

ETSI TS 103 462 V1.2.1 (2019-12)



TECHNICAL SPECIFICATION

Lawful Interception (LI); Inter LEMF Handover Interface

Reference

RTS/LI-00171

Keywords

handover, IP, lawful disclosure, lawful interception, retained data, security

ETSI

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

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

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

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

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

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

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

© ETSI 2019.

All rights reserved.

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

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	6
3.1 Terms.....	6
3.2 Symbols.....	7
3.3 Abbreviations	7
4 General aspects.....	8
5 Architecture overview and functional description	8
6 Delivery Handling	9
6.1 General	9
6.2 Description and purpose of the header fields	9
6.2.1 Inter LEMF LIID	9
6.2.2 Communication Identifier.....	10
6.2.3 Sequence Number.....	10
6.2.4 Timestamp	10
6.3 Integrity	10
6.4 Payload encryption.....	10
6.5 Reliability	10
6.6 Error Handling.....	11
6.7 Keep alive.....	11
7 Responding Interworking Function (resIWF)	11
7.1 General	11
7.2 Encapsulation function	11
7.3 Mapping function	11
7.3.1 General.....	11
7.3.2 Timestamp	12
7.3.3 Location information	12
7.4 Interoperability function.....	12
8 Encapsulation Handling	12
8.1 General	12
9 Transport layer	13
Annex A (informative): Operational roles.....	14
A.1 Introduction	14
A.2 Requesting party (reqLEA/reqAA)	15
A.3 Responding party (resLEA/resAA)	15
A.4 Executing Communication Service Provider	15
Annex B (normative): Inter LEMF Handover (ILHI) ASN.1.....	16
Annex C (informative): Change History	18
History	19

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The objective of the present document is to form the basis for a standardized handover interface, that will deliver the LI and/or RD information via IP-based networks between Law Enforcement Authorities under various European treaties and local regulations in case of:

- legal assistance;
- legal assistance regarding the European Investigation Order in criminal matters [i.1];
- (bilateral) administrative assistance.

The present document is intended to cover the following:

- transmission of intercepted Content of Communication (CC) and Intercept Related Information (IRI);

NOTE: This includes data that is already processed or stored on the LI system.

- transmission of traffic and location data (RD), administrative data according to ETSI TS 102 657 [3] and error codes according to ETSI TS 102 232-1 [6] are for further study.

Besides the EIO Directive, there is also a need in some countries to exchange stored or LI data in real time between different LEMFs or between a primary LEMF and a secondary analysis framework (this forms another use case for the interface).

1 Scope

The present document specifies the LEMF to LEMF interface to support (as a minimum) European Investigation Orders (EIOs) related to LI and/or RD. The present document aims to be capable of securely handling real-time and stored data transfer between LEMFs in accordance with ETSI TS 102 232 parts 1 [6] to 7 [12] and the related ETSI TS 133 108 [5] for LI.

In the present document RD is for further study.

Local LI handover interfaces frequently use dedicated networks for delivery with local specific security features. With the EIO Directive in place, there is a need to have a common Handover Interface to allow real-time exchange between LEMFs that can be located in different countries, under different jurisdictions.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference/>.

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

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

- [1] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: ETSI TS 101 671 is in status "historical" and is not maintained.

- [2] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".
- [3] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".
- [4] ETSI TS 103 307: "CYBER; Security aspects for LI and RD Interfaces".
- [5] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system (Phase 2+) (GSM); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".
- [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".
- [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".
- [8] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".
- [9] ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".
- [10] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

- [11] ETSI TS 102 232-6: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".
- [12] ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".
- [13] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions; Part 1: Country codes".
- [14] Recommendation ITU-T X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

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] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.
- [i.2] ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 101 671 [1], ETSI TS 102 232-1 [6] and the following apply:

NOTE: This may contain additional information.

mapping: function that maps every element of a given set to a distinct element of another set

mappingInfo: output of the mapping function

originalPayload: optional output part of the interoperability function containing the unmodified received data

real time: information and communication technologies that are able to generate and deliver information in a time-frame similar to the real-life process that it is assisting

requesting AA (reqAA): Authorized Authority from the country that takes the initiative for the LI request

requesting IWF (reqIWF): function to format data from ILHI format into local format

requesting LEA (reqLEA): Law Enforcement Agency from the country that takes the initiative for the LI request

requesting LEMF (reqLEMF): Law Enforcement Monitoring Facility from the country that takes the initiative for the LI request

resPayload: mandatory output part of the interoperability function

responding AA (resAA): Authorized Authority from the country that verifies the requesting party and translates the received warrant into a national warrant

responding IWF (resIWF): function to format data into ILHI format

responding LEA (resLEA): Law Enforcement Agency from the country that verifies the requesting party and translates the received warrant into a national warrant

responding LEMF (resLEMF): Law Enforcement Monitoring Facility from the country that verifies the requesting party and translates the received warrant into a national warrant

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	Third Generation Partnership Project
AA	Authorized Authority
ADMf	ADMinistration Function (at CSP)
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
CC IW	Content of Communication InterWorking
CC	Content of Communication
CIN	Communications Identity Number
CS	Circuit Switched
CSP	Communications Service Provider
EcsF	Encapsulation Function
EIO	European Investigation Order
ID	IDentifier
ILHI	Inter LEMF Handover Interface
IMS	IM Subsystem
IopF	Interoperability Function
IP	Internet Protocol
IRI IW	Intercept Related Information Interworking
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMf	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception IDentifier
MapF	Mapping Function
MF	Mediation Function (at CSP)
NID	Network IDentifier
OID	Object IDentifier
PDU	Protocol Data Unit
PS-PDU	Packet Switched - Protocol Data Unit
RD IW	Retained Data InterWorking
RD	Retained Data
reqAA	requesting Authorized Authority
reqIWf	requesting InterWorking Function
reqLEMf	requesting LEMF
resAA	responding Authorized Authority
resIWf	responding InterWorking Function
resLEMf	responding LEMF
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
WGS84	World Geodetic System 1984

4 General aspects

The Inter LEMF Handover Interface (ILHI) for LI is based on the ETSI TS 102 232 parts 1 [6] to 7 [12] for requesting data from the responding LEMF. ETSI TS 133 108 [5] data is provided by using mechanism defined by ETSI TS 102 232-1 [6] and ETSI TS 102 232-7 [12].

Figure 4.1 illustrates the ILHI in principle; a description of the legal assistance can be found in annex A.



Figure 4.1: Functional block diagram showing Inter LEMF Handover Interface

NOTE 1: Handover interfaces between CSP and resLEMF are out of scope of the present document.

The resLEMF sends the data via ILHI to the reqLEMF ensuring interoperability.

The reqLEMF receives the data transmitted by the resLEMF via the ILHI and processes the data into local format if necessary.

NOTE 2: If reqLEMF and resLEMF are in the same countries the term "national" equals the term "local".

Delivery of data shall be done without undue delay assuming that there is sufficient bandwidth available.

5 Architecture overview and functional description

Figure 5.1 shows the architecture overview of the ILHI.

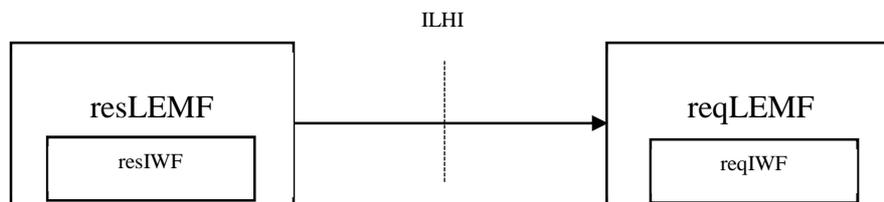


Figure 5.1: Architecture overview of Inter LEMF Handover Interface (ILHI)

The resLEMF sends the data in ILHI format to the reqLEMF. In addition, control messages (e.g. error codes, keep alive messages) can be sent between resLEMF and reqLEMF via ILHI.

For data processing an interworking function is defined for the resLEMF and for the reqLEMF.

The responding interworking function (resIWF) shall process the data to provide interoperability. For further details see clause 7.

NOTE 1: The resIWF could need to transcode data for interoperability reasons. The transcoding is out of the scope of the present document. Transcoding could apply e.g. for voice codecs.

The requesting interworking function (reqIWF) processes the data received over ILHI into local format as needed.

NOTE 2: The transcoding of the reqIWF is out of scope of the present document.

The ILHI format is defined as data in ETSI TS 102 232 family format with additional information. This additional information shall consist of a ILHIPayload comprising resPayload, optional mappingInfo and/or originalPayload where required (see figure 5.2). It is up to bilateral agreement which options are used.

The PS-PDU that contains the ILHIPayload has the LIID in the header used between the resLEMF and the reqLEMF. The format of this Inter LEMF LIID is described in clause 6.2.1. The resPayload and originalPayload contain an octet string.

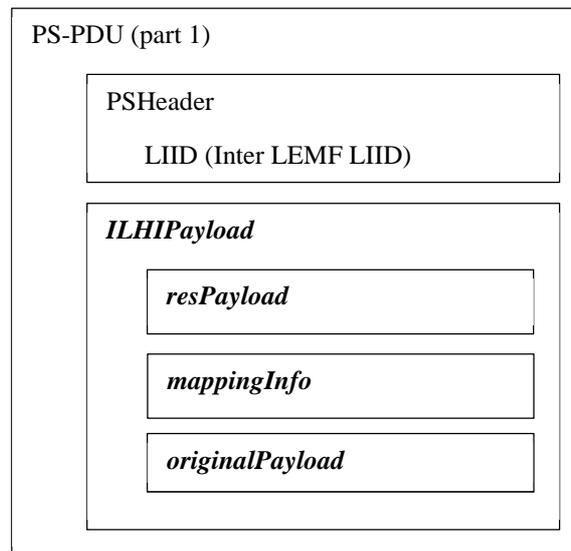


Figure 5.2: PDU structure for ILHI

6 Delivery Handling

6.1 General

In ILHI the role of the CSP is replaced by the resLEMF.

All information delivered by the CSP shall be forwarded by the resLEMF. The appropriate parameters from ETSI TS 102 232-1 [6] shall be used.

Payload aggregation may be used if agreed by the LEMFs. If payload aggregation is used, it shall be used as described in ETSI TS 102 232-1 [6], clause 6.2.3.

Nesting an ILHI PDU in an ILHI PDU shall not be used.

If for any reason an ILHI PDU needs to be forwarded, a new ILHI PDU shall be created that contains the payload of the original ILHI PDU and the header of the original ILHI PDU updated with a new timestamp and a new Inter LEMF LIID.

The following clauses provide additional clarification where needed.

6.2 Description and purpose of the header fields

6.2.1 Inter LEMF LIID

The globally unique Inter LEMF LIID is the LIID from ETSI TS 102 232-1 [6], defined by ETSI TS 103 280 [2], clause 6, that uses a restricted set of ASCII characters. It is used to identify the communication between the resLEMF and the reqLEMF and is part of the header of the PS-PDU for ILHI.

The globally unique Inter LEMF LIID has a length of 25 octets and can be defined within the warrant and shall be provided by the reqLEMF. The Inter LEMF LIID shall be structured according to the following patterns:

- Octets 1 and 2 shall contain the country code of reqLEMF.

- Octets 3-25 are reserved for internal ID definition.

For the Inter LEMF LIID only ASCII characters in "a" ... "z", "A" ... "Z", ".", "-", "_" and "0" ... "9" shall be used.

Country codes of reqLEMF and resLEMF shall be encoded according to ISO 3166-1 [13].

NOTE: It is up to the requesting country to ensure that the Inter LEMF LIID is unique.

EXAMPLE: DE01234567890123456789ABC.

6.2.2 Communication Identifier

The Network Identifier (NID) is described in ETSI TS 102 232-1 [6], clause 5.2.4. The operator identifier uniquely identifies the resLEMF within the applicable country and is mandatory.

NOTE: It is up to the resLEMF to ensure that the operator identifier is unique.

The network element identifier and Communications Identity Number (CIN) as described in ETSI TS 102 232-1 [6], clause 5.2.4. can be used to uniquely identify communication sessions if applicable.

6.2.3 Sequence Number

The sequence number shall be present as described in ETSI TS 102 232-1 [6], clause 5.2.5.

6.2.4 Timestamp

The timestamp shall be present as described in ETSI TS 102 232-1 [6], clause 5.2.6.

The QualifiedMicrosecondDateTime as per ETSI TS 103 280 [2] should be used.

6.3 Integrity

The integrity check mechanism shall be implemented for ILHI as described in ETSI TS 102 232-1 [6], clause 7.2.3.

6.4 Payload encryption

Any payload encryption provided by the CSP, e.g. as described in ETSI TS 102 232-1 [6], clause 6.2.6, shall be terminated (removed) by the resLEMF.

NOTE: When encryption/hashing/signing is used between CSP and resLEMF, resLEMF needs to reverse the steps as described in ETSI TS 102 232-1 [6], annex G before forwarding to the reqLEMF.

The resLEMF shall protect the information using payload encryption either based on ETSI TS 102 232-1 [6], clause 6.2.6 to the reqLEMF or by any other appropriate means, see e.g. ETSI TS 103 307 [4], annex A. In particular, the security of the ILHI shall not be dependent on the security of the network layer.

6.5 Reliability

The resLEMF shall implement buffering in accordance with ETSI TS 102 232-1 [6] and support multiple alternative/simultaneous endpoints/gateways for the delivery of a specific delivery set in accordance to ETSI TS 102 232-1 [6], clause 6.2.1.

NOTE: Although buffering to cover longer outages is out of scope of the present document, it is strongly recommended to implement buffering or any other solution in the resLEMF in order to avoid data loss in case of longer outages.

6.6 Error Handling

Any ILHI related errors impacting the data exchange between resLEMF and reqLEMF, e.g. connection problems or application failures, shall be logged at the resLEMF and should be reported to the reqLEMF.

NOTE: The means by which the reporting to the reqLEMF will be done is for further study.

6.7 Keep alive

A Keep alive mechanism between reqLEMF and resLEMF should be implemented and - if used - shall be based on ETSI TS 102 232-1 [6], clause 6.3.4.

7 Responding Interworking Function (resIWF)

7.1 General

The responding interworking function (resIWF) consists of three functions as shown in figure 7.1. These functions are described in detail in the following clauses.

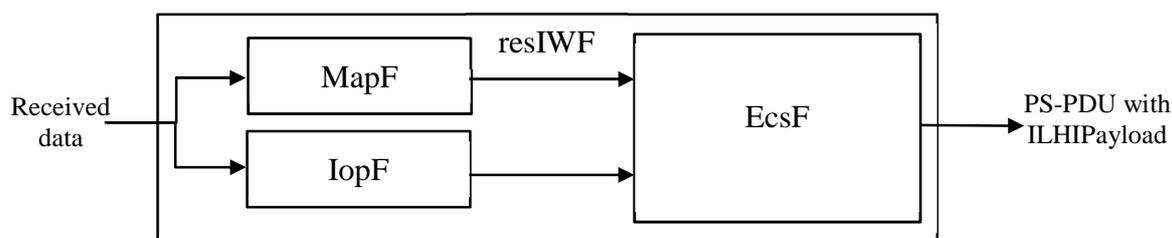


Figure 7.1: resIWF functions

The resIWF creates the PS-PDU with ILHIPayload that is provided by the EcsF. The resIWF shall populate the PSHeader as described in clause 6.

7.2 Encapsulation function

The encapsulation function (EcsF) creates the ILHIPayload. The ILHIPayload shall contain the data provided by the mapping function (see clause 7.3) and the interoperability function (see clause 7.4).

7.3 Mapping function

7.3.1 General

The implementation of the mapping function (MapF) is optional.

The decision if and how mapping is used shall be made by the resLEMF.

NOTE: The mapping e.g. of local CellID to geographical coordinates is for bilateral agreement and has no influence on the work flow of the mapping function.

The mapping function generates a mapping from every element of a given set to a distinct element of another set. It shall generate the mappingInfo as its output and pass it to the encapsulation function without undue delay. The parameters that can be mapped by the mapping function are described in the following clauses.

7.3.2 Timestamp

If used for timestamps the mapping function shall generate `QualifiedDateTime` or `QualifiedMicrosecondDateTime` as per ETSI TS 103 280 [2] and deliver the outcome and the original timestamp to the encapsulation function.

NOTE: The mapping of more than one timestamp is possible. It can only be uniquely mapped if the original timestamps are all unique within the `originalPayload`.

If the original timestamp is for any reason not mappable the choice value `unqualifiedDateTime` shall be used.

If the original timestamp is in national format and does not represent a `timeStamp` or `microSecondTimeStamp` as per ETSI TS 102 232-1 [6], `otherTimeStamp` shall be used and shall contain a human readable timestamp.

7.3.3 Location information

If used for location information coded as geographical coordinates the mapping function shall generate WGS84 based geographical coordinates as per ETSI TS 103 280 [2] without changing their resolution and deliver the outcome and the original location information to the encapsulation function.

The mapping of location information provided as postal address data is for further study.

7.4 Interoperability function

If the CSP delivers the data in accordance with one of the ETSI TS 102 232 specifications as described in table 7.1 the interoperability function (IopF) shall deliver the received PS-PDU as `resPayload` to the encapsulation function and the `originalPayload` shall not be present.

Otherwise (for example when national implementations of email interception are not using ETSI TS 102 232-2 [7]) the IopF shall generate the `resPayload` as a PS-PDU in accordance with the ETSI TS 102 232 family and in particular as described in table 7.1. In addition the IopF shall send the received data as `originalPayload` to the encapsulation function.

If there is more than one option, the choice which ETSI TS 102 232 part to be used will be done by the `resLEMF`.

Table 7.1: Overview of applicable specifications from ETSI TS 102 232

service	applicable specification
messaging	ETSI TS 102 232 part 2 [7]
fixed or wireless IP access	ETSI TS 102 232 part 3 [8]
Layer 2	ETSI TS 102 232 part 4 [9]
fixed VoIP telephony	ETSI TS 102 232 part 5 [10], part 6 [11] and/or part 7 [12]
PSTN/ISDN	ETSI TS 102 232 part 6 [11]
IMS (e.g. VoLTE, VoWiFi, RCSe)	ETSI TS 102 232 part 5 [10], part 6 [11] and/or part 7 [12]
CS mobile telephony	ETSI TS 102 232 part 6 [11] or part 7 [12]
mobile or wireless IP access (3GPP services)	ETSI TS 102 232 part 7 [12]

Data locally available in accordance to ETSI TS 133 108 [5] shall be formatted in accordance to ETSI TS 102 232-7 [12].

8 Encapsulation Handling

8.1 General

The `resPayload` and the `originalPayload` are provided as `EncapsulationPayload` including the content as an octet string, and an object identifier identifying how the content is to be processed. This allows for other content types to be used in the future without requiring an update to the ASN.1, by using an appropriate object identifier to identify the content.

If the content is a PS-PDU, either an original PS-PDU received from the CSP by the resLEMF or a PS-PDU generated by the IopF, the octet string will contain the original ASN.1 encoded information, and the identifier shall be LI-PS-PDU.li-psDomainId. If the content is another type with an object identifier, that identifier shall be used.

If a content type does not have an appropriate object identifier, one may be allocated under the iLHIDomainId identifiers(1) object identifier tree in the present document.

If the content is pre-agreed payload without the possibility to define an object identifier, the encoding of the information is left to bilateral agreement, and the identifier shall be preagreedObjId.

NOTE: Although the resLEMF has the lead the implementation options profiled by ETSI TS 102 232 parts 2 [7] to 7 [12] are to be agreed bilaterally by resLEA and reqLEA for the present document. If default profiles become available these might be used. Also modified profiles could be added to the present document.

9 Transport layer

The transport layer between reqLEMF and resLEMF shall be implemented based on ETSI TS 102 232-1 [6]. Unless otherwise bilaterally agreed, TLS as described in ETSI TS 102 232-1 [6], clause 6.3.1 should be used.

Session layer PDU acknowledgement shall be used over the transport layer connection according to ETSI TS 102 232-1 [6], clause 6.3.6. When the use of PDU acknowledgement is controlled via a required implementation in an endpoint as described in ETSI TS 102 232-1 [6], clause 6.3.6, Option 2) option negotiation is not needed.

NOTE: TCP does not guarantee that all PDU data transmitted by the resLEMF is received and processed by the reqLEMF. The use of Session layer PDU acknowledgement improves the reliability.

The reqLEMF and resLEMF shall communicate via the public Internet with IP-VPN interconnection between these LEMFs or via a network connection secured by other appropriate means for the transport layer.

Annex A (informative): Operational roles

A.1 Introduction

Figure A.1 shows the involved parties for handling an LI or RD based European Investigation Order and the steps that are involved in the process. An acknowledgement is sent for each single step to the requesting LEA/AA.

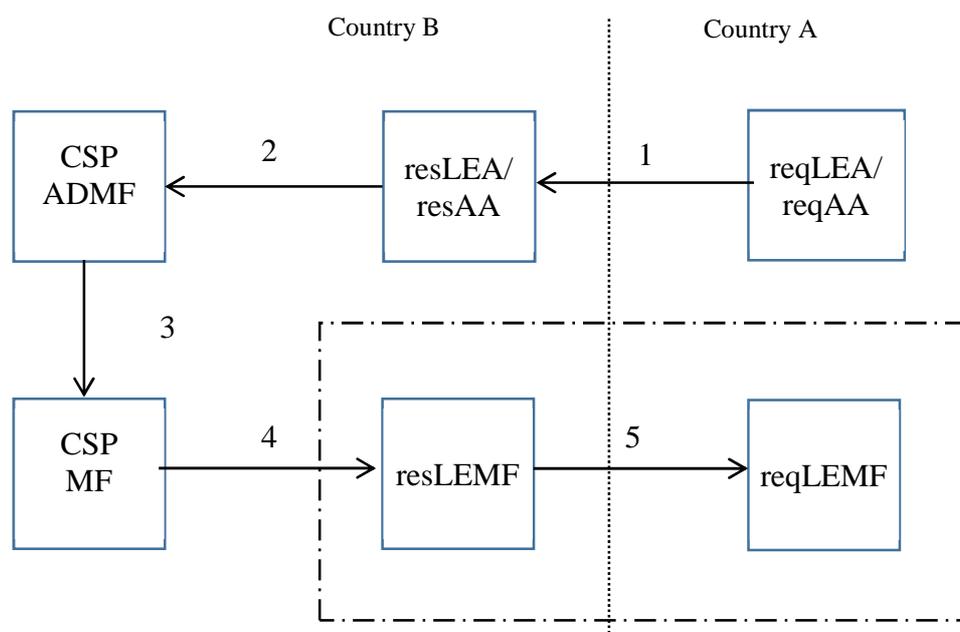


Figure A.1: Roles and steps of legal assistance using Inter LEMF handover Interface

In figure A.1, the following steps are identified:

- Step 1: The requesting LEA or requesting Authorized Authority (AA) sends a message in accordance with EIO [i.1] to the responding LEA or responding AA. Simultaneously the requesting LEA/AA sets up the reqLEMF to receive the corresponding data when delivered by the resLEMF.
- Step 2: If accepted, the resLEA or responding AA is forwarding this request to the CSP. Simultaneously the responding LEA /AA sets up the resLEMF in order to enable the forwarding of the requested Data towards the reqLEMF when received from the responding CSP Network.
- Step 3: The CSP activates the warrant request like a local request done by the CSP ADMF.
- Step 4: The CSP MF transfers the corresponding IRI and CC data or RD to the resLEMF (which pre-processes it in the same way as a local initiated LI or RD process).
- Step 5: The resLEMF forwards the pre-processed IRI IW and CC IW or RD IW data in real time to the reqLEMF.

The present document only specifies LI related parts of step 5, the Inter LEMF Handover Interface ILHI.

A.2 Requesting party (reqLEA/reqAA)

The requesting party is the party that takes the initiative for the LI request. It will send its warrant to the responding party which is the authorized authority in the jurisdiction that applies to the CSP which technically has to fulfil the warrant.

The role of the responding party and the protocols used between the requesting and responding party, and between the responding party and the executing CSP, are out of the scope of the present document.

A.3 Responding party (resLEA/resAA)

The responding party will verify the requesting party and transform the received warrant into a local warrant that can be issued to the executing CSP.

A.4 Executing Communication Service Provider

The executing CSP is the CSP which technical fulfils the warrant of the responding party (LEA/AA) and sends the CC and IRI to the forwarding party.

The role of the executing CSP and the Handover Interface between the CSP and the forwarding party (resLEMF) are out of the scope of the present document.

Annex B (normative): Inter LEMF Handover (ILHI) ASN.1

The ASN.1 (Recommendation ITU-T X.680 [14]) module that represents the information in the present document and meets all stated requirements is shown below. ETSI TR 102 503 [i.2] gives an overview of the relevant Object Identifiers (OID) used in ASN.1 modules of the Lawful Intercept specifications and points to the specification where the modules can be found.

The ASN.1 definitions are in .txt file "ILHIPDUver2.txt", contained in archive ts_103462v010201p0.zip which accompanies the present document.

```
-- =====
-- Description of the ILHI PDU
-- =====
```

ILHIPDU

```
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) informationHandover(4) ilhi(0)
ilhiPdu(0) version2(2)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

IMPORTS

```
-- from ETSI TS 102 232-1 [6]
TimeStampQualifier,
MicroSecondTimeStamp,
Location
    FROM LI-PS-PDU
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5)
genHeader (1) version28(28)}

-- from ETSI TS 103 280 [2]
QualifiedDateTime,
QualifiedMicrosecondDateTime,
WGS84CoordinateDecimal,
WGS84CoordinateAngular
    FROM Common-Parameters
    {itu-t(0) identified-organization(4) etsi(0) common-parameters(3280) version221(221)}
;

-- end of IMPORTS
```

```
-- =====
-- Object Identifier Definition
-- =====
```

```
ilHIDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) informationHandover(4) ilhi(0)}
```

```
ilHIObjId OBJECT IDENTIFIER ::= { ilHIDomainId ilhiPdu(0) version2(2)}
```

```
preagreedObjId OBJECT IDENTIFIER ::= { ilHIDomainId identifiers(1) preagreed(0)}
```

```
-- =====
-- Inter LEMF Handover Elements
-- =====
```

ILHIPayload ::= SEQUENCE

```
-- This Payload sends additional ILHI specific parameters, the resPayload and
-- the originalPayload.
{
  ilHIObjId [0] OBJECT IDENTIFIER,
  resPayload [1] EncapsulationPayload,
  mappingInfo [2] MappingInfo OPTIONAL,
  -- output from the MapF
  originalPayload [3] EncapsulationPayload OPTIONAL,
  ...
}
```

```

EncapsulationPayload ::= SEQUENCE
{
  identifier          [0] OBJECT IDENTIFIER,
  -- see clause 8.1
  contents           [1] OCTET STRING,
  ...
}

```

```

MappingInfo ::= SEQUENCE
{
  timestampMapping   [0] SEQUENCE OF TimestampMapping OPTIONAL,
  locationMapping    [1] SEQUENCE OF LocationMapping OPTIONAL,
  ...
}

```

```

TimestampMapping ::= SEQUENCE
{
  originalTimestamp  [0] OriginalTimestamp,
  normalizedTimestamp [1] ILHITimestamp,
  timeStampQualifier [2] LI-PS-PDU.TimeStampQualifier OPTIONAL,
  ...
}

```

```

ILHITimestamp ::= CHOICE
{
  qualifiedDateTime      [1] Common-Parameters.QualifiedDateTime,
  qualifiedMicrosecondDateTime [2] Common-Parameters.QualifiedMicrosecondDateTime,
  ...,
  unqualifiedDateTime    [3] NULL
  -- The unqualifiedDateTime choice is used if the timestamp is not mappable with
  -- the Mapping function because e.g. the timezone information is missing
}

```

```

OriginalTimestamp ::= CHOICE
{
  timeStamp          [1] GeneralizedTime,
  microSecondTimeStamp [2] LI-PS-PDU.MicroSecondTimeStamp,
  ...,
  otherTimeStamp     [3] UTF8String
  -- The otherTimeStamp choice contains a value if for any reason the received timestamp
  -- is not mappable into the fields timeStamp or the microSecondTimeStamp
}

```

```

LocationMapping ::= SEQUENCE
{
  originalLocation     [0] LI-PS-PDU.Location,
  normalizedLocation   [1] NormalizedLocationData,
  ...
}

```

```

NormalizedLocationData ::= SEQUENCE
{
  geocodedLocationData [0] GeocodedLocationData,
  supplementaryLocationData [1] SupplementaryLocationData OPTIONAL,
  -- any additional information for an improved presentation of location
  -- (e.g. details of the network elements like transmitter details) should
  -- be inserted into this parameter
  ...
}

```

```

GeocodedLocationData ::= CHOICE
{
  wGS84CoordinateDecimal [1] Common-Parameters.WGS84CoordinateDecimal,
  wGS84CoordinateAngular [2] Common-Parameters.WGS84CoordinateAngular,
  ...
}

```

```

SupplementaryLocationData ::= SEQUENCE
{
  azimuth [0] INTEGER (0..359) OPTIONAL,
  -- The azimuth is the bearing, relative to true north
  ...
}

```

END --end of ILHIPDU

Annex C (informative): Change History

TC LI approval date	Version	Information about changes
July 2018	1.1.1	First publication of the TS after approval ETSI TC LI#48. Document prepared by Markus Keil (rapporteur).
October 2019	1.2.1	Included Change Requests: TS103462CR001 Correction of Timestamp and clarification of payload aggregation. This CR was agreed by TC LI#52 (15-17 October 2019, Turin). Version 1.2.1 prepared by Rapporteur.

History

Document history		
V1.1.1	July 2018	Publication
V1.2.1	December 2019	Publication