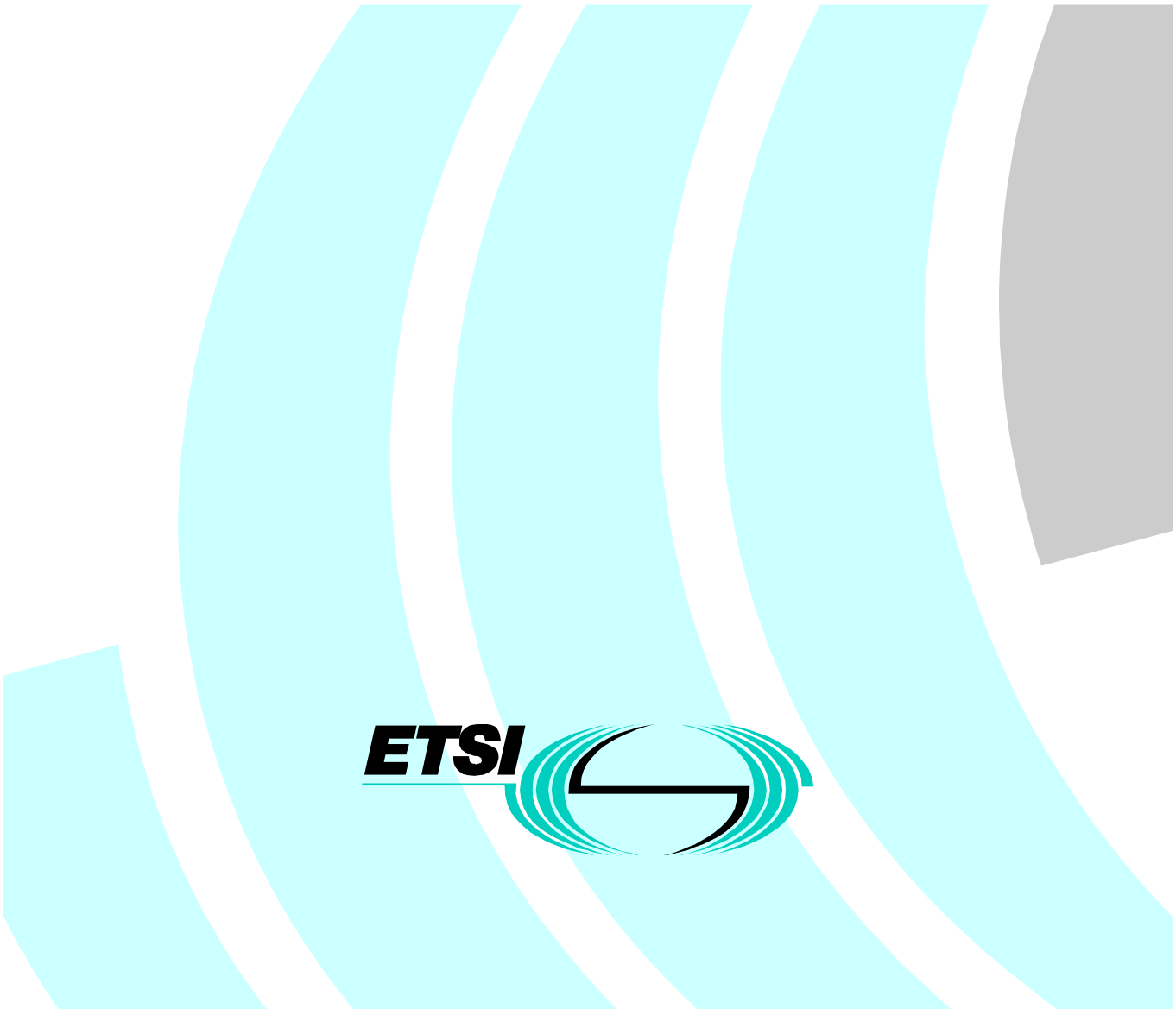
ES 201 158 V1.1.2 (1998-05)

ETSI Standard

Telecommunications security; Lawful Interception (LI); Requirements for network functions



Reference
DES/SEC-002311 (aq000idd.PDF)

Keywords
ISDN, multimedia, security

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet
secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

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 ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI Interim 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 ETR 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Security (SEC).

1 Scope

The present document describes the general requirements of Network Operators (NWOs), Service Providers (SPs) and Access Providers (APs) relating to the provision of lawful interception, with particular reference to the Handover Interface (HI). The provision of lawful interception is a requirement of national law, which is usually mandatory. From time to time, a NWO and/or SP will be required, according to a lawful authorization, to make available results of interception, relating to specific identities, to a specific Law Enforcement Agency (LEA).

The HI described in the present document is to be applied for every network technique, present or future, as long as the intercept requirements can be satisfied.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, subsequent revisions do apply.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETR 331: "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[2] Official Journal of the European Communities, 96/C 329/01: "Council resolution of 17 January 1995 on the lawful interception of telecommunications".

[3] GSM TS 02.33: "Digital cellular telecommunications system (Phase 2+); Lawful interception - stage 1 (GSM 02.33)".

[4] ETR 363: "Digital cellular telecommunications system; Lawful Interception requirements for GSM (GSM 10.20 version 5.0.1)".

[5] GSM TS 03.33: "Digital cellular telecommunications system (Phase 2+); Lawful interception - stage 2 (GSM 03.33)".

[6] ETR 279: "Satellite Personal Communications Networks (S-PCN); Need and objectives for standards in addition to the ETSs on essential requirements".

[7] EG 201 057: "Telecommunications Security; Trusted Third Parties (TTP); Requirements for TTP services".

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

3 Definitions, symbols and abbreviations

3.1 Definitions

The present document adopts the definitions of ETR 331 [1], which are reproduced in the list below as required, and defines further as necessary:

Access Provider (AP): An AP provides a user of some network with access from the user's terminal to that network.

NOTE 1: This definition applies specifically for the present document. In a particular case, the AP and Network Operator (NWO) may be a common commercial entity.

NOTE 2: The definitions from ETR 331 [1] have been expanded to include reference to an AP, where appropriate.

(to) buffer: The temporary storing of information in case the necessary telecommunication connection to transport information to the Law Enforcement Monitoring Facility (LEMF) is temporarily unavailable.

call: Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system. In this context a user may be a person or a machine.

content of communication: The information exchanged between two or more users of a telecommunications service, excluding Intercept Related Information (IRI). This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Handover Interface (HI): A physical and logical interface across which the results of interception are delivered from an AP/NWO/SP to a LEMF.

identity: A 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.

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

interception (lawful interception): The action (based on the law), performed by an AP/NWO/SP, of making available certain information and providing that information to a LEMF.

NOTE 3: In the present document, the term **interception** is not used to describe the action of observing communications by a LEA (see below).

interception interface: The physical and logical locations within the AP's/NWO's/SP's telecommunications facilities where access to the content of communication and IRI is provided. The interception interface is not necessarily a single, fixed point.

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

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

Internal Intercepting Function (IIF): A point within a network or network element at which the content of communication is made available.

Internal Network Interface (INI): The network's internal interface between the IIF and a mediation device.

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

Law Enforcement Monitoring Facility (LEMF): A law enforcement facility 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 AP/NWO/SP. Typically this refers to a warrant or order issued by a lawfully authorized body.

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

mediation device: A mechanism which passes information between an AP or NWO or SP and a HI.

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

Network Operator (NWO): The 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): The quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. 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: The 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 IRI, which is passed by an AP or NWO or SP to a LEA. IRI 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. The information may be established by an AP, NWO, a SP or a network user.

Service Provider (SvP): The natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routeing of signals on a telecommunications network. A SvP need not necessarily run his own network.

target identity: The identity associated with a target service (see below) used by the interception subject.

target identification: The identity which relates to a specific lawful authorization as such. This might be a serial number or similar. It is not related to the denoted interception subject or subjects.

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

NOTE 4: 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

The present document adopts the abbreviations of ETR 331 [1], which are reproduced in the list below as required, and uses further abbreviations as necessary:

AP	Access Provider
BC	Bearer Capability
DSS1	Digital Signalling System No.1
GSM	Global System for Mobile communications
HLC	Higher Layer Compatibility information
HI	Handover Interface
IIF	Internal Intercepting Function
IN	Intelligent Network
INI	Internal Network Interface
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part of ITU-T signalling system No.7

ITI	Interception Target Identity
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LLC	Lower Layer Compatibility information
NWO	Network Operator
PLMN	Public Land Mobile Network
PSPDN	Packet Switched Public Data Network
QoS	Quality of Service
SCP	Service Control Point
SMS	(GSM) Short Message Service
SSP	Service Switching Point
SvP	Service Provider
TCP-IP	Transmission Control Protocol - Internet Protocol
TE	Test Equipment
TTI	Test Target Identity
TTP	Trusted Third Party
UPT	Universal Personal Telecommunications
UUS	User-to-User Signalling

4 General requirements

The present document focuses on the HI between an AP and/or a NWO and/or a Service Provider (SvP) and a LEA.

4.1 Basic principles for the HI

The network requirements mentioned in the present document are derived, in part, from the requirements of LEAs regarding the HI for the interception of telecommunications, ETR 331 [1]. There are other requirements which relate to the operation of commercial telecommunications systems. Together, these requirements will be used to standardize HIs for specific telecommunications systems.

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

NOTE: The interface is intended to be extensible and will be extended in future. The LEMF needs to be able to handle changes, such as new data elements, cleanly.

4.2 Legal requirements

It shall be possible to configure the HI to:

- conform to national requirements;
- conform with national law;
- conform with the law applicable to a specific LEA.

Further information is given in ETR 331 [1] and ETR 330 [8].

4.3 Example of typical functional role model and process

The functional role model described in this subclause is a reference example to allow the typical procedural operation of interception, and the typical responsibilities of the various players, readily to be understood. In relation to a particular country national laws and procedures will apply.

4.3.1 Overview

There are various aspects of interception.

There is the national law that describes under what conditions and with what restrictions interception is allowed.

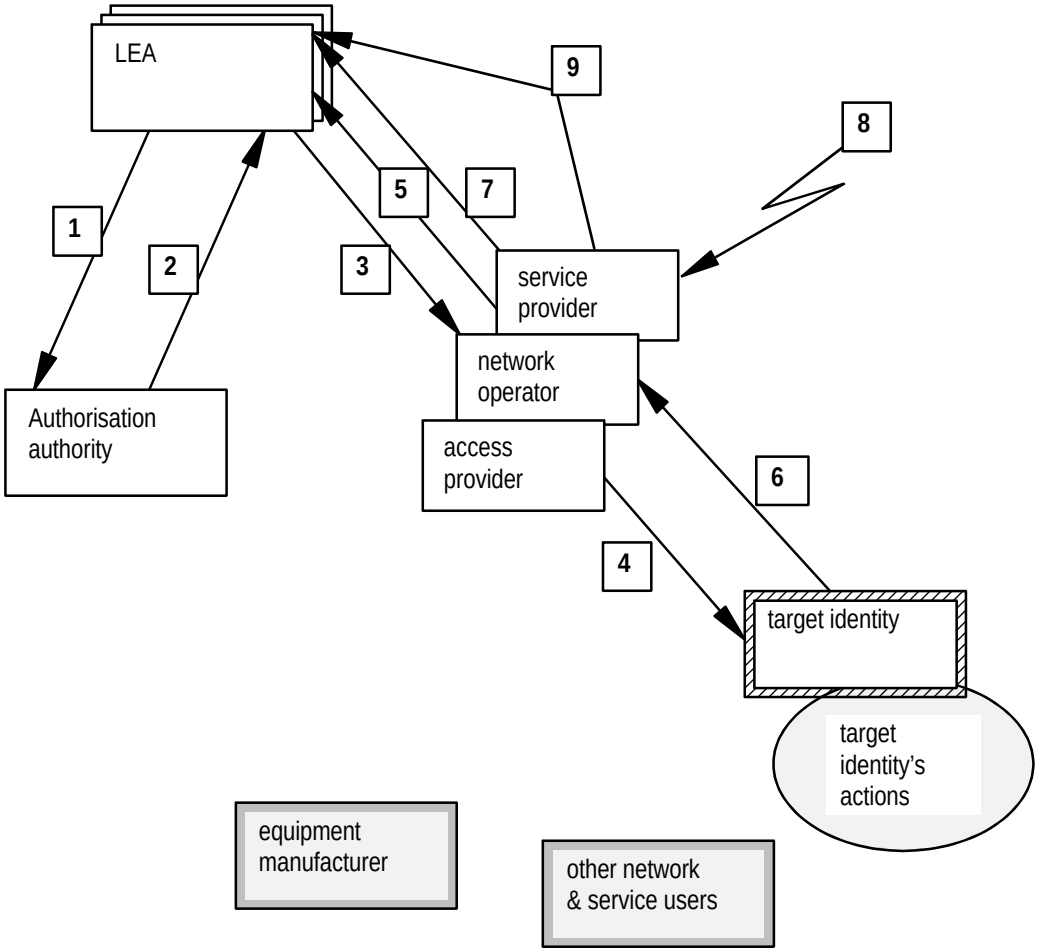
If a LEA wishes to use lawful interception as a tool that LEA will ask a prosecuting judge or other responsible body for a lawful authorization, such as a warrant. If the lawful authorization is granted the LEA will present the lawful authorization to the AP, NWO, SvP or AP via an administrative interface or procedure (interface port HI1).

When lawful interception is authorized the IRI and the content of communication is delivered to the LEMF (interface ports HI2 and HI3) of a LEA.

A lawful authorization may describe the IRI and the content of the communication that are allowed to be delivered for this LEA, investigation, period and interception subject. For different LEA's and for different investigations different constraints can apply that further limit the general borders set by the law. The interception subject may also be described in different ways in a lawful authorization (e.g. subscriber address, physical address, services etc.).

A lawful authorization or multiple lawful authorizations will be issued to one or more APs, NWOs and/or SvPs . This will depend on the subscribed services and on the networks which could be used by the interception subject.

A single interception subject may be the subject of interception of different LEA's and different investigations. It might be necessary to strictly separate these investigations and LEA's. It is therefore possible that more than one lawful authority (each based on a specific application for lawful authority) may be issued relating to the same interception subject. These various lawful interceptions might contain different constraints on the IRI and the content of communication. These various lawful interceptions could fall under different laws.



NOTE: The numbered lines relate to actions described in subclause 4.3.3 and table 2.

The law may require that checks and audits are possible. Therefore there should be facilities at the AP, NWO, SvP, and/or LEA that make such required checks and audits possible.

Figure 1: Functional role model

4.3.2 Players

The players in the functional role model are given in table 1.

Table 1: Players in the role model

Player	Role
Authorization authority	A judicial or administrative (etc.) authority. It gives the LEA the lawful authorization to intercept an interception subject.
LEA	The LEA requests NWOs (and also SvPs and APs) to intercept communications according to a lawful authorization. The LEA receives, through a LEMF, the result of interception (the content of communications and IRI) relating to a target identity. Several LEAs may request the interception of the same target identity at the same time.
NWO	A NWO operates the basic switched telecommunication network on which services are connected. The operator is responsible for providing interception to the LEAs via the HI. Several NWOs might be involved in interception with the same LEAs (see note).
SvP	A SvP provides services, additional to those provided by any network itself, to users of a network. A SvP may use and administer various (target) identities which are, of themselves, unknown to the network. The SvP is responsible for making arrangements, which may involve a NWO, for the lawful interception of communications. A SvP may be the same organization as the NWO. Interception may be required for several SvPs using the same telecommunication network. See also ETR 331 [1], clause A.2.
Access provider	The AP provides a user of the network with access from the user's terminal to the network. The AP may be the same organization as the NWO. Several APs may provide access to the same network.
Target identity	the target identity corresponds to the identity of a given interception subject which is a user of a given service offered by an AP, NWO or SvP. Neither the interception subject nor the other parties involved in his communications should be able to detect that interception is taking place.
Other network and service users	When an interception facility is set up, or interception is taking place in a network for some service, no other users of any telecommunications service should be able, by any means, to detect that any interception facility has been added or removed, or that interception is taking place. The communications of other network or service users shall not be intercepted unless those communications involve a target identity.
Manufacturers	Manufacturers provide equipment which is deployed and operated by APs, NWOs and SvPs. Pieces of equipment from different manufacturers may be integrated in a common telecommunications infrastructure.
NOTE: According to this definition, a provider of Transmission Control Protocol - Internet Protocol (TCP-IP) connectivity (or similar facilities) is to be considered to be a NWO.	

4.3.3 Process

The process as described in this subclause stands as an example. In a specific country, the national process will be based on various national laws and circumstances.

The Authorization authority requires, through the LEA, the interception of the interception subject when the latter uses a service via the telecommunication network. The LEA receives the communications involving the target identity(ies) which the AP, NWO, or SvP singly or severally have associated with the interception subject.

Referring to the functional role model, and assuming that the lawful authorization is to be given to an AP, NWO, or SvP, actions are shown in table 2.

Table 2: Functional role model process actions

Reference (figure 1)	Action
1	A LEA requests lawful authorization from an authorization authority, which may be a court of law
2	The authorization authority issues a lawful authorization to the LEA
3	The LEA passes the lawful authorization to the NWO, AP or SvP. The NWO, AP or SvP determines the relevant target identities from the information given in the lawful authorization.
4	The NWO, AP or SvP causes interception facilities to be applied to the relevant target identities
5	The NWO, AP or SvP informs the LEA that the lawful authorization has been received and acted upon. Information may be passed relating to the target identities and the target identification
6	IRI and content of communication are passed from the target identity to the NWO, AP or SvP
7	IRI and content of communication are passed from the NWO, AP (via a NWO) or SvP (via a NWO) to the LEMF of the LEA
8	Either on request from the LEA or when the period of authority of the lawful authorization has expired the AP, NWO or SvP will cease the interception arrangements.
9	The AP, NWO or SvP announces this cessation to the LEA

To apply interception, an administrator typically requires the following parameters for the special commands:

- target identity;
- LEMF identity for content of communication;
- LEMF identity for IRI;
- alarm routeing;
- closed user group(s) for LEMF;
- target identification;
- operator personal identity.

The syntax of the necessary commands may be different in various systems.

4.4 Co-operation

In a distributed / deregulated telecommunication environment an interception subject can subscribe to services offered by multiple SvPs and is able to choose one or more APs or NWOs . Such circumstances will require co-operation in the provision of interception.

4.4.1 Co-operation between APs, NWOs and SvPs

If required, APs and NWOs whose facilities are used by SvPs may co-operate in the provision of lawful interception.

No more than the strictly necessary information relating to operational activities to allow lawful interception of services used by the target should be given to any AP or NWO directly involved in the provision of interception facilities.

4.4.2 Co-operation between SvPs

In case of co-operative provision of services, any provider involved should be given no more information relating to operational activities than is strictly necessary to allow lawful interception of these services.

4.5 International aspects

Provision of telecommunications service which involves the crossing of national boundaries should make provision for lawful interception in accordance with relevant national laws, treaties and conventions as these may apply from time to time.

4.5.1 International provision of service

In this context, scenarios are possible where SvPs are involved either in the home country or in a foreign territory which may or may not be the same as the switching point is located in.

4.5.2 Co-operation and co-ordination across borders

The general requirements regarding co-operation between multiple APs/NWOs/SvPs should be independent of the transmission technology (satellite / radio links / cable network) and arrangements between multiple parties should be made such that:

- any other party involved in the provision of interception facilities is aware of the least detail of operational activities possible;
- there should be a legal entity, in each home (served) country, on whom lawful authorizations can be served.

5 Handover interface

The generic HI adopts a three port structure such that administrative information, IRI and the content of communication are logically separated. In principle this structure is applicable to all telecommunications systems. It is the intention that the HI described in the present document shall be of universal application. The network requirements for lawful interception, derived from the implementation of new networks or services, may lead to a revision or enhancement of the HI described in the present document. Diverging solutions should be avoided.

The three logical ports represent the channels across which information is exchanged. The mapping of the three logical ports to physical channels or protocols should be related to the network technology employed. The three logical ports could for example be mapped to:

- a single circuit oriented physical channel;
- a single packet oriented physical channel;
- several circuit oriented physical channels;
- several packet oriented physical channels;
- several circuit oriented physical channels and one or more packet oriented physical channel.

5.1 General

The chosen solution to the requirements of the LEAs is a three ported interface. Such an interface is shown in figure 2.

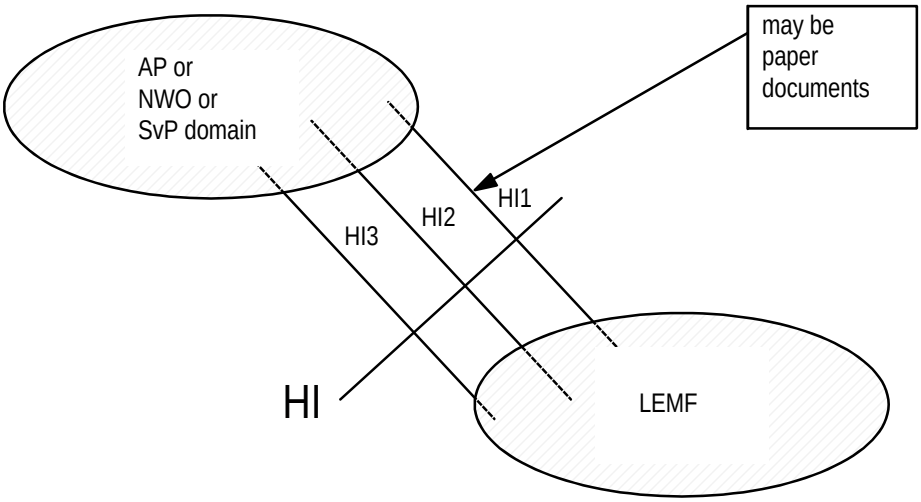


Figure 2: Diagram showing HI between AP/NWO/SvP and LEMF

The first HI port HI1 shall transport various kinds of administrative information from/to LEA and AP/NW0/SvP. In case of an automatic administrative interaction, there shall be a complete separation between the administrative interface and the technical interface of the AP/NWO/SvP, in order not to give the LEMF the possibility to establish or modify an interception without an action of a mandated agent of the AP/NWO/SvP. In case of a non automatic administrative interaction this interface may also be manual, rather than electronic.

Further description of HI1 is given in subclause 5.3.

The second HI port HI2 shall transport the IRI from the AP/NWO/SvP to the LEMF and is described in subclause 5.4.

The third HI port HI3 shall transport the content of communication from the AP/NWO/SvP to the LEMF and is described in subclause 5.5.

Other interfaces which may be necessary to support the interception of communications are of internal kind and are mentioned in clause 6 since they do not belong to the HI structure.

The three ports of the HI may use a common bearer or separate bearers, but would typically use convenient interfaces already provided by the telecommunications network. For example, in a 64 kbit/s channel structured network, delivery of the content of communication could be made across two 64 kbit/s channels.

There is a general requirement to deliver the result of interception in real time for real time services. Services which have an element of delay, such as mail services, may suffer a delay in the delivery of the result of interception.

The delivery of the result of interception may be via fixed or switched connections. When switched connections are used it may be appropriate for the LEMF and AP, NWO or SvP to authenticate each other before information is transmitted.

If encryption is provided by an AP/NWO/SvP, then in general, decryption needs to be made by the AP, NWO or SvP and the result of interception provided en-clair across the HI.

In certain circumstances encryption of the delivery of the result of interception may be necessary to protect confidentiality and to assure discretion.

Information provided by an AP, NWO or SvP is based on a target identity, which is a technical identity. Information passed to the LEMF (or LEA) will usually be tagged to indicate the target identification, which is the identity associated with the lawful authorization. A single target identification may relate to one or more target identities.

5.2 Functional block diagram

The functional components, as shown in figure 3, which facilitate the HI are given in table 3.

Table 3: Functional block diagram components

Component	Description
IIF	an IIF within the AP's, NWO's or SvPs domain. There may be more than one IIF involved in the provision of interception.
INI	an INI within the AP's, NWO's or SvPs domain which exists between an IIF and the mediation function.
AP/NWO/SvP administration centre	the administration centre contacted via the port HI1 (which may be partly electronic, and partly paper based depending on circumstances) is used to setup the interception action on the LEA request.
Mediation function	a function which selects, sequences and transforms information, including content of communication when necessary, between a number of IIFs and the HI. Sometimes the mediation function may be a null function e.g. direct delivery of the content of communication to the LEMF via HI3 with no changes. For example, in a Global System for Mobile communications (GSM) network the mediation function would not transform A law speech as used in a simple call, but would be required to transcode to A law speech when direct coding is employed on a call from one GSM terminal to another.
Delivery mechanism to LEA/LEMF	a) intercept requests, status and alarm reports are transmitted between the administration centre and the LEA/LEMF; b) the IRI is transmitted through the mediation function (may be transparent) to the LEMF; c) the content of communication is transmitted through the mediation function (may be transparent) to the LEMF.

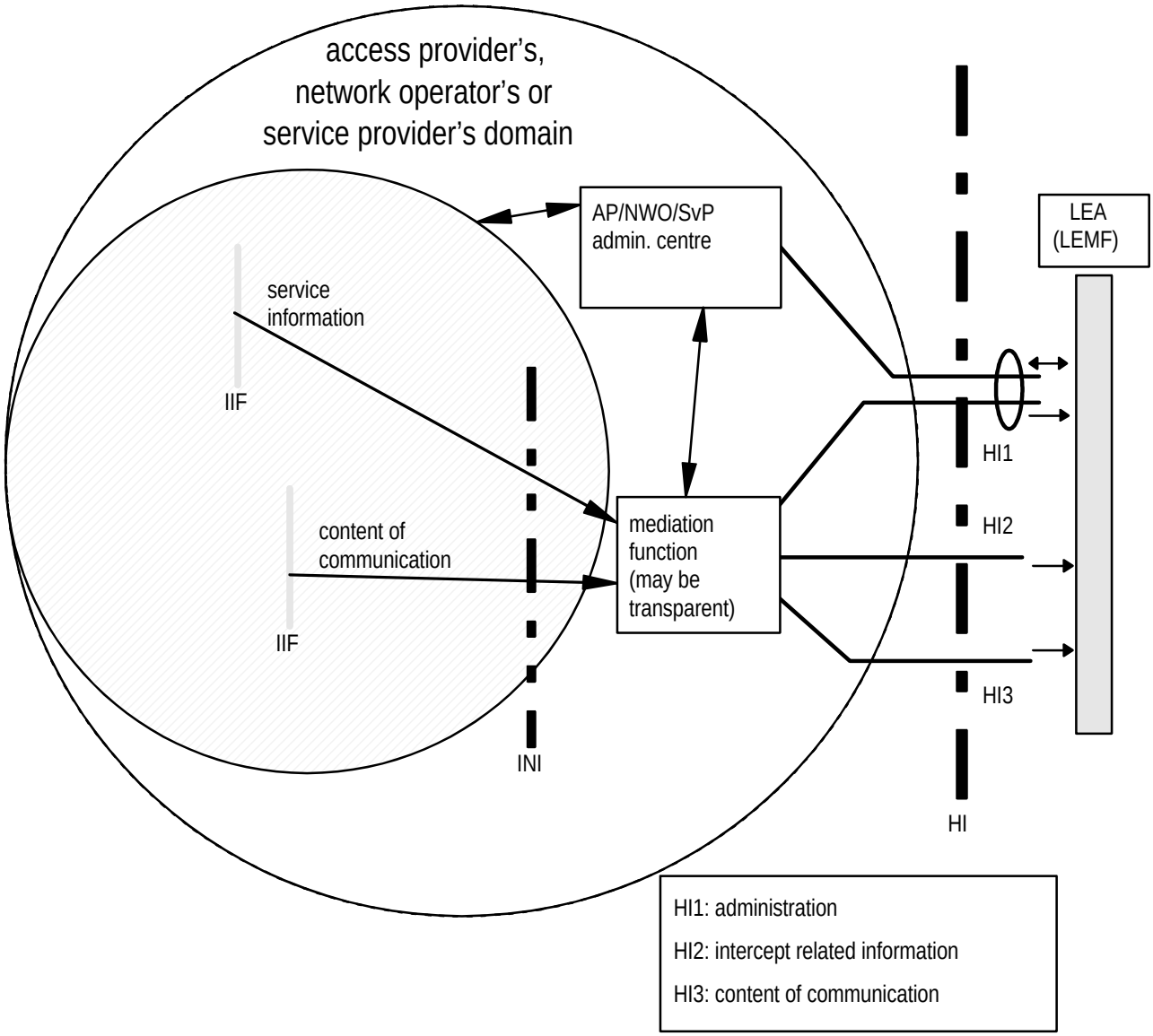


Figure 3: NWO/SvP functional block diagram showing HI

5.3 HI1 - interface for administrative information

The HI1 shall transport all kind of administrative information from/to LEA and NWO/SvP. This port shall be used for the transmission of the request to establish or to remove the interception action from the LEA to the NWO/SvP and the acknowledgement message back to the LEA. In case that a automatic transmission between LEA and NWO/SvP is not possible for some reasons, this port shall support manual transmission (e.g. voice, fax) and not only focus on automatic transmission from/to the LEMF and the NWO/SvP facility.

The status report should cover all kind of alarms, reports or information related to the intercept function. The status reports and the alarm reports are transmitted via HI1 to the LEMF or LEA if necessary. Alarms being not specific for a certain target identity can be received by all LEA´s, other alarms (e.g. LEMF busy, no answer from LEMF) should only be transmitted to the specific LEA to which the alarms apply.

The general status reports can typically be:

- target identity removed from service;
- target identity has changed within the network;
- bulk modification of subscriber numbers;
- individual modification of subscriber number;
- new MSN (multiple subscriber number) creation;
- LI database lost (e.g. software replacement, recovery, fall back);
- general setup failure.

Status reports indicating transmission problems between AP/NWO/SvP and LEMF can typically be:

- LEMF transmission problems;
- LEMF is busy;
- no answer from LEMF;
- transmission of IRI to the LEMF is not possible.

5.4 HI2 - interface for IRI

The HI2 shall transport all IRI. This interface shall be used to transmit information or data associated with the telecommunication services of the target identity apparent to the network. It includes signalling information used to establish the telecommunication service and to control its progress (e.g. target identification, identifications of the other parties of a communication, basic service used, direction of the call or the event, answer indication and/or release causes, time stamps). If available, further information such as supplementary service information or location information may be included.

Sending on of the IRI to the LEMF shall in general take place as soon as possible (in the range of a few seconds). In exceptional cases (e.g. data link failure), the IRI may be stored for later transmission for a specified period of time.

5.4.1 Types of records

IRI shall be structured as a sequence of records. To indicate the progress of the telecommunication service, these records shall be of certain types as shown in table 4:

Table 4: IRI record types

Record type	Description
Begin record	at the first event of a call or service attempt
End record	at the end of a call or service attempt
Continue record	at any time during a call or service attempt (e.g. in-call service activation/deactivation)
Report record	if no call association is available (e.g. activation/deactivation of features, use of a non-call associated service)

These four types of record are intended to be suitable for flexible application to all services.

5.4.2 Formatting and coding of IRI

IRI will be passed from the AP, NWO or SvP to the LEMF with no translation of information content. This has the advantage that:

- there is a minimum of translation to be kept up-to-date;
- the mediation functionality is minimized;
- the amendment required when introducing new services is minimized.

NOTE 1: The use of Intelligent Network (IN) protocols between interconnected INs involves digits being passed directly from one network, the slave network, to another network, the controlling network. The controlling network then exerts control on the slave network. This allows NWOs and SvPs, for example, to offer their customers a uniform service irrespective of geographic location. Such operation means that, in certain circumstances, an intercepting network does not (and can not) understand the meaning of digits sent by a target identity. Those digits will be understood and acted upon by the controlling network.

NOTE 2: Information may require enveloping before being passed to the LEMF.

5.5 HI3 - interface for content of communication

The port HI3 shall transport the content of the communication 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.

The transmission media used to support the HI3 port will usually be those associated with a telecommunications network or its access arrangements.

In cases of failure, the content of communication is lost. The network does not provide any recording functions.

5.6 Correlation of HI2 and HI3

When a HI3 port is established the target identification of the target identity shall be passed across to enable the LEMF to correlate the content of communication on HI3 with the intercepted related information on HI2.

In situations where a LEMF may be connected to more than one source of the result of interception it is necessary to ensure reliable correlation between the content of communication and IRI. Several mechanisms used at the same time will ensure correct correlation. Possible mechanisms are given below. The use of the given examples in a given circumstance will be dependent on national rules and technical considerations.

Table 5: Possible correlation mechanisms

group	content of communication	IRI
a)	Time of arrival of call at LEMF	Time stamp, in information record
b)	Unique number sent in an associated signalling channel	Unique number in information record
c)	LEMF address	LEMF address, in information record
d)	particular physical channel	particular physical channel
NOTE 1: A unique number may be devised in various ways. NOTE 2: This table is not exhaustive.		

5.7 Testing

It should be possible to test the correct operation of the lawful interception functionality and HI.

6 INIs

For the convenience of APs, NWOs and SvPs it will be convenient to define and standardize internal interfaces within the intercepted network. For example, GSM uses interfaces referred to as X.1, X.2, X.3. Such standardization will make the development and implementation of mediation functions faster and more convenient (see GSM TS 02.33 [3], ETR 363 [4] and GSM TS 03.33 [5]).

Another example is the transmission of information and data from an in-line Trusted Third Party (TTP) to the LEA. The in-line TTP is a network function which needs an INI. The requirements from a TTP point of view are described in EG 201 057 [7].

For the interception of services such as Universal Personal Telecommunications (UPT), provided according to IN principles, it is necessary to enlarge the interface between the Service Control Point (SCP) and the Service Switching Point (SSP) in such a way which enables interception of such services.

7 Performance and quality

7.1 Timing

As a general principle, within a telecommunication system IRI, if buffered, should be buffered in for as short a time as possible. (If the transmission of IRI fails, it may become necessary to buffer this information.)

7.2 Fault reporting

Fault reporting will be provided to the LEMF as described in subclause 5.3

7.3 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.

8 Security aspects

There is a general requirement that the operation of interception facilities should be discreet, confidential and efficient.

8.1 General

For prevention of unauthorized administration, as well as unauthorized use, appropriate security features are necessary.

A security management system should be established.

There should be physical and logical access controls.

Any necessary keys, passwords and user identifications for the authorization and the logical access to the Interception function should be securely stored.

Any transmission of passwords and user identifications for access to interception functions should be secure.

Physical interfaces should be secured mechanically and/or logically against unauthorized use.

8.2 Transmission to LEAs

Transmission of all information between the AP/NWO/SvP and LEMF across HI1, HI2 and HI3 shall be confidential.

During communication between systems that are not based on a leased line, appropriate mechanisms should ensure that the recipient is in the position to verify or authenticate the identity of the sender while connection is set up.

During communication between systems that are not based on a leased line, appropriate mechanisms should ensure that the sender can verify or authenticate the identity of the recipient at the start of a connection.

8.3 Verification or authentication of LEMF and AP, NWO or SvP's facility

If verification or authentication fails, the LEMF should reject the connection request. It should also generate a report.

If verification or authentication fails, the AP’s, NWO’s or SVP's facility should abort the connection attempt. It should also generate a report.

8.4 Storage of information

The number of network elements, in which data, directly relating to the act of interception, are stored, administered or processed should be minimized.

8.5 Control of interception

Only specifically authorized personnel should be able to control interception.

The LEA should have no access to any network element, other than the administration centre.

At first, when a LEA presents a lawful authorization referring to a particular interception subject, an administrator has to interrogate the conditions relating to this interception subject, to ensure compatibility (e.g. in relation to supplementary service information, multiple subscriber numbers, etc.).

8.5.1 Internal interception function

The entire communication between the administration system and the Interception function should be confidential.

8.5.2 Security of internal interfaces

There are security issues relating to interfaces between internal systems which permit automatic administration of intercepting measures. Such interfaces should be protected. The interface should support authentication of both systems as well as the confidentiality of communication on the interface. When authentication fails, a report should be made.

8.6 Discretion of interception functions

The interception functions shall be implemented in such a manner that:

- the interception subject and his correspondents can not know that a lawful interception is active;
- during the intercepted communication itself the quality of the communication shall remain the same as usual and the service shall be unchanged, including all supplementary services such as call forwarding, etc.;
- when there is no intercepted communication the quality of the communication shall remain the same as usual and the service shall be unchanged, such that there is no modification to services supplied or information received either by the interception subject or by some other party.

An employee of an AP/NWO/SvP who has been duly authorized may be permitted to know that interception is in progress, or that a subscriber is an interception subject.

An employee of an AP/NWO/SvP who has not been duly authorized may not be permitted to know that interception is in progress, or that a subscriber is an interception subject.

8.7 Remote application of lawful interception

To prevent unauthorized application of the lawful interception mechanisms, the access to the administration function shall only be possible from specified locations, which may include administration centres or remote access mechanisms. Any other logical administration interfaces should be disabled.

The HI1 port from the LEA to the administration centre should assure confidentiality of delivery of lawful authorizations.

No party other than an authorized AP, NWO or SvP shall have remote access.

9 Billing and charging

9.1 Relating to the interception subject and their correspondents

The operation of lawful interception mechanisms shall, of themselves, cause no charges to be raized which are payable by:

- the target identity;
- any correspondents of the target identity.

The operation of lawful interception mechanisms shall, of themselves, cause no charges, which would otherwize have been raized, to fail to be raized which are payable by:

- the target identity;
- any correspondents of the target identity.

9.2 Relating to the intercept itself

The AP, NWO or SvP may wish to raize charges for the provision and operation of a lawful interception facility. Charges may be based on one or more of the following:

- use of network resources;
- the use of other network facilities;
- provision and removal of interception relating to some target identity;
- call or service activity relating to a target identity;
- direct charges made by some other party.

Charging data shall be produced in such a way that it is only visible to authorized personnel.

Annex A (informative): Quantitative aspects

A.1 Networks

The number of intercepts to be allowed for in a network is a national issue.

A.2 Recipient LEMFs

From a single network the HI should be able to address up to one hundred LEMFs depending on national requirements and circumstances.

A.3 Number of simultaneous intercepts

It should be possible that at least three different LEMFs (may belong to different LEAs) are simultaneously provided with the result of the interception relating to the same target identity. These different LEMFs may be the subject of different lawful authorizations.

Annex B (informative): Typical interface implementations

B.1 Principles

There are two essential principles for the delivery of the results of interception:

- direct delivery from AP, NWO or SvP to the LEMF;
- indirect (hubbed) delivery from AP, NWO or SvP to the LEMF with the assistance of an interposed switching function.

B.2 Delivery of the content of communications

Delivery of the content of communications is possible by several methods, some of which are given in table B.1. A solution should be chosen which is as closely aligned with normal network or service operation as possible:

Table B.1: Examples of delivering the content of communication

Delivery method	Description and notes
Circuit switched to LEMF terminal	A network sets up one or more normal switched connections from itself, directly or indirectly, to a LEMF which has the status of a network termination.
Circuit switched to network interface, direct	A network sets up one or more normal switched connections from itself directly to a LEMF which has the status of a NWO.
Circuit switched to delivery network	A network sets up one or more normal switched connections from itself, directly to a delivery network. (The handover to the delivery network may use ITU-T signalling system No.7 signalling). The delivery network has the responsibility to deliver the content of communication to the LEMF.
Permanent leased connection per intercept, without signalling	A permanent path, associated with a specific target identity, is established from a point within the network to a LEMF. Each time that the target identity becomes active the content of communication is presented across the path. The path may comprize one or more channels, as appropriate.
Permanent leased connection, with signalling	A permanent path is established from a point within the network to a LEMF. Each time that a target identity becomes active the content of communication is presented across the path and the signalling indicates the specific active target identity.
Data circuit	A data path is established to the LEMF, across which the content of communication is delivered. The content of communication may require some enveloping procedure. The path may also carry IRI. Such an arrangement could be used for the interception of messaging services such as e-mail or paging.
Mixed methods	In a rich service the content of communication may exist in several possible forms. For instance, the GSM Short Message Service (SMS) supplements circuit switched speech and data. In this case circuit switched content of communication may be provided through a 64 kbit/s channel or channels, and the SMS content of communication may be provided through a X.25 link which also carries IRI.

For example, considering a 64 kbit/s circuit switched Integrated Services Digital Network (ISDN), the delivery of the content of communication could be made by the use of ISDN calls. Such calls from an internal network element to the LEA are set up as standard circuit switched ISDN calls, without any need to change the existing ISDN (Digital Signalling System No. 1 (DSS1) and ISDN User Part (ISUP)) protocols. These protocols allow the transport of call labelling information for correlation to the IRI, without any impact on normal network operation. The content of communication may be delivered to the LEMF either directly from the originating ISDN or via some intermediate ISDN without any need for protocol amendments.

Existing network functions can be used to set up and release calls providing delivery of the content of communication.

B.3 Delivery of IRI

Delivery of the IRI is possible by several methods, some of which are given in table B.2. The applicable methods are certainly network dependant.

Table B.2: Examples of delivering IRI

Delivery method	Description and notes
Packet Switched Public Data Network (PSPDN), X.25 link	A single PSPDN or several PSPDNs provide a path between a mediation device and a LEMF.
ISDN X.31 connection to the LEMF	As above, but delivery to the LEMF is via X.31. This offers the possibility of a single physical port carrying both the content of communication (speech, circuit switched data) in one or more B channels, and IRI in a D channel.
Transmission of IRI together with the content of communication using User-to-User Signalling (UUS) delivery.	In this scheme an ISDN call is (or calls are) established to the LEMF every time that the target identity becomes active. The B channel (or channels) carry the content of communication and UUS is used to carry IRI.

B.4 ISDN delivery

It is possible to use an ISDN B channel, or several B channels, as HI3. These B channels may be established by an ISDN call (or calls) to the appropriate LEMF each time that the target identity becomes active. When the target identity becomes inactive, the call is (or the calls are) released.

HI2 may be established as a completely separate mechanism, or HI2 may be associated with a B channel in some way such as the use of Q.931 signalling.

NOTE: This approach is well suited for a large number of networks including present day telephone networks, ISDN and most Public Land Mobile Networks (PLMNs). However the connection setup time in the target network cannot be allowed to be significantly shorter than the typical call setup time for the ISDN networks used for delivery.

Annex C (informative): Example direct delivery interface from an ISDN

This annex describes HI2 and HI3 and their coding appropriate to an ISDN supporting voice and data calls using 64 kbit/s channels. The detailed description part supports a simple call to establish the principles.

A simple call is a two party call, one party being the target identity. No supplementary services are invoked.

C.1 HI2 interface

C.1.1 IRI records

The HI2 interface port shall transport IRI within IRI records to the LEMF. Transport shall in general take place as soon as possible after a relevant event. Such IRI will in principle be available in the following phases of a call:

1) at call attempt initiation when the target identity becomes active, at which time call destination information may or may not be available;

2) at the end of a call attempt, when the target identity becomes inactive;

3) at certain times between the above events.

The records are sent in a connectionless manner, but in order to keep control of the *transaction* which a call attempt constitutes, the following record types shall be used during the 3 phases (same numbering as above, see also subclause 5.4.1):

1) Begin record;

2) End record;

3) Continue record.

Another record type, the Report record, is used for non-call-related events. For simple calls, it can be applicable for unsuccessful call attempts.

Each record may contain several parameters. In order to facilitate decoding, the parameters shall be assigned to logical fields in the records, depending on their origin and/or meaning.

Relevant information on a call is taken from the call handling process, using in general the coding specifications of the standardized ISDN protocols, with no translation of information content, see subclause 5.4.2. Lists of parameter types are specified, defining, which of the parameters appearing during a call shall be included in the IRI records.

In addition to parameters taken from the call handling process, further, lawful interception specific, parameters are included, see below.

C.1.2 IRI records content

For a simple call, the information given in table C.1 shall be sent.

Table C.1: IRI record fields

Field	Field Name	Remark
1	version indication	version of HI specification. Identification of the particular HI2 interface specification
2	record identification	unique identification of NWO. Contains a NWO identity and a NWO defined internal identification
3	type of record	begin / continue / end / report record
4	lawful authorization identifier	Number used to identify the interception subject (target identification). Reference number assigned to an act of interception; Format: see below.
5	call identifier	unique identity of the intercepted call (also part delivery call subaddress) Used for correlation between IRI records and CC Calls of a target (in case of multiple simultaneous calls); format: 16 bit binary value.
6	address of other party	communication partner of target identity address of party, to which the target sets up a call; depending on call type: calling or called party identification (number); may include a subaddress.
7	date and time	date and time of record trigger condition. Year / Month / Day / Hour / Minute / Second / Daylight saving time - Flag.
8	direction of call direction of call event	Begin Record: target identity is orig. or term. party. Other record types: event originated by target identity or another party.
9	basic service / Lower Layer Compatibility information (LLC)	parameters as received from signalling protocol (e.g. Bearer Capability (BC), Higher Layer Compatibility information (HLC), LLC).
10	supplementary services information	service associated parameters; several parameters possible. Service related information as received from protocol, including user-to-user information (not applicable for a simple call).
11	cause	reason for release of intercepted call. Cause value as received from protocol.
12	additional network parameters	e.g. Co-ordinates of radio cell, etc. Details to be decided.
13	CC Call failure indication	reason for failure of CC Call set up (network option). Cause value as received from CC Call protocol.
14	address of target	DN of target, for which LI has been activated (network option). As received from target Call protocol; depending on call type: calling or called party identification (number); may include a subaddress.
Mandatory / optional fields:		
fields are always present in all records		
field present, if its parameters are available in standard call procedures		
Remarks to table: This table lists all fields: - field 10 is not applicable for a simple two party call; - field 12 is reserved for networks supporting mobility; - the first 3 fields are housekeeping parameters; - the remaining parameters are partly optional, depending on their availability during the actual phase of a call, or within one of the 3 record types, respectively; - field 4, the *lawful authorization identifier*, identifies the specific interception. It is in general a digit string, defined by the NWO and/or the LEA. As a network option, it may be identical to the *delivery call destination* at the LEMF; - an additional parameter 5, *the call identity*, is used in order uniquely to identify several simultaneous calls relating to the same lawful authorization identifier. Parameters 4 and 5 constitute the identifier of the transaction associated with an intercepted call, and are as such used *for correlation of the IRI records to the delivery calls*. For that purpose, these parameters are also part of the *delivery call set up information*, see below.		

C.2 HI3 interface port

The content of communication is delivered in the following manner:

1) at call attempt initiation an ISDN delivery call (or calls) is established, in parallel with any activity relating to the target identity, from the mediation function to the LEMF. Typically this would be a pair of ISDN calls: one call offers the content of communication towards the target identity, the other call offers the content of communication from the target identity;

2) during the establishment of each of these calls a handshake takes place, using the Calling and Connected Line Identity parameters of the delivery calls (CLI, COL) so that the mediation function and the LEMF check each other's identity;

3) the mediation function passes information relating to the target identification to the LEMF. The LEMF uses this information to identify the source of the content of communication;

4) the mediation function passes the content of communication only after the identity check is satisfied;

5) at the end of a call attempt, each delivery call associated with that call attempt is released by the mediation function.

C.2.1 HI3 interface port, protocol impact

The delivery calls shall use unmodified standard ISDN protocols (DSS1, ISUP). To identify the delivered information, including mapping the delivery calls with the IRI records, parameters may be included in the call set up as shown in table C.2:

Table C.2: Identification of delivered information

Call set up information element	Information contained
CLI-Parameter	number identifying target exchange e.g. number out of target exchange's numbering plan
Calling Party Subaddress	lawful authorization identifier (same as IRI record field 4)
Called Party Subaddress	Call identifier (same as IRI record field 5)
	Direction indication (communication from / towards target)
	speech / data discriminator (for use by LEMF signal processing)

C.2 Information for calls invoking supplementary services

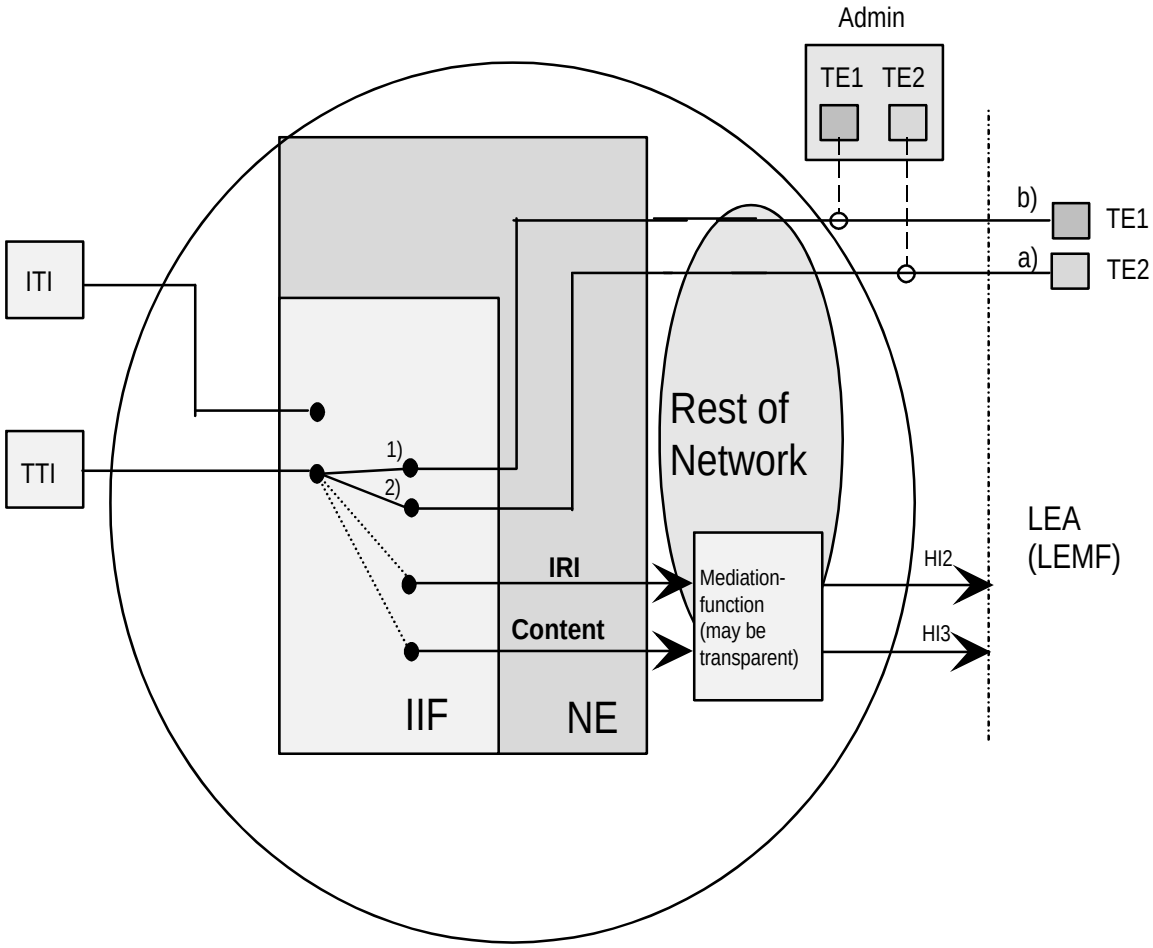
Depending on the type of an invoked supplementary service, further delivery calls to the LEMF may be required in addition to previous delivery calls. Within the IRI records, the transmission of additional, supplementary service specific data may be required, applying the same principles as described in subclause C.1.1.

No further details are described within this annex.

Annex D (informative): Testing

It should be possible to test the correct operation of the lawful interception functionality and HI. It should also be possible to test any fault reporting alarms. For the reason that some alarms are only of interest to the administrator of the NWO, there needs to be some restrictions for the LEA (LEMF) when receiving these alarms.

Two test cases are described below based on a test configuration as depicted in figure D.1. The tests require provision of an (interception) Test Target Identity (TTI) and shall be initiated by Test Equipment (TE), TE1 or TE2, located at the NWO and/or one or more LEAs. Correct operation shall be monitored at the HI (HI2 and HI3) by the LEMF of the LEA(s) and/or appropriate equipment of the NWO.



1) Simple test (only TE1, TTI)
2) Enhanced test (TE1, TE2, TTI, call deflection)

a) Test equipment belongs to LEA
b) Test equipment belongs to NWO

Figure D.1: Testing arrangements

D.1 Simple test

In the network element (NE) a TTI (which may be a "virtual" one) should be implemented by the administrator in order to test the function of the HI. For the lawful interception equipment the TTI should be treated like a normal Interception Target Identity (ITI). For test purposes test calls to the TTI are generated from the TE1 by the administrator or the LEA. Therefore it is possible to test the HI (HI2 and HI3) in a plain mode. In case of a successful test the IRI and the content of communication should reach the law enforcement monitoring facility (LEMF).

D.2 Enhanced test

Managing an enhanced test a second TE (TE2) is needed. The TTI should be incorporated in the systems as described in the simple test. For this TTI a call deflection to the TE2 is generated. With this feature it should be possible to test various telecommunication services. In case of a successful test the IRI and the content of communication should reach the law enforcement monitoring facility (LEMF).

History

Document history			
V1.1.1	February 1998	Membership Approval Procedure	MV 9814: 1998-02-03 to 1998-04-03
V1.1.2	May 1998	Publication	

ISBN 2-7437-2152-9
Dépôt légal : Mai 1998