B" is to be preferred to the method A (though the method A helps more the LEMF by pre-sorting the data sent).

Simple example of a batch file extract:

FTP commands usage scenario for transferring a list of files:

To prevent FTP cmd line buffer overflow the best way is to use wildcarded file names, and let the FTP implementation do the file name expansion (instead of shell). The number of files for one mput is not limited this way:

```
ftp <flags> <destaddr>
  user <leauser> <leapasswd>
  cd <destpath>
  lcd <srcpath>
  bin
  mput <files>
  nlist <lastfile> <checkfile>
  close
EOF
```

This set of commands opens an FTP connection to a LEA site, logs in with a given account (auto-login is disabled), transfers a list of files in binary mode, and checks the transfer status in a simplified way.

Brief descriptions for the FTP commands used in the example:

```
user <user-name> <password>           Identify the client to the remote FTP server.
cd <remote-directory>                 Change the working directory on the remote machine to
                                      remote-directory.
lcd <directory>                       Change the working directory on the local machine.
bin                                   Set the file transfer type to support binary image transfer
mput <local-files>                    Expand wild cards in the list of local files given as
                                      arguments and do a put for each file in the resulting list.
                                      Store each local file on the remote machine.
nlist <remote-directory> <local-file> Print a list of the files in a directory on the remote
                                      machine. Send the output to local-file.
close                                 Terminate the FTP session with the remote server, and return
                                      to the command interpreter. Any defined macros are erased.
```

The parameters are as follows:

<**flags**> contains the FTP command options, e.g. "-i -n -V -p" which equals to "interactive prompting off", "auto-login disabled", "verbose mode disabled", and "passive mode enabled". (These are dependent on the used ftp- version.)

<**destaddr**> contains the IP address or DNS address of the destination (LEA).

<**leauser**> contains the receiving (LEA) username.

<**leapasswd**> contains the receiving (LEA) user's password.

<**destpath**> contains the destination path.

<**srcpath**> contains the source path.

<**files**> wild carded file specification (matching the files to be transferred).

<**lastfile**> the name of the last file to be transferred.

<**checkfile**> is a (local) file to be checked upon transfer completion; if it exists then the transfer is considered successful.

The FTP application should to do the following things if the check file is not found:

- keep the failed files;
- raise "file transfer failure" error condition (i.e. send alarm to the corresponding LEA);
- the data can be buffered for a time that the buffer size allows. If that would finally be exhausted, DF would start dropping the corresponding target's data until the transfer failure is fixed;
- the transmission of the failed files is retried until the transfer eventually succeeds. Then the DF would again start collecting the data;
- upon successful file transfer the sent files are deleted from the DF.

The FTP server at LEMF shall not allow anonymous login of an FTP client.

C.2.4 File content

The file content is in method A relating to only one intercepted target.

In the file transfer method B, the file content may relate to any intercepted targets whose intercept records are sent to the particular LEMF address.

Individual IRI records shall not be fragmented into separate files at the FTP layer.

C.2.5 Exceptional procedures

Overflow at the receiving end (LEMF) is avoided due to the nature of the protocol.

In case the transit network or receiving end system (LEMF) is down for a reasonably short time period, the local buffering at the MF will be sufficient as a delivery reliability backup procedure.

In case the transit network or receiving end system (LEMF) is down for a very long period, the local buffering at the MF may have to be terminated. Then the following intercepted data coming from the intercepting nodes to the MF would be discarded, until the transit network or LEMF is up and running again.

C.2.6 Other considerations

The FTP protocol mode parameters used:

• Transmission Mode:	stream;
• Format:	non-print;
• Structure:	file-structure;
• Type:	binary.

The FTP client (= user-FTP process at the MF) uses e.g. the default standard FTP ports 20 (for data connection) and 21 (for control connection), "passive" mode is supported. The data transfer process listens the data port for a connection from a server-FTP process.

For the file transfer from the MF to the LEMF(s) e.g. the following data transfer parameters are provided for the FTP client (at the MF):

- transfer destination (IP) address, e.g. "194.89.205.4";
- transfer destination username, e.g. "LEA1";
- transfer destination directory path, e.g. "/usr/local/LEA1/1234-8291";
- transfer destination password;

- interception file type, "1" (this is needed only if the file naming method A is used).

LEMF may use various kind directory structures for the reception of interception files. It is strongly recommended that at the LEMF machine the structure and access and modification rights of the storage directories are adjusted to prevent unwanted directory operations by a FTP client.

Timing considerations for the HI2 FTP transmission:

The MF and LEMF sides control the timers to ensure reliable, near-real time data transfer. The transmission related timers are defined within the lower layers of the used protocol and are out of scope of the present document.

The following timers may be used within the LI application:

Name	Controlled by	Units	Description
T1 inactivity timer	LEMF	s	Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side.
T2 send file trigger	MF	ms	Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (see clause C.2.2).

Annex D (normative): Structure of data at the Handover Interface

This annex specifies the coding details at the Handover Interface (HI) for all data, which may be sent from the NWO/AP/SvP's equipment to the LEMF, across HI.

At the three Handover Interface ports, the following data may be present:

- interface port HI1: Interception administration information;
- interface port HI2: Intercept Related Information (IRI);
- interface port HI3: records containing Content of Communication (CC).

The detailed coding specification for these types of information is contained in this annex, including sufficient details for a consistent implementation in the NWO/AP/SvP's equipment and the LEMF.

It must be noticed some data are ROSE specific and have no meaning when FTP is used. Those specificities are described at the beginning of each clause (D.3, D.4, D.5 and D.6).

D.1 Syntax definitions

The transferred information and messages are encoded to be binary compatible with [15] (Abstract Syntax Notation One (ASN.1)) and [16] (Basic Encoding Rules (BER)).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased below for clarity.

A *type,* in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE.

The UNIVERSAL class is reserved for international standards such as [15] and [16]. Most parameter type identifiers in the HI ROSE operations are encoded as CONTEXT specific class. Users of the protocol may extend the syntax with PRIVATE class parameters without conflict with the present document, but risk conflict with other users' extensions. APPLICATION class parameters are reserved for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

A *parameter* in the present document is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be IMPLICIT or EXPLICIT. An IMPLICIT type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. EXPLICIT types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the *Number* tag, where an EXPLICIT number of type INTEGER would have the *INTEGER* tag within the *Number* tag. The present document uses IMPLICIT tagging for more compact message encoding.

For the coding of the value part of each parameter the general rule is to use a widely use a standardized format when it exists (ISUP, DSS1, MAP, etc.).

As a large part of the information exchanged between the users may be transmitted within ISUP/DSS1 signalling, the using of the coding defined for this signalling guarantee the integrity of the information provided to the LEMF and the evolution of the interface. For example if new values are used within existing ISUP parameters, this new values shall be transmitted transparently toward the LEMF.

D.2 Object tree

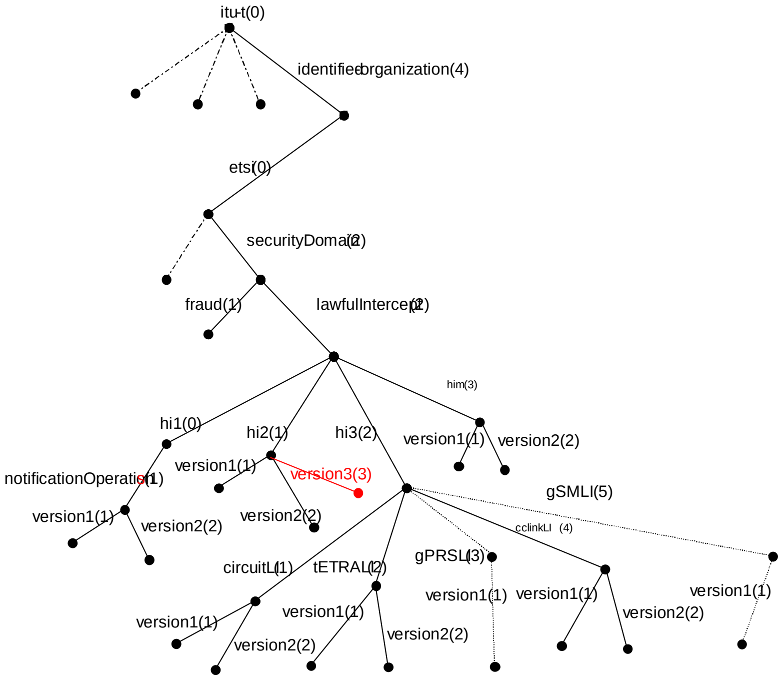


Figure D.2.1: Object Tree: Lawful InterceptionASN.1 description of security object tree

SecurityDomainDefinitions { itu-t (0) identified-organization (4) etsi (0) securityDomain (2)}

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Security DomainId
securityDomainId OBJECT IDENTIFIER  ::= { itu-t (0) identified-organization (4) etsi (0)
securityDomain (2)}

-- Security Subdomains
fraudSubDomainId OBJECT IDENTIFIER              ::= {securityDomainId fraud (1)}
lawfulInterceptSubDomainId OBJECT IDENTIFIER    ::= {securityDomainId lawfulIntercept (2)}

-- LawfulIntercept Subdomains
hi1DomainId OBJECT IDENTIFIER               ::= {lawfulInterceptSubDomainId hi1 (0)}
hi2DomainId OBJECT IDENTIFIER               ::= {lawfulInterceptSubDomainId hi2 (1)}
hi2DomainIDv3 OBJECT IDENTIFIER             ::= {hi2DomainId version (3)}

hi3DomainId OBJECT IDENTIFIER               ::= {lawfulInterceptSubDomainId hi3 (2)}
himDomainId OBJECT IDENTIFIER               ::= {lawfulInterceptSubDomainId him (3)}

-- HI1 Subdomains
hi1NotificationOperations OBJECT IDENTIFIER ::= {hi1DomainId notificationOperations (1)}

-- HI3 Subdomains
hi3CircuitLISubDomainId OBJECT IDENTIFIER   ::= {hi3DomainId circuitLI (1)}

hi3TETRALISubDomainId OBJECT IDENTIFIER ::= {hi3DomainId tETRALI (2)}
-- For further study

hi3GPRSLISubDomainId OBJECT IDENTIFIER  ::= {hi3DomainId gPRSLI (3)}
-- For further study

hi3CCLinkLISubDomainId OBJECT IDENTIFIER    ::= {hi3DomainId cclinkLI (4)}

hi3GSMLISubDomainId OBJECT IDENTIFIER ::= {hi3DomainId gSMLI (5)}
-- For further study
END -- SecurityDomainDefinitions
```

D.3 HI management operation

This data description applies only for ROSE delivery mechanism.

ASN.1 description of HI management operation (any HI interface)

```
HIManagementOperations
{ itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) him (3)
version2 (2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
EXPORTS                 sending-of-Password,
        data-Link-Test,
        end-Of-Connection;
```

```
IMPORTS                 OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

        himDomainId
            FROM SecurityDomainDefinitions
            { itu-t (0) identified-organization (4) etsi (0) securityDomain (2)};
```

```
sending-of-Password     OPERATION ::=
{
    ARGUMENT    Password-Name
    ERRORS      { ErrorsHim }
    CODE        global:{ himDomainId sending-of-Password (1) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3 s and 240s.
-- The timer default value is 60s.
```

```
data-Link-Test          OPERATION ::=
{
    ERRORS      { other-failure-causes }
    CODE        global:{ himDomainId data-link-test (2) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3s and 240s.
-- The timer default value is 60s.
```

```
end-Of-Connection       OPERATION ::=
{
    ERRORS      { other-failure-causes }
    CODE        global:{ himDomainId end-of-connection (3) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3s and 240s.
-- The timer default value is 60s.
```

```
other-failure-causes    ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter       ERROR ::= { CODE local:2}
erroneous-parameter     ERROR ::= { CODE local:3}

ErrorsHim               ERROR ::=
{
    other-failure-causes |
    missing-parameter |
    unknown-parameter |
    erroneous-parameter
}
```

```
Password-Name           ::= SEQUENCE
{
    password    [1] OCTET STRING (SIZE (1..25)),
    name        [2] OCTET STRING (SIZE (1..25)),
    ...
}
    --  IA5 string recommended
```

```
END -- HIManagementOperations
```

D.4 LI management notification

Declaration of ROSE operation sending-of-HI1-Notification is ROSE delivery mechanism specific. When using FTP delivery mechanism, data HI1-Operation must be considered.

NOTE: This annex does not describe an electronic Handover Interface, but HI1 information, using HI2 mechanism.

ASN.1 description of LI management notification operation (HI1 Interface)

```
HI1NotificationOperations
{ itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi1 (0)
notificationOperations (1) version2 (2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS
    OPERATION,
    ERROR
        FROM
        Remote-Operations-Information-Objects
        {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

    hi1NotificationOperations
        FROM
        SecurityDomainDefinitions
        { itu-t (0) identified-organization (4) etsi (0) securityDomain (2)}

    CommunicationIdentifier,
    TimeStamp,
    LawfulInterceptionIdentifier
        FROM HI2Operations
        { itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi2
(1)  version2 (2)};
```

```
sending-of-HI1-Notification     OPERATION ::=
{
    ARGUMENT    HI1-Operation
    ERRORS      { ErrorHI1Notifications }
    CODE        global:{ hi1NotificationOperations version1 (1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer default value is 60s.
-- NOTE: The value for this timer is to be set on the equipment waiting for the returned message;
-- its value shall be agreed between the NWO/AP/SvP and the LEA, depending on their equipment
-- properties.
```

```
other-failure-causes    ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter       ERROR ::= { CODE local:2}
erroneous-parameter     ERROR ::= { CODE local:3}

ErrorHI1Notifications ERROR ::=
{
    other-failure-causes |
    missing-parameter |
    unknown-parameter |
    erroneous-parameter
}
```

```
HI1-Operation   ::= CHOICE
{
    liActivated         [1] Notification,
    liDeactivated       [2] Notification,
    liModified          [3] Notification,
    alarms-indicator    [4] Alarm-Indicator
}
```

```
Notification ::= SEQUENCE
{
    lawfulInterceptionIdentifier    [1] LawfulInterceptionIdentifier,
        --This identifier is the LIID identity provided with the lawful authorization
        --for each target.
    communicationIdentifier         [2] CommunicationIdentifier OPTIONAL,
        --Only the NWO/PA/SvPIdentifier is provided (the one provided with the Lawful
        --authorization).
        --Called callIdentifier in Edition 1
    timeStamp                       [3] TimeStamp,
        --date and time of the report.
    ...
}
```

```
Alarm-Indicator ::= SEQUENCE
{
    communicationIdentifier     [1] CommunicationIdentifier OPTIONAL,
        --only the NWO/PA/SvPIdentifier is provided (the one provided with the
        --Lawful authorization)
    timeStamp                   [2] TimeStamp,
        --date and time of the report.
    alarm-information           [3] OCTET STRING    (SIZE (1..25)),
        --Provides information about alarms (free format).
    ...
}
```

```
--PARAMETERS

END -- H1CircuitDataOperations
```

D.5 Intercept related information (HI2)

Declaration of ROSE operation sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data IRI-Content must be considered.

ASN.1 description of IRI (HI2 interface)

```
HI2Operations
{ itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi2 (1)
version3 (3)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS OPERATION,
    ERROR
        FROM Remote-Operations-Information-Objects
        {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

    hi2DomainId,
    hi2DomainIDv3
        FROM
            SecurityDomainDefinitions
            { itu-t (0) identified-organization (4) etsi (0) securityDomain (2)};
```

```
sending-of-IRI  OPERATION ::=
{
    ARGUMENT    IRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{ hi2DomainId sending-of-IRI (1)  version1 (1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE: The same note as for HI management operation applies.
```

```
IRIsContent     ::= CHOICE
{
   iRIContent      IRIContent,
   iRISequence     IRISequence
)
```

```
IRISequence     ::= SEQUENCE OF IRIContent
   -- Aggregation of IRIContent is an optional feature.
   -- It may be applied in cases when at a given point in time several IRI records are
   -- available for delivery to the same LEA destination.
   -- As a general rule, records created at any event shall be sent immediately and shall
   -- not held in the DF or MF in order to apply aggregation.
   -- When aggregation is not to be applied, IRIContent needs to be chosen.
```

```
IRIContent      ::= CHOICE
{
    iRI-Begin-record        [1] IRI-Parameters,
        --at least one optional parameter must be included within the iRI-Begin-Record
    iRI-End-record          [2] IRI-Parameters,
    iRI-Continue-record     [3] IRI-Parameters,
        --at least one optional parameter must be included within the iRI-Continue-Record
    iRI-Report-record       [4] IRI-Parameters,
        --at least one optional parameter must be included within the iRI-Report-Record
    ...
}
```

```
unknown-version         ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter       ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
    unknown-version |
    missing-parameter |
    unknown-parameter-value |
    unknown-parameter
}
--These values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
IRI-Parameters      ::= SEQUENCE
{
    domainID                            [0] OBJECT IDENTIFIER (hi2DomainIDv3) OPTIONAL,
        -- for the sending entity the inclusion of the Object Identifier is mandatory
    iRIversion                          [23] ENUMERATED
    {
        version2(2),
        ... ,
        version3(3)
    } OPTIONAL,
        -- if not present, it means version 1 is handled
    lawfulInterceptionIdentifier        [1] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    communicationIdentifier             [2] CommunicationIdentifier,
        -- used to uniquely identify an intercepted call.
        -- called CallIdentifier in Edition 1 of the document
    timeStamp                           [3] TimeStamp,
        -- date and time of the event triggering the report.
    intercepted-Call-Direct             [4] ENUMERATED
    {
        not-Available(0),
        originating-Target(1),
            -- in case of GPRS, this indicates that the PDP context activation
            -- or deactivation is MS requested
        terminating-Target(2),
            -- in case of GPRS, this indicates that the PDP context activation or deactivation is
            -- network initiated
    ...
    } OPTIONAL,
    intercepted-Call-State              [5] Intercepted-Call-State OPTIONAL,
    ringingDuration                     [6] OCTET STRING (SIZE (3)) OPTIONAL,
        -- Duration in seconds. BCD coded : HHMMSS
    conversationDuration                [7] OCTET STRING (SIZE (3)) OPTIONAL,
        -- Duration in seconds. BCD coded : HHMMSS
    locationOfTheTarget                 [8] Location OPTIONAL,
        -- location of the target subscriber
    partyInformation                    [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
        -- This parameter provides the concerned party (Originating, Terminating or forwarded
        -- party), the identity(ies) of the party and all the information provided by the party.
    callContentLinkInformation          [10] SEQUENCE
    {
        cCLink1Characteristics      [1] CallContentLinkCharacteristics OPTIONAL,
            -- information concerning the Content of Communication Link Tx channel established
            -- toward the LEMF (or the sum signal channel, in case of mono mode).
        cCLink2Characteristics      [2] CallContentLinkCharacteristics OPTIONAL,
            -- information concerning the Content of Communication Link Rx channel established
            -- toward the LEMF.
        ...
    } OPTIONAL,
    release-Reason-Of-Intercepted-Call  [11] OCTET STRING (SIZE (2)) OPTIONAL,
        -- Release cause coded in [31] format.
        -- This parameter indicates the reason why the
        -- intercepted call cannot be established or why the intercepted call has been
        -- released after the active phase.
    nature-Of-The-intercepted-call      [12] ENUMERATED
    {
        --Nature of the intercepted "call":
        gSM-ISDN-PSTN-circuit-call(0),
            -- the possible UUS content is sent through the HI3 "data" interface
            -- the possible call content call is established through the HI3 „circuit„ interface
        gSM-SMS-Message(1),
            -- the SMS content is sent through the HI2 or HI3 "data" interface
        uUS4-Messages(2),
            -- the UUS content is sent through the HI3 "data" interface
        tETRA-circuit-call(3),
            -- the possible call content call is established through the HI3 "circuit" interface
            -- the possible data are sent through the HI3 "data" interface
        teTRA-Packet-Data(4),
            -- the data are sent through the HI3 "data" interface
        gPRS-Packet-Data(5),
            -- the data are sent through the HI3 "data" interface
        ...
    } OPTIONAL,
    serverCenterAddress                 [13] PartyInformation OPTIONAL,
        -- e.g. in case of SMS message this parameter provides the address of  the relevant
        -- server within the calling (if server is originating) or called
        -- (if server is terminating) party address parameters
    sMS                                 [14] SMS-report OPTIONAL,
        -- this parameter provides the SMS content and associated information
    cC-Link-Identifier                  [15] CC-Link-Identifier OPTIONAL,
        -- Depending on a network option, this parameter may be used to identify a CC link
        -- in case of multiparty calls.
    national-Parameters                 [16] National-Parameters OPTIONAL,
    gPRSCorrelationNumber               [18] GPRSCorrelationNumber OPTIONAL,
    gPRSevent                           [20] GPRSEvent OPTIONAL,
        -- This information is used to provide particular action of the target
        -- such as attach/detach
    sgsnAddress                         [21] DataNodeAddress OPTIONAL,
    gPRSOperationErrorCode              [22] GPRSOperationErrorCode OPTIONAL,
    ...,
    ggsnAddress                         [24] DataNodeAddress OPTIONAL,
    sIPMessage                          [30] OCTET STRING OPTIONAL
        -- This parameter is duplicated from 3GPP 33.108 [61].
}
```

```
-- PARAMETERS FORMATS
```

```
CommunicationIdentifier     ::= SEQUENCE
{
    communication-Identity-Number   [0] OCTET STRING (SIZE (1..8)) OPTIONAL,
        -- Temporary Identifier of an intercepted call to uniquely identify an intercepted call
        -- within the node (free format). This parameter is mandatory if there is associated
        -- information sent over HI3interface (CClink, data,..) or when
        -- CommunicationIdentifier is used for IRI other than IRI-Report-record
        -- This parameter was called call-Identity-Number in Ed.1 (v1.1.1) of the document.

    network-Identifier              [1] Network-Identifier,
    ...
}
-- NOTE: The same "CommunicationIdentifier" value is sent :
-- with the HI3 information for correlation purpose between the IRI and the information sent on
-- the HI3 interfaces (CCLink, data, ..) with each IRI associated to a same intercepted call
-- for correlation purpose between the different IRI.
```

```
Network-Identifier      ::= SEQUENCE
{
    operator-Identifier         [0] OCTET STRING (SIZE (1..5)),
        -- It is a notification of the NWO/AP/SvP in ASCII- characters.
        -- The parameter is mandatory.
    network-Element-Identifier  [1] Network-Element-Identifier OPTIONAL,
    ...
}
```

```
Network-Element-Identifier  ::= CHOICE
{
    e164-Format         [1] OCTET STRING (SIZE (1..25)),
        -- E164 address of the node in international format. Coded in the same format as the
        -- calling party number parameter of the ISUP (parameter part: [5]).
    x25-Format          [2] OCTET STRING (SIZE (1..25)),
        -- X25 address
    iP-Format           [3] OCTET STRING (SIZE (1..25)),
        -- IP address
    dNS-Format          [4] OCTET STRING (SIZE (1..25)),
        -- DNS address
    ...,
    iP-Address          [5] IPAddress,
    ...
}
```

```
CC-Link-Identifier      ::=     OCTET STRING (SIZE (1..8))
    -- Depending on a network option, this parameter may be used to identify a CClink
    -- in case of multiparty calls.
```

```
TimeStamp               ::= CHOICE
{
-- The minimum resolution required is one second.
    localTime           [0] LocalTimeStamp,
    utcTime             [1] UTCTime
}
```

```
LocalTimeStamp              ::= SEQUENCE
{
    generalizedTime                 [0] GeneralizedTime,
        -- The minimum resolution required is one second.
    winterSummerIndication          [1] ENUMERATED
    {
        notProvided(0),
        winterTime(1),
        summerTime(2),
        ...
    }
}
```

```
PartyInformation            ::= SEQUENCE
{
    party-Qualifier                     [0] ENUMERATED
    {
        originating-Party(0),
            -- In this case, the partyInformation parameter provides the identities related to
            -- the originating party and all information provided by this party.
            -- This parameter provides also all the information concerning the redirecting
            -- party when a forwarded call reaches a target.
        terminating-Party(1),
            -- In this case, the partyInformation parameter provides the identities related to
            -- the terminating party and all information provided by this party.
        forwarded-to-Party(2),
            -- In this case, the partyInformation parameter provides the identities related to
            -- the forwarded to party and parties beyond this one and all information
            -- provided by this parties, including the call forwarding reason.
        gPRS-Target(3),
        ...
    },
    partyIdentity                       [1] SEQUENCE
    {
        imei                [1] OCTET STRING (SIZE (8)) OPTIONAL,
            -- See MAP format [32]
        tei                 [2] OCTET STRING (SIZE (1..15)) OPTIONAL,
            -- ISDN-based Terminal Equipment Identity
        imsi                [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
            -- See MAP format [32] International Mobile
            -- Station Identity E.212 number beginning with Mobile Country Code
        callingPartyNumber  [4] CallingPartyNumber OPTIONAL,
            -- The calling party format is used to transmit the identity of a calling party
        calledPartyNumber   [5] CalledPartyNumber OPTIONAL,
            -- The called party format is used to transmit the identity of a called party or
            -- a forwarded to party.
        msISDN              [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
            -- MSISDN of the target, encoded in the same format as the AddressString
            -- parameters defined in MAP format document ref [32], clause 14.7.8.
        ...,
        e164-Format         [7] OCTET STRING (SIZE (1..25)) OPTIONAL,
            -- E164 address of the node in international format. Coded in the same format as
            -- the calling party number parameter of the ISUP (parameter part:[5])
        sip-url             [8] OCTET STRING OPTIONAL
            -- See RFC 2543 [59]. This parameter is duplicated from 3GPP 33.108 [61].
    },
    services-Information                [2] Services-Information OPTIONAL,
        -- This parameter is used to transmit all the information concerning the
        -- complementary information associated to the basic call
    supplementary-Services-Information  [3] Supplementary-Services OPTIONAL,
        -- This parameter is used to transmit all the information concerning the
        -- activation/invocation of supplementary services during a call or out-of call not
        -- provided by the previous parameters.
    services-Data-Information           [4] Services-Data-Information OPTIONAL,
        -- This parameter is used to transmit all the information concerning the complementary
        -- information associated to the basic data call.
    ...
}
```

```
CallingPartyNumber      ::= CHOICE
{
    iSUP-Format         [1] OCTET STRING (SIZE (1..25)),
        -- Encoded in the same format as the calling party number (parameter field)
        -- of the ISUP (see [5]).
    dSS1-Format         [2] OCTET STRING (SIZE (1..25)),
        -- Encoded in the format defined for the value part of the Calling party number
        -- information element of DSS1 protocol [6].
        -- The DSS1 Information element identifier and the DSS1 length are not included.
    ...
}
```

```
CalledPartyNumber       ::= CHOICE
{
    iSUP-Format         [1] OCTET STRING (SIZE (1..25)),
        -- Encoded in the same format as the called party number (parameter field)
        -- of the ISUP (see [5]).
    mAP-Format          [2] OCTET STRING (SIZE (1..25)),
        -- Encoded as AddressString of the MAP protocol [32]
    dSS1-Format         [3] OCTET STRING (SIZE (1..25)),
        -- Encoded in the format defined for the value part of the Called party number information
        -- element of DSS1 protocol [6].
        -- The DSS1 Information element identifier and the DSS1 length are not included.
    ...
}
```

```
Location    ::= SEQUENCE
{
    e164-Number         [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
        -- Coded in the same format as the ISUP location number (parameter
        --field) of the ISUP (see [5]).
    globalCellID        [2] OCTET STRING (SIZE (5..7)) OPTIONAL,
        -- See MAP format (see [32]).
    tetraLocation       [3] TetraLocation OPTIONAL,
    rAI                 [4] OCTET STRING (SIZE (6)) OPTIONAL,
        -- The Routeing Area Identifier is coded in accordance with the clause 10.5.5.15 of
        -- document ref [41] without the Routing Area Identification IEI (only the
        -- last 6 octets are used).
    gsmLocation         [5] GSMLocation OPTIONAL,
    umtsLocation        [6] UMTSLocation OPTIONAL,
    sAI                 [7] OCTET STRING (SIZE (7)) OPTIONAL,
        -- format:  PLMN-ID 3 octets (no. 1 - 3),
        --          LAC     2 octets (no. 4 - 5),
        --          SAC     2 octets (no. 6 - 7)
        --          (according to 3GPP TS 25.413 [62]).
    ...
}
```

```
TetraLocation   ::= CHOICE
{
    ms-Loc      [1] SEQUENCE
    {
        mcc             [1] INTEGER (0..1023),
            -- 16 bits ETS [40]
        mnc             [2] INTEGER (0..1023),
            -- 14 bits ETS [40]
        lai             [3] INTEGER (0..65535),
            -- 14 bits ETS [40]
        ci              [4] INTEGER OPTIONAL
    },
    -- (to be completed)
    ls-Loc      [2] INTEGER
    -- (to be confirmed and completed)
}
```

```
GSMLocation     ::= CHOICE
{
    geoCoordinates      [1] SEQUENCE
    {
        latitude    [1] PrintableString (SIZE(7..10)),
            -- format: XDDMMSS.SS
        longitude   [2] PrintableString (SIZE(8..11)),
            -- format: XDDDMMSS.SS
        mapDatum    [3] MapDatum DEFAULT wGS84,
        ...
    },
        -- format :     XDDDMMSS.SS
        --      X           : N(orth), S(outh), E(ast), W(est)
        --      DD or DDD   : degrees (numeric characters)
        --      MM          : minutes (numeric characters)
        --      SS.SS       : seconds, the second part (.SS) is optionnal
        -- Example:
        --      latitude short form     N502312
        --      longitude long form     E1122312.18

    utmCoordinates      [2] SEQUENCE
    {
        utm-East    [1] PrintableString (SIZE(10)),
        utm-North   [2] PrintableString (SIZE(7)),
            -- example  utm-East    32U0439955
            --          utm-North   5540736
        mapDatum    [3] MapDatum DEFAULT wGS84,
        ...
    },

    utmRefCoordinates   [3] SEQUENCE
    {
        utmref-string   PrintableString (SIZE(13)),
        mapDatum        MapDatum DEFAULT wGS84,
        ...
    },
        -- example  32UPU91294045

    wGS84Coordinates    [4] OCTET STRING (SIZE(7..10))
    -- format is as defined in GSM 03.32 [57]; polygon type of shape is not allowed.
}
```

```
MapDatum ::= ENUMERATED
{
    wGS84,
    wGS72,
    eD50,
        -- European Datum 50
    ...
}
```

```
UMTSLocation ::= CHOICE
{
    point                   [1] GA-Point,
    pointWithUnCertainty    [2] GA-PointWithUnCertainty,
    polygon                 [3] GA-Polygon,
    ...
}
```

```
GeographicalCoordinates ::= SEQUENCE
{
    latitudeSign    ENUMERATED
    {
        north,
        south
    },
    latitude        INTEGER (0..8388607),
    longitude       INTEGER (-8388608..8388607),
    ...
}
```

```
GA-Point ::= SEQUENCE
{
    geographicalCoordinates     GeographicalCoordinates,
    ...
}
```

```
GA-PointWithUnCertainty ::=SEQUENCE
{
    geographicalCoordinates     GeographicalCoordinates,
    uncertaintyCode             INTEGER (0..127)
}
```

```
maxNrOfPoints                   INTEGER ::= 15
```

```
GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF
    SEQUENCE
    {
        geographicalCoordinates     GeographicalCoordinates,
        ...
    }
```

```
CallContentLinkCharacteristics      ::= SEQUENCE
{
    cCLink-State            [1] CCLink-State OPTIONAL,
        -- current state of the CCLink
    release-Time            [2] TimeStamp OPTIONAL,
        -- date and time of the release of the Call Content Link.
    release-Reason          [3] OCTET STRING (SIZE(2)) OPTIONAL,
        -- Release cause coded in [31] format.
    lEMF-Address            [4] CalledPartyNumber OPTIONAL,
        -- Directory number used to route the call toward the LEMF.
    ...
}
```

```
CCLink-State    ::= ENUMERATED
{
    setUPInProcess(1),
    callActive(2),
    callReleased(3),
    lack-of-resource(4),
        -- The lack-of-resource state is sent when a CC Link cannot
        -- be established because of lack of resource at the MF level.
    ...
}
```

```
Intercepted-Call-State          ::= ENUMERATED
{
    idle(1),
        -- When the intercept call is released, the state is IDLE and the reason is provided
        -- by the release-Reason-Of-Intercepted-Call parameter.
    setUpInProcees(2),
        -- The setup of the call is in process.
    connected (3),
        -- The answer has been received.
    ...
}
```

```
Services-Information            ::= SEQUENCE
{
    iSUP-parameters             [1] ISUP-parameters OPTIONAL,
    dSS1-parameters-codeset-0   [2] DSS1-parameters-codeset-0 OPTIONAL,
    ...
}
```

```
ISUP-parameters         ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one additional ISUP parameter TLV coded not already defined in
-- the previous parameters. The Tag value is the one given in Recommendation [5].

    -- In version 1 of this specification "iSUP-parameters" is defined as mandatory.
    -- It might occur that no ISUP parameter is available. In that case in a version 1
    -- implementation the value "zero" may be included in the first octet string of the SET.

    -- The Length and the Value are coded in accordance with the parameter definition in
    -- recommendation [5]. Hereafter are listed the main parameters.
    -- However other parameters may be added:

    -- Transmission medium requirement: format defined in recommendation [5].
    -- This parameter can be provided with the "Party Information" of the "calling party".

    -- Transmission medium requirement prime: format defined in recommendation [5].
    -- This parameter can be provided with the "Party Information" of the "calling party".
```

```
DSS1-parameters-codeset-0       ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset 0. The parameter is coded as
-- described in recommendation [6] (The DSS1 Information element identifier and the DSS1 length
-- are included). Hereafter are listed the main parameters
-- (However other parameters may be added):

    -- Bearer capability: this parameter may be repeated. Format defined in recommendation [6].
    -- This parameter can be provided with the "Party Information" of the "calling party",
    -- "called party" or "forwarded to party".

    -- High Layer Compatibility: this parameter may be repeated. Format defined in
    -- recommendation [6].
    -- This parameter can be provided with the "Party Information" of the "calling party",
    -- "called party" or " forwarded to party".

    -- Low Layer capability: this parameter may be repeated. Format defined in
    -- recommendation [6].
    -- This parameter can be provided with the "Party Information" of the "calling party",
    -- "called party" or "forwarded to party".
```

```
Supplementary-Services          ::= SEQUENCE
{
    standard-Supplementary-Services     [1] Standard-Supplementary-Services OPTIONAL,
    non-Standard-Supplementary-Services [2] Non-Standard-Supplementary-Services OPTIONAL,
    other-Services                      [3] Other-Services OPTIONAL,
    ...
}
```

```
Standard-Supplementary-Services     ::= SEQUENCE
{
    iSUP-SS-parameters              [1] ISUP-SS-parameters OPTIONAL,
    dSS1-SS-parameters-codeset-0    [2] DSS1-SS-parameters-codeset-0 OPTIONAL,
    dSS1-SS-parameters-codeset-4    [3] DSS1-SS-parameters-codeset-4 OPTIONAL,
    dSS1-SS-parameters-codeset-5    [4] DSS1-SS-parameters-codeset-5 OPTIONAL,
    dSS1-SS-parameters-codeset-6    [5] DSS1-SS-parameters-codeset-6 OPTIONAL,
    dSS1-SS-parameters-codeset-7    [6] DSS1-SS-parameters-codeset-7 OPTIONAL,
    dSS1-SS-Invoke-components       [7] DSS1-SS-Invoke-Components OPTIONAL,
    mAP-SS-Parameters               [8] MAP-SS-Parameters OPTIONAL,
    mAP-SS-Invoke-Components        [9] MAP-SS-Invoke-Components OPTIONAL,
    ...
}
```

```
Non-Standard-Supplementary-Services ::= SET SIZE (1..20) OF CHOICE
{
    simpleIndication        [1] SimpleIndication,
    sciData                 [2] SciDataMode,
    ...
}
```

```
Other-Services              ::= SET SIZE (1..50) OF OCTET STRING (SIZE (1..256))
-- Reference manufacturer manuals.
```

```
ISUP-SS-parameters          ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- It must be noticed this parameter is retained for compatibility reasons.
-- It is recommended not to use it in new work but to use ISUP-parameters parameter.

-- Each "OCTET STRING" contains one additional ISUP parameter TLV coded not already defined in
-- the previous parameters. The Tag value is the one given in recommendation [5].
-- The Length and the Value are coded in accordance with the parameter definition in recommendation
-- [5]. Hereafter are listed the main parameters. However other parameters may be added:

    -- Connected Number: format defined in recommendation [5].
    -- This parameter can be provided with the " Party Information" of the
    -- "called party" or "forwarded to party".

    -- RedirectingNumber: format defined in recommendation [5].
    -- This parameter can be provided with the " Party Information" of the "originating party".

    -- Original Called Party Number: format defined in recommendation [5].
    -- This parameter can be provided with the " Party Information" of the "originating party".

    -- Redirection information: format defined in recommendation [5].
    -- This parameter can be provided with the "Party Information" of the
    -- "originating party", "forwarded to party" or/and "Terminating party".

    -- Redirection Number: format defined in recommendation [5].
    -- This parameter can be provided with the "Party Information" of the
    -- "forwarded to party" or "Terminating party".

    -- Call diversion information: format defined in recommendation [5].
    -- This parameter can be provided with the "Party Information" of the
    -- "forwarded to party" or "Terminating party".

    -- Generic Number: format defined in recommendation [5].
    -- This parameter can be provided with the "Party Information" of the
    -- "calling party", "called party" or "forwarded to party".
    -- This parameters are used to transmit additional identities (additional, calling party
    -- number, additional called number, …).

    -- Generic Notification: format defined in recommendation [5].
    -- This parameter may be provided with the "Party Information" of the
    -- "calling party", "called party" or "forwarded to party".
    -- This parameters transmit the notification to the other part of the call of the supplementary
    -- services activated or invoked by a subscriber during the call.

    -- CUG Interlock Code: format defined in recommendation [5].
    -- This parameter can be provided with the "Party Information" of the "calling party".
```

```
DSS1-SS-parameters-codeset-0    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset 0. The parameter is coded as
-- described in recommendation [6] (The DSS1 Information element identifier and the DSS1 length
-- are included). Hereafter are listed the main parameters (However other parameters may be added):

    -- Calling Party Subaddress: Format defined in recommendation [6].
    -- This parameter can be provided with the "Party Information" of the "calling party".

    -- Called Party Subaddress : Format defined in recommendation [6].
    -- This parameter can be provided with the "Party Information" of the "calling party".

    -- Connected Subaddress.: Format defined in recommendation (see [14]).
    -- This parameter can be provided with the "Party Information" of the
    -- "called party" or "forwarded to party".

    -- Connected Number : Format defined in recommendation (see [14]).
    -- This parameter can be provided with the "Party Information" of the
    -- "called party" or "forwarded to party".

    -- Keypad facility : Format defined in recommendation [6].
    -- This parameter can be provided with the "Party Information" of the
    -- "calling party", "called party" or "forwarded to party".

    -- Called Party Number: format defined in recommendation [5].
    -- This parameter could be provided with the "Party Information" of the "calling party"
    -- when target is the originating party; it contains the dialled digits before modification
    -- at network level (e.g. IN interaction, translation, etc …).
```

```
DSS1-SS-parameters-codeset-4    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset 4. The parameter is coded as
-- described in the relevant recommendation.
```

```
DSS1-SS-parameters-codeset-5    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset 5. The parameter is coded as
-- described in the relevant national recommendation.
```

```
DSS1-SS-parameters-codeset-6    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "OCTET STRING" contains one DSS1 parameter of the codeset 6. The parameter is coded as
-- described in the relevant local network recommendation.
```

```
DSS1-SS-parameters-codeset-7    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one DSS1 parameter of the codeset 7. The parameter is coded as
-- described in the relevant user specific recommendation.
```

```
DSS1-SS-Invoke-Components   ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one DSS1 Invoke or Return Result component.
-- The invoke or return result component is coded as
-- described in the relevant DSS1 supplementary service recommendation.
    -- Invoke or Return Result component (BeginCONF): reference [19]
    -- Invoke or Return Result component (AddCONF): reference [19]
    -- Invoke or Return Result component (SplitCONF): reference [19]
    -- Invoke or Return Result component (DropCONF): reference [19]
    -- Invoke or Return Result component (IsolateCONF): reference [19]
    -- Invoke or Return Result component (ReattachCONF): reference [19]
    -- Invoke or Return Result component (PartyDISC): reference [19]
    -- Invoke or Return Result component (MCIDRequest): reference [16]
    -- Invoke or Return Result component (Begin3PTY): reference [20]
    -- Invoke or Return Result component (End3PTY): reference [20]
    -- Invoke or Return Result component (ECTExecute): reference [25]
    -- Invoke or Return Result component (ECTInform): reference [25]
    -- Invoke or Return Result component (ECTLinkIdRequest): reference [25]
    -- Invoke or Return Result component (ECTLoopTest): reference [25]
    -- Invoke or Return Result component (ExplicitECTExecute): reference [25]
    -- Invoke or Return Result component (ECT: RequestSubaddress): reference [25]
    -- Invoke or Return Result component (ECT: SubaddressTransfer): reference [25]
    -- Invoke or Return Result component (CF: ActivationDiversion): reference [21]
    -- Invoke or Return Result component (CF: DeactivationDiversion): reference [21]
    -- Invoke or Return Result component (CF: ActivationStatusNotification): reference [21]
    -- Invoke or Return Result component (CF: DeactivationStatusNotification): reference [21]
    -- Invoke or Return Result component (CF: InterrogationDiversion): reference [21]
    -- Invoke or Return Result component (CF: InterrogationServedUserNumber): reference [21]
    -- Invoke or Return Result component (CF: DiversionInformation): reference [21]
    -- Invoke or Return Result component (CF: CallDeflection): reference [21]
    -- Invoke or Return Result component (CF: CallRerouteing): reference [21]
    -- Invoke or Return Result component (CF: DivertingLegInformation1): reference [21]
    -- Invoke or Return Result component (CF: DivertingLegInformation2): reference [21]
    -- Invoke or Return Result component (CF: DivertingLegInformation3): reference [21]
    -- other invoke or return result components ...
```

```
MAP-SS-Invoke-Components    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one MAP Invoke or Return Result component.
-- The invoke or return result component is coded as
-- described in the relevant MAP supplementary service recommendation.
```

```
MAP-SS-Parameters   ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- Each "octet string" contains one MAP Parameter. The parameter is coded as
-- described in the relevant MAP supplementary service recommendation.
```

```
SimpleIndication            ::= ENUMERATED
{
    call-Waiting-Indication(0),
        -- The target has received a call waiting indication for this call add-conf-Indication(1),
        -- this call has been added to a conference
    call-on-hold-Indication(2),
        -- indication that this call is on hold
    retrieve-Indication(3),
        -- indication that this call has been retrieved
    suspendIndication(4),
        -- indication that this call has been suspended
    resume-Indication(5),
        -- indication that this call has been resumed
    answer-Indication(6),
        -- indication that this call has been answered
    ...
}
```

```
SciDataMode     ::= OCTET STRING (SIZE (1..256))
```

```
SMS-report      ::= SEQUENCE
{
    communicationIdentifier     [1] CommunicationIdentifier,
        -- used to uniquely identify an intercepted call: the same used for the
        -- relevant IRI
        -- called CallIdentifier in Ed.1 (v.1.1.1) of the document
    timeStamp                   [2] TimeStamp,
        -- date and time of the report. The format is
        -- the one defined in case a) of the ASN.1 recommendation [33].
        -- (year month day hour minutes seconds)
    sMS-Contents                [3] SEQUENCE
    {
        initiator           [1] ENUMERATED
        {
            -- party which sent the SMS
            target(0),
            server(1),
            undefined-party(2),
            ...
        },
        transfer-status     [2] ENUMERATED
        {
            succeed-transfer(0),
                --the transfer of the SMS message succeeds
            not-succeed-transfer(1),
            undefined(2),
            ...
        } OPTIONAL,
        other-message       [3] ENUMERATED
        {
            -- In case of terminating call, indicates if the server will send other SMS.
            yes(0),
            no(1),
            undefined(2),
            ...
        } OPTIONAL,
        content             [4] OCTET STRING (SIZE (1..270)),
            -- Encoded in the format defined for the SMS mobile.
        ...
    }
}
```

```
LawfulInterceptionIdentifier    ::= OCTET STRING (SIZE (1..25))
-- It is recommended to use ASCII characters in "a"…"z", "A"…"Z", "-", "_", ".", and "0"…"9"
-- For subaddress option only "0"..."9" shall be us
```

```
National-Parameters     ::= SET SIZE (1..40) OF OCTET STRING (SIZE (1..256))
-- Content defined by national law
```

```
GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))
```

```
GPRSEvent ::= ENUMERATED
{
    pDPContextActivation(1),
    startOfInterceptionWithPDPContextActive(2),
    pDPContextDeactivation(4),
    gPRSAttach (5),
    gPRSDetach (6),
    cellOrRAUpdate (10),
    sMS (11),
    ... ,
    pDPContextModification (13)
}
-- see ref [42]
```

```
Services-Data-Information ::= SEQUENCE
{
    gPRS-parameters [1] GPRS-parameters OPTIONAL,
    ...
}
```

```
GPRS-parameters ::= SEQUENCE
{
    pDP-address-allocated-to-the-target     [1] DataNodeAddress OPTIONAL,
    aPN                                     [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
    pDP-type                                [3] OCTET STRING (SIZE(2)) OPTIONAL,
    ...
}
```

```
GPRSOperationErrorCode ::= OCTET STRING (SIZE(2))
-- Refer to standard [41] for values(GMM cause or SM cause parameter).
```

```
DataNodeAddress ::= CHOICE
{
    ipAddress   [1] IPAddress,
    x25Address  [2] X25Address,
    ...
}
```

```
IPAddress ::= SEQUENCE
{
    iP-type         [1] ENUMERATED
    {
        iPV4(0),
        iPV6(1),
        ...
    },
    iP-value        [2] IP-value,
    iP-assignment   [3] ENUMERATED
    {
        static(1),
        -- The static coding shall be used to report a static address.
        dynamic(2),
        -- The dynamic coding shall be used to report a dynamically allocated address.
        notKnown (3),
        -- The notKnown coding shall be used to report other then static or dynamically
        -- allocated IP addresses.
        ...
    } OPTIONAL,
    ...
}
```

```
IP-value ::= CHOICE
{
    iPBinaryAddress [1] OCTET STRING (SIZE(4..16)),
    iPTextAddress   [2] IA5String (SIZE(7..45)),
    ...
}
```

```
X25Address ::= OCTET STRING (SIZE(1..25))
```

```
END -- OF HI2Operations
```

D.6 User data packet transfer (HI3 interface)

Declaration of ROSE operations circuit-Call-related-Services and no-circuit-Call-related-Services are ROSE delivery mechanism specific. When using FTP delivery mechanism, data Content-Report must be considered.

ASN.1 description of circuit_data transfer operation (HI3 interface)

```
HI3CircuitDataOperations
{ itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi3 (2)
circuitLI (1) version2 (2)}

DEFINITIONS IMPLICIT TAGS ::=

--The following operations are used to transmit user data which can be exchanged via the DSS1, ISUP
--or MAP signalling (e.g. UUS, SMS)

BEGIN

IMPORTS OPERATION,
    ERROR
        FROM Remote-Operations-Information-Objects
        {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

    hi3CircuitLISubDomainId
        FROM
        SecurityDomainDefinitions
        { itu-t (0) identified-organization (4) etsi (0) securityDomain (2)}

    LawfulInterceptionIdentifier,
    CommunicationIdentifier,
    TimeStamp,
    OperationErrors,
    Supplementary-Services,
    SMS-report
        FROM
        HI2Operations
        { itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi2
(1) version2 (2)};
```

```
circuit-Call-related-Services   OPERATION ::=
{
    ARGUMENT    Content-Report
    ERRORS      { OperationErrors }
    CODE        global:{ hi3CircuitLISubDomainId circuit-Call-Serv (1) version1 (1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer default value is 60s.
-- NOTE: The same note as for HI management operation applies.
```

```
no-Circuit-Call-related-Services    OPERATION ::=
{
    ARGUMENT    Content-Report
    ERRORS      { OperationErrors }
    CODE        global:{ hi3CircuitLISubDomainId no-Circuit-Call-Serv (2) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 10s and 120s.
-- The timer default value is 60s.
```

```
Content-Report      ::= SEQUENCE
{
    lawfulInterceptionIdentifier    [6] LawfulInterceptionIdentifier OPTIONAL,
    communicationIdentifier         [1] CommunicationIdentifier,
        -- Used to uniquely identify an intercepted call: the same as used for the relevant IRI.
        -- Called CallIdentifier in edition 1 of the document.
    timeStamp                       [2] TimeStamp,
    initiator                       [3] ENUMERATED
    {
        originating-party(0),
        terminating-party(1),
        forwarded-to-party(2),
        undefined-party(3),
        ...
    } OPTIONAL,
    content                         [4] Supplementary-Services OPTIONAL,
        -- UUI are encoded in the format defined for the User-to-user information parameter
        -- of the ISUP protocol (see [5]). Only one UUI parameter is sent per message.
    sMS-report                      [5] SMS-report OPTIONAL,
    ...
}
```

```
END -- HI3CircuitDataOperations
```

D.7 TETRA data transfer (HI3 interface)

Not covered in the present document.

D.8 Definition of the UUS1 content associated to the CC link

ASN.1 description of the UUS1 content associated to the CC link

```
HI3CCLinkData
{ itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi3 (2)
cclinkLI (4) version2 (2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS
    LawfulInterceptionIdentifier,
    CommunicationIdentifier,
    CC-Link-Identifier
        FROM
        HI2Operations
        { itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi2
(1) version2 (2)};
```

```
UUS1-Content    ::= SEQUENCE
{
    lawfullInterceptionIdentifier   [1] LawfulInterceptionIdentifier,
    communicationIdentifier         [2] CommunicationIdentifier,
    cC-Link-Identifier              [3] CC-Link-Identifier OPTIONAL,
    direction-Indication            [4] Direction-Indication,
    bearer-capability               [5] OCTET STRING (SIZE(1..12)) OPTIONAL,
        -- transport the Bearer capability information element (value part)
        -- Protocol: ETS [6]
    service-Information             [7] Service-Information OPTIONAL,
    ...
}
```

```
Direction-Indication    ::= ENUMERATED
{
    mono-mode(0),
    cc-from-target(1),
    cc-from-other-party(2),
    ...
}
```

```
Service-Information ::= SET
{
    high-layer-capability   [0] OCTET STRING (SIZE(1)) OPTIONAL,
        -- HLC (octet 4 only)
        -- Protocol: ETS [6]
    tMR                     [1] OCTET STRING (SIZE(1)) OPTIONAL,
        -- Transmission Medium Required
        -- Protocol: ISUP [5]
    bearerServiceCode       [2] OCTET STRING (SIZE(1)) OPTIONAL,
    teleServiceCode         [3] OCTET STRING (SIZE(1)) OPTIONAL
        -- from MAP, ETS 300 974, clause 14.7.9 and clause 14.7.10
}
```

```
END -- HI3CCLinkData
```

Annex E (informative): Use of sub-address and calling party number to carry correlation information

E.1 Introduction

Not all ISDN networks fully support the use of the UUS1 service [11]. Some networks may be limited to the transfer of only 32 octets of UUS1 user information rather than the 128 required for full support of the UUS1 service. Some networks may not support UUS1 at all.

This annex describes a procedure to provide correlation information which is appropriate:

1) if a network does not support the delivery of UUS1; or

2) if a network does not support the delivery of 128 octets for UUS1.

If all network involved support the delivery of 128 octets for UUS1 then the procedure (described in this annex) is not appropriate.

The calling party number, the calling party subaddress (CgP Sub) and the called party subaddress (CdP Sub) are used to carry correlation information.

E.2 Subaddress options

The coding of a subaddress information element is given in [5]. The following options shall be chosen:

Table E.2.1: Subaddress options

Option	Value
Type of subaddress	user specified
Odd/even indicator	employed for called party subaddress when no national parameters are used

E.3 Subaddress coding

The coding of subaddress information shall be in accordance with [5].

E.3.1 BCD values

The values 0 to 9 shall be BCD coded according to their natural binary values. The hexadecimal value F shall be used as a field separator. This coding is indicated in table E.3.1.

Table E.3.1: Coding BCD values

Item	BCD representation			
	Bit 4	Bit 3	Bit 2	Bit 1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
Field separator	1	1	1	1

When items are packed two to an octet, the least significant item shall be coded by mapping bit 4 to bit 8, bit 3 to bit 7, etc.

E.3.2 Field order and layout

Fields shall be presented into the subaddress in the following order:

Table E.3.2: Fields in the called party subaddress

Order	Field
1	Operator-ID
2	CIN
3	CCLID
4	National Parameters

Table E.3.3: Fields in the calling party subaddress

Order	Field
1	Lawful Interception Identifier (LIID)
2	Direction
3	Service octets

Each field noted above shall be included, whether empty or not, and a field separator shall separate each field. When a field is empty, that shall be indicated by two consecutive field separators. There shall be a field separator after the final field, too.

The Service Octets as available shall always be mapped into octets 19 to 23 of the Calling Party Subaddress, as appropriate. If one of the parameters TMR, BC or HLC is not available, the octet shall be fill with "FF" hex. If Mobile Teleservice Code is not available, octet 23 shall not be transmitted. If Mobile Teleservice Code and Mobile Bearer Service Code are not available, octets 22 and 23 shall not be transmitted.

Table E.3.4 represents called party subaddress and table E.3.5 calling party subaddress with the maximum length of the identifiers.

Table E.3.4: Called party subaddress

Bits								Octets
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
Called party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
Operator-ID ②				Operator-ID ①				4
Operator-ID ④				Operator-ID ③				5
Field separator				Operator-ID ⑤				6
CIN ②				CIN ①				7
CIN ④				CIN ③				8
CIN ⑥				CIN ⑤				9
CIN ⑧				CIN ⑦				10
CCLID ①				Field separator				11
CCLID ③				CCLID ②				12
CCLID ⑤				CCLID ④				13
CCLID ⑦				CCLID ⑥				14
Field separator				CCLID ⑧				15
see note								16
								17
								18
								19
								20
								21
								22
								23
NOTE: The octets after the final field (CCLID) of the called party subaddress are reserved for national use, e.g. for authentication purposes.								

Table E.3.5: Calling party subaddress

Bits								Octets
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
Calling party subaddress identifier								1
Length of calling party subaddress contents								2
Type of subaddress = user specified, odd/even indicator according to the amount of BCD-digits								3
LIID ②				LIID ①				4
LIID ④				LIID ③				5
LIID ⑥				LIID ⑤				6
LIID ⑧				LIID ⑦				7
LIID ①⓪				LIID ⑨				8
LIID ①②				LIID ①①				9
LIID ①④				LIID ①③				10
LIID ①⑥				LIID ①⑤				11
LIID ①⑧				LIID ①⑦				12
LIID ②⓪				LIID ①⑨				13
LIID ②②				LIID ②①				14
LIID ②④				LIID ②③				15
Field separator				LIID ②⑤				16
Field separator				Direction				17
spare				spare				18
ITU-T Recommendation Q.763 [25] TMR (see note 1)								19
ITU-T Recommendation Q.931 BC [31] octet 3 (see note 2)								20
ITU-T Recommendation Q.931 HLC [31] octet 4 (see note 3)								21
Mobile Bearer Service Code (see note 4)								22
Mobile Teleservice Code (see note 5)								23
NOTE 1: If available, the Transmission Medium Requirement according to EN 300 356 [4]. If not available, the value is "FF" hex. NOTE 2: If available, only octet 3 of the Bearer Capability I.E. according to EN 300 403-1 [5] If not available, the value is "FF" hex. NOTE 3: If available, only octet 4 of the High Layer Compatibility I.E. according to EN 300 403-1 [5]. If not available, the value is "FF" hex. NOTE 4: If available, the Mobile Bearer Service Code according to ETS 300 974 [14], clause 14.7.10. If not available, the octets 22 and 23 shall not be transmitted. NOTE 5: If available, the Mobile Teleservice Code according to ETS 300 974 [14], clause 14.7.9. If not available, the octet 23 shall not be transmitted.								

E.4 Field coding

Each field shall employ decimal coding, except for the Service Octets (octets 19 to 23 of the CgP Sub) and the octets reserved for national use (octets 16 to 23 of the CdP Sub). Other values are not permitted.

E.4.1 Direction

The direction field shall be coded as follows:

Table E.4.1: Direction coding

Indication	Value
Mono mode (combined signal) (historic)	0
CC from target	1
CC to target	2

E.4.2 Coding of the calling party number

The Network Element Identifier (NEID) shall be carried by the calling party number information element. The coding shall be as follows, depending on the type of network access (see note 1):

Numbering plan identification: ISDN/telephony numbering plan (ITU-T Recommendation E.164 [32])

Nature of address: As specified in ITU-T Recommendation Q.731.3 [36] (see note 1) (e.g. national (significant) number or international number) (in case of ISUP signalling)

Type of number: As specified in ITU-T Recommendation Q.951 [37], EN 300 092 (e.g. unknown, subscriber number, national number or international number), and Network Operator specific type of access (BRA or PRA) (in case of DSS1 signalling, see notes 2 and 3)

Screening indicator: Network provided (in case ISUP signalling)

Screening indicator: User-provided, not screened (in case of DSS1 signalling, see note 3)

Presentation indicator: Presentation allowed

NOTE 1: The relevant national specification of the Signalling System Number 7 may also specify requirements on the Nature of address for national specific use in national variants of ISUP.

NOTE 2: Usually, the IIF respectively the Mediation Function is connected to the network by links using Signalling System Number 7 and ISDN User Part (ISUP), whereby the parameters are coded according to [4]. But in some cases, the IIF respectively the Mediation Function may be connected via a Basic Rate Access or a Primary Rate Access using D-Channel signalling, whereby the parameters are coded according to [5].

NOTE 3: The network will perform screening, i.e. the number will arrive at the LEMF as "user-provided, verified and passed" with the appropriate "type of number" indicator. A network provided number shall also be accepted at the LEMF.

E.5 Length of fields

The length of the identifiers is variable. The minimum and maximum length of each field shall be as given in table E.5.1.

Table E.5.1: Field length

Field	Minimum length (decimal digits)	Maximum length (decimal digits)	Maximum length (Half-octets)	i.e.
Operator ID	2	5	5 + 1	CdP Sub
CIN	6	8	8 + 1	CdP Sub
CCLID	1	8	8 + 1	CdP Sub
LIID	2	25	25 + 1	CgP Sub
Direction	1	1	1 + 1	CgP Sub
Service Octets			10	CgP Sub

Annex F (informative): GPRS HI3 Interface

F.1 Functional architecture

Figure F.1.1 contains the reference configuration for lawful interception (see TS 101 509 [21]).

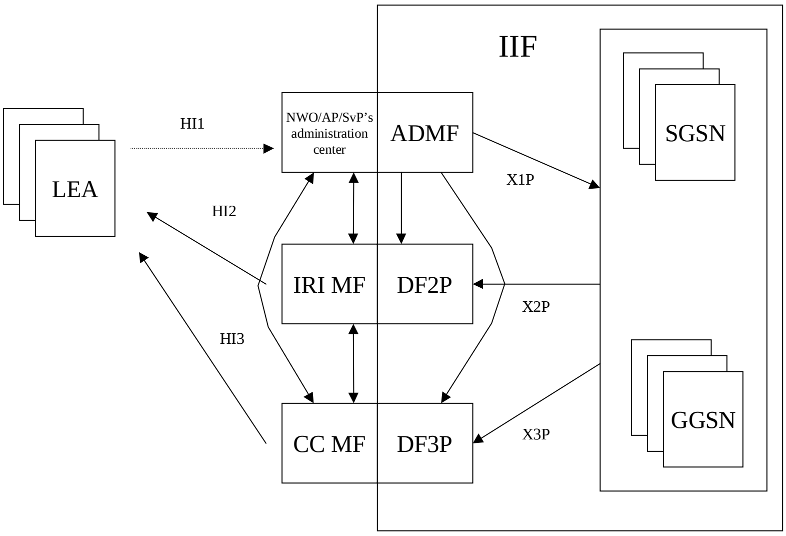


Figure F.1.1: Reference configuration

There is one Administration Function (ADMF) in the network. Together with the delivery functions it is used to hide from the xGSN that there might be multiple activations by different Law Enforcement Agencies (LEAs) on the same target.

NOTE: GGSN interception is a national option

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.

A call could be intercepted based on several identities (MSISDN, IMSI, IMEI) of the same target.

For the delivery of the CC and IRI the xGSN provides a correlation number and target identity to the DF2P and DF3P which is used there to select the different LEAs where CC/IRI shall be delivered to.

F.2 Correlation

Correlation of GSM ID's of TS 101 509 [21] to the present document ID's

Warrant reference number	→	Lawful interception identifier (LIID)
xGSN address	→	Network identifier (NID)

F.3 HI3 Delivery Content of Communication (CC)

There are two possible methods for delivery of Content of Communication to the LEMF:

- GPRS LI correlation header and UDP/TCP (see clause F.3.1);
- FTP (see clause F.3.2).

According to national requirements al least one of these methods have to be provided.

F.3.1 GPRS LI correlation header

F.3.1.1 Introduction

The header and the payload of the communication between the intercepted subscriber and the other party (later called: Information Element) are duplicated. A new header (later called: GLIC-Header, see table F.3.1) is added (see table F.3.3) before it is sent to LEMF.

Data packets with the GLIC header shall be sent to the LEA via UDP or TCP/IP.

F.3.1.2 Definition of GLIC header

GLIC header contains the following attributes:

- Correlation number;
- Message type (a value of 255 is used for HI3-PDU's);
- Direction;
- Sequence Number;
- Length.

T-PDU contains the intercepted information.

Table F.3.1: Outline of GLIC header

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Version ("0 0 0")			"1"	Spare "1 1"		DIR	"0"
2	Message Type (value 255)							
3-4	Length							
5-6	Sequence Number							
7-8	not used (value 0)							
9	not used (value 255)							
10	not used (value 255)							
11	not used (value 255)							
12	not used (value 255)							
13-20	correlation number							

- For interception tunnelling the GLIC header shall be used as follows;
- Version shall be set to 0 to indicate the first version of GLIC header;
- DIR indicates the direction of the T-PDU:
  - "1" indicating uplink (from observed mobile user); and
  - "0" indicating downlink (to observed mobile user).
- Message type shall be set to 255 (the unique value that is used for T-PDU within GTP [23]);

- Length shall be the length, in octets, of the signalling message excluding the GLIC header. Bit 8 of octet 3 is the most significant bit and bit 1 of octet 4 is the least significant bit of the length field;

- Sequence number is an increasing sequence number for tunnelled T-PDUs. Bit 8 of octet 5 is the most significant bit and bit 1 of octet 6 is the least significant bit of the sequence number field;

- Correlation number consists of two parts: GGSN-ID identifies the GGSN which creates the Charging-ID:

  - Charging-ID is defined in [23] and assigned uniquely to each PDP context activation on that GGSN (4 octets);

  - The correlation number consist of 8 octets and guarantees a unique identification of the tunnel to the LEA over a long time. The requirements for this identification are similar to that defined for charging in [23], clause 5.4. Therefore it is proposed to use the Charging-ID, defined in [23], clause 5.4 as part of correlation number. The Charging-ID is signalled to the new SGSN in case of SGSN-change so the tunnel identifier could be used "seamlessly" for the HI3 interface.

Table F.3.2: Outline of correlation number

0										1										2										3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
Charging-ID Octet 1								Charging-ID Octet 2								Charging-ID Octet 3								Charging-ID Octet 4								Octet 13 to 16
GGSN-ID																																Octet 17 to 20

The GLIC header is followed by a subsequent payload information element. Only one information element is allowed in a single signalling message.

Table F.3.3: GLIC header followed by the subsequent payload Information Element

	Bits							
Octets	8	7	6	5	4	3	2	1
1- 20	GLIC- Header							
21- n	Information Element							

The Information Element contains the header and the payload of the communication between the intercepted subscriber and the other party.

F.3.1.3 Exceptional procedure

With UDP and GLIC: the delivering node does not take care about any problems at LEMF.

With TCP and GLIC: TCP tries to establish a connection to LEMF and resending (buffering in the sending node) of packets is also supported by TCP.

In both cases it might happen that call content gets lost (in case the LEMF or the transit network between MF and LEMF is down for a long time).

F.3.1.4 Other considerations

The use of IPsec for this interface is recommended.

The required functions in LEMF are:

- Collecting and storing of the incoming packets inline with the sequence numbers.

- Correlating of CC to IRI with the use of the correlation number in the GLIC header.

F.3.2 FTP

F.3.2.1 Introduction

At HI3 interface FTP is used over the internet protocol stack for the delivery of the result of interception. FTP is defined in [24]. The IP is defined in [27]. The TCP is defined in [28].

FTP supports reliable delivery of data. The data may be temporarily buffered in the sending node (MF) in case of link failure. FTP is independent of the payload data it carries.

F.3.2.2 Usage of the FTP

In the packet data LI the MF acts as the FTP client and the receiving node (LEMF) acts as the FTP server. The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The sending entity (MF) may buffer files.

Several smaller intercepted data units may be gathered to bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing/file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms;
- frequency of transfer, based on volume trigger, e.g. X octets.

There are two possible ways how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (ref: "File naming method A)"). The other way is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (ref: "File naming method B)").

The HI2 and HI3 are logically different interfaces, even though in some installations the HI2 and HI3 packet streams might also be delivered via a common transmission path from a MF to a LEMF. It is possible to correlate HI2 and HI3 packet streams by having common (referencing) data fields embedded in the IRI and the CC packet streams.

File naming:

The names for the files transferred to a LEA are formed according to one of the 2 available formats, depending on the delivery file strategy chosen (e.g. due to national convention or operator preference).

Either each file contains data of only one observed target (as in method A) or several targets' data is put to files common to all observed target traffic through a particular MF node (as in method B).

The maximum set of allowed characters in interception file names are "a"…"z", "A"…"Z", "-", "_", ".", and decimals "0"…"9".

File naming method A):

<LIID>_<seq>.<ext>

LIID = as defined in the present document. This field has a character string value, e.g. "ABCD123456". This is a unique interception request identifier allocated by the ADMF. It will be given by the ADMF to the LEA via the HI1 interface after the ADMF has been authorized to command the start of the interception of a specific target. The possible network operator identifier part used should be agreed with (and allocated by) the regulatory organization administrating the local telecommunication practises.

Seq = integer ranging between [0..2^64-1], in ASCII form (not exceeding 20 ASCII digits), identifying the sequence number for file transfer from this node per a specific target.

Ext = ASCII integer ranging between ["1"..."7"] (in hex: 31H…37H), identifying the file type. The possible file type codings for intercepted data are shown in table F.3.4. But for the HI3 interface, only the types "2", "4", and "6" are possible.

Table F.3.4: Possible file types

File types that the LEA may get	Intercepted data types
"2" (in binary: 0011 0010)	CC (MO)
"4" (in binary: 0011 0100)	CC (MT)
"6" (in binary: 0011 0110)	CC (MO&MT)

(The least significant bit that is "1" in file type 1, is reserved for indicating IRI data.) The bit 2 of the **ext** tells whether the Mobile Originated (MO) Content of Communication (CC) is included to the intercepted data.

The bit 2 of the **ext** tells whether the Mobile Originated (MO) Content of Communication (CC) is included to the intercepted data.

The bit 3 of the **ext** tells whether the Mobile Terminated (MT) Content of Communication (CC) is included to the intercepted data.

Thus, for Mobile Originated Content of Communication data, the file type is "2", for MT CC data "4" and for MO&MT CC data "6".

This alternative A is used when each target's intercepted data is gathered per observed target to dedicated delivery files. This method provides the result of interception in a very refined form to the LEAs, but requires somewhat more resources in the sending node than alternative B. With this method, the data sorting and interpretation tasks of the LEMF are considerably easier to facilitate in near real time than in alternative B.

File naming method B):

The other choice is to use monolithic fixed format file names (with no trailing file type part in the file name):

<filenamestring> of the format ABXYyymmddhhmmsseeeet

where

AB = Two letter ASCII Operator ID (as agreed with the national telecom regulators).
XY = Two letter ASCII identification of the MF node (as assigned by the operator).
yy = Two digits ASCII integer ranging between ["00"..."99"], identifying the last to digits of the year.
mm = Two digits ASCII integer ranging between ["01"..."12"], identifying the month.
dd = Two digits ASCII integer ranging between ["01"..."31"], identifying the day.
hh = Two digits ASCII integer ranging between ["00"..."23"], identifying the hour.
mm = Two digits ASCII integer ranging between ["00"..."59"], identifying the minute.
ss = Two digits ASCII integer ranging between ["00"..."59"], identifying the second.
eeee = Alphanumeric extension made up of four characters chosen at the discretion of the Operator and/or the MF to avoid file name clashes within the MF. Each of the position shall be out of 'A'....'Z', '0'....'9'.
t = ASCII integer ranging between ["1"..."7"] (in hex: 31H…37H), identifying the file type. The possible file type codings for intercepted data are shown in table F.3.4.

EXAMPLE:

<filenamestring> (e.g. ABXY00041014084400006)

where:

ABXY = Source node identifier part, used for all files by the mobile network operator "AB" from this MF node named "XY".
00 = year 2000
04 = month April
10 = day 10
14 = hour
08 = minutes
44 = seconds
0000 = extension
6 = file type. Coding: "2" = CC (MO), "4" = CC (MT), "6" = CC (MO&MT).
(The type "1" is reserved for IRI data files).

This alternative B is used when several targets' intercepted data is gathered to common delivery files. This method does not provide the result of interception in as refined form to the LEAs as the alternative A, but it is faster in performance for the MF point of view. With this method, the MF does not need to keep many files open like in alternative A.

F.3.2.3 Exceptional procedures

Overflow at the receiving end (LEMF) is avoided due to the nature of the protocol.

In case the transit network or receiving end system (LEMF) is down for a reasonably short time period, the local buffering at the MF will be sufficient as a delivery reliability backup procedure.

In case the transit network or receiving end system (LEMF) is down for a very long period, the local buffering at the MF may have to be terminated. Then the following intercepted data coming from the intercepting nodes towards the MF would be discarded, until the transit network or LEMF is up and running again.

F.3.2.4 CC contents for FTP

F.3.2.4.1 Fields

The logical contents of the CC-header are described here.

CC-header = (Version, HeaderLength, PayloadLength, PayloadType, PayloadTimeStamp, PayloadDirection, CCSeqNumber, CorrelationNumber, LIID, PrivateExtension).

The Information Element CorrelationNumber forms the means to correlate the IRI and CC of the communication session intercepted.

The first column indicates whether the Information Element referred is Mandatory, Conditional or Optional.

The second column is the Type in decimal.

The third column is the length of the Value in octets.

(Notation used in table F.3.5: M = Mandatory, O = Optional, C = Conditional.)

Table F.3.5: Information elements in the fist version of the CC header

Mode	Type	Length	Value
M	130	2	**Version** = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.
O	131	2	**HeaderLength** = Length of the CC-header up to the start of the payload in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
O	132	2	**PayloadLength** = Length of the payload following the CC-header. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
M	133	1	**PayloadType** = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards, e.g. TS 101 347 [23]. The value 255 is reserved for future PDP Types and means: "Other".
O	134	4	**PayloadTimeStamp** = Payload timestamp according to intercepting node. (Precision: 1 s, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).
C	137	1	**PayloadDirection** = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (i.e. downstream), or 1 if the payload data is being sent from the target (i.e. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.
O	141	4	**CCSeqNumber** = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.
M	144	8 or 20	**CorrelationNumber** = Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see [26]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.
			<Possible future parameters are to be allocated between 145 and 253>.
O	254	1 to 25	**LIID** = Field indicating the LIID as defined in the present document. This field has a character string value, e.g. "ABCD123456".
O	255	1 to N	**PrivateExtension** = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document TS 101 347 [23].

Table F.3.6: Information elements in the second version of the CC header

Mode	Type	Length	Value
M	130	2	**Version** = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.
O	131	2	**HeaderLength** = Length of the CC-header up to the start of the payload in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
O	132	2	**PayloadLength** = Length of the payload following the CC-header in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
M	133	1	**PayloadType** = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards (e.g.TS 129 060 [33]). The value 255 is reserved for future PDP Types and means: "Other".
O	134	4	**PayloadTimeStamp** = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).
C	137	1	**PayloadDirection** = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (i.e. downstream), or 1 if the payload data is being sent from the target (i.e. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.
O	141	4	**CCSeqNumber** = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.
M	144	8 or 20	**CorrelationNumber** = Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see [7]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.
			<Possible future parameters are to be allocated between 145 and 250.>
M	251	2	**MainElementID** = Identifier for the TLV element that encompasses one or more HeaderElement-PayloadElement pairs for intercepted packets.
M	252	2	**HeaderElementID** = Identifier for the TLV element that encompasses the CC-header of a PayloadElement.
M	253	2	**PayloadElementID** = Identifier for the TLV element that encompasses one intercepted Payload packet.
O	254	1-25	**LIID** = Field indicating the LIID as defined in the present document. This field has a character string value, e.g. "ABCD123456".
O	255	1-N	**PrivateExtension** = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document TS 129 060 [33].

F.3.2.4.2 Information element syntax

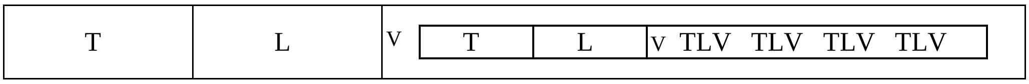
The dynamic TypeLengthValue (TLV) format is used for its ease of implementation and good encoding and decoding performance. Subfield sizes: Type = 2 octets, Length = 2 octets and Value = 0…N octets. From Length the T and L subfields are excluded. The Type is different for every different field standardized.

The octets in the Type and Length subfields are ordered in the little-endian order, (i.e. least significant octet first). Any multioctet Value subfield is also to be interpreted as being little-endian ordered (word/double word/long word) when it has a (hexadecimal 2/4/8-octet) numeric value, instead of being specified to have an ASCII character string value. This means that the least significant octet/word/double word is then sent before the more significant octet/word/double word.

TLV encoding:

Type (2 octets)	Length (2 octets)	Value (0-N octets)

TLV encoding can always be applied in a nested fashion for structured values.



NOTE: The small "v" refers to the start of a Value field that has inside it a nested structure.

In the following figure the TLV structure for GPRS HI3 transfer is presented for the case that there is just one intercepted packet inside the CC message. (There can be more CC Header IEs and CC Payload IEs in the CC, if there are more intercepted packets in the same CC message.)

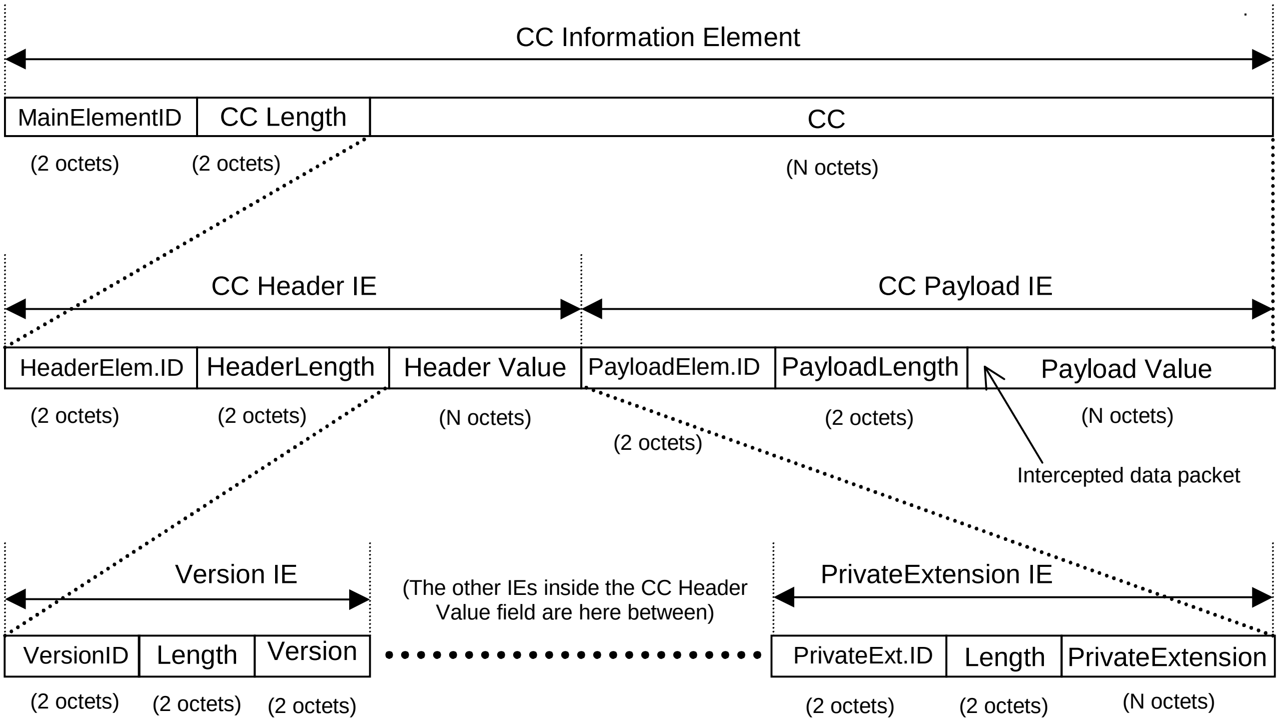


Figure F.3.1: IE structure of a CC message that contains one intercepted packet

The first octet of the first TLV element will start right after the last octet of the header of the protocol that is being used to carry the CC information.

The first TLV element (i.e. the main TLV IE) comprises the whole dynamic length CC information, i.e. the dynamic length CC header and the dynamic length CC payload.

Inside the main TLV IE there are at least 2 TLV elements: the header of the payload and the payload itself. The header contains all the ancillary IEs related to the intercepted CC packet. The Payload contains the actual intercepted packet.

There may be more than one intercepted packet in one GPRS HI3 delivery protocol message. If the Value of the main TLV IE is longer than the 2 (first) TLV Information Elements inside it, then it is an indication that there are more than one intercepted packets inside the main TLV IE (i.e. 4 or more TLV IEs in total). The number of TLV IEs in the main TLV IE is always even, since for every intercepted packet there is one TLV IE for header and one TLV IE for payload.

F.3.2.5 Other considerations

The FTP protocol mode parameters used:

- Transmission Mode: stream;
- Format: non-print;
- Structure: file-structure;
- Type: binary.

The FTP service command to define the file system function at the server side: STORE mode for data transmission.

The FTP client- (= user - FTP process at the MF) uses e.g. the default standard FTP ports 20 (for data connection) and 21 (for control connection), "passive" mode is supported. The data transfer process listens the data port for a connection from a server-FTP process.

For the file transfer from the MF to the LEMF(s) e.g. the following data transfer parameters are provided for the FTP client (at the MF):

- transfer destination (IP) address, e.g. "194.89.205.4";
- transfer destination username, e.g. "LEA1";
- transfer destination directory path, e.g. "/usr/local/LEA1/1234-8291";
- transfer destination password;
- interception file type, e.g. "2" (this is needed only if the file naming method A is used).

LEMF may use various kind directory structures for the reception of interception files. It is strongly recommended that at the LEMF machine the structure and access and modification rights of the storage directories are adjusted to prevent unwanted directory operations by a FTP client.

The use of IPSec services for this interface is recommended.

Timing considerations for the FTP transmission:

The MF and LEMF sides control the timers to ensure reliable, near-real time data transfer. The transmission related timers are defined within the lower layers of the used protocol and are out of scope of the present document.

The following timers may be used within the LI application:

Name	Controlled by	Units	Description
T1 inactivity timer	LEMF	s	Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side.
T2 send file trigger	MF	ms	Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (see clause C.2.2).

Annex G (informative): LEMF requirements - handling of unrecognized fields and parameters

During decoding of a record at the LEA, the following exceptional situations may occur:

1) Unrecognized parameter: The parameter layout can be recognized, but its name is not recognized:
The parameter shall be ignored, the processing of the record proceeds.

2) The parameter content or value is not recognized or not allowed:
The parameter shall be ignored, the processing of the record proceeds.

3) The record cannot be decoded (e.g. it seems to be corrupted):
The whole record shall be rejected when using ROSE delivery mechanism or ignored.

NOTE: In cases 2 and 3, the LEMF may wish to raise an alarm to the NWO/AP/SvP administration centre. For case 1, no special error or alarm procedures need be started at the LEA, because the reason may be the introduction of a new version of the specification in the network, not be an error as such security aspects.

Annex H (informative): Bibliography

- ETSI ETS 300 121: "Integrated Services Digital Network (ISDN); Application of the ISDN User Part (ISUP) of ITU-T Signalling System No.7 for international ISDN interconnections (ISUP version 1)".
- ETSI EN 300 052-1: "Integrated Services Digital Network (ISDN); Multiple Subscriber Number (MSN) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 055-1: "Integrated Services Digital Network (ISDN); Terminal Portability (TP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 058-1: "Integrated Services Digital Network (ISDN); Call Waiting (CW) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 064-1: "Integrated Services Digital Network (ISDN); Direct Dialling In (DDI) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 092-1 including Amendment 2: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 093-1: "Integrated Services Digital Network (ISDN); Calling Line Identification Restriction (CLIR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 141-1: "Integrated Services Digital Network (ISDN); Call Hold (HOLD) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 210-1: "Integrated Services Digital Network (ISDN); Freephone (FPH) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 359-1: "Integrated Services Digital Network (ISDN); Completion of Calls to Busy Subscriber (CCBS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 300 745-1: "Integrated Services Digital Network (ISDN); Message Waiting Indication (MWI) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 301 001-1 (V1.2.2): "Integrated Services Digital Network (ISDN); Outgoing Call Barring (OCB) supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ETSI EN 301 065-1 (V1.2.2): "Integrated Services Digital Network (ISDN); Completion of Calls on No Reply (CCNR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification"
- ITU-T Recommendation Q.699: "Interworking between ISDN access and non-ISDN access over ISDN User Part of Signalling System No. 7".
- ITU-T Recommendation I.210: "Principles of telecommunication services supported by an ISDN and the means to describe them".
- ISO 9798 (all parts): "Information technology - Security techniques - Entity authentication".
- ETSI EN 300 130-1: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

- ETSI EN 300 207-1 (V1.2.5): "Integrated Services Digital Network (ISDN); Diversion supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ITU-T Recommendation Q.850: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".
- ETSI ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".
- 3GPP TS 24.008: "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile radio interface Layer 3 specification".
- ETSI EN 301 344: "Digital cellular telecommunications system (Phase 2+) (GSM); General Packet Radio Service (GPRS); Service description; Stage 2 (GSM 03.60)".
- IETF RFC 2228: "FTP Security Extensions".
- ETSI TS 101 109: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Geographical Area Description (GAD) (GSM 03.32)".
- IETF RFC 2543: "SIP: Session Initiation Protocol"; M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg; March 1999.

Annex I (informative): Change Request History

Status of Technical Specification 101 671 Handover interface for the lawful interception of telecommunications traffic		
Date	**Version**	**Remarks**
July 2001	1.1.1	TS version of ES 201 671 v2.1.1 NOTE: The version of the TS should also have been v2.1.1 (PvdA).
December 2001	2.2.1	Included Change Requests: TS10167CR001 (category D) on Removal of reference to TR 101 876 TS10167CR002 rev1 (category D) on Example on missing information TS10167CR003 (category D) on Sending of IRI-END and IRI-CONTINUE records TS10167CR004 (category D) on Moving GPRS related text from main body to annex B TS10167CR005 rev1 (category F) on No additional work on HI1 interface port for administrative state TS10167CR006 rev1 (category F) on Version indication TS10167CR007 rev1 (category F) on No additional identifiers for Packet switched network handover TS10167CR008 rev2 (category D) on Several editorials TS10167CR009 (category F) on UUS1-parameter no. 6: "bearer capability of target call" TS10167CR010 rev1 (category D) on Modification of the definition "CC link" TS10167CR011 (category D) on Modification of the definition "internal network interface": change "mediation device" into "mediation function" TS10167CR013 (category D) on Deletion of the definition "mediation device" all CRs approved by SEC-LI#31 (27-29 November 2001; Wien) version 2.2.1 prepared by Peter van der Arend (KPN) (rapporteur)
April 2002	2.3.1	Included Change Requests: TS10167CR014 rev 2 (cat F) on Annex E, Coding of the Calling Party Number TS10167CR015 rev 2 (cat F) on Annex D.5 Coordinates TS10167CR016 (cat C) on Annex D.5 - Exports Capabilities TS10167CR017 rev 1 (cat D) on Annex C.2.2 - File naming method B; Annex F.3.2.2 - File naming method B TS10167CR018 rev 1 (cat C) on Annex D.5 - TimeStamp TS10167CR019 (cat F) on Correction of superfluous spaces in ASN.1 coding TS10167CR021 (cat D) on Reintroduction of deleted references TS10167CR022 rev 2 (cat F) on Aligning ETSI TS 101 671 with 3GPP TS 33.108 TS10167CR025 (cat F) on Correction of Misalignment between the text and the ASN.1 all CRs approved by SEC-LI#32 (19-21 March 2002,Sophia Antipolis) version 2.3.1 prepared by Peter van der Arend (KPN) (rapporteur)
June 2002	2.4.1	Included Change Requests: TS10167CR026 (cat F) on Correcting "ccitt" into "itu-t" in ASN.1 Object Tree TS10167CR027 rev 1 (cat C) on Missing ISUP parameter in version 1 TS10167CR028 rev 1 (cat B) on Use of the object identifier within the IRI TS10167CR030 rev 1 (cat B) on Extension / alignment of ASN.1 module with 33.108 TS10167CR031 (cat F) on Missing/old reference TS10167CR032 rev 2 (cat B) on ASN.1 alignment with the UMTS module TS10167CR033 (cat B) on Adding a graphical ASN.1- Object tree all CRs approved by SEC-LI#33 (18-20 June 2002,Sophia Antipolis); version 2.4.1 prepared by Peter van der Arend (KPN) (rapporteur)

History

Document history		
V1.1.1	July 2001	Publication
V2.5.0	November 2002	Publication