ETSI TS 103 221-1 V1.1.1 (2017-10)

Lawful Interception (LI);
Part 1: Internal Network Interface X1 for Lawful Interception

Reference
DTS/LI-00104-1

Keywords
interface, lawful interception

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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 (https://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.

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.

Foreword

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

The present document is part 1 of a multi-part deliverable covering the internal network interfaces for Lawful Interception as identified below:

Part 1: "Internal network interface X1 for Lawful Interception";

Part 2: "Internal network interface X2 for Lawful Interception";

Part 3: "Internal network interface X3 for Lawful Interception".

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.

1 Scope

The present document defines an electronic interface for the exchange of information relating to the establishment and management of Lawful Interception. Typically, this interface would be used between a central LI administration function and the network internal interception points.

Typical reference models for LI define an interface between law enforcement agencies (LEAs) and communication service providers (CSPs), called the handover interface. They also define an internal network interface within the CSP domain between administration and mediation functions for lawful interception and network internal functions, which facilitates the interception of communication. This internal network interface typically consists of three sub-interfaces; administration (called X1), transmission of intercept related information (X2) and transmission of content of communication (X3). The present document specifies the administration interface X1.

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 https://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.

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

[1] ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".

[2] IETF RFC 4122: "A Universally Unique Identifier (UUID) URN Namespace".

[3] W3C Recommendation 28 October 2004: "XML Schema Part 2: Datatypes Second Edition".

[4] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[5] Recommendation ITU-T E.212: "The international identification plan for public networks and subscriptions".

[6] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003)".

[7] IETF RFC 3261: "SIP: Session Initiation Protocol".

[8] IETF RFC 3966: "The tel URI for Telephone Numbers".

[9] IETF RFC 3508: "H.323 Uniform Resource Locator (URL) Scheme Registration".

[10] IETF RFC 4282: "The Network Access Identifier".

[11] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[12] IETF RFC 2818: "HTTP over TLS".

[13] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[14] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[15] IETF RFC 6176: "Prohibiting Secure Sockets Layer (SSL) Version 2.0".

[16] IETF RFC 7525: "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

[17] IETF RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)".

[18] IETF RFC 4519: "Lightweight Directory Access Protocol (LDAP): Schema for User Applications".

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] OWASP TLS Cheat Sheet.

NOTE: Available at https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet.

[i.2] ETSI TR 103 308: "CYBER; Security baseline regarding LI and RD for NFV and related platforms".

[i.3] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.4] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.5] OWASP XML Security Cheat Sheet.

NOTE: Available at https://www.owasp.org/index.php/XML_Security_Cheat_Sheet.

3 Definitions and abbreviations

3.1 Definitions

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

destination: Point to which IRI and/or CC is delivered by the NE

Destination Identifier (DID): identifier to uniquely identify a Destination internally to the X1 interface

protocol error: error at the X1 protocol level (rather than any fault with ADMF or NE)

NOTE: In the present document, the term "error" in general refers to a protocol error, whereas issues with systems not behaving correctly are called "faults".

task: continuous instance of interception at a single NE carried out against a set of target identifiers, identified by an X1 Identifier, starting from an activate command and ending with a deactivate command or terminating fault

terminating fault: fault signalled from NE to ADMF which terminates the specific Task

X1: LI interfaces internal to the CSP for management tasking

X2: LI interfaces internal to the CSP for IRI delivery

X3: LI interfaces internal to the CSP for CC delivery

X1 Identifier (XID): identifier to uniquely identify a Task internally to the X1 interface

X1 Transaction ID: identifier used to identify a specific request/response pair

3.2 Abbreviations

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

ADMF	Administration Function
AVP	Attribute-Value Pair
CC	Content of Communication
CIDR	Classless Inter Domain Routing
CSP	Communication Service Provider
DID	Destination IDentifier
FQDN	Full Qualified Domain Name
FTP	File Transfer Protocol
GTP-C	GPRS Tunnel Protocol (control plane)
GTP-U	GPRS Tunnel Protocol (user plane)
HI	Handover Interface
HTML	HyperText Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over TLS
IMEI	International Mobile Equipment Identity
IMPI	IP Mutltimedia Private Identity
IMPU	IP Mutltimedia Public identity
IMSI	International Mobile Station Identity
IP	Internet Protocol
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAC	Media Access Control
NAI	Network Access Identifier
NAT	Network Address Translation
NE	Network Element

NOTE: The element or function performing the interception

NFV	Network Functions Virtualisation
OWASP	Open Web Application Security Project
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UID	Unique IDentifier
URI	Uniform Resource Identifier
UTF	UCS Transformation Formats
UUID	Universally Unique IDentifier
XID	X1 IDentifier
XML	eXtended Markup Language
XSD	XML Schema Definition

4 Overview

4.1 Reference model

The X1 interface is based on communication between two entities; the CSP Administration Function (ADMF), and the Network Element (NE) performing interception. The X1 reference model is shown in figure 1.

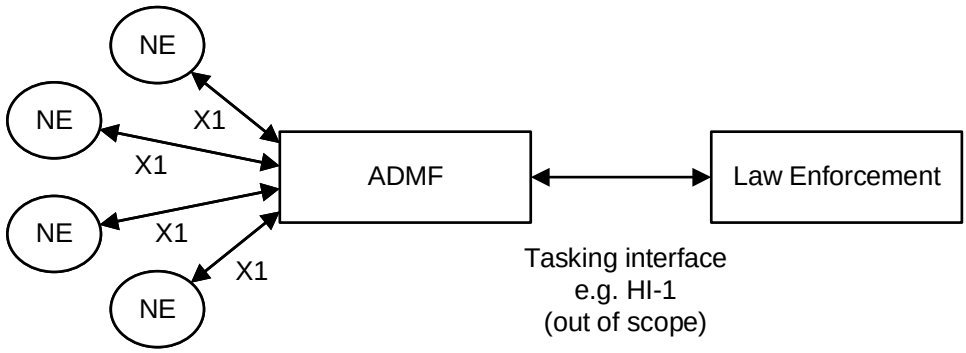

Figure 1: X1 reference model

Only one ADMF shall make changes by X1 to a given NE. This is called the ADMF which is "responsible" for that NE.

Onward delivery of information from the NE is called X2 (for IRI) and X3 (for CC). The choice of protocols for X2 and X3 are out of scope of the present document.

Some deployments may involve multiple ADMFs for redundancy or other purposes; where multiple ADMFs are required, the NE shall be implemented such that it presents itself as a separate NE to each ADMF.

ADMF and NE shall implement time synchronization where possible; in situations where it is not possible, the ADMF shall maintain knowledge of the timing offset between the ADMF and NE.

NOTE: The present document may be used in direct delivery scenarios, in which the NE delivers directly to the LEMF. Any consequences of using direct delivery are out of scope of the present document.

4.2 Reference model for X1: requesting and responding

X1 transactions consist of a request followed by a response.

Requests may be sent in either direction i.e. with the ADMF or NE initiating the request. The side initiating the request is called the "Requester"; this term is used when it is not specified whether it is the ADMF or NE making the request. The other side is called the "Responder".

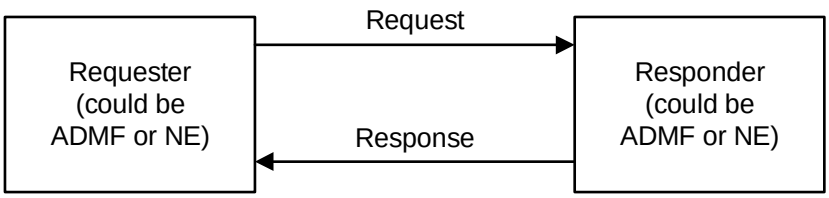

Figure 2: Showing generic terminology

It is likely that in most situations, the ADMF will initiate the message i.e. to distribute information or request status. However, it is possible that the NE will initiate the request in order to deliver fault reports, etc.

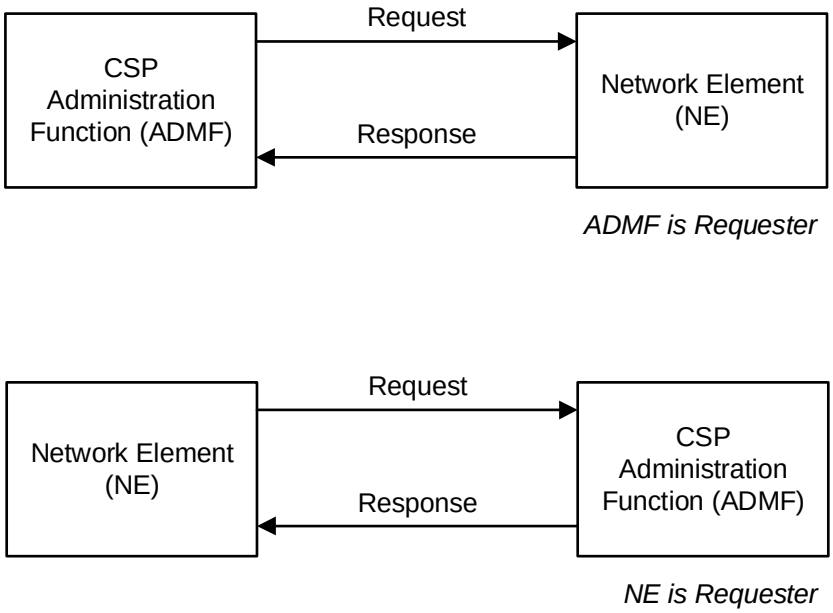

Figure 3: Showing two situations with either ADMF or NE as the requester

4.3 Overview of security

Security is based on creating public/private keys for the ADMF and each NE for which it is responsible. All transactions over X1 are performed using the security procedures in clause 8, which provide assurance that communication only takes place between an NE and ADMF which have been populated with the relevant key material.

NE implementers are strongly discouraged from exposing additional interfaces for controlling the LI functionality of the NE other than by X1 e.g. via a local administrative interface at the NE. If such additional interfaces exist, any such action performed on the NE shall be captured on the NE audit/logging, and any consequences of such actions shall be able to be seen and controlled by the ADMF that is responsible for the NE i.e. the ADMF shall be able to use the X1 interface to stop or undo any changes made over a local administrative interface. There may be broader consequences that are not covered by the present document if an NE is tasked independently of the X1 interface (e.g. security concerns).

4.4 Relationship to other standards

The present document forms part of a family of internal interface documents covering all of X1, X2 and X3 which are handled as separate standards.

Some models of LI (e.g. ETSI TS 133 107 [1]) define interfaces between ADMF and functions which perform mediation and delivery of content and IRI, (e.g. X1_2 and X1_3 defined by ETSI TS 133 107 [1]). The present document is designed to fulfil the requirements for X1_1 as defined in ETSI TS 133 107 [1].

4.5 Release management

This clause describes the release management requirements. The requirements are:

- The version of the present document is defined as <major>.<minor>.<patch>.
- The major version should be incremented when making a backwards incompatible change.
- The minor version should be incremented when adding backwards compatible functionality.
- The patch version should be incremented when fixing a backwards compatible bug.

Once a major version has been incremented, the previous major version will be supported for 2 years after publication of the new version. Change requests issued to a version that is no longer supported will need to be issued for the latest supported major version.

5 Basic concepts

5.1 The lifecycle of a Task

5.1.1 Start and end of a Task

A Task relates to a single target identifier, and goes from the point an ActivateTask Request is sent by the ADMF to the time a DeactivateTask Request is sent by the ADMF, or a "terminating fault" occurs.

The present document does not define which situations are categorized as "terminating faults". Local recovery procedures should be followed before a Task is ended with a "terminating fault". In general, irrecoverable failures with an interception, or major security issues at an NE should be considered terminating faults, and certain outcomes with keepalives are also terminating faults (where defined in clause 6.6.2).

5.1.2 Identification of a Task

Each Task on X1 is uniquely identified by an X1 Identifier (XID) and it is handled independently of all others. The ADMF shall assign the XID as a version 4 UUID as per IETF RFC 4122 [2]. The ADMF is responsible for correlating the XID to any LI instance identifiers used to communicate with Law Enforcement.

In addition, the XID is released once the Task has ended.

5.1.3 Destinations

Intercepted traffic is delivered by the NE to a Destination. Each Destination is uniquely identified by a Destination Identifier (DID), and is handled independently from details of the Task. Each Task is associated with one or more Destinations. Prior to associating a Task with a given DID, it is required that a Destination with the DID has already been created (as described in clause 6.3) but there is no requirement that a connection has been successfully established for that DID. Checks regarding availability and status of downstream delivery of information are outside the scope of the present document.

5.2 The lifecycle of an X1 request/response

5.2.1 Identification of X1 request/response

Each request and response shall be identified by an X1TransactionID. The requester (may be ADMF or NE) shall assign an X1TransactionID as a version 4 UUID as per IETF RFC 4122 [2].

5.2.2 Responding to the request

The response shall be sent without undue delay and shall be sent within TIME1 of receiving the request. TIME1 shall be configurable and by default TIME1 shall be five seconds. TIME2, the time a requester waits for a response, shall be configurable, it shall be at least twice TIME1 and by default shall be fifteen seconds.

An error response shall be sent if the request is not compliant syntactically (it does not match the schema) or semantically (it is not compliant or consistent with the existing state of the NE e.g. activating an existing XID).