



GROUP SPECIFICATION

**Network Functions Virtualisation (NFV)  
Release 3;  
Security;  
System architecture specification  
for execution of sensitive NFV components**

***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-SEC012

---

**Keywords**

architecture, NFV, security

**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/CommitteeSupportStaff.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 2017.  
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.....	6
3.1 Definitions .....	6
3.2 Abbreviations .....	6
4 Principles.....	7
4.1 Introduction .....	7
5 Platform requirements .....	7
5.1 Core hardware requirements.....	7
5.2 Core software requirements.....	8
6 Lifecycle.....	9
6.1 Trusted Computing Base .....	9
6.2 Workload provisioning.....	9
6.3 Runtime checks .....	10
6.4 Entropy and random numbers .....	10
6.5 Cryptographic primitives.....	11
6.6 Installed software and configurations on host system .....	12
6.7 De-provisioning workloads .....	12
6.8 Dealing with failure.....	13
6.8.0 General points.....	13
6.8.1 Requirements relating to failure conditions .....	13
7 External dependencies.....	13
8 Architecture section.....	13
8.0 System hardening techniques .....	13
8.1 Secure logging.....	14
8.2 OS-level access and confinement control.....	14
8.3 Physical controls and alarms .....	14
8.4 Authentication controls .....	14
8.5 Access controls.....	14
8.6 Communications security .....	15
8.7 Boot.....	15
8.8 Attestation .....	15
8.9 Hardware-mediated execution enclaves .....	15
8.10 Hardware-Based Root of Trust (HBRT) .....	15
8.11 Self-encrypting storage.....	15
8.12 Direct access to memory .....	16
8.13 Hardware Security Modules .....	16
8.14 Software integrity protection and verification.....	16
History .....	17

---

## 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 present document defines requirements for host system elements on which sensitive workloads are to be run. The present document defines requirements to ensure isolation of sensitive workloads from non-sensitive workloads sharing a platform. The present document discusses a wide range of different technologies which aim to increase the security of a host system for the workloads which will be executing on it.

---

## 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] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".
- [2] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".
- [3] ISO/IEC 18031:2001: "Information technology -- Security techniques -- Random bit generation or equivalent specification".

### 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] NIST Publication (SP) 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation".
- [i.2] NIST Publication (SP) 800-88 revision 1: "Guidelines for Media Sanitization".
- [i.3] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".
- [i.4] Greg Hoglund, Gary McGraw (2007): "Exploiting Online Games: Cheating Massively Distributed Systems", Addison-Wesley, New Jersey.
- [i.5] ETSI TS 103 487 "CYBER; Baseline security requirements regarding sensitive functions for NFV and related platforms".
- [i.6] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".