ETSI TR 103 727 V1.1.1 (2021-11)

Lawful Interception (LI);
Library and mapping for Lawful Interception (LI) and Lawful Disclosure (LD)

Reference
DTR/LI-00187

Keywords
lawful disclosure, lawful interception

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

Modal verbs terminology

In the present document "**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.

Introduction

The objective of the present document is to enable the exchange of information between Law Enforcement Agencies (LEAs), for example across the European Union and other partners or associated countries in the context of e-Evidence. For this purpose, the ETSI TS 102 232 family ([i.6] for part 1) of specification for LI, and ETSI TS 103 707 [i.2] related to messaging aspects for OTT CSPs, and the Inter LEA Handover Interface (ETSI TS 103 462 [i.5]), are used as *lingua franca* and are complemented by national formats when necessary. For matters related to Lawful Disclosure the same approach is taken with ETSI TS 102 657 [i.3] and ETSI TS 103 120 [i.4].

In a first part, mapping aspects between the indicated ETSI specifications and national formats are considered. The second part, which starts with clause 7, provides a library covering operational aspects such as connection parameters between the requesting and responding Law Enforcement Monitoring Facility (LEMF) or specific parameter formats (checklists, see also Annexes B and C of the present document).

The present document is not intended to promote the use of national formats, rather, it takes into account the existing situation (as of publication) with a view towards increased use of ETSI specifications.

1 Scope

The present document describes the handling of national parameters and implementations in the context of the Inter LEA Handover Interface and cross-border data exchange in criminal matters, e.g. through Mutual Legal Assistance Treaty (MLAT) or using the secure European Judicial Network. In combination with the Inter LEA Handover Interface (ILHI) specification this is a practical guideline for Law Enforcement Agencies and vendors of LEMF.

One aspect is the mapping of national data structures and single parameters into a related ETSI standard and, if necessary, also the mapping back into the national structure.

In addition, the present document gives an overview about the necessary parameters for the handover itself in the form of a library (checklists) for Lawful Interception (LI) and Lawful Disclosure (LD). For the library no special values for the parameters are specified, but the (bilateral) tuning of these parameters is facilitated. For the deployment cases where no ETSI conformant implementation is available, the present document provides examples of mapping between national formats and the ETSI format for LI.

The juridical aspects for using the provided mapping are out of scope of the present document.

The considerations provided in the present document do not modify, override, or otherwise introduce incompatible changes to ETSI or national standards, nor do they prescribe requirements on communication service providers.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 232-2 (V3.11.1): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[i.2] ETSI TS 103 707: "Lawful Interception (LI); Handover for messaging services over HTTP/XML".

[i.3] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".

[i.4] ETSI TS 103 120: "Lawful Interception (LI); Interface for warrant information".

[i.5] ETSI TS 103 462: "Lawful Interception (LI); Inter LEMF Handover Interface".

[i.6] 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".

[i.7] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[i.8] Bundesnetzagentur TR TKÜV 7.1: "Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften: Ausgabe 7.1" ("Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway: Technical Guideline for implementing legal measures for telecommunications surveillance and information disclosure: Edition 7.1").

[i.9] Bundesnetzagentur TR TKÜV: "Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften" ("Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway: Technical Guideline for implementing legal measures for telecommunications surveillance and information disclosure").

NOTE: Available in German and English under https://www.bnetza.de/tku. In case of doubt, the German version takes precedence.

[i.10] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[i.11] ETSI TS 103 643: "Techniques for assurance of digital material used in legal proceedings".

[i.12] EU Commission services: "E-evidence - cross border access to electronic evidence".

NOTE: Available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

[i.13] W3C® Recommendation: "Extensible Markup Language (XML) 1.0".

NOTE: Available at https://www.w3.org/TR/xml/.

[i.14] W3C® Recommendation: "XML Path Language (XPath) 3.1".

NOTE: Available at https://www.w3.org/TR/xpath-31/.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

administrator: member of administrative staff that can attend to the arrangements between authorities discussed in the present document

system operator: member of technical staff that can attend to the proper functioning of computing and network elements involved in the implementation of technical measures discussed in the present document

3.2 Symbols

Void.

3.3 Abbreviations

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

ASN.1	Abstract Syntax Notation One
CC	Content of Communication
CDATA	Character DATA
CSP	Communication Service Provider
DSL	Digital Subscriber Line
DTD	Document Type Definition
e-Codex	e-justice Communication via online data exchange

eEDES	e-Evidence Digital Exchange System
EIO	European Investigation Order
EJN	European Judicial Network
EPOC	European Production Order Certificate
EPOC-PR	European Preservation Order Certificate
HTTP	HyperText Transfer Protocol
ILHI	Inter LEA Handover Interface
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRI	Intercept Related Information
LD	Lawful Disclosure
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception IDentifier
LMTP	Local Mail Transfer Protocol
MAC	Medium Access Control
MapF	Mapping Function
MLAT	Mutual Legal Assistance Treaty
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NTT	Non-Traditional Telecommunication service provider
OCR	Optical Character Recognition
OID	Object IDentifier
OSI	Open Systems Interconnection
OTT	Over-The-Top
PCAP	Packet CAPture
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
POP3	Post Office Protocol
PS	Packet Switched
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SUPI	Subscriber Permanent Identifier
TIFF	Tag Image File Format
URI	Uniform Resource Identifier
VI	Valuation Indicator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WGS84	World Geodetic System 1984
XML	eXtensible Markup Language
XSD	eXtensible markup language Schema Definition

4 Overall aspects

4.1 Operational considerations

There exist technical and operational aspects that are outside the scope of the present document, in particular handling of operational and confidential information that cannot be provided herein. This includes, but is not limited to:

- Maintenance of mapping tables:
  - Technical update of the mapping (for example, the mapping tables or methods could be updated).
  - Description of the mapping in a distributable document (e.g. in a specification).

  - Configuration management including version management and archival of mappings.
  - Notification procedures between responsible parties regarding such updates.
  - Platform for information exchange of mapping updates.
- VPN configuration, for example:
  - Technical configuration (communication system, protocols, algorithms, encryption procedures, key management).
  - Registration and acceptance procedures.

Several options are available to responsible authorities for the handling of out-of-scope information, which may decide:

- To include such information as an informative annex to the present document.
- To disclose such information within the European Judicial Network (EJN)/e-Codex/eEDES.
- To disclose such information as part of bilateral agreements between the issuing and executing authorities.

4.2 Connectivity

Enabling information exchange between Law Enforcement Agencies implies that systems share compatible connection parameters at transport level. This is particularly relevant for aspects that are not fully defined in the ETSI TS 102 232 family ([i.6] for part 1) of specifications for LI and for example ETSI TS 102 657 [i.3] and ETSI TS 103 120 [i.4] for LD. These aspects are summarized in clause 7 while details are left to national implementation.

4.3 Information security and accuracy

For the transfer of information through ILHI mechanisms are needed to ensure at least integrity protection and proof of origin of the data. These mechanisms can be built into the transport layers or into the application layer.

In addition to the traditional requirements for information security, a translation mechanism between the ETSI formats for LI and LD, and national formats introduces additional requirements on the usability of the data. Indeed, the data is to be used in investigations and legal proceedings (also as e-evidence), implying several properties that are listed below:

- Data translated from one format to another retains its semantic value, i.e. the two parameters represent the same type of information (e.g. an IP address) even if the format is different.
- When data is translated, it remains accurate (i.e. the representation unit and value of a datum is not modified).
- When data is imported into a national system, where such data is not defined by the national framework, it is to be annotated in such a way that it can be interpreted without doubt.
- The digital processes transforming the data are repeatable and deterministic as defined in ETSI TS 103 643 [i.11].
- As an extension, non-purely digital processes such as digital scans or OCR are also repeatable and deterministic, in the sense that they always lead to equivalent results for all intend and purpose.

The high-level reference model to be used for guaranteeing information security and accuracy during the mapping process is illustrated in figure 4.3-1.

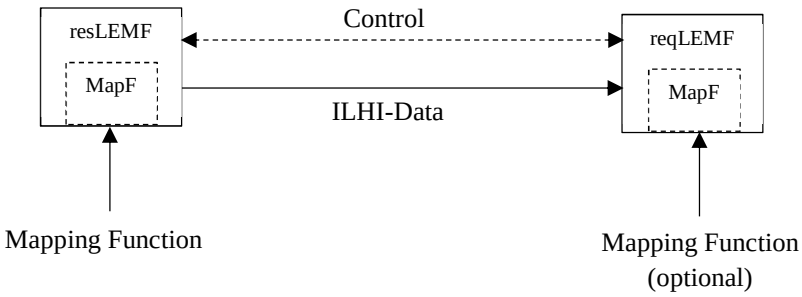

Figure 4.3-1: Reference model for the mapping process between requesting and responding LEMF

The following information is exchanged in the reference model:

- ILHI-Data: Payload of the requested data.
- Control: Connectivity for e.g. the tasking process keep-alive or error messages.

4.4 Handling of mapping details

Procedures are needed to identify and remedy cases where it is not possible to translate data between the ETSI format and the national format. Such procedures are described in clauses specific to each mapping.

5 Mapping methods

5.1 Overview

The present clause introduces common mapping methods that can be used when converting data instantiated according e.g. to the ETSI TS 102 232 ([i.6] for part 1) family of specifications and national formats. Beyond the general case, LI and LD specific methods, as well as real-time aspects, are considered.

An example mapping is provided in Annex A of the present document. In order to keep track of future mappings, it is envisioned that such mappings, or their references (if they are confidential), will be collected in revisions of the present document or will be stored in a registry, to ensure awareness among Law Enforcement Agencies on the matter of cross-border data exchange.

5.2 Mapping management

5.2.1 Generalities

A mapping is always defined against a specification number and version. For example, ETSI TS 102 232-2 [i.1] with German TR TKÜV version 7.1 [i.8]. This allows the requesting and responding parties to determine usability of a mapping and to manage mappings according to changes implemented either in the ETSI specifications or in the national specifications.

Because a mapping involves two sets of specifications, it is useful to name parameters differently to help the reader quickly understand where the parameter is coming from. For example, parameters coming from one set of specifications can be named *fields*, while parameters coming from the other set of specifications can be named *elements*. These names can be chosen according to the data format (typically, the name *elements* suits the XML convention).

There are cases where data formats can hold parameters with the same name in different positions of the data structure. Yet, these parameters are distinct and could be subject to different mapping rules. In such situation, it is recommended that the mapping includes a convention for locating a parameter within the relevant data structure. For example, XPath [i.14] can be used in the case of XML [i.13]. In the case of ASN.1, a convention can be to use a string containing each intermediary object, in the order of traversal, separated by dots. An example is given in clause A.2.2.3.1.

A mapping is normally accompanied by ancillary documentation where the requesting and responding parties agree at least on configuration of required support services and interconnections, as well as acceptance and management procedures, as described in clause 4.1.

5.2.2 Version handling

To facilitate identification and version control, it is recommended that a master version identifier (such as a version number) be assigned to each instantiation of the combination of the mapping documentation and ancillary documentation, such as instantiations that are (or were) in force as well as intermediary development versions. Within each instantiation, mapping documentation and ancillary documentation can also be versioned and summarized in a manifest to allow exhaustive inventory and avoid mistakes in the handling of mapping-related documents between the parties. It is recommended that the parties agree a versioning scheme for this purpose. Figure 5.2.2-1 below provides a documentation hierarchy example. Each component in the hierarchy can be versioned.

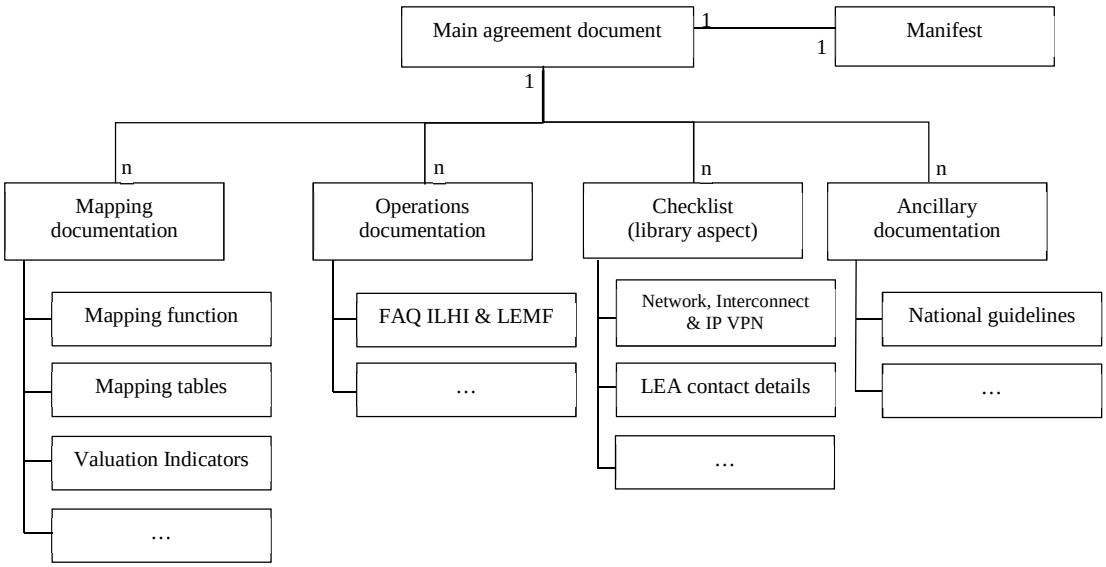

Figure 5.2.2-1: Documentation hierarchy example

The mapping tables are expected to be part of the documentation as reference for administrators and system operators. They can also be declared in machine-readable form usable by the Mapping Function (clause 6.1 of the present document) or by the requesting party for the automatic identification of usable data through valuation indicators (clause 6.2 of the present document).

5.2.3 Fully specified mapping

To ensure trust on the data by the requesting LEMF it is recommended that the mapping between the national format and ETSI TS 102 232 ([i.6] for part 1) family and other relevant specifications (for example ETSI TS 103 120 [i.4]) be fully documented and made available to all relevant stakeholders.

5.3 General methods

5.3.1 Name change

Differences in names are to be accounted for in the mapping rules between two formats.

5.3.2 Translation between sets

Parameters that can hold typed values (for example, flags) can have different values in each format, yet for each value of a parameter in a format, there will be a semantic equivalent in the other format. The mapping rules between the two formats are to provide clear correspondence rules between the two sets. Table A.2.2.3.1-1 provides an example of such translation.

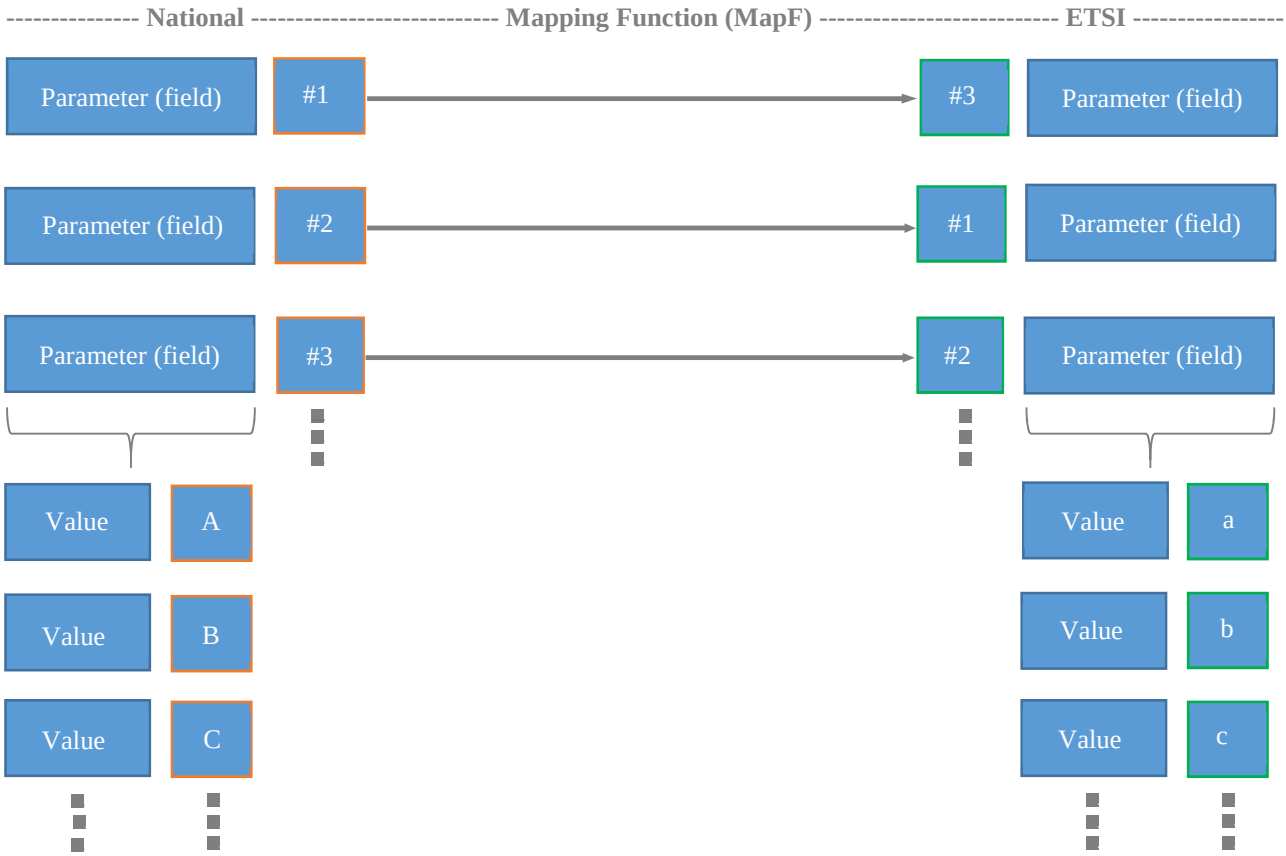

Figure 5.3.2-1: An example of translation between two sets

5.3.3 Format change

Parameters referring to the same data across two formats can be represented by different data types. This can be the case e.g. with phone numbers, timestamps, and location data but also basic data types such as integers and strings, which would also require careful considerations. The mapping is to provide clear rules to ensure proper conversion. In some cases, the conversion can lead to partial data loss, such as a loss in accuracy.

NOTE: Whether a loss in accuracy is relevant under clause 4.3 of the present document is to be evaluated on a per-parameter basis. This information can be conveyed through valuation indicators as defined in clause 6.2.

For example, phone numbers are represented in E.164 notation in ETSI TS 102 657 [i.3], location data is represented in WGS84 notation in ETSI TS 103 462 [i.5], and timestamps are represented in QualifiedDateTime or QualifiedMicrosecondDateTime notation in ETSI TS 103 280 [i.10].

5.3.4 Encodings

It can be necessary to convert data from one encoding to another. For example, between an octet string (binary string) representation or one of the ASN.1 encoding rules to base64. In such case, the specificities of each encoding is to be accounted for in order to prevent data corruption. This entails making sure that the set of possible values for raw data is the same in both encodings, or at least, the same for the conversion being considered. Sometimes this is not possible, in particular when comparing an encoding designed for transport to an encoding designed for data representation and processing, where the latter puts limits on what is valid data. Thus, it can become necessary to select a destination encoding that is not optimal for the representation of the data but allows transport between LEMF and processing by the requesting LEMF. A simple illustration of this problem is the digitization of physical documents. Table A.2.3.3.1-1 provides an example of such encodings.

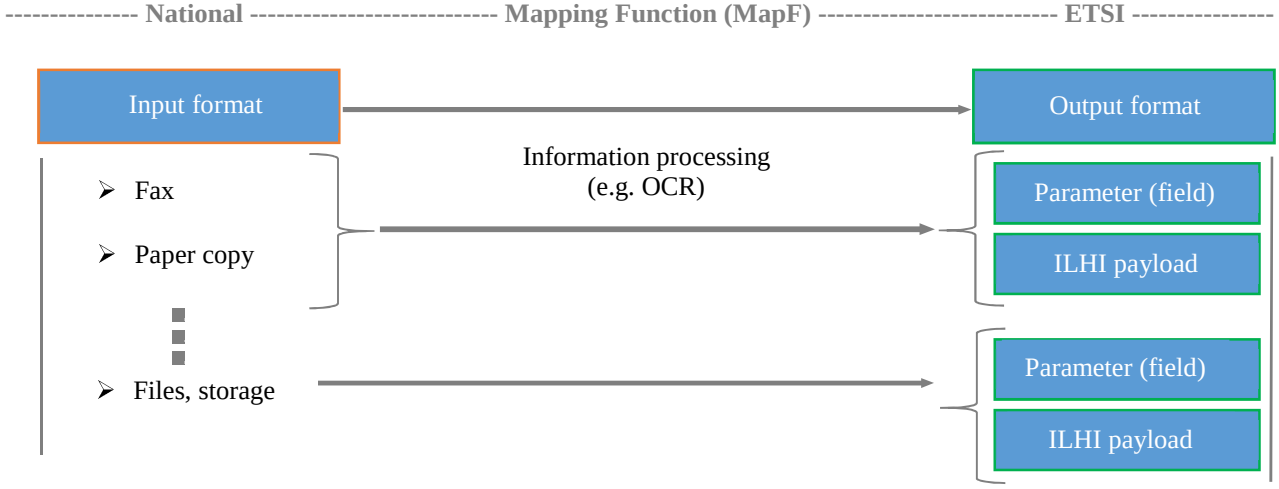

Figure 5.3.4-1: An example of mapping that can require reencoding

5.4 LI and real-time specific methods

The mapping is to consider several real-time or near real-time operations, that can have an impact for delivery across ILHI:

- Real-time transcoding of Content of Communication (CC), when different codecs are used.
- Real-time translation into CC-related LI-PS-PDU headers.
- Translation into IRI, whereby the responding side translates IRI from the national format to the relevant ETSI format, while the requesting side will possibly need to post-process the data, for example by looking-up identifiers.

5.5 LD and non-real-time specific methods

The mapping is to consider implementations aspects related to the processing of data at rest, such as data storage capabilities and processing of the data. Although the handover of LD data is expected to be mostly non real-time and can accommodate manual processing when automation is not possible, two aspects in particular are noteworthy:

- Firstly, data that has been provided to an LEA as part of Lawful Disclosure can have been subject to application layer protection measures arranged between the LEA and the originating CSP, such as encryption, proof of origin, and integrity protection, that depend on security parameters managed by the CSP and the LEA. Were the data to be provided to the requesting party as-is, it would not be possible for the requesting party to validate its security properties involving the originating CSP. If these are still present, it is recommended that the responding party removes the protection artefacts applied to the data by the originating CSP, and only applies those protection that have been agreed with the requesting party as part of the mapping (refer to clauses 7.4 and 7.5).
- Secondly, LD data, especially business data, can be in formats and languages that are not by default supported by the requesting party (for example, contracts are not written in an official language of the requesting party). The responding party will likely not be in a position to transform the LD data, as these can be in different formats in both jurisdictions, that have not been standardised at an international or even national level. It is recommended that the nature, format and languages of the LD data be examined during the establishment of the mapping, for the purpose of informing the requesting party.

The E-evidence homepage maintained by the EU Commission services [i.12] can help finding further information on non-real-time requirements for cross-border data exchange.

6 Identification and handling of mapping details

6.1 Overview

The present clause provides information on the mapping function and the various aspects to be considered when handling a mapping. A high-level view of the mapping definition and the mapping function is given in figures 6.1-1 and 6.1-2.

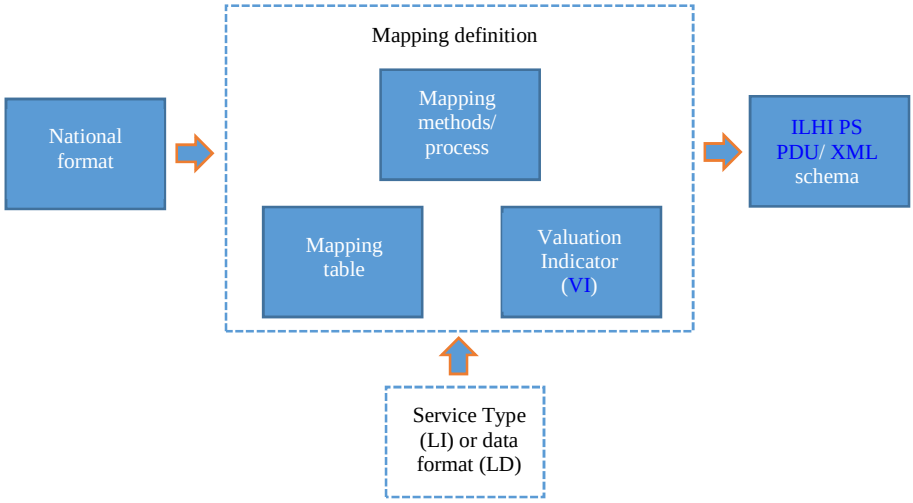

Figure 6.1-1: Relationship between national and ETSI formats through the Mapping definition

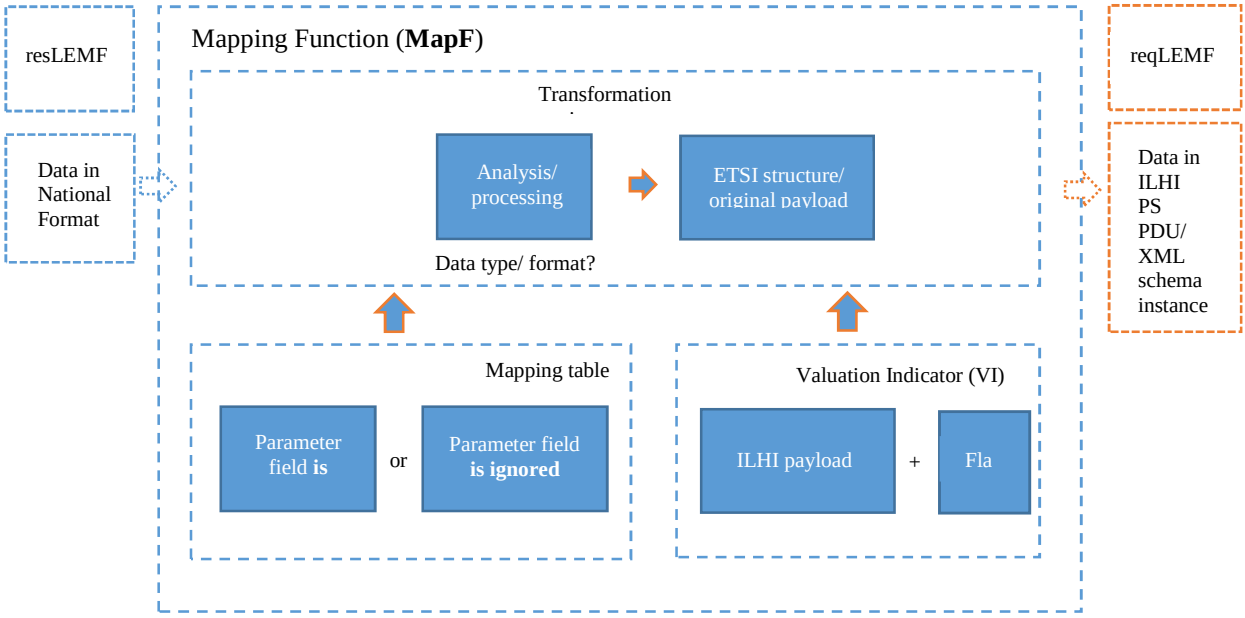

Figure 6.1-2: Data transformation through the Mapping Function

Depending on the service type or data format, a Mapping is defined that describes the correspondence between a specific national format and the ETSI ILHI PS PDU/XML schema format (figure 6.1-1). This Mapping is taken as input to the Mapping Function (MapF) that transforms data instantiated in a national format into data instantiated in the ETSI format through a transformation engine (figure 6.1-2). Further details regarding the Mapping Function are described in the following clauses.

6.2 Information on translation accuracy and data trustworthiness - valuation indicators

The translation engine evaluates a translated item according to its knowledge of the translation rule: either the rule allows 100 % accuracy translation, or it is technically known that it is not the case. The receiving party can find this information in the mapping table in the form of an additional indicator on accuracy, more generally named a valuation indicator on accuracy. A valuation indicator expresses the quality of the mapping information based on a technical assessment conducted during its establishment. The mapping table and Valuation Indicators (VI) are exchanged out-of-band between the parties (see figure 6.1-2).

Similarly, a **valuation indicator on completeness** can be used to indicate whether the mapping allows a particular piece of data to be translated in full (without loss of data).

The **evaluation of the mapping quality** (accuracy and completeness of the translated data) is not a real-time operation, it is the result of a study of the options available to the responding and requesting parties for the conversion of data from a national format to the ETSI format. When the sending and receiving party agree on a mapping, the indications of accuracy and completeness are used as formal reference by both parties. For cases where a translation does not permit full accuracy or completeness of specific data, both parties are to decide whether said data is to be converted and handed over through the mapping function, or whether it is to be handed over in its original form through the originalPayload mechanism, possibly with the responding authority providing assistance to the requesting authority for the interpretation of the data.

It can be tempting to label data as *not suitable for evidence* as a result of a technical evaluation of a mapping method, and to document this in the mapping documentation. In some countries this would not be appropriate because that is a matter which would be assessed by the court based on the situation under consideration. For example: a location with a possible inaccuracy of up to 5 km would still be suitable in evidence as a way to indicate that the individual in question was not 1 000 km away from the specified location (e.g. could safely be used to cast doubt on an assertion that the individual took a flight at a given time). In this situation it would be unhelpful and incorrect to have marked that location as *not suitable for evidence*. It is therefore recommended to evaluate the mapping methods on their technical merit, and to select the originalPayload mechanism in case the mapping method would not be technically suitable.

Tables 6.2-1 and 6.2-2 provide guidance on how to handle the information provided by the valuation indicators.

Table 6.2-1: Guidance on data handling depending on the valuation indicator on accuracy

Data handling (flag)	Details of evaluation in the mapping justifying the handling method	Comment
The data is to be handled in the mapping	The mapping method preserves 100 % accuracy of the data: • The translated data retains its semantic meaning. • The translated data retains the same level of accuracy as the original data (the representation unit and value of a datum is not modified). • The translation mechanism for the data used by the sending party is deterministic.	
The data is to be handled in the mapping under specific rules	The mapping method introduces an acceptable deviation from 100 % accuracy: • The translated data has a lower level of accuracy than the original.	Both parties, especially the requesting party, are to evaluate whether the deviation is acceptable. This typically depends on operational aspects of the requesting party. For example, a loss of accuracy on location data might still be acceptable to prove facts at the granularity of the new accuracy. In case the deviation is determined to be not acceptable, the data is to be handled outside of the mapping, through the originalPayload mechanism.
The data cannot be handled within the mapping, the original data is to be handed over as originalPayload	The mapping method(s) available, if it were used, would not allow to preserve data accuracy, and is therefore not to be used: • The translated data would have different semantic meaning. • The translated data would purport to have better accuracy than the original data. • The translation mechanism for the data used by the sending party would not be deterministic - part of the data would thus be "random".	

Table 6.2-2: Guidance on data handling depending on the valuation indicator on completeness

Data handling (flag)	Details of evaluation in the mapping justifying the handling method	Comment
The data is to be handled in the mapping	The translated data remains complete (the translation process does not filter out part of the data).	
The data is to be handled in the mapping under specific rules	The mapping method introduces an acceptable deviation from data completeness. The translated data is a filtered version of the original data.	Both parties, especially the requesting party, are to evaluate whether the deviation is acceptable. This typically depends on operational aspects of the requesting party. For example, a loss of completeness in the form of the oldest events being filtered out, but the more recent ones remaining in the data set, might still be acceptable. In case the deviation is determined to be not acceptable, the data is to be handled outside of the mapping, through the originalPayload mechanism.
The data cannot be handled within the mapping, the original data is to be handed over as originalPayload	The translated data is an augmented version of the original data.	

It is recommended that both parties aim for a thorough establishment of valuation indicators for each data translation when establishing the mapping. It is further recommended that the valuation indicators and selected handover method for each data type are indicated in the mapping documentation. An example evaluation of the valuation indicator on accuracy is given in Annex D of the present document.

The assurance on translation accuracy and data trustworthiness depends on the overall chain of events that are related to the processing and handover of the data from the trusted domain of the responding party to the trusted domain of the requesting party. This involves in particular:

- Gathering of the data by the responding party.
- Possible filtering of the data by the responding party.
- Translation of the data from the national format into the relevant ETSI format by the responding party.
- Reception of the data by the requesting party.
- Any additional processing required by the requesting party (such as filtering of the data).

NOTE: One reason for filtering data is the existence of legal requirements forbidding the sending or processing of certain types of data.

Through this chain of events, methods are required to ensure information security as well as accuracy. This includes, for example:

- Identification of the translation methods and indicators of translation accuracy as defined earlier in the present clause.
- Hashing mechanism.
- Version numbering.
- Packing and transmitting of the original payload and indication of format to serve as reference.

The valuation indicators can also be used by the requesting party for the automatic identification of the data source. This can be a useful feature for personnel relying on the data, as this avoids time-consuming manual checks against the mapping documentation. There is however no straightforward way to transfer the information as part of ILHI. One approach is to use a separate machine-readable configuration file, which would then need to be managed as any other documentation asset of the mapping (see clause 5.2.2 of the present document).

Last but not least, when the mapping method introduces an acceptable deviation from 100 % accuracy or from data completeness, it is recommended that the requesting party considers the ability of data processing system (outside the boundary of the handover interface) to distinguish between data that has not gone through a mapping and data that has been subject to a mapping where specific rules are required for the handling of said data (refer to Annex D of the present document for examples). How to conduct this evaluation is out of scope of the present document. When the distinction is not possible, it can be preferable to hand over the data unmodified, through an instance of originalPayload.

6.3 Information on parameters not defined in the ETSI format

When an equivalent parameter does not exist in the ETSI destination format, the following approaches are identified:

- The original parameter is ignored, and this is indicated in the mapping table.
- The national parameter field is used, and this is also indicated in the mapping table.
- The original payload parameter (in ILHI convention) is provided, and used by the receiving party to extract the parameter.

A field is to be added to the mapping table, indicating how non-supported parameters in the destination format are provided by the sender. When the original payload (in ILHI convention) is used, this field can include information on how the payload is structured and the relevant parameters encoded. Most importantly, it includes information on fields in the original payload that are relevant to a given topic, as agreed by administrators, allowing further automatic or manual processing on the receiving end. One possible solution is the use of the originalPayload field (as defined in ETSI TS 103 462 [i.5]) where the identifier field is set to a value reserved for the mapping and the structure of the originalPayload field described through a dictionary, following an approach similar to that of ETSI TS 103 120 [i.4], where ETSI TS 103 280 [i.10] is used as reference for the equivalence of parameters when appropriate. It is recommended that a national authority operating with a national format maintains a single mapping profile of fields not supported in the ETSI format into the original payload parameter, in order to avoid discrepancies in cross-border data exchange with multiple authorities.

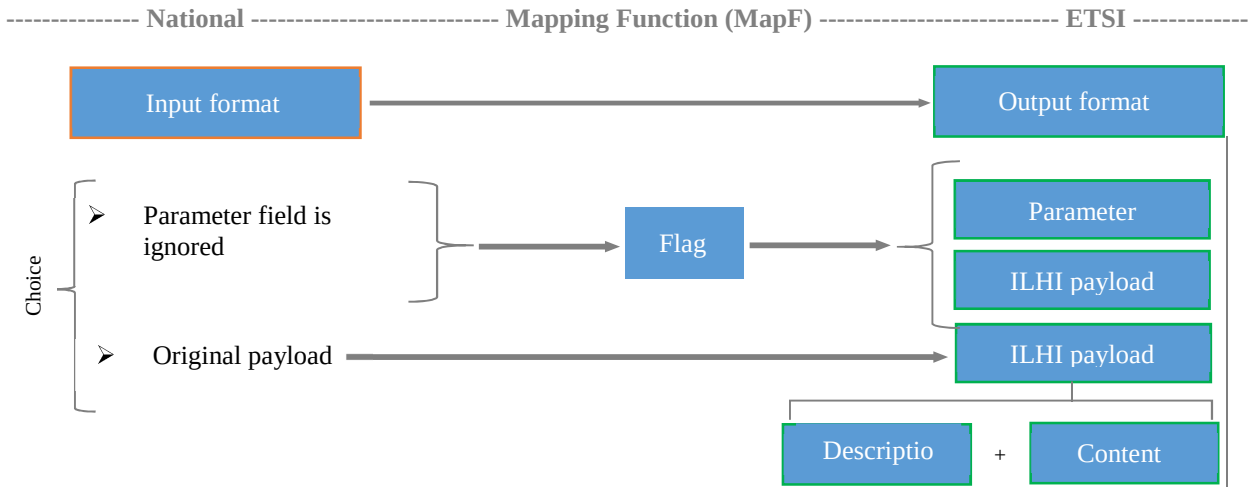

Figure 6.3-1: Mapping process for national parameters

Table 6.3-1 provides an exemplary description of the originalPayload used to transport unsupported parameters in the ETSI format.

Table 6.3-1: Example description of the originalPayload structure used to deliver unsupported ETSI parameters

Metadata			
Field	**Description**		
Title	The title of the present table		
Purpose	This field describes how the present table is used in the mapping, for example, what kind of unsupported data the table is valid for, or in which situations it is to be used		
Owner	This field provides a description of the authority(ies) that manage the present table		
Identifier	Value that identifies the present description and is used as the value of the identifier field in the EncapsulationPayload as defined in ETSI TS 103 462 [i.5]		
Version	Version of the present description (refer to clause 5.2)		
Local dictionary definitions			
Field	**Description**	**Format or reference**	
DictionaryEntry1	A description of the purpose and usage of this dictionary entry	Specification of the field format (e.g. as a regular expression) or reference to an entry of an existing dictionary (e.g. in ETSI TS 103 280 [i.10])	
DictionaryEntry2	A description of the purpose and usage of this dictionary entry	Specification of the field format (e.g. as a regular expression) or reference to an entry of an existing dictionary (e.g. in ETSI TS 103 280 [i.10])	
Structure description			
Field/Structure in originalPayload	**Reference to the ETSI format and use**	**Description**	**Format or reference**
Level1Field1	If the field/structure extends existing parameters in the ETSI format, this can be indicated here	Description of the field: what is represents, how it can be used by the requesting party	Specification of the field format (e.g. as a regular expression, ASN.1 or XML definition), or reference to a local dictionary definition, or to an entry of an existing dictionary (e.g. as in ETSI TS 103 280 [i.10]
Level1Struct1			
Level1Struct1Field1			
Level1Struct1Field2			
Level2Struct1			
…			
End of Level2Struct1			
End of Level1Struct1			
Level1Field2			
Level1Field3			
…			
NOTE: The structure description and names used in the originalPayload in the present table is to be taken as guidance. For example, each row of the table can describe one field/parameter or can be used to declare or close a new structure. The designer is free to express nested structures, fields as they see fit within the above table. The same goes for field and structure names.			

6.4 Mandatory parameter in the destination format that is not available in the source format

There can be cases where the destination format expects a mandatory parameter that is not available in the source format - for example, because such parameter is not considered relevant in the source format. This can be solved by using values in the destination format that represent the unavailability or inapplicability of the data (e.g. NULL in SQL), henceforth named inert values. Depending on the semantic of the parameter in the destination format, such inert value can be natively supported and used without requiring an extension of the destination format nor a modification of existing implementations. The concept of inert values is best illustrated by the NULL marker as defined in the Structured Query Language (SQL), which is used to indicate that information is not present (hence, the NULL marker is different from the value 0).

When the requesting and responding parties envision the use of an inert value, it is recommended that they consider the following steps:

1) An inert value is supported in the destination format and can be used to replace a value expected from the source format. This usability is verified up to the application layer and within existing implementations of the requesting parties.

2) An inert value is not available, but an alternative value can be selected, which achieves the same purpose, as with the previous point.

3) No solution based on an inert value or equivalent alternative value is available. In this case the requesting and responding parties cannot take the mapping in operation, and an alternative solution is to be found, which is out of scope of the present document.

6.5 Information that can only be provided by deduction

In some cases, information that is required by the destination format can be deduced from the source format. For example, a destination port can be deduced from a protocol identifier. When using such methods, the accuracy of the deduction is to be considered.

6.6 Parameter values that do not match across formats

A variant to clause 6.3 is that a parameter can have semantically different values across two formats. In such case, there is no other choice but to extend the destination format with new values for a parameter, that semantically match those in the source format.

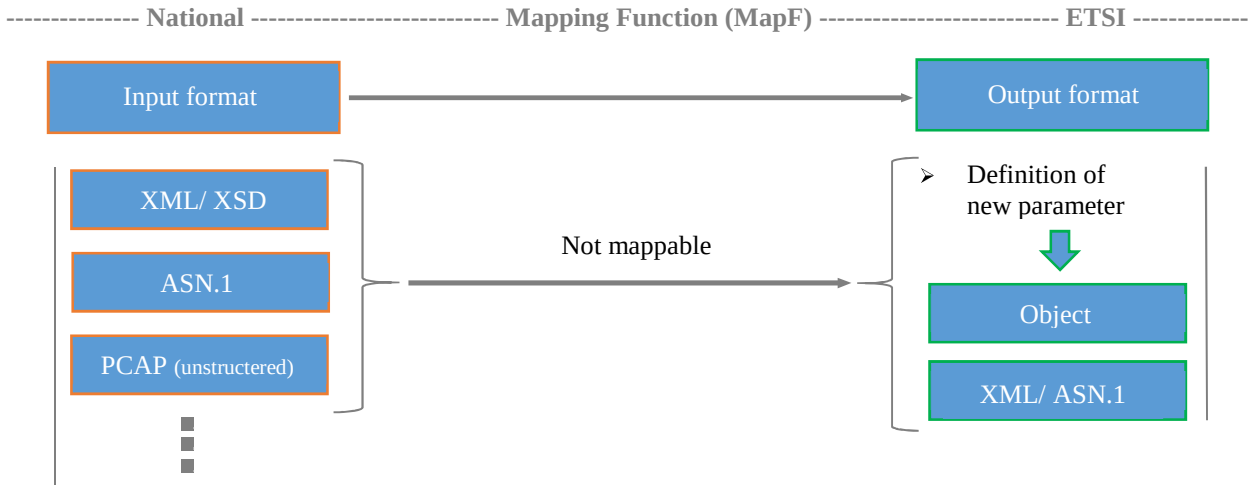

Figure 6.6-1: Approaches on not identified information on parameters in the ETSI format

6.7 Handling of information loss

As introduced in clause 5.4, some translation methods can result in information loss. This is the case where the translation results in a loss of accuracy, or when the destination format cannot be updated to support a new parameter or parameter value that is present in the source format. Whether such information loss is critical in view of clause 4.3 is to be analysed by the issuing and executing authorities and depends on each parameter and the expected technical and legal effect of the loss, on a case-by-case basis.

6.8 Translations requiring an out-of-band request

Some translations can require an out-of-band mechanism to translate one parameter to another. For example, the LIID according to ETSI TS 102 232-1 [i.6] might not be present in a national format. A supporting function for out-of-band requests would be required to perform such translation during processing. A translation could be needed during the following phases:

- At the moment a request is received from the requesting party by the responding party, in order to prepare the gathering of data on the side of the responding party. For example, the responding party might resolve a target identifier to the subject's identity, and from there resolve the subject's identity into all target identifiers the responding party is aware of. This implies that the responding party maintains capabilities for identifying and retrieving such relations (e.g. in the form of database lookups) or searching for them (e.g. in the form of full text search).
- At the moment data in a national format is being translated into the format as specified in the ETSI TS 102 232 ([i.6] for part 1) family of specifications. For example, a separate service would be used to request an LIID as an alias to a national identification number and, if such alias does not yet exist, to register it. This implies that the responding party maintains a facility allowing creation, and long-term storage and lookup of such information.

6.9 Details relevant to mappings into national formats

6.9.1 Handling of parameters that are not defined in the national format

It is possible that some fields in the ETSI format will have no equivalent in the national format. If it is needed to preserve such fields, then extensions to the national formats may be necessary. However, the ability of existing implementations that are using the national format, to cope with such new extensions, is to be verified before deciding on an extension. This includes parsing, storage, search, and display of the field value to the user, among other aspects.

6.9.2 Non extensible national format

When the destination format cannot be extended, it can be useful to consider an out-of-band mechanism to carry dedicated data objects in order to convey in raw form the information that could not be translated, typically using the grammar of the requesting LEMF (for example, ASN.1, XML or XML Schema) and adapting the data structure to hold a reference allowing a binding with the data sent as part of the destination format. This can be used to convey unsupported parameters or parameters holding unsupported values in both the LI and LD domains, and give the receiving LEA an opportunity to request further information about those or save them for later analysis. It is recommended that the receiving LEA identifies the information that will be provided as extension to the destination format, and consider obligations with regard to the processing of such data (for example, there may be data that the requesting LEA may not be allowed to process, such data is typically discarded by the responding LEMF or discarded by the requesting LEMF before further processing). The following flow chart provides an example of handling non-extensible destination format.

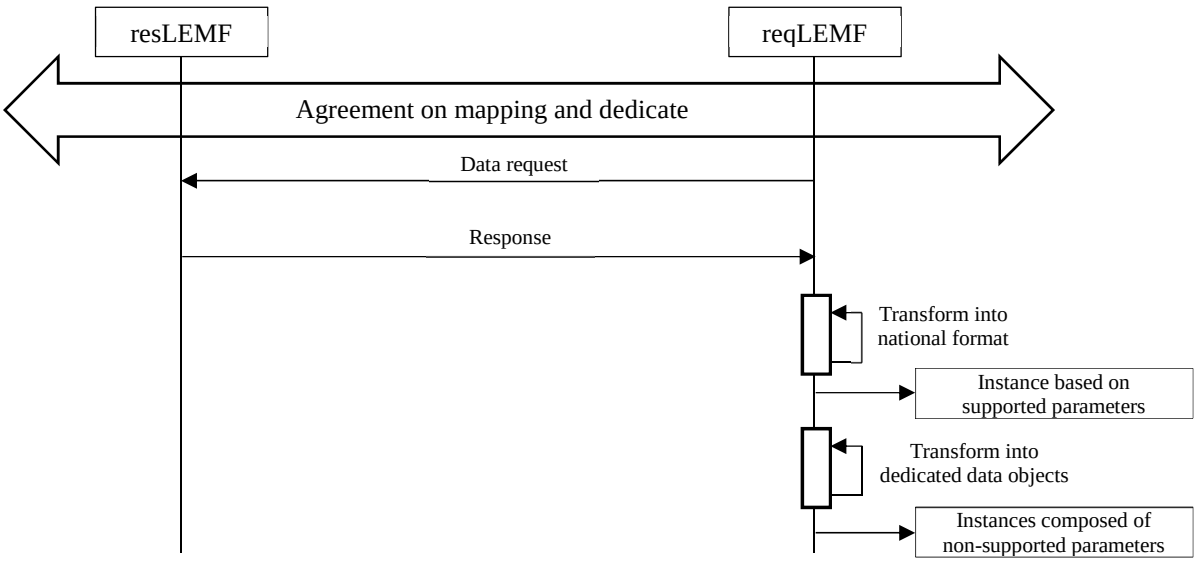

Figure 6.9.2-1: Example handling of non-supported parameter within a national format (done by the requesting LEMF)

6.10 Requirements on input data

Before the responding LEMF processes data through the mapping function, it is recommended that the following characteristics of the input data are validated:

- *Unmodified data*:
  - The responding LEMF checks that the input data to the mapping function is the original data as was provided by the CSP.
- *Compliance to the defined mapping*:
  - The responding LEMF checks that there is no *unknown* value or parameter in the input data set, that cannot be translated through the defined mapping.
- *Qualified data*:
  - For data that requires a qualifier, the responding LEMF checks that the qualifier is present (e.g. for a timestamp, a time zone is present or inferable). Enforcing these characteristics can be done through technical means or a legal framework that is applicable to the local jurisdiction. For example, it could be mandated that timestamps appended to digital evidence collected in a given jurisdiction be assumed to be in the local time zone when there is no time zone information.
- *Qualified processes*:
  - When the digital evidence, that is being provided as input to the transformation engine, is itself the result of a transformation, the responding LEMF checks that process which led to the digital evidence is clearly identified and described. For example, when material evidence is being digitized (typically, a scanned version is obtained from a paper contract), the requirements on the process, equipment and operator are clearly described and identified. While this aspect in not part of the response to the requesting LEMF itself, it can be an important factor to the continuity of data assurance.

6.11 Handling of errors and fail-safe behaviour

6.11.1 Generalities

The introduction of a transform between a dataset in a national format and a dataset in the ETSI format introduces a new potential point of failure. In order to avoid losing data or sending incorrect data, a responding LEMF can implement error handling mechanisms. At the most basic level this includes safekeeping and reporting of incorrectly formatted input data (refer to clause 6.10 of the present document), avoiding silent errors in the transformation engine (i.e. any execution path that does not lead to output data is to be reported), as well as the queuing and rescheduling of transforms that require out-of-band requests, until the services providing resolution of out-of-band requests are available again. It is recommended that transforms that can be rescheduled are also subject to a configurable maximum timeout, such that a system operator can be timely informed of any delays in providing information to the requesting LEMF.

In addition, it is likely that not all transform errors can be handled at the level of the system operator. It is therefore recommended that alternative means of providing the data to the requesting LEMF be agreed beforehand among administrators, and that processes are set to handle errors due to a misconfiguration of the mapping, e.g. to update the mapping arrangements.

6.11.2 Advanced scenarios

Many options for handling errors are possible, the following is a non-exclusive list of examples:

- The LEA operating the requesting LEMF is not interested in some of the possible data types that the responding LEMF may return. Such data types that are not relevant can be communicated to the responding LEMF, for example through a bilateral agreement managed by administrators, or as part of the mapping. When an error occurs on a data type that was indicated as not relevant by the requesting LEMF, the responding LEMF can ignore the offending data type. It is recommended that the error still be recorded and attended to, as the interests of the requesting LEMF may change over time.

- The raw data that is causing the error is packed and sent as-is to the requesting LEMF, which may be able to interpret the data with assistance from the authority managing the responding LEMF. While details for such arrangement are out of scope of the present document, it is recommended that alternative means for transferring data between two LEMFs and for interpreting the data are put in place by administrators to give good assurance that the requesting LEMF obtains the requested data.

- System updates, software errors, or hardware errors, may cause temporary failures with the transformation engine, which can be handled with deferral of protocol requests or routing the requests to a secondary endpoint. Ideally, both the requesting and the responding LEMF would be operating under principles of high availability. It is recommended that bilateral agreements cover service level agreements and the resolution of system unavailability through secondary channels.

7 Operational aspects

7.1 Overview

The present clause provides guidance for the setup of operational aspects of cross-border data exchange between two LEMFs. The intent is not to be prescriptive but rather highlight the various aspects that can influence connectivity and performance aspects when two information exchange systems are interconnected. A checklist summarizing the guidance in the form of action points is provided in Annexes B and C. The present document makes no assumption whether the agreed operational aspects are made public or kept private as part of bilateral agreements, or to which degree of detail such operational aspects are addressed.

The aspects covered in the present clause include:

- Interconnects, routing and transport in clause 7.2.

- The higher OSI layers in clause 7.3.

- Trust and assurance in clause 7.4.
- Security in clause 7.5.

7.2 Interconnects, routing and transport aspects

It is beneficial to identify early on the topology requirements for interconnection. The endpoints of a LEMF could be accessible on the public internet, reside on a private network accessible through a gateway, or require access through leased lines. Other configurations are possible. Practical aspects to considers include routing, identification of network errors, and, for the proper performance of higher protocol layers, available end-to-end bandwidth, MTU and round-trip times. Protocol encapsulation, packet or frame processing and forwarding, as well as cryptographic functions operating at the network layers in hardware or software can all affect performance.

The choice of interconnection between LEMF endpoints influences the trust and security models to be put in place: security requirements will be different, for example, between an approach based on domain security and firewalls, and a zero-trust approach.

Key parameters to agree can include, in an exemplary and non-limitative manner: protocol types, MPLS labels or VLAN tags, and scrambling boxes or VPN configuration information (protocol, endpoint addresses and ports, security parameters such a algorithms and keys).

It is to be noted that national authorities may rely on publicly available information exchange infrastructure, such as file upload or e-mail services, for the transfer of LI and LD data at national level. In such case, adaptation is required to provide an end-point compatible with cross-border data exchange protocols.

7.3 Higher OSI layers

Key aspects to consider include the choice or protocols at transport, session, and presentation layers, including the transactional model. Most of these aspects are standardized in ETSI TS 102 232-1 [i.6], ETSI TS 103 462 [i.5] and other relevant ETSI and 3GPP specifications, however the following parameters may also be considered for performance reasons:

- Where possible, PDU size at various protocol layers to ensure efficient transfer of large files. In particular, identification of all protocol encapsulation overhead is paramount to avoid inefficient packet fragmentation by intermediary network elements (which are configured according to known MTU), that can result in packet drops.
- Data retransmission features and configuration thereof.
- Size of in-memory and on-disk transmission buffers. For example, the maximum size of a single file and the maximum size of data transferred in a single session can be defined to ensure that receiving endpoints are configured accordingly and fitted with enough hardware capacity.
- Default timeouts for established sessions, keepalive methods and frequency, and session resumption arrangements.
- Failure modes and error reporting. In particular, situations where a system cannot fail gracefully, for example by queuing and rescheduling of transfer attempts, or cannot transfer information under time constraints, are to be identified and error reporting allowing operator intervention implemented.
- Maximum number of parallel sessions (or open connections per host).

7.4 Trust and assurance

The assurance that the data provided by the responding LEMF can be trusted by the requesting LEMF is an essential aspect to consider, in particular for digital evidence. Several options are possible.

One option is to consider that the authentication of the responding LEMF and integrity protection on the data provided by the transport or session layer between the responding LEMF and the requesting LEMF are enough to provide assurance on the legitimacy and integrity of the data.

Another option is to rely on the digital signature mechanisms in ETSI TS 102 232-1 [i.6] to provide assurance on the provenance and integrity of the data from the responding LEMF to the requesting LEMF. With this latter approach the responding LEMF is responsible for maintaining assurance internally and the requesting LEMF is responsible for maintaining the continuity of assurance after the data has been received from the responding LEMF.

In both cases data assurance can be maintained at each step of the data preparation by the responding LEMF, transfer to the requesting LEMF, and further processing by the requesting LEMF. The following steps illustrate an example approach based on digital signatures:

a) The responding LEMF uses locally defined methods for maintaining assurance on digital evidence within their jurisdiction (e.g. a hash-based mechanism as defined in ETSI TS 103 643 [i.11], or another method, is implemented by the LEA operating the responding LEMF).

b) The responding LEMF prepares the digital evidence and filters away those security artefacts that are used to maintain data assurance in the domain of the responding LEMF.

c) The responding LEMF ensures that the digital evidence that is input to the transformation engine fulfils the assurance requirements applicable within their jurisdiction.

d) The responding LEMF ensures that the digital evidence that is input to the transformation engine fulfils the characteristics requirements (as derived from the agreed mapping framework) applicable to the input data.

e) The responding LEMF ensures that the mapping configuration fulfils the requirements of the mapping framework agreed with the requesting LEMF.

f) The responding LEMF performs the data transformation and applies a digital signature to the resulting data according to ETSI TS 102 232-1 [i.6].

g) The requesting LEMF assumes that assurance on the digital evidence is provided by the responding LEMF by virtue of the ETSI TS 102 232-1 [i.6] compliant digital signature applied to the data transformed into the ETSI TS 102 232-1 [i.6] compliant format.

NOTE: These steps are meant for the responding and requesting LEMF. The CSPs are not involved in the above.

LEAs are likely to have differing approaches to handling trust but need to find common grounds for cross-border data exchange. For example, the use of the above approach requires agreement on the digital signature algorithm(s) to be used and on key management methods, including processes pertaining to a trusted authority, which can be a trusted third party. It is recommended that LEAs involved in cross-border data exchange identify their data assurance requirements and carefully select which measures to implement, such as those described in steps a) to f) above, in particular based on the risks, technical or legal, that can be introduced by any candidate measures.

The E-evidence homepage maintained by the EU Commission services [i.12] can help finding further information on requirements for cross-border data exchange including continuity of assurance.

7.5 Security

It is recommended that the mapping or bilateral agreement between authorities covers the security aspects of data transfer between the LEMFs. It is further recommended that the following properties be considered across the complete network and protocol stack:

- Confidentiality of communication, including the exposure of the LEMF as a network function related to law enforcement (non-detectability) and the identification of authorities.
- Integrity of communication.
- Authentication, authorization, and accountability of peers at any layer.
- Integrity and proof of origin of transferred LI and LD data.

Setting up protocol security between two LEMFs requires administrators to agree on configuration parameters as part of the mapping or bilateral agreement for all of the involved protocol layers, as illustrated in clauses 7.2 and 7.4 of the present document. Access control mechanisms at the session and application layers can also require specific configuration. This includes agreeing on stakeholders' roles as trusted third parties, and on the management of user identities, shared secrets, public keys and/or certificates, as well as the semantic value of digital signatures, when these are used - e.g. as in clause 7.4. It is therefore possible that the authorities will have to act as Certificate Authorities, or rely on trusted third parties for such purpose. It is beneficial for the authorities to identify the security measures that can give assurance on the validity and usability of the data as legal evidence. As with clause 6.11 of the present document, it is recommended that authorities have processes in place to monitor errors related to security mechanisms, and for handling those that relate to usability. Examples includes removal of users, failures with key rotations, expirations of certificates, and revocation of certificates. Certificate revocation is prone to many weaknesses and shows its limits in emergency situations. Polling mechanisms introduce delays while push mechanisms have scalability issues and are sensitive to communication failures. In any case, active monitoring is required to ensure all parties are up to date.

NOTE 1: These examples are illustrative, the actual scope of errors to monitor and handle depends on the actual deployment.

NOTE 2: Other aspects of security, such as the instantiation of the LEMF, are also relevant although not in scope of the present document.

While not directly related to the security of the ILHI, it is recommended that LEAs consider security measures for communications related to the operations of the ILHI, such as communications between administrators, and backup data transfer method. Examples for the former include secure messaging and teleconference services, and for the latter server-based or messaging-based secure file transfer methods.

The E-evidence homepage maintained by the EU Commission services [i.12] can help finding further information on requirements for cross-border data exchange including continuity of assurance.

Annex A:
Mapping catalogue

A.1 Overview

The present annex provides a placeholder for publicly available mappings. It can be extended as new mappings becomes available. To illustrate some of the principles laid out in the present document, an exemplary mapping between the German TR TKÜV 7.1 [i.8] and ETSI TS 102 232-2 [i.1] is provided in clause A.2.

A.2 Example mapping for e-mail: German TR TKÜV 7.1 and ETSI TS 102 232-2

A.2.1 Overview

The present annex provides an example of how a mapping could be defined, taking as illustration a possible way of mapping between the German e-mail xml-schema and the ETSI TS 102 232-2 [i.1] ASN.1 format. The German e-mail xml-schema taken as reference in the present example is the Technical Guideline TR TKÜV 7.1 [i.8] for implementing legal measures for telecommunications surveillance and information disclosure (Annex F, Specifications for storage equipment for the e-mail service). No assumption is made as to the compatibility of this mapping against any other versions of TR TKÜV [i.9]. It is recalled that a mapping is always defined against a specific version of a technical specification (refer to clause 5.2.1 of the present document).

The version in English of Technical Guideline TR TKÜV 7.1 [i.8] is provided for information only. While encoding the element and parameter names of the national based solutions (e.g. XML-Codecs in Annexes E and F) the corresponding German terms are to be used. Furthermore in cases of wrong or misleading translations the German version of the Technical Guideline supersedes this translation.

Throughout the present annex, in order to avoid confusion, parameters originating from ETSI TS 102 232-1 [i.6] and ETSI TS 102 232-2 [i.7] are named *fields*, while parameters from TR TKÜV 7.1 [i.8] are named *elements* (following the XML convention).

A.2.2 Mapping from German TR TKÜV to ETSI TS 102 232-2

A.2.2.1 Generalities

The information provided in the German TR TKÜV 7.1 [i.8] <hi3-email> element is to be converted into an ETSI TS 102 232-1 [i.6] compliant PDU with the extensions defined in ETSI TS 102 232-2 [i.1].

A.2.2.2 Mapping of parameter names

The fields in the target PDU are mapped from the <hi3-email> element according to tables A.2.2.2-1 and A.2.2.2-2.

Table A.2.2.2-1: EmailCC PDU

Field name in ETSI 102 232-2 [i.7]	Status in ETSI 102 232-2 [i.7]	Status in TR TKÜV/Analysis
emailCCObjId	M	To be set to OID value as per ETSI TS 102 232-2 [i.7], Annex D.
email-Format	M	To be set to application(2).
content	M	To be set to the content of the <email> element decoded from base64.

EmailIRI PDU

Table A.2.2.2-2: EmailIRI PDU

Field name in ETSI 102 232-2 [i.7]	Status in ETSI 102 232-2 [i.7]	Status in TR TKÜV/Analysis
emailIRIObjId	M	To be set to OID value as per ETSI TS 102 232-2 [i.7], Annex D
eventType	M	To be set from the value of the <Richtung> <direction> element according to tables A.2.2.3.1-1, A.2.2.3.2-1 and A.2.2.3.3-1
client-Address	O	To be set to the value of the <IP> element
server-Address	O	This information is not available, the field is not present
client-Port	O	This information is not available, the field is not present
server-Port	O	This information is not available, but could be inferred from the protocol identifier in the <Port> element using their officially registered ports (well-known ports), although this method may not be 100 % accurate - it may lead to incorrect information - and therefore it is advisable not to instantiate this field
server-Octets-Sent	M	This information is not available
client-Octets-Sent	M	This information is not available
protocol-ID	M	To be translated from the value of the <Port> element according to table A.2.2.3.5-1. However, there can be cases when the <Port> element is not set in the "TR TKÜV xml-file"
e-mail-Sender	O	To be set to the value of the <Partner-Kennung> <ID of the involved partner> element according to the rules in table A.2.2.3.5-1
e-mail-Recipients	O	To be set to the value of the <Partner-Kennung> <ID of the involved partner> element according to the rules in table A.2.2.3.5-1
status	M	To be set to SUCCESS when the value of the <Ausloesegrund-zueA> <reason of terminating the connection> element was 'erfolgreich'/'successful', or to FAILED for any other value of the element
total-Recipient-Count	O	Inference from the value of the <Partner-Kennung> < ID of the involved partner > element or analysis of the e-mail content may not provide a value semantically equivalent to ETSI TS 102 232-2 [i.7], clause 7.5
message-ID	O	To be set to the value of the <Zuordnungsnummer> <message identifier> element
nationalParameter	O	Not used in this mapping.
national-EM-ASN1parameters	O	The national-EM-ASN1parameters parameter is not used
aAAInformation	O	This information is not available
e-mail-Sender-Validity	O	This information is not available

The nationalParameter field may already be used to convey parameters defined within the national scope of the requesting party. It is therefore good practice that the responding party does not use this field to convey information available within the data format of the responding party, but not supported in the ETSI format. Instead, this information can be handed over within an instance of originalPayload.

In the context of the present mapping, the originalPayload instance could contain the following elements:

- <Versionskennung>/<version>.
- <Datensatzart>/<type of data set>.
- <Referenznummer>/<LIID>.
- <Kennung des zueA>/<target ID>.
- <Beginn>/<begin>.
- <Einstellungen>/<settings>.
- <Ausloesegrund-zueA>/<reason of terminating the connection>.
- <Beginn-UEM>/<begin UEM>.

- <Ende-UEM>/<end UEM>.

Some of these elements can be used to populate a LI-PS-PDU header.

NOTE: the parameter <Ausloesegrund-zueA> is kept as it can contain more information than the status field (in case of error).

A.2.2.3 Translation rules

A.2.2.3.1 Translation from <Richtung> (<direction>) element to eventType field when the protocol is SMTP

Source attribute	/hi3-email/Richtung/
Destination attribute	PS-PDU.payload.iLHIPayload.resPayload.contents.pspdu.payload.iRIPayloadSequence.iRIContents.emailIRI.eventType

In such case the translation is to follow the rules in table A.2.2.3.1-1.

Table A.2.2.3.1-1

Event	Comments	Element value	Corresponding eventType field value	Analysis
Receipt of an e-mail	Regardless of whether it is delivered directly to the monitored user or stored in the mailbox.	'received'	e-mail-receive(2)	No particular concern.
Transmission of an e-mail	The e-mail server transmits a stored e-mail.	'sent'	e-mail-send(1)	No particular concern.
Forwarding of an e-mail	E-mails which are received and subsequently forwarded.	'sent'	e-mail-send(1)	The semantic of 'forwarding' does not exist in ETSI TS 102 232-2 [i.7] and thus the information would be lost. Possible remedies are: 1) use the e-mail-send(1) value for the eventType field but include the <Richtung> <direction> element as part of the nationalParameter field to preserve the information; 2) extend E-mail-Event with a new e-mail-forward value in the ASN.1 module.

A.2.2.3.2 Translation from <Richtung> (<direction>) element to eventType field when the protocol is POP3

Source attribute	/hi3-email/Richtung/
Destination attribute	PS-PDU.payload.iLHIPayload.resPayload.contents.pspdu.payload.iRIPayloadSequence.iRIContents.emailIRI.eventType

In such case the translation is to follow the rules in table A.2.2.3.2-1.

Table A.2.2.3.2-1

Event	Comments	Element value	Corresponding eventType field value	Analysis
Retrieval of an e-mail	The monitored user retrieves a complete or partial e-mail from his mailbox (e.g. only the header, subject or attachment).	'retrieved'	e-mail-download(3)	In the TR TKÜV 7.1 [i.8] format there is no distinction between complete and partial download of an e-mail, thus the value should always be set to e-mail-download(3). In particular there is no way to determine the status when a file in TR TKÜV 7.1 [i.8] format is converted to the ETSI TS 102 232-2 [i.7] format.

A.2.2.3.3 Translation from <Richtung> (<direction>) element to eventType field when the protocol is IMAP

Source attribute	/hi3-email/Richtung/
Destination attribute	PS-PDU.payload.iLHIPayload.resPayload.contents.pspdu.payload. iRIPayloadSequence.iRIContents.emailIRI.eventType

In such case the translation is to follow the rules in table A.2.2.3.3-1.

Table A.2.2.3.3-1

Event	Comments	Element value	Corresponding eventType field value	Analysis
Storing an e-mail	A message produced by an e-mail client is stored in an IMAP directory (using the IMAP command APPEND) and then synchronized with the server.	'stored'	e-mail-upload(9)	No particular concern.
Retrieval of an e-mail	The monitored user retrieves a complete or partial e-mail from his mailbox (e.g. only the header, subject or attachment). In IMAP, however, only those e-mails transmitted between client and server as part of a synchronization of folders (as new e-mail) should be monitored.	'retrieved'	e-mail-download(3)	Similar as for e-mail retrieval with POP3.

A.2.2.3.4 Translation from <Port> element to protocol-ID field

Source attribute	/hi3-email/Port/
Destination attribute	PS-PDU.payload.iLHIPayload.resPayload.contents.pspdu. payload.iRIPayloadSequence.iRIContents.emailIRI.protocol-ID

In such case the translation is to follow the rules in table A.2.2.3.4-1.

Table A.2.2.3.4-1

Element value	Corresponding protocol-ID field value	Analysis
Absent	undefined(255)	This is a misuse of the undefined field since the protocol may be a known (standardised) one. One option would be to define an unknown(254) value to express that the information is not available.
POP3	pop3(2)	No particular concern.
SMTP	smtp(1)	No particular concern.
IMAP	imap4(2)	No particular concern.
HTTP	-	(webmail services, out of scope)

A.2.2.3.5 Translation from <Partner-Kennung> < ID of the involved partner > and <Kennung-des-zueA> element to e-mail-Sender and e-mail-Recipients fields

Depending on the case, either the e-mail-Sender or the e-mail-Recipient field is to be filed with the information from the <Partner-Kennung> (ID of the involved partner). The case is determined according to two criteria defined in table A.2.2.3.5-1. When the criteria are met, the corresponding target field is to be set to the value of the <Partner-Kennung> < ID of the involved partner > element and the other field is not present. When no criteria match, both fields are not present.

Source attribute	/hi3-email/Partner-Kennung/ /hi3-email/Kennung-des-zueA/
Destination attribute	PS-PDU.payload.iLHIPayload.resPayload.contents.pspdu. payload.iRIPayloadSequence.iRIContents.emailIRI.e-mail-Sender PS-PDU.payload.iLHIPayload.resPayload.contents.pspdu. payload.iRIPayloadSequence.iRIContents.emailIRI.e-mail-Recipients

Table A.2.2.3.5-1

Criterion 1: Value of Protocol element	Criterion 2: Value of <Richtung> element	Target field	Source field
SMTP	'empfangen'	e-mail-Sender	Partner-Kennung
SMTP	'empfangen'	e-mail-Recipients	Kennung-des-ZueA
SMTP	'eingestellt'	e-mail-Recipients	Partner-Kennung
			Kennung-des-ZueA
SMTP	'gesendet'	e-mail-Recipients	Partner-Kennung
			Kennung-des-ZueA
POP3	'abgerufen'	e-mail-Sender	Partner-Kennung
			Kennung-des-ZueA
IMAP	'eingestellt'	e-mail-Recipients	Partner-Kennung
			Kennung-des-ZueA
IMAP	'abgerufen'	e-mail-Sender	Partner-Kennung
			Kennung-des-ZueA

A.2.3 Mapping from ETSI TS 102 232-2 family to German TR TKÜV

A.2.3.1 Generalities

A.2.3.1.1 Handling of information that is not available in the ETSI TS 102 232 compliant PDU

It can be assumed that the TR TKÜV 7.1 [i.8] XML format requires an element to be present if the corresponding data is available. TR TKÜV 7.1 [i.8], Annex F.2.2 provides the following guidance:

"The following example of an XML structure has values included for all tags. These tags should, however, only be transmitted if the relevant event requires them. If there are no parameters for the relevant event data, an empty tag should be used in accordance with XML syntax, e.g. '<start-UEM/>'. Comment lines are not required and may be omitted."

A.2.3.1.2 Handling of fields unsupported in TR TKÜV

The German TR TKÜV 7.1 [i.8] XML DTD for e-mail has no element to embed extensions, but one could be defined. It is left for further study what to do with unsupported fields that cannot contribute to the <hi3-email> element.

A.2.3.2 Mapping of parameter names

The elements in the <hi3-email> element are mapped to the fields in the target PDU according to table A.2.3.2-1 below.

Table A.2.3.2-1

Element name in TR TKÜV 7.1 Annex F (elements under <hi3-email>)	**Status in ETSI TS 102 232/Analysis**
<Versionskennung> <*version*>	In TR TKÜV 7.1 [i.8] this is a free text field providing the interface version. It is assigned by the obligated party's telecommunications system. Several options are available for this element: 1) report the version of the entire interface, for this use the OID of the LI-PS-PDU or, if present, the value of the Version field NOTE: The Version field is specified in ETSI TS 102 232-1 [i.6] clause 5, but is not present in the ASN.1 specification in clause A.2. 2) confine the version reporting to the EmailPDU and use the OID of the EmailPD
<Datensatzart> <*type of data set*>	This element is always assigned the value 'Report'.
<Referenznummer> <*LIID*>	To be assigned the combination of authorizationCountryCode and LIID fields found in the header of the enclosing LI-PS-PDU.
<Zuordnungsnummer> <*message identifier*>	To be assigned the value of the message-ID field, if present, from the EmailIRI PDU. The message-ID can also be obtained by parsing of the e-mail, if an EmailCC PDU is provided.
<Kennung des züA> <*target ID*>	TR TKÜV 7.1 [i.8] provides the identity under interception directly as part of the <hi3-email> element handed over to the LEA. This is not the case with the LI-PS-PDU, which provides the LIID, and where the mapping between the LIID and the identity (or identities) under interception is negotiated between the CSP and the LEA outside of the HI2 and HI3 interfaces. For the value of this element to be trustworthy, the entity performing the conversion has to be able to request the mapping between the LIID and the identity under interception. If the mapping leads to multiple target identities, then uncertainty on the correctness of the element is introduced. The alternative approach to use the combination of eventType, protocol-ID, e-mail-Sender, and e-mail-Recipients fields is also bound to introduce such uncertainty.

Element name in TR TKÜV 7.1 Annex F (elements under <hi3-email>)	Status in ETSI TS 102 232/Analysis
<Partner-Kennung> <*ID of the involved partner*>	To be assigned the value of e-mail-Sender or e-mail-Recipients field depending on the value of the eventType field, according to the rules to specified in table A.2.3.3.2-1. Note that this element may have to hold a very large number of e-mail addresses.
<IP>	To be assigned the value of the client-Address field, if present.
<Port>	To be assigned a value translated from the protocol-ID field.
<Beginn> <*begin*>	This information can be obtained from the timeStamp field if the associated timeStampQualifier field is set to timeOfInterception(1). When there is no aggregation of payload, the timeStamp field in the PSHeader is to be referred to. When the translated payload is part of an aggregated PDU, the timestamp field of the corresponding CCpayload or IRIPayload is to be referred to. NOTE: How a CCPayload and IRIPayload are processed together to form an <hi3-email> with a non-empty <email> element, and how this affects the value of the <Beginn> element, are left for further study.
<Einstellungen> <*settings*>	There is no equivalent field(s). The element can be left empty.
<Richtung> <*direction*>	To be mapped from the eventType and protocol-ID fields according to tables A.2.3.3.3-1, A.2.3.3.4-1 and A.2.3.3.5-1.
<Ausloesegrund-zueA> <*reason of terminating the connection*>	To be mapped from status field according to table A.2.3.3.6-1.
<Beginn-UEM> <*begin UEM*>	This element indicates when interception action related to the <hi3-email> instance has started (was provisioned). This information is not available in the LI-PS-PDU, consequently this element is to be left empty.
<Ende-UEM> <*end UEM*>	This element indicates when interception action related to the <hi3-email> instance has terminated (was de-provisioned). This information is not available in the LI-PS-PDU, consequently this element is to be left empty.
<email>	Depending on the value of the email-Forward field in EmailCC: When set to ip-packet(1), the protocol session is first to be reconstructed from the available IP packet(s), after which the e-mail (envelope and body) can be extracted, encoded in Base64, and encapsulated in a CDATA section in the <email> element When set to application(2), the value of the content field is to be encoded in Base64 and encapsulated in a CDATA section in the <email> element.

A.2.3.3 Translation rules

A.2.3.3.1 Encodings of fields into elements

Several elements in the German TR TKÜV 7.1 [i.8], Annex F require that the value be embedded in a CDATA section and encoded in Base64. These are indicated in table A.2.3.3.1-1.

Table A.2.3.3.1-1

Element name in TR TKÜV 7.1 [i.8] Annex F (elements under <hi3-email>)	Base64 encoding in CDATA section is mandatory
<Versionskennung> <*version*>	No
<Datensatzart> <*type of data set*>	No
<Referenznummer> <*LIID*>	Yes
<Zuordnungsnummer> <*message identifier*>	Yes
<Kennung des züA> <*target ID*>	Yes
<Partner-Kennung> <*ID of the involved partner*>	Yes
<IP>	No
<Port>	No
<Beginn> <*begin*>	No
<Einstellungen> <*settings*>	Yes
<Richtung> <*direction*>	Yes
<Ausloesegrund-zueA> <*reason of terminating the connection*>	Yes
<Beginn-UEM> <*begin UEM*>	No
<Ende-UEM> <*end UEM*>	No
<email>	Yes

A.2.3.3.2 Translation from e-mail-Sender and e-mail-Recipients fields to <Partner-Kennung> < ID of the involved partner > element

The <Partner-Kennung> element is to receive a copy of the values stored either in the e-mail-Recipients or in the e-mail-Sender field, depending on the protocol and whether the e-mail was sent or received by the identity under surveillance. The decision whether to copy from the e-mail-Recipients or the e-mail-Sender field depend on two criteria, the protocol in use and the value of the eventType field, according to table A.2.3.3.2-1.

Table A.2.3.3.2-1

Criterion: Protocol	Criterion: Value of eventType field	Target field for <Partner-Kennung> <ID of the involved partner> element
SMTP	e-mail-send(1)	e-mail-Recipients (see note 1)
SMTP	e-mail-received(2) (see note 2)	e-mail-Sender
POP3	e-mail-download(3) e-mail-partial-download(8)	e-mail-Sender
IMAP	e-mail-download(3) e-mail-partial-download(8)	e-mail-Sender
IMAP	e-mail-upload(9)	e-mail-Recipients (see note 1)
NOTE 1: TR TKÜV 7.1 [i.8] requires exclusion of the address of the identity under interception. NOTE 2: Refer to the analysis in table A.2.2.3.4-1. NOTE 3: in cases where the e-mail-Sender and/or e-mail-Recipients field are not provided, but an EmailCC PDU is available, the addresses of the sender and of the recipients can be extracted from the e-mail body. This approach would however miss the recipients in blind carbon copy (bcc).		

A.2.3.3.3 Translation from eventType field to <Richtung> <*direction*> element when the protocol is SMTP

In such case the translation follows the rules defined in table A.2.3.3.3-1.

Table A.2.3.3.3-1

Value of eventType field	Corresponding <Richtung> element value	Analysis
e-mail-send(1)	'gesendet' (sent)	
e-mail-received(2)	'empfangen' (received)	ETSI TS 102 232-2 [i.7], clause A.2.3 is not clear on this, but it is assumed that indication of a "successful transfer" is from the point of view of a receiving SMTP server (i.e. that the message will be transferred to a mailbox, for example using LMTP).

Other values of the evenType field are to be ignored.

A.2.3.3.4 Translation from eventType field to <Richtung> <*direction*> element when the protocol is POP3

In such case the translation follows the rules defined in table A.2.3.3.4-1.

Table A.2.3.3.4-1

Value of eventType field	Corresponding <Richtung> element value	Analysis
e-mail-download(3)	'abgerufen' ('retrieved')	TR TKÜV 7.1 [i.8] makes no distinction between full download and partial download, therefore both values of the eventType field map to the same <Richtung> element value.
e-mail-partial-download(8)	'abgerufen' ('retrieved')	

Other values of the evenType field are to be ignored.

A.2.3.3.5 Translation from eventType field to <Richtung> <*direction*> element when the protocol is IMAP

In such case the translation follows the rules defined in table A.2.3.3.5-1.

Table A.2.3.3.5-1

Value of eventType field	Corresponding <Richtung> element value	Analysis
e-mail-download(3)	'abgerufen' ('retrieved')	TR TKÜV 7.1 [i.8] makes no distinction between full download and partial download, therefore both values of the eventType field map to the same <Richtung> element value.
e-mail-partial-download(8)	'abgerufen' ('retrieved')	
e-mail-upload(9)	'eingestellt' ('stored')	

Other values of the evenType field are to be ignored.

A.2.3.3.6 Translation from status field to <Ausloesegrund-zueA> <*reason of terminating the connection*> element

In such case the translation follows the rules defined in table A.2.3.3.6-1.

Table A.2.3.3.6-1

Value of status field	Corresponding <Ausloesegrund-zueA> element value	Analysis
status-unknown(1)	'unbekannter Fehler' (see note)	This mapping would need to be updated for new values of the status field that could be specified in a future version of ETSI TS 102 232-2 [i.7]. Such update would be of little consequences to implementations supporting the German TR TKÜV 7.1 [i.8], as the <Ausloesegrund-zueA> element embeds a free text string (only the presence or absence of the 'erfolgreich' value has significance). The situation is different for the operator having to act on the value of this element, and who may benefit from an official translation of the error code and from a reference semantic.
operation-failed(2)	'allgemeiner Fehler' (see note)	
operation-succeeded(3)	'erfolgreich'	
NOTE: This value is not defined in TR TKÜV 7.1 [i.8], it would need to be defined in a conversion profile.		

Annex B:
Warrant and tasking information for LI and LD

B.1 Overview

The present annex shows some typical examples of aspects of a warrant information, such as:

- Judicial.
- Technical.

B.2 Checklist warrant and tasking process

Table B.2-1

Judicial aspects				
Form	New			
	Renewal			
	Correction			
	other			
Authority	Court			
	Prosecution			
	LEA			
	other			
Case number or reference	Internal-ID			
Date and (max.) term				
Request type	e-Evidence	MLAT		
		EIO		
		EPOC/EPOC-PR		
		CLOUD Act		
		other		
Type of warrant	Request flag	Real-time	Lawful Interception	IRI-only
		None-real-time	Lawful Disclosure	
			Data request	
			Seizure	
			other	
Type of data	Subscriber			
	Access			
	Transactional			
	Content			
	other			
Priority	Emergency			
	Normal			

Table B.2-2

Technical Aspects			
General	Inter LEA ID		
	Country code		
	Request flag		
Connection type	Telephony	Fixed line	DSL
			Cable
			other
		Mobile	
	Internet access	Fixed line	DSL
			Cable
			other
		Mobile	
	E-mail services		
	OTT/NTT services		
	other		
Payload type	Audio		
	Video		
	Chat		
	other		
Target identifier	Service identifier	Telephone number	E.164
			SIP-URI
			Tel-URI
			other
		E-mail address	
		Account name/ID	
		IMSI	
		SUPI/SUCI	
	Equipment identifier	IMEI	
		MAC address	
	Network identifier	IP address	
		Internet access ID	
	other		

Table B.2-3

Technical Aspects	
Payload information (warrant)	TIFF
	PDF

Annex C:
Library: Operational aspects for LI and LD

C.1 Overview

The present annex contains examples of administrative and operational aspects of a mapping.

C.2 Checklist operational aspects and maintenance

Table C.2-1

Mapping checklist - technical aspects			
Reference	**Recommendation**	**Handled (y/n)**	**Arrangements (to be filled by involved parties)**
General (out-of-scope aspects to handle separately)			
Maintenance of mapping tables	Not applicable		Not applicable
General security aspects	Not applicable. This can also include physical security of bespoke equipment and data clearance levels		Not applicable
…			
Contact details involved persons resLEA/reqLEA			
Name			
Phone/fax			
e-mail address			
Postal address			
User profile			
…			
Mapping management			
Mapping name			
Mapping version			
Mapping date			
Source specification #1	Technical description of national/ETSI format		
Source specification #2	Technical description of national/ETSI format		
Documentation hierarchy	List of the document in the mapping with specific version information and technical reference when needed		
…			
Technical aspects			
Network			
Interconnect/type of environment			
IP Addresses	Ensure IP addresses of connection peers are identified		
Port numbers	Ensure source and destination port numbers for each communication stream are identified		
Other parameters			
PDU-size			
Time-out			
Bandwidth			
…			

Security (VPN and other connections)			
Type of environment	If hardware based also certificate and smartcard details		
Security level/profile			
Encryption - Key length	Ensure that allowed key length(s) are identified		
Encryption - Certification	Agree the means to assure the encryption method		
Encryption - Version			
…			
ILHI implementation and Mapping table			
Version			
Parameter			
Mapping method	(translations, encodings, deduction, real-time, etc.)		
Valuation indicators			
Analysis of potential information loss			
Use of originalPayload and structure thereof	Only in case the destination format does not support the source data		
Use of inert values			
Out-of-band requests			
Requirements of national format	When a national format is the destination of the data		
Requirements on input data			
…			
Maintenance and monitoring			
National settings/configurations	Ensure national settings that are relevant are identified and accounted for		
Trust and assurance	Consider in particular whether a PKI is needed		
Security measures for out-of-band communication between agencies			
Failsafe measures	Ensure processes are in place to monitor proper operations and detect errors such as non-conformity of input data and translation errors		
Interconnect status			
Keep-alive			
Error messages	…		
Status of the provision of the requested data	e.g. complete or incomplete		
System updates	Ensure that processes are in place to handle service disruptions, such as those caused by system updates		
Troubleshooting			
…			
Test Procedures			
General	Ensure processes are in place to test proper operations of the ILHI implementation and related support functions		
Version - ILHI implementation	…		
Version - Mapping table	…		
Test data	Ensure test and sample data are identified and available (e.g. from ETSI Plugtests)		
…			

Annex D:
Example considerations on the valuation indicator on accuracy for a mapping between some data types

D.1 Overview

The present annex contains example mappings between data types defined in ETSI TS 103 280 [i.10], illustrating the use of the valuation indicator.

D.2 Example

Table D.2-1

Input		Output		Valuation on accuracy	
Data type	**Value**	**Data type**	**Value**	**Corresponding indication**	**Comment**
QualifiedDateTime	2015-12-27T13:37:00+02:00	QualifiedDateTime	2015-12-27T13:37:00+02:00	The data is to be handled in the mapping	100 % accuracy
	2015-12-27T13:37:00+02:00	QualifiedMicrosecondDateTime	2015-12-27T13:37:00.000000+02:00	The data is to be handled in the mapping under specific rules	Specific rule: "digits after the decimal point should be ignored" (The translation into a format with higher precision requires the identification of the data that has no relation to the original data)
	2015-12-27T13:37:0+02:00	UTCDateTime	2015-12-27T11:37:00Z	The data is to be handled in the mapping under specific rules	Specific rule: "the value is accurate in the UTCDateTime format" Both the responding and the requesting party are to be aware of time conversion rules involving time zone, winter/summer time and leap seconds
	2015-12-27T13:37:00+02:00	UTCMicrosecondDateTime	2015-12-27T11:37:00.000000Z	The data is to be handled in the mapping under specific rules	Specific rules: • "digits after the decimal point should be ignored" • "the value is accurate in the UTCDateTime format"
	2015-12-27T13:37:00+02:00	No equivalent parameter available	N/A	The data cannot be handled within the mapping, the original data is to be handed over as originalPayload	Refer to clause 6.3 of the present document

Input		Output		Valuation on accuracy	
Data type	**Value**	**Data type**	**Value**	**Corresponding indication**	**Comment**
QualifiedMicrosecondDateTime	2015-12-27T13:37:00.012345+02:00	QualifiedMicrosecondDateTime	2015-12-27T13:37:00.012345+02:00	The data is to be handled in the mapping	100 % accuracy
	2015-12-27T13:37:00.012345+02:00	QualifiedDateTime	2015-12-27T13:37:00+02:00	The data is to be handled in the mapping under specific rule	Specific rules: • "digits after the decimal point.removed from the value", or • "unit second is the result of a rounding operation of the decimal points"
	2015-12-27T13:37:00.012345+02:00	UTCDateTime	2015-12-27T11:37:00Z	The data is to be handled in the mapping under specific rule	Specific rules: • "the value is accurate in the UTCDateTime format", and – "digits after the decimal point removed from the value", or – "unit second is the result of a rounding operation of the decimal points"
	2015-12-27T13:37:00.012345+02:00	UTCMicrosecondDateTime	2015-12-27T11:37:00.012345Z	The data is to be handled in the mapping under specific rule	Specific rule: • "the value is accurate in the UTCDateTime format" Both the responding and the requesting party are to be aware of time conversion rules involving time zone, winter/summer time and leap seconds
	2015-12-27T13:37:00.012345+02:00	No equivalent parameter available	N/A	The data cannot be handled within the mapping, the original data is to be handed over as originalPayload	Refer to clause 6.3 of the present document
UTCDateTime	2015-12-27T13:37:00Z	UTCDateTime	2015-12-27T13:37:00Z	The data is to be handled in the mapping	100 % accuracy
	2015-12-27T13:37:00Z	UTCMicrosecondDateTime	2015-12-27T11:37:00.000000Z	The data is to be handled in the mapping under specific rule	Specific rules: • "digits after the decimal point should be ignored" • "the value is accurate in the UTCDateTime format"

Input		Output		Valuation on accuracy	
Data type	**Value**	**Data type**	**Value**	**Corresponding indication**	**Comment**
	2015-12-27T13:37:00Z	QualifiedDateTime	2015-12-27T13:37:0+/-??:00	The data is to be handled in the mapping under specific rule	Specific rule: • The value is translated in the local timezone of the requesting party" A reference timezone needs to be agreed between the requesting and the responding party. In this example, the timezone is agreed to be that of the requesting party (but this is not mandatory) Both the responding and the requesting party are to be aware of time conversion rules involving time zone, winter/summer time and leap seconds
	2015-12-27T13:37:00Z	QualifiedMicrosecondDateTime	2015-12-27T13:37:00.000000+/-??:00	The data is to be handled in the mapping under specific rule	Specific rule: • The value is translated in the local timezone of the requesting party" • "digits after the decimal point should be ignored"
	2015-12-27T13:37:00Z	No equivalent parameter available	N/A	The data cannot be handled within the mapping, the original data is to be handed over as originalPayload	Refer to clause 6.3 of the present document
UTCMicrosecondDateTime	2015-12-27T13:37:00.012345Z	UTCMicrosecondDateTime	2015-12-27T13:37:00.012345Z	The data is to be handled in the mapping	100 % accuracy
	2015-12-27T13:37:00.012345Z	UTCDateTime	2015-12-27T13:37:00Z	The data is to be handled in the mapping under specific rule	Specific rules (either/or): • "digits after the decimal point removed from the value • "unit second is the result of a rounding operation of the decimal points"
	2015-12-27T13:37:00.012345Z	QualifiedDateTime	2015-12-27T13:37:00+/-??:00	The data is to be handled in the mapping under specific rule	Specific rule: • "The value is translated in the local timezone of the requesting party", and: – "digits after the decimal point removed from the value ", or – "unit second is the result of a rounding operation of the decimal points"

Input		Output		Valuation on accuracy	
Data type	**Value**	**Data type**	**Value**	**Corresponding indication**	**Comment**
	2015-12-27T13:37:00.012345Z	QualifiedMicrosecondDateTime	2015-12-27T13:37:00.012345+/-??:00	The data is to be handled in the mapping under specific rule	Specific rule: • "The value is translated in the local timezone of the requesting party"
	2015-12-27T13:37:00.012345Z	No equivalent parameter available	N/A	The data cannot be handled within the mapping, the original data is to be handed over as originalPayload	Refer to clause 6.3 of the present document

Annex E:
Change History

Status of the present document: Library and mapping for Lawful Interception (LI) and Lawful Disclosure (LD)		
TC LI approval date	**Version**	**Remarks**
October 2021	1.1.1	First publication of the TR after approval at TC LI#58e (electronic meeting)

History

Document history		
V1.1.1	November 2021	Publication