ETSI GS NFV-SEC 031 V5.2.1 (2024-11)

Network Function Virtualisation (NFV) Release 5; Security; Security Assurance Specification (SCAS) for NFVO

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-SEC031

Keywords
assurance, MANO, NFV, NFVO, orchestration,
SCAS, security, test

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

Contents

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 security assurance of Network Functions Virtualisation Orchestrator (NFVO) products, which is part of MANO system. The outcome of the present document expects the security assets, security threats, security requirements and test cases for evaluating the security NFVO products. In the present document, 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 in the ETSI docbox.

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 5; Security; Security Assurance Specification (SCAS) for Generic NFV-MANO".

[2] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Functional requirements specification".

[3] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV) Release 4; 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

4.1 Introduction

The present clause describes security functional requirements and the corresponding test cases for NFVO products. It is noted that the requirements for interfaces external to NFV-MANO in ETSI GS NFV-SEC 028 [1] are applicable to the interfaces for NFVO by default. Exceptions shall be listed with justifications.

4.2 Security functional requirements and related test cases

4.2.1 Introduction

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

4.2.2 Security functional requirements deriving from ETSI specifications and related test cases

4.2.2.1 Verification of VNF package integrity and authenticity during on-boarding procedure

Requirement Name: Verification of VNF package integrity and authenticity during on-boarding procedure

Requirement Reference: ETSI GS NFV-IFA 010 [2], clause 6.5.1

Requirement Description:

"The NFVO shall support the capability to verify the integrity and authenticity of the VNF Package". As specified in ETSI GS NFV-IFA 010 [2], clause 6.5.1, Nfvo.VnfPkgm.002.

Threat Reference: ETSI GS NFV-SEC 028 [1], clause B.3.4.1, Software Tampering

Test case:

Test Name: TC_VERIFICATION_VNF_PACKAGE_INTEGRITY_AUTHENTICATION

Purpose:

To test whether NFVO under test will verify the integrity and authenticity of the VNF package during on-boarding procedure.

Procedure and execution steps:

Pre-Conditions:

The NFVO documentation describes information regarding integrity and authenticity protection of VNF package.

A valid VNF package and an invalid VNF package (e.g. a tampered image in VNF package) are available.

A VNF package signed by the private key of A acting as the legitimate VNF vendor, and the same VNF package signed by the private key of B acting as the malicious VNF vendor.

The certificate or the public key which is used to verify the digital signature of VNF package has been pre-configured in the NFVO.

There is a simulated BSS in the test environment. The tester is able to trace traffic between the NFVO and the BSS.

Execution Steps:

Test case 1: Verify the integrity of the VNF package.

1) The tester intercepts the traffic between the BSS and the NFVO.

2) During VNF package on-boarding, the tester uploads the valid VNF package into the NFVO as BSS. The NFVO validates the digital signature of the VNF package using the pre-configured certificate.

3) During VNF package on-boarding, the tester uploads the invalid VNF package into the NFVO as BSS. The NFVO validates the digital signature of the VNF package using the pre-configured certificate.

Test case 2: Verify the authenticity of the VNF package.

1) The tester intercepts the traffic between the BSS and the NFVO.

2) During VNF package on-boarding, the tester uploads the VNF package whose signature is generated by A into the NFVO as BSS. The NFVO validates the digital signature of the VNF package using the pre-configured certificate.

3) During VNF package on-boarding, the tester uploads the VNF package whose signature is generated by B into the NFVO as BSS. The NFVO validates the digital signature of the VNF package using the pre-configured certificate.

Expected Results:

Test case 1:

The valid VNF package is successfully on-boarded into the NFVO. The invalid VNF package is not on-boarded.

Test case 2:

The VNF package signed by A is successfully on-boarded into the NFVO. The VNF package signed by B is not on-boarded.

Expected format of evidence:

Evidence suitable for the interface between BSS and NFVO, e.g. screenshot containing the results of VNF package on-boarding procedure from NFVO.

4.2.2.2 Verification of NSD integrity after on-boarding procedure

Requirement Name: Verification of NSD integrity after on-boarding procedure

Requirement Reference: ETSI GS NFV-IFA 010 [2], clause 6.6.1

Requirement Description:

"The NFVO shall support the capability to verify the integrity of the provided NSD". As specified in ETSI GS NFV-IFA 010 [2], clause 6.6.1, Nfvo.NsDtm.002.

Threat Reference: ETSI GS NFV-SEC 028 [1], clause B.3.4.1, Software Tampering

Test case:

Test Name: TC_VERIFICATION_NSD_INTEGRITY

Purpose:

To test whether NFVO under test will verify the integrity of the NSD after on-boarding procedure.

Procedure and execution steps:

Pre-Conditions:

The NFVO documentation describes information regarding integrity protection of NSD.

An available VNF package, a valid NSD and a tampered NSD corresponding to the VNF package are available.

The certificate or the public key which is used to verify the digital signature of VNF package and NSD has been pre-configured in the NFVO.

There is a simulated BSS in the test environment. The tester is able to trace traffic between the NFVO and the BSS.

Execution Steps:

1) The tester intercepts the traffic between the BSS and the NFVO.
2) During VNF package on-boarding, the tester uploads the VNF package into the NFVO as BSS.
3) After receiving the response from NFVO indicating that the VNF package is successfully on-boarded, the tester uploads the valid NSD into the NFVO as BSS. The NFVO validates the digital signature of the NSD using the pre-configured certificate.
4) After receiving the response from NFVO indicating that the VNF package is successfully on-boarded, the tester uploads the tampered NSD into the NFVO as BSS. The NFVO validates the digital signature of the NSD using the pre-configured certificate.

Expected Results:

The valid NSD is successfully on-boarded into the NFVO. The tampered NSD is not on-boarded.

Expected format of evidence:

Evidence suitable for the interface between BSS and NFVO, e.g. screenshot containing the results of VNF package on-boarding procedure from NFVO.

4.2.2.3 Anti-rollback protection for VNF package

Requirement Name: Anti-rollback protection for VNF package

Requirement Reference: In accordance with industrial best practice

Requirement Description:

A mechanism is needed to prevent the VNF Package from downgrading to that of an older version which is not available. For example, a version control system indicating that an older version of the VNF Package is invalid, or the certificate of an older version of the VNF Package is in the Certificate Revocation List.

Threat Reference: Clause A.2.2.3, failure to perform the anti-rollback protection

Test case:

Test Name: TC_ANTI_ROLLBACK_PROTECTION_VNF_PACKAGE

Purpose:

To test whether the anti-rollback protection is supported by NFVO under test.

Procedure and execution steps:

Pre-Conditions:

The NFVO documentation describes information on the feature of anti-rollback protection.

A VNF package of version A for a VNF has been on-boarded into NFVO.

A VNF package of version B which is older than A, for the same VNF. It is noted that this VNF package is actually not available, e.g. the VNF package is out-of-date in the version control system, or the certificate of the VNF package is in the certificate revocation list, etc.

There is a simulated BSS in the test environment. The tester is able to trace traffic between the NFVO and the BSS.

Execution Steps:

1) The tester intercepts the traffic between the BSS and the NFVO.

2) The tester uploads VNF package of version B to the NFVO as BSS.

Expected Results:

VNF package of version B is not on-boarded into the NFVO.

Expected format of evidence:

Evidence suitable for the interface between BSS and NFVO, e.g. screenshot containing the results of VNF package on-boarding procedure from NFVO.

4.3 Security requirements and related test cases related to hardening

4.3.1 Introduction

All test cases in clause 4.3 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 Reference: ETSI GS NFV-SEC 021 [3], clauses 5.1 and 6.1

Requirement Description:

ETSI GS NFV-SEC 021 [3], clause 5.1

"*Each individual artifact in a VNF Package shall have a cryptographic signature when it is stored in the NFV-MANO catalogue(s):*

- *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.*"

ETSI GS NFV-SEC 021 [3], clause 6.1

"*A VNF Package is composed of several components such as VNFD, software images, scripts, etc.*"

Therefore, if the service provider policy mandates to sign the VNF image, the VNF image shall be stored in the repository with its signature.

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 Reference: ETSI GS NFV-SEC 021 [3], clauses 6.1, 6.4 and 6.5

Requirement Description:

ETSI GS NFV-SEC 021 [3], clause 6.1

"*A VNF Package is composed of several components such as VNFD, software images, scripts, etc.*"

ETSI GS 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)."

ETSI GS 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."

Therefore, if the service provider policy for onboarding includes confidentiality protection for VNF image, the VNF image shall be encrypted and stored in the repository, then be decrypted before VNF instantiation.

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 shall 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.

Annex A (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 ETSI GS 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:
  - VNF package.

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.

A.2.2.3 Failure to perform the anti-rollback protection

- *Threat name:* Failure to perform the anti-rollback protection.
- *Threat Category:* Tampering.
- *Threat Description:* The anti-rollback protection (e.g. versioning, Certificate Revocation List) is used to prevent the VNF Package downgrading to an older version. If the anti-rollback protection is not supported, the attack will make the version of VNF package downgrade to an old one.
- *Threatened Asset:* VNF package.

History

Document history		
V5.2.1	November 2024	Publication