



GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 5; Security; Isolation and trust domain specification

Document Preview

[ETSI GS NFV-SEC 026 V5.1.1 \(2025-07\)](https://standards.iteh.ai/catalog/standards/etsi/62ed563b-9790-4028-badc-4192470ba5a7/etsi-gs-nfv-sec-026-v5-1-1-2025-07)

<https://standards.iteh.ai/catalog/standards/etsi/62ed563b-9790-4028-badc-4192470ba5a7/etsi-gs-nfv-sec-026-v5-1-1-2025-07>

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-SEC026

Keywordsaccess control, cybersecurity, NFV, NFVI,
security, trust**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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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

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.

© ETSI 2025.
All rights reserved.

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 Analysis of threat models in a multi-tenant NFV infrastructure	8
4.1 Introduction	8
4.2 Threat analysis.....	9
4.2.1 Use Case #0: Provide Isolation of two VNFs of a single NS.....	9
4.2.1.1 Description.....	9
4.2.1.2 Threat analysis	10
4.2.2 Use Case #1: Two users with own NFVO on shared NFVI.....	10
4.2.2.1 Description	10
4.2.2.2 Threat analysis	11
4.2.3 Use Case #2: Two users share the same NFV environment	11
4.2.3.1 Description	11
4.2.3.2 Threat analysis	11
4.2.4 Use Case #3: Network slicing by a single user	12
4.2.4.1 Description	12
4.2.4.2 Threat analysis	12
4.2.5 Use Case #4: Nested network services	13
4.2.5.1 Description	13
4.2.5.2 Threat analysis	13
4.2.6 Use Case #6: Two users with own MANO stack managed by provider MANO.....	14
4.2.6.1 Description	14
4.2.6.2 Threat analysis	15
4.2.7 Use Case #7: Provide Isolation on different levels	15
4.2.7.1 Description	15
4.2.7.2 Threat analysis	16
4.2.8 Use Case #8: Isolation of containerized VNF instances	17
4.2.8.1 Description.....	17
4.2.9 Use Case #9: Multiple NMTs use the same entity.....	17
4.2.9.1 Description.....	17
4.2.9.2 Threat analysis	18
4.3 Requirements.....	19
5 Trust domain separation at resource level	22
5.1 Introduction	22
5.2 Resource separation.....	23
5.3 Data protection	23
5.3.1 Introduction.....	23
5.3.2 Protection of data in transit	24
5.3.3 Protection of data at rest using transparent encryption	25
5.3.4 Protection of data in use.....	28
5.3.5 Protection of Software images	31
6 Hypervisor partitioning	36
6.1 Introduction	36
6.2 Solution description.....	36

6.2.0	Introduction.....	36
6.2.1	Spatial partitioning.....	36
6.2.1.0	Introduction.....	36
6.2.1.1	Memory Partitioning	36
6.2.1.2	Memory partition encryption	36
6.2.1.3	Cache Partitioning.....	37
6.2.1.4	I/O Partitioning	37
6.2.1.5	CPU Partitioning	37
6.2.1.6	Hardware resources Partitioning	37
6.2.1.7	Key vault Partitioning	37
6.2.1.8	Static Memory allocation	37
6.2.1.9	Interrupt Partitioning	38
6.2.2	Temporal partitioning	38
6.2.2.0	Introduction.....	38
6.2.2.1	Fixed Cyclic Scheduling	38
6.2.2.2	CPU registers reuse	38
6.2.2.3	Memory Bandwidth Reservation	38
6.2.2.4	Priority-based Scheduling	38
6.2.2.5	Worst-case execution time	38
6.2.2.6	Interrupt Management.....	38
6.2.2.7	Resource Reservation.....	38
6.2.3	Fault partitioning	38
6.2.3.0	Introduction.....	38
6.2.3.1	Resource Isolation.....	39
6.2.3.2	Memory Protection.....	39
6.2.3.3	Error Detection and Handling	39
6.2.3.4	Fault Containment.....	39
6.2.3.5	Redundancy and Checkpointing.....	39
7	Containerized VNF escape protection.....	39
7.1	Introduction	39
7.2	Solutions description	39
8	Key Management and access control	41
8.1	Introduction	41
8.2	Strong cryptographic algorithms	41
8.3	Secure key storage.....	41
8.4	Separation encrypted data and encryption keys.....	42
8.5	Regular key rotation	42
8.6	Access controls and auditing	42
8.7	Disaster recovery and high availability	42
8.8	Key management approaches	43
8.8.1	Introduction.....	43
8.8.2	Bring Your Own Key (BYOK).....	43
8.8.3	Hold Your Own Key (HYOK).....	43
8.8.4	Bring Your Own Encryption (BYOE).....	43
8.8.5	Key management approaches selection	43
8.9	Centralized Key management.....	44
9	Conclusion.....	45
Annex A (informative): Change history		46
History		47

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 IPR online database](#).

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™**, **LTE™** and **5G™** logo 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 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 the requirements and solutions for the NFV System to enhance network functions and services isolation between tenants.

For this aim, the present document includes in particular:

- Analysis of the threat models.
- Trust domain separation (multi-tenant NFVI, traffic and resource separation, tenant-dependant resource management and access control).
- Memory protection and access control (protection against memory introspection, confidentiality of sensitive data and credentials).
- Hypervisor trust partitioning.
- The Virtualization Container (e.g. Virtual Machine and OS container) Escape protection (e.g. protection against VNF compromising its local host OS, taking control of the hypervisor and then gaining access to private and sensitive data of co-resident Virtualization Containers).
- Associated key management system for all above items.

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 in the [ETSI docbox](https://standards.iteh.ai/catalog/standards/etsi/62ed563b-9790-4028-bade-4192470ba5a7/etsi-gs-nfv-sec-026-v5-1-1-2025-07).

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 GS NFV-SOL 004](#): "Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; VNF Package and PNFD Archive specification".
- [2] [IETF RFC 9334](#): "Remote Attestation procedureS (RATS) Architecture".
- [3] [OASIS KMIP](#): "Key Management Interoperability Protocol Specification Version 2.1".
- [4] [ETSI GS NFV-SEC 021](#): "Network Functions Virtualisation (NFV); Security; VNF Package Security 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.