ETSI GS NFV-SEC 029 V5.3.1 (2025-08)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 5; Security; Security Assurance Specification (SCAS) for VIM

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
RGS/NFV-SEC029ed531

Keywords
assurance, MANO, NFV, SCAS, security
requirements, test, VIM

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 VIM 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 VIM 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 VIM 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 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".

[4] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Architecture enhancement for Security Management 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 VIM product

4.1 Introduction

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

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 VIM 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 VM software image integrity and authenticity during instantiation

Requirement Name:

Verification of VM software image integrity and authenticity during instantiation

Requirement Reference:

ETSI GS NFV-IFA 010 [2], clause 8.5

Requirement Description:

"The VIM shall support the capability to verify the integrity and authenticity of the VM software images". As specified in ETSI GS NFV-IFA 010 [2], clause 8.5, Vim.Sim.002.

Threat Reference:

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

Test case:

Test Name: TC_VERIFICATION_VM_SOFTWARE_IMAGE_INTEGRITY_AUTHENTICATION

Purpose:

To test whether VIM under test will verify the integrity and authenticity of the VM software image during instantiation.

Procedure and execution steps:

Pre-Conditions:

The VIM documentation describes information regarding integrity and authenticity protection of VM software image.

A valid VM software image and an invalid VM software image are available.

A VM software image signed by the private key of A acting as the legitimate VNF vendor, and the same VM software image 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 VM software image has been pre-configured in the VIM.

There are simulated NFVO and VNFM in the test environment and the valid and invalid VM software images are on-boarded into the NFVO. The tester is able to trace traffic between the NFVO, VNFM and the VIM.

Execution Steps:

Test case 1: Verify the integrity of the VM software image:

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

2) The tester instantiates the valid VM software image from the NFVO. The VIM validates the integrity of the VM software image using the pre-configured digest.

3) The tester instantiates the invalid VM software image from the NFVO. The VIM validates the integrity of the VM software image using the pre-configured digest.

Test case 2: Verify the authenticity of the VM software image:

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

2) The tester instantiates the VM software image whose signature is generated by A from the NFVO. The VIM validates the digital signature of the VM software using the pre-configured certificate.

3) The tester instantiates the VM software image whose signature is generated by B from the NFVO. The VIM validates the digital signature of the VM software image using the pre-configured certificate.

Expected Results:

Test case 1:

The valid VM software image is successfully instantiated. The invalid VM software image is not instantiated.

Test case 2:

The VM software image signed by A is successfully instantiated. The VM software image signed by B is not instantiated.

For both test cases log entries are produced and sent to a remote logging collector indicating the attempt to instantiate both VM software images and the successful and failed instantiation of the VM software images. For the failed instantiation the log entry contains the reason why instantiation failed.

Expected format of evidence:

Evidence suitable for the interface between NFVO and VIM, e.g. screenshot containing the results of VM software image instantiation procedure from NFVO.

4.2.2.2 Delegation Mode VNF OAM & VNFCI Public/Private Key Pair Protection During VNF Instantiation

Requirement Name: Delegation Mode VNF OAM & VNFCI Public/Private Key Pair Protection During VNF Instantiation.

Requirement Reference: ETSI GS NFV-IFA 026 [4], clause B.4.2 requirement Vim.Sc.008.

Requirement Description:

If delegation mode is selected, the VIM shall securely delete the private key used for the VNF OAM certificate and VNFCI certificate, once the installation attempt of certificate into the VNFCI has been made.

Threat Reference: Clause A.2.2.1, Compromise of VNF OAM and VNFCI certificate private keys.

Test case:

Test Name:
TC_DELEGATION_MODE_VNF_OAM_&_VNFCI_KEY_MANAGEMENT_DURING_VNF_INSTANTIATION

Purpose:

To test whether the VNF OAM and/or VNFCI certificate key pair handled by the VIM under test are protected.

Procedure and execution steps:

Pre-Conditions:

System documentation of the VIM under test, describing the feature of VNF delegation mode key pair handling.

A VNFM is configured to delegation mode.

There is a CMF and associated CA to sign the requested certificate, with the CMF able to respond to delegation mode requests.

Test environment in which the VNFM and VIM which can instantiate and configure a new VNFI/VNFCI.

The tester is able to monitor the VIM operating system, application and storage.

Execution Steps:

1) The VNFM generates a public/private key pair for the VNFCI communication.
2) The VNFM generates a certificate signing request (from the public key and VNF identity data) and submits it to the CMF.
3) The CMF requests the CA to sign the certificate and returns the fully signed certificate to the VNFM.
4) The VNFM instantiates a new VNFI/VNFCI passing the certificate and private key to the VIM.
5) The VIM instantiates the VNFI/VNFCI passing the certificate and private key to the VNFI/VNFCI.
6) The VNFI/VNFCI is instantiated and has a valid certificate and private key for TLS VNFCI communication.
7) The VIM deletes its copy of the VNFCI private key.

Expected Results:

During VNFI/VNFCI instantiation the VNFCI private key cannot be accessed by anything other than the VIM.

When the VNFI/VNFCI is instantiated the VNFCI private key is securely deleted and cannot be recovered.

Expected format of evidence:

Evidence suitable for the interface e.g. screenshot containing the operational results and attempts to access or recover the private key.

4.3 Security requirements and related test cases related to hardening

4.3.1 Introduction

All test cases in clause 4.3 of ETSI GS NFV-SEC 028 [1] can be applied to VIM products with the exceptions listed in the following clauses.

4.3.2 Secure VIM VM software Image Repositories – Integrity Protection

Requirement Name: VM software image repositories in the VIM shall be secure.

Requirement Reference: ETSI GS NFV-SEC 021 [3], clause 5.2.

Requirement Description:

"Before instantiation, all available signatures on the artifacts shall be verified by NFV-MANO:

- *NFV-MANO shall not use any artifacts of a VNF Package without a VNF provider signature when instantiating a VNF component.*
- *If service provider policy mandates that artifacts are signed by the service provider, then the NFV MANO shall not use any artifact that is missing service provider or VNF provider signature when instantiating a VNF component."*

As specified in ETSI GS NFV-SEC 021 [3], clause 5.2.

Test Case:

Test Name:

TC_SECURE_VM_SOFTWARE_IMAGE_REPOS_INTEGRITY

Purpose:

The protect the integrity of VM software images stored in the VIM repositories during 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 VM software images to be instantiated.
3) Documentation which describes the VM software image instantiation procedures including how a user is authorized and authenticated to perform the instantiation processes.
4) A valid VM software image stored inside the repository that is integrity protected with a valid vendor signature and also integrity protected with a valid CSP signature.
5) From this valid VM software image, several invalid VM software 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 tries to extract the prepared valid VM software image stored inside the repository and instantiate it.

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

Expected Results:

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

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

3) Log entries are produced and sent to a remote logging collector indicating the attempt to instantiate both VM software images and the successful and failed instantiation of the VM software images. For the failed instantiation the log entry contains the reason why instantiation failed.

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 instantiation of the VM software images.

4.3.3 Secure VIM VM software Image Repositories – Confidentiality Protection

Requirement Name:

VM software image repositories in the VIM shall be secure.

Requirement Reference:

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

Requirement Description:

"A VNF Package is composed of several components such as VNFD, software images, scripts, etc.". As specified in ETSI GS NFV-SEC 021 [3], clause 6.1.

"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.". As specified in ETSI GS NFV-SEC 021 [3], clause 6.5.

Test Case:

Test Name:

TC_SECURE_VM_SOFTWARE_IMAGE_REPOS_CONFIDENTIALITY

Purpose:

The confidentiality protection of VM software images stored in the VIM repositories as part of service catalogues.

Procedure and execution steps:

Pre-Conditions:

1) Two identical VM software images inside the repository. VM software image A is encrypted with encryption key A'. VM software image B is encrypted with encryption key B'.

2) The valid decryption key corresponding to A' is stored in the key management system.

3) Documentation which describes the CSP VM software image encryption/decryption procedures including how a user is authorized and authenticated to perform the encryption/decryption processes.

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 instantiation processes.

2) The tester tries to instantiate VM software image A.

3) The tester tries to instantiate VM software image B.

Expected Results:

1) The instantiation operation for A is successful.

2) The instantiation operation for B is failed.

3) Log entries are produced and sent to a remote logging collector indicating the attempt to instantiate both VM software images and the successful and failed instantiation of the VM software images. For the failed instantiation the log entry contains the reason why instantiation failed.

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 instantiation of the VM software 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 GS NFV-SEC 028 [1] can be applied to VIM products.

Annex A (informative): Aspects specific to the network product class VIM

A.1 Network product class description for the VIM

A.1.1 Introduction

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

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

As part of the VIM network product, it is expected the VIM to contain VIM application, a set of running processes (typically more than one) executing the software package for the VIM functions and OAM functions that is specific to the VIM network product model. Functionalities specific to the VIM 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 VIM

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 VIM to be protected are:

- VIM Application.
- The interfaces of VIM product to be protected and which are within SECAM scope:
  - Interface between VIM and NFVO.
  - Interface between VIM and VNFM.
- VM software image and image description file.
- VM software image encryption/decryption keys.

A.2.2 Threats related to management procedures

A.2.2.1 Compromise of VNF OAM and VNFCI certificate private keys

In addition to the generic NFV-MANO threats identified in clause B.3 of ETSI GS NFV-SEC 028 [1], the threats specific to the VIM are:

- Threat name: Failure to protect cryptographic private keys.
- Threat Category: Information Disclosure.
- Threat Description: In delegate mode a VNFM generates and holds the public/private key pair for VNF OAM and VNFCI certificates during the certificate request/renewal and distribution process. During VNF instantiation, the VIM receives the public/private key pair for VNF OAM and VNFCI certificates from the VNFM. Any compromise of the private key(s) could result in a loss of confidentiality or integrity of data secured using the key pair.

- Threat Asset: VNFI/VNFCI assets including:
  - User account data and credentials (e.g. passwords).
  - Log data.
  - Configuration data, e.g. VNFI/VNFCI's IP address, ports, VPN ID, Management Objects (e.g. user group, command group), etc.

A.2.3 Threats related to orchestration procedures

A.2.3.1 VNF Image Tampering

- *Threat Name*: VNF image tampering.
- *Threat Category*: Tampering.
- *Threat Description*: Before the process of VNF package instantiation, 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.2.3.2 VNF Image Eavesdropping

- *Threat Name*: VNF image eavesdropping.
- *Threat Category*: Information Disclosure.
- *Threat Description*: Before the process of VNF package instantiation, 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 B (informative): Change History

Date	Version	Information about changes
07-2024	V0.0.1	First draft as baseline
11-2024	V0.0.2	To incorporate approved contribution NFVSEC(24)000202r1 with editorial change on Annex A.2.3 title number; To update release/version/date/ToC information.
02-2025	V5.2.1	To be stable draft for final approval.
06-2025	V5.2.2	Incorporates approved contribution NFVSEC(25)000074r1

History

Document history		
V5.2.1	March 2025	Publication
V5.3.1	August 2025	Publication