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

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

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.

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

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); 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.

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
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:

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

b) 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.

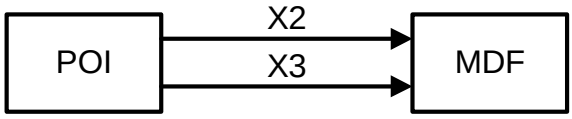

Figure 1: Reference Model

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.

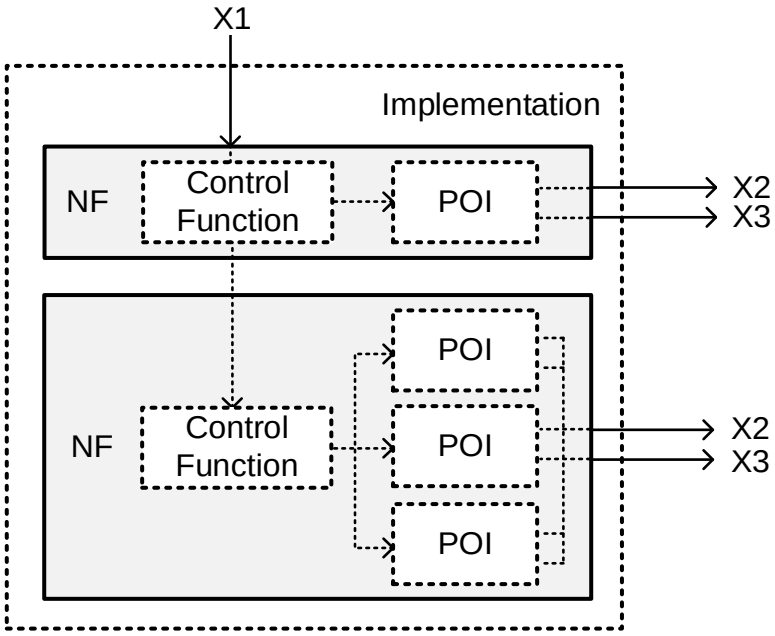

Figure 2: Assumed Implementation Model

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.

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 MDF is untrusted (see clause A.2.8) but assumes that the platform on which the POI, NF and MDF 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.

The present document assumes that X2/X3 is required to provide sufficient information, together with X1, to detect loss of material over X2/X3 (see clause 4.2.4 and clause A.1.8). Detection of loss of material is supported by the Sequence Number field as defined in clause 5.3.6. A mechanism to detect and prevent link failures is supported by the Keepalive /Keepalive Acknowledgement PDUs as defined in clause 5.2.2. Any other POI behaviour to support error recovery is out of scope.

An illustrative list of deployment scenarios that have been considered as part of the design of the X2/X3 interface is given in annex B.

4.2.4 Regulatory assumptions

The present document assumes that material delivered over X2/X3 may be used as evidence in court. As such, it assumes that the X2/X3 interface is capable of indicating when data has been lost over the X2/X3 interface (see clause A.1.8), but recovery of this data (e.g. by buffering and retransmission) are out of scope (as described in clause 4.2.1).

The present document assumes that material over X2/X3 is required to be delivered without undue delay (see clause A.1.5), but that any such latency requirements are not necessarily as stringent as those associated with the underlying communications session (e.g. there is no need for a latency which facilitates a two-way conversation or vehicle avoidance measures).

4.3 Relationship to other standards

The present document forms part of an overall set of standards together with ETSI TS 103 221-1 (X1) [1].

Some models of LI (e.g. ETSI TS 133 108 [15], ETSI TS 133 128 [20]) define interfaces for the purposes described in clause 4.1, (e.g. X2, X3 defined by ETSI TS 133 108 [15] or LI_X2, LI_X3 defined by ETSI TS 133 128 [20]). The present document is designed to fulfil the requirements for those interfaces.

5 Message contents and parameters

5.1 Overview

The POI sends data to the MDF as a binary stream of X2/X3 Protocol Data Units (PDUs). Each PDU is formatted as described in the following clauses.

Each X2/X3 PDU consists of three main sections:

- A set of mandatory header fields containing identifiers, routing and correlation information - see clause 5.2.
- A set of additional optional attributes conveying additional metadata about the intercepted material - see clause 5.3.

- A copy of the intercepted material - see clause 5.4.

The Keepalive mechanism is described in clause 6.2.4. Each Keepalive and Keepalive Acknowledgement PDU consists of:

- A set of mandatory header fields, where the Version, PDU Type and Header Length fields are populated as specified and all other mandatory fields are set to zero - see clause 5.2.
- A Sequence Number - see clause 5.3.9.

NOTE: Populating all other mandatory fields to zero means the Keepalive and Keepalive Acknowledgement PDU does not contain a payload as defined in clause 5.4.

Table 1: X2/X3 PDU Structure

Field Name	Length (octets)	Defined in clause
Version	2	5.2.1
PDU Type	2	5.2.2
Header Length	4	5.2.3
Payload Length	4	5.2.4
Payload Format	2	5.2.5
Payload Direction	2	5.2.6
XID	16	5.2.7
Correlation ID	8	5.2.8
Conditional Attribute Fields	Variable	5.3
Payload	Variable	5.4

Each PDU is sent across an instance of either the X2 or X3 interface. The choice of which interface to use for any given PDU shall be given by the relevant LI architecture.

Definitions and encodings for the fields are given in the clauses 5.2, 5.3 and 5.4. Unless otherwise specified by the present document or another referenced specification, header values shall be given as unsigned integers in network byte order (i.e. big endian).

5.2 PDU Header Fields

5.2.1 Version

The POI shall populate the Version field with the version of the specification used to create the PDU, given as a 16-bit unsigned integer.

For PDUs created against the present document, this shall be set to the value 1.

The version shall be increased by one when a technical change is made to clause 5 of the present document. A technical change is considered to be the addition, update or removal a field. Adding a new choice to a list of choices is also considered an update of a field.

5.2.2 PDU Type

The POI shall populate the PDU Type field to indicate the type of PDU. It shall take one of the following values.

Table 2: PDU Types

Value	Meaning
1	X2 PDU
2	X3 PDU
3	Keepalive
4	Keepalive Acknowledgement

5.2.3 Header Length

The POI shall populate the Header Length field with the length of the header in octets, including the mandatory and any conditional fields that have been populated.

5.2.4 Payload Length

The POI shall populate the Payload Length field with the length of the Payload field in octets.

Keepalive and Keepalive Acknowledgement PDU shall set the field to zero.

5.2.5 Payload Format

The POI shall indicate the format and encoding of the Payload field by setting the Payload Format field to the appropriate value. A list of valid values, and their definitions, is given in clause 5.4.

5.2.6 Payload Direction

The POI shall populate the Payload Direction field with an indication of the direction of the intercepted data or event contained in the PDU.

Permitted values are:

Table 3: Payload Direction

Direction Value	Meaning
0	Reserved for Keepalive mechanism as defined in clauses 5.1 and 6.2.4
1	The direction of the intercepted data or event is not known to the POI
2	The intercepted data or event was sent to (i.e. received by) the target
3	The intercepted data or event was sent from the target
4	The intercepted data or event is a result of intercepted data or events in more than one direction
5	The concept of direction is not applicable to this intercepted data or event

5.2.7 XID

The POI shall populate the XID field with the XID associated with the intercepted product, as assigned by the relevant X1 interface (see ETSI TS 103 221-1 [1]).

An XID is a UUID (see ETSI TS 103 221-1 [1], clause 5.1.2). The XID shall be given as a 128-bit unsigned integer.

Keepalive and Keepalive Acknowledgement PDU shall set the field to zero.

5.2.8 Correlation ID

Where the POI correlates X2/X3 PDUs, the POI shall ensure that PDUs associated with the same communication session are given the same Correlation ID value. The value shall uniquely identify the communication within a given context. The scheme for generating Correlation IDs is defined by the relevant LI architecture. The POI may have to adopt a convention for generating Correlation IDs which enables correlation of the same communication session across multiple POIs but such decisions are out of scope of the present document.

If the POI does not correlate the X2/X3 PDU with any other X2/X3 PDUs the POI shall set the field to zero.

Keepalive and Keepalive Acknowledgement PDU shall set the field to zero.

5.3 Conditional attribute fields

5.3.1 General structure

The POI may provide a number of conditional attributes at the end of the header, as directed by the relevant LI architecture. Each of these attributes has the following Type-Length-Value (TLV) structure.

Table 4: General Conditional Attribute Structure

Field Name	Description	Format
Attribute Type	Indicates the type of field - see table 5	16-bit unsigned integer
Attribute Length	Length of the following Attribute Contents in octets	16-bit unsigned integer
Attribute Contents	As defined by the relevant Field Type	Variable

The present document specifies the following conditional attribute types for use in the X2/X3 Content PDU.

Table 5: Conditional Attribute Types

Attribute Type	Name	Defined in clause
1	ETSI TS 102 232-1 [2] Defined Attribute	5.3.2
2	ETSI TS 133 128 [20] Defined Attribute	5.3.3
3	ETSI TS 133 108 [15] Defined Attribute	5.3.4
4	Proprietary Attribute	5.3.5
5	Domain ID (DID)	5.3.6
6	Network Function ID (NFID)	5.3.7
7	Interception Point ID (IPID)	5.3.8
8	Sequence Number	5.3.9
9	Timestamp	5.3.10
10	Source IPv4 address	5.3.11
11	Destination IPv4 address	5.3.12
12	Source IPv6 address	5.3.13
13	Destination IPv6 address	5.3.14
14	Source Port	5.3.15
15	Destination Port	5.3.16
16	IP Protocol	5.3.17
17	Matched Target Identifier	5.3.18
18	Other Target Identifier	5.3.19
NOTE: This list is designed to be easily extended. If implementers or other Standards Developing Organizations (SDO) find a need for additional attributes, they are encouraged to contact ETSI.		

5.3.2 ETSI TS 102 232-1 Defined Attribute

If used, the field shall contain an attribute defined by ETSI TS 102 232-1 [2].

5.3.3 ETSI TS 133 128 Defined Attribute

If used, the field shall contain an attribute defined by ETSI TS 133 128 [20].

5.3.4 ETSI TS 133 108 Defined Attribute

If used, the field shall contain an attribute defined by ETSI TS 133 108 [15].

5.3.5 Proprietary Attribute

If used, the field shall contain an attribute encoded as described in table 6.

Table 6: Proprietary Conditional Attribute Structure

Field Name	Description	Format
Attribute Owner Length	Indicates the length of the Attribute Owner field	8-bit unsigned integer
Attribute Owner	FQDN indicating the organization responsible for defining the encoding of the attribute. FQDN given in ASCII format according to IETF RFC 1123 [16]	ASCII string
Attribute Value	Contents, encoding defined by the attribute owner	Variable

The field is provided to allow temporary support for implementation where use of a standardized solution supported by the present document is not possible.

5.3.6 Domain ID (DID)

If used, the POI shall populate the DID field with a value that identifies the CSP, network or resource group in which the NF or POI exists. The format and content of the field is left to the relevant LI architecture to define.

5.3.7 Network Function ID (NFID)

If used, the POI shall populate the NFID field with a value that identifies the NF associated with the POI to the MDF. The format and content of the field is left to the relevant LI architecture to define. Depending on the architecture and deployment scenarios, it may be used as a way to identify the type of NF.

5.3.8 Interception Point ID (IPID)

If used, the POI shall populate the IPID field with a value that identifies the POI within the NF. The format and content of the field is left to the relevant LI architecture and implementation to define.

5.3.9 Sequence Number

If used, the POI shall populate the Sequence Number field with the sequence number of the X2/X3 PDU. If used, the Sequence Number shall start at zero and increment by one for each X2/X3 PDU with the same XID, DID, NFID, IPID and Correlation ID context. A separate sequence shall be maintained for X2 and X3 PDUs within the same context.

Once the maximum sequence number is reached, the POI shall restart the sequence number from zero. Use of the field shall be determined by the relevant LI architecture.

5.3.10 Timestamp

If used, the POI shall populate the Timestamp field with the time that the content for the PDU was intercepted.

The time shall be given in POSIX.1-2017 [3] timespec format (i.e. the number of elapsed seconds since the start of the Unix epoch in UTC). The value shall be given as two successive 32-bit unsigned integers, with the first giving the integral part in seconds and the second giving the fractional part in nanoseconds.

NOTE: The timespec format as defined in POSIX.1-2017 [3] identifies the issue that timestamps after the year 2038 cannot be encoded. There is no standardized solution available for this yet. A future version of the present document intends to resolve this when available.

5.3.11 Source IPv4 address

If used, the field shall contain the source IPv4 related to the payload given as four octets in network byte order (i.e. most significant octet first). This attribute is primarily intended for use when using payload formats that strip off the IP-layer encapsulation (e.g. SIP Message). However, implementers should use the IPv4 payload format instead of using this conditional attribute where possible.

5.3.12 Destination IPv4 address

If used, the field shall contain the destination IPv4 related to the payload given as four octets in network byte order (i.e. most significant octet first). This attribute is primarily intended for use when using payload formats that strip off the IP-layer encapsulation (e.g. SIP Message). However, implementers should use the IPv4 payload format instead of using this conditional attribute where possible.

5.3.13 Source IPv6 address

If used, the field shall contain the source IPv6 related to the payload given as sixteen octets in network byte order (i.e. most significant octet first). This attribute is primarily intended for use when using payload formats that strip off the IP-layer encapsulation (e.g. SIP Message). However, implementers should use the IPv6 payload format instead of using this conditional attribute where possible.

5.3.14 Destination IPv6 address

If used, the field shall contain the destination IPv6 related to the payload given as sixteen octets in network byte order (i.e. most significant octet first). This attribute is primarily intended for use when using payload formats that strip off the IP-layer encapsulation (e.g. SIP Message). However, implementers should use the IPv6 payload format instead of using this conditional attribute where possible.

5.3.15 Source Port

If used, the field shall contain the source TCP/UDP port related to the payload given as a 16-bit unsigned integer in network byte order.

5.3.16 Destination Port

If used, the field shall contain the destination TCP/UDP port related to the payload given as a 16-bit unsigned integer in network byte order.

5.3.17 IP Protocol

If used, the field shall contain the IP protocol related to the payload given as an 8-bit unsigned integer.

5.3.18 Matched Target Identifier

If used, the POI shall populate the Matched Target Identifier field with the target identifier that the POI matched against the payload and lead to the interception of this payload. The Matched Target Identifier field shall be given as a TargetIdentifier as defined in ETSI TS 103 221-1 [1], clause 6.2.1.2, table 5. The field shall be given as the contents of the TargetIdentifier tag without the enclosing TargetIdentifier tag itself, encoded in UTF-8.

NOTE: As an example of the above encoding, an IMSI would be encoded as the UTF-8 string "<imsi> 204081234567890</imsi>".

5.3.19 Other Target Identifier

If used, the POI shall populate one or more Other Target Identifier fields with other target identifiers that are known to the POI. The Other Target Identifier field shall be given using the same format as the Matched Target Identifier field (see clause 5.3.8).

5.4 Payload

5.4.1 Overview

The POI shall populate the Payload field with intercepted data, given in the format specified by the Payload Format field (see clause 5.2.5). Table 7 defines the set of permissible Payload Formats and whether each is permitted for use in X2 or X3 PDUs.

Table 7: Payload Formats

Value	Payload Format	Permitted in X2	Permitted in X3	Defined in clause
0	Reserved for Keepalive mechanism	N/A	N/A	5.1
1	ETSI TS 102 232-1 [2] Defined Payload	Yes	Yes	5.4.2
2	ETSI TS 133 128 [20] Defined Payload	Yes	Yes	5.4.3
3	ETSI TS 133 108 [15] Defined Payload	Yes	Yes	5.4.4
4	Proprietary Payload	Yes	Yes	5.4.5
5	IPv4 Packet	Yes	Yes	5.4.6
6	IPv6 Packet	Yes	Yes	5.4.7
7	Ethernet Frame	No	Yes	5.4.8
8	RTP Packet	No	Yes	5.4.9
9	SIP Message	Yes	No	5.4.10
10	DHCP Message	Yes	No	5.4.11
11	RADIUS Packet	Yes	No	5.4.12
12	GTP-U Message	No	Yes	5.4.13
13	MSRP Message	No	Yes	5.4.14
NOTE: This list is designed to be easily extended. If implementers or other Standards Developing Organizations (SDO) find a need for additional payload types, they are encouraged to contact ETSI.				

Where a choice is possible, and unless otherwise specified by the relevant LI architecture or national regulation, implementers should choose the payload format that provides the most encapsulation. As an example, IPv4 Packet should be chosen in preference to RTP packet if the IPv4 data is available.

5.4.2 ETSI TS 102 232-1 Defined Payload

If the ETSI TS 102 232-1 [2] Defined Payload is specified, the Payload field shall contain data specified and encoded by ETSI TS 102 232-1 [2].

5.4.3 ETSI TS 133 128 Defined Payload

If the 3GPP Payload is specified, the Payload field shall contain data specified and encoded according to ETSI TS 133 128 [20].

5.4.4 ETSI TS 133 108 Defined Payload

If the ETSI TS 133 128 [20] Payload is specified, the Payload field shall contain data specified and encoded according to ETSI TS 133 108 [15].

5.4.5 Proprietary Payload

If the Proprietary Payload is specified, the Payload field shall contain data encoded as described in table 8.

Table 8: Proprietary Conditional Attribute Structure

Field Name	Description	Format
Payload Owner Length	Indicates the length of the Payload Owner field.	8-bit unsigned integer
Payload Owner	FQDN indicating the organization responsible for defining the encoding of the payload. FQDN given in ASCII format according to IETF RFC 1123 [16].	ASCII string
Payload Value	Contents encoding defined by the attribute owner.	Variable

The payload type is provided to allow temporary support for implementation where use of a standardized solution supported by the present document is not possible.

5.4.6 IPv4 Packet

If the IPv4 Packet Payload Format is specified, the Payload field shall contain an IPv4 packet encoded as per IETF RFC 791 [4].

5.4.7 IPv6 Packet

If the IPv6 Payload Format is specified, the Payload field shall contain an IPv6 packet encoded as per IETF RFC 8200 [5].

5.4.8 Ethernet Frame Packet

If the Ethernet Payload Format is specified, the Payload field shall contain an ethernet frame encoded as per IEEE 802.3 [6].

5.4.9 RTP Packet

If the RTP Packet Payload Format is specified, the Payload field shall contain an RTP packet encoded as per "RTP packet" definition in clause 3 of IETF RFC 3550 [7], without any IP/UDP encapsulation.

Use of this Payload Format is discouraged for new implementations - handing over RTP with IPv4/IPv6 encapsulation is much preferred.

5.4.10 SIP Message

If the SIP Message Payload Format is specified, the Payload field shall contain a SIP message encoded as per clause 7 in IETF RFC 3261 [8], without any IP/UDP encapsulation.

NOTE: For implementations intending to support compliance with ETSI TS 102 232-5 [18], the use of the Source IPv4/IPv6 Address and Destination IPv4/IPv6 Address conditional attributes is recommended.

5.4.11 DHCP Message

If the DHCP Message Payload Format is specified, the Payload field shall contain a DHCP message encoded as per clause 5, figure 1 in IETF RFC 2131 [9], without any IP/UDP encapsulation.

5.4.12 RADIUS Packet

If the RADIUS Packet Payload Format is specified, the Payload field shall contain a RADIUS packet encoded as per IETF RFC 2865 [10].

5.4.13 GTP-U Message

If the GTP-U Message Payload Format is specified, the Payload field shall contain a GTP Message encoded as per clause 7 in ETSI TS 129 281 [11], without any IP/UDP encapsulation.

5.4.14 MSRP Message

If the MSRP Message Payload Format is specified, the Payload field shall contain an MSRP Message encoded as per IETF RFC 4975 [17], clause 5.1, without any IP/UDP/SIP encapsulation.

6 Transport

6.1 Summary

This clause provides transport profiles that may be used to transport encoded X2/X3 PDUs. The present document specifies a default profile, but further profiles may be defined in future or by the relevant LI architecture or SDO. Implementations shall support at least the default profile.

6.2 TLS Transport Profile

6.2.1 General

If using this profile to send X2/X3 PDUs to the MDF, the POI opens a TLS over TCP connection. TLS is used to perform mutual authentication and identification between the POI and MDF, and to provide confidentiality and integrity protection for X2/X3 PDUs.

NOTE: Multiple TLS connections may be used subject to local agreement. Schemes for distributing PDUs across multiple TLS connections are out of scope of the present document, and are for further study.

6.2.2 Profile

POIs and MDFs shall support TLS, using at least version 1.2 as defined in IETF RFC 5246 [12], supporting the recommendations given in IETF RFC 7525 [13]. Implementations are encouraged to support best practice e.g. the guidance given in OWASP TLS Cheat Sheet section 2.6 [i.1].

New implementations should support TLS 1.3 as defined in IETF RFC 8446 [19].

6.2.3 Authentication

Implementations shall perform mutual authentication using client and server X.509 certificates following IETF RFC 6125 [14].

6.2.4 Keepalive mechanism for reliability

The Keepalive and Keepalive Acknowledgement PDU type shall be supported by POIs and MDFs. This profile enables the use of this mechanism. It is intended as a means for the POI application to verify that the MDF application is still operational, and to disconnect the connection if the MDF is not.

The POI shall send out a Keepalive PDU as defined in clause 5.1 at least every TIME_P1 (by default TIME_P1 shall be 60 seconds).

The MDF shall respond to each Keepalive PDU by sending a Keepalive Acknowledgement PDU as defined in clause 5.1. The Sequence Number in the Keepalive Acknowledgement PDU shall be equal to the Sequence Number in the Keepalive PDU.

If the POI has not seen a Keepalive Acknowledgement PDU within TIME_P2 (by default TIME_P2 shall be 180 seconds) then the POI shall disconnect the connection and shall attempt to reconnect to the MDF and report an error through the X1 interface as defined in ETSI TS 103 221-1 [1].

The Keepalive mechanism may be used on both X2 and X3 interfaces.

Annex A (normative): Requirements

A.1 X2 Protocol & Architecture requirements

A.1.1 Basic Functionality

The interface shall be used for delivery of IRI from the network element, which created the copy of the original content of communication, to the mediation function.

A.1.2 Flexible

The X2 architecture and message exchange technique shall be flexible to allow implementation in both existing and future national and international operator network architectures.

A.1.3 Extensible

The basic message exchange protocol shall allow limited extensibility to support parameters not currently supported by the base protocol.

A.1.4 Lightweight

The protocol shall use a protocol containing minimal options or extensions which are not specifically required by X2.

A.1.5 Delay

The X2 architecture and message exchange technique shall by design not introduce undue delay compared with existing proprietary X2 implementations.

A.1.6 Permanent and Dynamic Connections

The X2 architecture and message exchange technique shall support both permanent connection and dynamic link/connection scenarios.

A.1.7 Reliability

The X2 architecture and message exchange technique shall provide reliable data transfer.

A.1.8 Error detection

The X2 architecture and message protocol shall support error detection (i.e. in case of data loss).

A.1.9 Redundancy

The X2 architecture and message protocol shall support both 1 to 1 and 1 to 2 end point configurations (i.e. for redundancy).

A.1.10 Correlation

The X2 protocol shall provide information necessary to allow correlation at the MDF for information provided over HI2 and HI3.

A.1.11 Mediation into HI2/HI3

The X2 protocol shall provide information necessary to allow correlation at the MDF to comply with the requirements of both the HI2 and HI3 interfaces, where applicable.

A.2 X2 Security requirements

A.2.1 Authentication and Authorization

The X2 architecture and message exchange technique shall provide authentication and authorization of end points.

A.2.2 Accounting and Audit

The X2 architecture and message exchange technique shall provide Accounting and Auditing.

A.2.3 Integrity Protection

The X2 message exchange technique shall provide integrity protection for all messages exchanged between nodes in the X2 architecture. Use of Integrity protection shall be mandatory.

A.2.4 Confidentiality Protection

The X2 message exchange technique shall provide confidentiality protection for all messages exchanged between nodes in the X2 architecture.

A.2.5 Replay Protection

The X2 message exchange technique shall provide replay protection for all messages exchanged between nodes in the X2 architecture.

A.2.6 Standalone interface

The X2 architecture and message exchange technique shall be designed as a standalone physically dedicated LI interface. The design and selection of the protocol shall where possible ensure that vulnerabilities in non-LI interfaces on the same node shall not impact LI interfaces and security.

A.2.7 Minimum Security Level

The X2 architecture and message exchange techniques shall provide a minimum level of security (including cypher suites and key length), which shall be supported by all nodes. At least two algorithms shall be specified. The protocol and algorithms shall be resistant to bid down attack.

A.2.8 Underlying Infrastructure Trust

The X2 architecture and message exchange techniques shall assume by default that the underlying network communication links and infrastructure are untrusted.

A.2.9 Firewall and NAT Transversal

The X2 message exchange technique shall be compatible with existing operator firewall and NAT transversal architectures. The message exchange technique shall not require unrestricted opening of common ports (e.g. port 80 or 21). The message exchange technique shall not prohibit the development of future X2 aware firewall filtering to provide rejection of malicious X2 message at operator security gateways.

A.2.10 Certificate and Key Management

The X2 architecture relies on (where applicable) Certificate and Key Management mechanisms (including Certificate and Key revocation) from X1.

A.3 X3 Protocol & Architecture requirements

A.3.1 Basic Functionality

The interface shall be used for delivery of CC from the network element, which created the copy of the original content of communication, to the mediation function.

A.3.2 Flexible

The X3 architecture and message exchange technique shall be flexible to allow implementation in both existing and future national and international operator network architectures.

A.3.3 Extensible

The basic message exchange protocol shall allow limited extensibility to support parameter not currently supported by the base protocol.

A.3.4 Lightweight

The protocol shall use a protocol containing minimal options or extensions which are not specifically required by X3.

A.3.5 Delay

The X3 architecture and message exchange technique shall not introduce undue delay.

A.3.6 Permanent and Dynamic Connections

The X3 architecture and message exchange technique shall support both permanent connection and dynamic link/connection scenarios.

A.3.7 Reliability

The X3 architecture and message exchange technique shall provide reliable data transfer.

A.3.8 Error detection

The X3 architecture and message protocol shall support error detection (i.e. in case of data loss) specifically only across the interface in question.

A.3.9 Redundancy

The X3 architecture and message protocol shall support both 1 to 1 and 1 to 2 end point configurations (i.e. for redundancy).

A.3.10 Correlation

The X3 protocol shall provide information necessary to allow correlation at the MDF for information provided over HI2 and HI3.

A.3.11 Mediation into HI2/HI3

The X3 protocol shall provide information necessary to allow correlation at the MDF to comply with the requirements of both the HI2 and HI3 interfaces, where applicable - at a minimum the packet-switched parts of the relevant HI2/3 handover standards.

A.4 X3 Security requirements

A.4.1 Authentication & Authorization

The X3 architecture and message exchange technique shall provide authentication and authorization of end points.

A.4.2 Accounting/Audit

The X3 architecture and message exchange technique shall provide Accounting & Auditing.

A.4.3 Integrity Protection

The X3 message exchange technique shall provide integrity protection for all messages exchanged between nodes in the X3 architecture. Use of Integrity protection shall be mandatory.

A.4.4 Confidentiality Protection

The X3 message exchange technique shall provide confidentiality protection for all messages exchanged between nodes in the X3 architecture.

A.4.5 Replay Protection

The X3 message exchange technique shall provide replay protection for all messages exchanged between nodes in the X3 architecture.

A.4.6 Standalone interface

The X3 architecture and message exchange technique shall be designed as a standalone physically dedicated LI interface. The design and selection of the protocol shall where possible ensure that vulnerabilities in non-LI interfaces on the same node shall not impact LI interfaces and security.

A.4.7 Minimum Security Level

The X3 architecture and message exchange techniques shall provide a minimum level of security (including cypher suites and key length), which shall be supported by all nodes. At least two algorithms shall be specified. The protocol and algorithms shall be resistant to bid down attack.

A.4.8 Underlying Infrastructure Trust

The X3 architecture and message exchange techniques shall assume by default that the underlying network communication links and infrastructure are untrusted.

A.4.9 Firewall and NAT Transversal

The X3 message exchange technique shall be compatible with existing operator firewall and NAT transversal architectures. The message exchange technique shall not require unrestricted opening of common ports (e.g. port 80 or 21). The message exchange technique shall not prohibit the development of future X3 aware firewall filtering to provide rejection of malicious X3 message at operator security gateways.

A.4.10 Certificate and Key Management

The X3 architecture relies on (where applicable) Certificate and Key Management mechanisms (including Certificate and Key revocation) from X1.

Annex B (informative): Illustrative deployment scenarios

B.1 Introduction

This annex provides a list of illustrative X2/X3 deployment scenarios for consideration during the drafting of the present document.

B.2 Simple deployment scenario

This scenario shows a simple deployment where separate POIs provide X2 and X3. Two POIs connect to a single MDF with an X2 interface from one POI and an X3 interface from another POI.

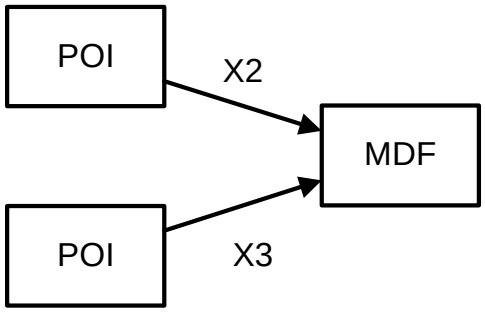

Figure B.1: Simple deployment scenario

B.3 Individual X3 POIs with shared X2 POI

This scenario shows a deployment scenario where a single physical POI provides X2 to multiple MDFs, while each MDF receives X3 from a different POI.

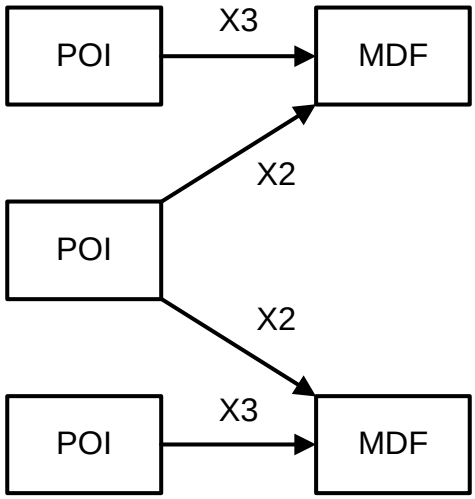

Figure B.2: Individual X3 POIs with shared X2 POIs

B.4 Separated interfaces

This scenario shows a deployment scenario where the X2 and X3 interfaces are delivered to different MDFs.

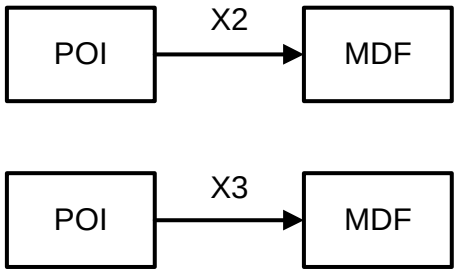

Figure B.3: Separated interfaces

Annex C (informative): Change History

Status of Technical Specification ETSI TS 103 221-2 Internal Network Interfaces; Part 2: X2/X3		
TC LI approval date	**Version**	**Remarks**
February 2019	1.1.1	First publication of the TS after approval by ETSI TC LI#50 (5-7 February 2019, Dubai)
October 2019	1.2.1	Included Change Requests: CR001 (cat D) Clarification on Encoding CR002r1 (cat C) Making the requirements annex informative CR003r2 (cat B) Update for TLS 1.3 CR004r1 (cat D) Alignment to 3GPP terminology These CRs were approved by TC LI#52 (15-17 October 2019, Turin)

History

Document history		
V1.1.1	March 2019	Publication
V1.2.1	December 2019	Publication