

# ETSI TS 103 221-2 V1.2.1 (2019-12)



## Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3

iTeh STANDARDS PREVIEW  
(standard:it/ai/1980-46af-  
4445-a3b-a846a56beef1/etsi-ts-103-221-2-v1-2-19-12)  
Full standard: <https://standards.itih.ai/catalog/standards/1980-46af-4445-a3b-a846a56beef1/etsi-ts-103-221-2-v1-2-19-12>



---

Reference

RTS/LI-00183-2

---

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](http://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**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

**3GPP™** and **LTE™** 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.

# Contents

Intellectual Property Rights .....	6
Foreword.....	6
Modal verbs terminology.....	6
1 Scope .....	7
2 References .....	7
2.1 Normative references .....	7
2.2 Informative references.....	8
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	8
3.3 Abbreviations .....	8
4 Introduction and reference model.....	9
4.1 Reference model.....	9
4.2 Assumptions .....	10
4.2.1 Architecture .....	10
4.2.2 Implementation/realization .....	10
4.2.3 Deployment infrastructure .....	11
4.2.4 Regulatory assumptions .....	11
4.3 Relationship to other standards .....	11
5 Message contents and parameters .....	11
5.1 Overview .....	11
5.2 PDU Header Fields.....	12
5.2.1 Version.....	12
5.2.2 PDU Type .....	12
5.2.3 Header Length .....	13
5.2.4 Payload Length .....	13
5.2.5 Payload Format .....	13
5.2.6 Payload Direction .....	13
5.2.7 XID .....	13
5.2.8 Correlation ID.....	13
5.3 Conditional attribute fields.....	14
5.3.1 General structure.....	14
5.3.2 ETSI TS 102 232-1 Defined Attribute.....	14
5.3.3 ETSI TS 133 128 Defined Attribute .....	14
5.3.4 ETSI TS 133 108 Defined Attribute .....	14
5.3.5 Proprietary Attribute .....	14
5.3.6 Domain ID (DID) .....	15
5.3.7 Network Function ID (NFID) .....	15
5.3.8 Interception Point ID (IPID) .....	15
5.3.9 Sequence Number.....	15
5.3.10 Timestamp .....	15
5.3.11 Source IPv4 address.....	15
5.3.12 Destination IPv4 address .....	16
5.3.13 Source IPv6 address.....	16
5.3.14 Destination IPv6 address .....	16
5.3.15 Source Port.....	16
5.3.16 Destination Port .....	16
5.3.17 IP Protocol .....	16
5.3.18 Matched Target Identifier .....	16
5.3.19 Other Target Identifier .....	16
5.4 Payload.....	17
5.4.1 Overview .....	17
5.4.2 ETSI TS 102 232-1 Defined Payload .....	17
5.4.3 ETSI TS 133 128 Defined Payload.....	17

5.4.4	ETSI TS 133 108 Defined Payload.....	17
5.4.5	Proprietary Payload.....	17
5.4.6	IPv4 Packet.....	18
5.4.7	IPv6 Packet.....	18
5.4.8	Ethernet Frame Packet.....	18
5.4.9	RTP Packet.....	18
5.4.10	SIP Message.....	18
5.4.11	DHCP Message.....	18
5.4.12	RADIUS Packet.....	18
5.4.13	GTP-U Message.....	18
5.4.14	MSRP Message.....	19
6	Transport.....	19
6.1	Summary.....	19
6.2	TLS Transport Profile.....	19
6.2.1	General.....	19
6.2.2	Profile.....	19
6.2.3	Authentication.....	19
6.2.4	Keepalive mechanism for reliability.....	19
<b>Annex A (normative): Requirements .....</b>		<b>20</b>
A.1	X2 Protocol & Architecture requirements.....	20
A.1.1	Basic Functionality.....	20
A.1.2	Flexible.....	20
A.1.3	Extensible.....	20
A.1.4	Lightweight.....	20
A.1.5	Delay.....	20
A.1.6	Permanent and Dynamic Connections.....	20
A.1.7	Reliability.....	20
A.1.8	Error detection.....	20
A.1.9	Redundancy.....	20
A.1.10	Correlation.....	21
A.1.11	Mediation into HI2/HI3.....	21
A.2	X2 Security requirements.....	21
A.2.1	Authentication and Authorization.....	21
A.2.2	Accounting and Audit.....	21
A.2.3	Integrity Protection.....	21
A.2.4	Confidentiality Protection.....	21
A.2.5	Replay Protection.....	21
A.2.6	Standalone interface.....	21
A.2.7	Minimum Security Level.....	21
A.2.8	Underlying Infrastructure Trust.....	21
A.2.9	Firewall and NAT Transversal.....	22
A.2.10	Certificate and Key Management.....	22
A.3	X3 Protocol & Architecture requirements.....	22
A.3.1	Basic Functionality.....	22
A.3.2	Flexible.....	22
A.3.3	Extensible.....	22
A.3.4	Lightweight.....	22
A.3.5	Delay.....	22
A.3.6	Permanent and Dynamic Connections.....	22
A.3.7	Reliability.....	22
A.3.8	Error detection.....	22
A.3.9	Redundancy.....	23
A.3.10	Correlation.....	23
A.3.11	Mediation into HI2/HI3.....	23
A.4	X3 Security requirements.....	23
A.4.1	Authentication & Authorization.....	23
A.4.2	Accounting/Audit.....	23
A.4.3	Integrity Protection.....	23

A.4.4	Confidentiality Protection .....	23
A.4.5	Replay Protection .....	23
A.4.6	Standalone interface .....	23
A.4.7	Minimum Security Level.....	24
A.4.8	Underlying Infrastructure Trust.....	24
A.4.9	Firewall and NAT Transversal .....	24
A.4.10	Certificate and Key Management.....	24
<b>Annex B (informative): Illustrative deployment scenarios.....</b>		<b>25</b>
B.1	Introduction .....	25
B.2	Simple deployment scenario .....	25
B.3	Individual X3 POIs with shared X2 POI.....	25
B.4	Separated interfaces.....	26
<b>Annex C (informative): Change History .....</b>		<b>27</b>
History .....		28

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)

Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/12f6c78d-46af-4445-a3b-a846a56bee11/etsi-ts-103-221-2-v1.2.1-2019-12>

---

## 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); Internal Network Interfaces; Part 1: X1".
- [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®) Base Specifications, Issue 7".
- [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".

NOTE: Obsoleted by IETF RFC 8446.

- [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".
- [19] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".
- [20] ETSI TS 133 128: "LTE; 5G; Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (3GPP TS 33.128)".

## 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 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://cheatsheetseries.owasp.org/cheatsheets/Transport\\_Layer\\_Protection\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html).

---

## 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	3 <sup>rd</sup> Generation Partnership Project
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
LI	Lawful Interception
MDF	Mediation and Delivery 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
xCC	X3 Content of Communications
xIRI	X2 Intercept Related Information
XID	X1 IDentifier

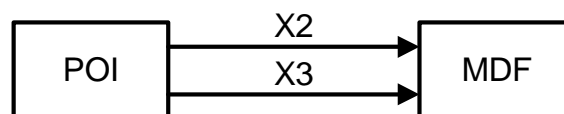
## 4 Introduction and reference model

### 4.1 Reference model

The X2/X3 interface is based on communication between:

- The Point Of Interception (POI), which performs interception.
- The Mediation and Delivery Function (MDF), 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 Intercept Related Information (xIRI) or Content of Communication (xCC). Material related to xIRI is transported via an X2 interface, while material related to xCC 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

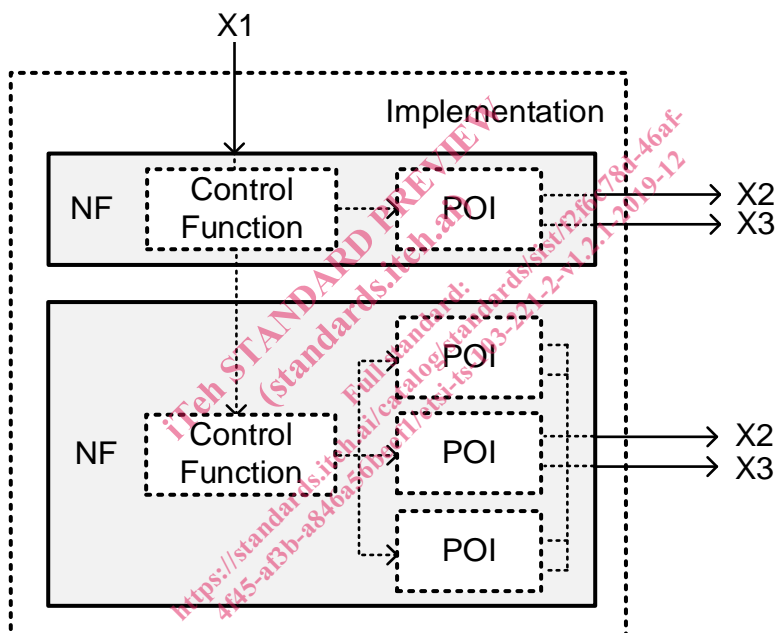
### 4.2.1 Architecture

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 MDF 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.