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 5

Foreword 5

Modal verbs terminology 5

1 Scope 6

2 References 6
2.1 Normative references 6
2.2 Informative references 6

3 Definition of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7

4 Structure of document and list of relevant interfaces 7
4.1 Introduction 7
4.2 List of LI and RD items covered in the present document 8

5 Common techniques 8
5.1 Introduction 8
5.2 Hash algorithms 8

Annex A (normative): Providing assurance for LI or RD material as evidence 9

A.1 Statement of problem 9

A.2 Techniques for providing assurance for LI or RD material as evidence 9
A.2.1 How to use the present document 9
A.2.2 Types of technique 10
A.2.3 Techniques in the present document 10

A.3 Detailed definition for hash-only technique in the context of Retained Data 10
A.3.1 Summary 10
A.3.2 Terminology used in clause A.3 10
A.3.3 Processes and testing 11
A.3.3.1 Process at CSP 11
A.3.3.1.1 Creation of response 11
A.3.3.1.2 Retrieval of a hash for a given piece of Evidence Data 11
A.3.3.2 Process at any LEA systems handling the Evidence Data 11
A.3.3.3 Process for use in legal proceedings 11
A.3.3.4 Recommended testing and assurance process at LEA Receiver 12
A.3.4 Choice of hashing algorithms 12
A.3.5 Meta-data required 12
A.3.5.1 Mandatory details 12
A.3.5.2 Additional details 12
A.3.6 Associating hashes with the Evidence Data 13
A.3.7 Storing information at the CSP 13
A.3.8 Other notes 13
A.3.9 Use with CSP proxy 14
A.3.9.1 Definition 14
A.3.9.2 Steps between the CSP and the CSP proxy 14
A.3.9.3 CSP proxy meta-data 14
A.3.9.4 Involvement of LEA in CSP proxies 14
A.3.9.4.1 Additional assurance 14
A.3.9.4.2 Example of an additional assurance process 15
A.3.9.5 Additional use for clause A.3.9 15

Annex B (informative): Security issues for global, third-party or virtualized functionality for Retained Data functionality 16

B.1 Introduction 16

B.2 Reference model and recommendations for Retained Data 16
B.2.1 Introduction 16
B.2.2 Reference models/use cases 16
B.2.3 Approaches to meeting the challenges 19
B.2.3.0 Introduction 19
B.2.3.1 Principle 1: Data in transit protection 20
B.2.3.2 Principle 2: Asset protection and resilience 20
B.2.3.3 Principle 3: Separation between consumers 20
B.2.3.4 Principle 4: Governance framework 21
B.2.3.5 Principle 5: Operational security 21
B.2.3.6 Principle 6: Personnel security 21
B.2.3.7 Principle 7: Secure development 22
B.2.3.8 Principle 8: Supply chain security 22
B.2.3.9 Principle 9: Secure consumer management 22
B.2.3.10 Principle 10: Identity and authentication 22
B.2.3.11 Principle 11: External interface protection 23
B.2.3.12 Principle 12: Secure service administration 23
B.2.3.13 Principle 13: Audit information provision to consumers 23
B.2.3.14 Principle 14: Secure use of the service by the consumer 24
B.2.3.15 Table summarizing the principles 24
B.2.4 Other recommendations for virtualized or globalized Retained Data 25
B.2.4.0 Introduction 25
B.2.4.1 Location information 25
B.2.4.2 Times and storage 25
B.2.4.3 Logs, audit and records for evidence 25

Annex C (informative): Change History 26

History 27

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).

A.3.3.4 Recommended testing and assurance process at LEA Receiver

The recipient (LEA Receiver, the first point on the LEA side to receive the RD) should store and test the hashes as described in this clause. The functionality in this clause is not a mandatory part of demonstrating assurance of material used in legal proceedings.

Receiving a response: Immediately on receiving the Evidence Data, the LEA Receiver should check that the hashes of the Evidence Data are correct (i.e. take the hashes of the Evidence Data and check they are the same as the hashes supplied) and check that the required information (see clause A.3.5) is present and correct (or, if it is not possible to check it is correct, it should be checked that it is formatted correctly and is not obviously wrong). If there are any problems (e.g. hash does not match), the CSP should be contacted immediately. Unless the problem is immediately and clearly resolvable in a way that is not open to doubt, then the request should be discarded and a new request submitted.

Storage: The LEA Receiver should store the data as listed in clause A.3.5.1 (but not necessarily the Evidence Data) at the point at which the Evidence Data is received. This is in addition to forwarding all the data (including the Evidence Data) elsewhere.

Test function: The LEA should perform a regular test of the relevant procedures system. This should be done using the appropriate representative interfaces. The LEA should pick certain records (e.g. an item at random from each CSP) and check all the hashes for the record with the CSP in accordance with clause A.3.3.1.2.

A.3.4 Choice of hashing algorithms

The hashing algorithms used shall be SHA-256 and SHA-512 as defined in clause 5.2.

Hashes shall be generated with both algorithms.

A.3.5 Meta-data required

A.3.5.1 Mandatory details

The following details shall be present within the Evidence Data (examples are given in italics for systems using ETSI TS 102 657 [i.1]):

1) Identity of requesting agency (e.g. "AuthorisedOrganisationCode" from ETSI TS 102 657 [i.1]).

2) Identity of CSP *(e.g. "CSPID").*

3) The time (including time-zone) taken immediately before the hash is created.

4) An unpredictable number (in the range 0 to 2^{128}-1) generated in a cryptographically random way by the CSP immediately prior to creating the hash.

A.3.5.2 Additional details

The following details should be present within the Evidence Data (examples are given in italics for systems using ETSI TS 102 657 [i.1]):

1) the details of the request that was sent to the CSP, in particular, the request parameters *(e.g. "RequestMessage")*; and

2) a statement about the purpose and intention of making and storing the hash[es]. The following text is suggested:

   - hashing was performed on this material at the point at which the request was answered by <<insert CSP name>> in accordance with ETSI TS 103 307 <<version x>>.

It is necessary that the information in clause A.3.5 can be extracted from the Evidence Data in a clear, consistent, unambiguous way. Where human-readable formats are being used, any information present shall be clearly labelled. Where machine-readable formats are used, any information present shall be marked with unambiguous tags against a published format with version control and care shall be taken to ensure fields are understandable in an unambiguous way (*e.g. data expressed in accordance with ETSI TS 102 657 [i.1] is a way to meet this criterion*).

A.3.6 Associating hashes with the Evidence Data

The hashes should be linked with the Evidence Data as they are delivered to the LEA, and they should continue to be closely linked as they are used and further forwarded across LEA systems. If the hashes are kept with the evidence, the LEA can make pre-trial checks that the hashes will be validated when they are to be relied upon in legal proceedings.

The following methods for associating hashes with the Evidence Data may be used:

1) Association through file naming convention. The hashes are stored in files that have a filename with a clear and unique correlation to the filename of the Evidence Data.

2) Use a container (AsiC container (ETSI TS 102 918 [i.3]) or zip) to associate the hashes with the Evidence Data. The container should be compatible with other systems e.g. that zip files can pass through all LEA firewalls.

3) Storing the hash(es) as a field within the Evidence Data (for example XML techniques are possible within a standard such as ETSI TS 102 657 [i.1] to include hashes within the same XML structure as the Evidence Data).

A.3.7 Storing information at the CSP

The CSP shall maintain a store of every hash produced in clause A.3.3.1.1 in accordance with the relevant local retention policy.

The CSP may store additional information e.g. identity of requesting agency, identity of CSP (name of CSP at the time the evidence data was created), a request number for the request, and/or the time the hashes were created and applied. Note that such information is typically required by national processes (e.g. for audit) but this is out of scope of the present document.

Appropriate steps shall be taken to ensure the integrity of this store is not compromised. These are to be defined on a national basis and may include the following techniques:

1) the integrity may be assured by adopting processes or procedures which have been defined nationally for other similar functions (e.g. those used for other secure government functions such as practices for dedicated RD data stores or Lawful Interception storage or audit);

2) the integrity assurance may be performed using cryptographic techniques such as hash chaining or Merkle Tree Hashing (the details of this are out of scope of the present document); or

3) other techniques as specified nationally.

The data shall be stored for as long as is required by national laws, relevant regulations and best practice.

A.3.8 Other notes

Use across national boundaries: From a technical point of view, there is no aspect of the present document which relies upon the CSP being in the same country as the LEA. Any legal and procedural aspects to this are out of scope of the present document.

A.3.9 Use with CSP proxy

A.3.9.1 Definition

This clause is used for situations in which assurance is required but the CSP itself is not performing the processes in clauses A.3.2 to A.3.8. This clause may also be used for the situation described in clause A.3.9.5.

A CSP proxy is defined to be a function which receives data from the CSP and performs hashing on behalf of the CSP.

When using a CSP proxy, the CSP proxy shall perform all of the functions assigned to the CSP in clauses A.3.3.1, A.3.3.3 and A.3.7.

When using a CSP proxy, the meta-data shall follow clause A.3.9.3 (instead of clause A.3.5).

A.3.9.2 Steps between the CSP and the CSP proxy

The CSP proxy should sit as early as possible in the processing chain i.e. the number of steps and processes that the data goes through (after leaving the CSP and before being handled by the CSP proxy) should be minimized.

The steps (between CSP and CSP proxy) should be listed and the design details of these steps should be made available, so that any associated risks can be examined and considered during legal proceedings.

The steps should consist mainly or entirely of steps to interpret basic transport and security protocols. These steps should be performed using tested, off-the-shelf software where practical.

Where appropriate, the transport or delivery protocols used for the step from the CSP to the CSP proxy should be chosen so that they give integrity protection (e.g. a transport protocol with integrity protection).

A.3.9.3 CSP proxy meta-data

The CSP proxy shall ensure that the information in clause A.3.5.1 is present in the material that it produces. It is interpreted as follows:

- The CSP proxy shall ensure that the identity of the requesting agency and CSP are present. If they were not present in the material from the CSP, then the CSP proxy shall be able to demonstrate how it attached this information with confidence that it was correct.
- A timestamp as defined in clause A.3.5.1.
- An unpredictable number created by the CSP proxy (as per clause A.3.5.1).

Regarding the information listed in clause A.3.5.2:

- The request details may be added by the CSP proxy if it reliably knows them, but shall not be included if it does not reliably know them.
- A statement may be added by CSP proxy. For a proxy the following text is suggested: "Hashing was performed on this material by <<insert organisation name>> in accordance with ETSI TS 103 307 <<version x>>".

A.3.9.4 Involvement of LEA in CSP proxies

A.3.9.4.1 Additional assurance

The CSP proxy may be run or managed by the LEA. If so, there shall be an additional process put in place to give additional assurance of the integrity of the CSP proxy hash store. An example of a process which fulfils this criterion is the process given in clause A.3.9.4.2, though others may be used.

A.3.9.4.2 Example of an additional assurance process

The following process may be used when a CSP proxy is run or managed by the LEA. This process is considered sufficient to meet the requirement of "additional assurance" as defined in clause A.3.9.4.1:

- Every week the CSP proxy creates a list-of-hashes document including all the hashes that the CSP proxy has produced during the last week. Additional random hashes may be added where there is a reason to do so (e.g. for disguising the number of requests that went through the system). The list-of-hashes document contains the previous week's hash as its first entry (except for the first week it is functioning).
- The CSP proxy hashes the list-of-hashes document using the hashes as defined in clause A.3.4, to create the "weekly hash".
- The CSP proxy uses at least one of the following ways to store the "weekly hash". The CSP proxy should use two ways where practical:
  - With a commercially-offered assurance service independent of the CSP proxy.
  - By publishing the hash in a way which can be checked by members of the public e.g. social media or in a published print journal. Some social media channels are potentially ephemeral (might be not stable for 5-10 years) and if so, more than one channel should be used. Print journals held by major libraries would give a level high confidence even if used without other channels.
  - Using a trusted timestamping service (as defined in IETF RFC 3161 [i.7]).
- If a hash (that has been stored by the CSP proxy) is challenged, if required, the list-of-hashes document for the week in question is produced by the CSP proxy. It can be checked that the relevant hash is present in that document. The hash (of the list-of-hashes document) can be taken and checked against the published hash.

A.3.9.5 Additional use for clause A.3.9

The details in clause A.3.9 may also be used for the following situation:

- A situation in which 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.

In this situation, a new set of "Evidence Data" shall be created by the CSP proxy and shall include:

- The material sent by the CSP, including:
  - the data sent by the CSP, including any meta-data sent by the CSP (such as a timestamp, if present);
  - the hash sent by the CSP.
- A set of meta-data as per clause A.3.9.3 (in addition to any meta-data provided by the CSP).

Annex B (informative): Security issues for global, third-party or virtualized functionality for Retained Data functionality

B.1 Introduction

The present annex provides recommendations for the provision of Retained Data through global, virtualized or third party functionality. Specifically it handles the provision of Retained Data storage and query (but not the collection of data).

Recommendations relating specifically to Network Functions Virtualisation (NFV) are covered in ETSI GS NFV-SEC 010 [i.6] and other standards from ETSI ISG NFV-SEC.

This is a technical evaluation and not a legal evaluation.

NOTE: Legal consideration has been given by the European Court of Justice, for example about locations of collection and/or retention of material.

The treatment of third-party or virtualized provision of LI (e.g. management and mediation) is out of scope for the present document but will be handled in a future version.

B.2 Reference model and recommendations for Retained Data

B.2.1 Introduction

This clause examines security concerns around global, virtualized Retained Data provision, including in the context where the provision is made through Third Parties.

There is a set of security concerns around RD which are well-understood and are not the scope of the present document. These are: security concerns which arise from providing functionality to respond to RD requests which are not international (i.e. requesting organization, CSP, subject of interest and data store all are in the same country) using software owned and managed by the CSP from a known and fixed set of locations (i.e. not a "cloud" or "virtual" environment) and only a small number of locations (e.g. main plus backup).

The following situations introduce additional security challenges:

- International components in terms of the business store of data being queried versus the requesting agency.
- Virtualized components e.g. the business store of data is subject to virtualisation (potentially internationally) or dedicated RD functionality is provided over a virtualized infrastructure.
- Third-Party suppliers can also play an important role. In simple situations then, provided the CSP takes ownership and responsibility for the Third-Party functionality, there are no new issues. However, if the Third Party is part of a virtualized or international approach then further concerns can arise.

A detailed threat model examining threat actors and their capabilities is out of scope of the present document and would need to be handled on a national basis.

B.2.2 Reference models/use cases

The shading in figures B.1 to B.8 is used to indicate components which are in different countries: one country is shown in solid yellow shading; where there are components in a different country, this is shown using hashed green shading.

A. Basic scenario

This is the basic scenario. Security concerns with this approach are not addressed in the present document.

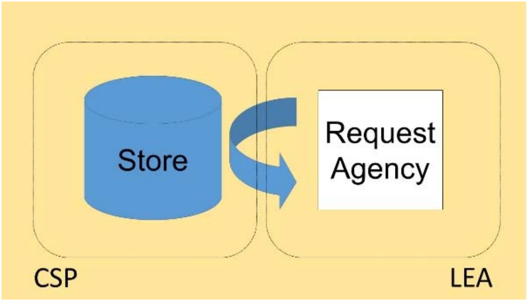

Figure B.1

B. Basic situation with international management

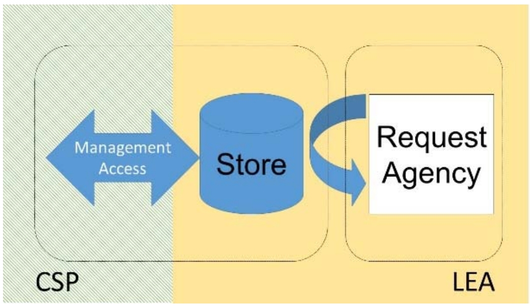

Figure B.2

Extra concerns can relate to the nationality of those who have management or oversight privileges relating to the Retained Data store.

C. Pass the request to the LEA in the country in which the data resides

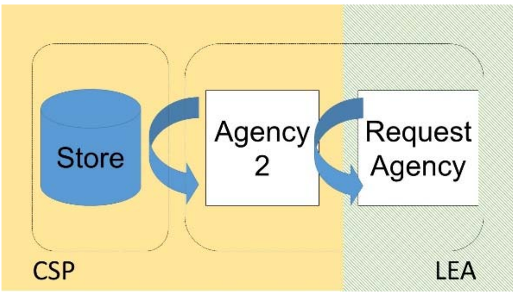

Figure B.3

There can be legal or operational reasons why this is not an appropriate route, e.g. Agency 2 to consider whether this is an appropriate request according to their own legislation and practices.

D. Copy of all relevant documents to in-country storage

In this scenario, the underlying business store of data is held abroad, but a copy of all relevant data is made to an in-country store.

Challenges: There will be a legal issue to decide which records are relevant to that country (out of scope for the present document). Otherwise this is similar to situation A.

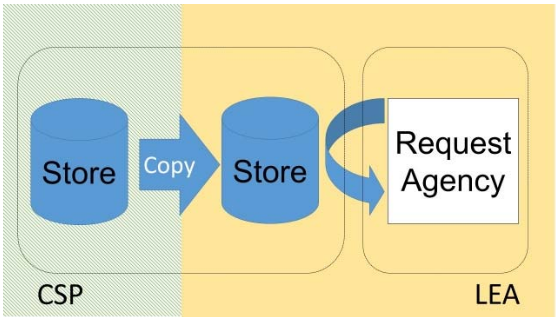

Figure B.4

E. Application layer request relay

In this scenario, a stateful relay manages requests and request acknowledgements etc. and could perform some basic checks if appropriate.

Challenges: The main challenge concerns the handling and storage of request parameters in the second country.

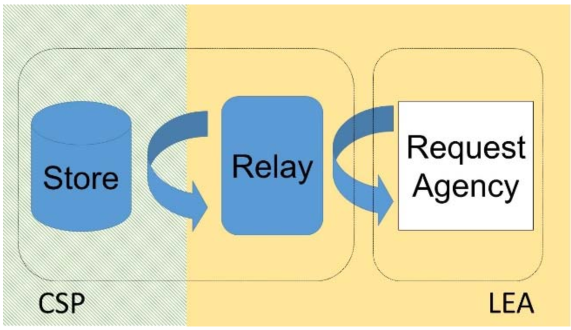

Figure B.5

F. Low-layer transport proxy

I.e. stateless proxy delivers requests/replies transparently. No checking or management of requests or responses is performed by the low-level (e.g. HTTP) proxy.

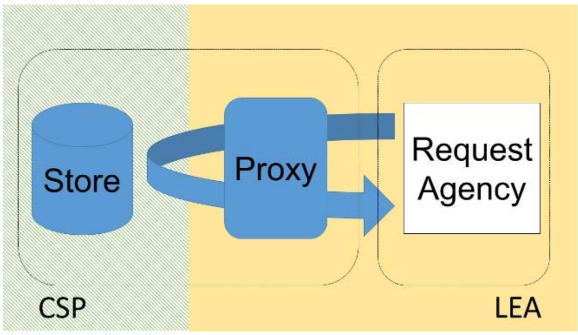

Figure B.6

G. One-country virtualized LEA function

This situation is where a CSP meets RD requirements using functionality which is virtualized but remains within a single country. This covers two situations: where the CSP holds a dedicated store of RD specifically for RD purposes (which can be virtualized) or where the CSP is querying its main stores of business data (which are virtualized).

Challenges: Provision of security in handling the request and protection of the identity involved.

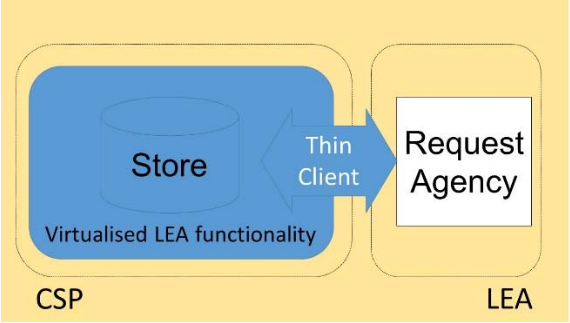

Figure B.7

H. International virtualized LEA function

As G, except that the virtualized functionality resides in a different country from the requesting agency.

Challenges: All of the challenges from A to G apply, as well as a range of legal considerations (out of scope of the present document).

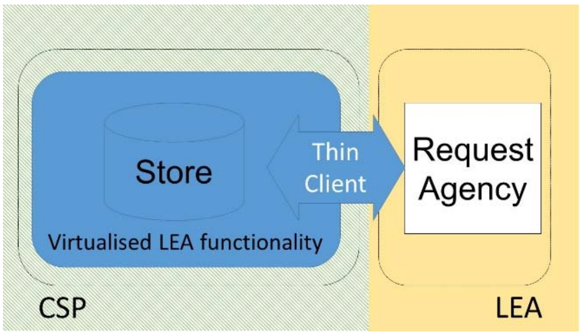

Figure B.8

I. International multi-CSP virtualized LEA function

As H, except that the store of information is combined across a number of different CSPs, either by one of those CSPs or by a third-party provider.

Challenges: All of the challenges of H apply. Also there is potentially an increase in risk due to the number and amount of requests which are present. There is a risk that people with privileges from one CSP (e.g. to see requests/responses) could get access to cross-CSP data. The "multi-CSP" approach can be added to many of the options A-G. The third-party approach can also be added to many of the options A-G.

B.2.3 Approaches to meeting the challenges

B.2.3.0 Introduction

The present document examines a number of security principles and frameworks and looks at them in the context of the challenges and use cases outlined above.

The present document considers ***CESG guidance - implementing the Cloud Security principles [i.4].*** Each principle is treated as follows:

1) The principle is stated (with the heading "Statement of the principle", copied from the original document).

2) The present document derives some recommendations from the principle (under the heading "recommendations").

The principles refer to "consumers" and "consumer data": the present document considers these phrases from two angles: firstly, the consumers as the customers of the CSP, secondly consumers as the end users of the RD i.e. the LEA.

The "service provider" is considered to be the owner or provider of the RD functionality (i.e. the CSP, or a third-party provider, or the LEA for any aspects of provision of the functionality provided by the LEA).

B.2.3.1 Principle 1: Data in transit protection

Statement of principle (see [i.4]): Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.

Recommendation: It is assumed that considerations from situation A (basic model) are already well-understood. Other recommendations:

- Situation B and others: Any situations involving international management functions should have protection for delivery of any management statistics or audit logs. Personal data should not be sent over the interfaces to the international management.

- Situations C, E, F and H, all involve personal data being sent over interfaces over international boundaries. Extra care should be taken in these situations (e.g. understanding of network protection on both sides of the boundaries, also key management or delivery for encryption to be coordinated internationally).

- "Multi-CSP" or "Third-party" approaches will increase the number of interfaces, and in particular will add interfaces which are between CSPs or with a new party (i.e. it will increase the number of external interfaces). These should be specified and tested accurately and agreed by all parties.

B.2.3.2 Principle 2: Asset protection and resilience

Statement of principle: Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

Recommendations: As with principle 1, it is assumed that Recommendations from basic situation A are already adequately handled:

- For C, E, F and H: The storage of sensitive or personal information should be avoided on systems which are not in-country (see clause B.2.4.3).

- For G and H (including "Multi-CSP" or "Third-party" approaches), controls for asset protection and resilience should be in line with Cloud Security Guidance [i.4].

B.2.3.3 Principle 3: Separation between consumers

Statement of principle: Separation between different consumers of the service prevents one malicious or compromised consumer from affecting the service or data of another.

Recommendation:

- In situations C, E, F and H, care should be taken so LEA users from one jurisdiction cannot see information relating to another. In some ways this is similar to the requirement within one jurisdiction that different Law Enforcement Agencies cannot see another's information. However, the possibility of hostile attack can be stronger when agencies from multiple jurisdictions are involved.

- "Multi-CSP" or "Third-party" approaches require care that there is separation between providers of data as well as between consumers. CSP representatives who have supervisory privileges for their own CSP's data should not get those privileges for all data. The privileges for those users who can see all CSPs data should be kept limited to those which are strictly necessary and the number of users with those privileges should be minimized.

B.2.3.4 Principle 4: Governance framework

Statement of principle: The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

Recommendation:

- The governance framework in place for CSPs for the basic situation A should be re-evaluated in the light of the new concerns from international or virtual providers.

- The named senior representative for security should be made aware of all jurisdictions which are involved in the RD and all regulatory requirements from those jurisdictions.

- Where third party providers are being used, this should be acknowledged at senior level at both the CSP and the third party organization, noting that the CSP requirements are unchanged with regards to security, even if this is via a third-party organization.

B.2.3.5 Principle 5: Operational security

Statement of principle: The service provider should have processes and procedures in place to ensure the operational security of the service. The service will need to be operated and managed securely in order to impede, detect or prevent attacks against it. The aspects to consider comprise:

- *Configuration and change management - ensuring that changes to the system do not unexpectedly alter security properties and have been properly tested and authorized.*

- *Vulnerability management - ensuring that security issues in constituent components are identified and mitigated.*

- *Protective monitoring - taking measures to detect attacks and unauthorised activity on the service.*

- *Incident management - ensuring the service can respond to incidents and recover a secure available service.*

Recommendation:

- Each additional interface or component should be assessed in line with "vulnerability management".

NOTE: Situation E provides fewer extra vulnerabilities than situation F provided it is implemented properly.

- Under G and H, the LEA should determine how material is to be extracted from the Thin Client system and take appropriate steps to check this material before forwarding it to onward systems.

- Protective monitoring systems should cover the system as a whole e.g. situations such as D and E need multi-national coordination of protective monitoring and reporting. Third-party providers should have their own protective monitoring and should also provide reports or audits to the CSPs they are representing.

B.2.3.6 Principle 6: Personnel security

Statement of principle: Service provider staff should be subject to personnel security screening and security education for their role. Personnel within a cloud service provider with access to consumer data and systems need to be trustworthy. Service providers need to make clear how they screen and manage personnel within any privileged roles. Personnel in those roles should understand their responsibilities and receive regular security training. More thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise of consumer data by service provider personnel.

Recommendation:

- Under B, the international management staff should not have access to sensitive information.

- Under E, F and G: Personnel vetting and security should be carried out against each jurisdiction's procedures as CSP staff have access to sensitive material from all the jurisdictions involved. An arrangement where countries trusted each other's vetting may help reduce the burden for CSPs, though this should not be at the expense of national security.

- Under G and H, personnel security training at CSP and LEA should be updated to note new security recommendations from virtualized or thin-client arrangements.

- For "Multi-CSP" or "Third-party" approaches, Third Party staff should be cleared for all the material they might access. In general the number of roles which have super-user privileges across many CSPs or many countries should be minimized.

B.2.3.7 Principle 7: Secure development

Statement of principle: Services should be designed and developed to identify and mitigate threats to their security. Services which are not designed securely may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.

Recommendation: In general there are no specific additional concerns here. Developers of systems based on virtualisation should be trained in the specific security development techniques relevant to virtualized systems.

B.2.3.8 Principle 8: Supply chain security

Statement of principle: The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement. Cloud services often rely upon third party products and services. Those third parties can have an impact on the overall security of the services. If this principle is not implemented then it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

Recommendation:

- This principle applies to all the scenarios.

- Third-party providers should pay particular attention.

B.2.3.9 Principle 9: Secure consumer management

Statement of principle: Consumers should be provided with the tools required to help them securely manage their service. Management interfaces and procedures are a vital security barrier in preventing unauthorised people accessing and altering consumers' resources, applications and data. The aspects to consider comprise:

- *Authentication of consumers to management interfaces and within support channels.*

- *Separation and access control within management interfaces.*

Recommendation:

- This principle applies to all scenarios.

- If LEAs are being presented with new types of interfaces or ways to access their data (e.g. G and H) then specific training should be provided.

- For scenario C, very specific training should be set up for all LEA users involved; a specific subset of LEA staff should be selected to perform requests in this way and appropriate training and management should be in place for these situations.

- Specific new training may be required where more than one CSP's information can be obtained from the same route.

B.2.3.10 Principle 10: Identity and authentication

Statement of principle: Consumer and service provider access to all service interfaces should be constrained to authenticated and authorized individuals. All cloud services will have some requirement to identify and authenticate users wishing to access service interfaces. Weak authentication or access control may allow unauthorised changes to a consumer's service, theft or modification of data, or denial of service. It is also important that authentication occurs over secure channels. Use of insecure channels such as email, HTTP or telephone can be more vulnerable to interception or social engineering attacks.

Recommendation:

- Situation C involves more complex identity and authentication processes. Specially identified and trained staff should be used.
- Situations E and F involve a single CSP store authenticating identities from a range of countries. In these cases, insecure channels, which were vulnerable to social engineering attacks even where informal routes had been used in-country in the past, should be avoided.

B.2.3.11 Principle 11: External interface protection

Statement of principle: All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them. If an interface is exposed to consumers or outsiders and it is not sufficiently robust, then it could be subverted by attackers in order to gain access to the service or data within it. If the interfaces exposed include private interfaces (such as management interfaces) then the impact may be more significant. Consumers can use different models to connect to cloud services which expose their enterprise systems to varying levels of risk.

Recommendation:

- The international interface in situation B (international management) is an important interface to limit and secure. This interface should not convey any personal or sensitive data.
- The copy interface in situation D should be restricted to a one-way flow of the required information only.
- Situations E and F involve a wider range of users accessing the data store but the interface is in theory the same as situation D.
- Situations G and H have an interface which is different from standard RD interfaces but not inherently more insecure. "Multi-CSP" or "Third-party" approaches have new external interfaces between new organizations. These should be specified and tested carefully and regularly.

B.2.3.12 Principle 12: Secure service administration

Statement of principle: The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. The security of a cloud service is closely tied to the security of the service provider's administration systems. Access to service administration systems gives an attacker high levels of privilege and the ability to affect the security of the service. Therefore the design, implementation and management of administration systems should reflect their higher value to an attacker. A service administration network is a specialized form of enterprise network. There are a wide range of options for how this can be designed, delivered, managed and secured. It is expected that standard enterprise good practice be followed in the design and operation of these systems, but at a level reflecting their higher value. The service management systems are likely to have the most privileged access to the internals of the service. Compromise of them would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

Recommendation:

- Situations E, F and H have sensitive information from a range of different jurisdictions in the same place, so the strongest consideration should be given to these elements.
- Under situation B service administration should be performed locally wherever possible.
- "Multi-CSP" or "Third-party" approaches can provide a particularly high value to an attacker and should be handled accordingly.

B.2.3.13 Principle 13: Audit information provision to consumers

Statement of principle: Consumers should be provided with the audit records they need to monitor access to their service and the data held within it. The type of audit information available to consumers will have a direct impact on their ability to detect and respond to inappropriate or malicious usage of their service or data within reasonable timescales.

Recommendation: The maintenance of accurate audit logs is a key part of providing RD functionality, from the point of view of audit in terms of the LEA itself but also from the independent bodies who monitor and check on RD. The following recommendations apply:

- Under situation C there should be very careful audit and accountability, with each stage able to account for their actions under the appropriate legislations.
- Under situations G and H, each individual request or response message should be logged and accounted for, even though this interface is in effect "internal" to the system providing the RD.
- "Multi-CSP" or "Third-party" approaches should have audit systems which are appropriate to each of the different CSPs involved.

B.2.3.14 Principle 14: Secure use of the service by the consumer

Statement of principle: Consumers have certain responsibilities when using a cloud service in order for their use of it to remain secure, and for their data to be adequately protected.

Recommendation:

- In the typical scenario (situation A), it is assumed that the requesting agency system is a tightly-controlled and well-managed network.
- Most of the remaining situations do not introduce new pressures or requirements on the agency systems.
- In scenarios G and H, there may be a variety of LEA systems used to access the virtualized LEA function. In these cases, principle 14 should be examined in more detail.

B.2.3.15 Table summarizing the principles

Table B.1

	A	B	C	D	E	F	G	H	multiCSP	3rdparty
Principle 1	~	<>	X	<>	X	X	<>	X	X	X
Principle 2	~	~	<>	~	<>	<>	~	<>	<>	<>
Principle 3	~	~	<>	~	<>	<>	~	<>	X	X
Principle 4	~	<>	<>	<>	<>	<>	<>	X	X	X
Principle 5	~	~	~	<>	<>	~	<>	<>	<>	<>
Principle 6	~	<>	~	~	<>	<>	<>	<>	<>	<>
Principle 7	~	~	~	~	~	~	~	~	~	~
Principle 8	~	~	~	~	~	~	~	~	~	<>
Principle 9	~	~	<>	~	~	~	~	~	<>	~
Principle 10	~	~	<>	~	<>	<>	<>	<>	<>	<>
Principle 11	~	<>	~	<>	<>	<>	<>	<>	<>	<>
Principle 12	~	<>	~	~	<>	<>	~	<>	X	X
Principle 13	~	~	<>	~	~	~	<>	<>	<>	<>
Principle 14	~	~	~	~	~	~	<>	<>	<>	<>

Key:

~ Means that this principle should be kept in mind and there are no new recommendations beyond those which apply to the basic situation (i.e. situation A).

<> Means that this principle should be addressed specifically as there are likely to be some concerns to address.

X Means that this principle is likely to present critical issues which will need to be reflected in key design and will need to be tested and monitored carefully.

B.2.4 Other recommendations for virtualized or globalized Retained Data

B.2.4.0 Introduction

The present document does not present legal requirements for Retained Data. In order to meet typical legal requirements (such as ETSI TS 102 656 [i.5]) in an environment where CSPs are handling services on a global basis, the following information provides recommendations to help support existing requirements.

B.2.4.1 Location information

In order to support typical requirements for Retained Data (such as ETSI TS 102 656 [i.5]), the present document makes the following recommendations:

- The location of activities and stages of the Retained Data process (collection, storage, query and delivery) should be recorded.
- The collection and storage locations should be recorded for each record in the store.
- The location of query and delivery functions should be noted for each request/response made.

B.2.4.2 Times and storage

In order to support typical requirements for Retained Data (such as ETSI TS 102 656 [i.5]), the present document makes the following recommendations:

- The times throughout the processes involved in RD should be recorded e.g. consider recording the time the event took place, time of collection of record, time request received, time response delivered. Times should have a time zone associated.

B.2.4.3 Logs, audit and records for evidence

Wherever possible, all logs, management information, audit information or records for assuring material in evidence should avoid containing personal data (e.g. the identity of the subject of interest of the request). For assuring material in evidence, signatures or hashes should be used (see annex A).

Annex C (informative): Change History

Date	Version	Information about changes
February 2018	1.3.1	Update based on experience of testing clause A.3
June 2021	1.4.1	Update to include clause A.3.9 for CSP proxies

History

Document history		
V1.1.1	April 2016	Publication
V1.2.1	October 2016	Publication
V1.3.1	April 2018	Publication
V1.4.1	June 2021	Publication