ETSI GS NFV-SOL 007 V2.5.1 (2018-12)

Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; Network Service Descriptor File Structure 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
DGS/NFV-SOL007

Keywords
data, information model, model, NFV,
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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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 2018.
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 of the Network Service Descriptor (NSD) file archive and the naming conventions for the different files it contains, fulfilling the requirements specified in ETSI GS NFV-IFA 014 [1] for an NSD file structure.

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 014: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Network Service Templates Specification".

[2] TOSCA-Simple-Profile-YAML-v1.2-csprd01: "TOSCA Simple Profile in YAML Version 1.2".

NOTE: Available at http://docs.oasis-open.org/tosca/TOSCA-Simple-Profile-YAML/v1.2/csprd01/TOSCA-Simple-Profile-YAML-v1.2-csprd01.pdf.

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

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

[5] IANA register for Hash Function Textual Names.

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

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

[9] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

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] TOSCA-v1.0-os: "TOSCA Version 1.0".

[i.2] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.3] ETSI GS NFV-SOL 001: "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; NFV descriptors based on TOSCA specification".

3 Definition of terms and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS NFV 003 [i.2] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.2] and the following apply:

CA	Certificate Authority
CMS	Cryptographic Message Syntax
CSAR	Cloud Service ARchive
IANA	Internet Assigned Number Association
TOSCA	Topology and Orchestration Specification for Cloud Applications
URI	Universal Resource Identifier
UTF	Unicode Transformation Format
YAML	YAML Ain't Markup Language

4 NSD file structure

4.1 TOSCA YAML Cloud Service Archive (CSAR)

A TOSCA YAML CSAR file is an archive file using the ZIP file format whose structure complies with the TOSCA Simple Profile in YAML version 1.2 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.

4.2 NSD file structure and format

The structure and format of an NSD file archive shall conform to the TOSCA Simple Profile in YAML version 1.2 specification of the CSAR format [2].

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

4.3 NSD file contents

4.3.1 General

An NSD file archive shall contain the NSD as the main TOSCA definitions YAML file, and additional files, and shall be structured according to one of the CSAR structure options described in clause 4.1.

NOTE: ETSI GS NFV-SOL 001 [i.3] specifies the structure and format of the NSD based on TOSCA 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 NSD) contained in the CSAR need not be declared in the TOSCA.meta file.

Examples of NSD file archive options are described in annex A.

4.3.2 NSD file archive manifest file

A CSAR NSD file archive shall contain 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 "Entry-Manifest".

The manifest file shall start with the NSD file archive 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. 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 NSD file archive metadata

Name	Value
nsd_designer	A sequence of UTF-8 [9] characters. See note 1.
nsd_invariant_id	A sequence of UTF-8 [9] characters. See note 1.
nsd_name	A sequence of UTF-8 [9] characters. See note 1.
nsd_release_date_time	String formatted according to IETF RFC 3339 [3].
nsd_file_structure_version	A string. See note 2.
NOTE 1: The value shall be identical to that specified in the NSD. NOTE 2: The value shall be identical to the version attribute specified in the NSD.	

An example of valid manifest file metadata entries follows.

EXAMPLE:

```
metadata:
nsd_designer: Mycompany
nsd_invariant_id: Sunshine
nsd_name: Sunshine
nsd_file_structure_version: 1.0
nsd_release_date_time: 2018-04-08T10:00+08:00
```

END OF EXAMPLE

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

If the NSD file archive does not refer to external files, the manifest files may contain digests of the individual files contained in the archive. If the manifest file does not include digests, the complete CSAR file shall be digitally signed by the NS designer. A consumer of the NSD file archive 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 an NSD file archive 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.

4.3.3 NSD file archive change history file

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

The NSD file archive 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 "Entry-Change-Log".

4.3.4 Testing files in the NSD file archive

To enable NS validation, an NS designer should include in an NSD file archive, files containing necessary information (e.g. test description) in order to perform NS testing. The contents of NS testing information included in the NSD file archive is outside the scope of the present document.

The NS testing information in the NSD file archive 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 "Entry-Tests".

4.3.5 Certificate file

If the manifest file is signed by the NS designer (see option 1 in clause 5.1), the CSAR NSD file archive 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 "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 NS designer (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.

5 Adding security to TOSCA CSAR

5.1 NSD file archive authenticity and integrity

An NSD file archive shall support a method for authenticity and integrity assurance.

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

Option 1: The NSD file archive shall contain a Digest (a.k.a. hash) for each of files it contains. The table of hashes shall be included in the manifest file, which is signed with the NS designer private key. In addition, the NS designer shall include a signing certificate that includes the NS designer public key, following a predefined 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 NS designer private key. The NS designer delivers one zip file consisting of the CSAR file, a signature file and a certificate file that includes the NS designer public key. The certificate may also be included in the signature container, if the signature format allows that.

In option 2, the NSD file archive delivered would therefore be structured according to figure 5.1-1.

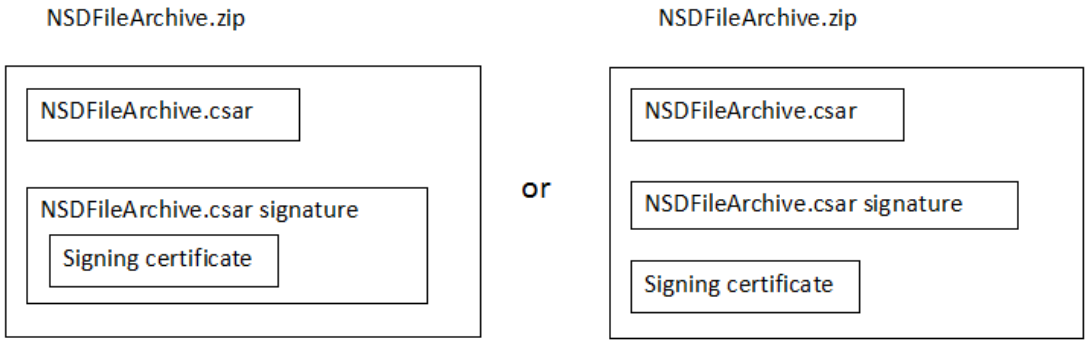

Figure 5.1-1: Composition of the NSD File Archive zip file in option 2

Option 2 is only valid if all artifacts are included in the NSD file archive, i.e. no external artifacts are referenced from the files contained in the NSD file archive.

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 NSD file structure) to the NFVO and be preinstalled in the NFVO before the on-boarding of the NSD file structure.

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 NS designer or by the NFVI provider.

5.2 Manifest and certificate files in the NSD file archive

In option 1 (see clause 5.1) the manifest file provides integrity assurance of the NSD file archive. In this option the manifest contains the digests (hashes) for each individual file locally stored within the NSD file archive 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 NSD file archive 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 option 1 authenticity of the NSD file archive is ensured by signing the manifest file with the NS designer private key. The digital signature is stored in the manifest file itself (see clause 5.3). The NS designer shall include an X.509 certificate [4] in the NSD file archive. 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 NS designer 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 "Entry-Certificate".

In option 2 (see clause 5.1), authenticity and integrity of the NSD file archive is ensured by signing the CSAR file with the NS designer private key (option 2 in clause 5.1). The digital signature is stored in a separate file. The NS designer 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 NS designer 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 artifact in the manifest file but it is recommended to include individual signatures of the artifacts (see clause 5.4). A consumer of the NSD file archive can verify the signature of the complete CSAR file with the NS designer public key.

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

Table 5.2-1: Options for NSD file archive 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 NSD file archive (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 NSD file archive, 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 [5]. An NSD file archive that complies 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 an archive 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: SunShine.yaml
Algorithm: SHA-256
Hash: ead2ca54bfd94b72fb210edb67049e8229e07760e7d69d771fea24c159cefda8

Source: scripts/install.sh
Algorithm: SHA-256
Hash: 16bb3cd7c2d685e0b6da9b1f3f67a11efba692d84f78c23f65f73a271be7726f

Source: https://www.designer_org.com/SunShine/v4.1/scripts/scale/scale.sh
Algorithm: SHA-256
Hash: 94fedf02af0c7f8d4974f0249d85575f167b48e3622bc9791a19eb7d5ce0d5de

-----BEGIN CMS-----

MIIFkwYJKoZIhvcNAQcCoIIFhDCCBYACAQExCTAHBgUrDgMCGjCCAacGCSqGSIb3
DQEHAaCCAZgEggGUU291cmNlOiBTdW5TaGluZS55YW1sDQpBbGdvcml0aG06IFNI
QS0yNTYNCkhhc2g6IGVhZDJjYTU0YmZkOTRiNzJmYjIxMGVkYjY3MDQ5ZTgyMjll
MDc3NjBlN2Q2OWQ3NzFmZWEyNGMxNTljZWZkYTgNCg0KU291cmNlOiBzY3JpcHRz
L2luc3RhbGwuc2gNCkFsZ29yaXRobTogU0hBLTI1Ng0KSGFzaDogMTZiYjNjZDdj
MmQ2ODVlMGI2ZGE5YjFmM2Y2N2ExMWVmYmE2OTJkODRmNzhjMjNmNjVmNzNhMjcx
YmU3NzI2Zg0KDQpTb3VyY2U6IGh0dHBzOi8vd3d3LmRlc2lnbmVyX29yZy5jb20v
U3VuU2hpbmUvdjQuMS9zY3JpcHRzL3NjYWxlL3NjYWxlLnNoDQpBbGdvcml0aG06
IFNIQS0yNTYNCkhhc2g6IDk0ZmVkZjAyYWYwYzdmOGQ0OTc0ZjAyNDlkODU1NzVm
MTY3YjQ4ZTM2MjJiYzk3OTFhMTllYjdkNWNlMGQ1ZGWgggIPMIICCzCCAZCgAwIB
AgIJAKGGlg5oMbwkMAoGCCqGSM49BAMCMEMxCzAJBgNVBAYTAmNuMQswCQYDVQQI
DAJqczELMAkGA1UEBwwCbmoxDDAKBgNVBAoMA3p0ZTEMMAoGA1UECwwDaG1mMB4X
DTE4MDMwOTA2NTQyNVoXDTI4MDMwNjA2NTQyNVowQzELMAkGA1UEBhMCY24xCzAJ
BgNVBAgMAmpzMQswCQYDVQQHDAJuajEMMAoGA1UECgwDenRlMQwwCgYDVQQLDANo
bWYwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAASJDqzsB3JidSB1RwqmtR2r12fqnVnp
rvEUQT/wxs+o8JfV7h2ywbXKm3HslE1gGQW+iYkOOPLquhXFp1TdTTrI0SeQ8p1t
Y5RX1Lh7P5su5DfRn5JEMQrhnNhQVOnlDyejUDBOMB0GA1UdDgQWBBSRS//oeOxs
m8wT3QuUHEkRBxRXWjAfBgNVHSMEGDAWgBSRS//oeOxsm8wT3QuUHEkRBxRXWjAM
BgNVHRMEBTADAQH/MAoGCCqGSM49BAMCA2kAMGYCMQC49ePO/17sVE7BMl+B6S78
DYFsSRHkp2RCFgY2Xi9ETdEujY1GgH3yLHz4D2QdRjwCMQDVAL1NhHBeDJR6hSdv
3QIEc8GUYLDjvTxrqEy4OJOgxrVZGV32ZZrH7w+irtH0fdkxggGwMIIBrAIBATBQ
MEMxCzAJBgNVBAYTAmNuMQswCQYDVQQIDAJqczELMAkGA1UEBwwCbmoxDDAKBgNV
BAoMA3p0ZTEMMAoGA1UECwwDaG1mAgkAoYaWDmgxvCQwBwYFKw4DAhqggdgwGAYJ
KoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMTgwOTA3MDMx
NTMzWjAjBgkqhkiG9w0BCQQxFgQU5M/XnNCoeTvXyE22n11tTh9Y30UweQYJKoZI
hvcNAQkPMWwwajALBglghkgBZQMEASowCwYJYIZIAWUDBAEWMAsGCWCGSAFlAwQB
AjAKBggqhkiG9w0DBzAOBggqhkiG9w0DAgICAIAwDQYIKoZIhvcNAwICAUAwBwYF
Kw4DAgcwDQYIKoZIhvcNAwICASgwCQYHKoZIzj0EAQRmMGQCMB7zcw46jub2JhHD
nQ6SGfqvMmBVOE+xDSboJ9WzCeVGzbclO56bNiB0PuwzmYV7ZAIwX/U/2l2lnhAd
/9UqRQKG6z/3WTd/Hm8MpRZSTEan0fPDfrPfU9sunvkV9JQ0Re2Z

-----END CMS-----
```

5.4 Signature of individual artifacts

The NS designer may optionally digitally sign some or all artifacts individually. 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 NSD file archive 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 NSD file archive are signed by 3-rd party designers.

- 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 "Entry-Certificate".

5.5 Support for security sensitive artifacts

If an artifact is security sensitive, the whole artifact may be encrypted by the NS designer 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 NSD file archive or to use the artifact, and the NS designer 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 NSD file archive or to use the artifact is used to encrypt a key generated by the NS designer. 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 NSD file archive. 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 [8], 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 archive including the TOSCA-Metadata, Definitions, Files and Scripts directories. The TOSCA-Metadata directory contains the TOSCA.meta file as specified in [i.1]. The NSD (Sunshine.yaml) and other templates files, if any, are included in the Definitions directory. The Files directory contains the change log file, certificate file and other artifact files. The Scripts directory includes the scripts files that may be called from the NSD. The manifest file (Sunshine.mf) is located at the root level of the archive.

EXAMPLE:

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

!------ Definitions
         !------ SunShine.yaml
         !------ Other Templates (e.g., type definitions)

!------ Files
         !------ ChangeLog.txt
         !------ Sunshine.cert
         !------ Other artifacts
         !------ Tests
                  !------ file(s)
         !------ Licenses
                  !------ file(s)

!------ Scripts
         !------ install.sh

!------ Sunshine.mf
```

END OF EXAMPLE.

A.2 CSAR without the TOSCA-Metadata directory

Below is the example of a CSAR directory structure including the NSD (Sunshine.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 NSD.

EXAMPLE:

```
!--------- Sunshine.yaml
!--------- Sunshine.mf
!--------- Sunshine.cert
!--------- ChangeLog.txt

!--------- Tests
         !----- file(s)

!--------- Licenses
         !----- file(s)

!--------- Artifacts
         !----- install.sh
         !----- start.yang
```

END OF EXAMPLE.

Annex B (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Manchang Ju, ZTE

Other contributors:
Ernest Bayha, Ericsson

Andrei Kojukhov, Amdocs

Bhumip Khasnabish, ZTE

Dmytro Gassanov, Netcracker

Jie Zhan, ZTE

Shitao Li, Huawei

Maopeng Zhang, ZTE

Baoguo Xie, ZTE

Bruno Chatras, Orange

Annex C (informative): Change History

Date	Version	Information about changes
April 2018	0.0.1	Initial version based on contributions that were agreed at the NFVSOL#57 meeting and during Email Approval (EA) following the NFVSOL#57. • NFVSOL(18)000105_ETSI_GS_NFV_SOL007_ToC • NFVSOL(18)000106_ETSI_GS_NFV_SOL007_Scope • NFVSOL(18)000107_ETSI_GS_NFV_SOL007_Normative_References
April 2018	0.0.2	Version 0.0.2 based on contributions that were agreed at the NFVSOL#60 meeting and during Email Approval (EA) following the NFVSOL#59 and NFVSOL#60 meetings. • NFVSOL(18)000140_SOL007_Adding_Normative_Reference • NFVSOL(18)000141_SOL007_Normative_text_for_CSAR_Structure_options • NFVSOL(18)000149_SOL007_Adding_4_1_TOSCA_YAML_CSAR • NFVSOL(18)000150_SOL007_Adding_Informative_References • NFVSOL(18)000151_SOL007_Clause_3_-_Fixing_Definitions_and_Abbreviations
August 2018	0.0.3	Version 0.0.3 based on contributions that were agreed at the NFVSOL#74 meeting and during Email Approval (EA) following the NFVSOL#61 and NFVSOL#74 meetings. • NFVSOL(18)000163_SOL007_Adding_NSD_file_contents_General • NFVSOL(18)000468r3_SOL007_NSD_file_structure_manifest_metadata • NFVSOL(18)000476r2_SOL007_Annex_A_CSAR_example_with_the_TOSCA-Metadata_director • NFVSOL(18)000480_SOL007_NSD_file_structure_change_history_file
September 2018	0.1.0	Version 0.1.0 based on contributions that were agreed at the NFVSOL#78 meeting and during Email Approval (EA) following the NFVSOL#75 and NFVSOL#77 meetings. • NFVSOL(18)000484r2_SOL007_NSD_file_structure_testing_files • NFVSOL(18)000509_SOL007_Adding_security_to_TOSCA_CSAR • NFVSOL(18)000512_SOL007_NSD_file_structure_authenticity and integrity_option2 • NFVSOL(18)000513_SOL007_Support_for_security_sensitive_artifacts • NFVSOL(18)000527_SOL007_Conventions_in_the_manifest_file • NFVSOL(18)000531_SOL007_Signature_of_individual_artifacts • NFVSOL(18)000532_SOL007_Certificate_file • NFVSOL(18)000533_SOL007_Clause_5_2_manifest_and_certificate_files
October 2018	0.2.0	Version 0.2.0 based on contributions that were agreed at the NFVSOL#79 meeting and during Email Approval (EA) following the NFVSOL#81 meeting. • NFVSOL(18)000568_SOL007_Annex_A_CSAR_example_without_the_TOSCA-Metadata_director • NFVSOL(18)000597_SOL007_-_Various_Wording_Improvements

History

Document history		
V2.5.1	December 2018	Publication