ETSI GS NFV-IFA 033 V5.2.1 (2024-12)

Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Reference points related to Security Manager and Certificate Management Function - Interface and Information Model 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-IFA033ed521

Keywords
cyber security, interface, management, MANO,
NFV, orchestration, 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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies the requirements applicable to the interfaces supported over reference points as well as the operations invoked over these interfaces related to Security Management and Certificate Management. The purpose of the interfaces is to support security monitoring and management as specified in ETSI GS NFV-SEC 013 [i.3] and ETSI GS NFV-IFA 026 [4], and to support the certificate management functions as specified in ETSI GS NFV-IFA 026 [4].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[2] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[3] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

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

[5] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[6] IETF RFC 2986: "PKCS #10: Certification Request Syntax Specification Version 1.7".

[7] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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] Void.

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

[i.3] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.4] Void.

[i.5] Void.

[i.6] ETSI GS NFV-SOL 003: "Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; RESTful protocols specification for the Or-Vnfm Reference Point".

[i.7] ETSI GS NFV 006: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Architectural Framework Specification".

[i.8] ETSI GR NFV-SEC 005: "Network Functions Virtualisation (NFV); Trust; Report on Certificate Management".

[i.9] ISO/IEC 9646-7: "Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements".

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.2] and ETSI GS NFV-IFA 026 [4] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI GR NFV 003 [i.2].

CMF	Certificate Management Function
FQDN	Fully Qualified Domain Name
HMEE	Hardware Mediated Execution Enclave
HSM	Hardware Security Module
OID	Object IDentifier
PSF	Passive, Semi-Active or Fully-Active
SF	Semi-Active or Fully-Active
SM	Security Manager
TPM	Trusted Platform Module

4 Overview of Security Manager related reference points

4.1 Introduction

4.1.1 Reference architecture

The requirements for the Sc-Or, Sc-Vnfm and Sc-Vi reference points are specified in ETSI GS NFV-IFA 026 [4].

4.1.2 NFVO as a proxy for getting information from other functional blocks

The Security Manager has requirements for getting information which originates from the NFVO, VIM, VNFM or OSS/BSS. As a general principle, the information originated from either the VIM, VNFM or OSS/BSS is sent to the NFVO from the originated entity, then the information is sent from the NFVO to the SM in which the NFVO acts as a proxy.

This principle is reflected by the present document in the following ways:

- The present document defines a reference point between the NFVO and the SM.
- The present document does not define a reference point between the OSS/BSS and the SM (NFVO as a proxy).
- The present document does not define a reference point between the VNFM and the SM (NFVO as a proxy).
- The present document defines a reference point between the VIM and the SM, and only one interface including a reduced set of operations compared to Or-Vi and Vi-Vnfm reference point is specified for this reference point.

4.1.3 Interfaces on the Sc-Or reference point

The Sc-Or reference point is used for exchanges between the SM and the NFVO, and supports the interfaces defined in Table 4.1.3-1.

Table 4.1.3-1: Interfaces on the Sc-Or reference point

Numbering	Name	Description	Produced by / consumed by
Sc-Or.NsLcm	NS Lifecycle Management	NS Lifecycle Management, derived from the NS LCM interface on the Os-Ma-nfvo reference point. This interface supports notification operations. For a Passive Security Manager there is no further action. Where the Semi-Active or Fully-Active Security Managers needs to take further action, it is done over the Security Policy Enforcement interface.	Produced by the NFVO, consumed by the SM.
Sc-Or.StatusInfo	Status Information Management	This interface supports request/response operations for getting status information such as lists of VNF and run-time information about an NS instance.	Produced by the NFVO, consumed by the SM.
Sc-Or.SecEnforce	Security Policy Enforcement	This interface support request/response operations for Fully-Active or Semi-Active SMs to e.g. request changes to active VNFs to enforce security policies.	Produced by the NFVO, consumed by the SM.
Sc-Or. SecurityVnfMgmt	Security VNF Management	This interface supports request/response operations for management of the VNFs required for security purposes.	Produced by NFVO, consumed by the SM.

4.1.4 Interfaces on the Sc-Vi reference point

The Sc-Vi reference point is used for exchanges between the SM and the VIM, and supports the interface shown in Table 4.1.4-1.

Table 4.1.4-1: Interfaces on the Sc-Vi reference point

Numbering	Name	Description	Produced by / consumed by
Sc-Vi.Telem	Telemetry Information Management	This interface supports notifications and request/response operations of telemetry information as seen by the VIM.	Produced by the VIM, consumed by the SM.

4.2 Relation to other NFV Group Specifications

Information about the reference points in the ETSI NFV architecture can be found in ETSI GS NFV 006 [i.7] and the security management architecture can be found in ETSI GS NFV-IFA 026 [4].

5 Reference point and interface requirements for Security Management

5.1 Introduction

This clause defines or references requirements applicable to interfaces in the context of the Sc-Or and Sc-Vi reference points, in order to support security monitoring and management as specified in ETSI GS NFV-SEC 013 [i.3].

Requirements are labelled according to whether they are applicable to Passive, Semi-Active or Fully-Active security monitoring, using the definitions from ETSI GS NFV-IFA 026 [4]. The right-most column of all tables in clause 5 is entitled "PSF" and is used to list the type of SMs to which the requirement applies. "S" and "F" indicate that it applies to "Semi-Active" or "Fully-Active", while "SF" indicates that it applies to Semi-Active and Fully-Active (this is therefore a conditional requirement). If the requirement applies to all types of SM (written as "All") then the requirement is considered to be a mandatory requirement, unless it is otherwise stated in the text of the requirement.

5.2 Reference point requirements

5.2.1 Sc-Or reference point requirements

Table 5.2.1-1 specifies requirements applicable to the Sc-Or reference point.

Table 5.2.1-1: Sc-Or reference point requirements

Numbering	Requirement	PSF (see clause 5.1)
Sc-Or.001	The Sc-Or reference point shall support the NS Lifecycle Management interface produced by the NFVO.	All
Sc-Or.002	The Sc-Or reference point shall support the Status Information Management interface produced by the NFVO.	All
Sc-Or.003	The Sc-Or reference point shall support the Security Policy Enforcement interface produced by the NFVO.	SF
Sc-Or.004	The Sc-Or reference point shall support the Security VNF Management interface produced by the NFVO.	All

5.2.2 Sc-Vi reference point requirements

Table 5.2.2-1 specifies requirements applicable to the Sc-Vi reference point.

Table 5.2.2-1: Sc-Vi reference point requirements

Numbering	Requirement	PSF (see clause 5.1)
Sc-Vi.001	The Sc-Vi reference point shall support the Telemetry Information Management interface produced by the VIM.	All

5.3 Interface requirements

5.3.1 Interface requirements for NS Lifecycle Management

This clause specifies requirements applicable to NS Lifecycle Management interface produced by the NFVO over the Sc-Or reference point. The consumer of the interface is the Security Manager. The requirements applicable to the Semi-Active and Fully-Active Security Manager can be met by a combination of operations provided by this interface with operations provided by other interfaces, i.e. a notification received on the NS Lifecycle Management interface may trigger subsequent operations on the Security Policy Enforcement interface over Sc-Or reference point.

Table 5.3.1-1 specifies requirements applicable to the NS Lifecycle Management interface produced by the NFVO over the Sc-Or reference point.

Table 5.3.1-1: NS Lifecycle Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Sc-Or.NsLcm.001	The NS Lifecycle Management interface shall support providing reports on NSs including information on their constituent VNFs and PNFs. See note 1.	R1.3.70	All
Sc-Or.NsLcm.002	The NS Lifecycle Management interface shall support the delivery of the package/artefact integrity information (e.g. checksum).	R2.1.250	All
Sc-Or.NsLcm.003	The NS Lifecycle Management interface shall support providing notifications of all unauthorized attempts to change VNFs (including on-boarding, instantiation, modification and termination).	R1.3.110 See note 2.	All
Sc-Or.NsLcm.004	The NS Lifecycle Management interface shall support providing details of topology changes including migration, scale-in and scale-out of VNFs.	R1.3.220 See note 2.	All
Sc-Or.NsLcm005	The NS Lifecycle Management interface shall support providing VNF lifecycle management event information when a VNF is created.	R2.1.150 See note 2. (The NFVO would know about the end result. The VNFM knows more detail e.g. changes of affected VNFs, intermediate steps for each VNF that is touched).	All
Sc-Or.NsLcm.006	The NS Lifecycle Management interface shall support providing the following information as part of the NS LCM notification related to a VNF instantiation event: • Source of request (see note 3). • VNF Package Identifier • VNFD Identifier. • Integrity check of VNF package/artefact. • VNF instance identifier. • Connectivity information (including connections to PNFs) as known by NFV-MANO.	R2.1.210 See note 2.	All

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Sc-Or.NsLcm.007	The NS Lifecycle Management interface shall support providing the following information relating to a VNF modification event (see note 4) and VNF termination event: • Source of request (see note 3). • VNF instance identifier • Details of the change.	R2.1.160 (modification) and R2.1.170 (termination). R2.1.220 (modification) and R2.1.230 (termination). See note 2 (anything at resource level is not seen by the NFVO).	All
Sc-Or.NsLcm.008	The NFVO shall be aware of the security mode (Passive, Semi-Active or Fully-Active) in which each SM entity is set to function and have the capability to enforce it.	Clause 5.1.2	All
NOTE 1: PNF information is limited to a description of their connection points, information about the virtual links they are attached to, and information about the network forwarding paths in which they are involved, if any. Additional information about PNFs is out of scope of ETSI NFV specifications. NOTE 2: These requirements are based on an underlying requirement (from ETSI GS NFV-IFA 026 [4]) for information that was originally stored or created by the VNFM. As described in clause 4.1.2, this information is being sent to the SM over the Sc-Or reference point. NOTE 3: The source of the event is e.g. application layer OSS/BSS, VNF, EMS, auto healing function. NOTE 4: Modification is any change to a VNF: - configuration; - run-time images or code version; - location (physical or logical); - host resources; - NFV layer communications peering relationships; - identification of the VNF instance (i.e. the identity generated during the instantiation); - changes to 1 or more VNFC instances within a VNF; - load balancing.			

5.3.2 Interface requirements for Status Information Management

Table 5.3.2-1 specifies requirements applicable to the Status Information Management interface produced by the NFVO over the Sc-Or reference point.

Table 5.3.2-1: Status Information Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Sc-Or.StatusInfo.001	The Status Information Management interface shall support providing the VNF instantiation state and operation state for all active VNFs. See note.	R2.1.320	All
NOTE: For more details on instantiation state see ETSI GS NFV-IFA 007 [5], clause 7.2.2 (INSTANTIATED, NOT_INSTANTIATED). For more details on operational states see: - ETSI GS NFV-IFA 007 [5], clause 7.2.11 (STARTED, STOPPED). - ETSI GS NFV-IFA 007 [5], clause 8.5.3 "vnfState" attribute in "InstantiatedVnfInfo". - ETSI GS NFV-SOL 003 [i.6], clauses 5.5.4.3 to 5.5.4.7 and 5.6.2.			

5.3.3 Interface requirements for Security Policy Enforcement

Table 5.3.3-1 specifies requirements applicable to the Security Policy Enforcement interface produced by the NFVO over the Sc-Or reference point. Any additional aspects of security policy management (beyond those listed below) are out of scope of the present document. Details are in ETSI GS NFV-IFA 026 [4] and ETSI GS NFV-SEC 013 [i.3].

Table 5.3.3-1: Security Policy Enforcement interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Sc-Or.SecEnforce.001	For Semi-Active and Fully-Active Security Managers, the Security Policy Enforcement interface shall support the provision of security policy instructions (e.g. immediately terminate one or more VNFs of a network service).	Derived from R2.1.30 (subset) R2.1.40 (subset)	SF
Sc-Or.SecEnforce.002	For Semi-Active Security Managers, the Security Policy Enforcement interface shall support terminating a VNF. The termination request shall be able to specify: • Whether another VNF may be created to replace the VNF being terminated. • Whether it wants a snapshot of the VNF to be made for later analysis.	R2.1.260 (re-phrased as interface requirement)	S
Sc-Or.SecEnforce.003	For Fully-Active Security Managers, the Security Policy Enforcement interface shall support terminating a VNF. The termination request shall be able to specify: • Whether another VNF may be created to replace the VNF being terminated. • Whether it wants a snapshot of the VNF to be made for later analysis. • Whether the VNF package and VNFD shall be disabled. • Whether all other VNFs running on the same host should be terminated. See note. • Whether NFV-MANO shall actively erase the resources used by all HMEEs, TPMs, HSMs or other storage used by the terminated VNF.	R2.1.270 (re-phrased as interface requirement)	F
Sc-Or.SecEnforce.004	For Semi-Active and Fully-Active Security Managers, the Security Policy Enforcement interface shall support terminating the use of a specific host: • The termination request shall allow the SM to specify whether VNFs running on the host may be migrated or shall be terminated. • The termination request shall allow the SM to specify whether to quarantine the host along with the hosted VNFs.	R2.1.290 (for S) R2.1.300 (for F)	SF
Sc-Or.SecEnforce.005	The NFVO shall be aware of the security mode (Passive, Semi-Active or Fully-Active) in which each SM entity is set to function and have the capability to enforce it.	Clause 5.1.2	All
NOTE: Requirement is met by determining all the other VNFs on the same host and terminating each of them.			

5.3.4 Interface requirements for Security VNF Management

Table 5.3.4-1 specifies requirements applicable to the Security VNF Management interface produced by the NFVO over the Sc-Or reference point.

Table 5.3.4-1: Security VNF Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Sc-Or.SecurityVnfMgmt.001	The Security VNF Management interface shall support creating/instantiating, modifying or terminating security VNFs to be inserted into or removed from a network service.	Derived from R2.1.310 (uses the term creating) and R1.2.100 and R1.2.120 (uses the term instantiating).	SF
Sc-Or.SecurityVnfMgmt.002	The NFVO shall be aware of the security mode (Passive, Semi-Active or Fully-Active) in which each SM entity is set to function and have the capability to enforce it.	Clause 5.1.2.	All

5.3.5 Interface requirements for Telemetry Information Management

Table 5.3.5-1 specifies requirements applicable to the Telemetry Information Management interface produced by VIM over the Sc-Vi reference point.

Table 5.3.5-1: Telemetry Information Management interface requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Sc-Vi.Telem.001	The Telemetry Information Management interface shall support querying and notifying telemetry information which includes: NFVI system configurations (including capacity, images, compute flavour), policies and packet headers.	Covers part of R1.3.140.	All
Sc-Vi.Telem.002	The Telemetry Information Management interface shall support providing location information from the VIM, e.g. HostID, ZoneID and physical location.	R2.1.160 and R2.1.210	All

5.4 Security requirements

Table 5.4-1 specifies the requirements relating to security in the realization of interface operations over Sc-Or and Sc-Vi reference point. Each requirement applies to all interfaces except where it is stated otherwise.

Table 5.4-1: Security requirements

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Security.001	Each set of SM to NFV-MANO interfaces on the reference points Sc-Or and Sc-Vi (for the same SM) shall use independent integrity and confidentially protection from all other SM to NFV-MANO interface sets. This is a requirement about having independent cryptographic keys from the interfaces not defined in the present document.	Clause 5.1.3	All
Security.002	All interfaces shall enable NFV-MANO to ensure that VNF lifecycle management events are sent to the correct one or more SMs subject to the trust domain separation model being implemented by a network.	Clause 5.1.3	All
Security.003	All interfaces shall support identification of parties to enable NFV-MANO to reject instructions from an SM in one trust domain for VNFs managed by another SM in another trust domain.	Clause 5.1.3	All
Security.004	Traffic of the SM shall be isolated and separated from other traffics in data/control planes, etc.	R.1.1.160	All
Security.005	The Telemetry Information Management interface shall support relevant additional data security policies and authorized access such as telemetry source and destination authentication, telemetry data integrity and confidentiality, opportunistic encryption, trusted time, and synchronization across multiple NFVI systems.	R.1.3.160	All

Numbering	Requirement	Reference to requirement in ETSI GS NFV-IFA 026 [4]	PSF (see clause 5.1)
Security.006	All interfaces shall enable the NFVO/VNFM/VIM to support separate independent security associations and keys for each SM on each logical interface.	R.2.1.70	All
Security.007	The identification and authentication over all interfaces shall enable the NFVO/VNFM/VIM to ensure that only lifecycle management events applicable to a specific SM(s) are sent to that SM(s).	R.2.1.80	All

6 Interfaces over Sc-Or reference point

6.1 Introduction

This clause defines the interfaces exposed by the NFVO towards the SM over the Sc-Or reference point.

6.2 NS Lifecycle Management Interface

This interface allows the SM to subscribe to notifications relating to NS lifecycle management operations from the NFVO. The requirements for this interface are specified in Table 5.3.1-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Subscription/Notification (refer to clauses 7.3.11 to 7.3.14 of ETSI GS NFV-IFA 013 [3]).

NOTE: The Subscription/Notifications operations in clauses 7.3.11 to 7.3.14 of ETSI GS NFV-IFA 013 [3] enable Sc-Or.NsLcm.006 to be met as follows:

- The Subscription/Notifications operations in clauses 7.3.11 to 7.3.14 return the information as shown in clause 8.3.2.2 of ETSI GS NFV-IFA 013 [3].
- This gives the appropriate identifiers in order to use the QueryNS operation to retrieve all the information required by Sc-Or.NsLcm.006. Specifically, QueryNS returns NSInfo which contains VnfInfo, which meets Sc-Or.NsLcm.006 as follows:
  - VNF Package Identifier = vnfinfo.onboardedVnfPkgInfoId.
  - VNFD Identifier = vnfinfo.vnfdId.
  - VNF instance identifier = vnfinfo.vnfInstanceId.
  - Connectivity information (including connections to PNFs) as known by NFV-MANO = vnfinfo.extVirtualLinkInfo.
  - Integrity check of VNF package/artefact = use onboardedVnfPkgInfoId to get to VnfPkgInfo, which has a checksum (and also the VNF Package has a SoftwareImageInformation element with a checksum).

6.3 Status Information Management Interface

This interface allows the SM to query status information from the NFVO. The requirements for this interface are specified in Table 5.3.2-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Query NS (refer to clause 7.3.6 of ETSI GS NFV-IFA 013 [3]).

6.4 Security Policy Enforcement Interface

This interface allows (Fully-Active or Semi-Active) SMs to request changes to active VNFs to enforce security policies. The requirements for this interface are specified in Table 5.3.3-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Update NS (refer to clause 7.3.5 of ETSI GS NFV-IFA 013 [3], see note 1).
- Update VNF Package Info (refer to clause 7.7.16 of ETSI GS NFV-IFA 013 [3], see note 3).

NOTE 1: Update NS is used as follows:

- To meet Sc-Or.SecEnforce.002 and .003 (terminating VNF), with updateType = RemoveVnf and a removeVnfInstanceId attribute set to the appropriate identifier (see note 2).
- To meet Sc-Or.SecEnforce.002 and .003 (create snapshot), with updateType = CreateSnapshot.
- To meet Sc-Or.SecEnforce.002 and .003 (whether another VNF may be created) by sending one UpdateNS request to kill the VNF instance and sending another UpdateNS request to recreate it if required.

NOTE 2: According to ETSI GS NFV-IFA 013 [3], note 1 of Table 7.3.5.2-1, a VNF instance is only terminated by the NFVO if it is no longer used by any NS. As a consequence, in order to terminate a VNF instance, the SM has to send an UpdateNS request to each NS where this VNF instance is a part.

NOTE 3: Update VNF Package Info is used as follows:

- To meet Sc-Or.SecEnforce.003 (disabling a VNF Package).

NOTE 4: An explanation of how to meet Sc-Or.SecEnforce.004 is not given in the present document.

6.5 Security VNF Management Interface

This interface allows the SM to manage security-related VNFs from the NFVO. The requirements for this interface are specified in Table 5.3.4-1.

The following operations are defined for this interface, and these operations shall follow the specification from ETSI GS NFV-IFA 013 [3], except that the producer is the NFVO and the consumer is the SM:

- Update NS (refer to clause 7.3.5 of ETSI GS NFV-IFA 013 [3]).

NOTE: It is assumed that the VNFD of the security-related VNF is referenced from the NSD.

7 Interfaces over Sc-Vnfm reference point

7.1 Introduction

The present document does not define any interfaces over the Sc-Vnfm reference point.

8 Interfaces over Sc-Vi reference point

8.1 Introduction

This clause defines the interfaces exposed by the VIM towards the SM over the Sc-Vi reference point.

8.2 Telemetry Information Management interface

8.2.1 Description

This interface allows the SM to query or subscribe to notifications related to telemetry information from the VIM. The requirements for this interface are specified in Table 5.3.5-1.

The following operations are defined for this interface, and these operations shall follow the specifications from ETSI GS NFV-IFA 005 [1] and ETSI GS NFV-IFA 006 [2], except that the producer is the VIM and the consumer is the SM.

The interface supports the following Query operations derived from interfaces in ETSI GS NFV-IFA 005 [1] and ETSI GS NFV-IFA 006 [2]:

- From ETSI GS NFV-IFA 005 [1], clause 7.3.4.2 Query Compute Capacity operation
- From ETSI GS NFV-IFA 005 [1], clause 7.3.4.5 Query Compute Resource Zone operation
- From ETSI GS NFV-IFA 005 [1], clause 7.3.4.6 Query NFVI-PoP Compute Information operation
- From ETSI GS NFV-IFA 005 [1], clause 7.4.4.2 Query Network Capacity operation
- From ETSI GS NFV-IFA 005 [1], clause 7.4.4.5 Query NFVI-PoP Network Information operation
- From ETSI GS NFV-IFA 005 [1], clause 7.4.5.3 Query NFP operation
- From ETSI GS NFV-IFA 005 [1], clause 7.5.4.5 Query NFVI-PoP Storage Information operation
- From ETSI GS NFV-IFA 005 [1], clause 7.5.4.6 Query Storage Resource Zone operation
- From ETSI GS NFV-IFA 005 [1], clause 7.9.3.3 Query Storage Resource Quota operation
- From ETSI GS NFV-IFA 005 [1], clause 7.10.3 Query Compute Host Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.2.2 Query Images operation
- From ETSI GS NFV-IFA 006 [2], clause 7.2.3 Query Image operation
- From ETSI GS NFV-IFA 006 [2], clause 7.3.1.3 Query Virtualised Compute Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.3.3.4 Query Virtualised Compute Resource Information operation
- From ETSI GS NFV-IFA 006 [2], clause 7.3.4.3 Query Compute Flavour operation
- From ETSI GS NFV-IFA 006 [2], clause 7.4.1.3 Query Virtualised Network Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.4.3.4 Query Virtualised Network Resource Information operation
- From ETSI GS NFV-IFA 006 [2], clause 7.5.1.3 Query Virtualised Storage Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.5.3.4 Query Virtualised Storage Resources Information operation
- From ETSI GS NFV-IFA 006 [2], clause 7.7.3 Query PM Job operation
- From ETSI GS NFV-IFA 006 [2], clause 7.7.8 Query Threshold operation
- From ETSI GS NFV-IFA 006 [2], clause 7.8.1.2 Query Compute Resource Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.8.2.2 Query Network Resource Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.8.3.2 Query Storage Resource Reservation operation
- From ETSI GS NFV-IFA 006 [2], clause 7.9.1.2 Query Compute Resource Quota operation

- From ETSI GS NFV-IFA 006 [2], clause 7.9.2.2 Query Network Resource Quota operation
- From ETSI GS NFV-IFA 006 [2], clause 7.9.3.2 Query Storage Resource operation
- From ETSI GS NFV-IFA 006 [2], clause 7.10.4 Query Policy operation
- From ETSI GS NFV-IFA 006 [2], clause 7.10.10 Query Subscription Info operation

The interface supports subscription/notification operations derived from the following interfaces in ETSI GS NFV-IFA 005 [1] and ETSI GS NFV-IFA 006 [2]:

- From ETSI GS NFV-IFA 005 [1], clause 7.3.4 Virtualised Compute Resources Capacity Management Interface
- From ETSI GS NFV-IFA 005 [1], clause 7.5.4 Virtualised Storage Resources Capacity Management Interface
- From ETSI GS NFV-IFA 005 [1], clause 7.11.1 Compute Host Capacity Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.3.2 Virtualised Compute Resources Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.3.3 Virtualised Compute Resources Information Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.4.2 Virtualised Network Resources Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.4.3 Virtualised Network Resources Information Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.5.2 Virtualised Storage Resources Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.5.3 Virtualised Storage Resources Information Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.6 Virtualised Resources Fault Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.7 Virtualised Resources Performance Management Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.8.4 Virtualised Resources Reservation Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.9.4 Virtualised Resources Quota Change Notification Interface
- From ETSI GS NFV-IFA 006 [2], clause 7.10 Policy Management Interface

9 Overview of Certificate Management related reference points

9.1 Introduction

The specification of the interfaces in the present document is based on the characteristics of the certificate management modes defined in ETSI GS NFV-IFA 026 [4] (i.e. direct-mode and delegation-mode) and on the requirements in Annex B of ETSI GS NFV-IFA 026 [4].

This clause describes Certificate Management related reference points and its interfaces, for the support of Certificate Management. The present document only specifies the reference point Cm-Vnfm as shown in clause 5.2 of ETSI GS NFV-IFA 026 [4].

For the management of NFV-MANO Certificates, no reference points are defined in this version of the present document.

For the management of VNFCI and VNF OAM certificate in direct mode, below reference points and interfaces are defined in this version of the present document:

- Cm-Vnfm, which supports a subset of the VNF LCM interface (operation occurrence event notifications and query VNF) exposed by the VNFM and consumed by the CMF.

For the management of VNFCI and VNF OAM certificate in delegation mode, below reference points are defined in this version of the present document:

- Cm-Vnfm, which supports the Certificate Management interface as introduced in clause 5.2 of ETSI GS NFV-IFA 026 [4]. The Certificate Management interface is exposed by the CMF and consumed by the VNFM.

The CMF exposed Certificate Notification Service interface, as introduced in clause 5.2 of ETSI GS NFV-IFA 026 [4], can also be supported over the Cm-Vnfm reference point with the VNFM as consumer of the service interface.

This version of the present document does not specify reference point and interfaces between the CMF and the CA. The CA produced interface, as introduced in clause 5.2 of ETSI GS NFV-IFA 026 [4], is not in scope of ETSI NFV but it is based on existing industry defined certificate management protocols specified by IETF, such as those listed in ETSI GR NFV-SEC 005 (V1.2.1) [i.8] and ETSI GS NFV-IFA 026 [4].

9.2 Conventions

The following notations, defined in ISO/IEC 9646-7 [i.9], are used for the qualifier column of interface information elements:

- M mandatory - the capability is required to be supported;
- O optional - the capability may be supported or not;
- CM conditional mandatory - the capability is required to be supported and is conditional on the support of some condition. This condition shall be specified in the Description column;
- CO conditional optional - the capability may be supported or not and is conditional on the support of some condition. This condition shall be specified in the Description column.

The following notation is used for parameters that represent identifiers, and for attributes that represent identifiers in information elements and notifications:

- If parameters are referring to an identifier of an actual object, their type is "Identifier".
- If an object (information element or notification) contains an attribute that identifies the object, the type of that attribute is "Identifier" and the description states that the attribute is the identifier of that particular notification or information element.

EXAMPLE 1: Identifier "resourceId" of the "NetworkSubnet information element" has type "Identifier" and description "Identifier of this NetworkSubnet information element".

- If an object (information element or notification) contains an attribute that references another object or objects defined in an ETSI NFV GS, the type of the attribute is "Identifier", followed by the list of objects it references.

EXAMPLE 2: "Identifier (Reference to Vnfc)" or "Identifier (Reference to Vnfc, VirtualLink or VirtualStorage)".

If the type of a parameter or attribute has been marked as "Not specified" in the "Content" column, this means that its specification is part of the protocol design/data model design.

9.3 Interfaces on Cm-Vnfm reference point

The Cm-Vnfm reference point is used for exchanges between the CMF and the VNFM, and supports the interfaces indicated in Table 9.3-1.

Table 9.3-1: Interfaces on the Cm-Vnfm reference point

Numbering	Name	Description	Produced by / consumed by	Certificate management mode
Cm-Vnfm.CertMgmt	Certificate Management Interface	This interface supports registration and signing request/response of VNFCI/VNF OAM certificates for the VNFCIs managed in delegation mode. It also supports de-registration of the end entities as subjects for certificates and certificate chains.	Produced by the CMF and consumed by the VNFM.	Delegation-mode
Cm-Vnfm.VnfLcmMgmt	VNF Lifecyle Management	This interface supports providing notifications of VNF LCM operation occurrence events and supports querying information about VNF instances (as per clause 7.2 in ETSI GS NFV-IFA 007 [5]).	Produced by the VNFM and consumed by the CMF.	Direct-mode
Cm-Vnfm.CertNotification	Certificate Notification Interface	This interface supports notifications about the VNFCI/VNF OAM certificate lifecycle states.	Produced by the CMF and consumed by the VNFM.	

10 Reference point and interface requirements for Certificate Management

10.1 Introduction

This clause defines or references requirements applicable to interfaces in the specific context of Certificate Management related reference points.

10.2 Reference point requirements

10.2.1 Cm-Vnfm Reference point requirements

Table 10.2.1-1 specifies requirements applicable to the Cm-Vnfm reference point. Requirements are labelled in the third column according to whether they are applicable to delegation-mode or to direct-mode.

Table 10.2.1-1: Cm-Vnfm reference point requirements

Identifier	Requirement	Certificate management mode
Cm-Vnfm.001	The Cm-Vnfm reference point shall support the Certificate Management interface produced by the CMF for the delegation mode support.	Delegation-mode
Cm-Vnfm.002	The Cm-Vnfm reference point shall support the VNF Lifecycle Management interface produced by the VNFM for the direct mode support.	Direct-mode
Cm-Vnfm.003	The Cm-Vnfm reference point shall support the Certificate Notification Service interface produced by the CMF.	

10.3 Interface requirements

10.3.1 Certificate Management Interface requirements

Table 10.3.1-1 provides requirements related to the interface for VNFCI/VNF OAM certificate management (see Annex B in ETSI GS NFV-IFA 026 [4]), which are specific for delegation mode.

Table 10.3.1-1: Certificate Management interface requirements for VNFCI/VNF OAM certificate management in delegation mode

Identifier	Requirement
CMF.Certm.Del.001	Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation. See note.
CMF.Certm.Del.002	Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities. See note.
CMF.Certm.Del.003	Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains. See note.
CMF.Certm.Del.004	Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains. See note.
CMF.Certm.Del.005	Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities. See note.
CMF.Certm.Del.006	Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities. See note.
NOTE: See clause 11.2.	

10.3.2 VNF Lifecycle Management Interface requirements

Table 10.3.2-1 provides requirements related to the interface for VNF Lifecycle management.

Table 10.3.2-1: VNF Lifecycle Management interface requirements

Identifier	Requirement
VNFM.LCM.001	The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support managing subscriptions to VNF lifecycle management operation occurrence notifications. See note.
VNFM.LCM.002	The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support querying information about a VNF instance. See note.
NOTE: See clause 11.3.	

10.3.3 Certificate Notification Service Interface requirements

Table 10.3.3-1 provides requirements related to the interface for the Certificate Notification Service.

Table 10.3.3-1: Certificate Notification Service interface requirements

Identifier	Requirement
CMF.CNS.001	The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support managing subscriptions to certificate lifecycle state notifications. See note.
CMF.CNS.002	The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support querying information about VNFCI or VNF OAM certificate states. See note.
NOTE: See clause 11.4.	

11 Interface specification on Certificate Management

11.1 Introduction

This clause defines the interfaces for enabling management of NFV-MANO, VNFCI and VNF-OAM certificates.

11.2 Certificate Management Interface

11.2.1 Description

This interface allows providing certificate management services such as signing certificates and providing certificate chains for registered entities.

The Certificate Management interface supports the following operations:

- Register.
- Certificate Signing Request.
- Deregister.
- Revoke.
- Query Subject Info.
- Query Certificate Info.

"Register" is the process for the producer to prepare enrolment of the requested certificates. The consumer registers the entity which is subject for certificates and certificate chains. During this registration, to enable the key attestation mechanism, public key of the generator of the key pair for the subject (e.g. an HSM), the attester, and the corresponding Object Identifier (OID) identifying the key attestation statement of this attester are registered as well.

"Certificate Signing Request" is the process to enrol the requested certificate and provide certificate chains. The producer validates the request by checking if the requested entity subject for the certificate has been correctly registered by Register operation.

The producer, if it is the key attestation verifier, validates the key attestation statement in the CSR (see note 1) using the registered public key and key attestation statement OID of the generator of keys for this subject, checking that the key attestation includes a public key and that this public key match the public key of the subject included in the CSR (see note 2). If the key attestation does not include a public key or this public key does not match the public key in the certificate request, the CSR should be rejected with no certificate issued. However, the CMF may elect to process the request as if the request did not contain a key attestation per local policy.

As result of a successful operation, the producer provides the signed certificate, and the certificate chain, if requested by the consumer.

NOTE 1: The details of the key attestation inclusion in the CSR are left for further specification.

NOTE 2: Alternatively, the producer can act as a relying party to delegate the key attestation validation to an external entity (e.g. Certificate Authority). The certificate issuing authority (e.g. a CA) may elect to issue a certificate as if the request did not contain a key attestation per local policy.

"Deregister" is the process for the producer to de-register the VNFCI(s) from VNFCI and VNF OAM certificate management, and to de-register the consumer's role as the VNFCI's delegate for certificate management. The producer validates the request by checking if the consumer is registered as the VNFCI's delegate for certificate management.

"Revoke" is the process to revoke the certificates which are signed and delivered to the end entities. The producer validates the request by checking if the consumer is registered as the VNFCI's delegate for certificate management. Based on the VNF LCM operation or any other criteria, e.g. detecting the VNFCI failures, the VNFM as consumer of this operation determines the need for the VNFCI and/or VNF OAM certificate to be 'revoked'.

"Query Subject info" is the process to query the information of the registered end entities as subjects. The producer validates the request by checking if the consumer is registered as the VNFCI's delegate for certificate management.

"Query Certificate info" is the process to query the information of the certificates which are signed and delivered to the end entities. The producer validates the request by checking if the consumer is registered as the VNFCI's delegate for certificate management.

11.2.2 Register Operation

11.2.2.1 Operation description

The operation described in this clause only applies for:

- the NFV-MANO certificate;
- VNFCI and VNF OAM certificate when delegation mode is selected.

This operation enables a consumer to register the MANO entities or VNFCI for the certificates. Table 11.2.2.1-1 lists the information flow exchanged between CMF and the consumer.

Table 11.2.2.1-1: Register operation

Message	Requirement	Direction
RegisterRequest	Mandatory	Consumer -> CMF
RegisterResponse	Mandatory	CMF -> Consumer

11.2.2.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.2.2.2-1.

Table 11.2.2.2-1: Register operation input parameters

Parameter	Qualifier	Cardinality		Content	Description
certType	M	1		Enum	Indicate the type of target certificate. The possible values are (see note 3): • MANO certificate • VNFCI certificate • VNF OAM certificate
subjectId	M	1..N		Structure (inlined)	Data about subjects and their certificates that need to be registered. This attribute shall be present only if certType is VNFCI certificate or VNF OAM certificate.
> subjectId	M	1		Identifier	Identifier of the VNFCI that is target for certificates.
> certificateData	M	1..N		Structure (inlined)	Data related to certificates for the target VNFCI.
>> subjectName	M	0..1		CertSubjectData	Subject data of the of VNFCI certificates, i.e. certificate fields related to common name, organization, country, etc. See note 2.
>> subjectAlternateName	M	1..N		String	Subject alternate names of VNFCI certificates.
typeOfVnfcCertHandling	CM	1		Enum	This parameter shall be present only if certType is VNFCI certificate or VNF OAM certificate. It indicates the mode of certificate management for the target entity. The possible values are: • direct mode • delegation mode See note 1.
NOTE 1: Only the value "delegation mode" is allowed for this version of the present document. NOTE 2: The content of this attribute shall be based on the 'CertSubjectData' information element specified in ETSI GS NFV-IFA 007 [5]. NOTE 3: Registration of target certificates of type 'MANO certificate' is not covered in this version of the present document.					

11.2.2.3 Output parameters

None.

NOTE: Further consideration on handling initial credentials for NFV-MANO certificate management is for future study.

11.2.2.4 Operation results

The procedure indicates to the consumer whether or not the operation was successful. In particular for error case, error information indicates the reason why the request has not been succeeded, e.g. input attribute is not appropriate, etc. For the VNFCI and VNF OAM certificate management, the consumer is also registered with VNFCI ID as the entity who manages the certificate on behalf of VNFCIs. If the CA is not integrated in that CMF, the CA is selected by CMF for the target certificate during this process.

11.2.3 Certificate Signing Request operation

11.2.3.1 Operation description

The operation defined in this clause applies for VNFCI certificate and VNF OAM certificate.

NOTE: This operation is only for delegation mode for this version of the present document.

This operation enables a consumer to request signing certificate. The operation of certificate management interface is produced by CMF, and the CMF process the request and forward it to the CA for signing certificate. Table 11.2.3.1-1 lists the information flow exchanged between CMF and the consumer.

Table 11.2.3.1-1: Certificate Signing Request operation

Message	Requirement	Direction
CSRRequest	Mandatory	Consumer -> CMF
CSRResponse	Mandatory	CMF -> Consumer

11.2.3.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.2.3.2-1.

Table 11.2.3.2-1: Certificate Signing Request operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
vnfcId	O	1	Identifier	If this operation is used for the VNFCI certification management, this parameter shall be present.
certType	M	1	Enum	Indicate type of requesting certificate. VALUES: • VnfciCert • VnfOAMCert
certChainRequest	M	1	Boolean	Indicate if requesting certificate chain in addition to the certificate (true) or not (false).
csr	M	1	Not Specified	Information for Certificate Signing Request. This includes information required for certification request according to common standard formats such as PKCS#10, specified in IETF RFC 2986 [6].

11.2.3.3 Output parameters

The output parameters returned by the operation shall follow the indications provided in Table 11.2.3.3-1.

Table 11.2.3.3-1: Certificate Signing Request operation output parameters

Parameter	Qualifier	Cardinality	Content	Description
certificate	M	1	Not Specified	This includes information of the issued certificate according to the X.509 certificate format as specified in IETF RFC 5280 [7]. The parameter "SerialNumber" included in this "certificate" parameter is used as CertificateId for identifying this certificate.
certificateChain	O	1..N	Not Specified	If certificate chain is requested by the consumer, this parameter shall be present. The information provided in this parameter is in accordance with the X.509 certificate format as specified in IETF RFC 5280 [7].

11.2.3.4 Operation results

Upon successful CSR operation, CA-signed x509 certificates are returned to the consumer. If the certificate chain is requested, the certificate chain is provided.

11.2.4 Deregister Operation

11.2.4.1 Operation description

The operation described in this clause only applies for VNFCI and VNF OAM certificate when delegation mode is selected.

This operation enables a consumer to deregister VNFCI(s) from VNFCI and VNF OAM certificate management. Table 11.2.4.1-1 lists the information flow exchanged between CMF and the consumer.

Table 11.2.4.1-1: Deregister operation

Message	Requirement	Direction
DeregisterRequest	Mandatory	Consumer -> CMF
DeregisterResponse	Mandatory	CMF -> Consumer

11.2.4.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.2.4.2-1.

Table 11.2.4.2-1: Deregister operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
subjectId	M	1..N	String	Identifier(s) of the VNFCI to be de-registered.

11.2.4.3 Output parameters

None.

11.2.4.4 Operation results

The procedure indicates to the consumer whether or not the operation was successful. In particular for error case, error information indicates the reason why the request has not been succeeded, e.g. input attribute is not appropriate, etc.

The consumer is also deregistered as the entity who manages the certificate on behalf of the VNFCI.

11.2.5 Revoke Operation

11.2.5.1 Operation description

The operation described in this clause only applies for VNFCI and VNF OAM certificate when delegation mode is selected.

This operation enables a consumer to revoke the certificate which are signed and delivered to the end entities. Table 11.2.5.1-1 lists the information flow exchanged between CMF and the consumer. The CMF shall only revoke certificates for which the consumer has initiated creation.

Table 11.2.5.1-1: Revoke operation

Message	Requirement	Direction
RevokeRequest	Mandatory	VNFM -> CMF
RevokeResponse	Mandatory	CMF -> VNFM

11.2.5.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.2.5.2-1.

Table 11.2.5.2-1: Revoke operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
CertificateId	M	1	Identifier	The identifier of the certificate which is subject to be revoked by this operation.

11.2.5.3 Output parameters

None.

11.2.5.4 Operation results

The procedure indicates to the consumer whether or not the operation was successful. In particular for error case, error information indicates the reason why the request has not been succeeded, e.g. input attribute is not appropriate, etc.

11.2.6 Query Subject Info Operation

11.2.6.1 Operation description

The operation described in this clause only applies for VNFCI and VNF OAM certificate when delegation mode is selected.

This operation enables a consumer to query the information of the end entities as subjects. Table 11.2.6.1-1 lists the information flow exchanged between CMF and the consumer.

Table 11.2.6.1-1: Query Subject Info operation

Message	Requirement	Direction
QuerySubjectinfoRequest	Mandatory	VNFM -> CMF
QuerySubjectInfoResponse	Mandatory	CMF -> VNFM

11.2.6.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.2.6.2-1.

Table 11.2.6.2-1: Query Subject Info operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
filter	M	1	Not specified	Filter to select the Subject instance(s) about which information is queried.

11.2.6.3 Output parameters

The output parameters returned by the operation shall follow the indications provided in Table 11.2.6.3-1.

Table 11.2.6.3-1: Query Subject Info operation output parameters

Parameter	Qualifier	Cardinality	Content	Description
SubjectInfo	M	0..N	Not specified	The information items about the selected Subject instance(s) that are returned. See note.
NOTE: The lower cardinality is 0 since there may be no matches to the provided filter.				

11.2.6.4 Operation results

In case of success, information related to the Subject instances that match the filter is returned. In case of failure, appropriate error information is returned.

11.2.7 Query Certificate Info Operation

11.2.7.1 Operation description

The operation described in this clause only applies for VNFCI and VNF OAM certificate when delegation mode is selected.

This operation enables a consumer to query the information of the certificate which are signed and delivered to the end entities. Table 11.2.7.1-1 lists the information flow exchanged between CMF and the consumer.

Table 11.2.7.1-1: Query Certificate Info operation

Message	Requirement	Direction
QueryCertificateinfoRequest	Mandatory	VNFM -> CMF
QueryCertificateInfoResponse	Mandatory	CMF -> VNFM

11.2.7.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.2.7.2-1.

Table 11.2.7.2-1: Query Certificate Info operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
filter	M	1	Not specified	Filter to select the Certificate instance(s) about which information is queried.

11.2.7.3 Output parameters

The output parameters returned by the operation shall follow the indications provided in Table 11.2.7.3-1.

Table 11.2.7.3-1: Query Subject Info operation output parameters

Parameter	Qualifier	Cardinality	Content	Description
CertificateInfo	M	0..N	Not specified	The information items about the selected Certificate instance(s) that are returned. See note.
NOTE: The lower cardinality is 0 since there may be no matches to the provided filter.				

11.2.7.4 Operation results

In case of success, information related to the Certificate instances that match the filter is returned. In case of failure, appropriate error information is returned.

11.3 VNF Lifecycle Management Interface

This interface allows managing subscriptions to VNF lifecycle management operation occurrence notifications and querying VNF information. VNF Lifecycle Management interface is specified in ETSI GS NFV-IFA 007 [5]. However, in the context of certificate management, VNF Lifecycle Management interface is produced by the VNFM and consumed by the CMF on the Cm-Vnfm reference point, described in clause 5.2 of ETSI GS NFV-IFA 026 [4].

Following operations apply for the VNF Lifecycle Management interface over the Cm-Vnfm reference point:

- "Subscribe operation" as described in clause 7.2.14 of ETSI GS NFV-IFA 007 [5];
- "Notify operation" as described in clause 7.2.15 of ETSI GS NFV-IFA 007 [5]; and
- "Query VNF operation" as described in clause 7.2.9 of ETSI GS NFV-IFA 007 [5].

11.4 Certificate Notification Service Interface

11.4.1 Description

This interface allows managing subscriptions to certificate lifecycle state notifications and querying VNFCI or VNF OAM certificate state information. The Certificate Notification Service interface is produced by the CMF and can be consumed by the VNFM on the Cm-Vnfm reference point, described in clause 5.2 of ETSI GS NFV-IFA 026 [4].

The Certificate Notification Service interface supports the following operations:

- Subscribe
- Notify
- Terminate Subscription
- Query Subscription Info
- Get Certificate Lifecycle State Info.

11.4.2 Subscribe

11.4.2.1 Description

This operation enables a consumer to subscribe with a filter for the notifications sent by the CMF which are related to certificate lifecycle state changes.

NOTE: Specification of filtering mechanism is part of the protocol design.

Table 11.4.2.1-1 lists the information flow exchanged between the CMF and the consumer.

Table 11.4.2.1-1: Subscribe operation

Message	Requirement	Direction
SubscribeRequest	Mandatory	Consumer → CMF
SubscribeResponse	Mandatory	CMF → Consumer

11.4.2.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.4.2.2-1.

Table 11.4.2.2-1: Subscribe operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
filter	M	1	Not Specified	Input filter for selecting e.g. the VNFCI or VNF OAM certificate subject instances of interest and the specific types of certificate lifecycle state changes of interest.
NOTE: Examples of certificate lifecycle states are non-existent, valid, expiring-soon, expired, revoked.				

11.4.2.3 Output parameters

The output parameters returned by the operation shall follow the indications provided in Table 11.4.2.3-1.

Table 11.4.2.3-1: Subscribe operation output parameters

Parameter	Qualifier	Cardinality	Content	Description
subscriptionId	M	1	Identifier	Identifier of the subscription realized.

11.4.2.4 Operation results

After successful subscription, the consumer is registered to receive notifications related to certificate lifecycle state changes.

The result of the operation shall indicate if the subscription has been successful or not with a standard success/error result. For a particular subscription, only notifications matching the filter will be delivered to the consumer.

11.4.3 Notify

11.4.3.1 Description

This operation notifies a subscriber about events related to certificate lifecycle state changes.

This operation distributes notifications to subscribers. It is a one-way operation issued by the producer (CMF) that cannot be invoked as an operation by the consumer. In order to receive notifications, the consumer has to perform an explicit Subscribe operation beforehand.

Table 11.4.3.1-1 lists the information flow exchanged between the CMF and the consumer.

Table 11.4.3.1-1: Notify operation

Message	Requirement	Direction
Notify	Mandatory	CMF → Consumer

The following notifications can be notified/sent by this operation:

- CertificateLifecycleStateChangeNotification

The definition of the CertificateLifecycleStateChangeNotification and its information elements is deferred to a later version of the present document.

11.4.4 Terminate Subscription

11.4.4.1 Description

This operation enables the consumer to terminate a particular subscription.

Table 11.4.4.1-1 lists the information flow exchanged between the consumer and the CMF.

Table 11.4.4.1-1: Terminate Subscription operation

Message	Requirement	Direction
TerminateSubscriptionRequest	Mandatory	Consumer → CMF
TerminateSubscriptionResponse	Mandatory	CMF → Consumer

11.4.4.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.4.4.2-1.

Table 11.4.4.2-1: Terminate Subscription operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
subscriptionId	M	1	Identifier	Identifier of the subscription to be terminated.

11.4.4.3 Output parameters

None.

11.4.4.4 Operation results

After successful termination of a subscription, the identified subscription does not exist anymore, and the consumer will not receive notifications related to that subscription any longer. The result of the operation shall indicate if the subscription termination has been successful or not with a standard success/error result.

11.4.5 Query Subscription Info

11.4.5.1 Description

This operation enables the consumer to query information about subscriptions.

Table 11.4.5.1-1 lists the information flow exchanged between the consumer and the CMF.

Table 11.4.5.1-1: Query Subscription operation

Message	Requirement	Direction
QuerySubscriptionInfoRequest	Mandatory	Consumer → CMF
QuerySubscriptionInfoResponse	Mandatory	CMF → Consumer

11.4.5.2 Input parameters

The input parameters sent when invoking the operation shall follow the indications provided in Table 11.4.5.2-1.

Table 11.4.5.2-1: Query Subscription Info operation input parameters

Parameter	Qualifier	Cardinality	Content	Description
filter	M	1	Not specified	Filtering criteria to select one or a set of subscriptions. Details are part of the protocol design.

11.4.5.3 Output parameters

The output parameters returned by the operation shall follow the indications provided in Table 11.4.5.3-1.

Table 11.4.5.3-1: Query Subscription Info operation output parameters

Parameter	Qualifier	Cardinality	Content	Description
queryResult	M	0..N	Not specified	Information about the subscription(s) matching the query.

11.4.5.4 Operation results

After successful operation, the CMF has queried the internal subscription objects. The result of the operation indicates if it has been successful or not with a standard success/error result. For a particular query, information about the certificate lifecycle state notifications subscriptions that the consumer has access to and match the filter shall be returned.

12 Information elements for Certificate Management

12.1 Introduction

The definition of information elements and notifications related to Certificate Management is deferred to a later version of the present document.

Annex A (informative): Change history

Date	Version	Information about changes
2018/09/12	V0.0.1	Skeleton (based on IFA-007) with example details populated in clauses 5, 6 and 7. The contents of these clauses is intended to be illustrative. Version viewed by SEC/IFA but no approval or consensus reached.
2018/12/03	V0.1.0	Version agreed for publication as a new draft version by IFA#128
2018/12/14	V0.1.1	Put forward as a draft preparing for the next published draft (which will be v0.2.0)
2019/01/03	V0.2.0	Version agreed as a draft for publication by SEC#137, as per instructions from joint IFA/SEC/SOL F2F at NFV#24
2019/02/15	V0.2.1	Version put forward to be the new published draft, for decision at joint IFA/SEC/SOL meeting NFV#25. Noted but no decision taken.
2019/03/29	V0.2.2	Put forward to get SEC approval at SEC call March 2019. Review received but no decision taken to publish.
2019/05/03	V0.2.3	Including output of SEC call and review from IFA and SEC members. Prepared for F2F May 2019.
2019/06/26	V0.2.4	It is now considered that sections 4 and 5 are essentially complete i.e. that we have the right set of interfaces on the right reference points, and that the requirements have been allocated to the right interfaces. It is hoped this can be agreed to be the new published draft v0.3.0 which can form a new baseline for future work.
2019/08/16	V0.3.0	Agreed by calls SEC#150 and IFA#162 that this is a new draft ready to be published (as a draft).
2019/11/11	V0.4.0	Version 0.4.0 is version 0.3.0 together with the CR from document IFA(19)000824.
2020/02/10	V0.4.2	Showing proposed changes from CR doc NFAIFA(20)00029r2
2020/02/24	V0.4.5	Showing changes from 29r4 and 128.
2020/02/28	V0.9.0	Proposed final draft
2020/03/04	V0.9.1	Incorporating changes received up to 2020/03/08.
2020/03/25	V0.9.2	Meeting notes from SEC#159
2020/08	V4.1.1	Issued version
2023/04/27	V4.4.2	New draft incorporating changes from: - NFVSEC(22)000097r4 - NFVSEC(23)000006r3 - NFVSEC(23)000007 - NFVSEC(23)000010r2 - NFVSEC(23)000038r1 - NFVSEC(23)000076r1
2023/06/25	V4.4.3	New draft incorporating changes from: - NFVSEC(23)000087r1 - NFVSEC(23)000120r2 - NFVSEC(23)000098r3 - NFVSEC(23)000113r2 - NFVSEC(23)000111r2 - NFVSEC(23)000024r3 - NFVSEC(23)000114r2 - NFVSEC(23)000112 - NFVSEC(23)000132r1 - NFVSEC(23)000100r1 - NFVSEC(23)000156r1 - NFVSEC(23)000157 - NFVSEC(23)000161 - NFVSEC(23)000163r1 - NFVIFA(23)000502r1
2023/08/11	V4.4.4	Final draft incorporating changes from: - NFVSEC(23)000181r3 / NFVIFA(23)000605r2
2024/06/27	V5.1.2	Initial draft version for ed521 created from published version v5.2.1
2024/08/02	V5.1.3	New draft incorporating changes from: - NFVSEC(24)000104r1 - NFVSEC(24)000111 - NFVSEC(24)000127 - NFVSEC(24)000138 Which are also covered by NFVIFA(24)000402r1

Date	Version	Information about changes
2024/09/23	V5.1.4	Incorporating changes from: - NFVSEC(24)000130r2 - NFVSEC(24)000149 - NFVSEC(24)000150 - NFVSEC(24)000153r1 Renumbered clauses from contribution NFVSEC(24)000149 changes #3 & #4 to better accommodate contribution NFVSEC(24)000153r1.
2024/10/02	V5.1.5	Incorporating fixes for review observations. - Clause 10.3.1 CMF.Certm.Del.005 spelling error - Clause 11.4.3.1 table reference - Clause 11.4.4.1 missing table - Clause 11.4.4.2 table heading corrected

History

Document history		
V5.2.1	December 2024	Publication