ETSI TS 103 221-2 V1.1.1 (2019-03)

Lawful Interception (LI);
Part 2: Internal Network Interface X2/X3 for Lawful Interception

Reference
DTS/LI-00104-2

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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 normative deliverables 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 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [1].

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 transmission of intercepted information as part of Lawful Interception. This interface is used from points of interception to LI mediation functions.

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/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 a protocol for delivering X2 and X3.

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 103 221-1: "Lawful Interception (LI); Part 1: Internal Network Interface X1 for Lawful Interception".

[2] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[3] IEEE Std 1003.1™-2017: "IEEE Standard for Information Technology - Portable Operating System Interface (POSIX®)".

[4] IETF RFC 791: "Internet Protocol".

[5] IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

[6] IEEE 802.3™: "IEEE Standard for Ethernet".

[7] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

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

[9] IETF RFC 2131: "Dynamic Host Configuration Protocol".

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

[11] ETSI TS 129 281: "Universal Mobile Telecommunications System (UMTS); LTE; General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (3GPP TS 29.281)".

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

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

[14] 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)".

[15] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system (Phase 2+) (GSM); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[16] IETF RFC 1123: "Requirements for Internet Hosts - Application and Support".

[17] IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".

[18] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

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] 3GPP TS 33.128: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security; Protocol and procedures for Lawful Interception (LI); Stage 3".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 221-1 [1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 221-1 [1] and the following apply:

3GPP	3rd Generation Partnership Project
CC	Content of Communication
CSP	Communications Service Provider
DHCP	Dynamic Host Configuration Protocol
DID	Domain IDentifier
GTP	GPRS Tunnelling Protocol
GTP-U	GPRS Tunnelling Protocol - User
GW	GateWay
IP	Internet Protocol
IPID	Interception Point IDentifier
IRI	Intercept Related Information
LI	Lawful Interception
MF	Mediation Function
NAT	Network Address Translation

NF	Network Function
NFID	Network Function IDentifier
OWASP	Open Web Application Security Protocol
PDU	Protocol Data Unit
POI	Point Of Interception
RADIUS	Remote Access Dial In User Service
RTP	Realtime Transport Protocol
SDO	Standards Development Organization
SIP	Session Initiation Protocol
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Tag - Length - Value
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
UUID	Unique Universal IDentifier
XID	X-1 IDentifier

4 Introduction and reference model

4.1 Reference model

The X2/X3 interface is based on communication between:

a) The Point Of Interception (POI), which performs interception.

b) The Mediation Function (MF), which performs the necessary translation, correlation and mediation for onward handover over material to LEAs via the HI2 and HI3 interfaces.

The X2/X3 reference model is shown in figure 1.

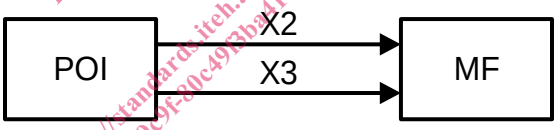

Figure 1: Reference Model

The POI produces internal interception product as part of its normal operation. This internal interception product may consist of copies of network traffic that contain material related to Intercepted Related Information (IRI) or Content of Communication (CC), as defined in ETSI TS 102 232-1 [2]. Material related to IRI is transported via an X2 interface, while material related to CC is transported via an X3 interface.

Any given POI may have one or both interfaces, as specified by the relevant LI architecture. Implementation and deployment scenarios may be more complex. An illustrative list of deployment scenarios is considered in annex B.

4.2 Assumptions

4.2.1 Architecture

The present document makes minimal assumptions about the LI architecture in which the X2/X3 interfaces are deployed. The X2/X3 interface is intended to be sufficiently flexible to be used as part of LI architectures defined elsewhere and assumes that the POI and MF are deployed following an LI architecture defined separately (e.g. by another SDO, industry body or local regulation).

As such, the present document makes no assumptions about the specific functional requirements on the POI with respect to e.g. buffering, de-duplication, filtering. It is expected that these requirements will be supplied by a combination of the relevant LI architecture and local regulation.

4.2.2 Implementation/realization

The present document assumes that implementations of an LI architecture which utilize X1, X2 and X3 can be described by the following high-level model.

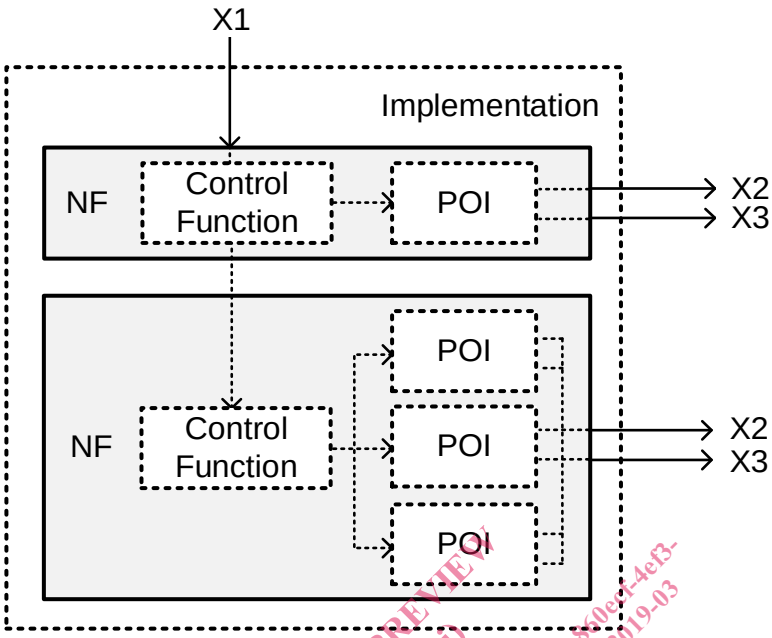

Figure 2: Assumed Implementation Model

The model consists of the following entities:

- An Implementation: This is a concrete realization of one or more NFs as deployed by an implementer.
- A NF: A function as defined by the relevant network and/or LI architecture (e.g. a P-GW in 3GPP LTE).
- Control Function: The sub-function of the NF which accepts LI tasking messages. This may be supplied over a standardized interface (e.g. X1 as defined by ETSI TS 103 221-1 [1]). However, it is assumed that tasking may also be passed between NFs using other unspecified interfaces.
- POI (Point of Interception): The sub-function of the NF which performs interception and emits data. An NF may contain multiple POIs; in this case it is assumed that the NF implementation will be responsible for multiplexing the output of these POIs into a single X2 or X3 output stream.

The present document does not consider the means by which tasking information is communicated from a NF's internal control function to the POI sub-functions but provides the NF implementation a means by which to identify on which NF and POI each piece of data originated.

The present document assumes that the NF may be required to deliver high volumes of traffic (e.g. a broadband connection), and may be implemented on a platform with tight resources and/or performance constraints (e.g. a packet gateway), and as such X2/X3 is required to minimize, as far as is practical, the amount of processing and additional bandwidth consumed (see clause A.1.4).

4.2.3 Deployment infrastructure

The present document assumes that the transport infrastructure between POI/NF and MF is untrusted (see clause A.2.8) but assumes that the platform on which the POI, NF and MF are realized is appropriately secured. It does not make any specific assumptions about whether either the platform or transport infrastructure are virtualized.

The present document does not assume that clocks on different POIs are synchronized. It assumes that while X3 event timestamps may be required by local regulations and can be added to aid describing chronologies of events (e.g. in court), timestamps will not in general permit re-ordering or re-synchronization of packets which have been intercepted at different NFs.