ETSI TS 103 707 V1.6.1 (2022-08)

TECHNICAL SPECIFICATION

Lawful Interception (LI); Handover Interface for HTTP delivery

Reference

RTS/LI-00228

Keywords

handover, 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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 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 present document provides the handover details for HTTP delivery of Lawful Interception (LI) and Lawful Disclosure (LD). For services which are fully standardized (fully and explicitly defined by an existing public standards document), it is recommended that the existing standards definitions are used as the basis of the handover interface. In particular, certain service types have existing LI handover formats and it is recommended to use these where they are applicable, e.g. ETSI TS 102 232-2 [i.5] and ETSI TS 102 232-5 [i.6].

1 Scope

The present document provides the handover details for HTTP delivery of LI and LD. The present document applies in particular to messaging services, but is not limited to messaging services.

The delivery of streaming content is not in the scope of the present document.

2 References

2.1 Normative references

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

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

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

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

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

[2] IETF RFC 2818: "HTTP Over TLS".

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

NOTE: Obsoleted by IETF RFC 8446.

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

[5] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[6] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

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

[8] IETF RFC 6838: "Media Type Specifications and Registration Procedures".

[9] FIPS Publication 180-4 (2015): "Secure Hash Standard (SHS)".

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] Recommendation ITU-T E.164: "The international public telecommunication numbering plan".

[i.2] IETF RFC 5322: "Internet Message Format".

[i.3] IETF RFC 5321: "Simple Mail Transfer Protocol".

[i.4] IETF RFC 3696: "Application Techniques for Checking and Transformation of Names".

[i.5] 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.6] 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".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Lawful Disclosure (LD): process by which a LEA requests and receives data from a CSP

NOTE: A formal definition of Lawful Disclosure (or the related terms "Retained Data" and "Stored Data") is not given in the present document but could be found in relevant applicable regulation.

messaging service: service which allows users to transfer messages to a finite number of users whereby the persons initiating or participating in the communications determine its recipient(s)

3.2 Symbols

Void.

3.3 Abbreviations

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

CA	Certificate Authority
CSP	Communications Service Provider
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ID	Identifier
IP	Internet Protocol
LD	Lawful Disclosure
LDID	Lawful Disclosure Identifier
LEA	Law Enforcement Agency
LI	Lawful Interception
LIID	Lawful Interception Identifier
MIME	Multipurpose Internet Mail Extensions
MSISDN	Mobile Station International Subscriber Directory Number
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
XML	eXtensible Markup Language
XSD	XML Schema Definition

4 Introductory material

4.1 Reference model

This clause provides a Reference Model which applies to request and delivery mechanisms between Law Enforcement Agencies (LEAs) and Communications Service Providers (CSPs) for the present document.

Request means submission of a request for data and delivery means handover of the material that was identified by the CSP as meeting the request. Figure 1 shows the reference model.

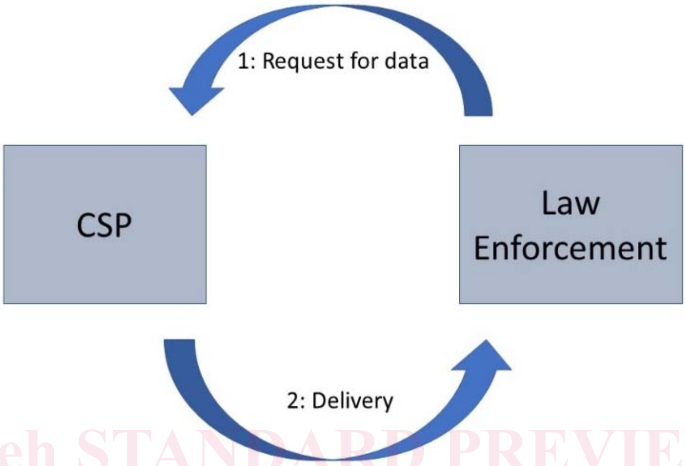

Figure 1: Reference model

The LEA/CSP standards should accommodate for a variety of different law enforcement agencies and for a variety of CSPs. In other words, it is important to support some variance in the internal procedures, processes and data structures. Such variance should not compromise the establishment of security best-practice.

4.2 Responsibilities

The LEA is responsible for creating a lawful request and the request needs to be clear. The LEA delivers the request to the CSP. The legal obligation on the CSP (e.g. what has to be delivered, what has to be retained) is managed independently of the delivery interface and is out of scope of the present document.

The CSP is responsible for the collection of the data within its system, and produces the data using its own capabilities and entirely under the control of the CSP system. The CSP identifies the data which matches the clear request, and only that data. The CSP needs to be able to perform a human review of the request and delivered material. The CSP packages the data, attaches relevant information (e.g. unique reference number, timestamp) and delivers it to the requesting LEA.

Each request is distinct and shall be handled independently of other requests.

5 Basic concepts

5.1 General

The object consists of the following components:

- Application level header (see clause 5.3).
- Core parameters (see clause 5.4).
- Glossary (see clause 5.5).

- CSP-defined information (see clause 5.6).

The components "Core parameters" and "Glossary" vary depending on the service in question. The details are given in clauses 5.4 and 5.5.

The object is delivered using ETSI TS 103 120 [1] as described in clause 5.2.

The following parameter definitions use the terminology of one of the following:

- Mandatory (M): required for every delivery.
- Conditional (C): required in situations where a condition is met (the condition is given in the description).
- Optional (O): provided at the discretion of the implementation.

5.2 Delivery

5.2.1 General

Handover items are delivered using the DeliveryObject as described in ETSI TS 103 120 [1], clause 10.
A DeliveryObject may contain either a single handover item (using the "handoverItem" root element) or a collection of handover items (using the "handoverItemCollection" root element). All handover items in a collection shall be related to the same Reference (see Table 3).

The present document does not require the use of any of the tasking components from ETSI TS 103 120 [1]. The present document does not require the use of national profiles (as per the definition of profiles in ETSI TS 103 120 [1]).

5.2.2 ETSI TS 103 120 Message header

The Message Header fields shall be populated as defined in ETSI TS 103 120 [1], clause 6.2, with the additional clarifications as shown in Table 1.

Table 1: ETSI TS 103 120 [1] Message Header population

Parameter	Description	M/O/C
senderIdentifier	The Sender is the CSP. The SenderIdentifier has two components: a CountryCode and a UniqueIdentifier. They shall be populated as follows: • The CSP shall choose the CountryCode; this may be "XX". • If the LEA has supplied a UniqueIdentifier then this shall be used; otherwise the CSP shall choose its own SenderIdentifier.	M
receiverIdentifier	The Receiver is the LEA. The ReceiverIdentifier has two components: a CountryCode and a UniqueIdentifier. They shall be populated as follows: • CountryCode: If the LEA has supplied a ReceiverIdentifier-CountryCode then this shall be used. It is recommended that this is populated in order to assist with uniqueness, see the text at the end of clause 5.2.3. If no CountryCode has been supplied or agreed with the LEA then "XX" shall be used. • UniqueIdentifier: If the LEA has supplied a ReceiverIdentifier-UniqueIdentifier then this shall be used. In general, the actual LEA should not be identified on this interface, and (unless agreed otherwise) the UniqueIdentifier should contain the text "Not specified".	M
timestamp	Shall specify the time the message was created.	M
version	Shall be set to the version of ETSI TS 103 120 [1] used. If national profiles are not used, the NationalProfileOwner and NationalProfileVersion strings shall be set to "N/A".	M

5.2.3 ETSI TS 103 120 Object header

The payload shall contain a "Delivery Request", which shall contain a DeliveryObject as per ETSI TS 103 120 [1], clause 10.

The common Object fields shall be specified as per ETSI TS 103 120 [1], clause 7.1.1 with the clarifications as shown in Table 2.

Table 2: Object top-level fields

Parameter	Description	M/O/C
countryCode	Shall be set to the Country Code used in the ReceiverIdentifier field (see Table 1).	M
ownerIdentifier	Shall be set to the value given in the ReceiverIdentifier.	M
nationalHandlingParameters	Shall not be used.	N/A

Parameters for the DeliveryObject shall be set as per ETSI TS 103 120 [1], clause 10, with the clarifications as shown in Table 3.

Table 3: Clarifications regarding DeliveryObject as per ETSI TS 103 120 [1], clause 10

Parameter	Description	M/O/C
Reference	Target identifier i.e. LIID or LDID. If an LIID or LDID has been supplied by the LEA then this shall be used. See paragraph at the end of clause 5.2.3. If an LIID or LDID has not been supplied by the LEA then it shall be chosen by the CSP in accordance with practices agreed by LEA and CSP.	M
Manifest	If present, it shall specify ETSI TS 103 707 (the present document) as the delivery type.	O
Delivery	Shall contain an XML-encoded object compliant with the ETSI TS 103 707 (the present document) schema (see clauses 5.3 to 5.6).	M

It is recommended that the LEA chooses the LIID and that specifies a country code for the ReceiverIdentifier-CountryCode as this is one way that can be used to ensure uniqueness of identifiers.

5.3 Application level header

5.3.1 General

Each handover item may contain an application level header, with the fields shown in Table 4.

Table 4: Application level Header structure

Parameter	Description	M/O/C
applicationCorrelation	May be used to indicate that a number of handover items are related to each other (see clause 5.3.2).	O

5.3.2 ApplicationCorrelation

If a number of handover items are related to each other, a CSP may use the ApplicationCorrelation structure to indicate that they are related.

When this mechanism is used, related items shall be allocated the same ApplicationLevelID value. This value shall be unique within a given LIID or LDID. The precise format and choice of value is an implementation decision for the CSP.

Each item with the same ApplicationLevelID value shall be allocated a sequence number which is then used to populate the ApplicationSequenceNumber field. The sequence number shall start at zero.

Table 5: ApplicationCorrelation structure

Parameter	Description	M/O/C
applicationLevelID	Application sequence context, unique within a given LIID or LDID. Given as a non-negative integer.	M
applicationSequenceNumber	Zero-based counter within the ApplicationLevelID.	M

5.4 Core parameters

5.4.1 General

Table 6 defines the core parameters of a messaging service.

NOTE: The present document does not contain core parameters for any other services than messaging services.

Table 6: MessagingCoreParameters

Parameter	Description	M/O/C
messageSender	Identifier of the sender of the message, if available. Given as a MessagingParty (see clause 5.4.2).	O
messageReceivers	List of identifiers of the receivers of the message, if available. Given as a list of MessagingParty (see clause 5.4.2).	O
timestamp	Time of the event given as a QualifiedDateTime as per ETSI TS 103 280 [7].	M
associatedBinaryData	List of binary objects (if any) associated with the event (see clause 5.4.3).	O
NOTE: The assumption is that the messaging service is offered as a closed ecosystem, i.e. both parties are subscribed to the same service.		

5.4.2 MessagingParty

The MessagingParty type is used to provide a list of identifiers associated with a messaging party (either a sender or a receiver). Multiple identifiers may be provided. The format and values of the identifiers are determined by the CSP.

Each MessagingParty may include an indication of whether the party was the subject of interception.

Table 7: MessagingParty parameters

Parameter	Description	M/O/C
identifiers	List of one or more identifiers associated with the messaging party.	M
isTargetedParty	Indication that the messaging party is the subject of interception. Absence of the indication may be taken to mean that either the party is not the subject of interception, or that it is not known whether it is the subject of interception.	C

5.4.3 AssociatedBinaryData

The associatedBinaryData field is used by the CSP to provide details of any data, such as attached images or video, associated with the delivered information. The data itself shall be delivered separately, according to the details in Annex C.

The associatedBinaryData field contains a set of binaryObject records, each structured as given in Table 8.