ETSI GS NFV-SOL 004 V2.6.1 (2019-04)

Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; VNF Package 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-SOL004ed261

Keywords
data, NFV, protocol, 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 - 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

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

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 2019.
All rights reserved.

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.

Contents

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/).

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 (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 specifies the structure and format of a VNF package file and its constituents, fulfilling the requirements specified in ETSI GS NFV-IFA 011 [1] for a VNF package.

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); Management and Orchestration; VNF Packaging Specification".

[2] OASIS Standard: "TOSCA Simple Profile in YAML Version 1.1".

[3] IETF RFC 3339: "Date and Time on the Internet: Timestamps".

[4] IANA register for Hash Function Textual Names.

NOTE: Available at https://www.iana.org/assignments/hash-function-text-names/hash-function-text-names.xhtml.

[5] IETF RFC 5652 (September 2009): "Cryptographic Message Syntax (CMS)".

[6] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures".

[7] IANA register for Media Types.

NOTE: Available at https://www.iana.org/assignments/media-types/media-types.txt.

[8] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

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] OASIS Standard-v1.0-os: "Topology and Orchestration Specification for Cloud Applications Version 1.0".

[i.2] OASIS Standard: "TOSCA Simple Profile in YAML Version 1.0".

[i.3] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.4] ETSI GS NFV-SOL 001: "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; NFV descriptors based on TOSCA specification".

[i.5] ETSI NFV registry of non-MANO artifact sets.

NOTE: Available at http://register.etsi.org/NFV.

[i.6] ETSI GS NFV-SOL 006: "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; NFV descriptors based on YANG specification".

[i.7] ETSI GS NFV-SOL 004 (V2.4.1): "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; VNF Package specification".

[i.8] ETSI GS NFV-SOL 004 (V2.5.1): "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; VNF Package specification".

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.3] and the following apply:

non-MANO artifact: artifact for use by functional blocks beyond NFV-MANO

non-MANO artifact set: set of related non-MANO artifacts which are intended to be used together

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CMS	Cryptographic Message Syntax
CSAR	Cloud Service ARchive
IANA	Internet Assigned Number Association
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
TOSCA	Topology and Orchestration Specification for Cloud Applications
URI	Universal Resource Identifier
UTF	Unicode Transformation Format
VNF	Virtualised Network Function
VNFC	VNF Component
VNFD	VNF Descriptor
YAML	YAML Ain't Markup Language
YANG	Yet Another Next Generation

4 VNF package

4.1 TOSCA YAML Cloud Service Archive (CSAR) overview

4.1.1 CSAR structure

TOSCA YAML CSAR file is an archive file using the ZIP file format whose structure complies with the TOSCA Simple Profile YAML v1.1 Specification [2]. The CSAR file may have one of the two following structures:

- CSAR containing a *TOSCA-Metadata* directory, which includes the TOSCA.meta metadata file providing an entry information for processing a CSAR file as defined in TOSCA v1.0 specification [i.1].
- CSAR containing a single yaml (.yml or .yaml) file at the root of the archive. The yaml file is a TOSCA definition template that contains a metadata section with *template_name* and *template_version* metadata. This file is the CSAR Entry-Definitions file.

In addition, the CSAR file may optionally contain other directories with bespoke names and contents.

4.1.2 CSAR with TOSCA-Metadata directory

4.1.2.1 General

The TOSCA.meta metadata file includes *block_0* with the *Entry-Definitions* keyword pointing to a TOSCA definitions YAML file used as entry for parsing the contents of the overall CSAR archive.

Any TOSCA definitions files besides the one denoted by the *Entry-Definitions* keyword can be found by processing respective *imports* statements in the entry definitions file (or in recursively imported files).

Any additional artifacts files (e.g. scripts, binaries, configuration files) can be either declared explicitly through blocks in the TOSCA.meta file as described in TOSCA v1.0 specification [i.1] or pointed to by relative path names through artifact definitions in one of the TOSCA definitions files contained in the CSAR file.

Extension of the TOSCA.meta file is described in clause 4.1.2.2.

In order to indicate that the simplified structure (i.e. not all files need to be declared explicitly) of TOSCA.meta file allowed by TOSCA Simple profile YAML 1.0 [i.2] is used, the *CSAR-Version* keyword listed in block_0 of the meta-file denotes the version 1.1 as described in the below example. Otherwise the CSAR-Version keyword denotes the version 1.0 and all files are declared explicitly.

EXAMPLE:

```
TOSCA-Meta-File-Version: 1.0
CSAR-Version: 1.1
Created-by: Onboarding portal
Entry-Definitions: Definitions/ MainServiceTemplate.yaml
```

END OF EXAMPLE.

4.1.2.2 TOSCA.meta file extension

The TOSCA.meta file structure extension is used when files defined in clause 4.3.2 to 4.3.6 of the present document are included in the VNF package and when using CSAR with TOSCA-Metadata directory, as described in clause 4.1.2.1.

NOTE: TOSCA v1.0 specification [i.1] does not preclude the TOSCA.meta file block _0 to be extended with key value pairs.

4.1.2.3 TOSCA.meta file keynames extension

Table 4.1.2.3-1 specifies an extension of the list of recognized TOSCA.meta file keynames as specified in TOSCA-v1.0 specification [i.1] for the TOSCA.meta file. The keynames represents the entries for artifacts defined in clauses 4.3.2 to 4.3.6 of the present document and shall be located in the block_0.

Table 4.1.2.3-1: List of TOSCA-meta file keynames extensions

Keyname	Required	Type	Description
ETSI-Entry-Manifest	yes	string	Location of the Manifest file as defined in clause 4.3.2
ETSI-Entry-Change-Log	yes	string	Location of the Change history file as defined in clause 4.3.3
ETSI-Entry-Tests	no	string	Location of the Testing files as defined in clause 4.3.4
ETSI-Entry-Licenses	yes	string	Location of the Licensing information as defined in clause 4.3.5
ETSI-Entry-Certificate	no	string	Location of the Certificate file as defined in clause 4.3.6

NOTE: Use of the Entry-Manifest, Entry-Change-Log, Entry-Tests, Entry-Licenses and Entry-Certificate keynames defined in version 2.4.1 [i.7] to 2.5.1 [i.8] of the present document is deprecated. These keynames are only provided for backward compatibility with legacy VNF Package consumers; VNF package providers are warned that support of these keynames can be removed in subsequent versions of the present document.

EXAMPLE:

```
TOSCA-Meta-File-Version: 1.0
CSAR-Version: 1.1
Created-By: MyCompany
Entry-Definitions: MRF.yaml
ETSI-Entry-Manifest: MRF.mf
ETSI-Entry-Licenses: Files/Licenses
ETSI-Entry-Change-Log: Files/ChangeLog.txt
```

END OF EXAMPLE.

4.1.3 CSAR zip without TOSCA-Metadata directory

The yaml file at the root of the archive is the *CSAR Entry-Definition* file. The CSAR-Version is defined by the *template_version* metadata as can be seen in the below example.

EXAMPLE:

```
tosca_definitions_version: tosca_simple_yaml_1_1
metadata:
   template_name: MainServiceTemplate
   template_author: Onboarding portal
   template_version: 1.0
```

END OF EXAMPLE.

4.1.4 TOSCA Entry definition file metadata extension

4.1.4.1 Metadata keynames

Table 4.1.4.1-1 specifies an extension of the list of recognized metadata keynames as specified in TOSCA-Simple-Profile-YAML-v1.1 [2] for the main TOSCA Service Template.

Table 4.1.4.1-1: List of metadata keynames extensions

Keyname	Required	Type	Description
yang_definitions	no	string	Reference to a YANG definition file representing the VNFD within a VNF Package

4.1.4.2 Additional requirement

If a YANG-based VNFD is included in the VNF Package, the main TOSCA definitions YAML file shall include a metadata section with a metadata entry, where the keyname is "yang_definitions" and the value is the path to the YANG file representing the VNFD within the VNF Package. No additional contents shall be included in the main TOSCA definitions YAML file.

NOTE: The above requirement ensures that there cannot be both a YANG-based and a TOSCA-based representation of a VNFD in the same package.

EXAMPLE

```
tosca_definitions_version: tosca_simple_yaml_1_1
metadata:
template_name: MainServiceTemplate
template_author: Onboarding portal
template_version: 1.0
yang_definitions: Definitions/myvnfd.xml
```

END OF EXAMPLE

4.2 VNF package structure and format

The structure and format of a VNF package shall conform to the TOSCA Simple Profile YAML v1.1 Specification of the CSAR format [2].

NOTE: This implies that the VNF package can be structured according to any of the two options described in clause 4.1.

4.3 VNF package file contents

4.3.1 General

A VNF Package shall contain a main TOSCA definitions YAML file representing all or part of the VNFD, and additional files. It shall be structured according to one of the CSAR structure options described in clause 4.1.

NOTE 1: ETSI GS NFV-SOL 001 [i.4] specifies the structure and format of the VNFD based on TOSCA specifications.

NOTE 2: ETSI GS NFV-SOL 006 [i.6] specifies the structure and format of the VNFD based on YANG specifications.

If the option with a TOSCA-Metadata directory is used and the CSAR-Version parameter indicates version 1.0, all files that are contained in the archive shall be referenced from the TOSCA.meta file. If the CSAR-Version parameter indicates version 1.1, the files that are referenced and pointed to by relative path names through artifact definitions in one of the TOSCA definitions files (e.g. the VNFD) contained in the CSAR need not be declared in the TOSCA.meta file.

If a YANG-based VNFD is included in the VNF Package only the option without a TOSCA-Metadata directory is applicable.

Examples of VNF package options are described in annex A.

4.3.2 VNF package manifest file

A CSAR VNF package shall have a manifest file. The manifest file shall have an extension .mf and the same name as the main TOSCA definitions YAML file and be located at the root of the archive (archive without TOSCA-Metadata directory) or in the location specified by the TOSCA.meta file (archive with a TOSCA-Metadata directory). In the latter case, the corresponding entry shall be named "ETSI-Entry-Manifest".

The manifest file shall start with the VNF package metadata in the form of a name-value pairs. Each pair shall appear on a different line. The "name" and the "value" shall be separated by a colon and, optionally, one or more blanks.

The name shall be one of those specified in table 4.3.2-1 and the values shall comply with the provisions specified in table 4.3.2-1.

Table 4.3.2-1: List of valid names and values for VNF package metadata

Name	Value
vnf_provider_id	A sequence of UTF-8 characters See note 1.
vnf_product_name	A sequence of UTF-8 characters0 See note 1.
vnf_release_date_time	String formatted according to IETF RFC 3339 [3].
vnf_package_version	A string See note 2.
NOTE 1: The value shall be identical to those specified in the VNFD. NOTE 2: The value shall be identical to the vnfdVersion attribute specified in the VNFD.	

An example of valid manifest file metadata entries follows.

EXAMPLE 1:

```
metadata:
vnf_product_name: vMRF
vnf_provider_id: Acme
vnf_package_version: 1.0
vnf_release_date_time: 2017-01-01T10:00:00+03:00
```

END OF EXAMPLE 1.

The manifest file shall include a list of all files contained in or referenced from the VNF package with their location, expressed using a Source: location/name key-value pair. The manifest file itself may be included in the list.

Below is an example of valid manifest file entries for files contained in or referenced from the VNF package.

EXAMPLE 2:

```
Source: MRF.yaml

Source: scripts/install.sh

Source: https://www.vendor_org.com/MRF/v4.1/scripts/scale/scale.sh
```

END OF EXAMPLE 2.

If the VNF package refers to external files, the manifest file shall contain digests of individual files in the package, both local files contained in the package and external files referenced in the package.

If the VNF package does not refer to external files, the manifest files may contain digests of individual files contained in the package. If the manifest file does not include digests, the complete CSAR file shall be digitally signed by the VNF provider. A consumer of the VNF package verifies the digests in the manifest file by computing the actual digests and comparing them with the digests listed in the manifest file.

The manifest file, or alternatively, the signature of the CSAR file, is the key for decision regarding a VNF package integrity and validity in terms of its contained artifacts. The specification of the manifest file and specific algorithms used in digest creation and validation is described in the security related clause.

The details of specifying the local or externally located files and their security protection are described in clause 5.

4.3.3 VNF package change history file

A CSAR VNF package shall have a humanly readable text file describing any change in the constituency of the VNF package. All the changes in the VNF package shall be versioned, tracked and inventoried in the change history file.

The VNF package change history file shall be named "ChangeLog.txt" and be located at the root of the archive (archive without TOSCA-Metadata directory) or in the location specified by the TOSCA.meta file (archive with a TOSCA-Metadata directory). In the latter case, the corresponding entry shall be named "ETSI-Entry-Change-Log".

4.3.4 VNF package testing files

To enable VNF package validation, a VNF Provider should include in a VNF package files containing necessary information (e.g. test description) in order to perform VNF testing. The contents of VNF testing information is outside the scope of the present document.

The VNF testing information shall be located in a directory named "Tests" located at the root of the archive (archive without TOSCA-Metadata directory) or in the location specified by the TOSCA.meta file (archive with a TOSCA-Metadata directory). In the latter case, the corresponding entry shall be named "ETSI-Entry-Tests".

4.3.5 VNF package licensing information

As required in ETSI GS NFV-IFA 011 [1] the VNF package shall contain license information for the released VNF. The license information shall include a single license term for the whole VNF. In addition the license information may also include license terms for each of the VNF package artifacts if different from the one of the released VNF.

The VNF licensing information shall be located in a directory named "Licenses" located at the root of the archive (archive without TOSCA-Metadata directory) or in the location specified by the TOSCA.meta file (archive with a TOSCA-Metadata directory). In the latter case, the corresponding entry shall be named "ETSI-Entry-Licenses".

4.3.6 Certificate file

If the manifest file is signed by the VNF provider (see option 1 in clause 5.1), the CSAR VNF package shall contain a certificate file if the certificate is not included in the signature container (see note) within the manifest file. In this case or if a single certificate is provided for the signature of multiple artifacts (see clause 5.4), the certificate file shall have an extension .cert and the same name as the main TOSCA definitions YAML file and be located at the root of the archive (archive without TOSCA-Metadata directory) or in the location specified by the TOSCA.meta file (archive with a TOSCA-Metadata directory). In the latter case, the corresponding entry shall be named "ETSI-Entry-Certificate".

NOTE: Signature container refers to a structure in a standard format (e.g. CMS) which contains signature and additional data needed to process the signature (e.g. certificates, algorithms, etc.).

If the complete CSAR file is signed by the VNF provider (see option 2 in clause 5.1), the certificate file shall be contained in a zip file together with the CSAR file and the signature file if the certificate is not included in the signature file. The certificate file shall have an extension .cert and the same name as the CSAR file.

4.3.7 Non-MANO artifact sets in a VNF package

As required in ETSI GS NFV-IFA 011 [1] the VNF package shall allow to store and identify non-MANO artifact sets in the VNF package file.

Every non-MANO artifact set shall be identified by a non-MANO artifact set identifier which shall be registered in the registry (specified in annex B). A non-MANO artifact set identifier shall be a string that consists of sub-strings which shall not contain characters other than the following: digits (0-9), lowercase ASCII characters (a-z), and the special characters underscore "_" and dash "-". Sub-strings shall be separated by the dot "." character.

All files belonging to the same non-MANO artifact set shall share a common path prefix other than the root of the package.

Non-MANO artifact sets shall be declared in the manifest file. If the package contains at least one non-MANO artifact set, an entry named "non_mano_artifact_sets:" shall be present in the package on its own line after the "metadata" section that is defined in clause 4.3.2. The section defined by the "non_mano_artifact_sets" keyname shall have the following structure:

- Every non-MANO artifact set shall be declared on its own line, by a key name that is equal to the non-MANO artifact set identifier.
- Below the key name, all artifacts that belong to the non-MANO artifact set shall be listed, each on its own line, starting with key name "Source", followed by a colon (":") and, optionally, one or more blanks, and further followed by a file name with path for a file in the CSAR archive that is not contained in the root of this archive.

If the Manifest file provides the integrity assurance of the VNF package (option 1 in clause 5.1), these artifacts shall also appear in the list of blocks of name-value pairs specified in clause 5.3.

An example of the section that declares the non-MANO artifact sets in the package is provided below.

EXAMPLE:

```
non_mano_artifact_sets:
   foo_bar:
      Source: foobar/foo/foo.yaml
      Source: foobar/foo/foo.script
      Source: foobar/bar/descriptor.xml
   prv.happy-nfv.cool:
      Source: happy/cool/123.html
      Source: happy/cool/cool.json
      Source: happy/cool/hot/hot_or_cool.json
```

END OF EXAMPLE.

5 Adding security to TOSCA CSAR

5.1 VNF package authenticity and integrity

As specified in ETSI GS NFV-IFA 011 [1] a VNF package shall support a method for authenticity and integrity assurance.

In order to provide the public key based authenticity and integrity for the whole VNF package one of the two following options shall be followed:

Option 1: The VNF package shall contain a Digest (a.k.a. hash) for each of the components of the VNF package. The table of hashes is included in the manifest file, which is signed with the VNF provider private key. In addition, the VNF provider shall include a signing certificate that includes the VNF provider public key, following a pre-defined naming convention and located either at the root of the archive or in a predefined location (e.g. directory).

The certificate may also be included in the signature container, if the signature format allows that. For example, the CMS format allows to include the certificate in the same container as the signature.

Option 2: The complete CSAR file shall be digitally signed with the VNF provider private key. The VNF provider delivers one zip file consisting of the CSAR file, a signature file and a certificate file that includes the VNF provider public key. The certificate may also be included in the signature container, if the signature format allows that.

In option 2, the VNF package delivered would therefore be according to figure 5.1-1.

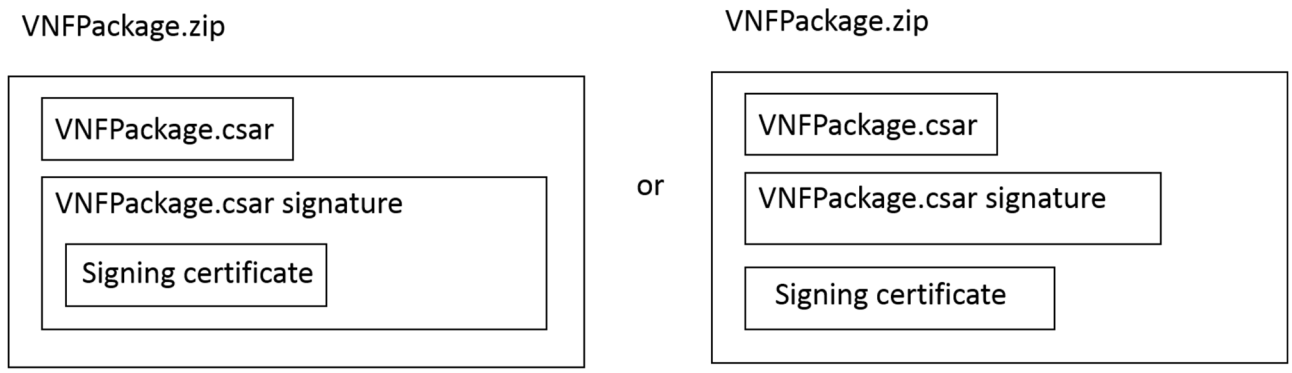

Figure 5.1-1: Composition of the VNF Package zip file in option 2

Option 2 is only valid if all artifacts are included in the package, i.e. no external artifacts are referenced in the package.

This solution, either option 1 or option 2, relies on the existence in the NFVO of a root certificate of a trusted CA that shall have been delivered via a trusted channel that preserves its integrity (separate from the VNF package) to the NFVO and be pre-installed in the NFVO before the on-boarding of the VNF package.

NOTE: The present document makes no assumption on who this trusted CA is. Furthermore, it does not exclude that the root certificate be issued by the VNF vendor or by the NFVI provider.

5.2 VNF package manifest and certificate files

In option 1 (see clause 5.1) the manifest file provides the VNF package integrity assurance. In this option the manifest contains the digests (hashes) for each individual file locally stored within the VNF package or referenced from it. Each file related entry of the manifest file includes the path or URI of the individual file, the hash algorithm and the generated digest. A consumer of the VNF package shall verify the digests in the manifest file by computing the actual digests and comparing them with the digests listed in the manifest file.

In option1 the VNF package authenticity is ensured by signing the manifest file with the VNF provider private key. The digital signature is stored in the manifest file itself (see clause 5.3). The VNF provider shall include an X.509 certificate [8] in the VNF Package. The certificate shall be either placed in a certificate file with extension .cert or, if the chosen signature format allows it, the certificate may be included in the signature container itself. The certificate provides the VNF provider public key. In a CSAR file without metadata directory the .cert file shall have the same name as the TOSCA definitions YAML file and be located at the root of the archive (archive without TOSCA-Metadata directory). In a CSAR file with a metadata directory, the .cert file shall be placed or in the location specified by the TOSCA.meta file (archive with a TOSCA-Metadata directory). In the latter case, the corresponding entry shall be named "ETSI-Entry-Certificate".

In option 2 (see clause 5.1), the VNF package authenticity and integrity is ensured by signing the CSAR file with the VNF provider private key (option 2 in clause 5.1). The digital signature is stored in a separate file. The VNF provider shall also include an X.509 certificate in a separate file with extension .cert or, if the signature format allows it, in the signature file itself. The VNF provider creates a zip file consisting of the CSAR file, signature and certificate files. The signature and certificate files shall be siblings of the CSAR file with extensions .cms and .cert respectively.

In this alternative (option 2 in clause 5.1) it is not required to include digests (hashes) per each individual file or artefact in the manifest file but it is recommended to include individual signatures of the artifacts (see clause 5.4). A consumer of the VNF package can verify the signature of the complete CSAR package with the VNF provider public key.

Table 5.2-1 summarizes the characteristics of the two possible options for integrity assurance.

Table 5.2-1: Options for VNF Package integrity assurance: summary of characteristics

Options	Digest per artifact	Signature per artifact	Support external artifacts	Signature as part of the manifest file	External Signature file for the whole CSAR	Certificate may be part of the signature	Certificate may be in a separate file
Option 1	Yes	Yes (allowed)	Yes	Yes	No	Yes	Yes
Option 2	No	Yes (recommended)	No	No	Yes	Yes	Yes

The X.509 certificate may contain one single signing certificate or a complete certificate chain. The root certificate that may be present in this X.509 certificate file shall not be used for validation purposes. Only trusted root certificate pre-installed in NFVO shall be used for validation (see clause 5.1).

5.3 Conventions in the manifest file

When the Manifest file provides the integrity assurance of the VNF package (option 1 in clause 5.1) it shall contain a list of blocks of name-value pairs, where each block is related to one file in the VNF package, where name and value are separated by a colon and, optionally, one or more blanks. Each block shall contain the following three name-value pair attributes:

- Source: identifier of the file used as input to the hash generation algorithm. The source can be either:
  - A file name for a file that is contained in the root of the CSAR archive.

  - A file name with path for a file in the CSAR archive that is not contained in the root of this archive.
  - A URI to an externally accessible artifact.

- Algorithm: name of a well-known algorithm used to generate the hash.
- Hash: text string corresponding to the hexadecimal representation of the hash.

The value for the Algorithm name-value pair shall be among those registered by IANA for hash function textual names [4]. VNF packages that comply with the present document shall either use "sha-256" or "sha-512".

Including the hash algorithm in each entry is optional if it is communicated by other means.

If option 1, as defined in clause 5.1, applies, the manifest file shall be signed. Otherwise signing the manifest file is optional. When the manifest file is signed, the signature shall be included at the end of the file. The signature and all necessary data to interpret it (algorithm used to generate the hash and encryption method) shall be included in a structure in a standard format following digital signatures best practices and encoded in a textual representation according to IETF RFC 7468 [6]. The format shall be among those registered by IANA for mime types [7] (e.g. "cms", "pkcs8", etc.).

Example of valid manifest file entries including manifest signature in CMS format.

EXAMPLE:

```
Source: MRF.yaml
Algorithm: SHA-256
Hash: 09e5a788acb180162c51679ae4c998039fa6644505db2415e35107d1ee213943

Source: scripts/install.sh
Algorithm: SHA-256
Hash: d0e7828293355a07c2dccaaa765c80b507e60e6167067c950dc2e6b0da0dbd8b

Source: https://www.vendor_org.com/MRF/v4.1/scripts/scale/scale.sh
Algorithm: SHA-256
Hash: 36f945953929812aca2701b114b068c71bd8c95ceb3609711428c26325649165

-----BEGIN CMS-----
MIGDBgsqhkiG9w0BCRABCaB0MHICAQAwDQYLKoZIhvcNAQkQAwgwXgYJKoZIhvcN
AQcBoFEET3icc87PK0nNK9ENqSxItVIoSa0o0S/ISczMs1ZIzkgsKk4tsQ0N1nUM
dvb05OXi5XLPLEtViMwvLVLwSE0sKlFIVHAqSk3MBkkBAJv0Fx0=
-----END CMS-----
```

END OF EXAMPLE.

5.4 Signature of individual artifacts

The VNF provider may optionally digitally sign some or all artifacts individually, in particular software images. This option exists for both option 1 and option 2 described in clause 5.1 but it is recommended when no individual hashes per artifact are included (i.e. in option 2 in clause 5.1). In this case a signature file in standard format (e.g. CMS, PKCS#7) will accompany the signed artifact. The signature file shall have the same name (different extension) as the signed artifact and be a sibling of it, i.e. placed in the same folder in the archive, which could also be the root of the archive.

A certificate shall also be included in the VNF package as per one of the two following alternatives:

- One certificate per signed artifact:
  Either a certificate file with extension .cert is included as a sibling of the signed artifact file, i.e. placed in the same folder as the signed artifact and having the same name (different extension) or the certificate is included in the signature file, provided that the signature format allows for it. This alternative allows to have different certificates per different artifacts, which may be needed e.g. if artifacts contained in the package are signed by 3rd party providers.

- One single certificate for all signed artifacts:
  One certificate file with extension .cert and the same name as the main TOSCA definitions YAML file and located at the root of the archive (archive without TOSCA-Metadata directory) or in the location specified by the TOSCA.meta file (archive with a TOSCA-Metadata directory). In the latter case, the corresponding entry shall be named "ETSI-Entry-Certificate".

Signing software images allows the VNF provider to ensure their integrity and authenticity until they are loaded in a VNFC instances at boot time.

If software images or other artifacts are not signed by the VNF provider, the service provider has the option, after having validated the VNF Package, to sign them before distributing the different package components to different function blocks or the NFVI in order to preserve their integrity within the cloud domain.

5.5 Support for security sensitive artifacts

If an artifact is security sensitive, the whole artifact may be encrypted by the VNF provider with an artifact specific key. In case of asymmetric encryption this key is a public key provided by the party who is responsible to on-board and validate the VNF package or to use the artifact, and the VNF provider uses it to encrypt the security sensitive artifact. The consumer of this artifact then decrypts the artifact with its own private key.

In case of symmetric encryption, the public key provided by the party responsible to on-board and validate the VNF package or to use the artifact is used to encrypt a key generated by the VNF provider. The artifact is encrypted with this latter key, which is to be shared with the consumer of the artifact and shall be included in encrypted form in the VNF package. The consumer of the artifact decrypts the shared key with its own private key and then uses the obtained shared key to decrypt the artifact.

In this scenario the encrypted artifact shall be delivered in a CMS file [5], which provides all necessary information to decrypt it: algorithm used for the artifact encryption, encrypted key used for artifact encryption and algorithm used to encrypt the key.

The encryption of an artifact occurs prior to the generation of a digest (hash) for the artifact.

Annex A (informative): TOSCA CSAR examples

A.1 CSAR with the TOSCA-Metadata directory

Below is an example of a CSAR directory structure for NFV including the TOSCA-Metadata, Definitions, Files and Scripts directories. The TOSCA-Metadata directory contains the TOSCA.meta file as specified in [i.1]. The VNFD (MRF.yaml) and other templates files, if any, are included in the Definitions directory. The Files directory contains the change log file, images and other artifact files. The Scripts directory includes the scripts files that may be called from the VNFD. The manifest file (MRF.mf) is located at the root level of the archive.

EXAMPLE:

```
!------TOSCA-Metadata
         !------TOSCA.meta

!------Definitions
         !----- MRF.yaml
         !----- OtherTemplates (e.g. type definitions)

!------Files
         !----- ChangeLog.txt
         !----- MRF.cert
         !----- image(s)
         !----- other artifacts
         !------Tests
         !----- file(s)
         !------Licenses
         !----- file(s)
!------Scripts
         !----- install.sh
!----- MRF.mf
```

END OF EXAMPLE.

A.2 CSAR without the TOSCA-Metadata directory

Below is the example of CSAR including the VNFD (MRF.yaml), manifest, certificate, testing, licensing and change log files located at the root level of the CSAR. The Artifacts directory includes the two scripts files that may be called from the VNFD.

EXAMPLE:

```
!--------- MRF.yaml

!---------  MRF.mf

!---------  MRF.cert

!---------  ChangeLog.txt

!--------- Tests

         !----- file(s)

!--------- Licenses

         !----- file(s)

!--------- Artifacts

         !----- install.sh

         !----- start.yang
```

END OF EXAMPLE.

A.3 CSAR with the YANG VNFD without TOSCA.meta directory

Below is an example of CSAR including the VNFD (CompanyVNFD.xml), a main TOSCA definition YAML file with metadata only (**CompanyVNFD.yaml)**, manifest, certificate, licensing and change log files located at the root level of the CSAR. The Scripts directory includes one script file that may be called from the VNFD. This example does not preclude having other YAML files at other locations than the root of the CSAR file.

EXAMPLE:

```
!——— CompanyVNFD.yaml

!——— CompanyVNFD.xml

!——— CompanyVNFD.mf

!——— CompanyVNFD.cert

!---- ChangeLog.txt

!-----Files

!— Instance Data Files
!— start.xml

!--------- Licenses

!--------- Scripts

!----- install.sh
```

END OF EXAMPLE.

Annex B (normative): Non-MANO artifact sets registry

B.1 General

Non-MANO artifact set identifiers shall be registered in the ETSI NFV registry of VNF package non-MANO artifact sets [i.5]. The registry has a private and a public part.

In the private part of the registry, e.g. vendor and product specific non-MANO artifact sets are registered. The private part is open to anybody.

In the public part, non-MANO artifact sets that have been documented by a standards-developing organization or industry forum in a publicly available specification are registered.

The allocation of the non-MANO artifact set identifiers is made on a first-come first-served basis.

B.2 Non-MANO artifact set identifier format

A non-MANO artifact set identifier shall be a string that shall comply with the following rules:

- For private non-MANO artifact sets , the identifier shall be the concatenation of: `"prv." <registrant> "." <specificPart>`.
- For public non-MANO artifact sets , the identifier shall be: `<specificPart>`.
- <registrant> and <specificPart> shall be strings that comply with the provisions defined in clause 4.3.7.
- <registrant> shall be a string that represents the registrant (e.g. the company or organization name) chosen at registration time.
- <specificPart> shall be a string that represents the non-MANO artifact set. For private non-MANO artifact sets, this string is scoped by <registrant>.

NOTE: The registration authority has the final right to accept or reject <registrant> and <specificPart> strings as part of the registry governance.

B.3 Registered information

The primary elements of the registry are:

Registered identifier

- nonManoArtifactSetId: Identifier of the non-MANO artifact set (mandatory). This identifier includes information whether the identifier is in the "public" or "private" part of the registry.

Registrant information

- Registrant Name: Name of the company or organization registering the non-MANO artifact set (mandatory).
- Previous Registrant Name(s): Name or names of the company or organization to whom the registered identifier has belonged previously, e.g. due to buyout, merger, acquisition (optional).

NOTE: It is assumed that the registration authority will manage further information related to the identity of the registrant (e.g. contact information).

Additional information

- Non-MANO Artifact Set Name: Name of the non-MANO artifact set (any string, mandatory).
- Description: General description of the non-MANO artifact set (any string, optional).
- Specification URI: Publically reachable URI of the specification that defines the non-MANO artifact set. Needs to be long-lived. (Mandatory for the public part, recommended for the private part).
- Registration Date: Date of the registration (mandatory).

B.4 Initial registration

B.4.1 Template

During initial registration, the information in the template defined in clause B.4.2 shall be provided.

B.4.2 Template

1 Non-MANO artifact set information

Artifact Set Name [M]	<Name of the non-MANO artifact set that is being registered>
Description [O]	<General description of the non-MANO artifact set that is being registered>
Specification reference [M/O]	<Publically reachable reference (such as a long-lived URI) of a specification that defines the non-MANO artifact set.> Mandatory for the public part, recommended for the private part of the registry.

2 Registration information

Registrant name [M]	<Name of the legal entity requesting registration>
Registrant address [M]	<Address of the legal entity requesting registration>
Registrant contact [M]	<Name and email address of the contact person or the function of the legal entity requesting registration>
Registration date [M]	<The date when the registration request was sent>

3 Requested non-MANO artifact set identifier

Either a private or a public identifier but not both shall be registered. The syntax requirements for sub-strings of the registered identifier are defined in clause 4.3.7 and are reproduced here for convenience: Each of these fields may contain digits (0-9), lowercase ASCII characters (a-z), and the special characters underscore "_" and dash "-", and shall not contain any other characters.

3.1 Alternative 1: Private non-MANO artifact set identifier

The private part of the registry is open to anybody, and allows to register, e.g. vendor and product specific non-MANO artifact sets.

Constant		Registrant		Specific part
prv	.		.	

3.2 Alternative 2: Public non-MANO artifact set identifier

The public part of the registry allows to register non-MANO artifact sets that have been documented by a standards-developing organization or industry forum in a publicly available specification.

Specific part

B.5 Registration update

Only limited parts of the registration information are allowed to be updated:

- Registrant name (in case of mergers, etc.). In this case, the registrant information will be updated and the previous registrant information will be preserved in a special "previous registrants" section.
- Registrant contact data (in case of change of contact person).
- Specification URI (in case of update of URI).

Annex C (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Andrei Kojukhov, Amdocs

Other contributors:
Arturo Martin de Nicolas, Ericsson

Bruno Chatras, Orange

Dan Druta, AT&T

Dmytro Gassanov, Netcracker

Ernest Bayha, Ericsson

Haibin Chu, Ericsson

Juan Postlbauer, HPE

Mahesh Jethanandani, VMWare

Marcus Brunner, Swisscom

Michael Brenner, GigaSpaces

Shitao Li, Huawei

Thinh Nguyenphu, Nokia

Uwe Rauschenbach, Nokia

Zohar Sacks, Amdocs

Annex D (informative): Change History

Date	Version	Information about changes
November 2016	0.0.1	Initial version based on: - NFVSOL(16)000150r2_ETSI_GS_NFV_SOL004_ToC - NFVSOL(16)000151R1_ETSI_GS_NFV_SOL004_Scope - NFVSOL(16)000152R1_ETSI_GS_NFV_SOL004_Normative_References
January 2017	0.0.2	Second version based on: - NFVSOL(17)000025r2_ETSI_GS_NFV_SOL004_Normative text for CSAR Structure options - NFVSOL(16)000188R4_ETSI_GS_NFV_SOL004_Adding content to 4.1 TOSCA YAML Cloud Service Archive (CSAR) Overview - NFVSOL(16)000189R1_ETSI_GS_NFV_SOL004_ Adding Informative References
February 2017	0.0.3	Third version based on: - NFVSOL(17)000018r5_ SOL004 6. Adding Security to TOSCA CSAR - NFVSOL(17)000063r4_ SOL004 Optional Support for Security Sensitive Artifacts - NFVSOL(17)000068r3_ SOL004 CSAR Format and Conventions - NFVSOL(17)000069r2_ SOL004 Consistency between TOSCA CSAR file contents and TOSCA VNFD content - NFVSOL(17)000108r3_ SOL004 - Adding Security to VNF package - merge of contributions 71r1 and 75
March 2017	0.0.4	Fourth version based on: - NFVSOL(17)000117r1_ SOL004 Annex A: CSAR example without the TOSCA-Metadata directory - NFVSOL(17)000070r4_ SOL004 Test Files in VNF package - NFVSOL(17)000140r4_ SOL004 Manifest File Signature - NFVSOL(17)000134r2_SOL004 Annex A: CSAR example with the TOSCA-Metadata directory - NFVSOL(17)000164r1_SOL004 Licensing Agreement in VNF package
May 2017	0.0.5	Fifth version based on: - NFVSOL(17)000248r1_SOL004_-_Editorial_changes - NFVSOL(17)000249r1_SOL004_-_Clause_3_-_Fixing_Definitions_and_Abbreviations - NFVSOL(17)000250_SOL004_-_Clause_5_-_Removal_of_the_clause 5 - NFVSOL(17)000253r2_SOL004_VNF_manifest_metadata - NFVSOL(17)000259r1_SOL004_-_Clause_6_3_-_Hash_Algorithms - NFVSOL(17)000272r3_SOL004_symmetric_encryption - NFVSOL(17)000273r1_SOL004_Description_of_signature_field - NFVSOL(17)000274_SOL004_-_Clause_6_4_-_Removal_of_superfluous_text - NFVSOL(17)000275_SOL004_-_Clause_6_3_-_Miscellaneous_improvements - NFVSOL(17)000277r1_SOL004_-_Clause_4_1_-_Miscellaneous_improvements - NFVSOL(17)000278r1_SOL004_-_Clause_4_2_-_4_3__-_Miscellaneous_improvements - NFVSOL(17)000353_SOL004__Removing_The_Note - NFVSOL(17)000279r3_SOL004_-_Clause_4__-_Clause_6_-_Naming_conventions_and_file_ - NFVSOL(17)000357_SOL004_Naming_Conventions_for_Testing_Files - NFVSOL(17)000290r2_SOL004_Clause_4_3_4_VNF_package_testing - NFVSOL(17)000215r3_SOL004_Signature_of_the_CSAR_file - NFVSOL(17)000216r2_SOL004_Signature_of_individual_artifacts - NFVSOL(17)000251r1_SOL004_-_Annex_A_-_Harmonization

Date	Version	Information about changes
May 2017	0.1.0	Sixth version based on: - NFVSOL(17)000286R2SOL004_Clause_4_3_2_others_VNF_Package_user_consumer - NFVSOL(17)000287R3SOL004_Clause_2_1_normative_reference_missing - NFVSOL(17)000369R2 SOL004 5.4 shared key for symmetric encryption - NFVSOL(17)000184r3 - SOL004 Root Certificate
December 2017	2.3.2	A first maintenance version is based on: - NFVSOL(17)000585r3_SOL004 3rd party VNF Package extensions
April 2018	2.4.2	A second maintenance version is based on: - NFVSOL(18)000092r1_ SOL004ed251: Updates to clause 4.3.2
July 2018	2.4.3	A third maintenance version is based on: - NFVSOL(18)000232_SOL004ed251: Add clarifying note to the description of the vnf_package_version in clause 4.3.2 - NFVSOL(18)000278_ SOL004ed251: Remove semantics of vnf_package_version consistent with SOL001 and SOL003 - NFVSOL(18)000307r2_ SOL004 Registration template - NFVSOL(18)000354r3_ SOL004 Additions and improvements - NFVSOL(18)000435_ SOL004_Multi-files VNFD
November 2018	2.5.2	Release 2 maintenance version is based on: - NFVSOL(18)000668 Correcting a wrong file suffix - NFVSOL(18)000669 Correcting a date/time format - NFVSOL(18)000670 Updating references to TOSCA YAML specs - NFVSOL(18)000671r2 SOL004 - Clarifying the using of a list of artifacts in Manifest file
December 2018	2.5.3	Release 2 maintenance version is based on: - NFVSOL(18)000672r8_SOL004_-_Adding_support_for_YANG_VNFD_
March 2019	2.5.4	Release 2 maintenance version is based on: - NFVSOL(19)000091r5_SOL004ed261_TOSCA_meta_file

History

Document history		
V2.3.1	July 2017	Publication
V2.4.1	February 2018	Publication
V2.5.1	September 2018	Publication
V2.6.1	April 2019	Publication