***Disclaimer***

The present document has been produced and approved by the <long ISGname> (<short ISGname>) 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.

ETSI GS NFV-SEC 029 V0.1.0 (2023-10)

**Group Specification**

Network Functions Virtualisation (NFV) Release 5;

Security;

Security Assurance Specification (SCAS) for NFVO

Release 5

<

**This DRAFT is a working document of ETSI. It is provided for information only and is for future development work within ETSI. DRAFTS may be updated, deleted, replaced, or obsoleted by other documents at any time.**

**ETSI and/or its Members have no liability for any current or further use/implementation of the present DRAFT.**

**Do not use as reference material.
Do not cite this document other than as "work in progress."**

**Any draft approved and PUBLISHED shall be obtained exclusively as a deliverables via the ETSI Standards search page at:**

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

Reference

DGS/NFV-SEC029

Keywords

NFV-MANO; Security; NFVO; test; SCAS

***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](http://www.etsi.org/standards-search#Pre-defined Collections)

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 at [www.etsi.org/deliver](http://www.etsi.org/deliver).

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.

© ETSI 2020.

All rights reserved.

**DECT**TM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
**3GPP**TM and **LTE**TM 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.

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 Definition of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 5

4 Catalogue of security requirements and related test cases for NFVO product 6

4.1 Introduction 6

4.2 Security functional requirements and related test cases 6

4.3 Security requirements and related test cases related to hardening 6

4.3.1 Introduction 6

4.4 Baseline vulnerability testing requirements 9

4.4.1 Introduction 9

Annex A (normative or informative): Aspects specific to the network product class NFVO 10

A.1 Network product class description for the NFVO 10

A.1.1 Introduction 10

A.1.2 Minimum set of functions defining the NFVO network product class 10

A.2 Assets and threats specific to the NFVO 10

A.2.1 Critical assets 10

A.2.2 Threats related to orchestration procedures 10

Annex (informative): Bibliography 10

Annex (informative): Change History 11

# Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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](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.

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.

# 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](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (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 security assurance of Network Functions Virtualisation Orchestrator(NFVO) products, which is part of MANO system. The outcome of this WI expects the security assets, security threats, security requirements and test cases for evaluating the security NFVO products. In this work item, the security assurance methodology introduced in 3GPP specifications will be leveraged. Security test cases including testing goals, testing steps, and evidence of testing results will be produced for evaluating whether the security requirements are implemented by NFVO based products.

# 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](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 GS NFV-SEC 028: "Network Functions Virtualisation (NFV) Release 4; Security; Security Assurance Specification (SCAS) for Generic NFV-MANO".

[2] ETSI GS NFV-SEC 025: "Network Functions Virtualisation (NFV) Release 4; Security; Secure End-to-End VNF and NS management specification".

[3] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV) Release 2; 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.

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 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in ETSI GS NFV 003 [i.1] apply.

## 3.2 Symbols

Void

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.1] apply.

# 4 Catalogue of security requirements and related test cases for NFVO product

Editor’s Note: The structure of sub-clause follows the structure of ETSI NFV SEC 028 [1]. This clause will describe requirements and test cases for NFVO.

## 4.1 Introduction

The present clause describes security functional requirements and the corresponding test cases for NFVO products.

## 4.2 Security functional requirements and related test cases

All test cases in clause 4.2 of ETSI NFV SEC 028 [1] can be applied to NFVO products with the exceptions listed in the following clauses.

## 4.3 Security requirements and related test cases related to hardening

### 4.3.1 Introduction

All test cases in clause 4.4 of ETSI NFV SEC 028 [1] can be applied to NFVO products with the exceptions listed in the following clauses.

4.3.2 Secure NFVO VNF Image Repositories – Integrity Protection

*Requirement Name*: VNF image repositories in the NFVO shall be secure

*Requirement Description*:

NFV SEC 025 [2], clause 6.2.2.

"The repositories shall support CSP signing/CSP provided integrity protection of VNF images."

NFV SEC 021 [3], Clause 5.1

- The VNF provider's signature on individual artifacts in a VNF Package shall be stored by NFV-MANO.

- Additionally, if the service provider policy mandates to sign an artifact, this service provider's signature on this individual artifact(s) shall be stored as well.

*Test Case*:

**Test Name**: TC\_SECURE\_VNF\_REPOS\_INTEGRITY

**Purpose:**

The protect the integrity of VNF images stored in the NFVO repositories during onboarding and instantiation.

**Procedure and execution steps:**

**Pre-Conditions:**

A list of all available software and libraries and associated components containing at least the following information shall be included in the documentation accompanying the Product:

1) A key management system using a known baseline set of CSP policies shall be established and interfaced to the repositories using standard protocols.

2) Identify all vendor and CSP keys, signing certificate(s) and chain(s) of trust that are needed to sign and verify integrity protected VNF images to be stored in the image repository and later instantiated.

3) Documentation which describes the VNF image onboarding and instantiation procedures including how a user is authorized and authenticated to perform the onboarding and instantiation processes.

4) A valid VNF image outside the repository that is integrity protected with a valid vendor signature.

5) From this valid image, several invalid VNF images outside the repository shall be prepared as follows:

a) Only alter the vendor signature of the image

b) Only alter the image itself

c) Alter both the vendor signature and the image itself

d) Remove the vendor signature from the image

6) A valid VNF image stored inside the repository that is integrity protected with a valid vendor signature and also integrity protected with a valid CSP signature.

7) From this valid image, several invalid VNF images stored inside the repository shall be prepared as follows:

a) Only alter the CSP signature of the image

b) Only alter the image itself

c) Alter both the CSP signature and the image itself

d) Remove the CSP signature from the image

**Execution Steps**

The accredited evaluator's test lab is required to execute the following steps:

1) The tester logs in using the account that is authorized to perform onboarding and instantiation processes.

2) The tester tries to onboard/store the prepared valid VNF image outside the repository where the CSP policies are configured to NOT require any additional CSP level signatures.

3) The tester tries to onboard/store the prepared valid VNF image outside the repository where the CSP policies are configured to require additional CSP signed integrity protection before storing into the repository.

4) The tester tries to onboard/store all the prepared invalid VNF images outside the repository.

5) The tester tries to extract the prepared valid VNF image stored inside the repository and instantiate it.

6) The tester tries to extract all the prepared invalid VNF images stored inside the repository and instantiate each of them.

**Expected Results:**

1) The onboarding operation is successful when using the valid VNF images outside the repository. Specifically, the vendor integrity check passes.

2) The onboarding operation fails when using any of the invalid VNF images outside the repository. Specifically, the vendor integrity checks fail.

3) The extraction and instantiation operation is successful when using the valid VNF image stored in the repository. Specifically, the CSP integrity check passes.

4) The extraction and instantiation operation fails when using any of the invalid VNF images stored in the repository. Specifically, the CSP integrity checks fail.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

1) Settings, protocols, and configurations used.

2) Snapshots containing the result of the onboarding of the VNF images.

3) Snapshots containing the result of the instantiation of the VNF images.

4.3.3 Secure NFVO VNF Image Repositories – Confidentiality Protection

*Requirement Name*: VNF image repositories in the NFVO shall be secure

*Requirement Description*:

NFV SEC 025 [2], clause 6.2.2.

"NFV-MANO and NFVI shall support the VNF images encryption in the repositories using CSP specific key(s) and Key management.

The need for encryption and key management used shall be configurable per CSP/per VNF image. The encryption/decryption process used shall be defined per CSP / per VNF image.

When encryption of VNF images is used, the encryption of VNF image shall be done before the signing of the VNF image, to enable an integrity verification without any need for decryption. "

NFV SEC 021 [3], Clause 6.4

"NFVO shall encrypt the VNF Package artefacts using the appropriate encryption key(s) provided by service provider.

NFVO shall store the encrypted VNF Package artefacts in corresponding catalogue(s). "

NFV SEC 021 [3], Clause 6.5

"Prior to instantiation of the VNF Package, if the service provider policy for onboarding includes confidentiality protection for VNF artefacts, then those VNF artefacts shall be decrypted before VNF instantiation.

The cryptographic key material used for decryption of the VNF Package shall be provided by the service provider. "

*Test Case*:

**Test Name**: TC\_SECURE\_VNF\_REPOS\_CONFIDENTIALITY

**Purpose:**

The confidentiality protection of VNF images stored in the NFVO repositories as part of service catalogues.

**Procedure and execution steps:**

**Pre-Conditions:**

1. A key management system using a known baseline set of CSP policies shall be established and interfaced to the repositories using standard protocols.
2. Identify all CSP encryption/decryption keys, encryption/decryption methods and policies related to confidentiality protection of each VNF image to be stored in the image repository and later instantiated.
3. Documentation which describes the CSP VNF image encryption/decryption procedures including how a user is authorized and authenticated to perform the encryption/decryption processes.
4. Two identical copies of a valid VNF image outside the repository. Integrity verification is not performed in this test but performed in a separate test case.
5. The two images each consist of a collection of artefacts A, B, C, etc.(e.g., computeVDU, storageVDU). Each artefact shall be independently configured to use different encryption/decryption methods and encryption/decryption keys for the two images when stored in the image repository.

**Execution Steps**

The accredited evaluator's test lab is required to execute the following steps:

1. The tester logs in using the account that is authorized to perform onboarding and instantiation processes.
2. The tester stores all artefacts of the first valid VNF image into the repository where the CSP policies are configured with encryption properties for each artefact.
3. The tester stores all artefacts of the second valid VNF image into the repository where the CSP policies are configured with different encryption properties for each artefact.
4. The tester tries to extract all artefacts of the first valid VNF image stored inside the repository intended for instantiation.
5. The tester tries to extract all artefacts of the second valid VNF image stored inside the repository intended for instantiation.
6. The tester compares each corresponding artefact that was extracted with the original artefact outside the repository.

**Expected Results:**

1. The onboarding operation is successful when each artefact of the images is encrypted using a different encryption key and encryption method. The two encrypted sets of artefacts of the image files must appear to be different.
2. The extraction operation is successful when each extracted artefact is identical and matches the original artefact within the images outside the repository.
3. After extraction, all artefacts of both images are discarded. They are not checked for validity nor instantiated.

**Expected format of evidence:**

A testing report provided by the testing agency which consists of the following information:

1. Settings, protocols, and configurations used.
2. Snapshots containing the result of the onboarding of the VNF images. Logs of encryption method used.

## 4.4 Baseline vulnerability testing requirements

### 4.4.1 Introduction

All test cases in clause 4.4 of ETSI NFV SEC 028 [1] can be applied to NFVO products with the exceptions listed in the following clauses.

# Annex A (normative or informative):Aspects specific to the network product class NFVO

## A.1 Network product class description for the NFVO

### A.1.1 Introduction

This annex captures the aspects specific to network product class NFVO.

### A.1.2 Minimum set of functions defining the NFVO network product class

As part of the NFVO network product, it is expected the NFVO to contain NFVO application, a set of running processes (typically more than one) executing the software package for the NFVO functions and OAM functions that is specific to the NFVO network product model. Functionalities specific to the NFVO network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in present document.

## A.2 Assets and threats specific to the NFVO

### A.2.1 Critical assets

In addition to the critical assets of a generic NFV-MANO product described in clause B.2 of NFV SEC 028 [1], the critical assets specific to the NFVO to be protected are:

- NFVO Application;

- The interfaces of NFVO product to be protected and which are within SECAM scope:

- Interface between NFVO and VNFM

- Interface between NFVO and VIM

- VNF image and image description file.

### A.2.2 Threats related to orchestration procedures

A.2.2.1 VNF Image Tampering

*- Threat Name*: VNF image tampering

*- Threat Category*: Tampering

- *Threat Description*: During the process of VNF package onboarding, the VNF image in the image repository can be tampered/altered if not protected. Attackers inject malicious or backdoor software, and a VNF instance set up by the compromised VNF image may lead to attacks like DoS, Information Stealing, etc.

*- Threatened Asset*: VNF image and image description file.

#### A.2.2.2 VNF Image Eavesdropping

*- Threat Name*: VNF image eavesdropping

*- Threat Category*: Information Disclosure

- *Threat Description*: During the process of VNF package onboarding, the VNF image in the image repository can be eavesdropped if not protected. Attackers are able to obtain data like algorithm, configuration illegally. It may lead to information theft.

*- Threatened Asset*: VNF image and image description file.

Annex (informative):
Bibliography

Annex (informative):
Change History

| Date | Version | Information about changes |
| --- | --- | --- |
| 10-2023 | V0.1.0 | First draft as baseline |