ETSI GS NFV-SEC 021 V4.5.1 (2023-10)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 4; Security; VNF Package Security Specification

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-SEC021ed451

Keywords

encryption, NFV, security, virtualisation

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:
https://www.etsi.org/standards-search

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.

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

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

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 VNF Package security requirements and procedures. The present document addresses the security issues related to the integrity, authenticity and confidentiality of the VNF Package artifacts. The VNF Package specification is already undertaken in ETSI GS NFV-IFA 011 [1] and ETSI GS NFV-SOL 004 [2], this is used as input to the present document.

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/.

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-IFA 011: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; VNF Descriptor and Packaging Specification".

[2] ETSI GS NFV-SOL 004: "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; VNF Package and PNFD Archive 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 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 Background and problem definition

4.1 Background

The present document outlines the requirements for integrity and authenticity protection by signing VNF Package artifacts and verifying these artifacts during instantiation. The present document also considers the confidentiality of VNF Package artifacts and outlines a process for the service provider to provide confidentiality during onboarding. The present document expands on requirements for security and integrity of a VNF Package that is defined in ETSI GS NFV-IFA 011 [1], clause 6.2.4 and ETSI GS NFV-SOL 004 [2], clause 5.

4.2 Problem definition

VNF Package security validation check during the onboarding is a crucial factor for the successful deployment of VNFs. During the onboarding, the authenticity and integrity of the VNF Package is verified against the signature provided by the VNF provider. There are more potential ways to exploit the VNF Packages while it is in the NFV-MANO domain (i.e. while the VNF package is stored within different NFV-MANO catalogues). The existing methods do not ensure that the operator has the opportunity and means to authorize VNF Packages for deployment on their network (e.g. avoid a VNF intended for one deployment scenario with a valid VNF provider certificate being loaded by an attacker into another network operator's catalogue). Furthermore, some operators might wish to undertake additional security validation of the VNF Package during the onboarding process and operator's signing could be used to certify the VNF as authorized to onboard into the operator's network.

5 Security requirements

5.1 Requirements during VNF onboarding

The following are the security requirements related to VNF Package onboarding are applicable:

- 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.

5.2 Requirements during VNF instantiation

The following are the security requirements related to VNF instantiation are applicable:

- 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.

NOTE: For checking the VNF provider signature during the VNF instantiation it is not required that NFV-MANO needs to contact the VNF provider outside of the service provider's security domain.

6 VNF Package artifact signing and confidentiality protection process

6.1 Introduction

A VNF Package is composed of several components such as VNFD, software images, scripts, etc. During the onboarding of the VNF Package, a validation of the package is performed. The validation is a procedure that verifies the authenticity and integrity of the VNF Package. The following clauses describe one way of signing and confidentiality protection for VNF artifacts during onboarding by a service provider.

6.2 Signing of VNF Package

Assumption: Service provider has obtained from the VNF provider in advance all necessary VNF Package artifacts (keys, certificates, other information's) in order to proceed the process below.

The procedures for VNF Package signing and verification shall comply with ETSI GS NFV-IFA 011 [1] and ETSI GS NFV-SOL 004 [2], with the following additions:

1) NFVO shall obtain a VNF provider-signed VNF Package.

2) NFVO shall verify the VNF provider's signature(s) of the VNF Package.

3) Service provider shall perform necessary steps to validate and test the VNF Package as described in the use case "VNF Package validation and certification" in ETSI GS NFV-IFA 011 [1], clause 5.5.

4) NFVO shall sign the VNF Package artifacts using the appropriate signing key(s).

5) NFVO shall store the signed VNF Package artifacts in the corresponding catalogue(s).

6.3 Verification of VNF Package during instantiation

The main objective of this step is to verify the VNF Package authenticity and integrity during VNF instantiation. Prior to instantiation of a VNF Package, if the service provider policy for onboarding includes signing of VNF Package artifacts, those signature(s) shall be verified. After service provider signature verification, any other VNF provider certificate shall be verified.

6.4 Handling of confidentiality protected for VNF Package during onboarding

Assumption: Service provider has obtained from the VNF provider in advance all necessary VNF Package artifacts (keys, certificates and other information's) in order to proceed the process below:

1) NFVO shall obtain a VNF provider-signed VNF Package.

2) NFVO shall verify the VNF provider's signature(s) of VNF Package.

3) Service provider shall perform necessary steps to validate and test the VNF Package as per use case "VNF Package validation and certification" in ETSI GS NFV-IFA 011 [1], clause 5.5.

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

5) NFVO shall store the encrypted VNF Package artifacts in corresponding catalogue(s).

NOTE: Exact mechanism of encryption of VNF artifacts with signature is not defined in the present document.

6.5 Handling of confidentiality protected of VNF Package during instantiation

The main objective of this clause is to describe confidentiality protection for a VNF Package during VNF instantiation. Prior to instantiation of the VNF Package, if the service provider policy for onboarding includes confidentiality protection for VNF artifacts, then those VNF artifacts shall be decrypted before VNF instantiation. After service provider VNF decryption, any signature shall be verified. The cryptographic key material used for decryption of the VNF Package shall be provided by the service provider.

NOTE: The present document does not specify detailed procedures for the handling of encrypted VNF artifacts.

6.6 Handling of Certificate Chain of Trust

In ETSI GS NFV-SOL 004 [2] VNF package authenticity and integrity relies on the existence in the NFVO of a root certificate of a trusted Certificate Authority (CA). However, no assumption is made as to who the trusted CA is (whether owned by the vendor or the service provider).

The public key certificate which corresponds to the private key used to sign VNF packages shall be signed by a higher-level Certificate Authority. This can be either a private CA within the entity signing the artefact or package (i.e. the VNF provider or service provider) or public CA (e.g. a commercial CA). There may also be a hierarchy of entities within the CA, with certificates being signed by an intermediate CA which in turn has its certificate signed by a root CA. Whether the CA is private or public it shall be trusted so that VNF package authentication, integrity and where required confidentiality can be verified.

Certificate chain handling shall as a minimum include the following:

1) Operator shall verify the source and full chain of the certificate and if verified install the certificate into the NFVO.

2) During VNF onboarding and instantiation, the NFVO shall validate the VNF package signature using an installed certificate.

Before checking the signature(s) of the VNF Package the signing certificate shall be checked. Where a private CA is used the CA chain of certificates shall be securely installed into the NFVO, the signing certificate can then be checked to make sure it was signed by a trusted entity in the CA chain. Where a public CA is used it is not enough to confirm that the signing certificate is itself signed by a trusted CA, as anyone could purchase such a signing certificate and modify the VNF package. In this scenario the signing certificate shall be securely installed into the NFVO before on-boarding the VNF package. During verification of a VNF package the certificate within or with the package shall be checked with those which are already trusted before checking the rest of the chain of trust.

7 Summary

The present document addresses security gaps during VNF instantiation. ETSI GS NFV-IFA0 11 [1] and ETSI GS NFV-SOL 004 [2] do not specify requirements on the verification of VNF Package authenticity and integrity protection by the service provider during VNF instantiation. The requirements specified in clauses 5 and 6 ensure the authenticity, integrity and confidentiality of VNF Packages before VNF instantiation.

Annex A (informative): Change History

Date	Version	Information about changes
05/2018	V.0.0.1	Updated the scope, TOC, clauses 4.1 and 4.2 were approved during NFVSEC#115 and NFVSEC#124 meetings
06/2018	V.0.0.2	Updated the SEC021V0.0.2 draft based on accepted contributions during NFVSEC#124 meeting i.e. NFVSEC(17)000171r8,NFVSEC(18)000034r4,NFVSEC(18)000060r2
09/2018	V.0.0.3	Updated the SEC021 based on NFVSEC#131 meeting approval
11/2018	V.0.0.4	Updated the SEC021 based on NFVSEC#135 meeting approval
12/2018	V.0.0.5	Updated the SEC021 based on NFVSEC#136 meeting approval
02/2019	V.0.0.6	Updated the SEC021 based on NFVSEC#137 meeting approval
03/2019	V.0.0.7	Updated the SEC021 based on NFV#25 meeting approval
03/2019	V.0.0.8	Updated the SEC021 based on NFVSEC#143meeting approval
03/2019	V.0.0.9	Updated the SEC021 based on NFVSEC#143meeting approval
03/2019	V.0.1.0	Updated the SEC021 based on NFVSEC#143meeting approval
04/2019	V. 0.1.1	Updated the SEC021 based on NFVSEC#145meeting approval
05/2019	V 0.1.2	Updated the SEC021 based on the comments and edits received from ETSI editHelp
06/2023	V4.4.2	Initial draft for ed451 incorporating NFVSEC(23)000129, release changes and changes in rapporteur and contributors.
07/2023	V4.4.3	Incorporating changes from contributions NFVSEC(23)000168.
25/08/23	V4.4.4	Correcting changes which were removed from NFVSEC(23)000168r1.

History

Document history		
V4.5.1	October 2023	Publication