ETSI TS 101 158 V1.3.1 (2014-02)

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

Reference

RTS/LI-00110

Keywords

lawful interception, security

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/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

1 Scope

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

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

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[2] European Union Council Resolution 96/C 329/01 of 17 January 1995 on the Lawful Interception of Telecommunications.

[3] Void.

[4] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 671 [4] and the following apply:

Access Provider (AP): natural or legal person providing (via a terminal) access to a network

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

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

call: any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system

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

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

communication: information transfer according to agreed conventions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

lawful interception: See interception.

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

mediation function: mechanism which passes information between a network operator, an access provider or service provider and a handover interface, and information between the internal network interface and the handover interface

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

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

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

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

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

result of interception: information relating to a target service, including the CC and IRI, which is passed by an NWO/AP/SvP to a LEA

NOTE: IRI is provided whether or not call activity is taking place.

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

NOTE: The information may be established by an NWO/AP/SvP or a network user.

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

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

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

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

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

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

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

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

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 101 671 [4] and the following apply:

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

4 General requirements

The present document focuses on the HI between an NWO/AP/SvP and a LEA.

4.1 Basic principles for the HI

The network requirements mentioned in the present document are derived, in part, from the requirements of LEAs regarding the HI for the interception of telecommunications, TS 101 331 [1]. There are other requirements which relate to the operation of commercial telecommunications systems. Together, these requirements will be used to standardize HIs for specific telecommunications systems.

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

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

4.2 Legal requirements

It shall be possible to configure the HI to:

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

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

4.3 Example of typical functional role model and process

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

4.3.1 Overview

There are various aspects of interception.

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

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

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

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

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

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