ETSI TS 103 487 V1.1.1 (2016-04)

CYBER;
Baseline security requirements regarding sensitive functions for NFV and related platforms

Reference
DTS/CYBER-0017

Keywords
Cybersecurity, NFV

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 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.

Introduction

The present document is based on the study performed in ETSI TR 103 308 [i.1] establishing the fundamental security principles for hardware supporting virtualised network functions and focusing on the LI and RD aspects.

1 Scope

The present document defines security baseline requirements for sensitive functions including lawful interception (LI) and retained data (RD) in an NFV hardware/platform environment.

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 TR 103 308: "CYBER; Security baseline regarding LI and RD for NFV and related platforms".

3 Abbreviations

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

GSMA	Global System for Mobile Communications
ISO	International Standards Organisation
LEA	Law Enforcement Agency
LI	Lawful Interception
NFV	Network Function Virtualisation
RD	Retained Data
TPM	Trusted Platform Module
VNF	Virtual Network Function
VNFI	Virtual Network Function Interface

4 Requirements on the hardware platform

4.1 Requirements possible using current technology

- The platform shall provide hardware support for the secure storage of LI target lists.
- The platform shall store LI target lists in such a way that the storage is resistant to a compromise of the hypervisor layer.
- The platform shall provide secured boot for the host.
- The platform shall provide secured boot for all VNFIs.
- Data storage and data communications systems shall prevent data tampering.
- The platform shall provide a location to store keys that cannot be compromised (e.g. by a privileged hypervisor manager, errant process, etc.).
- The platform shall provide the ability to perform cryptographic functions (such as decrypting LI target lists received from LEAs or signing LI VNFs prior to deployment) external to the virtualised platform.
- The platform shall provide a source of entropy which is external to the virtualised environment.
- The platform shall provide a source of random numbers using a standardized random number generator (e.g. those standardized in GSMA or ISO).
- The platform shall provide the ability to assign geographic locations to physical hardware elements.
- The physical hardware that hosts any virtual machine that runs LI entities shall provide a hardware root of trust, such as a TPM.
- The physical hardware that hosts any storage services for LI entities shall provide a hardware root of trust, such as a TPM.
- The host platform shall monitor resource usage by VNFs hosted on the platform and prevent actions that may harm the host (e.g. by causing overheating).
- The host platform shall be uniquely identifiable.

4.2 Requirements for further study

- The hypervisor environment shall prevent unauthorised suspension of virtual machines.
- The hypervisor environment shall prevent the inspection of memory of virtual machines.

History

Document history		
V1.1.1	April 2016	Publication