ETSI GS NFV-SEC 010 V1.1.1 (2016-04)

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

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

Contents

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.

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.

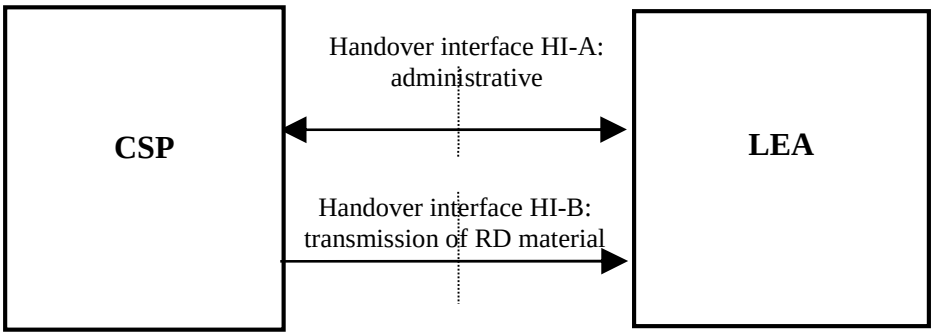

Figure 1

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.

The core to the approach is that any function involved in querying or delivering Retained Data should be treated according to the NFV architecture for the execution of sensitive components.

6.2 Secure Logging

As defined in clause 6.2 of ETSI GS NFV-SEC 009 [i.1].

Secure logging is an important feature for addressing the issues identified in clauses 5.5 and 5.6. ETSI GS NFV-SEC 009 [i.1] identifies three properties of secure logging:

1) Creation of entries which are confidential from other parties: in general steps should be taken to ensure there is no long-term requirement for confidential logging or storage of Retained Data information (i.e. the details of previous requests or responses) as described in clause 5.6.

2) Creation of entries whose integrity can be checked at the entry level. Secure logging techniques are required to help provide assurance about the integrity of the data store for material which may be used in court.

3) Creation of a chain of entries, where the chain itself can be checked for tampering or deletion. Currently no Retained Data recommendations are noted for integrity beyond item 2 in this list.

6.3 Access control, physical/personnel controls and alarms

As defined in clauses 6.3, 6.5 and 6.6 of ETSI GS NFV-SEC 009 [i.1].

In general there are extensive processes and procedures for handling physical controls and personnel controls which are in place for Retained Data according to national practices. Threat analysis in general takes place nationally against the possible threats to Retained Data systems and information. The same techniques and processes should be adopted wherever it is practical to secure infrastructure physically or through personnel checking. Where RD capability is being offered which is not linked to a hardware which can be secured physically, then the items in clause 6.8 are applicable.

6.4 Post-incident analysis

As defined in clause 6.4 of ETSI GS NFV-SEC 009 [i.1].

It is important that post-incident analysis helps identify whether any stores of material have been affected which may subsequently be used as evidence. The checks listed in clause 6.4 of [i.1] will provide a good level of assurance about the robustness of the appropriate stores of information.

6.5 Policies for workload placement

As defined in clause 6.10 of ETSI GS NFV-SEC 009 [i.1].

Workload placement is noted to include the following capabilities:

- Logical or physical network proximity to physical systems;
- The need to be sited on the same host as one or more other components.
- The need to be sited on a different host to one or more other components.
- Placement on hosting services with particular capabilities.
- Placement within particular geographic locations.

Within the context of Retained Data, the following issues can be met or partially met through workload placement:

- Issues from clause 5.3: implies workload placement to ensure that Retained Data storage and query workloads are only placed on hosting services with the appropriate security capabilities and controls.
- Issues from clause 5.3: implies workload placement to ensure that Retained Data collection, storage and query only takes place in a geographic location compatible with national legislation for Retained Data.
- Issues from clause 5.7 implies that functionality is only placed on hosting services which can meet the criteria for availability and timeliness.

6.6 Communications Security

As defined in clause 6.11 of ETSI GS NFV-SEC 009 [i.1].

This will be important in addressing a number of the issues from clause 5 of the present document:

- There is an integrity requirement on the collection of information for Retained Data storage. Typically an adequate level of assurance is that the data in the store meets applicable standards for business data.
- There is an integrity and confidentiality requirement on the delivery of information to and from the LEA (i.e. HI-A and HI-B from the reference model in clause 4 of the present document). The integrity requirement is important in providing evidential assurance of the information if it is used in court.

6.7 Measured or secured boot

See clauses 6.12 and 6.13 of ETSI GS NFV-SEC 009 [i.1] for a definition.

The core component to have a measured or secured boot would be any functionality which is involved in delivering, making or checking Retained Data requests. It would be beneficial in adding evidential assurance to the process if such components were run through a secured boot. In general measured boots are less effective in these situations, as there is little merit in running functionality for Retained Data which is known to have failed a checksum or other validation at boot time.

6.8 Attestation, Trusted Platform Modules and Hardware-Mediated Execution Enclaves

See clauses 6.15, 6.16 and 6.17 of ETSI GS NFV-SEC 009 [i.1] for a description.

Where Retained Data storage and query functionality is not able to be secured by Physical or Personnel checks (see clause 6.3 of the present document) then Hardware-Mediated Execution Enclaves are important to address issues in clauses 5.2, 5.4 and 5.5 of the present document. The TPMs are to be Hardware TPMs (see clause 6.17 from [i.1]).

Location attestation is important in order to address issues in clause 5.3 from the present document. Location attestation may apply to the location of collection of the data and the location of storage of the data, though it is for national regulations to determine in which cases it is critical to provide attestation regarding the locations involved.

6.9 Memory inspection as an attack vector.

Clause 6.1.1 of ETSI GS NFV-SEC 009 [i.1] notes the following issues:

- Confidentiality of Data, Data-Related Metadata, Processes and Process-Related Metadata.
- Concealment of Resource Usage.
- Secure Communications, Secure Storage, Secure Routing/Switching.
- Availability of Entropy Source.

The core issue regarding Retained Data is around the confidentiality of data and the secure communications, in order to address the issues from clauses 5.2 and 5.4 of the present document.

History

Document history		
V1.1.1	April 2016	Publication