ETSI TS 104 007 V1.1.1 (2024-11)

Lawful Interception (LI);
Lawful Interception Architecture

Reference
DTS/LI-00241

Keywords
functional architecture; interception;
lawful interception

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document describes a comprehensive blueprint for a Lawful Interception (LI) system, designed to align with the mandates of Law Enforcement Agencies (LEAs) for the surveillance of telecommunications with utility across varying legal and regulatory environments. The LI architecture detailed herein sets out to meet stringent requirements, outlining the necessary high-level entities, procedures, and the functional roles essential for the operation of interception. It specifies how lawful authorizations, such as warrants, are processed and executed by Communication Service Providers (CSPs) to deliver Intercept Related Information (IRI) and Content of Communication (CC) to LEAs through secure channels.

The present document emphasizes a security-centric approach, incorporating Zero Trust principles across the architecture to ensure secure operations. This security view is intertwined with the functional aspects, ensuring that both data integrity and privacy are preserved throughout the interception process. The architecture is designed to enable distinct LEAs to carry out interception activities simultaneously and independently, safeguarding against the risk of inter-agency or other non-authorized detection.

Through the definition of a methodical LI lifecycle, starting from authorization and ending with the delivery of intercepted communications, the present document covers the operational protocols, the interplay between the various entities, and the safeguarding mechanisms in place. The described LI system is adaptable to the dynamic and evolving landscape of national laws and telecommunication technologies, ensuring future-proof applications across different jurisdictions and technological paradigms.

Introduction

The present document explains thoroughly the intricate architecture of Lawful Interception (LI) systems as stipulated across varying regulatory environments, a cornerstone for maintaining the delicate balance between national security, law enforcement, and individual privacy. Mapped out herein are the protocols that govern the interception of telecommunications as per the legal frameworks established by ETSI TS 101 331 [1]. Commencing with a broad overview of the key players and their respective roles within the LI ecosystem, the present document progressively narrows down to a more detailed analysis of the functional and security viewpoints.

1 Scope

The present document on Lawful Interception architecture provides an overview of the technical framework and components involved in facilitating lawful interception of communications for law enforcement agencies. The present document outlines the key principles, standards, and protocols governing lawful interception, including the roles and responsibilities.

2 References

2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at ETSI docbox.

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

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] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Architecture enhancement for Security Management Specification".

[4] ETSI TS 104 000: "Lawful Interception (LI); Internal Network Interface X0".

[5] ETSI TS 133 126: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Lawful Interception requirements (3GPP TS 33.126)".

[6] ETSI TS 133 127: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Lawful Interception (LI) architecture and functions (3GPP TS 33.127)".

[7] IETF RFC 9334: "Remote ATtestation procedureS (RATS) Architecture".

2.2 Informative 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 referenced document (including any amendments) applies.

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

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".

[i.2] ETSI GR NFV-IFA 029 (V3.3.1): "Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"".

[i.3] ETSI GS NFV-IFA 040 (V4.1.1): "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification".

[i.4] NIST Special Publication (NIST SP) 800-207: "Zero Trust Architecture".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

root of trust: hardware-based seed/key material or function that contains it, upon which a hierarchy of keys are built to support higher functions

trust anchor: root certificate authority in the network

zero trust: security concept where no entity, whether inside or outside a network perimeter, is automatically trusted, but granularly authorized

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ABAC	Attribute Based Access Control
ADMF	ADMinistrative Function
API	Application Programming Interface
ARP	Attestation Relying Party
AVS	Attestation Verifier Service
CA	Certificate Authority
CC	Content of Communication
CISM	Container Infrastructure Service Manager
CMF	Certificate Management Function
CPU	Central Processing Unit
CSP	Communication Service Provider
CSR	Certificate Signing Request
CTDGW	Cross Trust Domain GateWay
DMZ	De-Militarized Zone
ELI	Element of LI
HMEE	Hardware Mediated Execution Enclave
ID	IDentifier
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Function/Facility
LI	Lawful Interception
LI-Admf	Lawful Interception-ADMinistrative Function interface
LI-Ap	Lawful Interception-Application interface
LI-No	Lawful Interception-Network Output interface
LI-Os	Lawful Interception-Operations support interface
LI-Vn	Lawful Interception-Virtual network interface

LICA	Lawful Interception Certificate Authority
LICF	Lawful Interception Control Function
LICM	Lawful Interception Certificate Management function
LIGW	Lawful Interception GateWay
LIID	Lawful Interception IDentifier
LIPF	Lawful Interception Provisioning Function
LISE	LI Security Engine
LRPG	LI Routing Proxy Gateway
MANO	MANagment and Orchestration
MDF	Mediation and Delivery Function
MOGW	ManO GateWay
NE-Admf	Network-Administrative function interface
NF	Network Function
NFIID	Network Function Instance IDentity
NFV	Network Function Virtualization
NFVO	Network Function Virtualization Orchestrator
NOGW	Network Output GateWay
NRF	NF Repository Function
NWF	NetWork functionality Function
OS	Operating System
Os-Mano	Operations support-MANO interface
Oss-LI	Operations support-Lawful Interception interface
OSS/BSS	Operations Support System/Business Support System
POI	Point Of Interception
RAM	Random Access Memory
RATS	Remote ATtestation procedureS
SDN	Software Defined Network
SOC	System On Chip
SIRF	System Information Retrieval Function
TD	Trust Domain
TF	Triggering Function
TLS	Transport Layer Security
TPM	Trusted Program Module
UEFI	Universal Extensible Firmware Interface
VM	Virtual Machine
VNF	Virtual Network Function
ZTA	Zero Trust Architecture

4 Approach

4.1 General approach

The present document defines the Lawful Interception (LI) architecture to meet the requirements of LEAs regarding the Handover Interface for the interception of telecommunications (see ETSI TS 101 331 [1]).

Clause 4.2 describes a high-level view of the entities and procedures that are generally required to be supported in LI systems.

Clause 5 sets out the functional view of the architecture that supports the elements and procedures required by clause 4.2.

Clause 6 sets out the security view of the architecture that supports secure operation following Zero Trust principles as defined by NIST [i.4].

Clauses 5 and 6 are to be read together, as the security view in clause 6 motivates the functional view of clause 5.

Clause 7 gives an overview of the provisioning process.

4.2 LI entities and procedures

4.2.1 Overview

The functional role model described in this clause is a reference example to facilitate a general understanding of the typical operation of interception and the typical responsibilities of the various elements.

National laws that describe the conditions and restrictions of interception and procedures will apply as described in references [2] and [i.1].

The LEA obtains a lawful authorization, such as a warrant, from a court of law or other responsible body (the "authority" in figure 4.2.1-1). The LEA presents the lawful authorization to the CSP via an administrative interface or procedure (interface port HI1).

Intercept Related Information (IRI) and the Content of Communication (CC) are delivered to the Law Enforcement Monitoring Function (LEMF) of the requesting LEA, via interfaces HI2 and HI3, respectively.

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

A target may be the subject of interception of different authorizations. It is necessary to support strict separation of these lawful interceptions. It is therefore possible that more than one lawful authorization may be issued relating to the same interception target. These various lawful interceptions may contain different constraints on the IRI and the CC. These various lawful interceptions may fall under different laws.

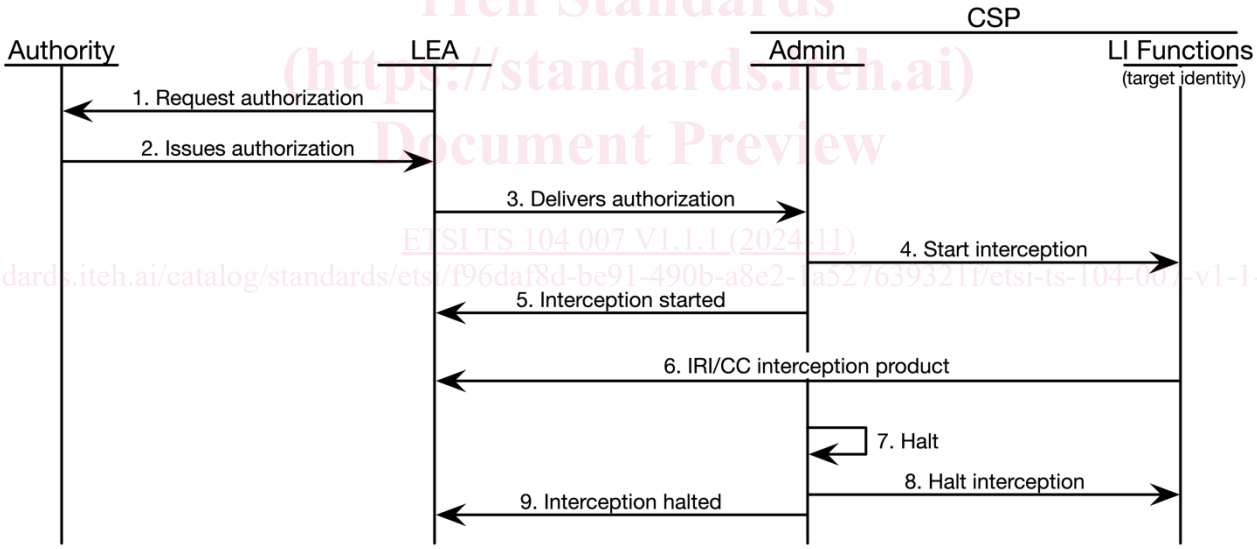

Figure 4.2.1-1: General provisioning flow

4.2.2 Entities

The entities in the functional flow in figure 4.2.1-1 are given in table 4.2.2-1.

Table 4.2.2-1: Provisioning entities

Entity	Role
Authority	The authorization authority is a judicial or administrative body designated by local laws or regulations. It gives the LEA the lawful authorization to intercept a target.
LEA	The LEA requests that the CSP intercept communications according to a lawful authorization. The LEA receives, through a Law Enforcement Monitoring Function, the interception product (CC and IRI) relating to a target identity.
CSP	An entity which provides communication services to subscribers.
Target identity	The target identity corresponds to the identity of a given interception target, which is an entity that makes use of a given service offered by a CSP.

4.2.3 Process

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

The authorization authority requires, through the LEA, the interception of services utilized via the telecommunication network by the interception target. The LEA receives the communications involving the target identity(ies) which the CSP has associated with the interception target.

Referring to the functional role model, and assuming that the lawful authorization is to be given to a CSP, actions are shown in table 4.2.3-1.

Table 4.2.3-1: Functional role model process actions

Reference (see figure 4.2.1-1)	Action
1	An 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 sends the request for lawful interception along with the lawful authorization to the CSP. The CSP determines the relevant target identities from the information given in the lawful authorization.
4	The CSP causes interception facilities to be applied to the relevant target identities.
5	The CSP informs the LEA that the lawful authorization has been received and acted upon. Information may be passed relating to the target identities and the target identification.
6	IRI and CC related to the target identity are passed from the CSP facilities to the LEA LEMF.
7	Either on request from the LEA or when the period of authority of the lawful authorization has expired the CSP will cease the interception arrangements.
8	The CSP signals its facilities to halt interception (see note).
9	The CSP announces the cessation to the LEA (see note).
NOTE: Steps 8 and 9 may be asynchronous.	

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

- Target identification.
- LEMF address for CC.
- LEMF address for IRI.
- Delivery address parameters for LEMF (e.g. for authentication and security).
- Alarm routing (if different from the delivery address).

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

4.2.4 LI lifecycle

Figure 4.2.4-1 depicts the general LI lifecycle state machine.

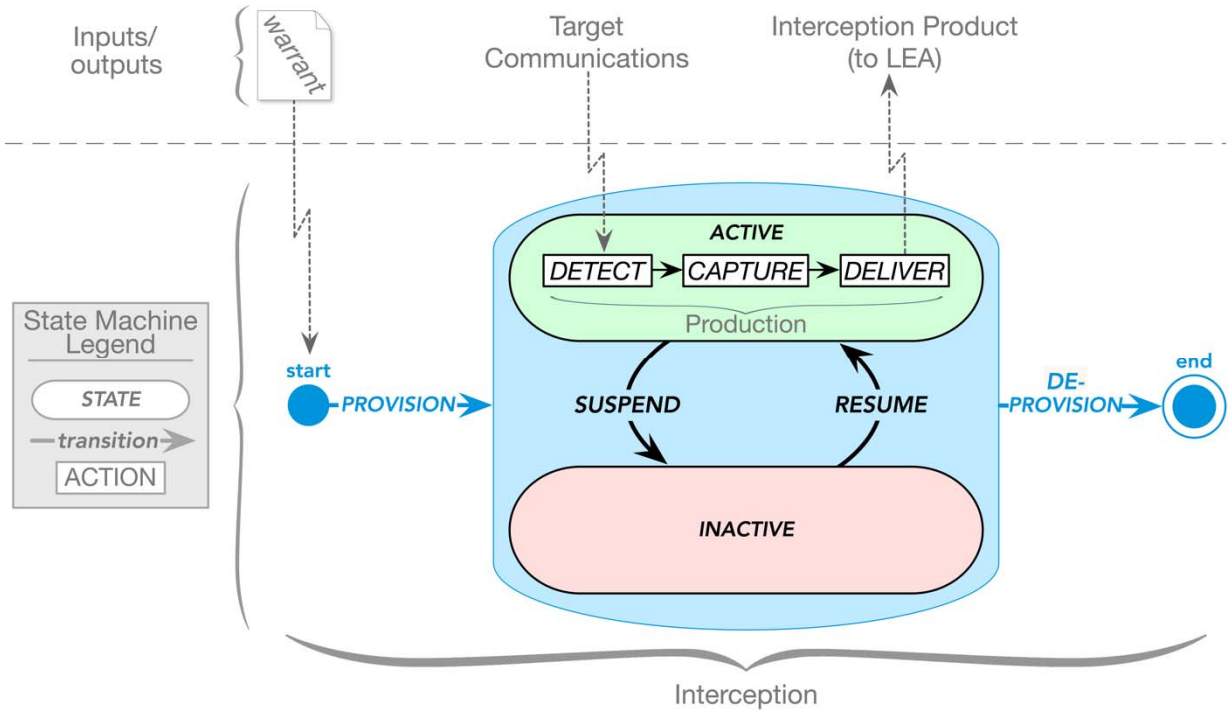

Figure 4.2.4-1: LI lifecycle state machine

After an LEA delivers a warrant to the CSP, the CSP provisions the interception. In the ACTIVE state, the Lawful Interception system elements *detect*, *capture* and *deliver* interception product to the LEA (labelled "production" in figure 4.2.4-1). These three production actions occur each time a targeted communication is identified, and therefore may happen many times during the lifecycle.

Depending on requirements, once provisioned, the LI system can enter directly into the ACTIVE state (immediate activation of LI), or enter the INACTIVE state (for delayed activation of LI), in which it still requires a RESUME transition to enter the ACTIVE state. The "production" activities of *detect*, *capture*, and *deliver* from figure 4.2.4-1 happen only in the ACTIVE state. It is in this ACTIVE state only that interception product is delivered to the requesting LEA.

A transition from INACTIVE to ACTIVE will resume the process from the *detect* action. Conversely, a transition from ACTIVE to INACTIVE will immediately stop *detection* and *capture*, but finish *delivery* to Law Enforcement of previously captured (during the ACTIVE state) product.

If provisioning causes LI to enter the INACTIVE state for a delayed start of interception, once the delay period is over the RESUME transition will occur moving the LI into the ACTIVE state.

Some jurisdictions may not support the delayed start of the interception. In such cases, provisioning of interception causes LI to immediately transition to the ACTIVE state, thus the production actions start directly upon provisioning, and stop directly upon de-provisioning.

5 Functional view

5.1 General

A high-level functional view of the LI architecture is given in figure 5.1-1 below.