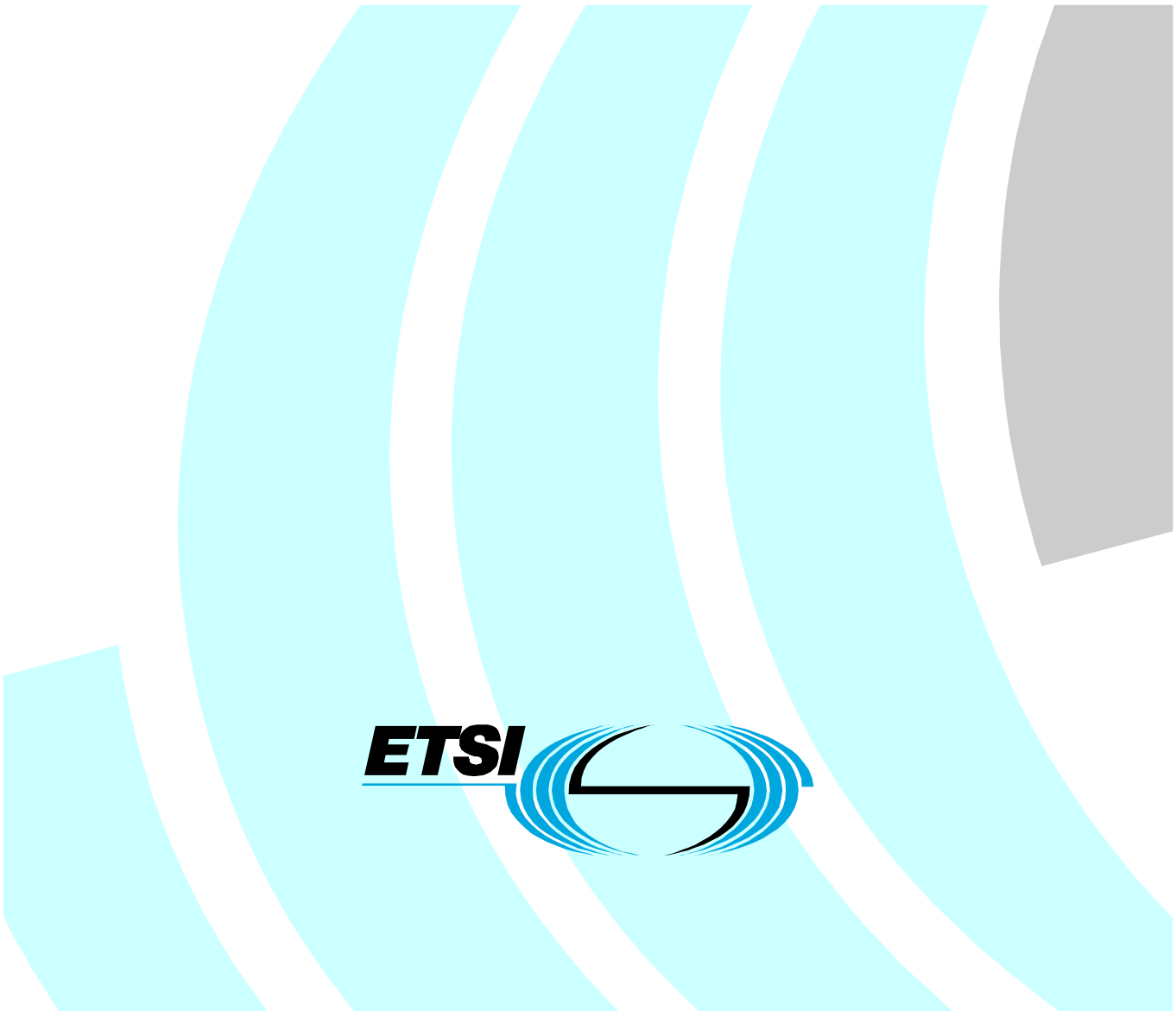
ETSI ES 201 158 V1.2.1 (2002-04)

ETSI Standard

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



Reference
RES/SEC-003015

Keywords
security, lawful interception

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

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 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 (SvPs) 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 SvP and/or AP 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 general approach of 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 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] Official Journal of the European Communities, 96/C 329/01: "Council resolution of 17 January 1995 on the lawful interception of telecommunications".

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

[4] ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover Interface for the lawful interception of telecommunications traffic".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ES 201 671 [4] and the following apply:

Access Provider (AP): 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 AP and Network Operator may be a common commercial entity.

(to) buffer: 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

NOTE 1: In this context a user may be a person or a machine.

NOTE 2: It is used for transmission of the content of communication. This term refers to circuit switched only.

communication: information transfer according to agreed conventions

Content of Communication (CC): information exchanged between two or more users of a telecommunications service, excluding Intercept Related Information (IRI)

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

Content of Communication link: communication channel for HI3 information between a mediation function and a LEMF

handover interface: 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.

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

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

interception interface: physical and logical locations within the NWO/AP/SvP telecommunications facilities where access to the CC and IRI 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

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

intercept related information: 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

internal network interface: network's internal interface between the Internal Intercepting Function and a mediation function

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

Law Enforcement Monitoring Facility (LEMF): 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 an NWO/AP/SvP

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

lawful interception: See interception.

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

mediation function: 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 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 CC and IRI, which is passed by an NWO/AP/SvP to a LEA

NOTE: 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

NOTE: The information may be established by an NWO/AP/SvP 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 routeing of signals on a telecommunications network

NOTE: An SvP need not necessarily run his own network.

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

target identification: identity which relates to a specific lawful authorization as such

NOTE: This might be a serial number or similar. It is not related to the denoted interception subject or subjects.

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.

telecommunication: 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 abbreviations given in ES 201 671 [4] and the following apply:

AP	Access Provider
CC	Content of Communication
GSM	Global System for Mobile communications
HI	Handover Interface
IIF	Internal Intercepting Function
INI	Internal Network Interface
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ITI	Interception Target Identity
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MSN	Multiple Subscriber Number
NE	Network Element
NWO	Network Operator
QoS	Quality of Service
SvP	Service Provider
TE	Test Equipment
TTI	Test Target Identity

4 General requirements

The present document focuses on the HI between an NWO/AP/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, TS 101 331 [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 telecommunications network elements.

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

Further information is given in TS 101 331 [1], Official Journal of the European Communities, 96/C 329/01 [2] and ETR 330 [3].

4.3 Example of typical functional role model and process

The functional role model described in this clause 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.

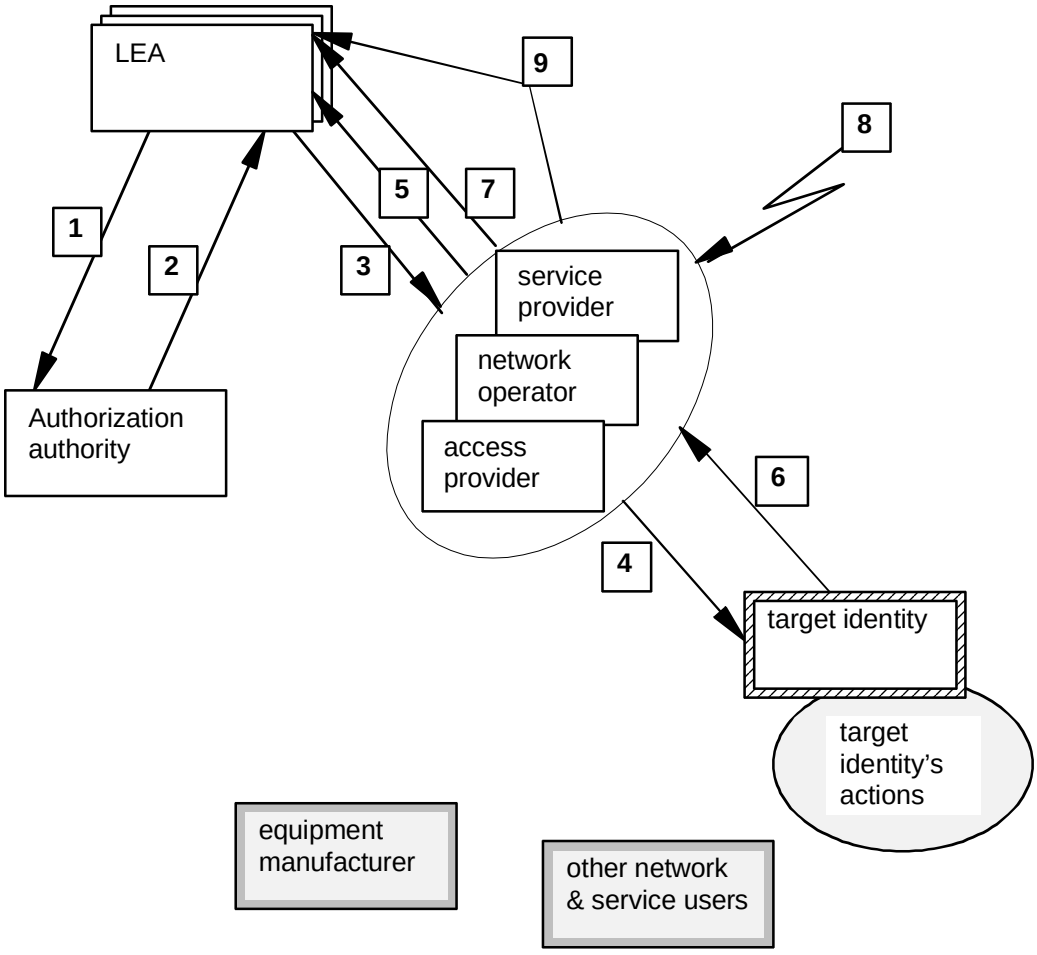
If a LEA wishes to use lawful interception as a tool that LEA will ask a prosecuting judge or other responsible body for a lawful authorization, such as a warrant. If the lawful authorization is granted the LEA will present the lawful authorization to the NWO/AP/SvP via an administrative interface or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

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

A lawful authorization may describe the IRI and the CC that are allowed to be delivered for this LEA, investigation, period and interception subject. For different LEAs 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 NWO/AP/SvP. 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 LEAs and different investigations. It might be necessary to strictly separate these investigations and LEAs. 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 CC. These various lawful interceptions could fall under different laws.



NOTE: The numbered lines relate to actions described in clause 4.3.3 and table 2.
The law may require that checks and audits are possible. Therefore there should be facilities at the NWO/AP/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 NWO/AP/SvP to intercept communications according to a lawful authorization. The LEA receives, through a LEMF, the result of interception (CC and IRI) relating to a target identity. Several LEAs may request the interception of the same target identity at the same time.
NWO	An NWO operates the 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.
SvP	An SvP provides services, additional to those provided by any network itself, to users of a network. An 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. An SvP may be the same organization as the NWO. Interception may be required for several SvPs using the same telecommunication network. See also TS 101 331 [1].
AP	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 NWO/AP/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 NWO/AP/SvP. Pieces of equipment from different manufacturers may be integrated in a common telecommunications infrastructure.

4.3.3 Process

The process as described in this clause 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 NWO/AP/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 NWO/AP/SvP, actions are shown in table 2.

Table 2: Functional role model process actions

Reference (see 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/SvP. The NWO/AP/SvP determines the relevant target identities from the information given in the lawful authorization.
4	The NWO/AP/SvP causes interception facilities to be applied to the relevant target identities.
5	The NWO/AP/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 CC are passed from the target identity to the NWO/AP/SvP.
7	IRI and CC are passed from the NWO/AP/SvP 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 NWO/AP/SvP will cease the interception arrangements.
9	The NWO/AP/SvP announces this cessation to the LEA.

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

- target identity;
- target identification;
- LEMF address for CC;
- LEMF address for IRI;
- address parameters for LEMF (e.g. for authentication and security);
- alarm routing;
- NWO/AP/SvP 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 NWO/AP/SvP

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 NWO/AP/SvP should be independent of the transmission technology (e.g. 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 CC 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.

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.

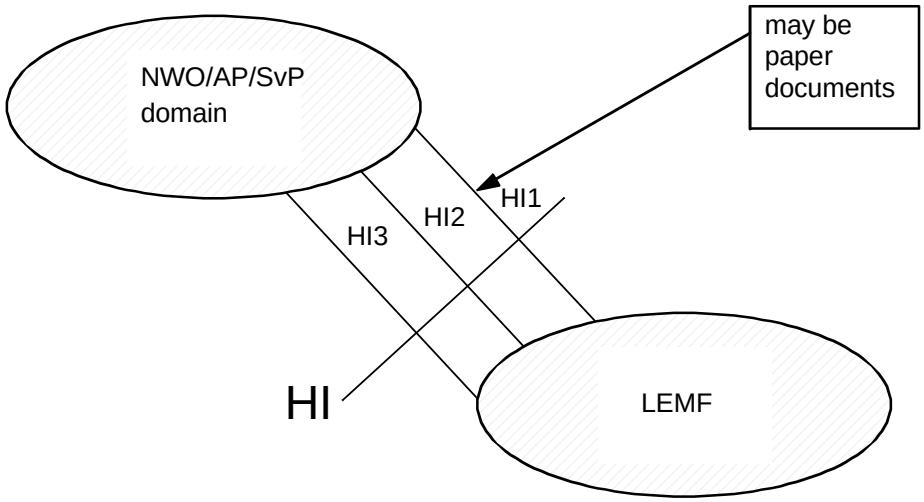


Figure 2: Diagram showing HI between NWO/AP/SvP and LEMF

The first HI port HI1 shall transport various kinds of administrative information from/to LEA and NWO/AP/SvP. There shall be a complete separation between the administrative interface (HI1) and the technical interface (HI2 and HI3) of the NWO/AP/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 NWO/AP/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 clause 5.3.

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

The third HI port HI3 shall transport the CC from the NWO/AP/SvP to the LEMF and is described in clause 5.5.

The HI2 and HI3 logical ports could for example physically be mapped to:

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

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.

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.

It may be appropriate for the LEMF and NWO/AP/SvP equipment to mutually authenticate each other before the information is transmitted.

If encryption is provided by the NWO/AP/SvP, then in general, decryption needs to be made by the NWO/AP/SvP and the result of interception needs to be 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.

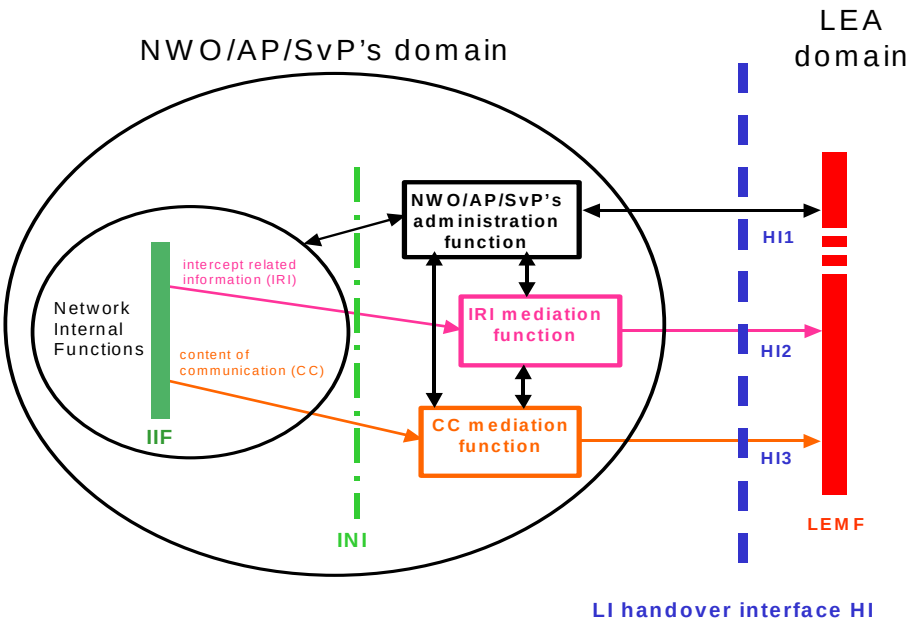
Information provided by an NWO/AP/SvP is based on a target identity, which is a technical identity. Information passed to the LEMF (or LEA) will usually be tagged to indicate the target identification, which is the identity associated with the lawful authorization. A single lawful authorization may relate 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 NWO/AP/SvP domain. There may be more than one IIF involved in the provision of interception.
INI	An INI within the NWO/AP/SvP domain which exists between an IIF and the mediation function.
NWO/AP/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 CC when necessary, between a number of IIFs and the HI. Sometimes the mediation function may be a null function, e.g. direct delivery of CC to the LEMF via HI3 with no changes.
Delivery mechanism to LEA/LEMF	a) intercept requests, status and alarm reports are transmitted between the administration centre and the LEA/LEMF; b) IRI is transmitted through the mediation function (may be transparent) to the LEMF; c) CC is transmitted through the mediation function (may be transparent) to the LEMF.



IIF: internal interception function
INI: internal network interface
HI1: administrative information
HI2: intercept related information
HI3: content of communication

Figure 3: NWO/AP/SvP functional block diagram showing HI

NOTE: The standardization of INI is out of scope of the present document.

5.3 HI1 - interface for administrative information

The HI1 shall transport all kind of administrative information from/to LEA and NWO/AP/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/AP/SvP and the acknowledgement message back to the LEA. The transmission between LEA and NWO/AP/SvP should support manual and/or electronic transmission from/to the LEMF and the NWO/AP/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 LEAs, 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 NWO/AP/SvP and LEMF can typically be:

- transmission problems to LEMF;
- LEMF is busy;
- no answer from LEMF.

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 buffered 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 below:

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.

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 NWO/AP/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: Information may require enveloping before being passed to the LEMF.

5.5 HI3 - interface for CC

The port HI3 shall transport the CC of the intercepted telecommunication service to the LEMF. The CC 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 CC 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 CC on HI3 with the IRI 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 CC 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 4: Possible correlation mechanisms

group	CC	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. A further description is given in annex D.

6 Void

7 Performance and quality

7.1 Timing

As a general principle, within a telecommunication system IRI, if buffered, should be buffered 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 clause 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 provided to the intercepted subject.

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 NWO/AP/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 NWO/AP/SvP 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 NWO/AP/SvP 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.

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 (IIF)

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 cannot 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 NWO/AP/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 NWO/AP/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 NWO/AP/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 raised 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 otherwise have been raised, to fail to be raised which are payable by:

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

9.2 Relating to the intercept itself

The NWO/AP/SvP may wish to raise 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 NWO/AP/SvP to the LEMF;
- indirect (e.g. via a hub) delivery from NWO/AP/SvP to the LEMF with the assistance of an interposed switching function.

Delivery of the IRI is possible by several methods. The applicable methods are certainly network dependant.

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

C.1 IRI records content

For a simple call, the information given in table C.1 shall be sent. The following table gives a minimum set of IRI parameters, which are not exhaustive. Technologies specific parameters may be added if necessary.

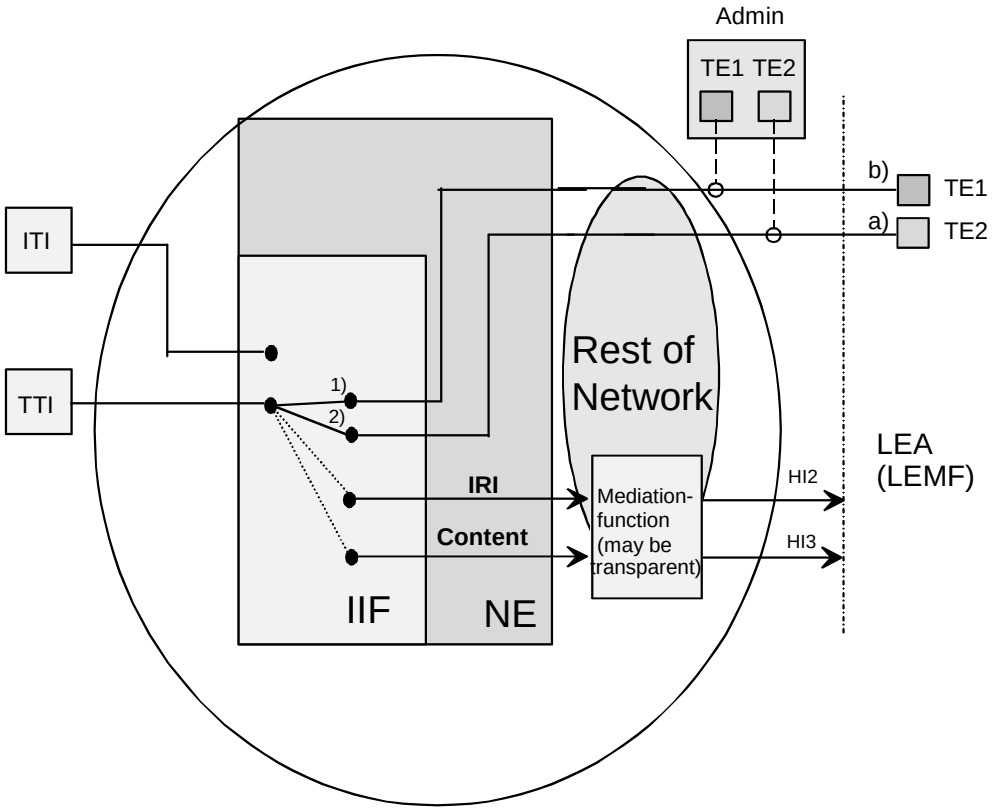
Table C.1: Example of IRI record parameters

Parameter Name	Remark
version indication	Version of HI specification. Identification of the particular HI2 interface specification.
operator identification	Unique identification of NWO/AP/SvP. Contains an NWO/AP/SvP identification.
type of record	E.g. begin/continue/end/report record.
lawful interception identifier	Number used to identify the target.
communication identifier	Unique identity of the intercepted communication. Used for correlation between IRI records and CC of a target.
address of other party	Communication partner of target identity address of party, to which the target sets up a call.
date and time	Date and time of record trigger condition.
direction	Direction of this event originated by target or other parties.
(supplementary) services information	Service and associated parameters.
cause	Reason for release or rejection of intercepted call (attempt).
CC delivery failure indication	Reason for failure of CC delivery set up.
identity of target	Target identity, for which LI has been activated.

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)

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 CC 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 CC should reach the Law Enforcement Monitoring Facility (LEMF).

Annex E (informative): Bibliography

ETSI TS 101 507: "Digital cellular telecommunications system (Phase 2+); Lawful interception - Stage 1 (GSM 02.33 version 8.0.1 Release 1999)".

ETSI ETR 363: "Digital cellular telecommunications system; Lawful interception requirements for GSM (GSM 10.20 version 5.0.1)".

History

Document history		
V1.1.2	May 1998	Publication
V1.2.1	February 2002	Membership Approval Procedure MV 20020426: 2002-02-26 to 2002-04-26
V1.2.1	April 2002	Publication