ETSI GS NFV-IFA 026 V4.5.1 (2023-10)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Architecture enhancement for Security Management 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-IFA026ed451

Keywords

architecture, management, MANO, NFV,
orchestration, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights ... 7

Foreword ... 7

Modal verbs terminology ... 7

1 Scope ... 8

2 References ... 8
2.1 Normative references ... 8
2.2 Informative references ... 9

3 Definition of terms, symbols and abbreviations ... 10
3.1 Terms ... 10
3.2 Symbols ... 10
3.3 Abbreviations ... 10

4 Introduction ... 11

5 Interface and Architectural Requirements ... 12
5.1 Security Management ... 12
5.1.1 Security Manager functional blocks and reference points ... 12
5.1.2 SM Modes ... 13
5.1.3 Multiple Trust Domains and Security Managers ... 13
5.2 Certificate Management ... 14
5.2.1 General ... 14
5.2.1.1 Introduction ... 14
5.2.1.2 General Certificate Management Architecture ... 14
5.2.2 Certificate management function(s) and reference points ... 16
5.2.3 Certificate management options ... 17
5.2.3.1 Overview of certificate management modes for VNFC certificates and VNF OAM certificates ... 17
5.2.3.2 Direct mode ... 17
5.2.3.3 Delegation mode ... 18
5.2.4 Types of Certificates ... 18
5.2.4.1 Description of the types of certificates ... 18
5.2.4.2 VNF Package certificate management ... 18
5.2.4.3 VNFCI certificate management ... 19
5.2.4.3.1 Certificate management ("direct-mode") ... 19
5.2.4.3.2 Certificate management ("delegation-mode") ... 19
5.2.4.4 VNF OAM certificate management ... 20
5.2.4.4.1 Certificate management ("direct-mode") ... 20
5.2.4.4.2 Certificate management ("delegation-mode") ... 20
5.2.4.5 NFV MANO certificate management ... 20
5.2.4.6 Virtualised computation environment control plane certificate ... 20
5.2.5 Multiple Trust Domains and Certificate Management ... 20
5.2.6 General requirements for PKI ... 20

Annex A (normative): SM Reference point functional requirements ... 23

A.0 General ... 23

A.1 Requirements on security management and monitoring from ETSI GS NFV-SEC 013 ... 23

A.2 Additional Requirements ... 26

Annex B (normative): Certificate Management functional requirements ... 31

B.1 Requirements on Certificate Management for certificate management function ... 31
B.1.1 Functional requirements for certificate management function ... 31
B.1.1.1 General considerations ... 31
B.1.1.2 Functional requirements for certificate lifecycle management ... 32

B.2 Functional requirements on Certificate Management for NFVO ... 33

B.3 Functional requirements on Certificate Management for VNFM 33
B.4 Functional requirements on Certificate Management for VIM 34
B.4.1 Functional requirements for virtualised resource management 34
B.4.2 Functional requirements for security consideration 35
B.5 Functional requirements on Certificate Management for WIM 36
B.6 Functional requirements on Certificate Management for CISM 36
B.7 Functional requirements on Certificate Management for CIR 37
B.8 Functional requirements on Certificate Management for CA 37
B.9 General requirements to NFV management and orchestration interface design 37
Annex C (informative): Use Cases for Certificate Management 38
C.1 Use cases for VNF Package certificate management 38
C.2 Use cases for VNFCI certificate management 38
C.2.1 Direct mode 38
C.2.1.1 VNFCI certificate enrollment in direct-mode 38
C.2.1.1.1 Introduction 38
C.2.1.1.2 Trigger 38
C.2.1.1.3 Actors and roles 38
C.2.1.1.4 Pre-conditions 39
C.2.1.1.5 Post-conditions 39
C.2.1.1.6 Operational flows 39
C.2.1.2 VNFCI certificate enrollment with remote attestation in direct-mode 40
C.2.1.2.1 Introduction 40
C.2.1.2.2 Trigger 40
C.2.1.2.3 Actors and roles 40
C.2.1.2.4 Pre-conditions 41
C.2.1.2.5 Post-conditions 41
C.2.1.2.6 Operational flows 41
C.2.1.3 VNFCI certificate enrolment using an HSM in direct-mode 42
C.2.1.3.1 Introduction 42
C.2.1.3.2 Trigger 42
C.2.1.3.3 Actors and roles 43
C.2.1.3.4 Pre-conditions 43
C.2.1.3.5 Post-conditions 43
C.2.1.3.6 Operational flows 44
C.2.1.4 VNFCI certificate renewal in direct-mode 45
C.2.1.4.1 Introduction 45
C.2.1.4.2 Trigger 45
C.2.1.4.3 Actors and roles 45
C.2.1.4.4 Pre-conditions 45
C.2.1.4.5 Post-conditions 45
C.2.1.4.6 Operational flows 46
C.2.2 Delegation mode 46
C.2.2.1 Registration of VNFM as entity in charge of VNFCI certifate management 46
C.2.2.1.1 Intrduction 46
C.2.2.1.2 Trigger 46
C.2.2.1.3 Actors and roles 46
C.2.2.1.4 Pre-conditions 47
C.2.2.1.5 Post-conditions 47
C.2.2.1.6 Operational Flows 47
C.2.2.2 CSR Request for VNFCI certificate 47
C.2.2.2.1 Introduction 47
C.2.2.2.2 Trigger 47
C.2.2.2.3 Actors and roles 48
C.2.2.2.4 Pre-conditions 48
C.2.2.2.5 Post-conditions 48
C.2.2.2.6 Operational Flows 48

C.2.2.2.7 Operational Flows with the use of HSM 48
C.2.2.3 VNFCI certificate installation during VNF Instantiation 49
C.2.2.3.1 Introduction 49
C.2.2.3.2 Trigger 49
C.2.2.3.3 Actors and roles 49
C.2.2.3.4 Pre-conditions 50
C.2.2.3.5 Post-conditions 50
C.2.2.3.6 Operational Flows 50
C.2.2.4 VNFCI certificate installation after VNF Instantiation 50
C.2.2.4.1 Introduction 50
C.2.2.4.2 Trigger 51
C.2.2.4.3 Actors and roles 51
C.2.2.4.4 Pre-conditions 51
C.2.2.4.5 Post-conditions 51
C.2.2.4.6 Operational Flows 52
C.2.2.4.7 Operational Flows with the use of an HSM 52
C.3 Use cases for VNF OAM certificate management 53
C.3.1 Direct mode 53
C.3.2 Delegation mode 53
C.3.2.1 Registration of VNFM as entity in charge of VNF OAM certificate management 53
C.3.2.2 CSR Request for VNF OAM certificate 53
C.3.2.3 VNF OAM certificate installation during VNF Instantiation 53
C.3.2.3.1 Introduction 53
C.3.2.3.2 Trigger 53
C.3.2.3.3 Actors and roles 53
C.3.2.3.4 Pre-conditions 54
C.3.2.3.5 Post-conditions 54
C.3.2.3.6 Operational Flows 54
C.4 Use cases for NFV-MANO certificate management 55
C.4.1 NFVO certificate management 55
C.4.1.1 Registration of NFVO 55
C.4.1.1.1 Introduction 55
C.4.1.1.2 Trigger 55
C.4.1.1.3 Actors and roles 55
C.4.1.1.4 Pre-conditions 55
C.4.1.1.5 Post-conditions 55
C.4.1.1.6 Operational Flows 56
C.4.1.2 CSR Request for NFVO certificate 56
C.4.1.2.1 Introduction 56
C.4.1.2.2 Trigger 56
C.4.1.2.3 Actors and roles 56
C.4.1.2.4 Pre-conditions 56
C.4.1.2.5 Post-conditions 57
C.4.1.2.6 Operational Flows 57
C.4.1.2.7 Operational Flows with the use of HSM 57
C.4.2 VNFM certificate management 58
C.4.2.1 Registration of VNFM 58
C.4.2.1.1 Introduction 58
C.4.2.1.2 Trigger 58
C.4.2.1.3 Actors and roles 58
C.4.2.1.4 Pre-conditions 59
C.4.2.1.5 Post-conditions 59
C.4.2.1.6 Operational Flows 59
C.4.2.2 CSR Request for VNFM certificate 59
C.4.2.2.1 Introduction 59
C.4.2.2.2 Trigger 59
C.4.2.2.3 Actors and roles 60
C.4.2.2.4 Pre-conditions 60
C.4.2.2.5 Post-conditions 60
C.4.2.2.6 Operational Flows 60

C.4.2.2.7 Operational Flows with the use of HSM 60
C.4.3 VIM certificate management 61
C.4.3.1 Registration of VIM 61
C.4.3.1.1 Introduction 61
C.4.3.1.2 Trigger 61
C.4.3.1.3 Actors and roles 61
C.4.3.1.4 Pre-conditions 62
C.4.3.1.5 Post-conditions 62
C.4.3.1.6 Operational Flows 62
C.4.3.2 CSR Request for VIM certificate 62
C.4.3.2.1 Introduction 62
C.4.3.2.2 Trigger 62
C.4.3.2.3 Actors and roles 63
C.4.3.2.4 Pre-conditions 63
C.4.3.2.5 Post-conditions 63
C.4.3.2.6 Operational Flows 63
C.4.3.2.7 Operational Flows with the use of HSM 64

C.5 Use cases for Virtualised computation environment control plane certificate management 64

C.6 VNFCI Certificate Profile Example 64

Annex D (informative): Security consideration for Certificate Management 67

D.1 Additional security considerations and implications for the direct-mode and delegation-mode 67

Annex E (informative): Change History 69

History 71

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document defines the requirements to:

1) interface the Security Control to NFV-MANO as described in ETSI GS NFV-SEC 013 [1];

2) support management of virtualised lawful interception functionality as described in ETSI GR NFV-SEC 011 [i.8], ETSI TS 133 127 [6] and ETSI TS 102 232-1 [7]);

3) interface the Certificate Management Function to NFV-MANO.

The present document identifies the extensions to the NFV-MANO architecture related to security management and monitoring. Multiple trust domains are considered.

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-SEC 013 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security ; Security Management and Monitoring specification".

[2] Void.

[3] ETSI GS NFV-SEC 012 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[4] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement".

[5] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Functional requirements specification".

[6] ETSI TS 133 127: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Lawful Interception (LI) architecture and functions (3GPP TS 33.127)".

[7] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[8] Void.

[9] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[10] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[11] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[12] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[13] IETF RFC 7030: "Enrollment over Secure Transport".

[14] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)".

[15] NIST Special Publication 800-90A Rev 1: "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

[16] NIST Special Publication 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation".

[17] NIST Special Publication 800-90C: "Recommendation for Random Bit Generator (RBG) Constructions"; Third Public Draft (3rd).

[18] FIPS PUB 140-2: "Security Requirements for Cryptographic Modules".

[19] FIPS PUB 140-3: "Security Requirements for Cryptographic Modules".

[20] ISO/IEC 15408-1:2022: "Information security, cybersecurity and privacy protection -- Evaluation criteria for IT security -- Part 1: Introduction and general model".

[21] ISO/IEC 15408-2:2022: "Information security, cybersecurity and privacy protection -- Evaluation criteria for IT security -- Part 2: Security functional components".

[22] ISO/IEC 15408-3:2022 : "Information security, cybersecurity and privacy protection -- Evaluation criteria for IT security -- Part 3: Security assurance components".

[23] EN 419221-5: "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services" (produced by CEN).

[24] ETSI GS NFV-IFA 040: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification".

2.2 Informative references

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

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS NFV-IFA 033: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Sc-Or, Sc-Vnfm, Sc-Vi reference points - Interface and Information Model Specification".

[i.2] ETSI GR NFV 003 (V1.7.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.3] ETSI GR NFV-SEC 005 (V1.2.1): "Network Functions Virtualisation (NFV); Trust; Report on Certificate Management".

[i.4] ETSI GS NFV-SEC 021 (V4.5.1): "Network Functions Virtualisation (NFV) Release 4; Security; VNF Package Security Specification".

[i.5] ETSI TS 133 310 (V16.14.0): "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310 version 16.14.0 Release 16)".

[i.6] Void.

[i.7] ETSI GS NFV-SEC 018: "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".

[i.8] ETSI GR NFV-SEC 011 (V1.1.1): "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[i.9] ETSI TS 102 165-1 (V5.2.5): "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.10] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.11] IETF RFC 7633: "X.509v3 Transport Layer Security (TLS) Feature Extension".

[i.12] IETF RFC 9310: "X.509 Certificate Extension for 5G Network Function Types".

[i.13] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV); Management and Orchestration; VNF Descriptor and Packaging Specification".

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 the following apply:

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

Certificate Management Function: function within an NFV network responsible for the management of certificates, including certificate registration, certificate enrollment, certificate renewal, certificate removal, certificate revocation, certificate monitoring

NOTE 1: The CMF can manage multiple layer certificates (e.g. tenant domain, infrastructure domain, etc.).

NOTE 2: The CMF can manage the following types of certificates: VNF Package certificate, VNFCI certificate, VNF OAM certificate, NFV-MANO (i.e. NFVO, VNFM, VIM) certificate, and virtualised computation environment control plane certificate.

NOTE 3: For container deployments, a local CMF (with sub-CA) may be implemented within the container cluster CISM instance(s) to manage inter VNFCI communication certificates within the CIS cluster.

Security Manager: function within an NFV network responsible for enforcing security policy for VNFs and for instructing NFV-MANO to take VNF specific or system wide security actions

NOTE: The security manager is a logical sub component of a CSP's overall network security management and monitoring systems.

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].

CA	Certificate Authority
CC	Common Criteria
CMF	Certificate Management Function
CMP	Certificate Management Protocol
CSP	Communication Service Provider
CSR	Certificate Signing Request
EAL	Evaluation Assurance Level
EST	Enrollment over Secure Transport
FQDN	Fully Qualified Domain Name
HMEE	Hardware Mediated Execution Environment
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
SAN	Subject Alternate Name
SM	Security Manager
sNSD	security enhanced Network Service Descriptor

4 Introduction

Within a CSP's network, it is necessary to be able to cover different security aspects such as security management and monitoring, authentication and authorization, including certificate management.

Part of the security management aspects includes the need to monitor and manage all components making up a network (including application layer software, NFVI software and hardware components). Therefore, a CSP's overall security management platform needs to have real-time access and understanding of NFV-MANO VNF orchestration and management events. In some scenarios it is sufficient to simply observe and alert on those events from a security perspective, while in other scenarios the CSP security management platform may be required to specifically authorize some or all actions undertaken by NFV-MANO. A CSP security management platform may require one or more Security Manager (SM) depending on the security isolation required between different trust domains.

ETSI GS NFV-SEC 013 [1] describes security management and monitoring in an NFV environment. The NFV SM as described in ETSI GS NFV-SEC 013 [1] is responsible for making security decisions associated with the instantiation, modification and termination of VNFs.

In order to achieve this the SM requires real-time information from NFV-MANO on VNF instantiation, modification and termination. This information needs to be sufficiently detailed for the SM to be able to resolve the type and version of a VNF(s) being instantiated, VNFD constraints applied to those VNFs, OSS/BSS application layer VNF(s) ID(s) (i.e. VNF instance name) and information about the intended physical hardware environment (host IDs/location, etc.). It is not important to the SM which NFV-MANO sub-components provide which specific pieces of information but it is important that the information is provided in an intelligible format. The SM is responsible for maintaining the cumulative state of the information received from NFV-MANO. However, in the case of SM failure or for state recovery under network/NFV-MANO failure conditions, it is desirable for NFV-MANO to be able to provide the SM with the current state of all VNFs (including hardware/resource usage and VNF and VNFCI interconnections routing table).

The SM is responsible for analysing information received from NFV-MANO and where necessary instructing NFV-MANO to take actions accordingly (e.g. applying security policy to a VNF being instantiated). In addition, when the SM becomes aware of a security event (e.g. VNF compromise) the SM is responsible for instructing NFV-MANO to take appropriate mitigating actions (e.g. terminate a VNF instance or put a VNF into quarantine). NFV-MANO and wider network auto recovery mechanisms need to ensure that they are able to handle SM enforced VNF decisions and NFV-MANO does not attempt to restart or migrate VNFs that the SM has requested be terminated or quarantined.

In scenarios where there is not a single legal entity or CSP operating the entire virtual network (e.g. tenant hosted scenarios), the SM(s) implementation will need to ensure isolation of information, events or policy is maintained between different entities.

Where NFV-MANO has visibility of PNFs (e.g. by association with SDN routing to and from VNFs), that information also needs to be provided to the SM by NFV-MANO.

In addition, a CSP's network is expected to include solutions for network secure communications. The deployment of these solutions heavily depends on the orchestration and management of public key certificates at different realization layers.

As described in ETSI GR NFV-SEC 005 [i.3], there are several types of public key certificates to be managed in the CSP network through the establishment of one or more PKIs. In ETSI GS NFV-IFA 010 [5], the Certificate Management Function (CMF) is introduced for the automated management of certificates for secure communications in the NFV architectural framework. A CSP may require one or more CMFs depending on the security isolation required between different domains. An CMF interacts with the various CSP CA(s) and their functions to provide various certificate management services (e.g. end-entity registration, certificate enrolment, revocation, etc.) and is responsible to synchronize the LCM operations for certificates with the VNF LCM.

The present document contains the NFV architectural framework enhancements with the respective security entities, including SM, CMF and CA.

Annex A, contains a set of requirements and analysis for each of the reference points between NFV-MANO and the SM defined in clause 5. These requirements are derived from but not limited to those in ETSI GS NFV-SEC 013 [1].

Annex B addresses the certificate management related requirements.

5 Interface and Architectural Requirements

5.1 Security Management

5.1.1 Security Manager functional blocks and reference points

Figure 5.1-1 shows the three new reference points and one new functional block which are required to be added to the underlying NFV architecture to support security monitoring and management, as defined in ETSI GS NFV-SEC 013 [1].

The new functional block is the Security Manager (SM). It may be necessary to have more than one Security Manager in order to meet all the security requirements, in which case each SM shall be handled independently within a separate trust domain using separate instances of endpoints on relevant interfaces defined over the three reference points. In the case of multiple security managers, each security manager may be authorized to perform different sub-sets of the requirements listed in annex A.

The three reference points are:

- Sc-Or: the reference point between the Security Manager and the NFV Orchestrator.
- Sc-Vnfm: the reference point between the Security Manager and VNF Manager.
- Sc-Vi: the reference point between the Security Manager and Virtualised Infrastructure Manager.

NOTE: The interfaces which run over these reference points are defined in ETSI GS NFV-IFA 033 [i.1], which also contains requirements for those interfaces.

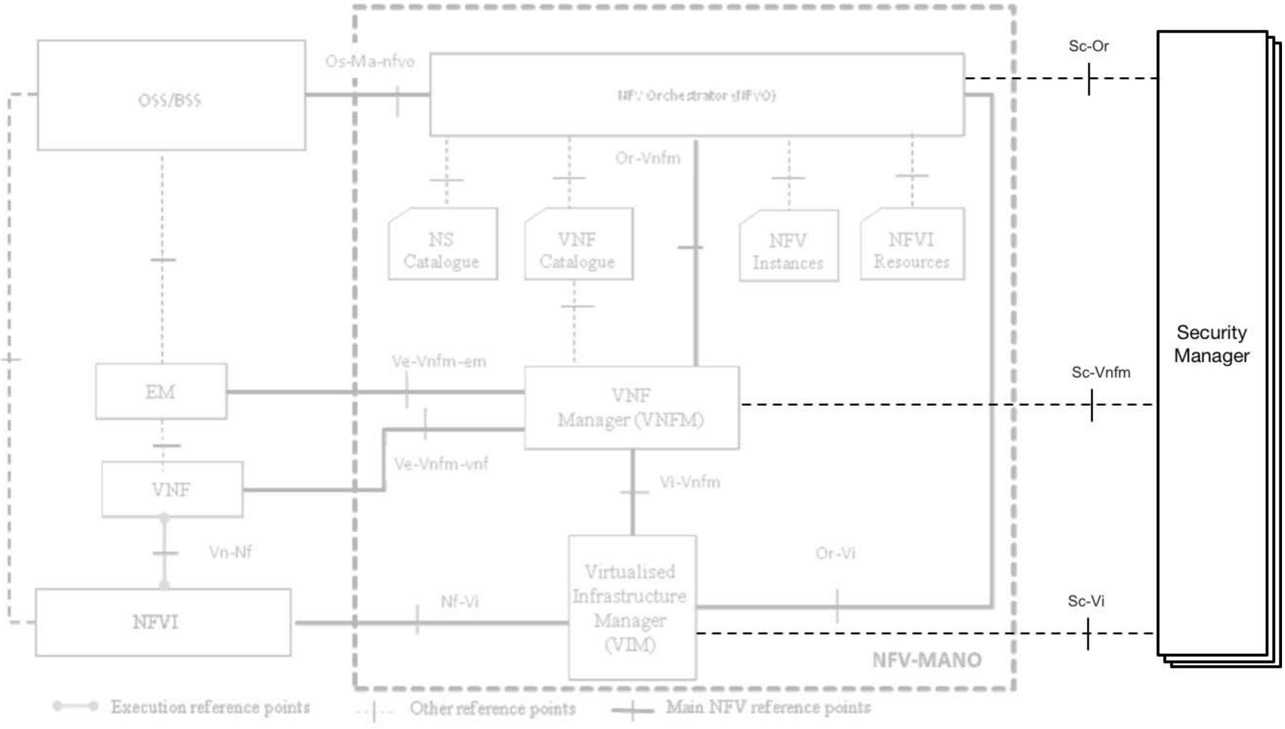

Figure 5.1-1: Security Manager and NFV-MANO Reference Architecture

5.1.2 SM Modes

The SM and NFV-MANO shall support three modes of operation:

- Passive: SM is able to subscribe to applicable lifecycle management events passed to it by NFV-MANO but the SM does not take any active part in the lifecycle management of the VNFs.
- Semi-Active: SM analyses applicable lifecycle management events passed to it by NFV-MANO. The SM may provide security policies to NFV-MANO as part of a VNF lifecycle management but the SM takes an otherwise passive part in VNF lifecycle management. The SM is able to request NFV-MANO to undertake security mitigation actions (e.g. terminate a VNF instance).
- Fully-Active: NFV-MANO passes applicable VNF lifecycle events to the SM and requests approval from the SM. The SM authorizes, modifies with security policy, or rejects NFV-MANO requests. The SM is also able to instruct NFV-MANO to take security mitigation actions (e.g. immediately terminate a VNF instance).

NOTE: The full scope of lifecycle events which are applicable to the SM in Passive, Semi-Active and Fully-Active modes are outside the scope of the present document. However, the applicability of specific VNF lifecycle management events would be determined based on the necessity to meet the requirements defined in clause 5 and annex A.

5.1.3 Multiple Trust Domains and Security Managers

In networks with multiple trust domains or where a CSP wishes to achieve security role separation, there may be one or more SMs. Each SM may operate in Passive, or Semi-Active or Fully Active mode as described in clause 5.1.2.

It shall be possible for the SMs to act independently of each other or for SMs to operate in a hierarchical arrangement where one SM may be able to issue VNF termination instructions across all trust domains of one or more sub SMs.

NOTE: In hierarchy terms, a sub SM is an SM which is overseen or controlled by another higher security level SM. For example, a sub SM in Semi-Active Mode may be subservient to a network wide Fully Active SM. The sub SM is able to fulfil its role autonomously but the higher-level SM would be able to overrule it at any time. NFV-MANO needs to be able to support such hierarchical models and provide interface instance isolation for such sub SM to SM relationships.

Each SM shall interface to NFV-MANO using a logically separate, dedicated instance of interfaces as defined in clause 5.1. Each set of SM to NFV-MANO interfaces shall use independent integrity and confidentially protection from all other SM to NFV-MANO interface sets.

NFV-MANO is responsible for ensuring 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.

NFV-MANO shall not accept instructions from an SM in one trust domain for VNFs managed by another SM in another trust domain (hierarchical layering requirement above notwithstanding).

SM to NFV-MANO trust domain separation shall include support for management of sensitive components as defined in ETSI GS NFV-SEC 012 [3].

NFV-MANO shall support an authorization framework where each SM is authorized in Passive or Semi-Active or Fully-Active mode to undertake interactions with NFV-MANO.

Each SM to NFV-MANO authorization shall be independent of any other SM binding. NFV-MANO shall ensure that each SM is invisible to any other SM (hierarchical layering requirement notwithstanding).

Where one SM spans multiple trust domains, it shall be possible for the SM to operate in different modes (Passive, Semi-Active, Fully-Active) for each trust domain.

NFV-MANO shall be able to manage and authorize these different modes for different trust domain for a single SM independently.

The present document assumes that where more than one SM exist in an NFV implementation, one SM will act as a master SM such that is able to instruct NFV-MANO to immediately terminate any VNF belonging to any sub SM trust domain or over-rule the actions of a sub SM.

Where NFV-MANO is required to maintain audit logs of lifecycle managements events, NFV-MANO shall be able to separate these based on the SM and trust domain separation requirements above.

Detailed requirements for multiple trust domains and multiple SMs are defined in annex A.

5.2 Certificate Management

5.2.1 General

5.2.1.1 Introduction

The NFV Architectural Framework shall support automated certificate management for the NFV-MANO functional entities and VNF in order to secure the connections on all the interfaces in NFV Architectural Framework.

The present document introduces the Certificate Management Function (CMF) in the NFV Architecture Framework to manage certificates of NFV-MANO and VNFs. CMFs enable the distribution and management of trusted certificates issued by a centralized authority, which are used for verifying the identity of VNFs and other components in NFV systems.

The following sections will outline certificate management function(s), the integration of CMF and Certification Authority (CA) in the NFV Framework Architecture, and the requirements for its secure implementation in NFV-MANO.

5.2.1.2 General Certificate Management Architecture

Figures 5.2.1.2-1, 5.2.1.2-2 and 5.2.1.2-3 show the overall interactions expected between the NFV-MANO architectural framework and certificate management functions such as the CMF and CA:

- Figure 5.2.1.2-1 shows the certificate management architecture in "direct-mode" (see clause 5.2.3) for VNFCI and VNF OAM certificates (see clause 5.2.4) in the context of the NFV architectural framework.

- Figure 5.2.1.2-2 shows the certificate management architecture in "delegation-mode" (see clause 5.2.3) for VNFCI and VNF OAM certificates (see clause 5.2.4) in the context of the NFV architectural framework.

- Figure 5.2.1.2-3 shows the certificate management architecture for NFV-MANO certificates (see clause 5.2.4) in the context of the NFV architectural framework.

NOTE: Definition of interfaces marked with dotted-line as out of scope of the current version of the present document requires further study and requires alignment with existing security standards (e.g. 3GPP, IETF, etc.)

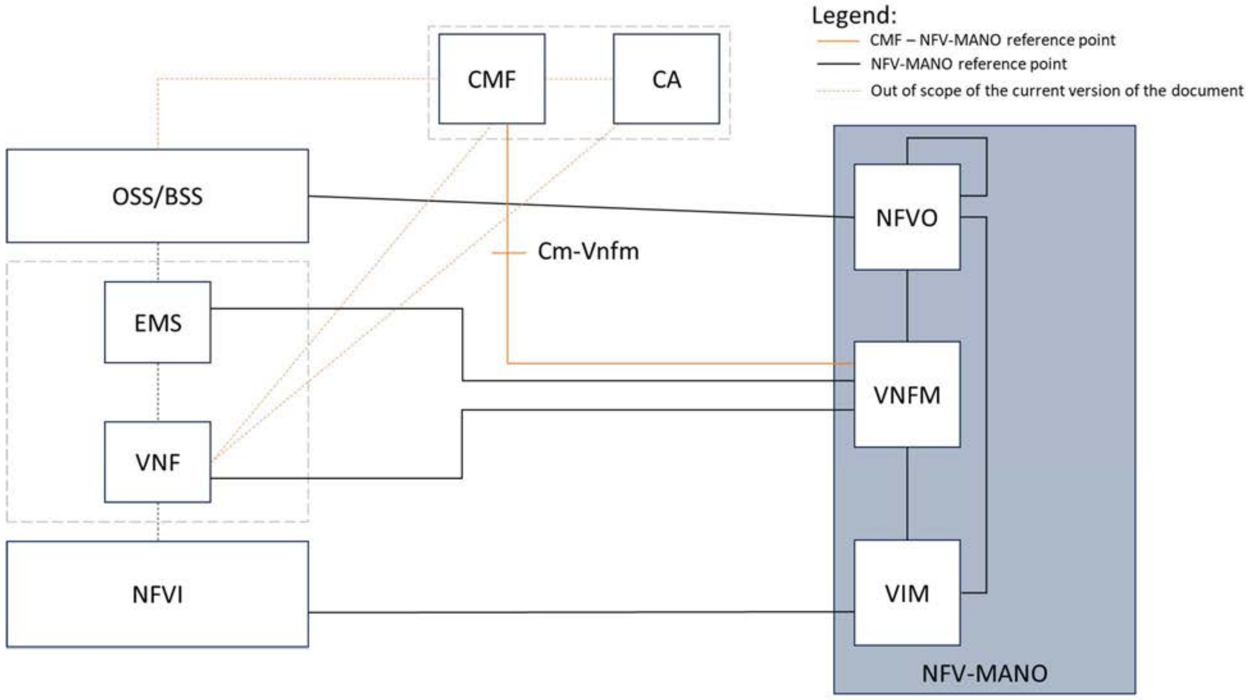
Legend:
CMF – NFV-MANO reference point
NFV-MANO reference point
Out of scope of the current version of the document
CMF
CA
OSS/BSS
Cm-Vnfm
NFVO
EMS
VNFM
VNF
NFVI
VIM
NFV-MANO

Figure 5.2.1.2-1: Certificate management in the NFV architecture - "direct-mode" for VNFCI and VNF OAM certificate management

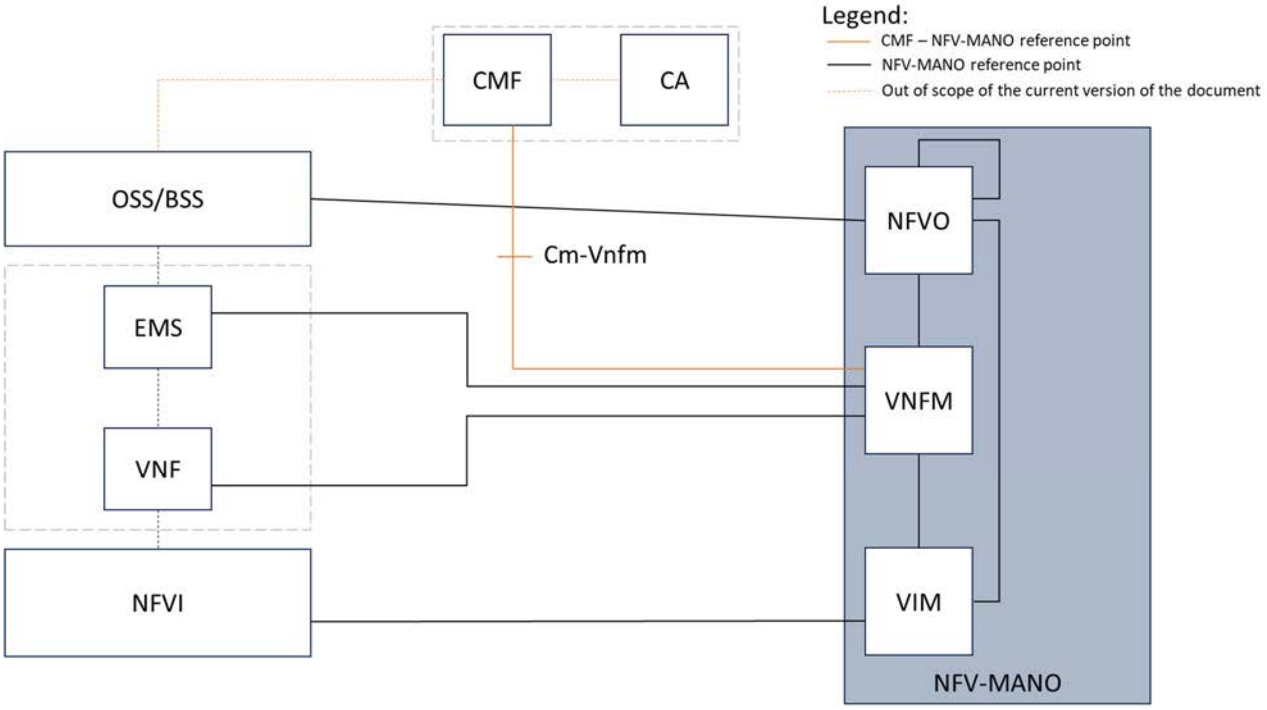
Legend:
CMF – NFV-MANO reference point
NFV-MANO reference point
Out of scope of the current version of the document
CMF
CA
OSS/BSS
NFVO
Cm-Vnfm
EMS
VNFM
VNF
NFVI
VIM
NFV-MANO

Figure 5.2.1.2-2: Certificate management in the NFV architecture - "delegation-mode" for VNFCI and VNF OAM certificate management

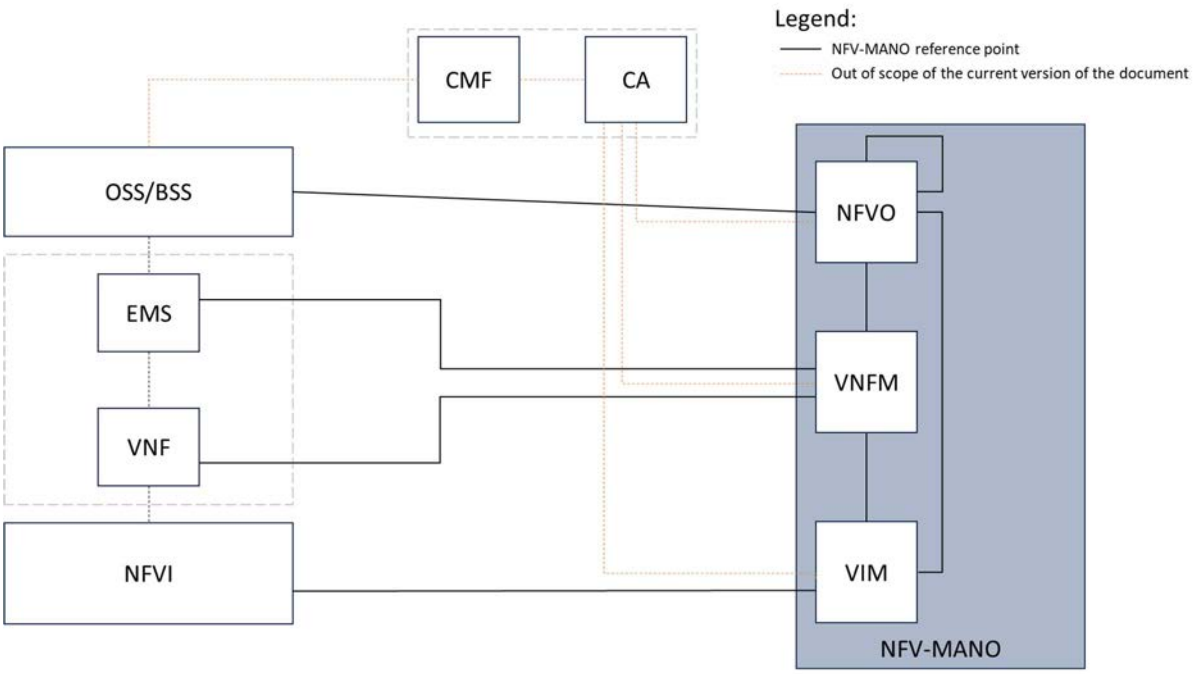

Figure 5.2.1.2-3: Certificate management in the NFV architecture NFV-MANO certificate management

While the above figures show a logical and functional separation of CMF and CA, they do not preclude deployments where the CMF and CA are collocated by CSP operator decision, see also clause 5.2.1.1.

5.2.2 Certificate management function(s) and reference points

The Certificate Management Function (CMF) provides services for the certificate management in the NFV architectural framework. The CMF offers certificate management services to support establishing secure communications (e.g. TLS) for VNFs and for NFV-MANO entities.

More than one CMF may be required to achieve certificate management requirements depending on the CSP network architecture, existing Certificate Authority (CA) hierarchies, or domains isolation. The CMF is trusted by the CSP's or the tenant's CA.

The CMF exposes certificate management services over an interface referred here in as CMF-1, as illustrated in Figure 5.2.2-1. This interface is described in ETSI GS NFV-IFA 033 [i.1].

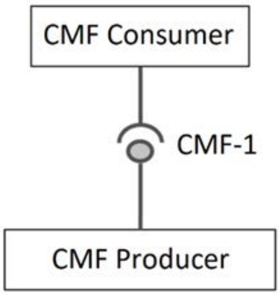

Figure 5.2.2-1: CMF-1 interface exposed by a CMF for CMF consumers

For VNF certificate management, the CMF synchronizes the certificate LCM with the respective VNF LCM events. For this purpose, CMF consumes NFV-MANO interfaces for VNF LCM occurrence events. A CMF supports certificate monitoring of these VNF instances and obtains relevant information from NFV-MANO, e.g. VNF/VNFC(s) runtime information, etc. The information exchanges between CMF and the NFV architectural framework are captured in the new reference points:

- Cm-Vnfm: the reference point between CMF and VNFM, as described in ETSI GS NFV-IFA 033 [i.1].

The CA exposes certificate automation services over an interface referred here in as CA-1, as illustrated in Figure 5.2.2-2. This interface is described in ETSI GS NFV-IFA 033 [i.1]. This interface is defined in IETF.

NOTE: CA-1 is assumed to be used for dotted-lines terminating into the CA in the figures 5.2.1.2-1, 5.2.1.2-2 and 5.2.1.2-3 of clause 5.2.1.2.

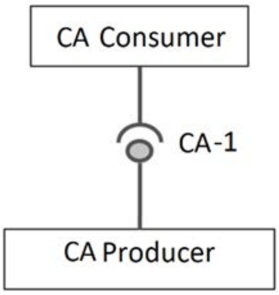

Figure 5.2.2-2: CA-1 interface exposed by a CA for CA consumers

CMF and CA communicate for purposes of certificate end-entity registration, protocol support for certificate enrollment, end-entity certificate revocation support, OCSP stapling, CRL, etc. The full detail of the interfaces between the CA and CMF are out of scope of the present document.

5.2.3 Certificate management options

5.2.3.1 Overview of certificate management modes for VNFC certificates and VNF OAM certificates

The CMF shall support at least one of the following options: direct-mode or delegation-mode (as described in clauses 5.2.3.2 and 5.2.3.3, respectively). In some scenarios, both modes may be supported for interoperability. VNFs shall support one of the two modes for simplicity, VNFM shall support at least one of the two modes and shall support both in the context of a generic VNFM. NFVO, VIM and CISM shall support both of the two modes for interoperability.

These modes apply to the management of VNFC certificate (see clause 5.2.1.2) and VNF OAM certificates (see clause 5.2.1.2). In direct-mode, VNFI(s)/VNFCI(s) directly communicate with CA for their certificate and certificate chain. In delegation-mode, VNFM, on behalf of VNFI(s)/VNFCI(s), requests CMF for their certificate and certificate chain. NFV-MANO entity then goes on to install the certificate and certificate chain into VNFI(s)/VNFCI(s).

In direct mode it is assumed that the private keys are generated by a tamper resistant function and are never exposed outside of the function for which they are generated, whereas delegation mode requires transport of private keys from the VNFM to the VNFs. The mode(s) to be used is decided based on the operator's decision.

Additional security considerations and implications for the two modes are provided in Annex D.

5.2.3.2 Direct mode

This mode corresponds to the PKI arrangement which uses the interfaces between VNF and CMF and between VNF and CA, as illustrated in Figure 5.2.1.2-1. Adapted to the domain specific requirements, an CMF mediates and automates initial registration at the CA for the VNFI(s)/VNFCI(s) end-entities dedicated to inter-VNFI secure communications. In the direct mode, the VNFI(s)/VNFCI(s) themselves generate public and private key pairs for their VNFI(s)/VNFCI(s) certificates, initiate the CSR request toward CA for their certificate enrolment, and certificate chains.

In direct mode, as detailed in ETSI GS NFV-IFA 033 [i.1], the Cm-Vnfm reference point consists only of the VNF LCM interface consumed by the CMF for the notifications of VNF LCM operation occurrence events and Query VNF.

5.2.3.3 Delegation mode

This mode corresponds to the PKI arrangement illustrated in Figure 5.2.1.2-2. In this mode, the interfaces between VNF and CMF and between VNF and CA are not used for managing VNFC certificates and VNF OAM certificates. Instead, VNFM acts as a delegate for certificate management operations on behalf of VNFI(s)/VNFCI(s) by doing the following:

- generating VNFI(s)/VNFCI(s)'s public and private key pair(s);
- mediating registration for VNFI(s)/VNFCI(s) toward CMF;
- initiating CSR request toward CMF to acquire certificates for VNFI(s)/VNFCI(s); and
- installing the certificates and certificate chains to VNFI(s)/VNFCI(s) by VNF LCM via VIM/CISM (on Vi-Vnfm/CISM service interface) or directly to the VNFI(s)/VNFCI(s) (on Ve-Vnfm-vnf).

5.2.4 Types of Certificates

5.2.4.1 Description of the types of certificates

As described in ETSI GR NFV-SEC 005 [i.3] and ETSI GS NFV-SEC 021 [i.4], the types of certificates used in the NFV Architectural Framework are as follows:

- VNF Package certificate: used for signing and verification of VNF Package, as defined in clause 6.2 of ETSI GS NFV-SEC 021 [i.4]).
- VNFCI certificate: used for securing the connection between applications of VNFCIs; this type of certificates includes the certificate(s) for inter-VNFI secure communications and certificates for intra-VNFI secure communication (see note 1).
- VNF OAM certificate: used for securing the connection between VNFCI and NFV-MANO/EM (see note 2).
- NFV-MANO certificate: used for securing the connection between NFV-MANO functional entities (see note 3).
- Virtualised computation environment control plane certificate: used for the secure communications between control plane components of the given virtualised computation environment (see note 4).

NOTE 1: Defined as "VNFCI transport certificates and Application OM certificates" in clause 7.2 of ETSI GR NFV-SEC 005 [i.3]. The "VNFCI transport certificates" category is further detailed in clause 10.5.2 of ETSI GR NFV-SEC 005 [i.3].

NOTE 2: Defined as "VNF OM certificate" in clause 7.2 of ETSI GR NFV-SEC 005 [i.3].

NOTE 3: Defined as "MANO certificate" in clause 7.2 of ETSI GR NFV-SEC 005 [i.3].

NOTE 4: Defined as "VM certificate" for hypervisor-based virtualisation and CIS cluster control plane layer certificate for OS container-based virtualization in clauses 7.2 and 10.5.2, respectively, of ETSI GR NFV-SEC 005 [i.3].

5.2.4.2 VNF Package certificate management

Management of VNF Package certificates is not considered in the current version of the present document.

5.2.4.3 VNFCI certificate management

5.2.4.3.1 Certificate management ("direct-mode")

The initial configuration of each CA responsible to issue VNFCI certificates in the CSP domain(s) is expected to include the following:

- Information necessary for the CMF - CA secure communication.
- Information related to the expected VNFCIs certificate templates in the given CSP domain(s).
- Information including the VNFCI end-entities certificate enrolment profiles, which typically indicate the CA supported certificate management protocol(s) (e.g, CMPv2, EST) and corresponding protocol(s) configuration.

Prior to any certificate enrolment procedures, the initial configuration of each CMF in the CSP domain(s) is expected to include the following:

- CA-related information including the set of trusted CA(s) in charge of issuing the VNFCI end-entities certificates for the given domain.
- Information necessary for the CMF - CA secure communication.
- Information related to the expected VNFCIs certificate templates, with the set of CA-supported enrolment protocols.
- Information related to the CMF - VNFCI authentication credentials (e.g. trusted CMF certificate in case of TLS, host keys in case of SSH).

These CMF and CA initial configurations, which include critical information such as the list of trusted CA(s), set of permitted certificate templates in the given CSP domain(s), etc., should be realized with human actions over secure management interfaces (such channels may be offline physical interventions).

Based on the CMF initial configuration as well as on the retrieved VNF LCM occurrence events from NFV-MANO, the CMF mediates various certificate management operations. In case of a newly instantiated VNFCI with identities to be registered to the CA the CMF obtains VNFCI asset data through interacting with external entities including details for each identity of the VNFCI. Examples of such VNFCI configuration details are certificate DN fields, certificate profile SAN fields (e.g. DNS name/FQDN), which are used by the CMF to register the VNFCI to the CA. This configuration and interaction is outside the scope of the present document.

The flow in clause C.2.1.1 provides more details on the various steps for the VNFCI certificate enrolment in "direct-mode". The flow in clause C.2.1.2 provides details on how to couple the VNFCI certificate enrolment in "direct-mode" with remote attestation and HMEE. Clause C.2.1.3 provides an additional flow using an HSM. In clause C.6, a certificate profile is exemplified with certificate fields expected to be either part of a predefined certificate profile in the CA or coming from a CSR supplied by the VNFCI end-entity. The flow in clause C.2.1.4 provides details on the VNFCI certificate renewal in "direct-mode".

5.2.4.3.2 Certificate management ("delegation-mode")

In delegation-mode, VNFM acts as a delegate for certificate management operations on behalf of VNFI(s)/VNFCI(s). During VNF instantiation process, the VNFM registers the VNFI(s)/VNFCI(s) with the CMF as end entities, initiates certificate signing request (CSR) toward the CMF, gets certificates on behalf of VNFI(s)/VNFCI(s), then provides the certificates to VNFI(s)/VNFCI(s).

The VNFM obtains information required for registration and CSR from the VNFD and OSS via NFVO. Examples of such details are certificate DN fields, certificate profile SAN fields (e.g. DNS name/FQDN).

The initial configuration of each CA/CMF responsible to issue VNFCI certificates in the CSP domain(s) is expected to include the following:

- CA/CMF supported certificate management protocol(s) (e.g. CMPv2, SCEP) and corresponding protocol(s) configuration.

- MANO entities, i.e. NFVO, VNFM and VIM, have already obtained their own certificates communicating with CMF/CA. As a result, MANO entities have their own certificates and have established secured connections between CMF and other MANO entities.

The flows in clauses C.2.2.1 to C.2.2.4 provide more details on the various steps for the VNFCI certificate management in "delegation-mode".

5.2.4.4 VNF OAM certificate management

5.2.4.4.1 Certificate management ("direct-mode")

VNF OAM certificate management is the same as VNFCI certificate management as described in clause 5.2.4.3.1 for the distribution of VNFCI certificates (see clause C.3.1).

5.2.4.4.2 Certificate management ("delegation-mode")

VNF OAM certificate management is the same as VNFCI certificate management as described in clause 5.2.4.3.2 for the distribution of VNFCI certificates. VNF OAM certificate is needed before secure communication with NFV-MANO can be established.

5.2.4.5 NFV MANO certificate management

Registration of NFV-MANO functional entities, i.e. NFVO, VNFM and VIM, is done by OSS. If the registration is successful, NFV-MANO functional entities initiate Certificate Signing Request (CSR) toward the CMF/CA and obtain their respective NFV-MANO certificates.

The initial configuration of each CA/CMF responsible to issue MANO certificates in the CSP domain(s) is expected to include the following:

- CA/CMF supported certificate management protocol(s) (e.g. CMPv2, SCEP) and corresponding protocol(s) configuration.

- Certificate Chain information including the set of trusted CA(s) in charge of issuing the MANO certificates for the given domain.

The flows in clause C.4 provide more details on the various steps for MANO certificate management.

5.2.4.6 Virtualised computation environment control plane certificate

Management of Virtualised computation environment control plane certificates is not considered in the current version of the present document.

5.2.5 Multiple Trust Domains and Certificate Management

Multiple Trust Domains and Certificate Management is not considered in the current version of the present document.

5.2.6 General requirements for PKI

As described in ETSI GR NFV-SEC 005 [i.3], management of these certificates as described in clause 5.2.4 shall include the establishment of one or more PKIs. The set of participants in a PKI include end-entities to which certificates are issued, the CA issuing them, and RA collecting and verifying client information. A PKI may have multiple issuing CAs organized in hierarchies. RA may also be involved in PKIs.

A CA refers to the entity that manages one PKI and is not seen as the organization or system that can manage several PKIs. CMF has PKI capability and communicate with the operator's Centralized CA.

Figure 5.2.6-1 illustrates an example of a PKI arrangement for a high-level view of an NFV deployment with both OS container-based and VM-based VNFs and with a common central root CA. The illustrated CMF includes the NFV-MANO functions that manage and orchestrate this NFV deployment. The illustrated layers are associated with one or several of the certificate categories introduced in the present clause:

- VNF application layer includes VNFCI certificates for the inter-VNFI secure communications.
- VNF layer includes VNFCI certificates for the intra-VNFI secure communications and the VNF OAM certificates.
- Hypervisor (for VM-based VNF) and CIS instance/CISM layer (for OS container-based VNFs) include virtualized computation environment control plane certificates.

Regarding the centralized CA and CMF, figure 5.2.6-1 illustrates a logical and functional separation of CA and CMF. CA and CMF deployments shall be separated; exceptions include specific network deployments where the high-level of risks (see note 1) of combining CA and CMF can be mitigated through specific scenarios of ensuring that the functions are not exposed to external networks, e.g. closed and dedicated networks industrial network not connected to the Internet.

NOTE 1: For more information about risks levels definitions refer to ETSI TS 102 165-1 [i.9].

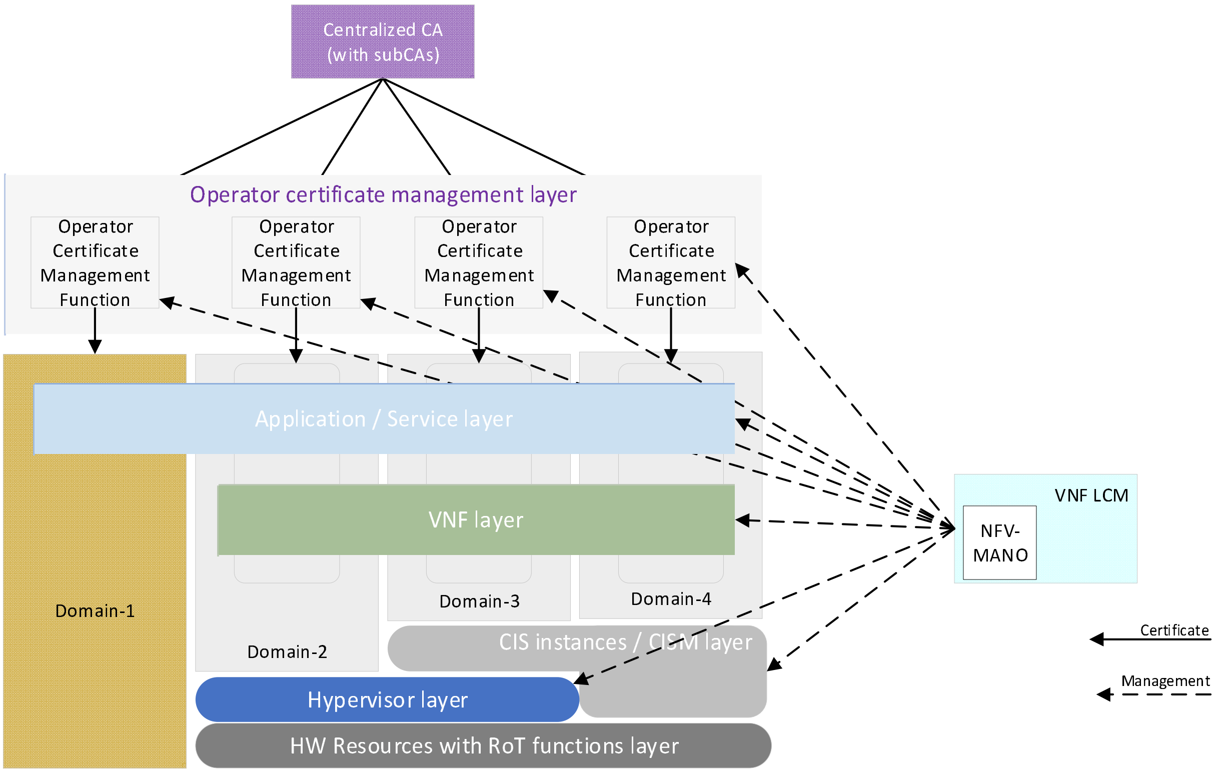
Centralized CA (with subCAs)
Operator certificate management layer
Operator Certificate Management Function
Operator Certificate Management Function
Operator Certificate Management Function
Operator Certificate Management Function
Application / Service layer
VNF layer
Domain-1
Domain-2
Domain-3
Domain-4
CIS instances / CISM layer
Hypervisor layer
HW Resources with RoT functions layer
VNF LCM
NFV-MANO
Certificate
Management

Figure 5.2.6-1: High-level view showing CA components

In this example, it is implied that VNFCI certificates (e.g. for the inter-VNFI secure communications) come from the centralized CA via an CMF implementing a CA specific API (see Annex B for the functional requirements for Certificate Management Function). One CMF is illustrated per domain (e.g. trust-domain, infrastructure network domain) although deployments may also use one CMF for multiple domains according to the security policy, certificate policy, etc. defined by the network operator.

In the case of direct-mode, each CMF communicates with VNFM for purposes of synchronizing LCM operations for certificates with VNF LCM. An CMF coordinates and monitors lifecycle management of certificates in their associated domain(s) and supports retrieval from the VNFM of VNF/VNFC runtime information and VNF LCM events. Additionally, CMF keeps track of the associated certificates with each of the VNF/VNFC instances and is able to query runtime information for those VNF/VNFCs. In the case of delegation-mode, VNFM, acting as a Delegate for VNFCIs, initiates registration and CSRs towards the CMF for VNFCI certificates. VNFM coordinates and monitors lifecycle management of certificates in their associated domain(s) instead of a CMF.

Adapted to the domain specific requirements, an CMF mediates and automates initial registration and certification at the CA for at least the VNFCI(s) end-entities dedicated to inter-VNFI secure communications. This implies that CMF is trusted by the CA and may also act in one or several of the following roles:

- a certificate enrolment server, which may implement an RA role;
- a proxy between tenant CA and other PKI participants (e.g. RAs) which are closely involved in handling for example certificate requests for intra-VNFI secure communications (see note 2).

NOTE 2: An example of PKI participant closely involved in handling VNFCI certification for intra-VNFI secure communications is the Certificate Client in clause 10.5.4 of ETSI GR NFV-SEC 005 [i.3].

The initial registration of an end-entity such as a VNFCI is a process through which the end-entity is made known to a CA or RA. Successful end-entity initial registration at the CA eventually results in the CA issuing a certificate for the end-entity public key. Prior to the issuing, several steps are typically executed: end-entity initialization with generation of initial credentials required during the certificate enrolment procedure, private/public key pair(s) generation, certificate chain certificate secure provisioning necessary to validate certificate paths and other configurations for successful generation of initial certificate requests.

Only those VNFCIs with VNF external secure communication requirements may be registered at the CA during their instantiation. For intra-VNFCI secure communications requirements VNFCIs may be registered with a CA local to the VNF. In the case of direct-mode, the VNFC lifecycle is monitored by CMF so that CMF, acting for example as an RA, can trigger certificate lifecycle management operations leading to for example creation or revocation of certificates. Thus, CMF is aware of the VNFI internal components, relationship between them as well as the service topology in a given domain. In the case of delegation-mode, the VNFC lifecycle is monitored by VNFM, and OSS can trigger certificate lifecycle management operations via NFVO to VNFM.

CMF may also have an active role in NFV deployments involving VNF secure bootstrapping with remote attestation and HMEE where VNFCI initial registration at CA is conditioned by a successful remote attestation. In this case, CMF may interact with an attestation service (see note 3) so that certificate requests be validated as originating attested VNFCIs.

NOTE 3: An example of "attestation service" is the Verification Function in clause 5.1 of ETSI GR NFV-SEC 018 [i.7].

Annex A (normative): SM Reference point functional requirements

A.0 General

This annex provides requirements to be supported by NFV-MANO over the three functional reference points identified in clause 5.1 and the consequential functional requirements on the NFV-MANO functional blocks terminating those reference points. Clause A.1 provides requirements derived directly from ETSI GS NFV-SEC 013 [1], while clause A.2 provides additional requirements to address areas which are not covered in ETSI GS NFV-SEC 013 [1] in sufficient detail.

A specific NFV-MANO and SM pairing will support a subset of these requirements depending on the operational deployment model and the role of the SM.

The requirements includes functionality required to support the LI Controller as specified in ETSI GR NFV-SEC 011 [i.8].

The assignment of specific requirements in this annex to one or more of the 3 functional reference points (Sc-Or, Sc-Vnfm, Sc-Vi) as described in clause 5, is provided in ETSI GS NFV-IFA 033 [i.1].

A.1 Requirements on security management and monitoring from ETSI GS NFV-SEC 013

The following requirements are derived from ETSI GS NFV-SEC 013 [1].

In ETSI GS NFV-SEC 013 [1], clause 6.5.1 "Requirements for Multi-Trust-Domain Security Management":

R1.1.10. Entities (e.g. VNFs) building up telco networks (e.g. IMS network) shall be assignable to different trust domains.

R1.1.20. One or more dedicated NFV-MANO trust domains shall exist.

R1.1.30. Each NFV-MANO functional block shall be assignable to one or more dedicated NFV-MANO trust domain(s).

R1.1.40. Trust relationships shall be defined between trust domains.

R1.1.50. For two or more domains without existing trust relationships, the effect of an attack on one domain shall not impact the other domains either directly or indirectly (e.g. through Management channels).

R1.1.60. MANO shall support one or more NFV SMs, per trust domain.

R1.1.70. There shall be controls enforcing separation of duties and privileges, least privilege use and least common mechanism between security management and NFV-MANO. These controls shall apply in conjunction with the corresponding separation of trust domains.

R1.1.80. A NFV SM shall manage security policies and implement the security requirements of a trust domain to be implemented by dedicated security functions or security functions embedded within VNFs.

R1.1.90. A SM shall manage security policies and requirements between trust domains according to the defined trust relationship, including establishing security association between VNFs in different trust domains and between VNFs and NFV-MANO entities when it has visibility and permissions available to perform such duties:

- Security policies reflecting trust relationships between trust domains could include access control (authentication and authorization), traffic/resource separation and segmentation, VPN SeGW, etc.

R1.1.100. A SM shall manage security policies within a trust domain, including establishing security association between VNFs within a single trust domain.

Security policies within each trust domain included e.g. initial key provisioning for secure communication between VNFs, authentication and authorization mechanisms, firewalls, etc.

R1.1.110. SMs shall be able to interact (where authorized) with each other for requesting/providing required security services for e.g. cross-domain security management.

R1.1.120. One or more dedicated trust domains for Security Management shall exist.

R1.1.130. SM shall be assignable to one of the dedicated Security Management trust domains.

R1.1.140. The SM shall be instantiated on a host system which meets the requirements laid out in ETSI GS NFV-SEC 012 [3].

R1.1.150. The SM may be deployed as virtualised workload.

R1.1.160. Traffic of SM shall be isolated and separated from other traffics in data/control planes, etc.

In ETSI GS NFV-SEC 013 [1], clause 6.5.2 "Requirements for Network Security Management":

R1.2.10. The NFV security management system shall support the security lifecycle management as introduced in ETSI GS NFV-SEC 013 [1], clause 6.1:

- The security management system shall support capabilities allowing operators to perform security policy planning for network services, which includes security policy initial design and optimization.

- The security management system shall support a capability allowing operators to enforce (including validate) the designed security policies throughout the network service lifecycle.

- The security management system shall support a capability allowing operators to perform security monitoring as described in ETSI GS NFV-SEC 013 [1], clause 7.

R1.2.20. The operator's security management system shall support a capability to manage security functions in both virtualised and physical networks within bounds of trust domains.

R1.2.30. The NFV security management system shall support a capability allowing operators to automate the security management functions.

R1.2.40. To facilitate security policy design, the SM shall support checking the availability and capabilities of VSFs and ISFs (via ISM), as well as PSFs (via the associated EM(s)).

R1.2.50. The SM shall support extending NSD with the security information contained in the designed security policies to create sNSD.

R1.2.60. The sNSD shall support the security zone/placement, the connectivity and the description of the VSFs needed for controlling the traffic to VNFs.

R1.2.70. The sNSD shall be made available to the NFVO for deploying network services with security protection.

R1.2.80. If sNSD is available before a network service is deployed, the sNSD shall be used by the NFVO for initial deployment of the network service. The VSFs (e.g. the virtual firewalls included in sNSD) for protecting the network service are instantiated together with the VNFs assigned to the network service.

R1.2.90. If sNSD is not available before a network service is deployed, the SM shall be able to get the information of the deployed network service (or VNFs) from the NFVO for applying security policies to the unprotected network service.

R1.2.100. To enforce security policies on unprotected network services, the SM shall be able to trigger the instantiation of the required VSF(s) (via the VNFM) according to the designed security policies and update network topology accordingly.

R1.2.110. For updating the enforced security policies when network services are scaled-in/scaled-out, the SM shall be informed (by the NFVO) of the result of the scaled network services.

R1.2.120. The SM shall be able to trigger the instantiation of new VSF(s) required for protecting the instantiated VNF(s) for scaled network service or termination of affected VSF(s) via the VNFM, based on the designed security policies.

R1.2.130. The SM shall have the capability to configure security rules on VSFs/PSFs (via the associated EMs) and ISFs (via ISM) following the designed security policies.

R1.2.140. Network Security Management shall provide an interface from the SM to the VSFs/PSFs (via the associated EMs) and ISFs (via ISM) to allow configuration of the instantiated VSFs (e.g. initial credentials, etc.).

R1.2.150. The SM shall have the capability to configure security policy validation for the deployed/scaled network services.

R1.2.160. Network Security Management shall provide an interface from the SM for security policy validation for the deployed/scaled network services.

R1.2.170. The SM shall have the capability to clean-up of enforced security policies related resources for the terminated network services.

In ETSI GS NFV-SEC 013 [1], clause 7.5 "NFV Security Monitoring & Management Requirements":

R1.3.10. Network monitoring solution shall not render vulnerable the security of the network or the user data any more than it is without the network monitoring solution in place.

R1.3.20. The monitoring solution in NFV shall provide an equivalent or higher level of security than the monitoring solutions in existing non-virtualised networks.

R1.3.30. Active Monitoring failures should be fail safe. Passive monitoring failures should be silent from user perspective.

R1.3.40. The Security Monitoring components should be protected from other NFV system components, and should execute in Hardware Mediated Execution Enclave (HMEE) within appropriate trust domains.

R1.3.50. Security Monitoring should not impact IaaS, PaaS, and SaaS SLAs, except as otherwise defined in the present document.

R1.3.60. Security Monitoring depends upon security requirements established by the ETSI GS NFV-SEC 001 [4], including Secure and Measured boot and establishing secure channels based on mutual authentication.

R1.3.70. A comprehensive deployment of Security Monitoring solution will monitor both virtualised and non-virtualised network functions.

R1.3.80. NFVI resource allocation and platform quality of service technologies should be put in place to ensure that the Security Monitoring functions are not starved of NFVI resources causing unexpected security consequences. Such mechanisms should reliably ensure that starvation and DoS attacks against Security Monitoring functions are minimized or eliminated.

R1.3.90. Security Monitoring components shall be securely provisioned within the system, which means that these systems will be provisioned for deployments in a trusted environment. This includes root key provisioning, setting up HMEE, certificate provisioning, etc.

R1.3.100. Security Monitoring components shall be booted using secured and measured boot technologies.

R1.3.110. Once Security Monitoring and Management systems are in place, these shall detect authorized and unauthorized on-boarding, deployments, activation, and run time integrity checking of VNFs.

R1.3.120. Once VNFs are deployed, Security Monitoring and Management System shall ensure that the security policies of the deployed VNFs are enforced.

R1.3.130. Security Monitoring systems shall protect Telemetry data-at-rest, both at local or remote secure storage.

R1.3.140. Security Monitoring telemetry may be compressed prior to storage and/or during transit.

R1.3.150. A Security Monitoring and Management system will ensure that the VNFs and SFCs have been securely configured, meaning that start-up and security enforcement policies (e.g. VNFDs, Configuration) were delivered to the VNFs in a protected manner. It is assumed that the configuration data itself is vetted and accurate, per the security policy.

R1.3.160. Once provisioned, Security Monitoring and Management system will ensure that the VNFs are not activated unless their security policy is addressed. For example, all VNFs in a SFC should be deployed prior to activation of a specific VNF.

R1.3.170. The Security Monitoring and Management system will help monitor VNF topology changes, including migration, scale-in, and scale-out of VNFs.

R1.3.180. Security Monitoring and Management will observe the VNFs instantiation and termination process and it should be able to detect and remediate improperly authorized actions.

R1.3.190. The Security Monitoring and Management system will help detect and remediate VNF exploits during the normal course of VNF's operational life-cycle. For instance, attacker could attempt to exploit a known vulnerability in a VNF, which can be detected and blocked by the security monitoring system.

R1.3.200. NFV Security Monitoring components should run in a HMEE.

R1.3.210. The NFV Security Monitoring and Management system shall ensure that all Security Monitoring services and policies are securely provisioned and activated prior to NFV system bring-up.

R1.3.220. NFV Security Monitoring and Management system shall interface with the NFV system life-cycle, including hardware, firmware, and software updates, to ensure that these are authorized and occur per security policy.

R1.3.230. Security Monitoring may perform Active and Passive Security Monitoring of the Control, Management, and Data planes in a VNF.

R1.3.240. Security Monitoring can be continuous, manual, or triggered by a specific set of events, as in automated anomaly detection. Monitoring can also be triggered by an administrator based on their specific criteria.

R1.3.250. NFV Security Monitoring system may securely distribute telemetry to multiple Security Monitoring Collection and Analytics Systems, based on the security policies for minimizing latencies associated with detection remediation of threats.

R1.3.260. Security Monitoring components should follow security best practices for auditing, including secure logging and tracing.

R1.3.270. Audit logs contain sensitive information, and based on security policy, Audit Log data-at-rest should be confidentiality and/or integrity protected with a securely provisioned key.

R1.3.280. The Audit Logs, in transit, should be integrity and confidentiality protected using pairwise unique keys.

R1.3.290. Network Monitoring should not lower the reliability of the system from its state prior to enabling Security Monitoring.

A.2 Additional Requirements

The following requirements are in addition to those derived from ETSI GS NFV-SEC 013 [1] in clause A.1 of the present document:

R2.1.10. NFV-MANO shall support SMs that are Passive, or Semi-Active or Fully Active as defined in clause 5.1.2.

R2.1.20. For SMs in Passive mode, NFV-MANO shall send applicable lifecycle management events to the SM but NFV-MANO shall not wait for the SM to provide any response to NFV-MANO, nor shall NFV-MANO accept requests to modify the VNF lifecycle.

R2.1.30. For SMs in Semi-Active mode, NFV-MANO shall send applicable lifecycle management events to the SM. For VNFs which require security policy management, the SM shall provide NFV-MANO with the necessary info and NFV-MANO shall act on it accordingly. However, in general NFV-MANO shall carry on with lifecycle management without SM intervention unless the SM responds negatively. SMs may request NFV-MANO to take lifecycle management action at any time.

R2.1.40. For SMs in Full-Active mode, NFV-MANO shall send applicable lifecycle management events to the SM. NFV-MANO shall not proceed with lifecycle management until the SM positively confirms permission and provides any security policy instructions. NFV-MANO shall immediately action instructions from an Active SM regardless of the impact on the network application layer services (e.g. immediately kill one or more VNFs).

NOTE 1: An SM fully implementing the requirements of ETSI GS NFV-SEC 013 [1], is a Fully-Active SM.

R2.1.50. NFV-MANO shall support hierarchical relationships for networks with multiple SMs or trust domains.

R2.1.60. NFV-MANO shall support a dedicated logical set of interfaces (as defined in clause 5.1.1) for each SM.

R2.1.70. NFV-MANO shall support separate independent security associations and keys for each SM on each logical interface.

R2.1.80. NFV-MANO shall ensure that only lifecycle management events applicable to a specific SM(s) are sent to that SM(s).

R2.1.90. NFV-MANO shall not accept instructions from an SM in one trust domain for VNFs managed by another SM in another trust domain.

R2.1.100. SM to NFV-MANO trust domain separation shall include support for management of sensitive components as defined in ETSI GS NFV-SEC 012 [3].

R2.1.110. NFV-MANO shall support an authorization framework where each SM is authorized in Passive or Semi-Active or Fully-Active mode to undertake interactions with NFV-MANO.

R2.1.120. Each SM to NFV-MANO authorization shall be independent of any other SM binding and NFV-MANO shall ensure that each SM is invisible (if required) to any other SM.

R2.1.130. Where one SM spans multiple trust domains, it shall be possible for the SM to have different modes (Passive, Semi-Active, Fully-Active) for each trust domain.

R2.1.140. Where one SM has multiple modes for different trust domains, NFV-MANO shall be able to manage and authorize these rolls independently.

R2.1.150. NFV-MANO shall provide VNF lifecycle management event information to the SM(s) when a VNF instance is created.

R2.1.160. NFV-MANO shall provide VNF lifecycle management event information to the SM(s) when a VNF instance is modified. Modification is any change to a VNF but not limited to:

- configuration;
- run-time images or code version;
- location (physical or logical);
- host resources;
- NFV layer communications peering relationships (including PNFs where visible to NFV-MANO);

- identification;
- changes to one or more VNFCI with a VNF;
- load balancing;
- any other change which could have an impact on security policy or management.

R2.1.170. NFV-MANO shall provide VNF lifecycle management event information to the SM(s) when a VNF instance is terminated, crashes or ceases to exist for any reason.

R2.1.180. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide information on the source of the VNF lifecycle management event (e.g. application layer OSS/BSS, VNF, EMs, auto healing function, etc.).

R2.1.190. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide information on the reason for the VNF lifecycle management event (e.g. new VNF instance requested).

R2.1.200. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide the ability to hide specific lifecycle events for sensitive functions as specified in ETSI GS NFV-SEC 012 [3] from one or more SMs.

R2.1.210. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide as a minimum the following information in a VNF instantiation event:

- Source of request (e.g. OSS/BSS or NFV-MANO automated process).
- VNF Package Identifier.
- VNFD Identifier.
- VNFD (if required by SM).
- Integrity checksum of VNF package (including indication of pass or fail from NFV-MANO perspective).
- MANO Reference Identifier for VNF instance being created.
- Requestor Reference Identifier used for VNF instance being created (e.g. OSS/BSS application layer VNF ID).
- SDN Connectivity information (including PNFs) as known by NFV-MANO.
- Group reference (e.g. NS ID) for VNFs being created as part of a VNFD or Orchestration request.
- Intended host(s) and physical location(s) of VNF.

R2.1.220. As part of the VNF lifecycle management event information to the SM(s), NFV-MANO shall provide as a minimum the following information in a VNF modification event:

- Source of request.
- Reason for modification.
- Reference identifier for VNF Instance being modified.
- Details of the change.

R2.1.230. NFV-MANO shall provide as a minimum the following information in a VNF termination event:

- Source of request.
- Reference identifier for VNF Instance being terminated.
- Reason for termination.

R2.1.240. NFV-MANO shall be able to provide SM(s) with information to understand the context of lifecycle events.

R2.1.250. Where a VNF package has been signed, NFV-MANO shall provide the package integrity information for the VNF being created. For Semi-Active and Fully-Active SMs, the SM shall verify the package integrity and provide a confirmation to NFV-MANO. The start-up integrity check for sensitive components described in ETSI GR NFV-SEC 011 [i.8] shall be supported.

R2.1.260. If NFV-MANO receives a VNF termination request from a semi-active SM, NFV-MANO shall initiate automated termination of the VNF and associated service chain. NFV-MANO shall inform the OSS/BSS before terminating the VNF but shall not seek permission to terminate:

- The SM shall be able to specify to NFV-MANO whether another VNF instance may be created to replace the VNF being terminated.
- The SM shall be able to specify to NFV-MANO whether it wants a copy of the VNF to be quarantined for later analysis.
- The SM shall be able to specify to NFV-MANO whether other recovery action may be performed in relation to the terminated VNF instance.

R2.1.270. If NFV-MANO receives a VNF termination instruction from a fully-active SM, NFV-MANO shall immediately terminate the VNF instance. NFV-MANO shall not inform the OSS/BSS before terminating the VNF instance:

- The SM shall be able to specify to NFV-MANO whether another VNF instance may be created to replace the VNF instance being terminated.
- The SM shall be able to specify to NFV-MANO whether it wants a copy of the VNF instance to be quarantined for later analysis.
- The SM shall be able to specify whether the VNF image and VNFD can be reused for new VNF instances or should also be quarantined.
- The SM shall be able to specify whether the host should be made available for use by other VNF instances or should also be quarantined.
- The SM shall be able to specify to NFV-MANO whether other recovery action may be performed in relation to the terminated VNF instance.
- The SM shall be able to specify whether all other VNF instances running on the same host should be terminated.
- The SM shall be able to specify whether NFV-MANO shall actively erase all HMEEs, HSMs or other storage used by the terminated VNF instance, in addition to normal NFV-MANO routine resource re-use procedures.

R2.1.280. When a fully-active SM or semi-active SM instructs/requests termination of one or more VNF instances, the SM shall provide NFV-MANO with a list of VNF instances to be terminated.

R2.1.290. MANO shall support VNF termination requests/instructions using lists of VNF instance identifiers based on NFV-MANO managed IDs.

R2.1.300. MANO shall provide sufficient OSS/BSS application ID information to the SM so that SM is able to understand the mapping between VNF lifecycle events and the equivalent OSS/BSS application IDs.

R2.1.310. An SM shall be able to provide NFV-MANO with security policy management instructions during a VNF lifecycle event or at any other time required by the SM.

NOTE 2: Content or format of the security policy information is outside the scope of the present document.

R2.1.320. A Semi-Active SM shall be able to request NFV-MANO to terminate the use of a specific host:

- The SM shall be able to specify to NFV-MANO whether VNF instances running on the host can be migrated or shall be terminated.

- The SM shall be able to specify to NFV-MANO whether to quarantine the host along with the hosted VNF instances.

R2.1.330. A Fully-Active SM shall be able to instruct NFV-MANO to immediately terminate the use of a specific host:

- The SM shall be able to specify to NFV-MANO whether VNFs running on the host can be migrated or shall be terminated.
- The SM shall be able to specify to NFV-MANO whether to quarantine the host along with the hosted VNFs.

R2.1.340. Semi-Active and Fully-Active SM shall be able to request instantiation, modification or termination of security functions to be inserted into or removed from the network service (e.g. between any two VNF instances or between sub-components within a single VNF instance) either as part of the NFV-MANO lifecycle management events notified by NFV-MANO to the SM(s) or at any other time required by the SM.

R2.1.350. An SM shall be able to request a network status list for all active VNF instances under control of NFV-MANO for that trust domain.

R2.1.360. An SM shall be able to request from NFV-MANO a list of VNF instances and their lifecycle history which previously existed in the network over a requested time period.

NOTE 3: The level of information required and period for which data should be held is outside the scope of the present document. However, the information retained needs to be sufficient to allow after the event network forensics over a reasonable timescale to be performed where a persistence attack has penetrated the network but the VNF instance or host which was compromised is no longer active.

Annex B (normative): Certificate Management functional requirements

B.1 Requirements on Certificate Management for certificate management function

B.1.1 Functional requirements for certificate management function

B.1.1.1 General considerations

The management of certificates in the NFV Architectural Framework requires the services of one or several Certificate Management Function(s) (CMF).

The following statement on the scope of CMF applies to all CMF related requirements:

- The CMF provides the following services for the automated certificate management for the NFV Architectural Framework and interacts with the various CAs and their functions: certificate registration, certificate enrolment, certificate renewal, certificate removal, certificate revocation, certificate monitoring.

- The CMF has the capability to manage all types of certificates, i.e. VNF Package certificate, VNFCI certificate, VNF OAM certificate, NFV-MANO certificate, and virtualised computation environment control plane certificate, as defined in clause 5.2.1.

For certificates used by a single VNF instance or for local management of OS containers, sub-certificates may be managed locally as a sub-CA domain of the CMF. However, lack of support of partial chain verification can imply the need to use isolated PKIs if isolation of domains is needed (for more information refer to clause 10.5 of ETSI GR NFV-SEC 005 [i.3]).

More detailed information about the certificates management functions such as enrolment is provided in ETSI GR NFV-SEC 005 [i.3].

NOTE: In the present document, the CMF certificate enrolment service is equivalent to the service provided by the "Operator Certificate Enrolment Server" used in the referred ETSI GR NFV-SEC 005 [i.3].

The CMF is an operator sensitive critical security function; therefore, the CMF is expected to be protected accordingly. The certificate enrolment from the CAs is to be protected through the protocol specific mechanisms, e.g. those provided in IETF RFC 7030 [13] regarding EST and IETF RFC 4210 [14] regarding CMPv2.

B.1.1.2 Functional requirements for certificate lifecycle management

Table B.1.1.2-1: Functional requirements for certificate lifecycle management

Numbering	Functional requirements description
Cmf.CertLcm.001	The CMF shall support the capability of certificate lifecycle management, i.e. registration, enrolment, renewal, removal, revocation, monitoring of certificate.
Cmf.CertLcm.002	The CMF shall support the capability to manage registration of NFV-MANO entities.
Cmf.CertLcm.003	If delegation mode is selected, the CMF shall support the capability to manage registration of VNFM for delegation mode.
Cmf.CertLcm.004	The CMF shall support the capability to select the CAs for the registered entities which are responsible to create and sign the certificates to enrol.
Cmf.CertLcm.005	The CMF shall support creation and signing of certificates by forwarding the CSR toward CA upon received CSR from NFV-MANO entities.
Cmf.CertLcm.006	If delegation mode is selected, the CMF shall support creation and signing of certificates by forwarding the CSR toward CA upon received CSR from the VNFM for delegation mode.
Cmf.CertLcm.007	The CMF shall support the capability to distribute all types of certificates and certificate chains (all intermediate and root CA certificates) to NFV-MANO functional entities.
Cmf.CertLcm.008	The CMF shall support the capability to provide FQDN and authorization to enable certificate management.
Cmf.CertLcm.009	If the CMF is the certificate signing entity then key attestation statement for NFVO key pair shall, depending on the CMF certificate policy, be validated by the CMF before the CSR for NFVO's NFV-MANO certificate is accepted and the certificate generated.
Cmf.CertLcm.010	If the CMF is the certificate signing entity then key attestation statement for VNFM key pair shall, depending on the CMF certificate policy, be validated by the CMF before the CSR for VNFM's NFV-MANO certificate is accepted and the certificate generated.
Cmf.CertLcm.011	If delegation mode is selected and if the CMF is the certificate signing entity then key attestation statement for VNF OAM and VNFCI key pairs shall, depending on the CMF certificate policy, be validated before the CSRs for VNF OAM and VNFCI certificates are accepted and the certificates generated.
Cmf.CertLcm.012	If the CMF is the certificate signing entity then key attestation statement for VIM key pair shall, depending on the CMF certificate policy, be validated by the CMF before the CSR for VIM's NFV-MANO certificate is accepted and the certificate generated.
Cmf.CertLcm.013	If the CMF is the certificate signing entity then key attestation statement for WIM key pair shall, depending on the CMF certificate policy, be validated by the CMF before the CSR for WIM's NFV-MANO certificate is accepted and the certificate generated.
Cmf.CertLcm.014	If the CMF is the certificate signing entity then key attestation statement for CISM key pair shall, depending on the CMF certificate policy, be validated by the CMF before the CSR for CISM's NFV-MANO certificate is accepted and the certificate generated.
Cmf.CertLcm.015	If the CMF is the certificate signing entity then key attestation statement for CIR key pair shall, depending on the CMF certificate policy, be validated by the CMF before the CSR for CIR's NFV-MANO certificate is accepted and the certificate generated.

B.2 Functional requirements on Certificate Management for NFVO

Table B.2-1: Functional requirements for security consideration

Numbering	Functional requirements description
Nfvo.Sc.001	The NFVO shall support the capability to establish secure connections between the NFVO and its peer entities using the NFVO's NFV-MANO certificate provided by the CMF, the certificate(s) issued to the peer entity and the peer certificate chain.
Nfvo.Sc.002	The NFVO shall support the capability to generate key pairs of public key and private key for NFVO's NFV-MANO certificate with a random number generation following industry standards for example NIST SP800-90A/B and C [15], [16], and [17].
Nfvo.Sc.003	The NFVO shall support the capability to protect the key pairs at rest and when used within a tamper resistant storage, for example FIPS 140-3 [19] L3 or FIPS 140-2 [18] or CC EAL4+ [20], [21], [22] and [23] certified device, for the NFVO's NFV-MANO certificate.
Nfvo.Sc.004	The NFVO shall support the capability of certificate lifecycle management (including management of key pairs of public key and private key), i.e. CSR generation, enrolment, renewal, removal, revocation, monitoring of certificate for NFVO's NFV-MANO certificate.
Nfvo.Sc.005	The NFVO shall support the capability of configuring the information required to construct CSR for NFVO's NFV-MANO certificate from OSS.
Nfvo.Sc.006	If indicated by OSS via NS lifecycle procedures, the NFVO shall support delegation mode for the VNF OAM certificate/VNFCI certificate management.
Nfvo.Sc.007	If delegation mode is selected, the NFVO shall support the capability of configuring the information required to construct CSR for VNF OAM certificate/VNFCI certificate from OSS via NS lifecycle management procedures and conveying such information to VNFM via VNF lifecycle management procedures.
Nfvo.Sc.008	There shall be a key attestation mechanism (see note) in the NFVO that can attest the key pair for the NFVO's NFV-MANO certificate has been generated and protected in accordance with Nfvo.Sc.002 and Nfvo.Sc.003.
Nfvo.Sc.009	The NFVO should provide attestation of key generation and storage before the CSR of the NFVO's NFV-MANO certificate is processed.
NOTE: Key attestation refers to the originator of a cryptographic key pair providing information (Key Attestation Statement) about the provenance of that key pair, in a manner that can be cryptographically verified.	

B.3 Functional requirements on Certificate Management for VNFM

Table B.3-1: Functional requirements for security consideration

Numbering	Functional requirements description
Vnfm.Sc.001	The VNFM shall support the capability to establish secure connections between the VNFM and its peer entities using the VNFM's NFV-MANO certificate provided by the CMF, the certificate(s) issued to the peer entity and the peer certificate chain.
Vnfm.Sc.002	The VNFM shall support the capability to generate key pairs of public key and private key for VNFM's NFV-MANO certificate with a random number generation following industry standards for example NIST SP800-90A/B and C.
Vnfm.Sc.003	If delegation mode is selected, the VNFM shall support the capability to generate key pairs of public key and private key for VNF OAM certificate and VNFCI certificate with a random number generation following industry standards, for example NIST SP800-90A/B and C [15], [16] and [17].
Vnfm.Sc.004	The VNFM shall support the capability to protect the key pairs at rest and when used within a tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ [20], [21], [22] and [23] certified device, for the VNFM's NFV-MANO certificate.
Vnfm.Sc.005	If delegation mode is selected, the VNFM shall securely delete the private keys used for the VNF OAM certificate and VNFCI certificate, once a certain number of attempts to install the certificates into the VNFCI have been made, or the key retention period is expired, whichever comes first. The number of attempts and the retention time period are configurable. See note 1.
Vnfm.Sc.006	If delegation mode is selected, the VNFM shall support the capability to protect the key pairs at rest and when used within tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ [20], [21], [22] and [23] certified device, for the VNF OAM certificate and VNFCI certificate.

Numbering	Functional requirements description
Vnfm.Sc.007	The VNFM shall support the capability to support the delegation mode for VNF OAM certificate and VNFCI certificate, if required.
Vnfm.Sc.008	The VNFM shall support the capability of certificate lifecycle management (including management of key pairs of public and private key), i.e. CSR generation, enrolment, renewal, removal, revocation, monitoring of certificate for VNFM's NFV-MANO certificate.
Vnfm.Sc.009	The VNFM shall support the capability of configuring the information required to construct CSR for VNFM's NFV-MANO certificate
Vnfm.Sc.010	If delegation mode is selected, the VNFM shall support the capability of certificate lifecycle management (including management of key pairs of public and private keys), i.e. registration, CSR generation, enrolment, renewal, removal, revocation, monitoring of certificate for VNF OAM certificate and VNFCI certificate in delegation mode.
Vnfm.Sc.011	If delegation mode is selected, the VNFM shall support the capability of configuring the information required to construct CSR for VNF OAM certificate/VNFCI certificate from NFVO via VNF lifecycle management procedures.
Vnfm.Sc.012	If delegation mode is selected, the VNFM shall support the capability to install VNF OAM certificate and VNFCI certificate into VNFCI, during VNF instantiation and after VNF instantiation.
Vnfm.Sc.013	If delegation mode is selected, the VNFM shall support the capability to uniquely identify the VNFCs to be instantiated within the scope of the VNFM.
Vnfm.Sc.014	If delegation mode is selected, the VNFM shall support the capability to make available unique identifiers of the VNFCs, for the purpose of Registration/CSR generation process of certificate for VNF OAM certificate and VNFCI certificate.
Vnfm.Sc.015	There shall be a key attestation mechanism (see note) in the VNFM that can attest the key pair for the VNFM's NFV-MANO certificate has been generated and protected in accordance with VnfmSc.002 and Vnfm.Sc.004.
Vnfm.Sc.016	The VNFM should provide attestation of key generation and storage before the CSR of the VNFM's NFV-MANO certificate is processed.
Vnfm.Sc.017	If delegation mode is selected, there shall be a key attestation mechanism in the VNFM that can attest the key pairs for VNF OAM certificate and VNFCI certificate have been generated and protected in accordance with VnfmSc.003 and Vnfm.Sc.006.
Vnfm.Sc.018	If delegation mode is selected, the VNFM should provide attestation of key generation and storage before the CSRs for VNF OAM and VNFCI certificates is processed.
Vnfm.Sc.019	If delegation mode is selected, the VNFM should validate private/public keys when VNFC installs VNF OAM certificate and VNFCI certificate. See notes 3 and 4.
NOTE 1: Cybersecurity best practices shall be followed for configuring number of attempts and retention time period. NOTE 2: Key attestation refers to the originator of a cryptographic key pair providing information (Key Attestation Statement) about the provenance of that key pair, in a manner that can be cryptographically verified. NOTE 3: Certificates ensure authenticity of the key pairs of private key and public key. NOTE 4: MAC (Message Authentication Code) of TLS ensures Integrity of the data in the communication path, e.g. Cm-Vnfm, Ve-Vnfm-vnf, Vi-Vnfm.	

B.4 Functional requirements on Certificate Management for VIM

B.4.1 Functional requirements for virtualised resource management

Table B.4.1-1: Functional requirements for virtualised resource management

Numbering	Functional requirements description
Vim.Vrm.010	The VIM shall support the capability to collect, initiate creation of initial credential or signed certificates from certain virtualised resource and transfer them to VNFM and/or NFVO.

B.4.2 Functional requirements for security consideration

Table B.4.2-1: Functional requirements for security consideration

Numbering	Functional requirements description
Vim.Sc.001	The VIM shall support the capability to establish secure connections between the VIM and its peer entities using the VIM's NFV-MANO certificate provided by the CMF, the certificate(s) issued to the peer entity and the peer certificate chain.
Vim.Sc.002	The VIM shall support the capability to generate key pairs of public key and private key for VIM's NFV-MANO certificate with a random number generation following industry standards for example NIST SP800-90A/B and C [15], [16] and [17].
Vim.Sc.003	The VIM shall support the capability to protect the key pairs at rest and when used within a tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ [20], [21], [22] and [23] certified device for the VIM's NFV-MANO certificate.
Vim.Sc.004	The VIM shall support the capability of certificate lifecycle management (including management of key pairs of public and private key), i.e. CSR generation, enrolment, renewal, removal, revocation, monitoring of certificate for VIM's NFV-MANO certificate.
Vim.Sc.005	The VIM shall support the capability of configuring the information required to construct CSR for VIM's NFV-MANO certificate from OSS.
Vim.Sc.006	If delegation mode is selected, the VIM shall support the capability to install VNF OAM certificate and VNFCI certificate into VNFCI for delegation mode, during VNF/VNFC instantiation.
Vim.Sc.007	If delegation mode is selected, the VIM shall support the capability to manage the key pairs of public and private key for VNF OAM/VNFCI certificate.
Vim.Sc.008	If delegation mode is selected, the VIM shall securely delete the private key used for the VNF OAM certificate and VNFCI certificate, once the installation attempt of certificate into the VNFCI has been made.
Vim.Sc.009	There shall be a key attestation mechanism (see note) in the VIM that can attest the key pair for VIM's NFV-MANO certificate has been generated and protected in accordance with Vim.Sc.002 and Vim.Sc.003.
Vim.Sc.010	The VIM should provide attestation of key generation and storage before the CSR of the VIM's NFV-MANO certificate is processed.
NOTE: Key attestation refers to the originator of a cryptographic key pair providing information (Key Attestation Statement) about the provenance of that key pair, in a manner that can be cryptographically verified.	

B.5 Functional requirements on Certificate Management for WIM

Table B.5-1: Functional requirements for security consideration

Numbering	Functional requirements description
Wim.Sc.001	The WIM shall support the capability to validate that the received message is from an authenticated and authorized consumer.
Wim.Sc.002	The WIM shall support the capability to verify the integrity of the received message.
Wim.Sc.003	The WIM shall support the capability to encrypt the sent message or decrypt the received message using negotiated key and algorithm to or from an authenticated and authorised consumer or producer.
Wim.Sc.004	The WIM shall support the capability to establish secure connections between the WIM and its peer entities using the WIM's NFV-MANO certificate provided by the CMF, the certificate(s) issued to the peer entity and the peer certificate chain.
Wim.Sc.005	The WIM shall support the capability to generate key pairs of public key and private key for WIM NFV-MANO certificate with a random number generation following industry standards for example NIST SP800-90A/B and C [15], [16] and [17].
Wim.Sc.006	The WIM shall support the capability to protect the key pairs at rest and when used within a tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ [20], [21], [22] and [23] certified device for the WIM's NFV-MANO certificate.
Wim.Sc.007	The WIM shall support the capability of certificate lifecycle management (including management of key pairs of public key and private key), i.e. CSR generation, enrolment, renewal, removal, revocation, monitoring of certificate for WIM's NFV-MANO certificate.
Wim.Sc.008	The WIM shall support the capability of configuring the information required to construct CSR for WIM's NFV-MANO certificate from OSS/NFVO.
Wim.Sc.009	There shall be a key attestation mechanism (see note) in the WIM that can attest the key pair for WIM's NFV-MANO certificate has been generated and protected in accordance with Wim.Sc.005 and Wim.Sc.006.
Wim.Sc.010	The WIM should provide attestation of key generation and storage before the CSR of the WIM's NFV-MANO certificate is processed.
NOTE: Key attestation refers to the originator of a cryptographic key pair providing information (Key Attestation Statement) about the provenance of that key pair, in a manner that can be cryptographically verified.	

B.6 Functional requirements on Certificate Management for CISM

Table B.6-1: Functional requirements for security consideration

Numbering	Functional requirements description
Cism.Sc.001	The CISM shall support the capability to validate that the received message is from an authenticated and authorized consumer.
Cism.Sc.002	The CISM shall support the capability to verify the integrity of the received message.
Cism.Sc.003	The CISM shall support the capability to encrypt the sent message or decrypt the received message using negotiated key and algorithm to or from an authenticated and authorised consumer or producer.
Cism.Sc.004	The CISM shall support the capability to establish secure connections between the CISM and its peer entities using the CISM's NFV-MANO certificate provided by the CMF, the certificate(s) issued to the peer entity and the peer certificate chain.
Cism.Sc.005	The CISM shall support the capability to generate key pairs of public key and private key for CISM's NFV-MANO certificate with a random number generation following industry standards for example NIST SP800-90A/B and C [15], [16] and [17].
Cism.Sc.006	The CISM shall support the capability to protect the key pairs at rest and when used within a tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ [20], [21], [22] and [23] certified device for the CISM's NFV-MANO certificate.
Cism.Sc.007	The CISM shall support the capability of certificate lifecycle management (including management of key pairs of public key and private key), i.e. CSR generation, enrolment, renewal, removal, revocation, monitoring of certificate for CISM's NFV-MANO certificate.
Cism.Sc.008	The CISM shall support the capability of configuring the information required to construct CSR for CISM's NFV-MANO certificate.

Numbering	Functional requirements description
Cism.Sc.009	There shall be a key attestation mechanism (see note) in the CISM that can attest the key pair for CISM's NFV-MANO certificate has been generated and protected in accordance with Cism.Sc.005 and Cism.Sc.006.
Cism.Sc.010	The CISM should provide attestation of key generation and storage before the CSR of the CISM's NFV-MANO certificate is processed.
NOTE: Key attestation refers to the originator of a cryptographic key pair providing information (Key Attestation Statement) about the provenance of that key pair, in a manner that can be cryptographically verified.	

B.7 Functional requirements on Certificate Management for CIR

Table B.7-1: Functional requirements for security consideration

Numbering	Functional requirements description
Cir.Sc.001	The CIR shall support the capability to validate that the received message is from an authenticated and authorized consumer.
Cir.Sc.002	The CIR shall support the capability to verify the integrity of the received message.
Cir.Sc.003	The CIR shall support the capability to encrypt the sent message or decrypt the received message using negotiated key and algorithm to or from an authenticated and authorised consumer or producer.
Cir.Sc.004	The CIR shall support the capability to establish secure connections between the CIR and its peer entities using the CIR's NFV-MANO certificate provided by the CMF, the certificate(s) issued to the peer entity and the peer certificate chain.
Cir.Sc.005	The CIR shall support the capability to generate key pairs of public key and private key for CIR's NFV-MANO certificate with a random number generation following industry standards for example NIST SP800-90A/B and C [15], [16] and [17].
Cir.Sc.006	The CIR shall support the capability to protect the key pairs at rest and when used within a tamper resistant storage, for example FIPS 140-3 L3 or FIPS 140-2 or CC EAL4+ [20], [21], [22] and [23] certified device, for the CIR's NFV-MANO certificate.
Cir.Sc.007	The CIR shall support the capability of certificate lifecycle management (including management of key pairs of public key and private key), i.e. CSR generation, enrolment, renewal, removal, revocation, monitoring of certificate for CIR's NFV-MANO certificate.
Cir.Sc.008	The CIR shall support the capability of configuring the information required to construct CSR for CIR's NFV-MANO certificate.
Cir.Sc.009	There shall be a key attestation mechanism (see note) in the CIR that can attest the key pair for CIR's NFV-MANO certificate has been generated and protected in accordance with Cir.Sc.005 and Cir.Sc.006
Cir.Sc.010	The CIR should provide attestation of key generation and storage before the CSR of the CIR's NFV-MANO certificate is processed.
NOTE: Key attestation refers to the originator of a cryptographic key pair providing information (Key Attestation Statement) about the provenance of that key pair, in a manner that can be cryptographically verified.	

B.8 Functional requirements on Certificate Management for CA

No functional requirements on Certificate Management for CA are specified in this edition of the present document.

B.9 General requirements to NFV management and orchestration interface design

This clause defines general interface requirements applicable to all NFV-MANO interfaces.

NOTE: The requirements for individual interfaces will not be covered in this clause.

These requirements are applicable for interface specifications.

Annex C (informative):
Use Cases for Certificate Management

C.1 Use cases for VNF Package certificate management

Management of VNF Package certificates is not considered in the current version of the present document.

C.2 Use cases for VNFCI certificate management

C.2.1 Direct mode

C.2.1.1 VNFCI certificate enrollment in direct-mode

C.2.1.1.1 Introduction

The goal of the use case is to demonstrate the operation of VNFCI certificate enrolment for Option1 ("direct-mode").

Depending on its design, a VNFI/VNFCI can bring in one or several interfaces with the VNFCI end-point(s) acting as "client" or "server". Consequently, a given VNFCI can be associated with multiple identities (i.e. multiple certificates) to be managed by the CMF.

C.2.1.1.2 Trigger

Table C.2.1.1.2-1: Trigger

Trigger	Description
CMF obtained all information related to newly instantiated VNFCI.	CMF can use existing VNF LCM interface to query and subscribe to VNFI/VNFCI LCM information.
NOTE 1: Based on such information the details on the VNFCI reachability (e.g. the IP address of VNFCI) are available to CMF. NOTE 2: Prior to this information, the VNFCI can be subject to remote-attestation with the outcome (e.g. successfully attested) accessible by CMF, which can interact with a remote-attestation service.	

C.2.1.1.3 Actors and roles

Table C.2.1.1.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VNFCI certificate management in direct-mode.
3	CA	Certificate Authority in charge of signing and issuing certificate for the requested VNFCI identity.
4	VNFCI	VNF Component Instance requesting a certificate for each of its identities managed by the CMF.

C.2.1.1.4 Pre-conditions

Table C.2.1.1.4-1: Pre-conditions

#	Pre-condition	Description
0	The mutually authenticated TLS connection between VNFM and CMF has been configured	
1	The initial credentials for CMF - VNFCI authentication is obtained via a trust bootstrap procedure which can be realized by day-0 configuration or by interactions of the CMF as a relying party to an attestation server that has attested the VNFCI	If protection is provided by SSH or mutually authenticated TLS, the day-0 information can be the host-key (SSH) or certificates (mutually authenticated TLS). In case of attestation, the CMF itself has already been attested prior to this enrolment procedure; these initial credentials are derived during the attestation process and the attestation binds the credentials to the verified instances (i.e. CMF and VNFCI).
2	The CMF has obtained VNFCI asset data using VNF LCM interface operations (see note)	See ETSI GS NFV-IFA 007 [10].
3	The information to form the Certificate Signing Request (CSR) for the VNFCI certificate(s) is available to CMF. This information is expected to include at least the "Subject" and "SubjectAltName" for each VNFCI identity. A reference to a possibly predefined certificate profile can also be available	The information necessary for each VNFCI identity is established by the service provider in the given CMF network domain.
NOTE: CMF and VNFM communication has taken place over a secure channel for indicating the VNFCI instantiation.		

C.2.1.1.5 Post-conditions

Table C.2.1.1.5-1: Post-conditions

#	Post-condition	Description
1	The VNFCI has received the associated VNFCI certificate for each of its identities.	

C.2.1.1.6 Operational flows

Table C.2.1.1.6-1: Operational flow

#	Flow	Description
0	CMF	CMF receives the trigger: based on the indication that a new VNFC is instantiated, the CMF can query VNFM and/or subscribe to retrieve VNF LCM occurrence events to obtain asset information.
1	CMF	The CMF creates one or several identities required for the VNFCI (see note 1).
2	CMF->CA	The CMF requests the CA to register the VNFCI end-entity for every identity created in the previous step. The CMF can include an initial credential based on which VNFCI certificate signing request is to be authenticated (see note 2).
3	CMF->VNFCI	The CMF sends a configuration to the VNFCI with details necessary to build the corresponding certificate signing request for every VNFCI identity created in step-1. The configuration typically includes the trust anchor for the VNFCI identity, details on the corresponding certificate enrolment server and CA (e.g. full path to the responder for the step-5), the initial credential to authenticate the CSR for the given identity, and a trigger for certificate enrolment for the specific identity registered in the CA (see note 4).
4	VNFCI	The VNFCI generates a key-pair and the corresponding CSR for every identity created in step-1.
5	VNFCI->CA	The VNFCI sends a certificate enrolment request to the CA along with initial credential to authenticate the VNFCI/CSR based on the configuration received from the CMF in step-3 for every CSR built in step-4.
6	CA	The CA validates the received CSR request and the initial credential and issues the VNFCI certificate for the corresponding VNFCI registered identity.
7	CA->VNFCI	The CA responds by returning the requested certificate to the VNFCI (see note 3).

NOTE 1: If the VNFCI identity creation is controlled via VNFC instantiation monitoring or via remote attestation, then the CMF can interact with the entity that performs monitoring or remote attestation to check that the VNFC instantiation is in accordance with the service provider policy.
NOTE 2: The CA is expected to acknowledge the successful VNFCI end-entity registration alongside acceptance of the communicated initial credential.
NOTE 3: Depending on the certificate management protocol options, the full chain for the VNFCI own certificate can be included in the CA certificate response in step-7.
NOTE 4: Measures to limit the usage of "initial credential" can be a counter at the CA or a lifetime indication; it is out of scope of the present document.

C.2.1.2 VNFCI certificate enrollment with remote attestation in direct-mode

C.2.1.2.1 Introduction

The goal of this use-case is to demonstrate the role of the CMF in NFV deployments involving VNF secure bootstrapping with remote attestation and HMEE. In "direct-mode", the CMF interacts with an attestation service (see note) so that the certificate initial registration at the CA of a VNFCI requiring such secure bootstrapping is conditioned by a successful remote attestation of the VNFCI. Consequently, the VNFCI certificate requests are validated as originating from attested VNFCIs.

NOTE: An example of "attestation service" is the Verification Function in clause 5.1 of ETSI GR NFV-SEC 018 [i.7].

C.2.1.2.2 Trigger

Table C.2.1.2.2-1: Trigger

Trigger	Description
CMF obtained all information related to newly instantiated VNFCI.	CMF can use existing VNF LCM interface to query and subscribe to VNFI/VNFCI LCM information. The CMF is aware that the VNFCI requires secure bootstrapping with remote attestation and HMEE.
NOTE: Based on such information the details on the VNFCI reachability (e.g. the IP address of VNFCI) are available to CMF.	

C.2.1.2.3 Actors and roles

Table C.2.1.2.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VNFCI certificate management in direct-mode. The CMF acts as a Relying Party for the VNF remote attestation procedure.
2	CA	Certificate Authority in charge of signing and issuing certificate for the requested VNFCI identity.
3	VNFCI	VNF Component Instance requesting a certificate for each of its identities managed by the CMF. The VNFCI is subject to secure bootstrapping with remote attestation and HMEE.
4	Attestation Service	The attestation service deployed in the domain where the VNF is instantiated.

C.2.1.2.4 Pre-conditions

Table C.2.1.2.4-1: Pre-conditions

#	Pre-condition	Description
0	The mutually authenticated TLS connection between VNFM and CMF has been configured.	
1	The CMF is trusted as the Relying Party.	
2	The CMF - Attestation service secure connection has been established.	
3	The VNFCI has executed the remote attestation procedure with the Attestation Service (see note 2).	VNFCI initial credential(s) useful to establish secure communications with other parties attested in the same domain, e.g. CMF, can be derived during the attestation process and proved to be bound to the verified and attested VNFCI instance (see note 3).
4	The CMF has obtained VNFCI asset data using VNF LCM interface operations (see note 1).	See ETSI GS NFV-IFA 007 [10].
5	The information to form the Certificate Signing Request (CSR) for the VNFCI certificate(s) is available to CMF. This information is expected to include at least the "Subject" and "SubjectAltName" for each VNFCI identity. A reference to a possibly predefined certificate profile can also be available.	The information necessary for each VNFCI identity is established by the service provider in the given CMF network domain.
NOTE 1: CMF and VNFM communication has taken place over a secure channel for indicating the VNFCI instantiation. NOTE 2: The status of the newly instantiated VNFCI subject to remote attestation (e.g. successfully attested) is available to the Attestation service. NOTE 3: An example of such initial credential establishment is presented in clause 8.1 of ETSI GR NFV-SEC 005 [i.3].		

C.2.1.2.5 Post-conditions

Table C.2.1.2.5-1: Post-conditions

#	Post-condition	Description
1	The VNFCI has received the associated VNFCI certificate for each of its identities.	

C.2.1.2.6 Operational flows

Table C.2.1.2.6-1: Operational flow

#	Flow	Description
1	CMF	CMF receives the trigger: based on the indication that a new VNFC is instantiated, the CMF can query VNFM and/or subscribe to retrieve VNF LCM occurrence events to obtain asset information.
2	CMF->Attestation Service	Acting as Relying Party, the CMF verifies the VNFCI remote attestation status by interacting with the Attestation service. The next step follows only if the Attestation service signals that the VNFCI is successfully attested (see note 4).
3	CMF	The CMF creates one or several identities required for the attested VNFCI, which has been verified in the previous step.
4	CMF->CA	The CMF requests the CA to register the VNFCI end-entity for every identity created in the previous step. The CMF can include an initial credential based on which the VNFCI certificate signing request is to be authenticated (see note 1).

#	Flow	Description
5	CMF->VNFCI	The CMF sends a configuration to the VNFCI with details necessary to build the corresponding certificate signing request for every VNFCI identity created in step-3. The configuration typically includes the trust anchor for the VNFCI identity, details on the corresponding certificate enrolment server and CA (e.g. full path to the responder for the step-7), the initial credential to authenticate the CSR for the given identity, and a trigger for certificate enrolment for the specific identity registered in the CA (see note 3). Having been attested in the same domain, the CMF and VNFCI can establish their secure communication using the initial credentials derived during their attestation procedure.
6	VNFCI	The VNFCI generates a key-pair and the corresponding CSR for every identity created in step-3.
7	VNFCI->CA	The VNFCI sends a certificate enrolment request to the CA along with initial credential to authenticate the VNFCI/CSR based on the configuration received from the CMF in step-5 for every CSR built in step-6.
8	CA	The CA validates the received CSR request and the initial credential and issues the VNFCI certificate for the corresponding VNFCI registered identity.
9	CA->VNFCI	The CA responds by returning the requested certificate to the VNFCI (see note 2).
NOTE 1: The CA is expected to acknowledge the successful VNFCI end-entity registration alongside acceptance of the communicated initial credential. NOTE 2: Depending on the certificate management protocol options, the full chain for the VNFCI own certificate can be included in the CA certificate response in step-7. NOTE 3: Measures to limit the usage of "initial credential" can be a counter at the CA or a lifetime indication; it is out of scope of the present document. NOTE 4: Ligning with the IETF (RATS) terminology, the following mapping may be considered: CMF acts as a "Relying Party"; the Attestation Service acts as a "Verifier"; the VNFCI portion running inside the HMEE acts as an "Attester".		

C.2.1.3 VNFCI certificate enrolment using an HSM in direct-mode

C.2.1.3.1 Introduction

The goal of this use-case is to demonstrate the role of the CMF in NFV deployments involving VNF secure bootstrapping with remote attestation, HMEE and HSM.

ETSI GR NFV-SEC 005 [i.3] describes in clause 8.1.1.1.3 the key pair generation mechanism implemented by an HSM, with a random generator compliant to ETSI GS NFV-SEC 012 [3]. In this solution, the HSM is linked to the HMEE through a secure channel established after a mutual authentication process. This solution may be combined with the solution in the previous sections C.2.1.1 and C.2.1.2 for the following advantages:

- Enabling the mobility of the VNFCI.
- A control of the key pairs by the service provider, owner of the HSM, independent to the infrastructure manufacturer implementing the confidential computing technology.

NOTE: Mobility could be done with re-enrolment as an alternative.

Thus, there is an interest to use an external Hardware Security Module (HSM), controlled by the service provider to generate the keys of the VNFCI and provide identity documents to the VNFCI.

The description below includes the remote attestation as described in clause C.2.1.2, but the use of HSM could apply as well for the VNFCI certificate enrolment as described in clause C.2.1.1.

C.2.1.3.2 Trigger

Table C.2.1.3.2-1: Trigger

Trigger	Description
CMF obtained all information related to newly instantiated VNFCI.	CMF can use existing VNF LCM interface to query and subscribe to VNFI/VNFCI LCM information. The CMF is aware that the VNFCI requires secure bootstrapping with remote attestation and HMEE.
NOTE: Based on such information the details on the VNFCI reachability (e.g. the IP address of VNFCI, and associated hardware root certificate of the corresponding infrastructure) are available to CMF.	

C.2.1.3.3 Actors and roles

Table C.2.1.3.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VNFCI certificate management in direct-mode. The CMF acts as a Relying Party for the VNF remote attestation procedure.
2	HSM	NFVI includes an HSM with associated KMS system acting as a key pair generation and signing purpose for a specific trust domain.
3	CA	Certificate Authority in charge of signing and issuing certificate for the requested VNFCI identity document.
4	VNFCI	VNF Component Instance requesting a certificate for each of its identities managed by the CMF. The VNFCI is subject to secure bootstrapping with remote attestation and HMEE.
5	Attestation Service	The attestation service deployed in the domain where the VNF is instantiated.

C.2.1.3.4 Pre-conditions

Table C.2.1.3.4-1: Pre-conditions

#	Pre-condition	Description
0	The mutually authenticated TLS connection between VNFM and CMF has been configured.	
1	The CMF is trusted as the Relying Party.	
2	The CMF - Attestation service secure connection has been established.	
3	The VNFCI has executed the remote attestation procedure with the Attestation Service (see note 2)	VNFCI initial credential(s) useful to establish secure communications with other parties attested in the same domain, e.g. CMF, can be derived during the attestation process and proved to be bound to the verified and attested VNFCI instance (see note 3).
4	The CMF has obtained VNFCI asset data using VNF LCM interface operations (see note 1).	See ETSI GS NFV-IFA 007 [10].
5	The information to form the Certificate Signing Request (CSR) for the VNFCI certificate(s) is available to CMF. This information is expected to include at least the "Subject" and "SubjectAltName" for each VNFCI identity. A reference to a possibly predefined certificate profile can also be available.	The information necessary for each VNFCI identity is established by the service provider in the given CMF network domain.
6	The HSM has been configured with hardware root certificate of the corresponding infrastructure.	
NOTE 1: CMF and VNFM communication has taken place over a secure channel for indicating the VNFCI instantiation. NOTE 2: The status of the newly instantiated VNFCI subject to remote attestation (e.g. successfully attested) is available to the Attestation service. NOTE 3: An example of such initial credential establishment is presented in clause 8.1 of ETSI GR NFV-SEC 005 [i.3].		

C.2.1.3.5 Post-conditions

Table C.2.1.3.5-1: Post-conditions

#	Post-condition	Description
1	The VNFCI has received the associated VNFCI certificate and ID document for each of its identities.	

C.2.1.3.6 Operational flows

Table C.2.1.3.6-1: Operational flow

#	Flow	Description
1	CMF	CMF receives the trigger: based on the indication that a new VNFC is instantiated, the CMF can query VNFM and/or subscribe to retrieve VNF LCM occurrence events to obtain asset information.
2	CMF->Attestation Service	Acting as Relying Party, the CMF verifies the VNFCI remote attestation status by interacting with the Attestation service. The next step follows only if the Attestation service signals that the VNFCI is successfully attested (see note 7).
3	CMF	The CMF creates one or several identities required for the attested VNFCI, which has been verified in the step-2.
4	CMF->CA	The CMF requests the CA to register the VNFCI end-entity for every identity created in the previous step. The CMF can include an initial credential based on which the VNFCI certificate signing request is to be authenticated (see note 1).
5	CMF->VNFCI	The CMF sends a configuration to the VNFCI with details necessary to build the corresponding certificate signing request for every VNFCI identity created in step-3. The configuration typically includes the trust anchor for the VNFCI identity, details on the corresponding certificate enrolment server, HSM and CA (e.g. full path to the responder for the step-6 and step-13), the initial credential to authenticate the CSR for the given identity, and a trigger for certificate enrolment for the specific identity registered in the CA (see note 3). Having been attested in the same domain, the CMF and VNFCI can establish their secure communication using the initial credentials derived during their attestation procedure.
6	VNFCI(HMEE) -> HSM	Establishment of a secure TLS channel between the HSM and the VNFCI using the remote attestation credentials of HMEE and HSM certificate. (see note 6).
7	VNFCI(HMEE) -> HSM	The VNFCI request the generation of key pairs to the HSM for each identity of the VNFCI.
8	HSM -> VNFCI(HMEE)	The HSM provides the key pairs to the VNFCI through the secure channel established in step-6.
9	VNFCI	The VNFCI generates the corresponding CSR for every identity created in step-3.
10	VNFCI -> HSM	VNFCI sends the CSR payload to HSM for signing (see note 5).
11	HSM	The HSM signs the content of the CSR with the private key and sends back to the VNFCI.
12	VNFCI	The VNFCI finalizes the construction of the CSR (see note 5).
13	VNFCI -> CA	VNFCI sends the CSR to the CA along with initial credential to authenticate the VNFCI/CSR based on the configuration received from the CMF in step-5 for every CSR built in step-12.
14	CA	The CA validates the received CSR request and the initial credential and issues the VNFCI certificate for the corresponding VNFCI registered identity.
15	CA->VNFCI	The CA responds by returning the requested certificate to the VNFCI (see notes 2 and 4).

NOTE 1: The CA is expected to acknowledge the successful VNFCI end-entity registration alongside acceptance of the communicated initial credential.

NOTE 2: Depending on the certificate management protocol options, the full chain for the VNFCI own certificate can be included in the CA certificate signing response in step-15.

NOTE 3: Measures to limit the usage of "initial credential" can be a counter at the CA or a lifetime indication; it is out of scope of the present document.

NOTE 4: To enhance the security, a rotation of the key pair could be in place, repeating the steps 6 to 15 regularly.

NOTE 5: Step 10 and step-11 are optional.

NOTE 6: The protocol used between the HMEE and HSM is out of scope of the present document. A technology like Gramine could be used.

NOTE 7: Aligning with the IETF (RATS) terminology, the following mapping may be considered: CMF acts as a "Relying Party"; the Attestation Service acts as a "Verifier"; the VNFCI portion running inside the HMEE acts as an "Attester".

C.2.1.4 VNFCI certificate renewal in direct-mode

C.2.1.4.1 Introduction

The goal of the use case is to demonstrate the operation of VNFCI certificate renewal in "direct-mode".

In direct-mode, the VNFCI certificate renewal procedure reuses the automated online certificate update operation of the certificate management protocol supported by the VNFCI. All examples of IETF protocols referenced in ETSI GR NFV-SEC 005 [i.3], clause 8.1.2.0 and throughout the present document are known to support such a certificate update operation. The VNFCI uses this procedure to request an update for one of its certificates that is still valid.

C.2.1.4.2 Trigger

Table C.2.1.4.2-1: Trigger

Trigger	Description
A predefined condition to renew the VNFCI certificate.	A predefined time interval before the certificate expiry is an example of condition to trigger certificate renewal.

C.2.1.4.3 Actors and roles

Table C.2.1.4.3-1: Actors and roles

#	Actor	Description
1	CMF	The CMF configures the trigger for renewal.
2	VNFCI	VNF Component Instance requesting an update for one of its certificates.
3	CA	Certificate Authority having signed and issued the VNFCI certificate to be updated.

C.2.1.4.4 Pre-conditions

Table C.2.1.4.4-1: Pre-conditions

#	Pre-condition	Description
1	The certificate the VNFCI wishes to update is still valid.	The VNFCI certificate is not expired or revoked and has been issued by the addressed CA. A reference to a possibly predefined certificate profile can also be available.

C.2.1.4.5 Post-conditions

Table C.2.1.4.5-1: Post-conditions

#	Post-condition	Description
1	The VNFCI has received the new certificate.	

C.2.1.4.6 Operational flows

Table C.2.1.4.6-1: Operational flow

#	Flow	Description
0	CMF	CMF configures the condition to renew the certificate (see note 1).
1	VNFCI	The condition indicating that the VNFCI certificate is to be renewed is activated.
2	VNFCI	The VNFCI generates a new key-pair and the corresponding certificate update request, which is according to the supported certificate management protocol.
3	VNFCI->CA	The VNFCI sends the certificate update request to the CA. The certificate to be updated is used by the VNFCI for authenticating itself and for proving ownership of this certificate towards the CA.
4	CA	The CA validates the received certificate update request and issues the new VNFCI certificate for the corresponding VNFCI identity.
5	CA->VNFCI	The CA responds by returning the new certificate to the VNFCI (see note 2).
NOTE 1: This configuration can happen at the initial certificate enrolment or any time later. The exact mechanism for how this is performed is for future study. NOTE 2: Depending on the certificate management protocol options, the full chain for the VNFCI own certificate can be included in the CA certificate response in step-5.		

C.2.2 Delegation mode

C.2.2.1 Registration of VNFM as entity in charge of VNFCI certifate management

C.2.2.1.1 Intrduction

The goal of the use case is to demonstrate the operation of registration of VNFM as delegate for, i.e. being in charge of, the certificate management for VNFCIs of VNFI.

C.2.2.1.2 Trigger

Table C.2.2.1.2-1: Trigger

Trigger	Description
CMF receives a request to register an identifier of a VNFCI	The consumer sends a request to the CMF to register the VNFM which manages the VNFCI as a delegate for the VNFCI certificate management.

C.2.2.1.3 Actors and roles

Table C.2.2.1.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VNFCI certificate management.
2	Consumer	VNFM in charge of managing the VNFCI and which acts as a delegate for certificate management, i.e. requesting issuance/signing of certificate, delivering the certificate/certificate chain into VNFCIs.

C.2.2.1.4 Pre-conditions

Table C.2.2.1.4-1: Pre-conditions

#	Pre-condition	Description
1	Delegation mode is chosen for the VNFCI certificate management.	When using Delegation mode, "certificateDesc" shall be defined in VNFD. See note.
2	The NFV MANO certificate for the VNFM has been issued/signed and stored in the VNFM.	The use case for NFV MANO certicficate distribution to VNFM is described in clause C.4.
3	The mTLS connection between CMF and VNFM has been configured.	
4	The VNFM role and permissions have been setup.	
NOTE: "certificateDesc" is described in table 7.1.2.2-1 in ETSI GS NFV-IFA 011 [i.13].		

C.2.2.1.5 Post-conditions

Table C.2.2.1.5-1: Post-conditions

#	Post-condition	Description
1	The CMF has registered the VNFM as the entity which is in charge of the requested VNFCI certificate.	

C.2.2.1.6 Operational Flows

Table C.2.2.1.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The consumer sends a registration request to register the VNFM as the entity which is in charge of the VNFCI certificate management for the requested VNFCI. The consumer provides the identifier(s) of the target VNFCI as input parameter. The registration request is sent after the VNFM receives "InstantiateVnfRequest" on Or-Vnfm reference point as specified in clause 7.2.3 of ETSI GS NFV-IFA 007 [10].
1	CMF	The CMF validates the registration request. If valid, the CMF registers the VNFM as the entity which is in charge of the VNFCI certificate management for the requested VNFCI. The CMF selects the certificate authority for the requested certificate management. If the registration request is invalid, a rejection message is returned to the consumer.
2	CMF -> Consumer	The CMF sends the response of success or failure to the consumer.

NOTE: Set of VNFCIs for a VNF or multiple sets per NS are considered in the later version.

C.2.2.2 CSR Request for VNFCI certificate

C.2.2.2.1 Introduction

The goal of the use case is to demonstrate the operation of Certificate Signing Request for VNFCI certificates, where the request to the CMF originates from the VNFM that is in charge of the certificate management for VNFCIs of VNFI. The CMF is requested to, in cooperation with the Certificate Authority, issue and sign the VNFCI certificate and to return the VNFCI certificate and certificate chain to the VNFM.

C.2.2.2.2 Trigger

Table C.2.2.2.2-1: Trigger

Trigger	Description
CMF receives a request to issue a VNFCI certificate	The consumer sends a request to the CMF to issue and sign a certificate(s) for the VNFCI.

C.2.2.2.3 Actors and roles

Table C.2.2.2.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VNFCI certificate management.
2	Consumer	VNFM in charge of managing the VNFCI and acting as a delegate for the VNFCI certificate management, i.e. requesting issuance/signing of the VNFCI certificate, injecting the VNFCI certificate/certificate chain into the VNFCI.
3	CA	Certificate Authority in charge of issuing and signing the VNFCI certificates.

C.2.2.2.4 Pre-conditions

Table C.2.2.2.4-1: Pre-conditions

#	Pre-condition	Description
1	The CMF has registered the VNFM as entity which acts as delegate for the VNFCI certificate management	See clause C.2.2.1 Registration of VNFM as entity in charge of VNFCI certificate management.
2	The information to form the Certificate Signing Request for the requested VNFCI certificates have been known to the VNFM via Os-Ma-Nfvo (from OSS to NFVO) and Or-Vnfm (from NFVO to VNFM). The information are e.g. "Common Name", "Organization", "Country", "State", "Locality", "CertificationType" and "SubjectAltName".	See ETSI GS NFV-IFA 013 [11] and ETSI GS NFV-IFA 007 [10].

C.2.2.2.5 Post-conditions

Table C.2.2.2.5-1: Post-conditions

#	Post-condition	Description
1	The VNFM has the requested VNFCI certificate and the certificate chain for the VNFCI certificate.	

C.2.2.2.6 Operational Flows

Table C2.3.2.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer generates the key pairs of public key and private key for the VNFCI certificate. The consumer generates Certificate Signing Request with the information, which the consumer prepared via Os-Ma-Nfvo/Or-Vnfm/VNFM itself and signs with the VNFCI private key. The consumer sends a Certificate Signing Request to the CMF to obtain a VNFCI certificate.
1	CMF	The CMF verifies whether the consumer is registered as delegate for the VNFCI certificate management; i.e. the entity in charge of the requested VNFCI certificate management. If the verification fails, the CMF returns an error response to the consumer.
2	CMF	The CMF validates the information in the CSR. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue and sign the VNFCI certificate.
4	CA	The CA issues the VNFCI certificate (including VNFCI public key) and signs it with the private key of the CA and binds the certificate to the VNFCI ID.
5	CA->CMF	The CA returns the requested VNFCI certificate and certificate chain to the CMF.
6	CMF->Consumer	The CMF returns the requested VNFCI certificate and certificate chain for the VNFCI certificate to the consumer.

C.2.2.2.7 Operational Flows with the use of HSM

Table C.2.2.2.7-1 lists the additional pre-conditions applicable for the CSR request for VNFCI certificate with the use of HSM.

Table C.2.2.2.7-1: Pre-conditions

#	Pre-condition	Description
1	The VNFM integrates an HSM	The VNFM support a connection with an HSM for the key pair generation and the CSR signing for the VNFCI certificate

Table C.2.2.2.7-2: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer requests to the HSM the generation of the key pairs of public key and private key for the VNFCI certificate and the transmission of the corresponding public key. If key attestation is used, the consumer requests the key attestation statement to the HSM. The consumer generates Certificate Signing Request with the information (note), which the consumer prepared via Os-Ma-Nfvo/Or-Vnfm/VNFM itself and request the HSM to sign the CSR with the VNFCI private key. The consumer sends a Certificate Signing Request to the CMF to obtain a VNFCI certificate.
1	CMF	The CMF verifies whether the consumer is registered as delegate for the VNFCI certificate management; i.e. the entity in charge of the requested VNFCI certificate management. If the verification fails, the CMF returns an error response to the consumer
2	CMF	The CMF validates the information in the CSR. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue and sign the VNFCI certificate.
4	CA	The CA issues the VNFCI certificate (including VNFCI public key) and signs it with the private key of the CA and binds the certificate to the VNFCI ID.
5	CA->CMF	The CA returns the requested VNFCI certificate and certificate chain to the CMF
6	CMF->Consumer	The CMF returns the requested VNFCI certificate and certificate chain for the VNFCI certificate to the consumer.
NOTE: The details of the key attestation inclusion in the CSR is left for further specification.		

C.2.2.3 VNFCI certificate installation during VNF Instantiation

C.2.2.3.1 Introduction

The goal of the use case is to demonstrate the operation of VNFCI certificate installation to VNFCI during VNF instantiation. In delegation mode, the VNFM that is in charge of the certificate management for VNFCIs of VNFI, has the VNFI certificate, private key for that certificate and certificate chain, see clause C.2.2.2 CSR Request for VNFCI. The VNFM conveys such certificate, private key and certificate chain to VNFCI by VNF instantiation procedure.

C.2.2.3.2 Trigger

Table C.2.2.3.2-1: Trigger

Trigger	Description
VIM/CISM receives the request for VNF instantiation	The VIM/CISM receives the request for VNF instantiation from the VNFM.

C.2.2.3.3 Actors and roles

Table C.2.2.3.3-1: Actors and roles

#	Actor	Description
1	VNFM	VNFM in charge of managing the VNFCI and acting as a delegate for the VNFCI certificate management, i.e. requesting issuance/signing of the VNFCI certificate, installing the VNFCI certificate/certificate chain into the VNFCI.
2	VIM/CISM	VIM/CISM, which is involved in the VNF instantiation procedure, i.e. the procedures run among VNFM/VIM or VNFM/CISM.
3	VNFI	VNFI has the VNFCIs whose VNFCI certificates are managed by the delegate VNFM.

C.2.2.3.4 Pre-conditions

Table C2.3.3.4-1: Pre-conditions

#	Pre-condition	Description
1	Delegation mode is chosen for the VNFCI certificate management.	
2	The VNFM has the credentials (i.e. key pairs of public and private key) of the VNFCI, for the VNFCI certificate.	See clause C.2.2.1 Registration of VNFM as entity in charge of VNFCI certificate management. Pre-conditions described in clause C.2.2.1.4 Registration of VNFM as entity in charge of VNFCI certificate management are also considered to be met.
3	The VNFM has the VNFCI certificate and certificate chain issued and signed by CA.	See clause C.2.2.2 CSR Request for VNFCI. Pre-conditions described in clause C.2.2.2.4 CSR Request for VNFCI are also considered to be met.
4	The NFV MANO certificate for the VIM/CISM has been issued/signed and stored in the VIM/CISM.	The use case for NFV MANO certificate distribution to VIM/CISM is described in clause C.4.
5	The mTLS connection between VNFM and VIM/CISM has been configured.	

C.2.2.3.5 Post-conditions

Table C.2.2.3.5-1: Post-conditions

#	Post-condition	Description
1	The VNFCI has the VNFCI certificate, the certificate chain and VNFCI private key.	

C.2.2.3.6 Operational Flows

Table C.2.2.3.6-1: Operational flow

#	Flow	Description
0	VNFM -> VIM/CISM	The VIM/CISM receives the trigger: The VNFM sends a "AllocateComputeRequest" to the VIM as part of VNF Instantiation processes, see ETSI GS NFV-IFA 006 [9], or consume OS container workload management service interface, see ETSI GS NFV-IFA 040 [24]. In that message, the VNFM provides the VNFCI certificate, private key for the certificate and certificate chain.
1	VIM/CISM	The VIM process the "Allocate Virtulalized Compute Resource" or the CISM process the "Os container workload management service" and instantiates the VNF with the containing VNFCI and installs the VNFCI certificate, private key for the certificate and certificate chain.
2	VNFI	The instantiated VNFI includes the VNFCI with VNFCI certificate, certificate chain and private key in the VNFCI.
3	VIM/CISM -> VNFM	The VIM returns "AllocateComputeResponse" or the CISM returns response on "Os container workload management service interface" to the VNFM.

C.2.2.4 VNFCI certificate installation after VNF Instantiation

C.2.2.4.1 Introduction

The goal of the use case is to demonstrate the operation of VNFCI certificate installation to VNFCI after VNF instantiation. In delegation mode, the VNFM that is in charge of the certificate management for VNFCIs of VNFI, has the VNFCI certificate, private key for that certificate and certificate chain, see clause C.2.2.2 CSR Request for VNFCI.

The VNFM conveys that certificate, private key and certificate chain to VNFCI with VNF configuration procedure between VNF and VNFM after VNF instantiated.

C.2.2.4.2 Trigger

Table C.2.2.4.2-1: Trigger

Trigger	Description
VNF receives the request for VNF configuration	The VNF receives the request for VNF configuration from VNFM.

C.2.2.4.3 Actors and roles

Table C.2.2.4.3-1: Actors and roles

#	Actor	Description
1	VNFM/CISM	VNFM/CISM in charge of managing the VNFCI and acting as a delegate for the VNFCI certificate management, i.e. requesting issuance/signing of the VNFCI certificate, installing the VNFCI certificate/certificate chain into the VNFCI.
2	VNFI/VNFCI	VNFI, which has as component the VNFCI into which the VNFCI certificate that is managed by the VNFM should be installed.

C.2.2.4.4 Pre-conditions

Table C.2.2.4.4-1: Pre-conditions

#	Pre-condition	Description
1	Delegation mode is chosen for the VNFCI certificate management.	
2	The VNFM has the credentials (i.e. key pairs of public and private key) of the VNFCI, for the VNFCI certificate.	See clause C.2.2.1 Registration of VNFM as entity in charge of VNFCI certificate management. Pre-conditions described in clause C.2.2.1 Registration of VNFM as entity in charge of VNFCI certificate management are also considered to be met.
3	The VNFM has the VNFCI certificate and certificate chain issued and signed by CA.	See clause C.2.2.2 CSR Request for VNFCI. Pre-conditions described in clause C.2.2.2.4 CSR Request for VNFCI are also considered to be met.
4	The VNF has been instantiated, which includes VNFCI as target to inject the VNFCI certificate.	
5	The VNF OAM certificate for the VNFCI in the VNFI has been issued/signed and stored in the VNFCI.	The use case for VNF OAM certificate distribution to VNFCI is described in clause C.3.2.
6	The mTLS connection between VNFM and VNFCI has been configured.	

C.2.2.4.5 Post-conditions

Table C.2.2.4.5-1: Post-conditions

#	Post-condition	Description
1	The VNFCI has the VNFCI certificate, the certificate chain and VNFCI private key.	

C.2.2.4.6 Operational Flows

Table C.2.2.4.6-1: Operational flow

#	Flow	Description
0	VNFM -> (CISM->) VNFI	The VNFI receives the trigger: The VNFM sends a "SetConfigurationRequest" to the VNFI as part of the VNF configuration process, see ETSI GS NFV-IFA 008 [12] or consume "Os container configuration management service interface" produced by CISM, see ETSI GS NFV-IFA 040 [24] in case that the VNFCIs are realized as container-based and managed by CISM. As parameter in that message, the VNFM provides the VNFCI certificate, private key for the certificate and certificate chain.
1	VNFI/VNFCI	The VNFCI certificate, certificate chain and private key are installed into the VNFCI.
2	VNFI -> (CISM->) VNFM	The VNFI returns "SetConfigurationResponse" to the VNFM, or response on "Os container configuration management service" to the CISM in case that the VNFCIs are realized as container-based and managed by CISM.

C.2.2.4.7 Operational Flows with the use of an HSM

The private key of VNFCI is a critical asset and needs specific care for its installation in the VNFCI, and should be installed in a secure area. The generation of the key pair in an HSM (see clause C.2.2.2.7), the use of a HMEE in the VNFCI to install the private key, and the establishment of a secure channel end-to-end between the HMEE and the HSM for this installation is a best practice.

As additional pre-condition, the VNFCI (HMEE) has been successfully attested by the attestation service.

Table C.2.2.4.7-1 lists the additional pre-conditions applicable for the VNFCI certificate installation after VNF Instantiation with the use of HSM.

Table C.2.2.4.7-1: Pre-conditions

#	Pre-condition	Description
1	The VNFM integrates an HSM	The VNFM support a connection with an HSM for the key pair generation and the CSR signing for the VNFCI certificate
2	The VNFCI is instantiated in a secure area (e.g. HMEE)	
3	The key pair for the VNFCI has been generated in the HSM as described in clause C.2.2.2.7	
4	The VNFCI in the HMEE has been successfully attested by the attestation service	

Table C.2.2.4.7-2: Operational flow

#	Flow	Description
0	VNFM -> VNFI	The VNFI receives the trigger: The VNFM sends a "SetConfigurationRequest" to the VNFI as part of the VNF configuration process, see ETSI GS NFV-IFA 008 [12]. As parameter in that message, the VNFM provides the VNFCI certificate, certificate chain and details on HSM (HSM certificate).
1	VNFI/VNFCI (HMEE)	The VNFCI certificate, certificate chain are installed into the VNFCI.
2	VNFCI (HMEE) -> HSM	Establishment of a secure TLS channel between the HSM and the VNFCI using the remote attestation credentials of HMEE and HSM certificate. (See note)
3	VNFCI (HMEE) -> HSM	The VNFCI request the key pairs to the HSM.
4	HSM-> VNFCI (HMEE)	The HSM provides the key pairs to the VNFCI through the secure channel established in step-2.
5	VNFI -> VNFM	The VNFI returns "SetConfigurationResponse" to the VNFM.
NOTE: The protocol used between the HMEE and HSM is out of scope of the present document. A technology like Gramine could be used.		

NOTE: Use of HSM for certificate installation in Delegation mode may require further specification work (e.g. updates in different IFA interfaces). This potential normative work is left for future versions of the present document.

C.3 Use cases for VNF OAM certificate management

C.3.1 Direct mode

As described in clause C.2.1.1.1, a given VNFCI can be associated with multiple identities (i.e. multiple certificates) to be managed by the CMF. Among them, there can be also one or multiple VNF OAM certificates. These are handled in the same manner as the rest of the VNFCI certificates following the flow described in clause C.2.1.1 for certificate(s) enrolment.

C.3.2 Delegation mode

C.3.2.1 Registration of VNFM as entity in charge of VNF OAM certificate management

The operation of registration of VNFM as entity in charge of VNF OAM certificate management is the same as for VNFCI certificate as described in clause C.2.2.1, except that the type of certificate is VNF OAM certificate.

C.3.2.2 CSR Request for VNF OAM certificate

The operation of Certificate Signing Request for VNF OAM certificates is the same as for VNFCI certificates as described in clause C.2.2.1, except that the type of certificate is VNF OAM certificate and VNF OAM certificates are distributed during VNF instantiation.

C.3.2.3 VNF OAM certificate installation during VNF Instantiation

C.3.2.3.1 Introduction

The goal of the use case is to demonstrate the operation of VNF OAM certicate installation to VNFCI during VNF instantiation. In delegation mode, the VNFM that is in charge of the certificate management for the VNFI, has the VNF OAM certificate, private key for that certificate and certificate chain, see clause C.2.2.2 CSR Request for VNFCI. The VNFM conveys such certificate, private key and certificate chain to VNFCI by VNF instantiation procedure.

C.3.2.3.2 Trigger

Table C.3.2.3.2-1: Trigger

Trigger	Description
VIM receives the request for VNF instantiation	The VIM receives the request for VNFI instantiation from the VNFM.

C.3.2.3.3 Actors and roles

Table C.3.2.3.3-1: Actors and roles

#	Actor	Description
1	VNFM	VNFM in charge of managing the VNFCI and acting as a delegate for the VNF OAM certificate management, i.e. requesting issuance/signing of the VNF OAM certificate, installing the VNF OAM certificate/certificate chain into the VNFCI.
2	VIM	VIM, which is involved in the VNF instantiation procedure, i.e. the procedures run among VNFM/VIM.
3	VNFI	VNFI that contains the VNFCIs whose VNF OAM certificate is managed by the delegate VNFM.

C.3.2.3.4 Pre-conditions

Table C.3.2.3.4-1: Pre-conditions

#	Pre-condition	Description
1	Delegation mode is chosen for the VNFCI certificate management.	
2	The VNFM has the credentials (i.e. key pairs of public and private key) of the VNFCI, for the VNF OAM certificate.	See clause C.2.2.1 Registration of VNFM as entity in charge of VNFCI certificate management. Pre-conditions described in clause C.2.2.1.4 Registration of VNFM as entity in charge of VNFCI certificate management are also considered to be met.
3	The VNFM has the VNF OAM certificate and certificate chain issued and signed by CA.	See clause C.2.2.2 CSR Request for VNFCI. Pre-conditions described in clause C.2.2.2.4 CSR Request for VNFCI are also considered to be met.
4	The NFV MANO certificate for the VIM has been issued/signed and stored in the VIM.	The use case for NFV MANO certificate distribution to VIM is described in clause C.4.
5	The mTLS connection between VNFM and VIM has been configured.	

C.3.2.3.5 Post-conditions

Table C.3.2.3.5-1: Post-conditions

#	Post-condition	Description
1	The VNFCI has the VNF OAM certificate, the certificate chain and VNFCI private key.	

C.3.2.3.6 Operational Flows

Table C.3.2.3.6-1: Operational flow

#	Flow	Description
0	VNFM -> VIM	The VIM receives the trigger: The VNFM sends a "AllocateComputeRequest" to the VIM as part of VNF Instantiation process, see ETSI GS NFV-IFA 006 [9]. In that message, the VNFM provides the VNF OAM certificate, private key for the certificate and certificate chain.
1	VIM	The VIM processes the "Allocate Virtualized Compute Resource" and instantiates the VNF including VNFCI and installs the VNF OAM certificate, private key for the certificate and certificate chain in the VNFCI.
2	VNFI	The instantiated VNFI includes the VNFCI with VNF OAM certificate, certificate chain and private key in the VNFCI.
3	VIM -> VNFM	The VIM returns "AllocateComputeResponse" to the VNFM.

C.4 Use cases for NFV-MANO certificate management

C.4.1 NFVO certificate management

C.4.1.1 Registration of NFVO

C.4.1.1.1 Introduction

The goal of the use case is to demonstrate the operation of registration of NFVO.

C.4.1.1.2 Trigger

Table C.4.1.1.2-1: Trigger

Trigger	Description
CMF receives a request to register an FQDN of a NFVO	The consumer sends a request to the CMF to register a NFVO.

C.4.1.1.3 Actors and roles

Table C.4.1.1.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for NFVO certificate management.
2	Consumer	OSS.

C.4.1.1.4 Pre-conditions

Table C.4.1.1.4-1: Pre-conditions

#	Pre-condition	Description
1	The CA has generated the key pair of public key and private key for the CA.	
2	The CA has certificate for the CA issued and signed by the Root CA and the certificate chain.	
3	The CMF has generated the key pair of public key and private key for the CMF.	
4	The CMF has certificate for the CMF issued and signed by the CA and the certificate chain.	
5	The CMF is capable to validate the FQDN in the incoming registration request.	
6	The consumer is trusted.	

NOTE: This version of the present document does not specify reference point and interfaces between the CA and CMF.

C.4.1.1.5 Post-conditions

Table C.4.1.1.5-1: Post-conditions

#	Post-condition	Description
1	The CMF has registered the FQDN of the NFVO.	

C.4.1.1.6 Operational Flows

Table C.4.1.1.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The consumer sends a registration request to register the NFVO. The consumer provides the FQDN of the NFVO as input parameters.
1	CMF	The CMF validates the registration request and that the consumer is trusted to make the request. If valid, the CMF registers the FQDN of the NFVO. The CMF selects the certificate authority for the requested certificate management. If the registration request is invalid, a rejection message is returned to the consumer. The CMF can create an initial credential to authenticate the connection between the CMF, CA and NFVO for the purpose the certificate signing request.
2	CMF -> Consumer	The CMF sends the response of success or failure to the consumer. The response includes the initial credential if it was created above.

C.4.1.2 CSR Request for NFVO certificate

C.4.1.2.1 Introduction

The goal of the use case is to demonstrate the operation of Certificate Signing Request for NFVO certificate. The CMF is requested to, in cooperation with the Certificate Authority, issue and sign the NFVO certificate and to return the NFVO certificate and certificate chain to the NFVO.

C.4.1.2.2 Trigger

Table C.4.1.2.2-1: Trigger

Trigger	Description
CMF receives a request to issue a NFVO certificate	The consumer sends a request to the CMF to issue and sign a certificate for NFVO.

C.4.1.2.3 Actors and roles

Table C.4.1.2.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for NFVO certificate management.
2	Consumer	NFVO requesting its own certificate.
3	CA	Certificate Authority in charge of issuing and signing the NFVO certificate.

C.4.1.2.4 Pre-conditions

Table C.4.1.2.4-1: Pre-conditions

#	Pre-condition	Description
1	The CMF has registered the FQDN of the NFVO.	See clause C.4.1.1.1 Registration of NFVO.
2	The information to form the Certificate Signing Request for the requested NFVO certificates have been known to the NFVO via Os-Ma-Nfvo (from OSS to NFVO). The information are e.g. "Common Name", "Organization", "Country", "State", "Locality", "CertificationType" and "SubjectAltName" and initial credential where required.	See ETSI GS NFV-IFA 013 [11] and ETSI GS NFV-IFA 007 [10].

C.4.1.2.5 Post-conditions

Table C.4.1.2.5-1: Post-conditions

#	Post-condition	Description
1	The NFVO has the requested NFVO certificate and the certificate chain for the NFVO certificate.	

C.4.1.2.6 Operational Flows

Table C.4.1.2.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer generates the key pairs of public key and private key for the NFVO certificate. The consumer generates Certificate Signing Request with the information, which the consumer prepared via Os-Ma-Nfvo/NFVO itself and signs with the NFVO private key. The consumer sends a Certificate Signing Request to the CMF to obtain a NFVO certificate including the initial credential if required (see note).
1	CMF	The CMF verifies whether the consumer is registered. If the verification fails, the CMF returns an error response to the consumer.
2	CMF	The CMF validates the information in the CSR and initial credential where used. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue and sign the NFVO certificate.
4	CA	The CA issues the NFVO certificate (including NFVO public key) and signs it with the private key of the CA.
5	CA->CMF	The CA returns the requested NFVO certificate and certificate chain to the CMF.
6	CMF->Consumer	The CMF returns the requested NFVO certificate and certificate chain for the NFVO certificate to the consumer.
NOTE: The initial credential will not be used for authentication/authorization at the CMF where a valid certificate and private key exists in the NFVO that is recognized by the CMF.		

C.4.1.2.7 Operational Flows with the use of HSM

Table C.4.1.2.7-1 lists the additional pre-conditions applicable for the CSR request for NFVO certificate with the use of HSM

Table C.4.1.2.7-1: Pre-conditions

#	Pre-condition	Description
1	The NFVO integrates an HSM	The NFVO support a connection with an HSM for the key pair generation and the CSR signing

Table C.4.1.2.7-2: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer requests to the HSM the generation of the key pairs of public key and private key for the NFVO certificate and the transmission of the corresponding public key. If key attestation is used, the Consumer requests the key attestation statement to the HSM. The consumer generates Certificate Signing Request with the information (see note 2), which the consumer prepared via Os-Ma-Nfvo/NFVO itself and requests the HSM to sign the CSR with the NFVO private key. The consumer sends a Certificate Signing Request to the CMF to obtain a NFVO certificate including the initial credential if required (see note 1).
1	CMF	The CMF verifies whether the consumer is registered. If the verification fails, the CMF returns an error response to the consumer
2	CMF	The CMF validates the information in the CSR and initial credential where used. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue and sign the NFVO certificate.
4	CA	The CA issues the NFVO certificate (including NFVO public key) and signs it with the private key of the CA.
5	CA->CMF	The CA returns the requested NFVO certificate and certificate chain to the CMF.
6	CMF->Consumer	The CMF returns the requested NFVO certificate and certificate chain for the NFVO certificate to the consumer.
NOTE 1: The initial credential will not be used for authentication/authorization at the CMF where a valid certificate and private key exists in the NFVO that is recognized by the CMF. NOTE 2: The details of the key attestation inclusion in the CSR is left for further specification.		

C.4.2 VNFM certificate management

C.4.2.1 Registration of VNFM

C.4.2.1.1 Introduction

The goal of the use case is to demonstrate the operation of registration of VNFM.

C.4.2.1.2 Trigger

Table C.4.2.1.2-1: Trigger

Trigger	Description
CMF receives a request to register an FQDN of a VNFM	The consumer sends a request to the CMF to register a VNFM.

C.4.2.1.3 Actors and roles

Table C.4.2.1.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VNFM certificate management.
2	Consumer	OSS.

C.4.2.1.4 Pre-conditions

Table C.4.2.1.4-1: Post-conditions

#	Pre-condition	Description
1	The CA has generated the key pair of public key and private key for the CA.	
2	The CA has certificate for the CA issued and signed by the Root CA and the certificate chain.	
3	The CMF has generated the key pair of public key and private key for the CMF.	
4	The CMF has the certificate for the CMF issued and signed by the CA and the certificate chain.	
5	The CMF is capable to validate the FQDN in the incoming registration request.	
6	The consumer is trusted.	

NOTE: This version of the present document does not specify reference point and interfaces between the CA and CMF.

C.4.2.1.5 Post-conditions

Table C.4.2.1.5-1: Post-conditions

#	Post-condition	Description
1	The CMF has registered the FQDN of the VNFM.	

C.4.2.1.6 Operational Flows

Table C.4.2.1.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The consumer sends a registration request to register the VNFM. The consumer provides the FQDN of the VNFM as input parameters.
1	CMF	The CMF validates the registration request and that the consumer is authorized to make the request. If valid, the CMF registers the FQDN of the VNFM. The CMF selects the certificate authority for the requested certificate management. If the registration request is invalid, a rejection message is returned to the consumer. The CMF can create an initial credential to authenticate the connection between the CMF, CA and VNFM for the purpose the certificate signing request.
2	CMF -> Consumer	The CMF sends the response of success or failure to the consumer. The response includes the initial credential if it was created above.

C.4.2.2 CSR Request for VNFM certificate

C.4.2.2.1 Introduction

The goal of the use case is to demonstrate the operation of Certificate Signing Request for VNFM certificate. The CMF is requested to, in cooperation with the Certificate Authority, issue and sign the VNFM certificate and to return the VNFM certificate and certificate chain to the VNFM.

C.4.2.2.2 Trigger

Table C.4.2.2.2-1: Trigger

Trigger	Description
CMF receives a request to issue a VNFM certificate	The consumer sends a request to the CMF to issue and sign a certificate for VNFM.

C.4.2.2.3 Actors and roles

Table C.4.2.2.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VNFM certificate management.
2	Consumer	VNFM requesting its own certificate.
3	CA	Certificate Authority in charge of issuing and signing the VNFM certificate.

C.4.2.2.4 Pre-conditions

Table C.4.2.2.4-1: Pre-conditions

#	Pre-condition	Description
1	The CMF has registered the FQDN of the VNFM.	See clause C.4.2.1 Registration of VNFM.
2	The information to form the Certificate Signing Request for the requested VNFM certificates have been known to the VNFM via Os-Ma-Nfvo (from OSS to NFVO) and Or-Vnfm (from NFVO to VNFM). The information are e.g. "Common Name", "Organization", "Country", "State", "Locality", "CertificationType" and "SubjectAltName" and initial credential where required.	See ETSI GS NFV-IFA 013 [11] and ETSI GS NFV-IFA 007 [10].

C.4.2.2.5 Post-conditions

Table C.4.2.2.5-1: Post-conditions

#	Post-condition	Description
1	The VNFM has the requested VNFM certificate and the certificate chain for the VNFM certificate.	

C.4.2.2.6 Operational Flows

Table C.4.2.2.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer generates the key pairs of public key and private key for the VNFM certificate. The consumer generates Certificate Signing Request with the information, which the consumer prepared via Os-Ma-Nfvo/Or-Vnfm/VNFM itself and signs with the VNFM private key. The consumer sends a Certificate Signing Request to the CMF to obtain a VNFM certificate including the initial credential if required (see note).
1	CMF	The CMF verifies whether the consumer is registered. If the verification fails, the CMF returns an error response to the consumer.
2	CMF	The CMF validates the information in the CSR and initial credential where used. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue/ and sign the VNFM certificate.
4	CA	The CA issues the VNFM certificate (including VNFM public key) and signs it with the private key of the CA.
5	CA->CMF	The CA returns the requested VNFM certificate and certificate chain to the CMF.
6	CMF->Consumer	The CMF returns the requested VNFM certificate and certificate chain for the VNFM certificate to the consumer.
NOTE: The initial credential will not be used for authentication/authorization at the CMF where a valid certificate and private key exists in the VNFM that is recognized by the CMF.		

C.4.2.2.7 Operational Flows with the use of HSM

Table C.4.2.2.7-1 lists the additional pre-conditions applicable for the CSR request for VNFM certificate with the use of HSM.

Table C.4.2.2.7-1: Pre-conditions

#	Pre-condition	Description
1	The VNFM integrates an HSM	The VNFM support a connection with an HSM for the key pair generation and the CSR signing

Table C.4.2.2.7-2: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer requests to the HSM the generation of the key pairs of public key and private key for the VNFM certificate and the transmission of the corresponding public key. If key attestation is used, the Consumer requests the key attestation statement to the HSM. The consumer generates Certificate Signing Request with the information (see note 2), which the consumer prepared via Os-Ma-Nfvo/Or-Vnfm/VNFM itself and requests the HSM to sign the CSR with the VNFM private key. The consumer sends a Certificate Signing Request to the CMF to obtain a VNFM certificate including the initial credential if required (see note 1).
1	CMF	The CMF verifies whether the consumer is registered. If the verification fails, the CMF returns an error response to the consumer
2	CMF	The CMF validates the information in the CSR and initial credential where used. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue/ and sign the VNFM certificate.
4	CA	The CA issues the VNFM certificate (including VNFM public key) and signs it with the private key of the CA.
5	CA->CMF	The CA returns the requested VNFM certificate and certificate chain to the CMF.
6	CMF->Consumer	The CMF returns the requested VNFM certificate and certificate chain for the VNFM certificate to the consumer.
NOTE 1: The initial credential will not be used for authentication/authorization at the CMF where a valid certificate and private key exists in the VNFM that is recognized by the CMF. NOTE 2: The details of the key attestation inclusion in the CSR is left for further specification.		

C.4.3 VIM certificate management

C.4.3.1 Registration of VIM

C.4.3.1.1 Introduction

The goal of the use case is to demonstrate the operation of registration of VIM.

C.4.3.1.2 Trigger

Table C.4.3.1.2-1: Trigger

Trigger	Description
CMF receives a request to register an FQDN of a VIM	The consumer sends a request to the CMF to register a VIM.

C.4.3.1.3 Actors and roles

Table C.4.3.1.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VIM certificate management.
2	Consumer	OSS

C.4.3.1.4 Pre-conditions

Table C.4.3.1.4-1: Pre-conditions

#	Pre-condition	Description
1	The CA has generated the key pair of public key and private key for the CA.	
2	The CA has certificate for the CA issued and signed by the Root CA and the certificate chain.	
3	The CMF has generated the key pair of public key and private key for the CMF.	
4	The CMF has certificate for the CMF issued and signed by the CA and the certificate chain.	
5	The CMF is capable to validate the FQDN in the incoming registration request.	
6	The consumer is trusted.	

NOTE: This version of the present document does not specify reference point and interfaces between the CA and CMF.

C.4.3.1.5 Post-conditions

Table C.4.3.1.5-1: Post-conditions

#	Post-condition	Description
1	The CMF has registered the FQDN of the VIM.	

C.4.3.1.6 Operational Flows

Table C.4.3.1.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The consumer sends a registration request to register the VIM. The consumer provides the FQDN of the VIM as input parameters.
1	CMF	The CMF validates the registration request and that the consumer is authorized to make the request. If valid, the CMF registers the FQDN of the VIM. The CMF selects the certificate authority for the requested certificate management. If the registration request is invalid, a rejection message is returned to the consumer. The CMF can create an initial credential to authenticate the connection between the CMF, CA and VIM for the purpose the certificate signing request.
2	CMF -> Consumer	The CMF sends the response of success or failure to the consumer. The response includes the initial credential if it was created above.

C.4.3.2 CSR Request for VIM certificate

C.4.3.2.1 Introduction

The goal of the use case is to demonstrate the operation of Certificate Signing Request for VIM certificate. The CMF is requested to, in cooperation with the Certificate Authority, issue and sign the VIM certificate and to return the VIM certificate and certificate chain to the VIM.

C.4.3.2.2 Trigger

Table C.4.3.2.2-1: Trigger

Trigger	Description
CMF receives a request to issue a VIM certificate	The consumer sends a request to the CMF to issue and sign a certificate for VIM.

C.4.3.2.3 Actors and roles

Table C.4.3.2.3-1: Actors and roles

#	Actor	Description
1	CMF	Certificate Management Function for VIM certificate management.
2	Consumer	VIM requesting its own certificate.
3	CA	Certificate Authority in charge of issuing and signing the VIM certificate.

C.4.3.2.4 Pre-conditions

Table C.4.3.2.4-1: Pre-conditions

#	Pre-condition	Description
1	The CMF has registered the FQDN of the VIM.	See clause C.4.3.1 Registration of VNFM.
2	The information to form the Certificate Signing Request for the requested VIM certificates have been known to the VIM via Os-Ma-Nfvo (from OSS to NFVO), Or-Vnfm (from NFVO to VNFM) and Vi-Vnfm (From NFVM to VIM). The information are e.g. "Common Name", "Organization", "Country", "State", "Locality", "CertificationType" and "SubjectAltName" and initial credential where required.	See ETSI GS NFV-IFA 013 [11] and ETSII GS NFV-IFA 007 [10].

C.4.3.2.5 Post-conditions

Table C.4.3.2.5-1: Post-conditions

#	Post-condition	Description
1	The VIM has the requested VIM certificate and the certificate chain for the VIM certificate.	

C.4.3.2.6 Operational Flows

Table C.4.3.2.6-1: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer generates the key pairs of public key and private key for the VIM certificate. The consumer generates Certificate Signing Request with the information, which the consumer prepared via Os-Ma-Nfvo/Or-Vnfm/Vi-Vnfm/VIM itself and signs with the VIM private key. The consumer sends a Certificate Signing Request to the CMF to obtain a VIM certificate including the initial credential if required (see note).
1	CMF	The CMF verifies whether the consumer is registered. If the verification fails, the CMF returns an error response to the consumer
2	CMF	The CMF validates the information in the CSR and initial credential where used. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue and sign the VIM certificate.
4	CA	The CA issues the VIM certificate (including VIM public key) and signs it with the private key of the CA.
5	CA->CMF	The CA returns the requested VIM certificate and certificate chain to the CMF.
6	CMF->Consumer	The CMF returns the requested VIM certificate and certificate chain for the VIM certificate to the consumer.
NOTE: The initial credential will not be used for authentication/authorization at the CMF where a valid certificate and private key exists in the VIM that is recognized by the CMF.		

C.4.3.2.7 Operational Flows with the use of HSM

Table C.4.3.2.7-1 lists the additional pre-conditions applicable for the CSR request for VIM certificate with the use of HSM.

Table C.4.3.2.7-1: Pre-conditions

#	Pre-condition	Description
1	The VIM integrates an HSM	The VIM support a connection with an HSM for the key pair generation and the CSR signing

Table C.4.3.2.7-2: Operational flow

#	Flow	Description
0	Consumer -> CMF	The CMF receives the trigger: The Consumer requests to the HSM the generation of the key pairs of public key and private key for the VIM certificate and the transmission of the corresponding public key. If key attestation is used, the Consumer requests the key attestation statement to the HSM. The consumer generates Certificate Signing Request with the information (see note 2), which the consumer prepared via Os-Ma-Nfvo/Or-Vnfm/Vi-Vnfm/VIM itself and requests the HSM to sign the CSR with the VIM private key. The consumer sends a Certificate Signing Request to the CMF to obtain a VIM certificate including the initial credential if required (see note 1).
1	CMF	The CMF verifies whether the consumer is registered. If the verification fails, the CMF returns an error response to the consumer.
2	CMF	The CMF validates the information in the CSR and initial credential where used. If the validation fails, the CMF returns an error response to the consumer.
3	CMF->CA	The CMF requests CA to issue and sign the VIM certificate.
4	CA	The CA issues the VIM certificate (including VIM public key) and signs it with the private key of the CA.
5	CA->CMF	The CA returns the requested VIM certificate and certificate chain to the CMF.
6	CMF->Consumer	The CMF returns the requested VIM certificate and certificate chain for the VIM certificate to the consumer.
NOTE 1: The initial credential will not be used for authentication/authorization at the CMF where a valid certificate and private key exists in the VIM that is recognized by the CMF. NOTE 2: The details of the key attestation inclusion in the CSR is left for further specification.		

C.5 Use cases for Virtualised computation environment control plane certificate management

Management of Virtualised computation environment control plane certificates is not considered in the current version of the present document.

C.6 VNFCI Certificate Profile Example

Table C.6-1 provides an example of certificate profile based on the 3GPP Rel-16 SBA NF TLS Client and Server Certificate Profile [i.5]. The two right-most columns indicate if the corresponding certificate attribute value may be set by the CA from a CA preconfigured certificate profile or if the value is supplied by the VNFCI through the CSR. While most of the information on Subject DN and subjectAltName is available to the CMF, a subset of the subjectAltName may also be locally generated by the VNFCI (e.g. the 3GPP NFInstanceID [i.5]).

Table C.6-1: Example of VNFCI certificate profile based on the SBA NF TLS Client and Server Certificate Profile in ETSI TS 133 310 [i.5]

SBA NF TLS Client and Server Certificate Profile					CA set from profile	CA set from CSR Request (see note 1)
Version		v3			x	
Serial Number		Unique Positive Integer in the context of the issuing Root CA and not longer than 20 octets.			x	
Subject DN		C=<Country> O= Home Domain Name (e.g. in "5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" format) example: "C=SE,O=5gc.mnc060.mcc240.3gppnetwork.org" CN should be empty				x
Validity Period		3 years or less			x	
Signature		RSAEncryption or ECDSA			x	
Subject Public Key Info		rsaEncryption or id-ecPublicKey			x	
Extensions	**OID**	**Mandatory**	**Criticality**	**Value**		
keyUsage	{id-ce 15}	TRUE	TRUE	digitalSignature for TLS clients and servers	x x	
extendedKeyUsage	{id-ce 37}	TRUE	FALSE	id-kp-clientAuth TLS clients	x	
				id-kp-serverAuth for TLS servers NF that may be both client and server shall have both OIDs set.	x	
authorityKeyIdentifier	{id-ce 35}	TRUE	FALSE	This shall be the same as subjectKeyIdentifier of the Issuer's certificate. CA shall utilitize the method (1) as defined in clause 4.2.1.2 of IETF RFC 5280 [i.10] to generate the value for this extension.	x	
subjectKeyIdentifier	{id-ce 14}	FALSE	FALSE	This shall be calculated by the issuing CA utilitizing the method (1) as defined in clause 4.2.1.2 of IETF RFC 5280 [i.10] to generate the value for this extension.	x	
cRLDistributionPoint	{id-ce 31}	TRUE	FALSE	distributionPoint According to IETF RFC 5280 [i.10] this indicates if the CRL is available for retrieval using access protocol and location with LDAP or HTTP URI.	x	
subjectAltName	{id-ce 17}	TRUE	TRUE	Multiple subjectAltName entries can be used as a sequence, see below for the detailed instructions.		x
authorityInfoAccess	{id-pe 1}	FALSE	FALSE	id-ad-caIssuers According to IETF RFC 5280 [i.10] id-ad-caIssuers describes the referenced description server and the access protocol and location, for example, using one or multiple HTTP and/or LDAP URIs.	x	
				id-ad-ocsp According to IETF RFC 5280 [i.10] id-ad-ocsp defines the location of the OCSP responder using HTTP URI.	x	
TLS feature extension	{id-pe 24}	FALSE	FALSE	id-pe-tlsfeature This can be used according to IETF RFC 7633 [i.11] to prevent downgrade attacks that are not otherwise prevented by the TLS protocol; also to be used with OCSP stapling with TLS server end-entity certificates.	x	
nfTypes	{id-pe 34}	TRUE	FALSE	id-pe-nftypes specified in IETF RFC 9310 [i.12] enables including Network Function types (NFTypes) for the 5G System in X.509 v3 public key certificates.		x

NOTE: The certificate request may carry information for the DN, SubjectAltName as well as of the NFType extensions but the CA may ignore data values and use instead values set during VNFCI end-entity registration. Whether the CA will do such an override or not and instead use the values in the request is a CA policy (configuration) decision.

Annex D (informative): Security consideration for Certificate Management

D.1 Additional security considerations and implications for the direct-mode and delegation-mode

Different factors may affect the security assurances provided in an NFV deployment where the CMF and NFV-MANO implement one of the two modes described in clause 5.2.3.1. Furthermore, the security of direct mode VNFs in a dual mode deployment is comparatively less secure than that of direct mode VNFs in a direct mode only deployment. The following four factors related to private key management are considered relevant given the characteristics of the two modes for VNFCI certificate enrolment:

- **Key proof-of-possession:** an entity receiving a public key is expected to obtain assurance that the claiming owner of the key-pair possesses the private key corresponding to the received public key. For example, prior to issuing a certificate, the CA obtains a proof of the private key possession from the entity claiming ownership of the public key submitted for certification.

- **Key storage protection:** to minimize the consequences of a private key compromise, protective measures are taken to protect private keys during all their lifecycle, including storage.

- **Key transport:** if the lifecycle of a private key includes its distribution (e.g. over the network), then protective measures are taken to ensure such secure operation.

- **Key entropy:** an adequate Random Number Generator (RNG) is required for private key generation.

These factors apply to the two modes described in clause 5.2.3.1 as follows.

In direct-mode:

- **Key proof-of-possession:** each VNFCI generates its own VNFCI key-pair(s) (see clause C.2.1). At VNFCI certificate enrolment, the proof-of-possession is obtained by the CA directly from VNFCI, i.e. the unique owner of its private key. An implication is that the direct-mode is suitable in NFV deployments requiring VNF secure bootstrap with remote attestation and HMEE where it is required that the VNFCI private key associated with the certified public key never leaves the HMEE instance having generated the private key.

- **Key storage protection:** VNFCI key storage security is expected to be implemented at the VNFCI level where the private key is generated and stored. Note that, in NFV deployments requiring VNF secure bootstrap with remote attestation and HMEE, by having the CMF as a relying party of an attest verifier of the VNFCI such protection and storage means in the VNFCI can be attested.

- **Key transport:** not applicable (i.e. the VNFCI private keys are not transported in direct-mode).

- **Key entropy:** a proper configuration (following well-known hardening guidelines) of the NFVI to expose HW RNGs to VNFCIs is required.

In delegation-mode:

- **Key proof-of-possession:** the VNFCI does not generate its own private key. The VNFCI private key is generated by the VNFM, which is responsible to provide the key proof-of-possession to the CMF when the VNFCI public key is submitted for certification. The CA certifies the VNFCI public key before the reputed owner of the corresponding private key owns the key-pair. An implication of VNFM acting as a delegate in the VNFCI private key management is that the CA does not find in the proof-of-possession that only the VNFCI is the holder of the private key. This lowers the level of trust in issued certificates compared to the direct-mode case: while a VNFM in both direct and delegation modes is trusted for the typical VNF lifecycle management operations, the VNFM shall be further trusted in delegation-mode to handle the VNFCI keys securely. Another implication is that the delegation-mode is less suitable in NFV deployments requiring VNF secure bootstrap with remote attestation and HMEE where it is required that the VNFCI private key associated with the certified public key never leaves the HMEE instance having generated the private key.

- **Key storage:** VNFCI key storage security is expected to be implemented at the VNFM (where the VNFCI key-pairs are generated), VIM (where the key-pair and certificate are copied and transmitted), and at the VNFCI level where the private key is stored. Once the VNFCI key is no longer required on the VNFM and VIM it shall be securely deleted.

- **Key transport:** the VNFCI private key being generated at VNFM and sent to the VNFCI via VIM (during VNF instantiation), a secure transport procedure is required on these channels.

- **Key entropy:** the VNFCI implicitly trusts the external source of entropy, which is used at the VNFM to generate the VNFCI private key.

Table D.1-1 summarizes the above description applicable to the direct and delegation modes.

Table D.1-1: Description of the four private key factors applicable to the direct and delegation modes

Factor \ Mode	Direct-mode	Delegation-mode
Key Proof-of-possession	The proof-of-possession is guaranteed coupled to the VNFCI end-point	The proof-of-possession no longer implies guaranteed key ownership
Key storage protection	VNFCI key storage security to be implemented at VNF(C)I	VNFCI key storage security to be implemented at VNF(C)I, VIM, VNFM
Key Transport	Not applicable (VNFCI private keys are not transported)	VNFCI private key secure transport procedure is required from the VNFM
Key entropy	Configuration of NVFI to expose HW RNG to VNFCIs is required	VNFCIs trust the external source of entropy used to generate their private keys at VNFM

Annex E (informative): Change History

Date	Version	Information about changes
2016-11	0.1.0	Implemented NFVIFA#40 approved contributions NFVIFA(16)0001320r1, NFVIFA(16)0001334 and NFVIFA(16)0001380r2.
2017-05	0.2.0	Implemented NFVIFA#52 approved contribution NFVIFA(17)000315.
2017-08	0.3.0	Implemented approved contribution NFVIFA(17)000500.
2018-09	0.4.0	Major re-write of document to align with transfer of document ownership to NFV-SEC. Output of SEC in NFV SEC#131 F2F as SEC(18)000111. This version entirely replaces all sections of v0.3.0.
2018-12	0.5.0	Output from SEC#136F2F. Includes NFVSEC(18)000138r3.
2019-02	0.5.1	Editorial formatting and drafting rule corrections.
2019-02	0.5.2	Implementing comments in NFVIFA(19)000161r1 and some comments in NFVIFA(19)000162.
2019-02	0.5.2a & b	Address comments in NFVIFA(19)000156r1.
2019-03	0.6.0	Agreed baseline at NFVSEC#142. Content same as v0.5.2b.
2019-05	0.6.1	Drafting rule compliance ("must" replaced in Notes).
2019-05	0.6.2	Further final review comments addressed (see IFA/SEC email lists).
2020-06	3.4.1	Publication (unmodified with respect to version V3.2.1).
2023-03	4.4.2	Contributions incorporated: • NFVIFA(23)000088r1_Enh01_01_IFA026_add_usecase_and_functional_requirements
2023-03	4.4.3	Contributions incorporated: • NFVSEC(22)000113r2 • NFVSEC(22)000116r2 • NFVSEC(23)000033r2 • NFVSEC(23)000035 • NFVIFA(23)000220
2023-05	4.4.4	Contributions incorporated: • NFVSEC(23)000036r1 • NFVSEC(23)000053 • NFVSEC(23)000056 • NFVSEC(23)000072 • NFVSEC(23)000073 • NFVSEC(23)000079r1 • NFVSEC(23)000080r1 • NFVIFA(23)000369

Date	Version	Information about changes
2023-06	4.4.5	Contributions incorporated: • NFVSEC(23)000037 • NFVSEC(23)000044r2 • NFVSEC(23)000081 • NFVSEC(23)000099r1 • NFVSEC(23)000101r1 • NFVSEC(23)000102r1 • NFVSEC(23)000103 • NFVSEC(23)000104r1 • NFVSEC(23)000105 • NFVSEC(23)000106r2 • NFVSEC(23)000107r1 • NFVSEC(23)000109 • NFVSEC(23)000115 • NFVSEC(23)000122r3 • NFVSEC(23)000128 • NFVSEC(23)000150r1 • NFVSEC(23)000151r1 • NFVSEC(23)000152 • NFVSEC(23)000153r2 • NFVSEC(23)000154r2 • NFVSEC(23)000155r1 • NFVSEC(23)000158 • NFVSEC(23)000170r1 • NFVSEC(23)000176 • NFVIFA(23)000369 Editorial improvements.
2023-08	4.4.6	Incorporating contribution NFVSEC(23)000180r1 / NFVIFA(23)000604r1

History

Document history		
V4.5.1	October 2023	Publication