ETSI TS 103 707 V1.2.1 (2021-03)

Lawful Interception (LI);
Handover for messaging services over HTTP/XML

Reference
RTS/LI-00203

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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 delivery over HTTP/XML of LI (Lawful Interception) and LD (Lawful Disclosure). The present document applies in particular, but is not limited to, messaging services. The CSP may opt to use other standards to facilitate LI over TCP/ASN.1 as an alternative message format, e.g. ETSI TS 102 232-2 [i.5] (for messaging services) and ETSI TS 102 232-5 [i.6] (for IP Multimedia Services).

1 Scope

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

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): the 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
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.

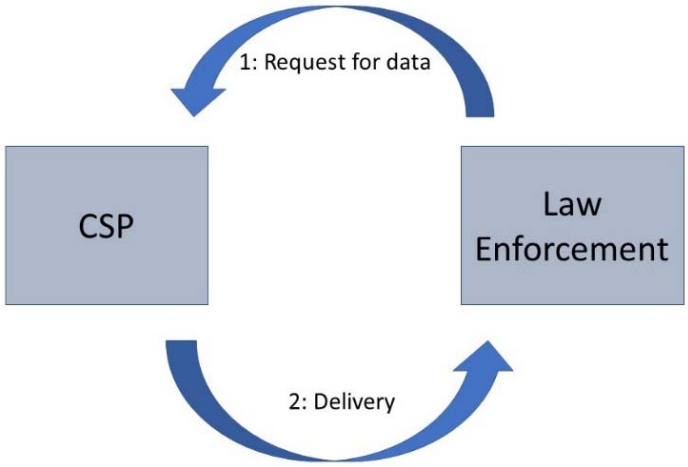

Figure 1: Reference model

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.

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 (if available) given as a QualifiedDateTime as per ETSI TS 103 280 [7].	O
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.

Table 8: BinaryObject structure

Parameter	Description	M/O/C
url	URL associated with the delivery of the binary data (see Annex C). Shall be unique for a given binary object from a CSP and shall not be re-used by the CSP to identify other binary objects in future.	M
contentLength	Size of the data transferred, given in octets (i.e. equivalent to the Content-Length header in the HTTP transfer), see Annex C.	O
contentType	MIME type that described the form of the data (i.e. equivalent to the Content-Type header in the HTTP transfer) if present. Given as per IETF RFC 6838 [8].	O
expiry	Time at which the URL ceases to be valid for delivery of the data (when using Model A delivery, see Annex C). Given as QualifiedDateTime as per ETSI TS 103 280 [7].	C
checksum	If used, SHA-256 checksum (as defined in FIPS Publication 180-4 [9]) of the binary data before any encryption, compression or other transfer encoding are employed.	O
originalFilename	Original filename associated with the data, if applicable and available.	C
cspDefinedIdentifier	A CSP-defined identifier associated with the data (e.g. as used within the CSP-defined parameters block) if applicable.	C

5.5 Glossary

The term glossary is used to refer to parameters for which there is a common definition, context and meaning as agreed by LEAs and CSPs.

NOTE: The present document does not contain any glossary parameters.

The use of the glossary is in addition to the technique in clause 5.6 in which the parameter definitions from ETSI TC LI's standard LI dictionary (ETSI TS 103 280 [7]) are re-used.

5.6 CSP-defined information

5.6.1 General

The CSP-defined information includes any self-described information that the CSP can provide for the interception (meta-data and the content of communication) or LD. The parameters themselves are not defined by the present document.

Some examples of items which might be present for messaging services are:

- Time of receiving message.
- Status information - drafted/read/deleted/not consistent.
- Network layer details or hardware ID.
- Group events - joins/leaves/is admin/makes changes to a group.
- Location information.
- Group name.
- Thread title.
- Thread ID.
- Event type.

CSP-defined information shall be provided in the CSPDefinedParameters field.

5.6.2 CSP-defined schema

The CSP is required to describe the schema of data provided in the CSP-defined information and provide appropriate descriptions.

Details of the schema shall be provided using the schemaDetails structure shown in Table 9.

Table 9: SchemaDetails structure

Parameter	Description	M/O/C
schemaIdentifier	A unique identifier for the schema assigned by the CSP. If a schema is changed or updated, the CSP shall assign a new schemaIdentifier. The LEA can use the schemaIdentifier to identify the correct schema to interpret the CSP-defined data.	M
schemaURL	Optional URL to indicate where the contents of the schema may be retrieved from.	O
schemaContent	Optional field that the CSP may use to provide the content of the schema as part of the delivery. Alternatively, the schema contents may be provided out-of-band.	O

If the CSP has already provided the schema to the LEA, it may provide only the schemaIdentifier which refers the specific schema previously provided.

5.6.3 Use of common types from ETSI TS 103 280

Where CSP-defined schemas contain information elements which correspond to common types already defined in ETSI TS 103 280 [7] (e.g. MSISDN) CSPs should use the types defined in ETSI TS 103 280 [7] as part of their schema definitions.

NOTE: This technique is in addition to the use of Glossary terms as defined in clause 5.5.

5.6.4 Including binary data in the CSP-defined content

Details for the delivery of binary data associated with a message are given in Annex C.

5.7 Error reporting

In the reference model, the request for data and submission of warrant information may not happen on the same logical channel as the delivery of data. Hence, two types of error reporting are required: error reporting related to the transfer and management of warrant information as well as requests for data on the one hand, and error reporting related to the handing over of data by the CSP using the XML/HTTP mechanism specified in the present document on the other hand. Errors related to the latter case are as described in clause 6.2.

6 Transport details

6.1 HTTP details

There shall be a mechanism to establish the destination information as per ETSI TS 103 120 [1], clause 8.3.6 (specifically clause 8.3.6.2). This is not specified in the present document.

The delivery protocol is as specified in ETSI TS 103 120 [1] clause 9, except that the security details (ETSI TS 103 120 [1], clause 9.3.4) are not used and clause 7 of the present document is used.

6.2 Error reporting for transport

Errors relating to the transport mechanism are handled in accordance with the transport mechanism as per ETSI TS 103 120 [1].

7 Security

Implementations shall support HTTPS as defined in IETF RFC 2818 [2]. The TLS version shall be at least 1.2, as defined in IETF RFC 5246 [3]. TLS 1.2 implementations should support the recommendations given in IETF RFC 7525 [4]. TLS 1.3 may be supported, as defined in IETF RFC 8446 [5]. TLS implementations shall support mutual authentication through bidirectional certificate usage.

Implementations shall use HTTPS.

Security requirements shall be mutually agreed for the transport layer, including specification of any necessary encryption, signatures or hash functions and any requirements for encryption of data at rest.

Payload security is for further study.

Issues such as key management, key length, key exchange, choice of cryptographic algorithm, etc., are outside of the scope of the present document.

The use of pre-shared keys may be considered for authentication at the transport layer. If this option is selected, the specifications set forth in IETF RFC 4279 [6] shall be followed.

Additional security considerations are given in Annex D.

Annex A (informative): Messaging service identifiers

A.1 Identifiers

This annex identifies three different categories of identifiers of messaging services.

Table A.1: Types of messaging identifiers

Type of identifier	Definition	Example	How it is used
Category 1: Long-term unique ID	This is an identifier that the provider uses for the business purpose of keeping a handle on a single subscriber. It might be internal.	Company specific IDs. Note that these may be unique across different services and linking between identifiers for different services is not necessarily easy.	These are a good basis for submitting and fulfilling a request for information. The identifier may be in a non-public or non-readable format (it may be binary or hex digits) and the present document allows flexibility of formats.
Category 2: Unique but potentially brittle ID	This is an identifier which is likely to be unique at a given point in time but might change over time (e.g. daily/weekly/every few years but not every minute).	Phone number, email address. Note that there are good security reasons for rotating certain identifiers in this category e.g. certain crypto keys which are associated with some IDs.	These are a good basis for making a request provided they have an accurate observed time associated with them (which should not be assumed to be the time of the request). Potentially the provider can then map the brittle identity to their own internal unique ID (i.e. a category 1 identifier). This process (of determining the best possible identifier) may work differently in different situations and is out of scope of the present document.
Category 3: Not unique identity or name	This is an identifier which can be changed or chosen freely and frequently.	A username or informal ID.	These would be useful to be delivered as part of returning information about a subject. It should be noted that there could potentially be many matches to any particular username, even for names that appear to be very rare or unusual.

There is a process which involves discussions between LEA and CSP which needs to result in an identifier to be used as the basis of the authorization. This process is outside of the scope of the present document though it may involve a category 2 identifier and a timestamp to create an agreed identifier (e.g. a category 1 identifier). The conclusion of this process would result in identifiers and the present document lists possible types of identifier where this is necessary for it to be understood. This could be one of a standardized type (phone number, username or user ID, email address) as described in Table A.2 or a free-text description.

Table A.2: Parameters and references of messaging identifiers

Identifier	Parameters	Comments or references
User ID	Userid	
Username	username or username-and-timestamp	username-and-timestamp is made of username and of timestamp.
Phone number	msisdn or msisdn-and-timestamp, e164-format or e164-format-and-timestamp	msisdn, and e164-format, are defined in the Recommendation ITU-T E.164 [i.1]. msisdn-and-timestamp is made of msisdn and of timestamp. E164-format-and-timestamp is made of e164-format and of timestamp.
Email address	email-address or email-address-and timestamp	IETF RFC 5322 [i.2], IETF RFC 5321 [i.3] and IETF RFC 3696 [i.4] define the email-address. email-address-and-timestamp is made of email-address and of timestamp.

Annex B (normative): Messaging XSD definition

The XSD is provided as an XML XSD schema set, contained in archive ts_103707v010201p0.zip which accompanies the present document.

Annex C (normative): Content delivery

C.1 General

This clause describes the procedures for delivering binary data associated with a DeliveryObject. As described in clause 5.4.3, each DeliveryObject may contain one or more binaryData records. Each record describes a binary object to be delivered from CSP to LEA. Each binary object is delivered using HTTPS following the details in clause 7.

Two models are described in the present document (chosen by mutual agreement):

- Model A: Each binary object is represented by a URL that may be queried by the LEA (see clause C.2).
- Model B: The CSP POSTs each binary object to a URL owned by the LEA (see clause C.3).

Developers should be aware of situations in which there is a mix of very large files and some small files (which could potentially be very urgent). Care should be taken to avoid head-of-line blocking issues i.e. try to share available bandwidth between large and small files thus allowing the small files to be delivered in a timely manner.

C.2 Model A

Each binaryData record contains a URL hosted by the CSP. On receiving the URL, the LEA system may automatically query the URL using the same authentication factors as the original request (see clause 7). The CSP shall then deliver the contents to the LEA using an HTTP Response with the appropriate MIME type.

It is the responsibility of the LEAs to maintain the association between the binary file, the LIID and the particular message (if any).

If a request is made to a valid URL but using the wrong SSL certificate, the CSP shall ensure that the error message returned does not reveal that the URL was valid.

C.3 Model B

The LEA defines a URL scheme for delivery of binary data that can be reached by the CSP. The URL scheme shall contain a single parameter for a unique identifier associated with the binary object:

- https://lea.example.com/binaryData/{*object identifier*}/

The LEA shares the scheme with the CSP in advance. When delivering binary data, the CSP forms a complete URL for each binary object by allocating a UUID to it and inserting it into the appropriate part of the URL scheme. The CSP uses this URL to populate the URL field in the binaryData record for that object.

The CSP shall deliver the binary data after delivering the DeliveryObject containing the binaryData record. The CSP delivers the data by HTTP POST to the appropriate URL using the appropriate MIME type. The CSP client shall use the Expect request header field to expect a 100 CONTINUE response from the LEA server. If the size of a file is known ahead of time, it shall be added to the HTTP message's Content-Length header. It is recommended that the CSP's client continue timeout be set according to the expiry time given in the binaryData record (see Table 8), and that the timeout should be sufficient to allow the DeliveryObject to be processed by the LEA before the binary data is transferred.

The LEA is responsible for maintaining the association between the binary data, the LIID and the message by using the URL. LEA implementations should provide for the possibility that the DeliveryObject is processed after an attempt to deliver binary content is made.

Annex D (informative): Additional security considerations

D.1 Reference model

The reference model in Figure D.1 is used for this annex.

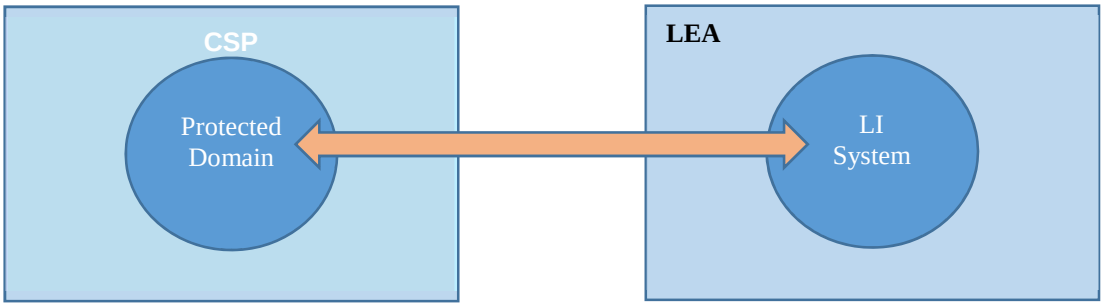

Figure D.1: Reference model showing Protected Domain

This Annex considers the provision of security via the isolation of a Protected Domain within the CSP. This domain or enclave is used for providing LEA support within the CSP.

D.2 Summary of considerations

Each CSP is different and has different concerns and designs so the present document does not put forward a one-size-fits-all solution. However, there are important considerations which are relevant to most or all situations; the approach of the present document is to provide a list of these security considerations. CSPs should take these into account and should try to provide reassurance to LEAs on relevant considerations.

D.3 Considerations in more detail

D.3.1 Data-at-rest

Sensitive data is being stored by the CSP in two stages:

a) While a task is active / while a query is being answered. During an active task, there is sensitive data present (e.g. in order to match against target identifiers). Care should be taken to keep these within the Protected Domain except where necessary (see clause D.3.4).

b) After a task or query has been completed e.g. for audit purposes. It is important to give careful consideration to audit data. Where data is stored for long periods of time (e.g. years) then it is particularly important to avoid keeping large stores of sensitive data. A useful technique is to hash or obscure those fields which are particularly sensitive (typically it will be the personally identifiable information e.g. the target identifier). A process for obscuring sensitive fields is given in section D.4. This allows most fields to remain and provides a process for the CSPs to re-instate the sensitive fields where necessary (but not on a blanket or ad hoc basis).

D.3.2 Measures for assuring the Protected Domain

The following considerations are relevant for assuring the Protected Domain:

a) How is the Protected Domain defined? It is important to look at how the boundary of the Protected Domain is created and enforced. Where practical, then it is helpful for there to be some sort of physical separation but the concerns around "following the sun" (see also point b) apply. There should be software boundaries and isolation to restrict access so that data within the Protected Domain is only seen by those with authority to do so.

b) People. Consideration should be given to the process by which people are given privileges to work within the Protected Domain. It is important to consider that many CSP operations have to work 24/7 and potentially "follow the sun" so consideration should be given to the situation where staff in the Protected Domain come from a variety of nationalities.

c) Data leaving the Protected Domain. It is important to look at any data that might potentially leave the Protected Domain. Consideration should be given to alarms, logs and backups. Wherever possible, care should be taken to ensure that alarms, logs and backups do not contain sensitive information. If it is necessary that these do contain sensitive information, then they should not leave the Protected Domain. Audit logs should also be considered: see clause D.3.1.

d) Protective monitoring should be considered in line with industry best practice. Specific examples relating to Protected Domains include the monitoring of:

   - When people are assigned to (or removed from) the privileges within the Protected Domain.
   - Access to sensitive data stores within the Protected Domain.
   - Account behaviour for people who have privileges within the Protected Domain.

D.3.3 Certificate Authorities

Certificate Authorities (CAs) are used to help identify where the data came from i.e. clear assurance that data came from the relevant CSP. Consideration should be given to whether a CA can help give assurance that the data came from within the Protected Domain.

D.3.4 Collection of data from outside the Protected Domain

Data collection is typically taking place on systems outside the Protected Domain. The following considerations apply to data that is collected from outside the Protected Domain:

- The footprint of this collection process should be as small as possible.
- Specifically look at audit logs and error/alarm procedures. They should either not have sensitive information or should be passed to systems within the Protected Domain.

D.4 Using hashing to obscure sensitive data in audit stores

D.4.1 Overview

This section provides a solution to meet two important considerations:

1) CSPs should keep audit records so that all necessary data fields can be checked when needed.

2) To protect LEA operations and subscribers' privacy, the CSPs should not store sensitive personal information for longer than is necessary.

The present document does not define the meaning of the word "necessary" in either point (1) or point (2). The purpose of this section is to provide a technique that facilitates audit and also reduces the storage of sensitive information.

D.4.2 Process

The process is based on the following situation:

- That there is sensitive information (e.g. a selector used to identify a subject of interest) which is part of the tasking/request to the CSP.
- That the CSP wants to be able to check or audit this information after the request/tasking has been completed.
- That there is a concern about the CSP keeping a large store of sensitive information.

The following process is designed to be useful for the above situation:

- The LEA generates the sensitive field as part of the tasking/warrant/requesting process.
- The LEA also generates a random value (called a salt).
- The LEA also generates a hash based on the sensitive field and the salt.
- The LEA sends the sensitive field, salt and hash to the CSP.
- The CSP checks that the hash has been properly created (i.e. that it is the hash of the sensitive field and the salt).
- Once the request has been fulfilled (i.e. the tasking is complete or the order has expired), the CSP deletes the sensitive field and the salt, but keeps the hash as part of the audit record.
- In many cases, the CSP audit can be performed without knowing the value of the sensitive field (for example, if they need to check the tasking numbers, or the dates of requests, or how many there were).

If, as part of a future audit process, the CSP needs to know the sensitive field, they would ask the LEA. The LEA would send the sensitive field and the salt, so that the CSP can check the hash is correct and have confidence that the value has not been changed. The audit would be completed and then the sensitive field and salt would be deleted by the CSP.

Annex E (informative): Change History

Status of Technical Specification ETSI TS 103 707 Handover for messaging services over HTTP/XML		
TC LI approval date	**Version**	**Remarks**
March 2020	1.1.1	First publication of the TS after approval by Remote Consensus following the agreements at ETSI TC LI#53 (4-6 February 2020, Sophia Antipolis, France)
February 2021	1.2.1	Included Change Requests agreed by ETSI TC LI#56e CR001, LI(21)P56019r2 (Cat B) Addition of security recommendations CR003, LI(21)P56023r4 (Cat B) Delivery of Lawful Disclosure Information

History

Document history		
V1.1.1	March 2020	Publication
V1.2.1	March 2021	Publication