ETSI TS 103 307 V1.4.1 (2021-06)

TECHNICAL SPECIFICATION

CYBER; Security Aspects for LI and RD Interfaces

Reference

RTS/CYBER-0071

Keywords

cyber security, lawful interception, retained data

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

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 Cyber Security (CYBER).

Modal verbs terminology

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

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

1 Scope

The present document specifies security processes and techniques for LI and RD systems.

The present document is limited to:

1) The provision of evidential assurance of RD material.

2) Security issues around the role for global, third-party or virtualized components for RD systems.

Future versions of the present document will cover:

1) Assurance of the integrity and originator of approvals/authorizations.

2) Security aspects of internal interfaces for Lawful Interception.

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

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

[i.3] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC)".

[i.4]	CESG guidance: "Cloud Security Guidance: Implementing Cloud Security Principles".

NOTE 1: Available at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles.

NOTE 2: Text extracted from [i.4] and used in the present document is in italics and done according to the Open Government Licence available at http://www.nationalarchives.gov.uk/doc/open-government-licence/version/1/open-government-licence.htm.

[i.5]	ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".
[i.6]	ETSI GS NFV-SEC 010: "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements".
[i.7]	IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 657 [i.1] and the following apply:

third party: organization other than the CSP or LEA who is engaged to assist in providing RD or LI services

NOTE: Often the phrase "Trusted Third Party" is used. Clearly the CSP or LEA are expected to engage Third Parties whom they consider to be trusted.

3.2 Symbols

Void.

3.3 Abbreviations

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

CESG	Communications Electronic Security Group
CSP	Communications Service Provider
LEA	Law Enforcement Agency
LI	Lawful Interception
PDF	Portable Document Format
RD	Retained Data
SHA	Secure Hash Algorithm
XML	eXtensible Markup Language

4 Structure of document and list of relevant interfaces

4.1 Introduction

The present document considers the list of particular information flows and interfaces for RD and LI specified in clause 4.2. It examines them from a security (confidentiality, integrity and authenticity) perspective and specifies implementation details (technologies, algorithms, options, minimum requirements on keys, etc.).

An underlying reference model for LI is given in ETSI TS 102 232-1 [i.2] and an underlying reference model for RD is given in ETSI TS 102 657 [i.1].

Certain techniques are applicable to more than one information flow or interface. Generic techniques are addressed in clause 5.

For each information flow or interface, the present document contains the following information (where applicable):

- Statement of the problem, including reference model.
- Identification of the threats and risks to the extent it is appropriate to publish in a standard.
- Statement of the techniques which are recommended as a solution.

4.2 List of LI and RD items covered in the present document

The present document addresses the following LI and RD items:

1) Providing evidential assurance of LI or RD material (annex A).

2) Security issues around the role for global, third-party or virtualized components of Retained Data facilities (annex B).

The following topics will be covered in future versions of the present document:

1) Assurance of the integrity and originator of approvals/authorizations.

2) Security aspects of internal interfaces for Lawful Interception.

5 Common techniques

5.1 Introduction

The following techniques are used in a number of the annexes of the present document:

- Algorithms for hashing data.

The following techniques will be included in future versions of the present document:

- Digital signature algorithms.
- Procedures for Trusted timestamp.
- Transport-layer security.

5.2 Hash algorithms

The SHA-256 algorithm shall be as defined in FIPS Publication 180-4 [1].

The SHA-512 algorithm shall be as defined in FIPS Publication 180-4 [1].

Annex A (normative): Providing assurance for LI or RD material as evidence

A.1 Statement of problem

The requirement is to provide assurance about the integrity of the LI or RD material (i.e. to help with assurance that it has not been altered during the course of delivery and/or storage with end user authorities) and to provide assurance about the originator of the material (i.e. the organization that produced it). The present document does not look at any requirement for confidentiality in this annex.

The goal of this clause is to add assurance to LI or RD material if it is presented as evidence in court. The present document does not attempt to examine legal aspects and no assurance is given that the process in the present document provides a complete or adequate level of assurance for any particular jurisdiction.

The reference model for this clause consists of two parties:

- The originator: the party that creates the material and wishes to provide assurance about its integrity and origin.
- The receiver: the party that wishes to check the integrity and originator of the material.

In a typical situation:

- The originator is the CSP, and the information flow starts at the point where material is selected by the CSP for use as RD or LI. The present document does not examine the integrity of existing CSP business records.
- The receiver is wherever there is a requirement to check the integrity and origin. This can include:
    - immediately upon receiving the material at a government/police agency; or
    - as a check by police or prosecution teams prior to court; or
    - for checking at any time during court proceedings.

The information contained within the flow is not defined within the present document, except where it is noted that parameters (such as identifiers or timestamps) would be needed in order to meet the requirements.

A.2 Techniques for providing assurance for LI or RD material as evidence

A.2.1 How to use the present document

The present document lists a set of techniques which may be used to help provide assurance of LI or RD material used in evidence.

A threat analysis should be performed on a national basis to determine the set of techniques which is appropriate for any given jurisdiction or situation.

Systems should be designed to avoid a "bid-down" attack where techniques can be selected which are not appropriate for the threats they are trying to mitigate.

A.2.2 Types of technique

Techniques for assuring evidence can be categorized as:

- Process-based: It is possible to assure evidence by demonstrating that a process was followed in accordance with approved procedures.

EXAMPLE 1: Use a published procedure for how a Retained Data response file is stored, and demonstrate that these procedures had been followed.

- Cryptography-based: It is possible to assure evidence based on cryptographic assurance of the integrity and origin of material.

EXAMPLE 2: If material is signed using a private key which has been stored securely, there is cryptographic assurance that it was produced by the owner of the private key.

Many countries/jurisdictions use a mix of both process-based techniques and cryptographic techniques. The present document does not state that one type of technique is fundamentally better than the other. It is national choice whether to use process-based techniques, or cryptographic techniques or a mixture of the two.

A.2.3 Techniques in the present document

The present document lists two cryptography-based techniques:

- "Hash-only technique": clause A.3 specifies a technique by which hashes give assurance to Retained Data records. This technique provides assurance that evidence has not been altered from originator to receiver. It places a requirement on the sender to keep a record of the hashes it created.

- "Digital-signature technique": this technique provides assurance of the integrity and origin of the material. The details of this technique (in an LI context) is given in ETSI TS 102 232-1 [i.2]. It relies on the cryptographic material being stored securely.

A.3 Detailed definition for hash-only technique in the context of Retained Data

A.3.1 Summary

This clause defines a technique based on hashing without using signatures. The present document describes this technique in the context of assuring the integrity of Retained Data records from the point when a request is answered by the CSP (e.g. through to its use in legal proceedings). However, it can be used in other contexts e.g. for material other than Retained Data or for assuring Retained Data at other stages.

This clause highlights how the present document can be used in conjunction with ETSI TS 102 657 [i.1].

This clause covers the cases where:

- The CSP performs hashing of the Evidence Data as per clauses A.3.2 to A.3.8;

- A CSP proxy performs hashing on behalf of the CSP (clauses A.3.9.1 to A.3.9.4);

- The CSP has produced a hash but the hashing process did not follow all the processes in clauses A.3.2 to A.3.8 (clause A.3.9.5).

A.3.2 Terminology used in clause A.3

The terms "Request" and "Response" are defined in ETSI TS 102 657 [i.1].

The "Evidence Data" is the response generated by the CSP that is required to be assured for use as potential evidence. The Evidence Data is considered to be immutable or "atomic" i.e. it is not possible to discard part of the evidence and assure the remainder. If information has sub-components that can be used independently then each component is considered to be a single piece of Evidence Data and is hashed separately. Clause A.3.6 details how the Evidence Data and hashes can be associated.

The "LEA Receiver" is the function on the Police/LEA side of the interface which is the first function to receive the Evidence Data. Clause A.3.3.4 provides recommendations for the LEA Receiver.

A.3.3 Processes and testing

A.3.3.1 Process at CSP

A.3.3.1.1 Creation of response

Once the Evidence Data is generated, the CSP shall produce a CSP-generated hash or hashes, using the algorithms defined in clause A.3.4 and the meta-data from clause A.3.5. Clause A.3.6 specifies how the Evidence Data and hashes can be associated The CSP shall then store information as described in clause A.3.7. Deletion of the Evidence Data occurs in accordance with the relevant record retention policy (which may be different to the retention policy for the CSP-generated hash) and is out of scope of the present document. There is no need (from the point of view of the present document) for the Evidence Data to be retained by the CSP once it is known to be successfully delivered.

A.3.3.1.2 Retrieval of a hash for a given piece of Evidence Data

The CSP shall respond promptly to requests for verifying the existence of a hash. A hash shall be submitted to the CSP, and the CSP shall respond with "yes" if the hash is present in its hash store (see clause A.3.7) and "no" if it is not. The method by which this occurs shall be in accordance with national processes - for example manually (email, in writing) or via automated services.

A.3.3.2 Process at any LEA systems handling the Evidence Data

Wherever the LEA stores the Evidence Data, the hashes should be stored with it, maintaining the association as listed in clause A.3.6.

A.3.3.3 Process for use in legal proceedings

Initial checks: As soon as it is clear that the Evidence Data will be used in evidence, the following checks should be performed:

1) Calculate the hash(es) of the Evidence Data.

NOTE: Various web site provide freely-available software for on-line or off-line hash checking, though the present document does not warrant the accuracy of any particular software.

2) Check that the calculated hashes match the hashes associated with the Evidence Data.

3) Check at least one of the hashes for the Evidence Data with the CSP in accordance with clause A.3.3.1.2.

Use in legal proceedings: If the integrity of the Evidence Data is challenged or questioned in legal proceedings, in some contexts it may be beneficial to note the process that has been followed to create hashes of this material at the point at which the request was answered (e.g. a reference to the present document and any appropriate national standard could be given).

If further corroboration is required, the hash of the Evidence Data may be calculated and checked with the CSP in accordance with clause A.3.3.1.2 via an appropriately secure process or interface. National processes will determine which type of check is acceptable (e.g. an on-line or automated check and/or a CSP provides a response manually).