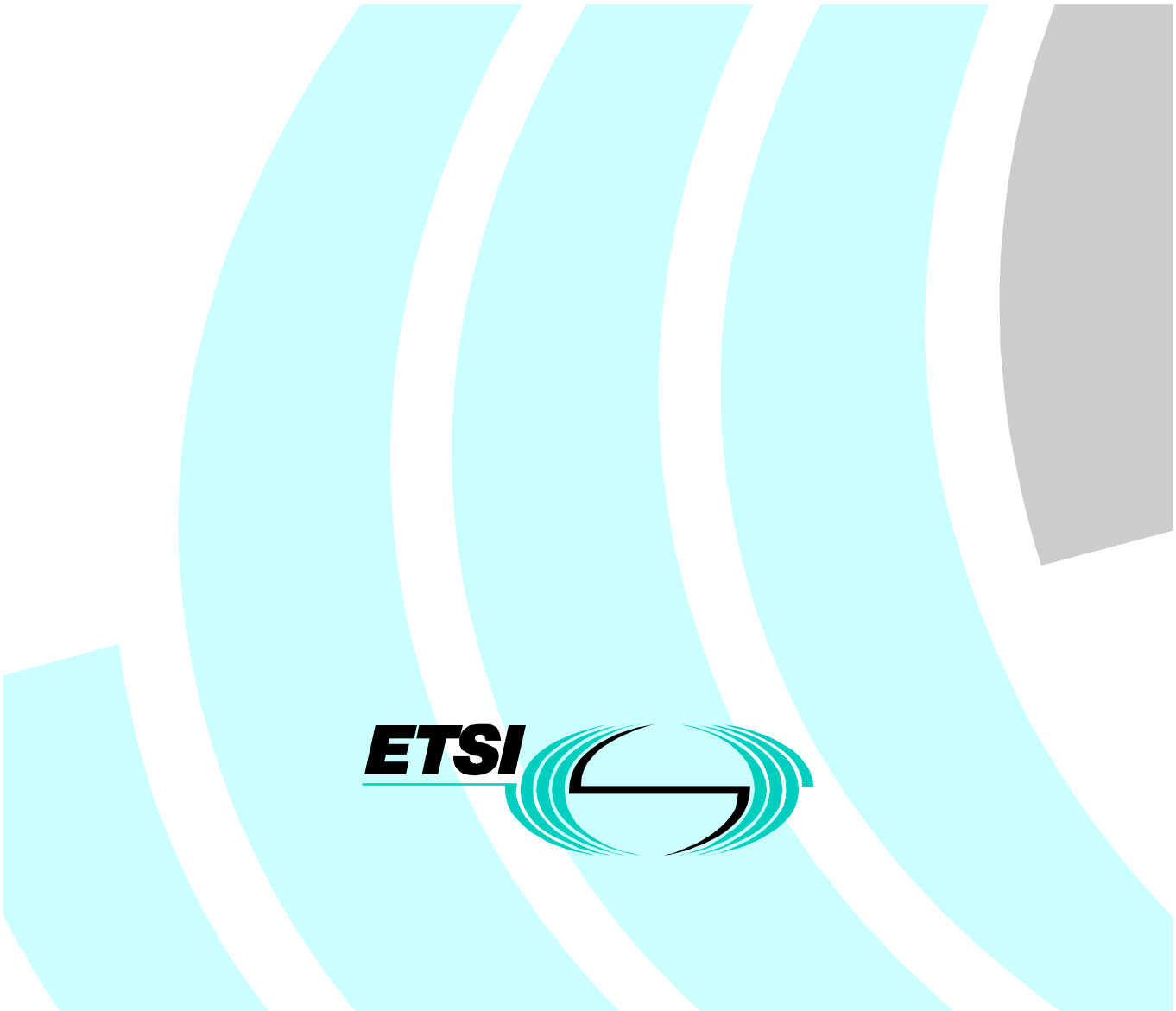
ETSI TR 101 943 V1.1.1 (2001-07)

Technical Report

Telecommunications security;
Lawful Interception (LI);
Concepts of Interception in a Generic Network Architecture



Reference
DTR/SEC-003008

Keywords
architecture, data, IP, security, telephony

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://www.etsi.org/ipr).

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

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Security (SEC).

1 Scope

The present document provides an informative overview and principles regarding implementation of Lawful Interception (LI) for telecommunications. It is based on ETSI requirements in this area. National requirements are not addressed here. The application of these principles is covered in other documents that address specific technologies and network types.

The topics, which are covered here, are:

- Introduction to scope of requirements for LI;
- Description of actors and roles related to network architecture;
- Architecture overview;
- Description of network nodes relating to LI;
- Interception scenarios related to subject identities;
- Delivery of results of interception;
- Relation between communication services and communication technology;
- Fulfillment of requirements relative to technical capabilities.

Please observe that this is not a requirements document.

2 References

For the purposes of this Technical Report (TR) the following references apply:

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

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

[3] ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the Lawful Interception of telecommunications traffic".

[4] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETR 331 [1] and ES 201 158 [2] and the following apply:

Access Provider (AP): acces provider 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 access provider and network operator may be a common commercial entity.

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

authorizing authority: authority, such as court of law, that is entitled to authorize Lawful Interception

(to) buffer: temporary storing of information in case the necessary telecommunication connection to transport information to the 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 (CC): information exchanged between two or more users of a telecommunications service, excluding Intercept Related Information

NOTE 3: This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Domain Name Server (DNS): network element, which functions as a translator between logical names and network addresses

NOTE 4: This type of element is widely used for IP traffic today. It can be anticipated that similar functionality will be introduced also for telephony in the near future.

Handover Interface (HI): physical and logical interface across which the interception measures are requested from an AP/NWO/SvP, and the results of interception are delivered from an AP/NWO/SvP to an LEMF

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

Intercept Related Information (IRI): 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 (or Lawful Interception): action (based on applicable laws and regulations), performed by an AP/NWO/SvP, of making available certain information and providing that information to an LEMF

NOTE 5: In the present document the term *interception* is not used to describe the action of observing communications by an LEA (see below).

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

NOTE 6: The interception interface is not necessarily a single, fixed point.

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

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

internal intercepting function: point within a network or network element at which the Content of Communication is made available

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

Internet Service Provider (ISP): business entity that offers connectivity to the Internet, primarily for dial-in subscribers

NOTE 7: The ISP will generally also provide e-mail facilities and other higher-level Internet services.

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

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

lawful authorization: permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a AP/NWO/SvP

NOTE 8: Typically this refers to a warrant or order issued by a lawfully authorized body.

LEA network: network connections and special protocol functions that are required for delivery of intercept products from a mediation function or delivery function to the LEMF(s)

NOTE 9: This network is specified by and normally belongs to the LEA domain.

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

mail server: network element which serves as a "point of presence" (POP) for receiving and storing and forwarding e-mail on behalf of a registered mail user on that server

NOTE 10: A variant of the mail server is the send mail server (SMTP), which dispatches mail from the user to the e-mail network. The POP usually requires login with a password on the application level, while the SMTP can be used after session or link validation only.

Mediation Function (MF): mechanism which passes information between an access provider or network operator or service provider and a handover interface

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

network operator: 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

Open System Interconnect (OSI) model: model with 7 layers for interconnection of network nodes

NOTE 11: The model implies that nodes are to communicate on equivalent layers, for instance layer 3 (network) to layer 3, or telephone number to IP-address.

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

NOTE 12: Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

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

result of interception: information relating to a target service, including the Content of Communication and Intercept Related Information, which is passed by an access provider or network operator or service provider to an LEA

NOTE 13: Intercept related information shall be provided whether or not call activity is taking place.

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

NOTE 14: The information may be established by an access provider, network operator, a service provider or a network user.

service provider: natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network

NOTE 15: A service provider does not necessarily need to run his own network.

session: period of interaction with an information or communication system during which the user is authenticated and connected to a user identity with certain authorities

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 16: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 17: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

telecommunication service provider: can be a network operator, an access provider or a service provider

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETR 331 [1] and ES 201 158 [2] and the following apply:

AA	Authorizing Authority
AP	Access Provider
ADMF	Administration Function
CC	Contents of Communication
DNS	Domain Name Server
ETR	ETSI Technical Report
GSM	Global System for Mobile communications
HI	Handover Interface
IIF	Internal Intercepting Function
IN	Intelligent Network
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MF	Mediation Function
NWO	NetWork Operator
OSI	Open System Interconnect
PTN	Public Telecommunications Network
PTO	Public Telephony Operator
QoS	Quality of Service
SMF	Service Management Function (in IN)
SMS	GSM Short Message Service
SvP	Service Provider
TCP/IP	Transmission Control Protocol/Internet Protocol
TM	Transport Mechanism
NWO/AP/SvP	Telecommunication Service Provider

4 Common considerations for LI

Please refer to ES 201 671 [3].

Facilities for implementing and invoking functions of Lawful Interception are required to be implemented in telecommunications systems and networks. These networks proliferate in type and connectivity. As global networks merge and integrate, they extend across national borders thereby complicating and compromising, if not invalidating, current concepts of Lawful Interception.

The standard model for Lawful Interception is that it is a purely national requirement. It is justified under the telecommunications and security laws of a single national jurisdiction expressed as a condition of national license, and exercised under legal warrant by the appropriate national authorities on national Public Telecommunications Operators under their jurisdiction.

This model also assumes that such warrants apply uniformly across the entire telecommunications network of the licensed operator, that national gateways form distinct boundaries between domestic network elements (domestic meaning in terms of the national PTO, the Telecommunications Regulator and Law Enforcement Agencies) and extra-jurisdictional network elements, and that mutual conventions for co-operative cross-border LI assistance can be respected.

Given the proliferation of new forms of communications such as satellite, third-generation mobile, Internet (IP) and the various ways in which such systems "plug & play", this "national" regulatory model is becoming outdated. Mobile voice and data communications rely on radio-based elements which incorporate network switching functions, and neither user terminals nor radio base-station systems contain any inherent capability to prevent their radio-modulations from reaching cross-border co-respondents, satellite systems perhaps exemplifying an extreme case.

Under these new circumstances a user may be registered in one country, located in a second, using the network facilities in a third, and communicating with correspondent(s) in fourth, fifth, and so on.

Neither in such networks would it necessarily be sensible for a communication traversing a multiplicity of network elements, e.g. IP datagrams of whatever type, to be the target of interception at each and every one of these networks.

Additionally, the implementation of Public Telecommunications Network (PTN) functions for Lawful Interception should never extend to the incorporation of Law Enforcement Network systems directly into the public network architecture. Rather, the design of the PTN should not extend further than the Mediation functions required to support the buffering of PTN and Law Enforcement networks.

Nor should Lawful Interception or other security functions ever be implemented in such a way as to mediate the delivery of public services on behalf of the PTN.

Consequently an LI Architecture will have to take a broader look at the principles of LI, particularly as they apply in a trans-national telecommunications environment.

Guiding principles:

It must be borne in mind that the Public Telecommunications Network (PTN) is explicitly designed and licensed solely for the provision of telecommunications services to a commercial public market.

To the extent that functions of Lawful interception are required by national law or regulation to be incorporated into a PTN, such functions are secondary and must not intrude on the functionality or performance of the PTN. The design of an LI architecture should not involve fundamental design or architectural **changes** to the PTN.

The proper functioning of Lawful Interception requires network-to-network interworking and mediation between Public Telecommunication Networks and separate Law Enforcement Monitoring Facility (LEMF) networks. The LEMF facilities of a Law Enforcement Agency, complete with handover & handshaking functions connecting to LI Mediation functions and Functions, for reception of Lawful Interception products comprise a private and separate network, whose architecture is beyond the scope and interest of the PTN.

Mediation Functions (MF) required for Lawful interception constitutes a Gateway Device between these two distinct networks. If no protocol conversions or other special measures are required to transform the LI output from the PTN to the LEMF, the mediation function may be transparent, i.e. not implemented in any separate physical node.

It is the responsibility of PTOs to ensure that internal interception functions are implemented in the relevant network nodes and that the delivery requirements for protocols, formats, etc are met. This responsibility is however operational in nature and does not imply a responsibility for technical interconnection.

Protocols, formats, and specifications for the delivery of Lawful Interception products across the MF/LEMF network interface should not of themselves have a constraining influence on PTN design.

Multiple & duplicated interception in a network should be avoided. That is to say that rather than being applied uniformly across a "national" network, interception should be invoked selectively at a subset of nodes in a network. This implies "marking-up" node(s) at which LI is to be invoked for a given target. Such selection of nodes should not be allowed to restrict how a connection can be routed through a network.

Where a network contains nodes in different jurisdictions, each separate jurisdiction should be capable of marking up a target at any **definable set** of nodes within its territory.

Location dependency (of Lawful interception) means that the identity of the requesting jurisdiction necessarily influences the selection of the nodes within the PTN at which Lawful interception is to be effected.

Location dependency of Lawful Interception requires also that information of a target's location should be available at each intercepting network node.

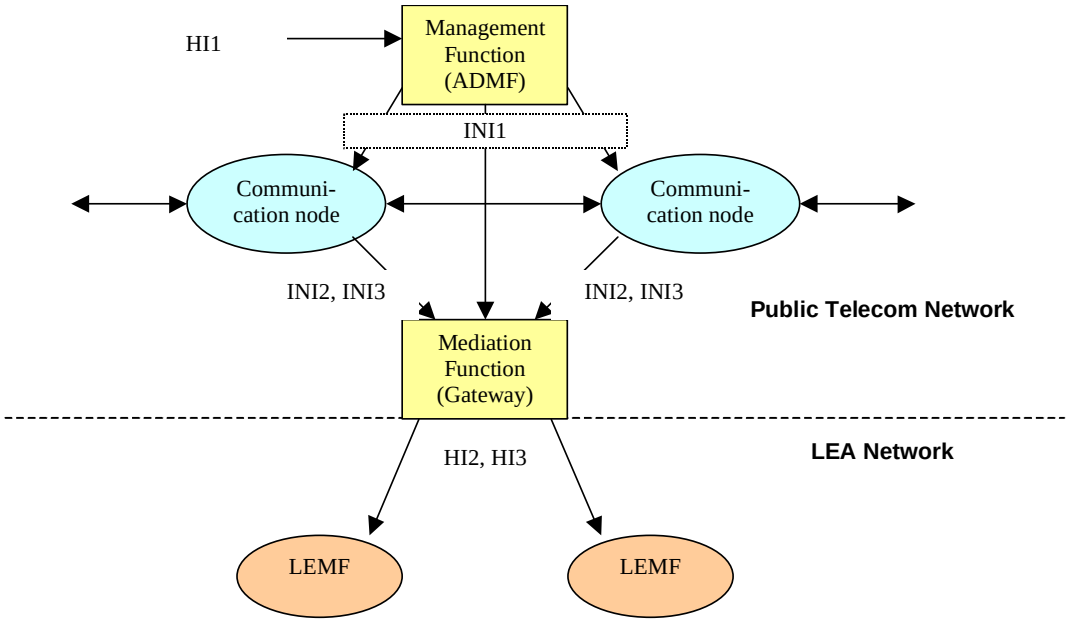


Figure 1: Distinction between public telecommunication networks and law enforcement network

Figure 1 highlights the distinction between the Public Telecommunications Network, which is built and maintained to provide cost-effective and ubiquitous communication for public use, and a network for distribution and processing of Lawful Interception products. This later network is built according to other design principles, for instance with high security and capabilities for preventing loss of data. The interfaces from the PTN are standardized (HI2, HI3), while the internal interfaces within the PTN (INI) are proprietary. The mediation function acts as a gateway from the PTN to the LEA network. There is also a management function (Intercept Control Centre), which receives HI1 data and sends out commands over an INI to set up communication nodes in the PTN and the mediation function to perform interception and send the products to the designated recipients.

5 General design principles

5.1 Design for reusability

One of the most important factors for producing software in a cost-effective way under good quality control is to build it such that it can be re-used for similar applications with different requirements. In order to enhance this, the following main architectural elements are recommended.

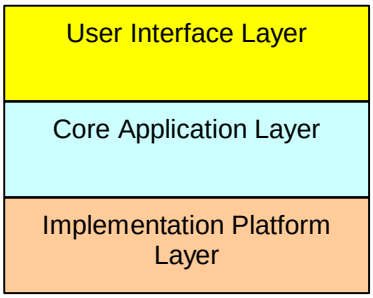


Figure 2: Application layers for re-usable design

The user interface is standardized through the definitions of handover interface channels: HI2 and HI3. Alarms from the LI system towards LEMFs may also be included in the interface towards an LEMF and then as part of HI1. The goal of standardization is to make this interface the same for all vendors and thus enhance competition in the area of LEMF equipment and provisioning of LEA network components.

The core application layer is the Internal Interception Function in the communication nodes and the Mediation Function. The design of this layer is dictated by the needs of LI as an application, independent of user interfaces or implementation platform. It will to a large extent be specific for each manufacturer of communication equipment. It will be expanded as new forms of communication are brought into operation. It will also have to be adapted and verified for new versions of the communication node elements (switches).

The implementation platform layer is the hardware, operating systems (e.g. UNIX) and application frameworks (e.g. real-time kernels) where the LI software runs. As technology moves on, the implementation platforms change. It is desirable to have invariant interfaces from the core application to the underlying platform in order to enhance portability and reduce sensitivity to technology changes.

5.2 LEA interface

This layer exists at the output side of a mediation function. It is the agreed-on protocol and delivery mechanisms of LI products to the LEMF network.

Different technologies and product versions in the PTN will input LI information via interfaces that are more or less specific to the respective technology. If necessary, this information is supposed to be unified in a mediation function, providing a uniform interface to LEMFs. The LEMF side of this interface may include several variants in order to make provisions for different types of LEMF equipment, specifically when migrating to new technology.

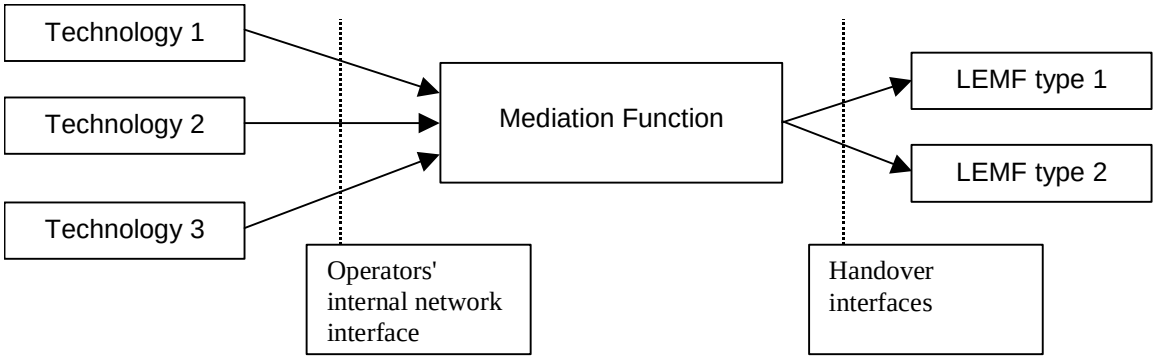


Figure 3: Mediation function for delivery of LI products

5.3 Core application layer

The core application layer in this case is the internal interception function in the PTN nodes. It will contain central algorithms and logic pertaining to the application, regardless of user interfaces and implementation hardware. The core application will be affected by new standards and requirements for how Lawful Interception is to be performed, for instance regarding intercept identities, control of the communication and handling of data. It should however not be affected by changes in user interfaces and implementation platforms.

5.4 Platform layer

The implementation platform is represented by the hardware, networking, application environment and operating system where the Lawful Interception software is implemented. It will change over time as equipment is modernized and software standards evolve. It is important to be able to port applications onto new platforms with a minimum of change, for instance when installations are modernized, but requirements on Lawful Interception stay the same.

6 Actors within the area of Lawful Interception

Lawful interception is based on orders from law enforcement agencies to NWO/AP/SvP for interception of call contents and reporting on communication activities performed by the subject of interception. The actors in this area are:

1) legal establishment (e.g. court of law) that authorizes Lawful Interception;

2) Law Enforcement Agency (LEA) that receives authorization for Lawful Interception from a legal establishment and forwards that as orders for interception to NWO/AP/SvP;

3) subject or target for interception is the person or organization whose communication is intercepted;

4) network operator provides connectivity between nodes in a Public Telecommunication Network (PTN) and has thus access to Contents of Communication;

5) service provider is in charge of the communication services used by the subject. For provision of these services, the provider may need to have cooperation with network operator and access provider;

EXAMPLE: voicemail service

6) access provider gives the subject access to a communication network, either on a per-call basis or semi-permanently.

Traditionally NWO/AP/SvP has been the same entity: the traditional phone company. Communication networks have however evolved such that these roles now may be played by separate entities, for instance a calling-card service provider, an electricity company operating a telecom network and a cable-TV operator providing access for phone calls.

7 Basic architectural elements for LI

The basic elements in an LI architecture are:

1) an Internal Intercept Function (IIF), located in network nodes;

2) a Mediation Function (MF), or gateway, between the Public Telecommunications Network (PTN) and law enforcement monitoring facility (LEMF);

3) an Administrative Function (ADMF) to manage orders for interception in the PTN;

4) an LEA network, including monitoring centers and related law enforcement management functions;

5) an Internal Network Interface (INI) between IIF and MF.

Elements 2 and 5, the MF and INI communication, are the responsibility of network operators.

Element 4, the LEA network, is arranged for by law enforcement agencies (LEAs). This may be done through assignment to NWOs, but the cost and responsibility is to be carried by the LEAs.

In most legislations, element 3, the ADMF, is the responsibility of the telecommunications service provider who is responsible for serving interception orders.

Element 1, the IIF, is to be provisioned through cooperation between NWO/AP/SvP, depending on how the intercepted identity is specified and where Contents of Communication are intercepted.

7.1 Relation to OSI model

The Open System Interconnect (OSI) model can serve as a vehicle for classifying different architectural elements for Lawful Interception. The intercepted identities are related to the OSI layer where they apply. An IP address or telephone number is for instance an identity for layer 3 - network, while an e-mail address relates to layer 7 - application and an ATM channel identity is assigned for layer 2 - link.

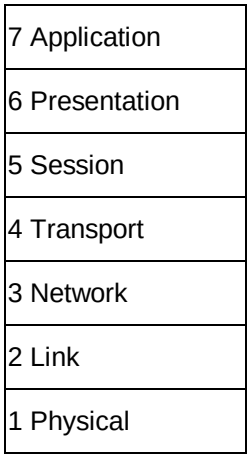


Figure 4: Open System Interconnection layered model

7.2 Services

LI system architecture will also be affected by the kinds of services that are intercepted. Traditionally this is speech only, but modern communication methods and systems have introduced an increasing number of services, which are of interest for interception by law enforcement agencies.

Examples of such services are:

- E-mail;
- Universal Personal Telephony (UPT - an IN service);
- Short messages (e.g. user-to-user in ISDN and SMS for GSM);
- World Wide Web;
- Voicemail servers;
- Satellite telephony;
- Interception on service-related identity.

7.3 Intercepted identities

The telephone number is the traditional identity for interception. With the advent of new types of carriers, like IP telephony, new kinds of identities for interception can also be used. A target identity may be intercepted on different kinds of identities, also simultaneously.

Table 1: Examples of theoretically possible OSI-related identities, though not necessarily available in all networks

OSI level	Identities	Intercepting Node	Comment
Application	e-mail address	Server	
	web address	Domain Name Server	IP Address may also be used
Presentation			
Session	ISP customer id	Server	User-id at login to ISP service
Transport			The intercepting mechanism is not allowed to request error recovery
Network	Telephone number	Switch	
	IP address	Router	Applicable only for permanently assigned IP addresses
Link	ATM channel/path	ATM switch	VPN trunk
Physical	Trunk id		With advanced equipment it may however be possible to analyse traffic on the physical line to extract higher-order identities

Table 2: Other identities for interception, examples

Identity type	Based on	Related to
Geographical location	Geographic area as determined through base station or satellite	Target id
Equipment identity	IMEI for mobile equipment	Target id
	MAC-address (Ethernet)	IP address
Physical connection	Point of connection in network	Subject address
Subscriber id	IMSI number	Target id

These other identities would typically be deduced through observation during interception. A cellular phone user, who is intercepted on his or her telephone address, could also be prompted on the IMEI number of the used mobile equipment, which then in turn could be initiated for interception in order to prevent evasion through change of SIM-cards. In a given surveillance situation, there may be an order to intercept all calls within a certain area. Geographical location will also play a role in determining the juridical validity of an interception, specifically in the case of satellite telephony.

7.4 Example of basic elements of the Internal Interception Function

This clause describes relationships between nodes with abstract layers of services, control and connectivity, as for instance in intelligent networks.

NOTE: The layering shown here relates to an abstract system structure. It does not prescribe (nor preclude) division into separated physical entities. The protocols used for communication between layers may be either according to common standards or proprietary. No generic requirements exist to implement an actual IIF in a layered manner.

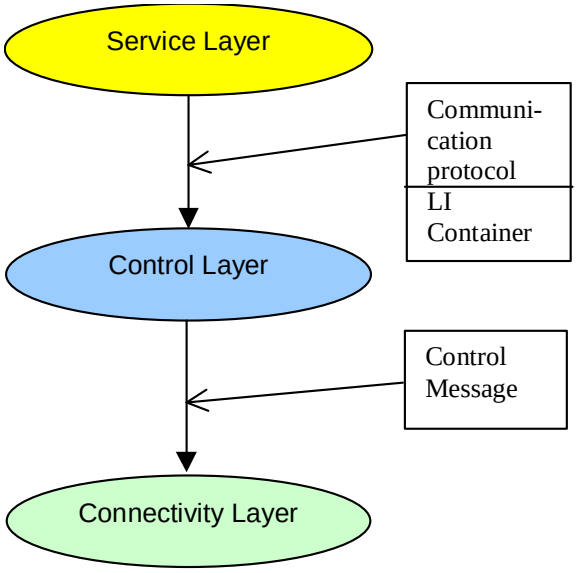


Figure 5: An example of functional layers and LI-specifics in a modern network

In certain technologies the communication in question may be carried over some sort of protocol, for instance INAP for intelligent networks. The service layer is aware of user identity and handles authentication of a user and authorization for use of certain services. The service layer communicates with the control layer. In order to perform Lawful Interception, such a protocol has to be augmented with LI-specific data. The contents of such an LI related message depend on whether target detection is done in the service layer or in the control layer, see below.

The control layer analyses orders for provision of communication services, coming from the service layer. It will also be able to determine how to set up connections. The control layer sends connection orders to the connectivity layer. It is assumed that no LI-specific data need to be transported from the control layer; it should suffice to use regular control messages to set up the communication to the LEMF.

As shown farther down in this text, the control layer, and in some cases the service layer, will be responsible for extracting IRI. The connectivity layer will be required to distribute Contents of Communication to designated LEMF network addresses.

The following informative table illustrates possible functionalities of the abstract architectural elements, relevant for an IIF, and example locations.

Table 3: Other identities for interception, examples

Function	Located in	Role
Management Function	Service Layer and Control Layer	Initiation/termination of interception, report on active interceptions, setup of system parameters (LEMF addresses etc)
Data Extraction	Service Layer	Extract data on subject identities
Target Detection	Service or Control Layer	Analyse subject identities and decide if interception shall be done
Delivery of IRI	Service or Control Layer	Deliver data on communication to LEMF(s)
Setup of Communication Contents Channel	Connectivity Layer in cooperation with Control Layer	Establish connection(s) to LEMF(s) for delivery of Contents of Communication
Delivery of Contents of Communication	Connectivity Layer	Deliver Contents of Communication to LEMF(s)
Service-specific HI2 data (report record)	Service Layer	This kind of data is related to service manipulation, like subscriber services or IN services. For IN services this will be handled by the SMF.

Figure 6 gives an outline of the interrelations in certain networks, for instance IN.

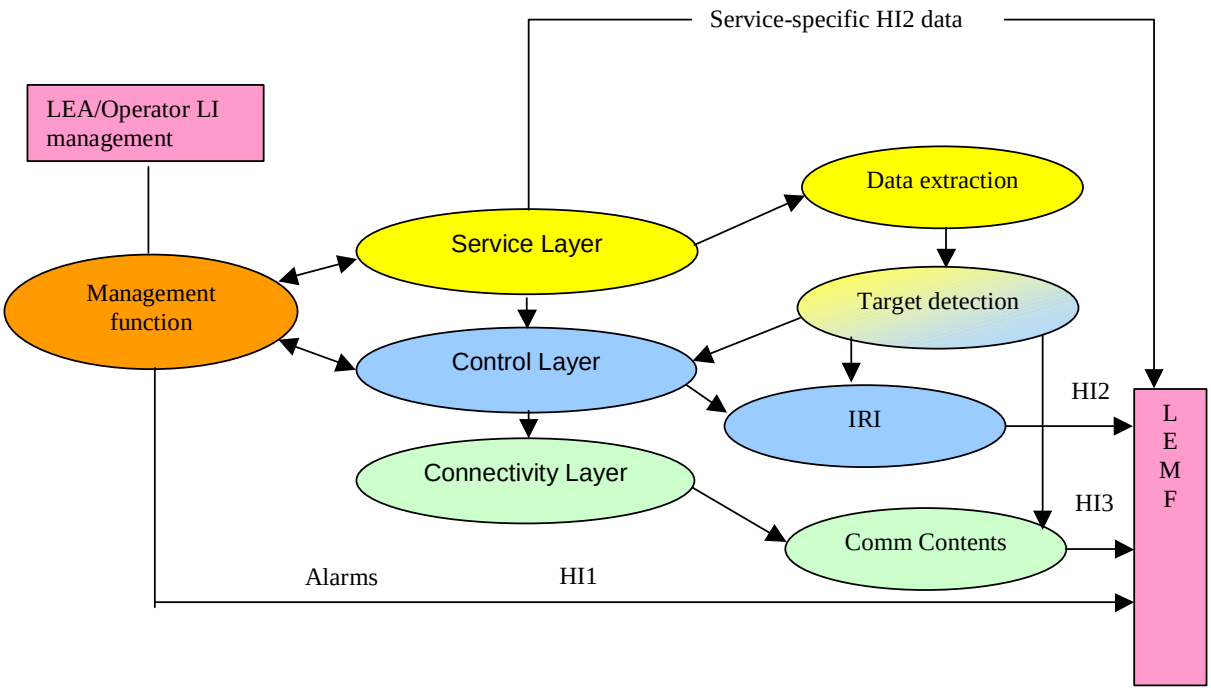


Figure 6: Basic abstract functional elements for Lawful Interception

In this diagram the service-specific HI2 data is shown as going directly from a service layer to an LEMF. It is however likely that it will pass through some sort of mediation function, which might be shared with other delivery channels.

7.5 Target identity data

An important aspect of Lawful Interception is where in the network and how interception subjects are detected. This will depend on the intercepted identity, as identities are visible only in certain parts of the network and at certain stages in a communication. Please refer to clause 7.3 for details on this.

The identity of a subject involved in communication can be established only through that subject's property as a user of a service. This is because it is in the interest of the operator of the communication services to make sure they are protected against unauthorized use and therefore identification and authentication of the users is required. Such authentication is more or less well established. A telephone "user id" is the number itself and it is "authorized" to use the service through physical access to a phone connection. An Internet service user is authenticated through a log-on procedure to an Internet Service Provider (ISP), involving a password. Systems for biometric authentication through voice patterns, fingerprints etc are available and will probably come into more frequent use as secure means of connecting an identity to a person.

In this context it may be appropriate to point out that the concept of a service also may apply to an access. If there for instance is a digital subscriber line network, which may be used for Internet access, that will be the service towards a user. In most cases such an access service has to be backed up by an Internet access at an ISP, in which case the suitable point of interception is at the ISP rather than at a connection point for the digital line access. LI of GPRS traffic is an example of access-based interception, where the Contents of Communication (IP packets) are transferred to the LEMF without relation to any specific service. They may contain voice communication, file transfers, e-mail messages etc, but this is not known at the point of interception.

7.6 Correlation information

Correlation between IRI and CC is necessary in order to permit a unique matching between these two sets of information. The correlation information on the HI3 channel consists of a set of identifiers related to the interception event. These identifiers are used to match the recorded Contents of Communication with the corresponding IRI.

The correlation information is transported to the LEMF using standard protocols, by use of elements that are accessed only by the originating (IIF/MF) and terminating (LEMF) entities. This information is transmitted transparently across other protocols that may be used for setting up connections to LEMFs.

EXAMPLE: Some ISDN subaddress fields are used to send the correlation information. These fields will be filled in by the IIF when the ISDN connection is set up. They do not however affect any intermediary nodes in the connection path.

Correlation may also for example be arranged for by assigning a unique CC delivery address for each interception case. That address would be referred to in the IRI.

7.7 Example of communication between layers

Depending on where target detection is done, different sets of data will be sent between the layers for service, control and connectivity. The service layer provides identification of the user and may also perform triggering against a list of users to be intercepted. The control layer prepares and sends off HI2 data (IRI) to the LEMF(s) and orders the connectivity layer to set up delivery of Contents of Communication, if required. The communication layer copies the Contents of Communication and sends that to the designated LEMF(s). The HI2 data may be delivered through a separate data port or using the communication mechanisms provided through the connectivity layer.

7.7.1 Target detection in service layer

The service layer of a communication system may be aware of user id. If the target detection is located there, the data for distribution to LEMFs will have to be sent to the lower layers of control and connectivity. The control layer will not have any prior knowledge of who to intercept, so all information relating to the interception order (HI1 interface) will have to be provided from the service layer.

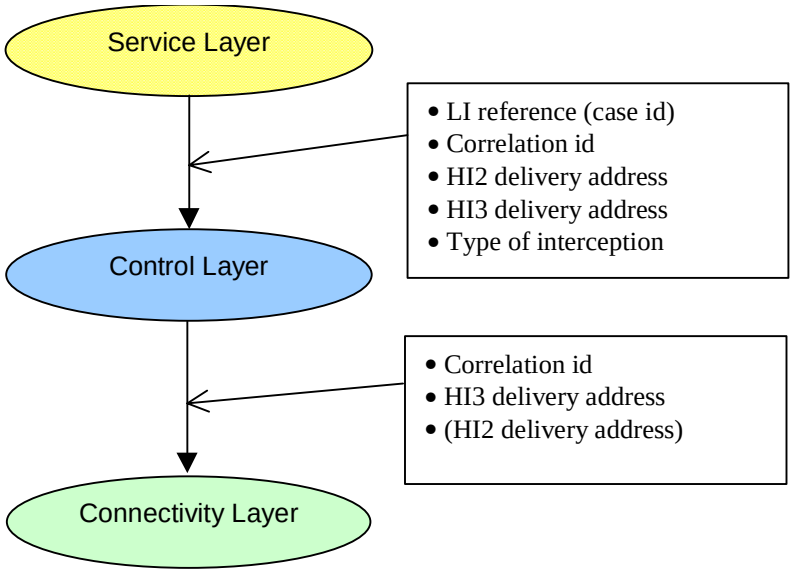


Figure 7: Target detection in service layer

Since detailed data about intercepted users is kept in the service layer, this equipment has to be secured against unauthorized access. The communication link from the service layer to the control layer also has to be secured, for instance with encryption.

7.7.2 Target detection in control layer

In this case the communication between layers will be much simpler, since target detection and assembly of IRI to be sent to LEMF(s) is contained within the control layer.

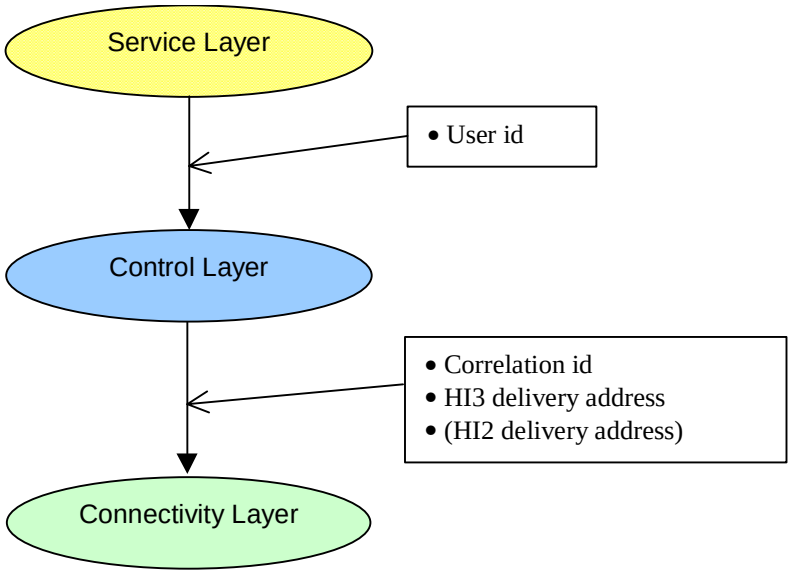


Figure 8: Target detection in control layer

7.7.3 Discussion of options

Target detection in the service layer has the advantage of a possible concentration of interception data to relatively few nodes. The control nodes will also be fairly simple. Only a limited set of mechanisms for processing LI information will be needed there. Security issues do however need to be considered carefully and the cost for implementing and maintaining the necessary security level weighed against the savings in reduced complexity.

Target detection in the control layer relieves the service layer from security requirements, if all user id's are sent for analysis, since the service layer would then not have to be built to safeguard any LI information against unauthorized access. The action of sending all user ids would not increase load on processing nor transmission in any significant degree.

The choice of where to locate triggering will in most cases be based on overall architectural properties. In an intelligent network with many IN service providers connected to a backbone switching network, it is probably better to place triggering in the switches (control), since it will be difficult to have all the IN SCPs built with the necessary security arrangements (secure SDFs) and secure the INAP links. In an IP-based network with many routers and a few service nodes (for instance domain name servers), it is probably better to have triggering in the service layer.

7.8 Use of a special delivery node

In some cases it is suitable to have a special node type for delivery to the LEMFs. This will unburden the common nodes from having to implement all the functionality necessary for that; it will suffice to do only triggering in the intercepting node and then send the triggered-on traffic along a detour. This may be motivated in for instance a network where the majority of the nodes allow only rudimentary interception functions or where it would be too expensive to implement full IIF functionality everywhere. This kind of setup requires that an interception is initiated in at least two places: the triggering node and the delivery node.

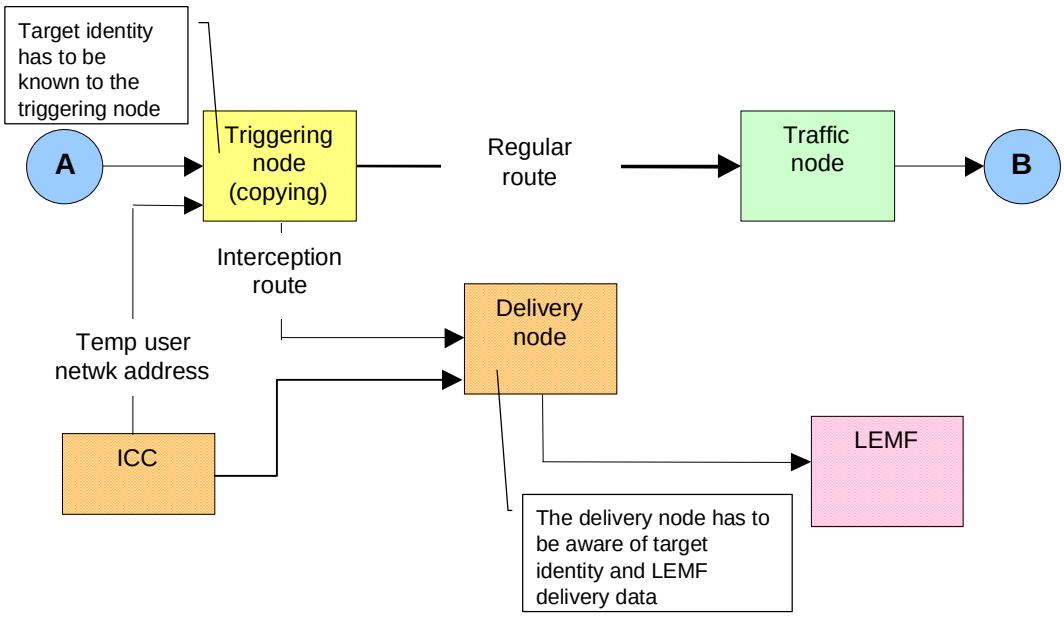


Figure 9: The Delivery Node will contain target identity information and LEMF delivery data, while the triggering node will contain only target identity information

8 Inter-network communication for LI

8.1 Separate LEA network

As discussed in clause 4, there is a separate network for transmission of LI information. This network will have provisions for transmission of data across HI2, HI3 and possibly also the HI1 interface.

The lower levels of the HI2 interface to the LEA network can be chosen freely and may be dictated by national regulations. It is likely that TCP/IP or UDP/IP will be the transmission method of choice. The presentation layer is according to ES 201 671 [3], i.e. ASN.1/BER. The application layer protocols are specified to be ROSE or FTP, but there may be national variations to this. The picture below shows some alternative implementations of an LI protocol stack in the LEMF.

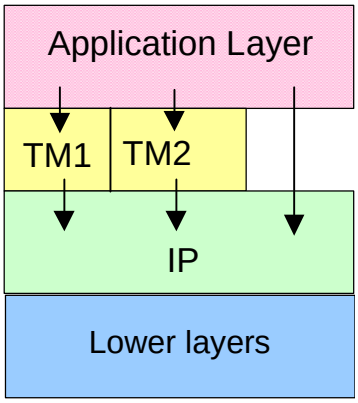


Figure 10: Protocol stacks for LEA network

For the contents delivery from the intercepting node to the LEMF there must be application-level protocols. This is because the delivery must be isolated from the regular communication to prevent that any backwards communication would be sent from the LEMF to the intercepted party, like for instance requests to re-send. In this figure, no statement is made about the presentation layer. This will be affected by the degree of knowledge about the kind of communication being intercepted. If for instance voice over IP contents are being sent to the LEMF, there should be provisions for decoding that kind of traffic. If the kind of traffic is not known, as for instance when a stream of IP packets is intercepted at a modem connection or associated ISP user account, the contents will be transmitted transparently as a bit stream or stream of IP packages etc to be decoded in the LEMF. Initiation messages in the communication may possibly be used by the LEMF to conclude what kind of application the subsequent payload information relates to.

8.2 Termination, triggering and transmission

Figure 11 shows how a communication stream is terminated in an intercepting node. The IIF Application in this figure represents a combination of the triggering node and the delivery node shown in figure 7. At initiation, the stream is sent to the IIF to determine whether interception is to be done. If this is not the case, the IIF will be bypassed for the remainder of the communication. Intercepted communication will have to continue passing through the IIF to allow for capturing of LI-related events, which occur during the communication session.

If the protocol termination is made at OSI level "K", the IIF will be able to trigger on identities related to level "K" or lower levels. If for instance the IIF is set up to capture a certain IP-address, the protocol has to be terminated at OSI layer 3 or higher. An IP-terminated stream, for instance, may also be caught by doing interception at the link layer, for instance on a certain ATM channel, which carries the related IP stream. Interception at the link layer will of course catch also all other network connections through that link. It will then be up to the LEMF to separate out the communication related to the targeted IP-address. This is not legal in all countries, so it is important to make informed decisions about design and allocation of mechanisms for interception.

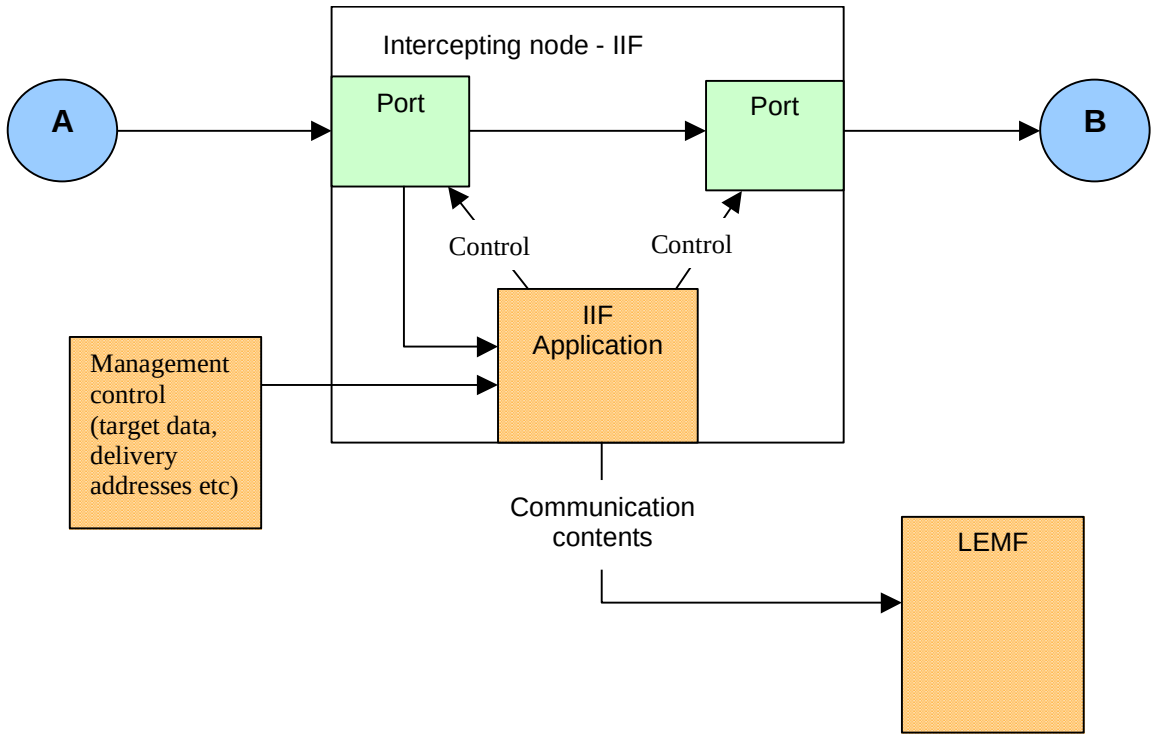


Figure 11: Interception of a communication stream and transmission of contents to LEMF

The lower the level of interception is, the more work has to be performed by the LEMF to "understand" the contents. If for instance an ATM channel is intercepted, the LEMF will be faced with a task similar to decryption to find out what is being communicated.

The reasoning above is perhaps a bit hypothetical, since interception is based on a service and thus usually relates to an application layer. Only rarely will the interception be triggered by a low-level identity such as IP address or ATM channel. It is however important to be aware of the fact that looking for higher-level identities in a communication stream is a formidable task that requires special equipment and tends to impact the throughput.

8.3 Communication between networks performing Lawful Interception

At this stage in the development of Lawful Interception standards, it is not expected that any mechanisms will support propagation of LI related messages between networks. This would relate for instance to the case where a telephony server is located in one country, while access and switching nodes are in another country. Any interception orders have to be handled in the country where the subject is located. It is not conceivable that the remote telephony server would contain for instance triggering information and send an LI related message across an international border to a switching node.

Two special cases may deserve to be discussed here. The first is the case where traffic passes from a private domain into a public domain. Say for instance that there is a neighbourhood network within some community, which is classified as private. A calling B within that network would not be interceptable, even if A is a target for interception. If A however calls a subscriber C in the Public Telecommunications Network, the call would be interceptable. Therefore the gateway between the private and the public network would need to be equipped for Lawful Interception.

The second case relates to international police co-operation. The mobility of criminal activities across borders makes it necessary for LEAs to have mutual assistance in preventing and detecting crime. There is however an issue of national sovereignty in this case. One country will be reluctant to allow the police of another country to perform unrestricted phone tapping in its area of jurisdiction. Some sort of gateway arrangement will probably be necessary in order to define a distinct point of delivery between the countries. This is really not an issue for an NWO/AP/SvP, but should be handled within the LEMF network communicating with another LEMF network. At the time of writing (1st quarter 2001) there are neither clear rules nor agreements relating to LI within the area of mutual legal assistance between countries.

8.4 Quality of Service in LEA network

The general rule is that QoS in the LEA network must be at least as good as the QoS for the intercepted traffic. If for instance a high-speed data channel is being intercepted, it will not do to try to send that to an LEA network built for interception of voice traffic. Likewise the LEA network needs to provide a high degree of reliability in order to minimize the risk of losing interception products.

Table 4: Survey of QoS related to different layers in the OSI model

OSI level	QoS Considerations
1 and 2: Physical/link	The transmission capacity for the LEA network must be sufficient to handle the intercepted traffic. Occasional bursts may be compensated for through buffering. The adequate security provisions are to be made, according to requirements (for instance separate physical connections and/or encryption at link level).
3 and 4: Network/transport	The LEA network must be able to communicate with the delivery function. The adequate security provisions are to be made, according to requirements (for instance encryption at network level).
5: Session	The delivery function must be able to establish a session with the LEMF(s) and with adequate security in terms of data integrity and authentication of endpoints.
6: Presentation	The LEMF must be capable of interpreting the presentation format of the delivery function.
7: Application	The LEMF must be capable of running an application to assemble and process the interception products (IRI and CC).

8.5 Buffering of the Result of Interception

8.5.1 General

There is a conflict between a requirement to buffer Intercept Related Information (IRI) or Contents of Communication (CC) and the requirement that an operator *must not permanently* store such information. In the definition clause above, it is stated that buffering is a temporary measure, taken when the connection to an LEMF is temporarily unavailable. There will therefore be limits on buffer sizes and for how long a buffer is kept. If these limits are exceeded due to a longer outage of the LEA network and/or LEMF(s), interception products will be lost.

It must also be clearly understood that any buffering outside of what is regular practice for the protocols used is to be regarded as part of LI activities and not as requirements on the public telephony service.

8.5.2 Buffering of IRI

Intercept related information can be buffered in protocol stacks in transmission from the IIF to the LEMF. It is a tuning issue to set up communication parameters to obtain suitable buffer sizes. If extra buffering, outside of the scope and capacity of regular data networks is needed, this may be handled in a mediation function for the HI2 channel.

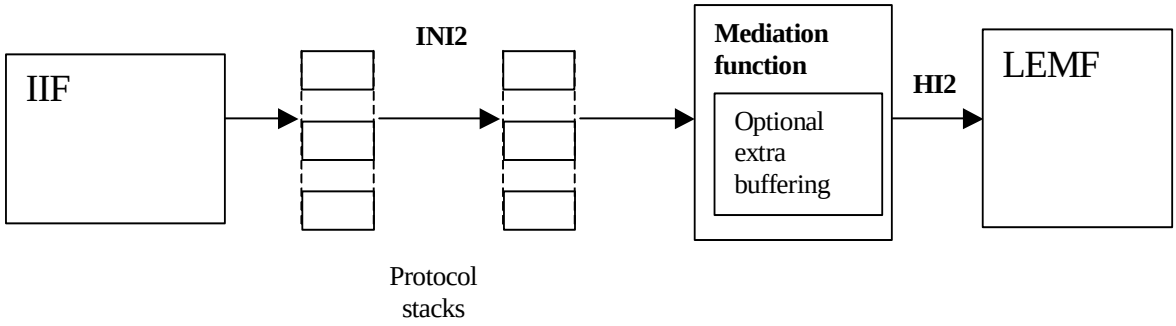


Figure 12: Buffering of IRI in protocol stacks (the HI2 link will also contain buffering stacks)

8.5.3 Buffering of Content of Communication

The Content of Communication for Lawful Interception is not buffered in the network. If there are requirements for buffering, this is to be done in a mediation function for the HI3 channel. It should be observed that for packet data communication, buffering may be offered through the mechanisms of protocol stacks.

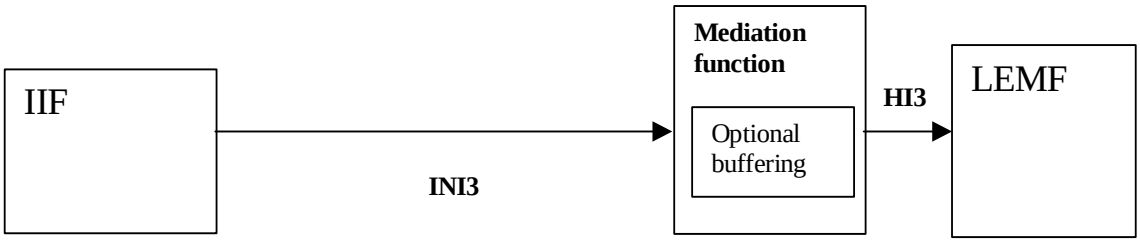


Figure 13: Optional buffering of Content of Communication in mediation function

9 Hand-Over interfaces

9.1 HI1 - Administration

The administration interface will have to be standardized towards the authorities that issue orders for interception, in order for the interception management to work smoothly. National laws will have provisions for this. The HI1 interface is often paper-based, but it can be anticipated that electronic transfer of data and automated activation/deactivation of interceptions will become more common in the future. There is also a need to find a standard for translation between external HI1 protocols and the internal network interfaces towards vendor-specific equipment. Many operators use equipment from several vendors and it is in their interest to be able to handle this in a uniform way, through a common management system. There is also a technology aspect of bridging different types of nodes to initiate interception of several types of communication, like telephony and IP, for a certain subject. This calls for compatibility between INIs of different manufacturers.

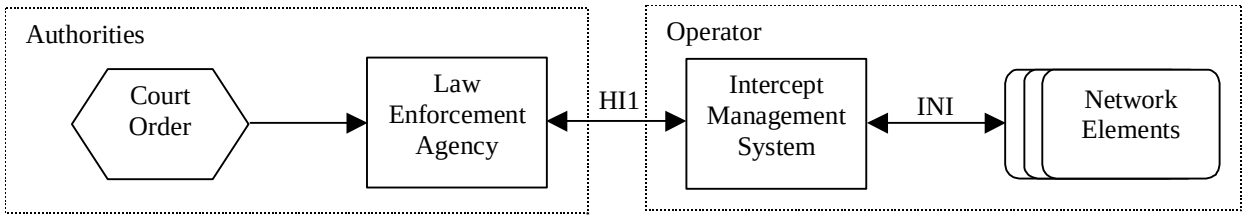


Figure 14: Information flow through HI1 interface

For certain types of interception, for instance cellular telephony or universal personal telephony (UPT), it may be necessary to perform a network-wide initialization of interception. This is due to the fact that it cannot be known in which switch the communication will be initiated. An alternative approach could be to initialize interception in a central service node, like a Home Location Register (HLR) or Service Control Point (SCP) and let these nodes perform target detection. This does however involve some security issues, as discussed above, since HLRs and SCPs are much more open to access than switching nodes are. Also the cost of having to implement LI functions in a larger number of different types of equipment needs to be considered.

9.2 HI2 - Intercept Related Information

IRI is sent to the LEMF as a result of LI-related events in the communication. Such events may also lead to establishment or disconnection of a content delivery channel on the HI3 interface.

The IRI would need to be collected from multiple nodes for a given communication, since several functional entities are involved in handling the communication. This collection may have to be made across several types of nodes, like access nodes, switching nodes and service nodes. It may also cross different boundaries - between operators, between types of vendor equipment, across national borders.

The following diagram with a functional role model, which is derived from ES 201 158 [2] LI Requirements for Network Functions, shows how entities interact.

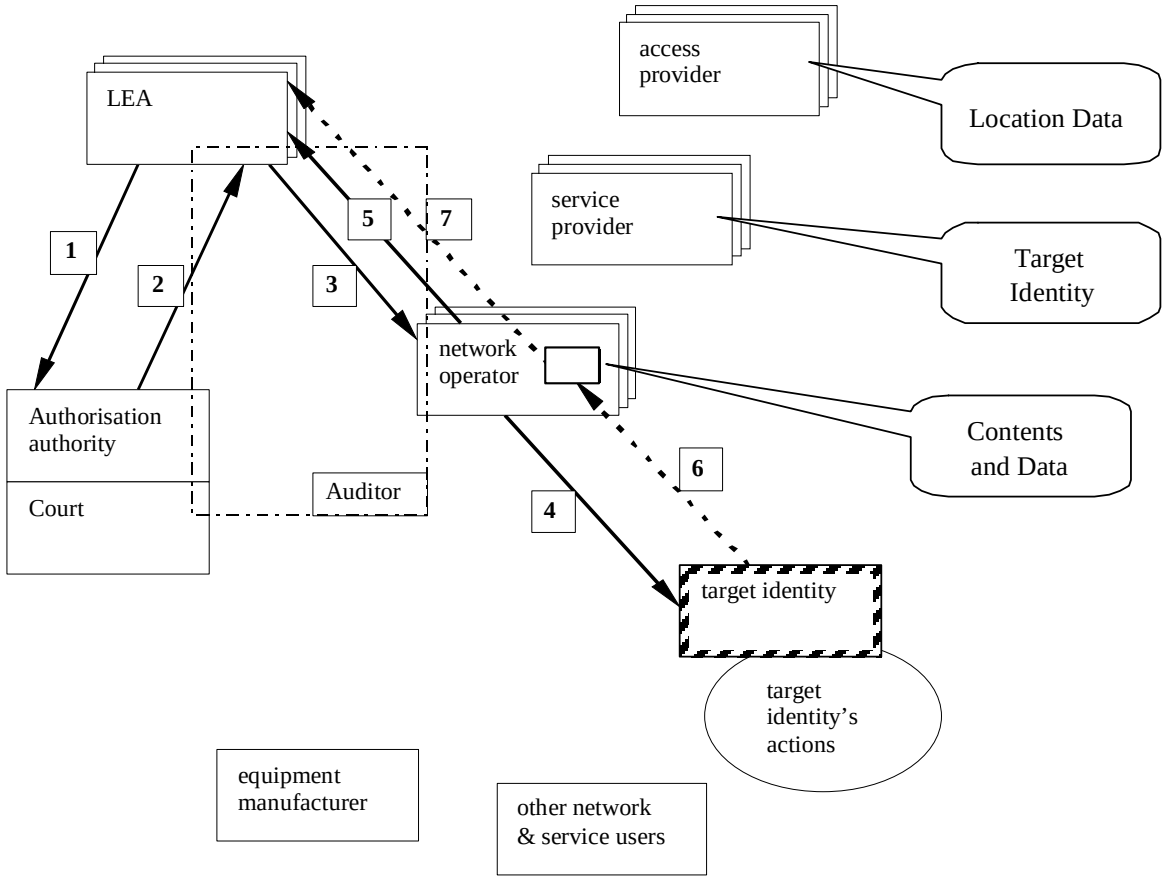


Figure 15: Functional and role model for interception

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.

9.3 HI3 - Contents of Communication

Delivery of call contents is initiated and discontinued based on specific LI-related events in the communication.

The communication contents data stream will correspond to the intercepted identity. If for instance an e-mail address is used as target for interception, the contents will be delivered to the LEMF as e-mail. If the interception triggers on ATM channel identity, an ATM data stream will be delivered.

The call contents would have to be obtained from a single point of interception, unless multiple interceptions of the same call are to be accepted (for instance intercepting both on a UPT number and the routed-to actual number).

10 Security

10.1 Threat model

This clause about security is an ad-hoc discussion about threats to the integrity of an LI system. In ETR 332 [4] on security there is a systematic approach to analysis of threats and security. The following types of threats are listed there:

1) impersonation;
2) masquerade of communicating parties and entities;
3) identity interception;
4) password interception;
5) data interception of signalling and user data;
6) replay of signalling and user data unauthorized copying;
7) modification and violation of data;
8) access right manipulation;
9) misuse of access rights;
10) denial of service;
11) denial of sending respectively authorship (repudiation);
12) denial of receipt access control;
13) installation of intentional malfunction;
14) sabotage.

In this discussion about security of LI systems, the following types of threats are considered:

3) identity interception;
4) password interception;
5) data interception of signalling and user data;
7) modification and violation of data;
8) access right manipulation;
9) misuse of access rights;
10) denial of service;
13) installation of intentional malfunction;
14) sabotage.

The discussion is based on suggested arrangements to counteract these threats. A more thorough analysis, where severity of threats is considered, should be done on a national and network basis.

10.2 Securing against unauthorized access

Threat types: 3, 4, 5, 8, 9, 14.

There are always concerns about unauthorized access and manipulation of interception services. This could be both hostile interference or interference through curiosity (hacking). The related transactions and commands have to be protected, for instance through encryption and passwords. It should be satisfactory to use standard procedures for this, like IPSEC.

It is important to be able to audit interception activities, however without leaving audit trails that may be accessible to unauthorized personnel. In a network where interception data are distributed between different nodes, it is necessary to have some sort of synchronization mechanism to check for inconsistencies. That would also reveal and make it possible to act against unauthorized interception.

10.3 Information hiding

Threat types: 3, 5, 14.

Modern system design involves concepts like "information hiding", where each module keeps a set of "private" data that are not accessible to the outside world. A global system, like Lawful Interception, will tend to break this rule of information hiding. If LI is added to an already existing system solution, re-design will be needed in order to give the LI system access to all the data and control mechanisms it needs. The solution to this may be to define a generic type of interface with a minimal set of data and control parameters for LI to meet basic requirements. That kind of interface would be included as a requirement for all systems to match, as appropriate considering their respective roles in the communication. This type of generic LI interface has to include provisions for security.

10.4 Security activities

Table 5: Threat types vs security activities

Activity	Related threat types
Screening of personnel	5, 8, 9, 13, 14
Restricting access to LI facilities	3, 4, 5, 8
Authentication of LI system operators	8, 9
Auditing of LI activities	8, 9
Alarms for irregular behaviour	8, 9
Make interception function non-detectable in the systems	3, 4, 5, 13
Hide LI data in protocols and memory images	3, 4, 5, 13
Secure any backups of LI data against unauthorized access	3, 4, 5, 13
Make LI data communication resilient to interception	3, 4, 5, 13
Prevent denial-of-service attacks	10
Prevent forging of interception products (distortions)	7, 13

The following figure shows an example of how these activities would apply to the different elements of an interception systems. Since the LEA and the LEMF are under government control, it is assumed that adequate security measures are observed for them. Please observe that the Mediation Functions (MF) may be transparent, i.e. no specific equipment would be required for them.

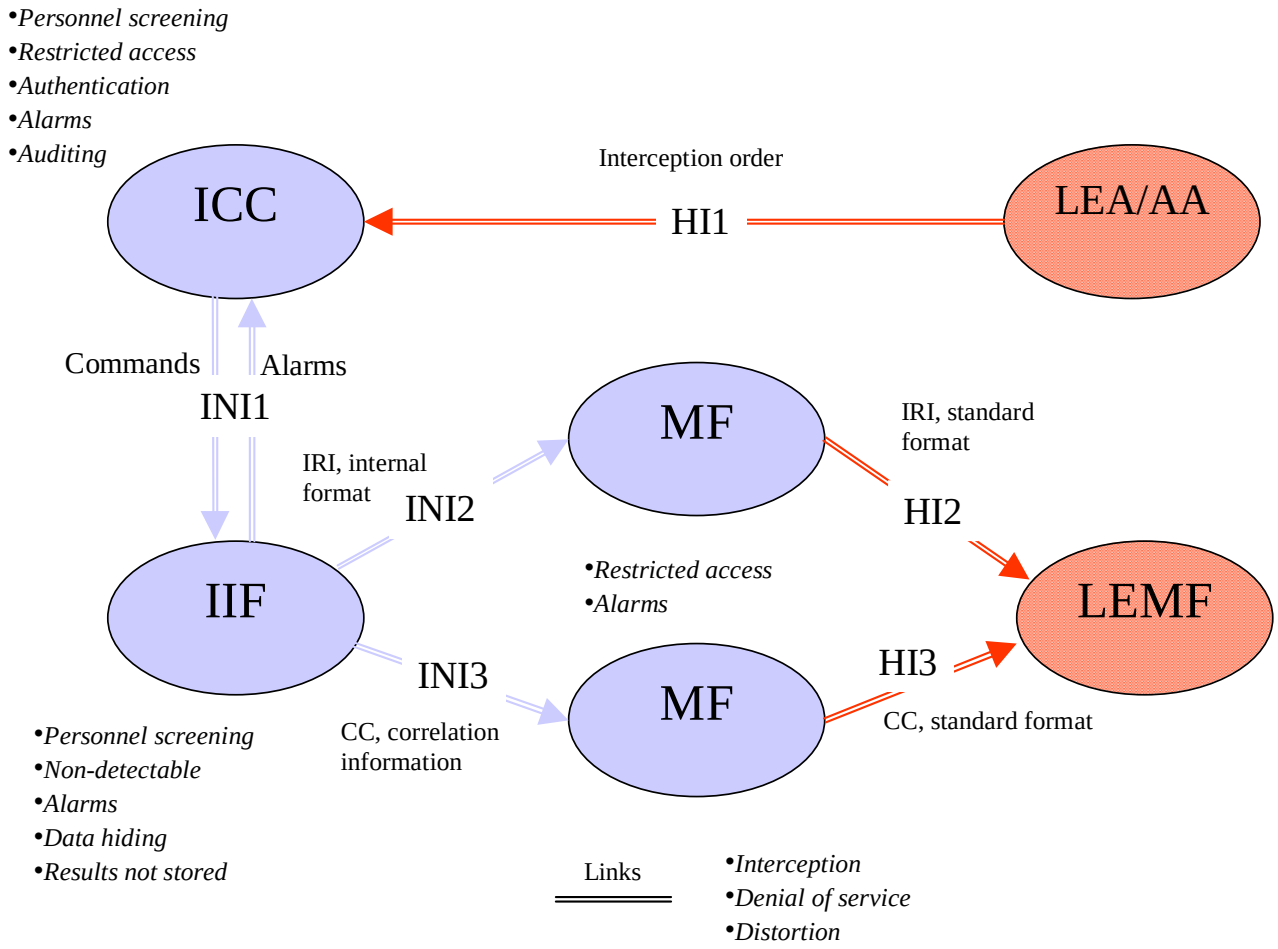


Figure 16: Example of Threat Model

History

Document history		
V1.1.1	July 2001	Publication