

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



Reference

RTR/LI-00040

Keywords

architecture, data, IP, Lawful Interception,
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

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2006.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights	4
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
3 Definitions and abbreviations.....	6
3.1 Definitions	6
3.2 Abbreviations	9
4 Overview of LI requirements and standards	10
4.1 General	10
4.1.1 National adaptations	10
4.1.2 Influence from new forms of telecommunication	10
4.1.3 Guiding principles	11
4.2 Internationally based requirements.....	14
4.3 Characteristics of national requirements	14
4.3.1 General.....	14
4.3.2 Migration from legacy technology.....	14
4.3.3 National parameters	15
4.3.4 Security	15
4.3.5 Protocols	15
4.4 Requirement implementation process	15
4.5 Overview of LI standards	16
5 Interception of communication services.....	18
5.1 General	18
5.1.1 LI requirements related to services	18
5.1.2 Migration to separate service platforms.....	18
5.1.3 Layered model related to LI functions	19
5.2 Access services.....	19
5.3 Communication application services	21
5.4 Intelligent network services.....	22
6 Interfaces	23
6.1 General	23
6.2 Internal interfaces	23
6.3 Handover interfaces.....	24
6.4 Interface protocols	25
6.5 Mapping IRI from PS Contents	25
7 Security.....	26
7.1 General	26
7.2 Threat model	27
7.3 System security	28
7.3.1 Encryption of stored data.....	28
7.3.2 Logical access control.....	28
7.3.3 Physical access control	28
7.4 Interface and link security	29
7.4.1 Protection of transmitted data	29
7.4.2 Management of keys.....	29
7.4.3 Use of leased lines	29
Annex A: Change Request History	30
History	31

Intellectual Property Rights

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

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

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

Introduction

The present document is an overview description of various aspects of lawful interception requirements, relations to communication services, interface technology and security. The present document is intended to serve as a guide that covers some practical issues regarding implementation of LI systems.

1 Scope

The present document provides a high-level informative overview and principles regarding implementation of LI for telecommunications. Details about these principles is covered in other documents that address specific technologies and network types.

The following areas are covered here:

- A general discussion about the role and position of Lawful Interception related to public communication services.
- Origin of LI requirements - overview of characteristics of national legislation and regulations as well as international cooperation on LI.
- A high-level description of LI related to an abstract model of communications systems (service/control/connectivity layers).
- Discussion of interception at access service level versus application service.
- Discussion of interception of IN services.
- Overview of issues regarding interception of IP traffic.
- Description of internal interfaces and internal network units involved in LI processing.
- Description of handover interfaces and interface protocols with some practical hints regarding implementation choices.
- Discussion about security issues, related to the standard threat model described in ETR 332 [4].

2 References

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

- [1] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".
- [2] ETSI ES 201 158: "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".
- [3] Void.
- [4] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".
- [5] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the Lawful Interception of telecommunications traffic".

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

- [6] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 Release 6)".
- [7] ETSI TS 102 232: "Lawful Interception (LI); Handover specification for IP delivery" (will be re-issued with the designation TS 102 232-1).
- [8] ETSI TS 102 234: "Lawful Interception (LI); Service-specific details for internet access services" (will be re-issued with the designation TS 102 232-3).
- [9] IETF RFC 3924: "Cisco Architecture for Lawful Intercept in IP Networks".

- [10] ETSI EG 201 781: "Intelligent Network (IN); Lawful interception".
- [11] EU Council ETS 185: "Convention on Cybercrime", 23.XI.2001.
- [12] ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".
- [13] ETSI TS 133 106: "Universal Mobile Telecommunications System (UMTS); Lawful interception requirements (3GPP TS 33.106)".
- [14] ETSI TS 102 227: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception".
- [15] ETSI TS 102 815: "Service-specific details for Layer 2 Lawful Interception" (will be re-issued with the designation TS 102 232-4).
- [16] ETSI TR 102 528: "Lawful Interception (LI) Architecture for IP Networks within a Communication Service Provider's domain".
- [17] ETSI TS 101 909-20: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception".
- [18] ETSI TR 102 053: "Telecommunications security; Lawful Interception (LI); Notes on ISDN lawful interception functionality".
- [19] ETSI TS 102 233: "Lawful Interception (LI); Service specific details for E-mail services" (will be re-issued with the designation TS 102 232-2).
- [20] ETSI EN 301 040: "Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface".
- [21] ETSI TR 101 514: "Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (GSM 01.33)".
- [22] ETSI TS 101 507: "Digital cellular telecommunications system (Phase 2+); Lawful interception - Stage 1 (GSM 02.33)".
- [23] ETSI TS 101 509: "Digital cellular telecommunications system (Phase 2+) (GSM); Lawful interception; Stage 2 (3GPP TS 03.33)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 331 [1], ES 201 158 [2] and the following apply:

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

NOTE 1: This definition applies specifically for the present document. In a particular case, the access provider and network operator may be a common commercial entity.

NOTE 2: The definitions from TS 101 331 [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: This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Domain Name System (DNS): set of network elements, which function as translators between logical names and network addresses on the Internet

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

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 (CC) and Intercept Related Information is provided

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

interception measure: technical measure that 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 (INI): 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: 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 a LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a AP/NWO/SvP

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

LI products: The same as **result of interception**.

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: 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: 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. For the Internet a 5-layer model is more commonly applied, where the OSI layers 5 to 7 are collapsed into a common layer called "application".

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

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

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

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

NOTE: According to law enforcement requirements, intercept related information shall be provided whether or not call activity is taking place.

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

NOTE: The information may be established by 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: 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 used by the interception subject

target identification: identity that 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.

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, photo electronic 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 TS 101 331 [1], ES 201 158 [2] and the following apply:

AAA	Authentication, Authorization and Accounting
ADMF	ADMInistration Function
AP	Access Provider
CALEA	Communications Assistance for Law Enforcement Act (USA)
CC IIF	CC Internal Interception Function
CC	Contents of Communication
CS	Circuit Switched
DF	Delivery Function (delivery to LEMFs)
DNS	Domain Name System
ETR	ETSI Technical Report
EU	European Union
FTP	File Transfer Protocol
GSM	Global System for Mobile communications
HI	Handover Interface
IIF	Internal Intercepting Function
IKE	Internet Key Exchange (protocol)
IN	Intelligent Network
INI	Internal Network Interface
IP	Internet Protocol
IPSEC	IP Security (protocol)
IRI IIF	IRI Internal Interception Function
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IUR	International User Requirements (on lawful interception)
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MF	Mediation Function
NGN	New Generation Networks
NWO	NetWork Operator
OSI	Open System Interconnect
POTS	Plain Old Telephone Service
PS	Packet Switched
PTN	Public Telecommunications Network
PTO	Public Telephony Operator
QoS	Quality of Service
SCF	Service Control Function (in IN)
SCI	Subscriber Controlled Input
SNMP	Simple Network Management Protocol
SSF	Service Switching Function (in IN)
SvP	Service Provider
TLV	Type-Length-Value (encoding)

TSP	Telecommunication Service Provider
VPN	Virtual Private Network (encrypted communication)
XML	eXtended Markup Language

4 Overview of LI requirements and standards

4.1 General

4.1.1 National adaptations

Each country is in sovereign control over which requirements on LI are imposed in the national legislature. It is however recommended to keep specific national requirements to a minimum for two main reasons:

- Cost and time, since special adaptation of LI systems that are built to comply with commonly accepted international requirements will be costly and cause delays.
- Mutual legal assistance, since it will become difficult and costly to handle delivery of LI results between countries, if their format and the scope differs widely between countries.

4.1.2 Influence from new forms of telecommunication

Facilities for implementing and invoking functions of Lawful Interception are required to be implemented in telecommunications systems and networks. As global networks merge and integrate, they will extend across national borders, thereby complicating 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 and 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 LI Architecture will have to take a broader look at the principles of LI, particularly as they apply in a trans-national telecommunications environment.

4.1.3 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 should not intrude on the functionality or performance of the PTN. The design of 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 monitoring facilities of a Law Enforcement Agency, complete with handover and handshaking functions connecting to MF/DF for reception of Lawful Interception products comprise a private and separate network, whose architecture is beyond the scope and interest of the PTN.

Mediation and Delivery Functions (MF/DF) required for Lawful interception constitute Gateway Devices 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 MF/DF may be transparent, i.e. not implemented in any separate physical node.

It is the responsibility of TSPs 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 and 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.

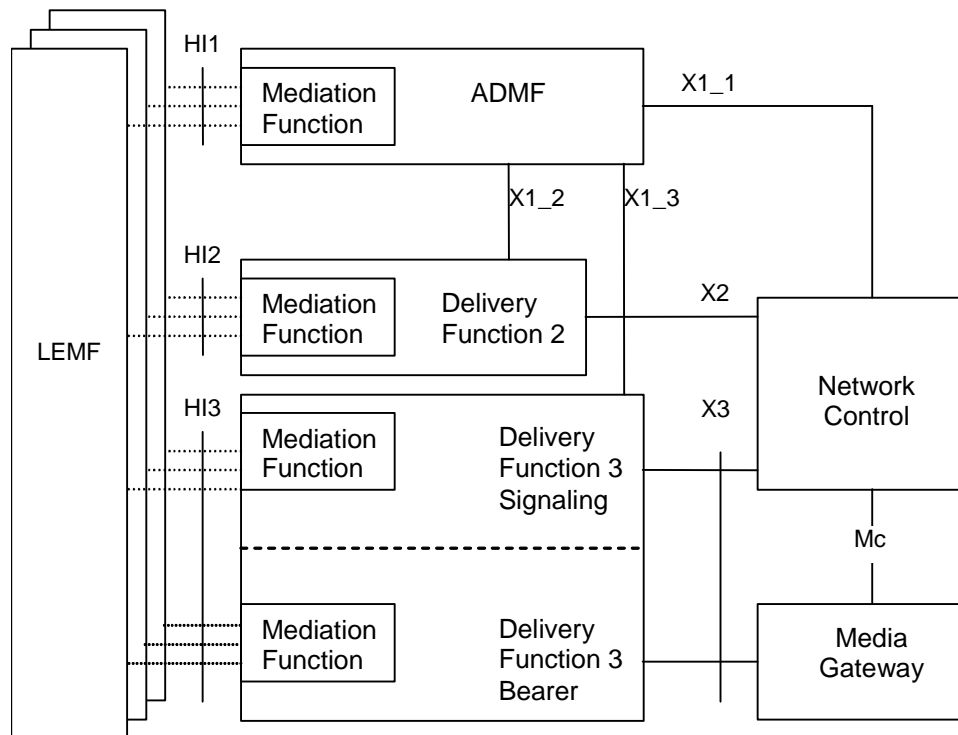


Figure 1: Reference model for LI system

Figure 1 (see TS 133 107 [12]) shows a standard reference model for LI. The interfaces from the PTN are standardized (HI2, HI3), while the internal interfaces within the PTN (X1, X2, X3) are proprietary. The mediation function acts as a gateway from the PTN to the LEA network. There is also a management function (ADMF), which receives HI1 data and sends out commands over X1 to set up communication nodes in the PTN and the LI System MF/DF to perform interception and send the products to the designated recipients.

For IP systems a slightly different model has been introduced (see TR 102 528 [16]).

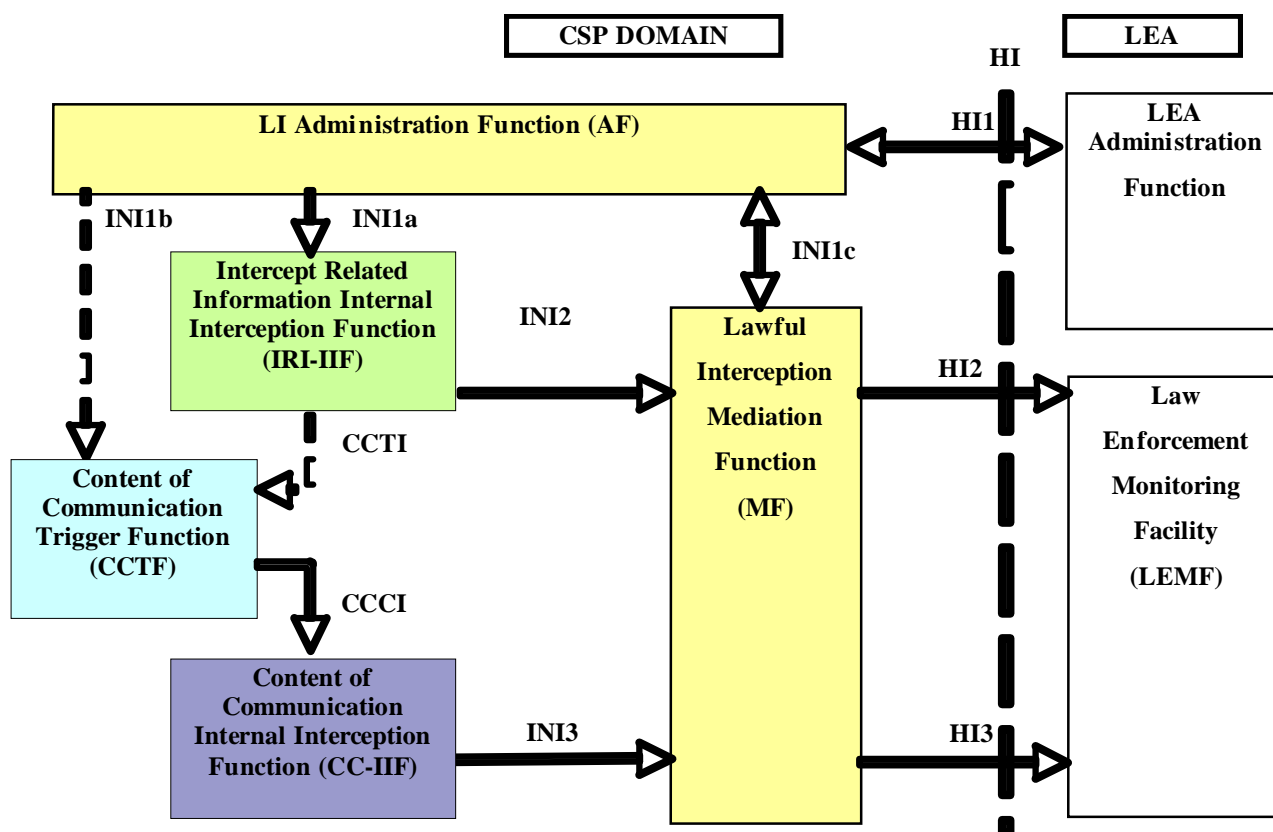


Figure 1a: Reference model for LI system in IP network

Intercept Related Information Intercept Function (IRI-IIF) generates IRI.

Content of Communication Intercept Function (CC-IIF) generates CC.

Content of Communication Trigger Function (CCTF) controls the CC-IIF.

Internal interface INI1 carries provisioning information from the Lawful Interception Administration Function (AF) to the Internal Intercept Functions (IIF).

- INI1a provisions Intercept Related Information Intercept Function (IRI-IIF).
- INI1b may (statically) provision Content of Communications Control Function (CC-IIF).
- INI1c provisions the Mediation Function (MF).

Internal interface INI2 carries Intercept Related Information (IRI) from the IRI-IIF to the MF.

Internal interface INI3 carries Content of Communication (CC) information from the CC-IIF to the MF.

Content of Communication Trigger Interface (CCTI) carries trigger information from the IRI-IIF to the CCTF.

Content of Communication Control Interface (CCCI) carries controls information from the CCTF to the CC-IIF.

4.2 Internationally based requirements

Figure 2 shows the hierarchy and relationship between requirements in the LI area.

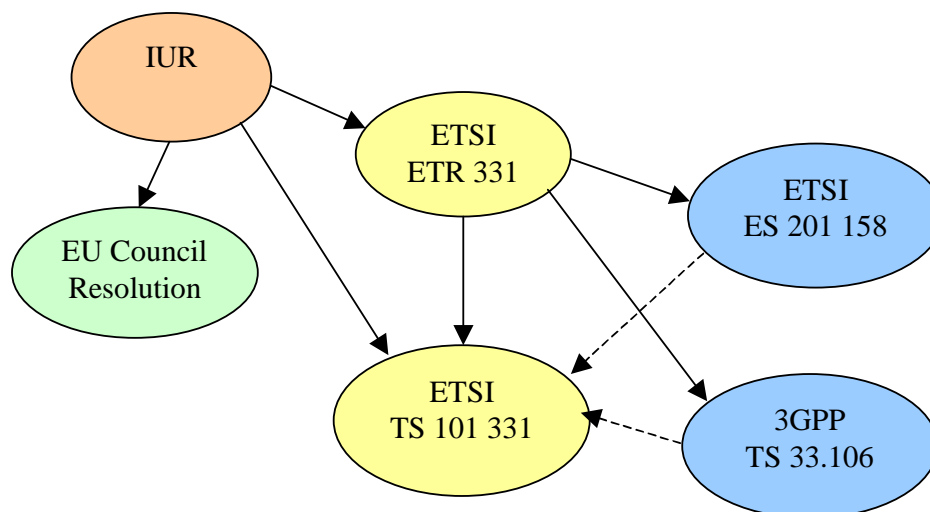


Figure 2: Development of international LI requirements

International User Requirements (IUR) have been worked out on an international basis, stating some basic needs of Law Enforcement for lawful interception. The EU council has adopted a resolution in January 1995, encouraging national governments to include requirements for lawful interception in their respective legal systems. The EU Council resolution has not had any apparent and direct impact on technical LI requirements.

The report ETR 331 was published within ETSI as a summary of LEA needs. This report was later re-issued as a technical standard (TS 101 331 [1]) under influence of the specific technical requirements of ES 201 158 [2] and TS 133 106 [13] as well as considerations of modern communication technology.

4.3 Characteristics of national requirements

4.3.1 General

The purpose of standardization is of course to create a framework for uniform design, thus reducing costs and enhancing interoperability. There are however certain areas that need to be left open due to differences in national conditions, such as how to migrate from legacy LI installations, specialities in national networks, national security requirements and locally preferred protocols for transmission.

4.3.2 Migration from legacy technology

Since lawful interception has been in operation in many countries for a long time before international standards emerged, there is a need to apply a strategy for technical and administrative migration from such legacy solutions. LEAs may not be prepared, or have the funding, for immediate and synchronous transition. Operators may want to align the transition to modern LI standards with a generation shift in their equipment. There may also be legal and business implications that influence the transition. All of this is outside the scope of international standardization and needs to be addressed on a national level.

4.3.3 National parameters

National communication networks may incorporate special services or technologies, which affect implementation of interception. International standards have provisions for this by offering open parameters, which need to be given values according to national conditions. An example of such parameters may be how to handle Subscriber Controlled Input (SCI), or whether or not to intercept transferred calls (see note).

NOTE: The model case for this is that intercepted subscriber A calls B and then C, neither of whom is intercepted. Then A hangs up, leaving B and C communicating with each other. Should interception still be in effect?

Another area, similar to choice of national options, is how to define formats for parameters that are declared as OCTET STRING or other open formats in the data definitions. There are probably national conventions for the format of for instance Lawful Interception IDentifier (LIID). This needs to be clarified in national adaptations of the standards.

4.3.4 Security

Most LEAs are likely to have their own requirements on security arrangements for confidential communication, like transmission and storage of LI-data. Such requirements may call for specific encryption procedures, private network arrangements, special hardware etc. When implementing LI systems, such requirements (and the costs for meeting them!) need to be taken into account and planned for.

See clause 7 for further discussion about security issues.

4.3.5 Protocols

International LI standards define only a limited scope of protocols for transmission of LI products. When implementing an LI system, the full protocol stack will have to be agreed on between operators and LEAs. Security considerations will also play a role here, as discussed further in clause 6.4.

4.4 Requirement implementation process

The development cycle for telecommunication systems from formulation of a requirement until it has been implemented and is met in a system in operation is usually a process spanning over several years. For LI systems there is a number of players in addition to international standards groups: national legislators and regulators, telecom equipment manufacturers, telecom service operators, 3rd party vendors, law enforcement agencies. Each of these players will influence how an LI system is implemented and at what pace new requirements are introduced and complied with.

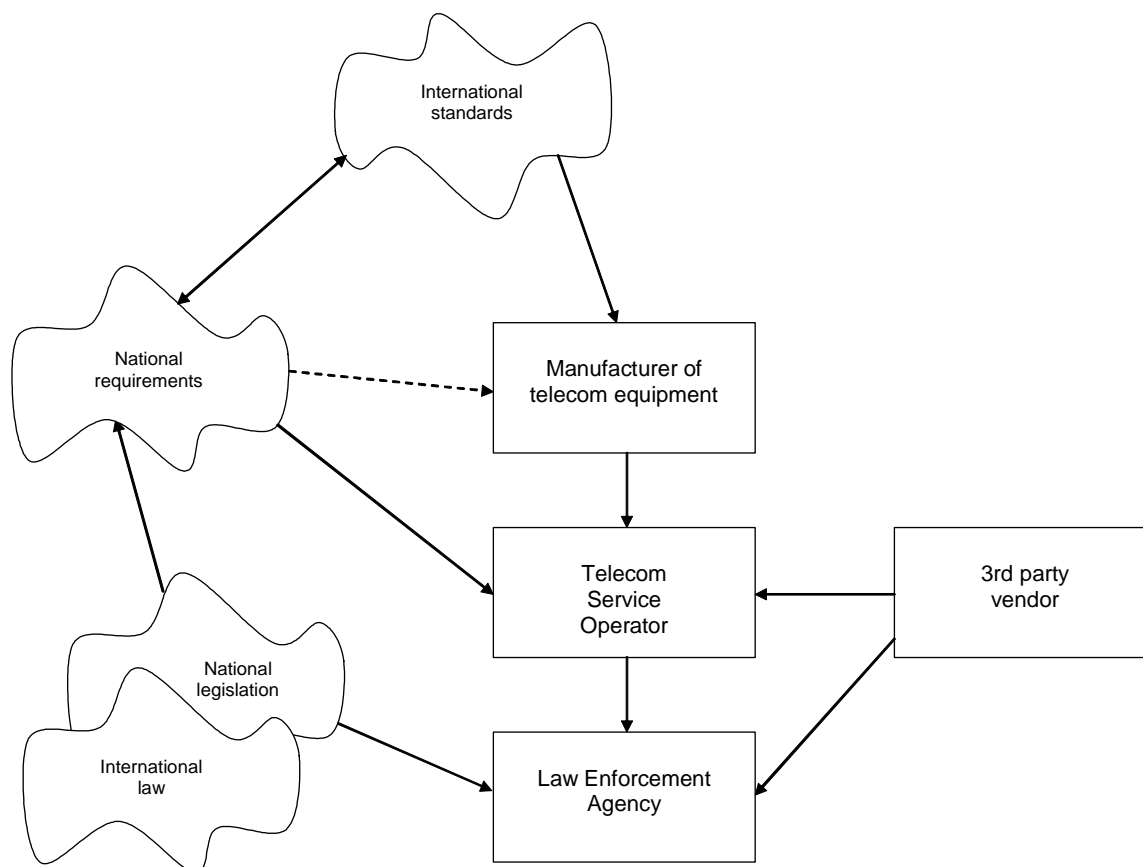


Figure 3: Requirement implementation process

The diagram above is intended to illustrate the process for implementation of requirements on an LI system. International standards will be influenced by national requirements. National requirements, in turn, will be based on national legislation and applicable standards. Telecom equipment manufacturers will build their LI systems for global markets based on international standards and with some consideration of national requirements, although it cannot be expected that telecom systems for a global market will be able to incorporate the union of all national specials. Telecom operators will need to meet national requirements in countries where they run business. Operators may also have their own technical requirements and may be able to tailor the standard products from manufacturers, often by including products (e.g. mediation functions) from 3rd party vendors. LEAs will be dependent on what operators have implemented and can apply 3rd party vendor equipment to cover special cases, which are not handled in the preinstalled LI functions. The operation of a Law Enforcement Agency is of course based on national legislation.

4.5 Overview of LI standards

When referring to standards of various origins, it is important to keep in mind that some of them may be proprietary and thus not immediately available for public use. This overview of current standards is limited to *international standards*, i.e. ETSI and 3GPP. It is common for individual nations to set up their own specific adaptations of international standards, prescribing choice of options, transfer protocols, security provisions, etc. National standards, such as ANS J-STD-025, have been excluded intentionally from this discussion, even though they are important for implementation of LI systems and may even be adopted in countries other than the one which first created them.

NOTE: ANS = American National Standard, ANS J-STD-025 has been developed by the telecommunications industry in the U.S.A. as a joint standard (through TIA and ATIS) to meet requirements according to the CALEA law.

The diagram below shows both the requirements on internal functionality of telecommunications networks, i.e. the Internal Interception Functions (IIF), and the specifications for handover interfaces to LEAs. As can be seen, a considerable number of IIF requirements drive just a few handover interface specifications. It is desirable to keep that number low in order to avoid proliferation of solutions in this area, which would increase cost and reduce reliability.

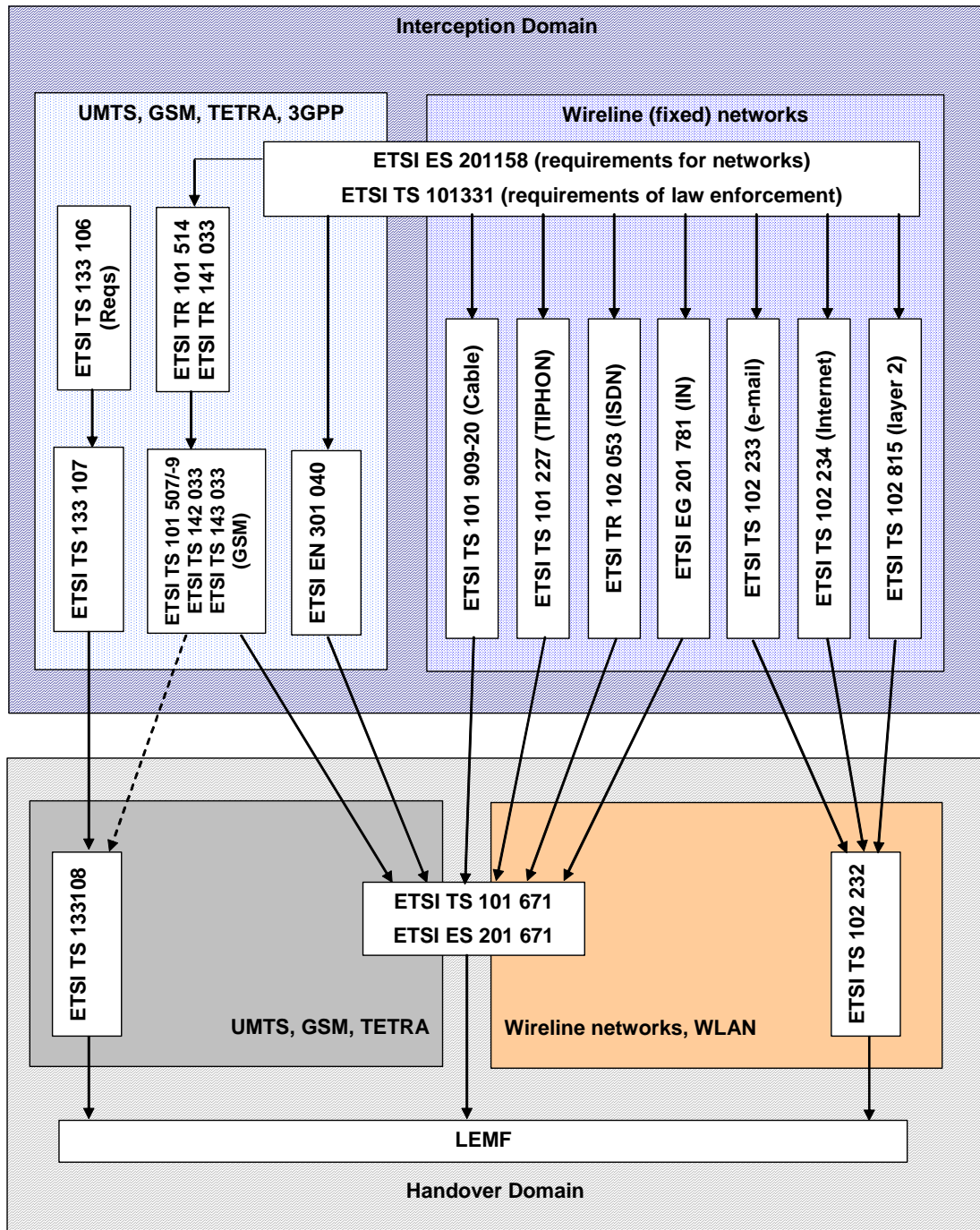


Figure 4: Overview of international standards for interception and handover

5 Interception of communication services

5.1 General

5.1.1 LI requirements related to services

When discussing interception, there is a tendency to focus on technologies and for instance view "IP Telephony" as something different from POTS. From the viewpoint of law enforcement, no such distinction should be made. Public telephony is supposed to be interceptable, regardless of how it is transmitted. In practice there will of course be moderations to this statement, since some technologies (as of yet) may defy interception. One might for instance consider the case where a conferencing system on the Internet is used to set up voice communication between computer users.

Interception of speech communication assumes adherence to the basic call model, so IRI messages are tailored to reflect state transitions in that model. When the implementation is moved out from the intercepting node and into user premises equipment, it will not be possible to generate standard IRI messages, unless the intercepting node performs some sort of interpretation based on lower-level protocols. It may for instance be possible to look into IP packets to determine that they contain phone call data and then watch for contents that correspond to signalling information in the basic call model. This would however be an attempt at second-guessing whatever a LEMF might conclude based on CC contents and involve TSPs in the role of a LEA.

5.1.2 Migration to separate service platforms

Traditionally, communication services have been provided in what might be called "aggregated form" - technology and service were combined on several levels: network access, speech or modem communication, communication protocols, hardware, etc. In POTS, for instance, the service is both speech communication and access, the target-id is the phone number, the protocols are integrated with the speech communication concept and the hardware consists of integrated function mainframe switches.

In New Generation Networks (NGN), services have been made more independent of technology, such that each service may be provided over several different technologies. Three layers of abstraction can be defined according to this NGN model.

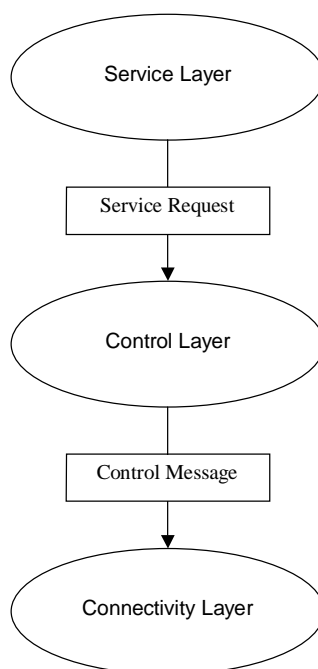


Figure 5: Three-layer model for communication system

The **Service Layer** will provide some specific service, such as Internet access, telephony or e-mail. That layer will also be responsible for AAA (Authentication, Authorization and Accounting) functionality. The Service Layer will send a request to the **Control Layer** to set up the technical means for providing the service. The Control Layer in turn will issue messages to the **Connectivity Layer** to set up the connections to provide the service.

5.1.3 Layered model related to LI functions

An application for lawful interception will use the Service Layer to identify the user, the Control Layer to provide IRI and the Connectivity Layer to get a copy of the CC.

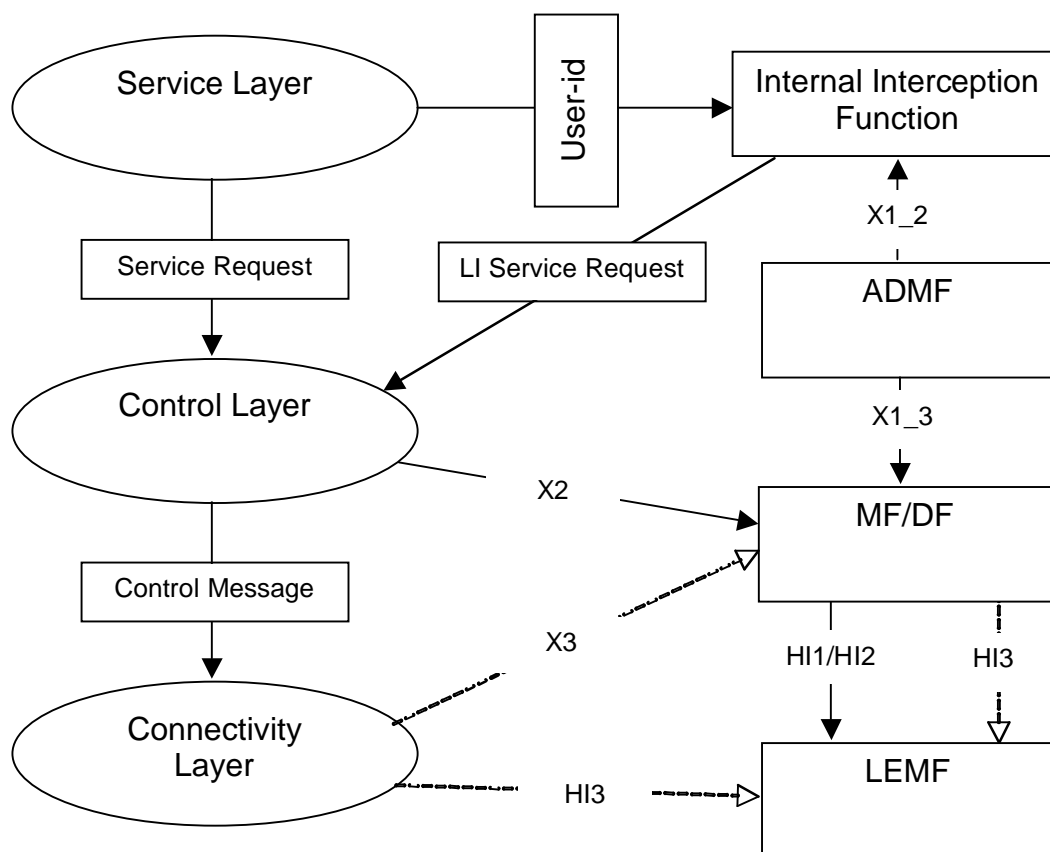


Figure 6: Mapping between LI service and communication system

This is a conceptual diagram, which is based on the NGN model with distinct functional layers for service, control and connectivity. An LI-specific administrative function is included in the model. In the mapping of LI services onto the three-layer model, it is assumed that the Service Layer holds the user-id, which would be used to identify a target for LI. In case the IIF finds a match between user-id and the list of targets held in the IIF, a request for LI services is sent to the Control Layer. The Control Layer will then be set up to report IRI to the MF/DF. In case CC is to be included in the interception, the Control Layer will send a message to the Connectivity Layer to deliver a copy of the communication. It is a matter of implementation choice whether to deliver the CC over an X3 link to the MF/DF for conversion to HI3, or to deliver directly in HI3 format to the LEMF(s). This model assumes that the control layer will be able to set up delivery of contents to arbitrary and multiple destinations through standard procedures, which are not specific to LI functionality.

5.2 Access services

Higher-level services are dependent of there being a service to gain access to the network. This makes the access service the lowest common denominator for provision of lawful interception. In lieu of being able to intercept for instance an e-mail server, a LEA may intercept access to the network that connects to the e-mail service.

Traditionally, access to a network for general services was provided over the phone line through modems or over special data networks, such as X.25. Today there is a multitude of technologies for access to the Internet.

When intercepting an access service, the point of interception needs to be close to the user, such that all contents of communication can be caught, preferably without inclusion of communication to/from other users. As an alternative, there may be requirements for all traffic to pass through a point where it can be intercepted. Network address translations may make it unfeasible to identify the traffic coming from a specific user. This has some similarity to interception of PABX users (the group number may be intercepted, but not the local extensions).

A rough outline of the functional architecture for interception of access service involves several functions, as shown in figure 7.

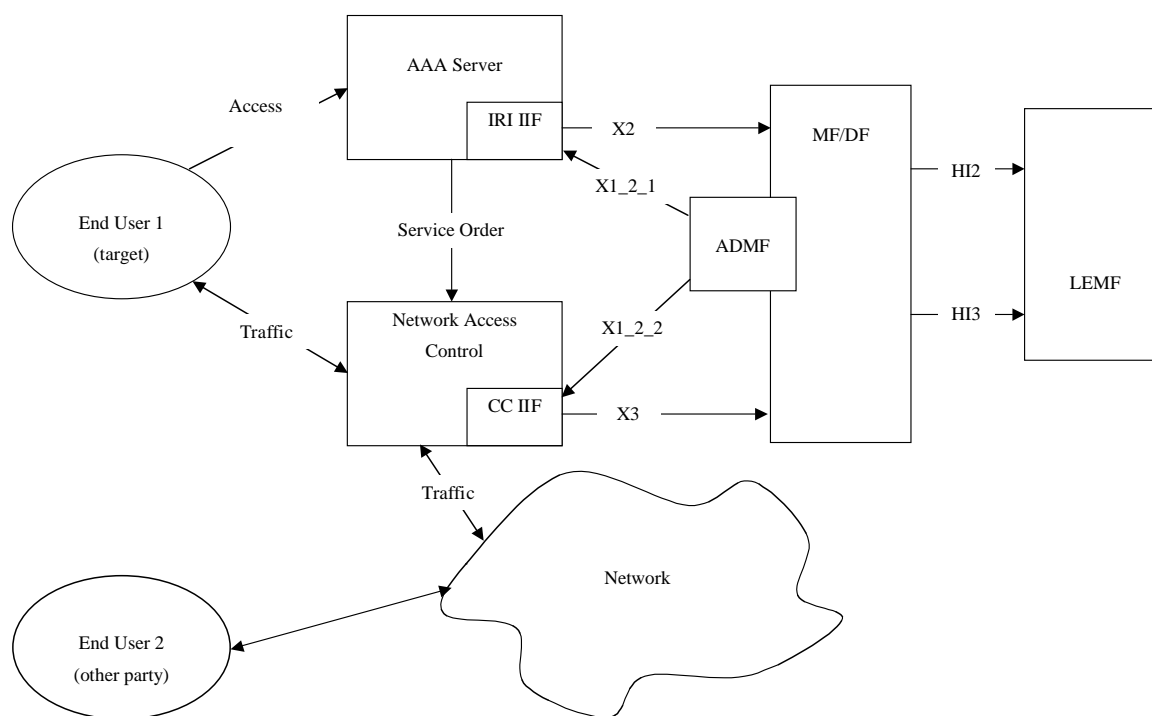


Figure 7: Functional architecture for interception of access service - user side interception

In this case it is assumed that the Network Access Control unit (typically a DHCP server or relay agent) is accessible for installation and operation of LI functions with sufficient security. If this is not the case, another type of architecture might be applicable, as shown in figure 8. The functions of ADMF and the IIFs are assumed to be:

- **IRI IIF:** Receive and manage interception orders from the ADMF in such a way that the function will trigger on the targeted user identities. When triggering occurs, an X2 message will be sent to the MF/DF.
- The **ADMF**, which is assumed to be more or less integrated with the MF/DF, will send an X1_2 message to the IRI IIF in the AAA server, setting up triggering on designated target identities. When an X2 message has been received in the MF/DF, the ADMF will send an X1_2 message to the CC IIF, setting up triggering for the network address (IP number), which has been assigned to the target (through the AAA server). Other functions of the ADMF are to respond to queries about target list, remove targets and send cancellation orders to the IIFs when monitoring of a target is discontinued.
- **CC IIF:** Receive and manage interception orders from the ADMF, based on targeted network identities (IP addresses). The CC IIF will copy and forward all IP packets to and from the targeted addresses.

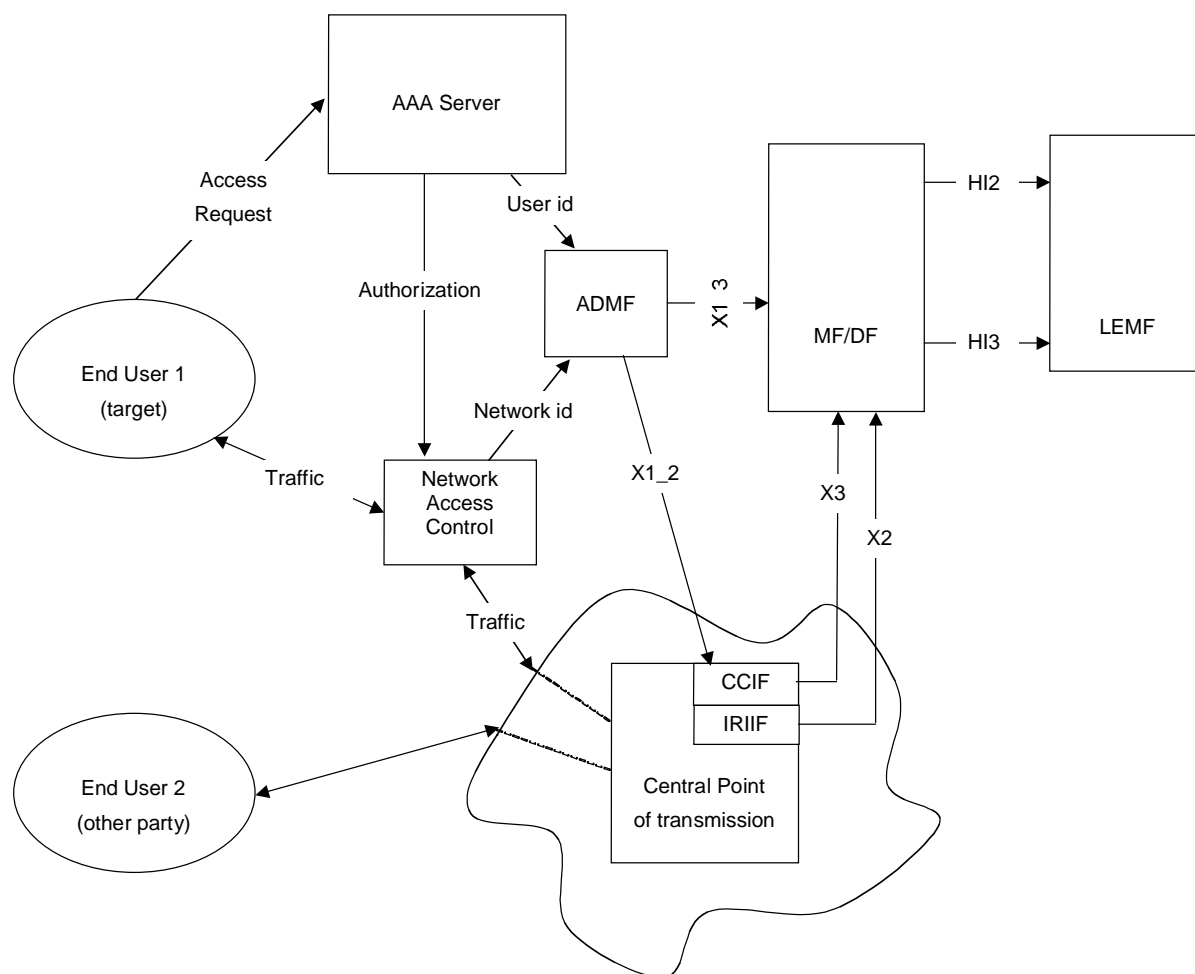


Figure 8: Functional architecture for interception of access service - network side interception

Here there is an assumption that all traffic can be forced to pass through one or more central points of transmission, where packets may be intercepted. Such interception points would typically be located in the ISPs internal network. The LI functions in such interception points need to be in communication with all relevant AAA servers such that the user identities can be screened for interception. This would rid the AAA server of any LI functions, but would require that it can send information about user identities and allocated network identifiers (e.g. IP-address) to a central point. When the ADMF has triggered on a targeted user_id, it will be matched with the associated network id (typically IP address) provided through the Network Access Control unit. The ADMF will then send X1_2 messages to the IIFs in the central point of transmission, requesting information about events and copies of traffic, as appropriate, to be sent to the MF/DF.

For details about interception of IP traffic at the network and link layer, respectively, please see references TS 102 815 [15] and TR 102 528 [16].

5.3 Communication application services

In a modern communications network, an increasing number of different kinds of application services are offered. It may also be the case that the same kind of application service is offered through many different technologies, for instance telephony over CS or PS, e-mail over modem line or cable modem etc. If standard interfaces can be agreed on and security requirements satisfied, it is simpler for a LEA to intercept at the application level than at the access channel.

Figure 9 shows the main architectural elements for interception of application service.

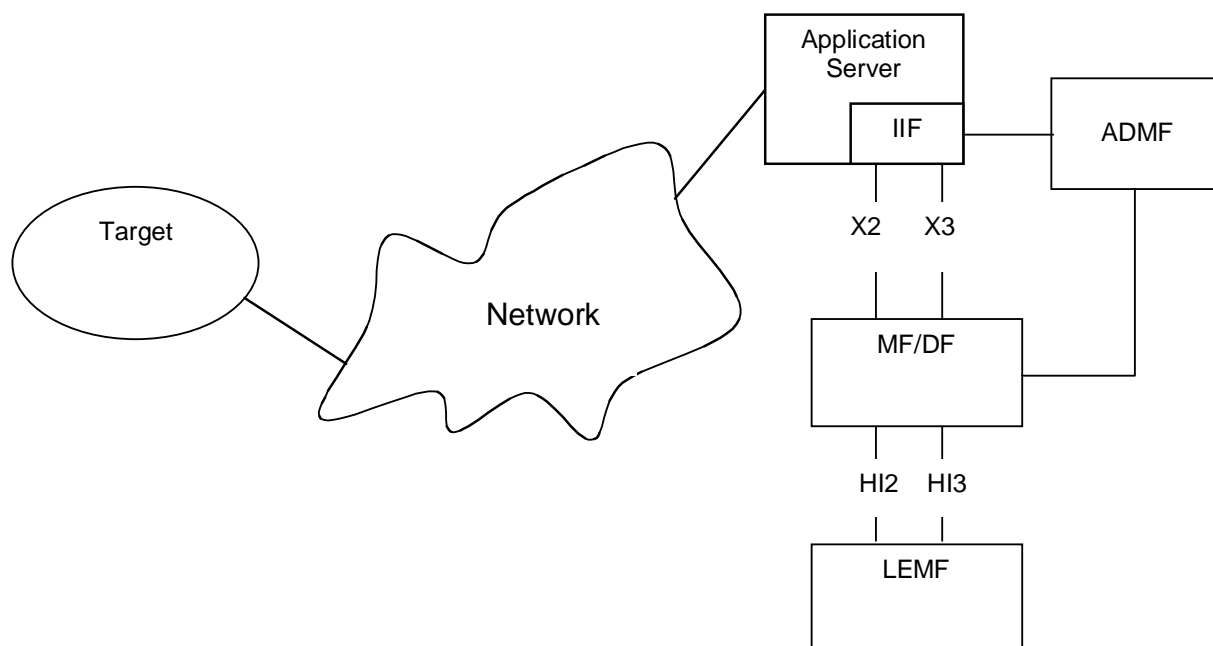


Figure 9: Interception of an application service

5.4 Intelligent network services

Intelligent network services form a somewhat special case for interception, since the application server (the IN Service Control Function - SCF) controls the access service (the IN Service Switching Function/Call Control Function - SSF/CCF) to set up connections. Thus the SCF will be aware of user identity (e.g. calling card number), but not have control over contents of communication, while the SSF/CCF will know only network identities (connected phone numbers). In order to handle this case, some LI-specific additional protocols or protocol extensions would have to be devised to set up interception of call contents.

There are some recent initiatives for development of standards for internal interfaces, such as the RFC 3924 [9]. This interface technology is based on the Simple Network Management Protocol (SNMP), which of course may impose a certain extra load on node design, unless SNMP is already being used for other purposes in the node in question.

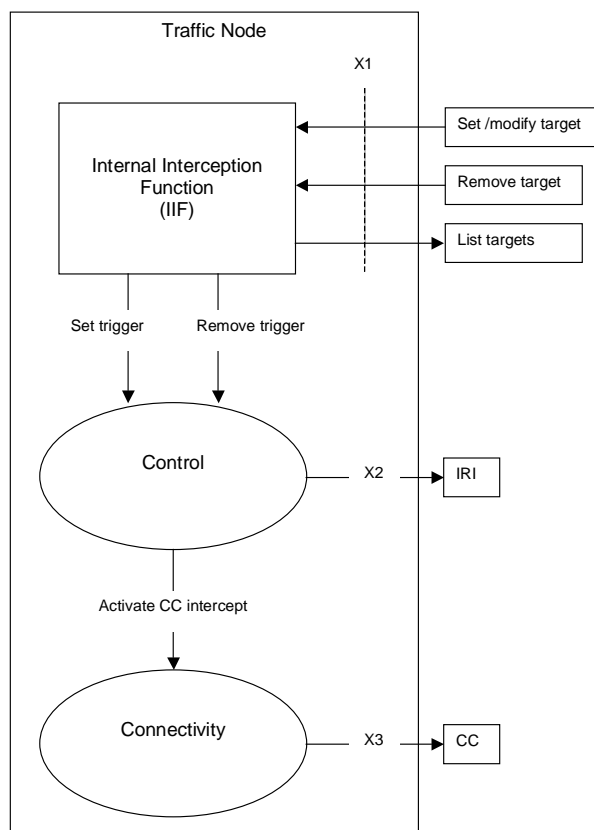


Figure 11: Node structure with internal interfaces

The interface for setting/modifying target and setting trigger, respectively, may contain information about internal or external delivery address for IRI and CC. There will also be information about whether the interception is IRI only or IRI + CC.

6.3 Handover interfaces

The mediation function will receive IRI and possibly also CC for transformation from internal interface format to the handover format. The delivery function will then handle dispatching of these LI products to the designated LEA(s). The syntactic elements of the HI2 and HI3 interfaces are described in several (partially overlapping) international and national standards. Currently ASN.1/BER is used for the presentation, but XML has been proposed as an alternative format.

At the application level in the protocol stack, FTP and ROSE are alternatives for IRI transmission. When using FTP, throughput requirements (IRI/hour) should be considered and the transmission mode, i.e. whether a transmitted file contains one IRI record or several records (see TS 101 671 [5], clause C.2) selected accordingly.

CC for circuit switched traffic is delivered over standard PCM links. The correlation information is to be sent as UUS1 messages in the signal phase, ASN.1/BER-encoded. If the network does not support UUS, correlation data may be sent in ISDN subaddress fields. This will impose some limitations on extent and format of the data in the correlation information.

6.4 Interface protocols

CC for packet data can be delivered either as a stream of IP packets with a special correlation header, or as files over FTP. In the case of FTP delivery, TLV is used for encoding the correlation information, while a fixed layout for the correlation header part is applied when IP delivery is used (see TS 101 671 [5], clause F.3). Since the data load on CC transmission may be quite heavy, performance issues related to packaging that into files should be considered before deciding to use FTP. When straight IP delivery is used, there is an ambiguity as to what session/application protocol to use. TPKT has been specified for the USA, see TS 133 108 [6], clause G.3. In theory it is possible to have a "virtual session" going - the LEA will order CC delivery to a certain IP address and port number and then make sure that the designated port is open in the LEMF. This means that the communication does not extend beyond the transport layer at each side - the DF and the LEMF applications will not communicate with each other. In case there is a problem in transmission, leading for instance to buffer overflow on the sending side or if the received data turn out to be corrupt, there is no protocol mechanism to handle the case. When intercepting CC for packet data, the LI products received at the LEMF will be plain copies of all the data exchange between the parties. There will of course not be any way for the LEMF to ask any of the parties for a retransmission. If some portion of the traffic between the parties is re-transmitted, this will also be copied to the LEMF.

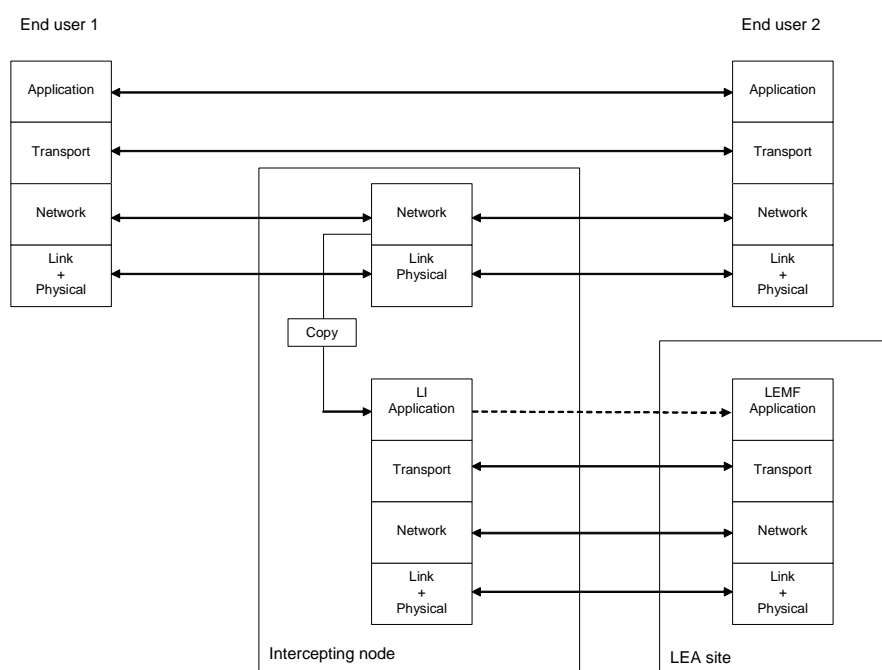


Figure 12: Protocol stacks with CC interception of packet data

Figure 12 shows how the intercepting node triggers on the network address of the intercepted user and sends copies of the thus intercepted packets to the LI application. After having identified the target user, the LI application will add a correlation header and then use the underlying protocol stack, from transport layer and downwards, to forward the intercepted packets to the LEMF. The LI Application and the LEMF Application will however not be aware of each other, except that the LEMF application may perform certain checks. For instance sequence numbers in LI headers may be used to synchronize between disjunct TCP sessions. This is indicated with a dotted line in figure 12.

6.5 Mapping IRI from PS Contents

When analysing results of interception of packet switched communication, it may be necessary to map IRI that is embedded in the protocols, which are used to emulate certain services. This information is found in the payload and requires special functionality in the analysis function, which also may depend on information in SIP or other types of control messages received over the HI2 channel.

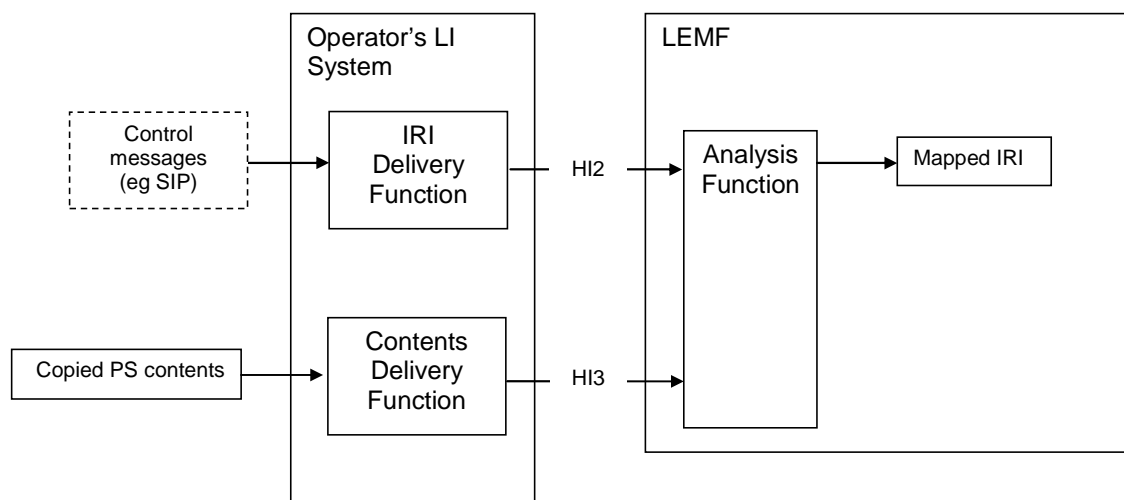


Figure 13: Mapping of IRI equivalents for service extracted in LEMF Analysis Function

It has been proposed to place the mapping function on the operator side, thus obliging the TSP to perform certain analysis work. This leaves considerable responsibility with the operator to make interpretations and avoid loss of essential information. The LEA should be in control of how mapping is to be done.

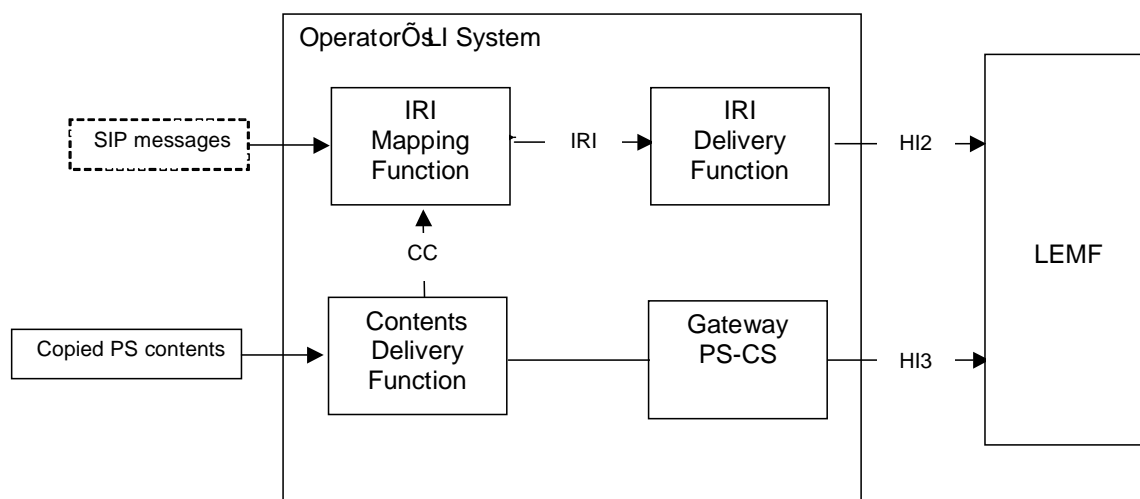


Figure 14: PS CC and control message IRI used to map IRI for service on operator's side

7 Security

7.1 General

The security of LI systems will be partially embedded in general network security provisions according to local requirements, which of course will override any international standards. It is just as necessary to protect the critical parts of the telecommunication system from intrusion as it is required to do so for the LI system. There are however some special aspects of the LI system that are related to the necessity to keep its operation secret. The most sensitive information in the LI system is data about who is intercepted. Results of interception are also sensitive information, which have to be protected against intrusion and tampering. Criminal organizations are potentially interested in blocking the function of LI systems and even taking control of them to use them for their own purposes. Such threats must be considered and provisions made to avert them. Experience shows that the most damaging actions tend to come from within, i.e. from corrupt or intimidated staff. Therefore screening and monitoring of personnel is one of the most important actions to enhance security.

7.2 Threat model

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:

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

The discussion is based on suggested arrangements to counteract these threats. Further studies will be necessary to adapt to national requirements and special conditions.

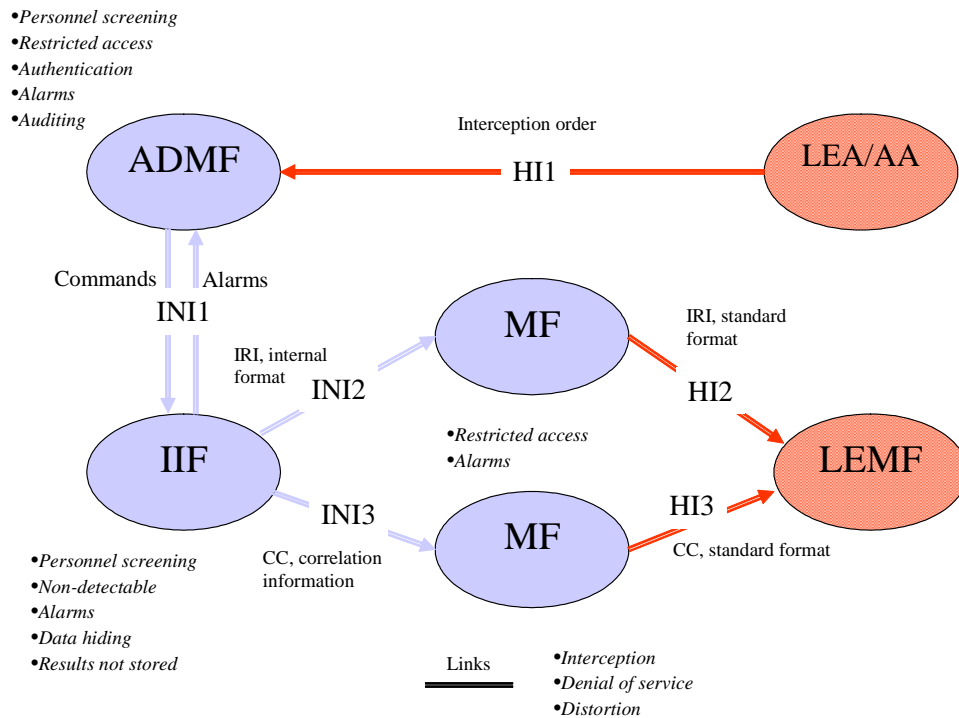


Figure 15: Diagram showing application of threat model to LI system

7.3 System security

7.3.1 Encryption of stored data

Data about intercepted subscribers, which is stored in the LI system, might be encrypted to enhance security. This is however likely to have adverse effects on performance. There is also some risk that the added complexity of managing encryption keys may cause problems. It should in most cases be sufficient to protect access paths to the stored data. Special care should however be taken to prevent that LI data leaks out from backups and transaction logs. The general rule is to exclude LI data from being backed up and logged outside the LI system itself, where it can be assumed to be adequately protected.

7.3.2 Logical access control

Access to LI systems should be restricted with strong authentication and authorization control. It is also to be recommended that operational information about the LI systems, such as how they are implemented, where they reside and how they are operated and maintained, should be kept within a small group of authorized persons.

7.3.3 Physical access control

Telecommunication systems are regularly protected against unauthorized access and the location of critical components is not commonly known. Buildings, floors and rooms that house telecom systems are usually protected through access control. LI systems may be embedded in such security regimes and should be further protected through anonymity (no "red boxes" or such).

7.4 Interface and link security

7.4.1 Protection of transmitted data

If there is a risk that LI data may be intercepted or tampered with while in transmission, encryption may be used as protection. Standard procedures and products, such as IPSEC, should be preferred for this task. Proprietary encryption systems run the risk of becoming obsolete and unsafe, unless they are maintained to match development in communication technology and cryptology.

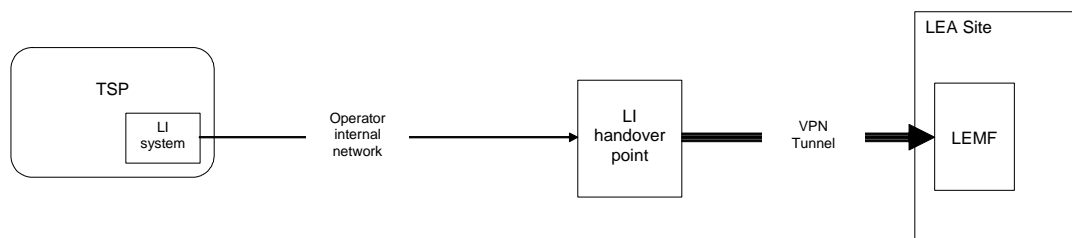


Figure 16: Secured IP delivery over VPN tunnel

For circuit switched CC, which is transmitted over phone lines, the standards allow for use of closed user groups and special screening of phone numbers for the sending LI system side and the receiving LEMF.

7.4.2 Management of keys

Keys for encryption of transmitted data might be managed through IKE (Internet Key Exchange), which is standard routine for IPSEC.

7.4.3 Use of leased lines

By using leased lines it is possible to protect interfaces and links such that encryption would not be necessary. By such an arrangement, LI data will never pass through public networks, so the network addresses for delivery of LI products can be defined in a private address space (e.g. 192.168.X.X) and E164 numbers defined outside of national routing tables. It is assumed that the private link is protected against physical tampering, for instance by using optical fiber in anonymous routing or protected ducts or both.

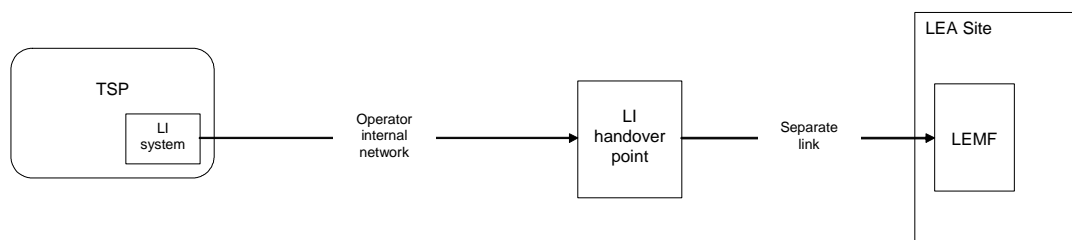


Figure 17: Handover point with separate links

Annex A: Change Request History

Status of Technical Report TR 101 943 Concepts of Interception in a Generic Network Architecture		
Date	Version	Remarks
July 2001	1.1.1	First publication of the TR after approval by ETSI/ SEC WGLI #28; (15-17 May 2001, Hamburg) Version 1.1.1 prepared by Stefan Björnson (Ericsson) (rapporteur edition 1)
September 2004	2.1.1	Included Change Request: TR101943CR001 (cat F) Publication of a new edition, version 2.1.1 This CR and updated TR was approved by TC LI#07 (28-30 September 2004, Bremen) Version 2.1.1 prepared by Stefan Björnson (Cecratech) (rapporteur edition 2)
May 2006	2.2.1	Included Change Request: TR101943CR002 (cat F) LI in a generic network architecture This CR and updated TR was approved by TC LI#13 (6-8 September 2006, Stockholm) Version 2.2.1 prepared by Stefan Björnson (Cecratech) (rapporteur)

History

Document history		
V1.1.1	July 2001	Publication
V2.1.1	October 2004	Publication
V2.2.1	November 2006	Publication