



Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements

*iTeh Standards PREVIEW
(standards.iteh.ai)
Full standards list: <https://standards.iteh.ai/catalog/standards/sist/b7b348ac-5959-433b-a62f-a105255df2d9/etsi-gs-nfv-sec-010-v1.1.1-2016-04>*

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/NFV-SEC010

Keywords

accessibility, privacy, retained data, safety,
security, usability

ETSI

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

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

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

Important notice

The present document can be downloaded from:

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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>

Copyright Notification

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

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

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

© European Telecommunications Standards Institute 2016.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definitions and abbreviations.....	5
3.1 Definitions.....	5
3.2 Abbreviations	6
4 Introduction to Retained Data	6
4.1 Legal basis and definition.....	6
4.2 Reference model.....	6
4.3 Stages of the RD process.....	7
5 NFV Retained Data problem statement.....	7
5.1 Overview	7
5.2 Data collection integrity and completeness	7
5.3 Multiple jurisdictions for storage and querying of data.....	8
5.4 Assurance of evidence for Retained Data.....	8
5.5 Confidentiality of Retained Data requests and responses.....	8
5.6 Retained Data logs and audit.....	9
5.7 Retained Data availability and timeliness	9
6 Available measures for meeting NFV Retained Data problem set.....	9
6.1 Introduction and core approach	9
6.2 Secure Logging	10
6.3 Access control, physical/personnel controls and alarms	10
6.4 Post-incident analysis	10
6.5 Policies for workload placement	10
6.6 Communications Security	11
6.7 Measured or secured boot.....	11
6.8 Attestation, Trusted Platform Modules and Hardware-Mediated Execution Enclaves	11
6.9 Memory inspection as an attack vector.	11
History	12

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

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.

ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/b77444ec-5959-433b-a62f-a105255df2d9/etsi-gs-nfv-sec-010-v1.1.1>
2016-04

1 Scope

The purpose of the present document is to provide a problem statement and articulate the requirements for NFV Retained Data. The present document examines the core underlying requirements for Retained Data such as those presented by ETSI TC LI (ETSI TS 102 656 [i.2] and ETSI TS 102 657 [i.3]). The present document aims to identify solutions or mitigations to the problems identified.

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.

Not applicable.

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 GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".
- [i.2] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".
- [i.3] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".
- [i.4] ETSI TS 103 307: "CYBER; Security Aspects for LI and RD Interfaces".

3 Definitions and abbreviations

3.1 Definitions

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

Communication Service Provider (CSP): organisations who are obliged by law to provide Retained Data functionality

jurisdiction: physical or virtual location subject to the authority of the LEA requesting access to retained data

Law Enforcement Agency (LEA): organization authorized by a lawful authorization based on a national law to make requests for Retained Data Functionality or receive the results of it

3.2 Abbreviations

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

CSP	Communication Service Provider
HI	Handover Interface
HI-A	Handover Interface-A (used for administration and requesting of RD)
HI-B	Handover Interface-B (used for transmission of RD material)
LEA	Law Enforcement Agency
NFV	Network Functions Virtualisation
RD	Retained Data

4 Introduction to Retained Data

4.1 Legal basis and definition

The present document is designed to support Retained Data functionality. For the present document, "Retained Data functionality" is defined as situations in which CSPs, or their equivalent in NFV provisioning architectures, are performing the following tasks:

- 1) store data (either in their existing business stores, or in dedicated stores of data); and
- 2) at a later point, when presented with an appropriate request, make available the data that meets the request to the appropriate authority.

The present document is not a legal document. It does not define when or whether these tasks should take place, nor does it define what counts as an appropriate request or appropriate authority. The definition of what is or is not a "Communications Service Provider" (from the point of view of Retained Data) is out of scope. It is a pre-requisite to the present document that Retained Data functionality is in line with appropriate and relevant legislation on privacy and data protection.

The term "Data" in the present document is used to describe information which is collected, stored or queried as part of Retained Data functionality.

NOTE: In some jurisdictions, Retained Data may include "customer or subscriber data" (i.e. records with information about the customer (e.g. name, address) and their subscription) and "usage data" (i.e. records describing how the service was used). This note is included for background information but is not a definition.

4.2 Reference model

Baseline requirements for Retained Data are provided in ETSI TS 102 656 [i.2], with specific handover requirements articulated in ETSI TS 102 657 [i.3].

The reference model is defined in ETSI TS 102 657 [i.3] and is shown in figure 1.

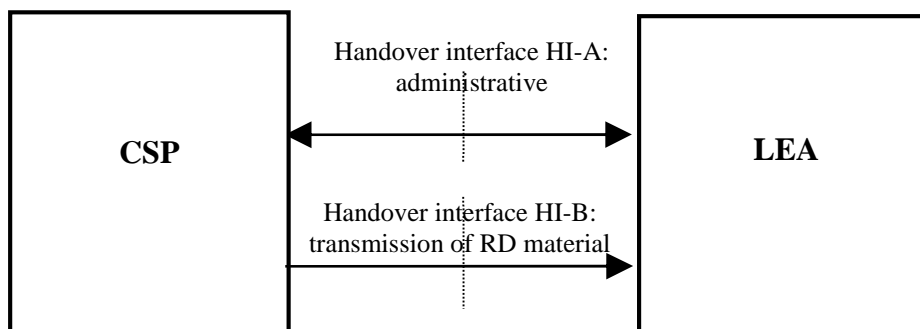


Figure 1

NOTE: In ETSI TS 102 657 [i.3], the LEA is designated as "Authorized Organisation". For compatibility with other standards, the present document uses the term LEA.

4.3 Stages of the RD process

Retained Data consists of:

- The collection of Data.
- The storage of Data.
- The querying mechanism.
- The delivery of requests and the handover of results.

The collection and storage of Data may be performed as part of ordinary business processes (with the business data being stored for longer than is necessary for business purposes only where required by appropriate legislation), or there may be a dedicated store of Data specifically for RD purposes. The querying of Data takes place specifically for RD purposes and involves matching any records in the store against the request received and returning the results.

5 NFV Retained Data problem statement

5.1 Overview

The problems listed in clause 5 are those which relate specifically to NFV. For issues relating to the services which are offered on top of an NFV architecture, then in general these are handled by the standards relating to those services (e.g. 3GPP standards).

In general the problems will come from the use of NFV in two different ways:

- Challenges arising because the underlying service is handled using an NFV architecture.
- Challenges arising because RD functionality is provided within an NFV architecture.

The present document does not cover issues relating to globalisation of CSPs in general or global/third-party provision of RD functionality. These are covered in TC CYBER ETSI TS 103 307 [i.4].

5.2 Data collection integrity and completeness

The goal is to gain an understanding of the completeness of the Data as it is collected, and any assurances that can be given about the integrity/completeness of its transmission to a Data store. In this context, integrity and completeness is used to mean that the meaning of any particular record or item has not been altered (nothing changed, added or removed) and that all records or items are present.

In general, the Data is collected for business purposes and the goal is to establish the integrity and completeness of the existing business processes. Where data collection and storage is used for business purposes, it should meet applicable standards for that purpose e.g. billing records should meet applicable billing standards.

The specific challenges relating to NFV are:

- To check that any new interfaces / delivery / transport mechanisms introduced in using NFV architectures were as robust as the non-NFV equivalents.
- To check that hypervisors do not have the ability to alter or remove data during the collection process.

5.3 Multiple jurisdictions for storage and querying of data

When Retained Data queries are being handled by a network component which is virtualised and/or the RD storage is not necessarily in the same jurisdiction as the users of the service or the agency which is making the request - which may be exacerbated in NFV architectures - additional measures may be necessary

For some CSPs it may be practical to copy all relevant Retained Data to meet jurisdictional requirements. However, this practice is inefficient and costly, and data storage is likely to be in a common multi-national location. Under these circumstances, security requirements will be critical and appropriate access controls will be essential to meet privacy and other common requirements.

The specific challenge relating to NFV is around determining the location where data is collected, stored or queried with appropriate levels of assurance. Control may be required to prevent collection or query functions moving to jurisdictions which were not compatible with national legislation. Storage may need to be enhanced to indicate the locations involved in collecting and delivering the data. Extra care should be taken if a single request is fulfilled using information from different data stores.

5.4 Assurance of evidence for Retained Data

There are the following stages to the assurance process:

- 1) Data collection integrity and completeness (see clause 5.2)
- 2) Integrity of data storage.
- 3) Accuracy and integrity of data querying.
- 4) Integrity and assuring origin of data delivery.

In general the techniques for assuring origin and data delivery are common across NFV and non-NFV architectures and are handled by ETSI TS 103 307 [i.4].

The specific challenge relating to NFV are:

- As per clause 5.2 in terms of the collection processes.
- Where storage and querying is provided over NFV, assurances that hypervisors did not have the ability to manipulate data during the storage. Attestation that querying functionality was created and run without having been manipulated.

5.5 Confidentiality of Retained Data requests and responses

This includes the following areas:

- 1) The confidentiality of the store of Retained Data.
- 2) The confidentiality of the Retained Data querying function, plus any additional requirements on the handover/delivery interfaces if they are provided through NFV infrastructures.
- 3) The confidentiality of Retained Data logs and audit trails, see clause 5.6.

The present document notes that the precautions are strongest for functions which contain the personal identifiers for people who are the subject of a Retained Data request (i.e. item 2 from the above list).

It is also required to protect the general stores of personal information (item 1 from the above list) in line with appropriate Data Protection and Privacy regulation. The confidentiality requirement for this data is equal to confidentiality requirements for all stores of personal data. However, based on the issues in clauses 5.2 and 5.4, it should be noted that integrity is important to consider, in terms of providing assurance for this material should it be used in evidence.

The specific challenges relating to NFV are:

- To handle confidentiality requirements for item 2 where querying functions are provided over NFV architectures.
- To handle the integrity requirement for data stores in relation to providing evidential assurance.

5.6 Retained Data logs and audit

For audit purposes, Retained Data systems are required to contain log files to store information as described by appropriate legislation and practices. Typically the audit information is used by the organisation which is responsible for checking that proper procedures are followed for Retained Data disclosures. Typically this information would contain:

- 1) Reference number (and other information needed to uniquely identify the request).
- 2) Time and date that the request was received.
- 3) Time and date that the request was delivered.
- 4) If needed, a hash and/or signature of the data or other material to help with assurance for use in evidence.

The following considerations apply to non-NFV systems but are particularly relevant in an NFV environment e.g. where information may be being stored in a variety of physical locations, or where hypervisor functions may have access to logs or storage.

Item 1 - Reference numbers: It is highly desirable that the "reference number" information (used to identify the request) does not include a direct reference to the name of the agency or organisation who made the request.

Items 2 and 3 - Times and dates: Times stored in a format where the time zone is clear. The accuracy of the clock should be in line with other systems used at the CSP for audit i.e. industry best practice techniques should be adopted to assure the accuracy of the system clocks.

Item 4 - Material to help assure RD used in evidence - storage of sensitive information: For systems involving virtualised components, it is strongly recommended that the material used to help with assuring evidence does not contain sensitive information such as names, address, phone numbers or other personally-identifiable information. It is recommended to use techniques such as those in ETSI TS 103 307 [i.4] which would mean that the personally-identifiable information could be deleted as soon as it has been successfully delivered. If personally-identifiable information is stored in the audit function, then security of such storage should be re-evaluated and additional techniques may be required beyond that covered in the present document.

5.7 Retained Data availability and timeliness

Retained Data is sometimes required in a threat-to-life situation. Responses are not required in real-time (e.g. < 100 ms) but it is critical that there are no long delays (e.g. no 1 minute delays).

This requirement is present in non-NFV situations however the specific challenge to NFV would be to ensure that providing storage and query functionality over NFV did not introduce unacceptable delays.

6 Available measures for meeting NFV Retained Data problem set

6.1 Introduction and core approach

The present document examines measures as described in ETSI GS NFV-SEC 009 [i.1] and then considers whether any additional measures are required in order to address the issues identified in clause 5.