ETSI GS NFV-SEC 030 V5.3.1 (2025-08)

GROUP SPECIFICATION

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

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-SEC030ed531

Keywords
MANO, NFV, SCAS, security, test, VNF

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 VNFM 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 VNFM 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 VNFM 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-SOL 003: "Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; RESTful protocols specification for the Or-Vnfm Reference Point".

[3] ETSI GS NFV-SOL 016: "Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; NFV-MANO procedures specification".

[4] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV) Release 4; Security; VNF Package Security Specification".

[5] 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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR 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 GR NFV 003 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

4 Catalogue of security requirements and related test cases for VNFM product

4.1 Introduction

The present clause describes security functional requirements and the corresponding test cases for VNFM 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 VNFM 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 VNFM 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 Signature Verification for files in VNFD

Requirement Name: Signature Verification for files in VNFD.

Requirement Reference: ETSI GS NFV-SEC 021 [4], clause 6.2. ETSI GS NFV-SOL 016 [3], clauses 5.1.3 and 5.2.3. ETSI GS NFV-SOL 003 [2], clause 10.4.4.3.2.

Requirement Description:

During VNF package on-boarding procedure, NFVO shall sign the VNF package artifacts using the appropriate signing key(s), as specified in ETSI GS NFV-SEC 021 [4], clause 6.2.

If VNFM requires VNFD in the VNF package, the VNFM fetches the VNFD from NFVO, as specified in ETSI GS NFV-SOL 016 [3], clause 5.1.3, step 12 and clause 5.2.3, step 6.

Then NFVO provides VNFD as a ZIP archive embedding files with their signatures (if available) to VNFM for response, as specified in ETSI GS NFV-SOL 003 [2], clause 10.4.4.3.2. Therefore, VNFM will verify the signatures of the files.

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

Test case:

Test Name: TC_SIGNATURE_VERIFICATION_FILES_VNFD

Purpose:

To test whether VNFM under test shall verify the signatures of the files in VNFD when NFVO provides them.

Procedure and execution steps:

Pre-Conditions:

The VNFM documentation describes information regarding verifying signatures of files in VNFD.

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

File A and its corresponding signature, and file B which is tampered based on file A, for a particular VNFD, are stored in NFVO.

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

Execution Steps:

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

2) The VNFM requests to fetch the VNFD of the VNF package from the tester.

3) The tester provides VNFD in a ZIP archive, containing file A and the signature to the VNFM as NFVO.

4) The tester provides VNFD in a ZIP archive, containing file B and the signature to the VNFM as NFVO.

Expected Results:

File A is accepted by VNFM, and file B is not.

Expected format of evidence:

Evidence suitable for the interface between VNFM and NFVO, e.g. screenshot containing the verification results from VNFM.

4.2.2.2 Unique VNF instance ID

Requirement Name: Unique VNF instance ID.

Requirement Reference: In accordance with industrial best practice.

Requirement Description:

The identity of the VNF instance shall be universally unique to be used as a handle to reference the instance upon which to execute further operations.

Threat Reference: Clause A.2.2.1, VNF instance ID uniqueness failure.

Test case:

Test Name: TC_UNIQUE_VNF_INSTANCE_ID

Purpose:

To test whether the VNF ID generated by VNFM under test is unique.

Procedure and execution steps:

Pre-Conditions:

The VNFM documentation describes information on the feature of VNF instance ID uniqueness.

The VNFM is configured to generate the VNF instance ID.

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

Execution Steps:

1) The tester intercepts the traffic between the NFVO and the VNFM.
2) The tester triggers the maximum number of VNF setup requests that the VNFM can handle as NFVO.
3) The tester captures the VNF setup response sent from the VNFM to the NFVO, and records each VNF instance ID.

Expected Results:

Each VNF instance ID in the VNF setup response is unique.

Expected format of evidence:

Evidence suitable for the interface between VNFM and NFVO, e.g. screenshot containing the results of VNF setup response from the VNFM.

4.2.2.3 Delegation Mode VNF OAM Public/Private Key Pair Protection

Requirement Name: Delegation Mode VNF OAM Public/Private Key Pair Protection.

Requirement Reference: ETSI GS NFV-IFA 026 [5] clause B.3 requirement Vnfm.Sc.006.

Requirement Description:

If delegation mode is selected, the VNFM shall support the capability to protect the key pairs at rest and when used within tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ certified device, for the VNF OAM certificate and VNFCI certificate.

Threat Reference: Clause A.2.2.2, Compromise of VNF OAM and VNFCI certificate private keys.

Test case:

Test Name: TC_DELEGATION_MODE_VNF_OAM_KEY_MANAGEMENT

Purpose:

To test whether the VNF OAM certificate key pair generated by VNFM under test are protected.

Procedure and execution steps:

Pre-Conditions:

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

The 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 can instantiate and configure a new VNFI/VNFCI.

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

Execution Steps:

1) The VNFM generates a public/private key pair for the VNF OAM 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 VNFI/VNFCI is instantiated and has a valid certificate and private key for TLS VNF OAM communication.
6) The VNFI/VNFCI establishes a TLS connection to the VNFM.
7) The VNFM deletes the VNF OAM private key.

Expected Results:

During VNFI/VNFCI instantiation they VNF OAM private key can not be accessed by anything other than the VNFM.

When the VNFI/VNFCI is instantiated the VNF OAM 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.

4.2.2.4 Delegation Mode VNFCI Public/Private Key Pair Protection During VNF Instantiation

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

Requirement Reference: ETSI GS NFV-IFA 026 [5] clause B.3 requirement Vnfm.Sc.006.

Requirement Description:

If delegation mode is selected, the VNFM shall support the capability to protect the key pairs at rest and when used within tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ certified device, for the VNF OAM certificate and VNFCI certificate.

Threat Reference: Clause A.2.2.2, Compromise of VNF OAM and VNFCI certificate private keys.

Test case:

Test Name: TC_DELEGATION_MODE_VNFCI_KEY_MANAGEMENT_DURING_VNF_INSTANTIATION

Purpose:

To test whether the VNFCI certificate key pair generated by VNFM under test are protected.

Procedure and execution steps:

Pre-Conditions:

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

The 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 can instantiate and configure a new VNFI/VNFCI.

The tester is able to monitor the VNFM 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 VNFI/VNFCI is instantiated and has a valid certificate and private key for TLS VNFCI communication.
6) The VNFM 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 VNFM.

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.

4.2.2.5 Delegation Mode VNFCI Public/Private Key Pair Protection After VNF Instantiation

Requirement Name: Delegation Mode VNFCI Public/Private Key Pair Protection After VNF Instantiation.

Requirement Reference: ETSI GS NFV-IFA 026 [5] clause B.3 requirement Vnfm.Sc.006.

Requirement Description:

If delegation mode is selected, the VNFM shall support the capability to protect the key pairs at rest and when used within tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ certified device, for the VNF OAM certificate and VNFCI certificate.

Threat Reference: Clause A.2.2.2, Compromise of VNF OAM and VNFCI certificate private keys.

Test case:

Test Name: TC_DELEGATION_MODE_VNFCI_KEY_MANAGEMENT_AFTER_VNF_INSTANTIATION

Purpose:

To test whether the VNFCI certificate key pair generated by VNFM under test are protected.

Procedure and execution steps:

Pre-Conditions:

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

The 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 a VNF has been instantiated, which includes VNFCI as target to inject the VNFCI certificate and a VNFM which can configure the VNFI/VNFCI.

The tester is able to monitor the VNFM 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 configures the VNFI as part of the VNF configuration process, passing the certificate and private key to the VNFI/VNFCI.
5) The VNFM deletes its copy of the VNFCI private key.

Expected Results:

During VNFCI certificate installation the VNFCI private key cannot be accessed by anything other than the VNFM.

When the VNFCI certificate and private key is installed 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 VNFM products with the exceptions listed in the following clauses.

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 VNFM products with the exceptions listed in the following clauses.

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

A.1 Network product class description for the VNFM

A.1.1 Introduction

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

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

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

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 VNFM to be protected are:

- VNFM Application.
- The interfaces of VNFM product to be protected and which are within SECAM scope:
  - Interface between VNFM and NFVO
  - Interface between VNFM and VIM

A.2.2 Threats related to management procedures

A.2.2.1 VNF instance ID uniqueness failure

- *Threat name:* Failure to assign a unique VNF instance ID for each VNF instance.
- *Threat Category:* Spoofing Identity, Tampering data.
- *Threat Description:* VNF instance ID is assigned by VNFM, if it is not universally unique, i.e. two or more VNFs share the same instance ID, the request to a particular VNF may impact others, resulting in unavailability or error.
- *Threatened Asset:* Configuration data.

A.2.2.2 Compromise of VNF OAM and VNFCI certificate private keys

- 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. 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.

Annex B (informative): Change history

Date	Version	Information about changes
10-2023	V0.1.0	First draft as baseline
09-2024	V0.0.2	Incorporate approved contribution NFVSEC(24)000134r3, not including changes on changes, to revise A.2.2 to fit updated content.
05-2025	V5.2.2	Incorporated contribution NFVSEC(25)000049r1 and NFVSEC(25)000070r3

History

Document history		
V5.2.1	November 2024	Publication
V5.3.1	August 2025	Publication