ETSI GR NFV-SEC 005 V1.2.1 (2021-07)

Network Functions Virtualisation (NFV);
Trust;
Report on Certificate Management

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
RGR/NFV-SEC005ed121

Keywords
certificate, NFV, 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:
http://www.etsi.org/standards-search

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

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

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

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2021.
All rights reserved.

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

In the present document "**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 provides guidance to the development community on the use of Public Key Certificates, Attribute Certificates and the supporting infrastructure, including Registration Authorities, and Certificate Authorities. The present document provides this guidance in the context of a number of use cases and references to other publications of ETSI ISG NFV.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] Void.

[i.2] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

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

[i.4] ETSI GS NFV 004: "Network Functions Virtualisation (NFV); Virtualisation Requirements".

[i.5] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.6] Void.

[i.7] Void.

[i.8] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement".

[i.9] Void.

[i.10] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.11] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.12] Void.

[i.13] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.14] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.15] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.16] IETF RFC 7030: "Enrollment over Secure Transport".

[i.17] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.18] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)".

[i.19] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".

[i.20] IETF RFC 8894: "Simplified Certificate Enrollment Protocol".

[i.21] IETF RFC 8295: "EST (Enrollment over Secure Transport) Extensions".

[i.22] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV) Release 2; Security; VNF Package Security Specification".

[i.23] ETSI GS NFV-SEC 023: "Network Functions Virtualisation (NFV) Release 4; Security; Container Security Specification".

[i.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".

[i.25] Kubernetes® API v1.21.

NOTE: Available at https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.21/.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS NFV 003 [i.3] and the following apply:

attribute certificate: data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder

trust chain: data structure, containing a sequence of Certificate Authority certificates where each certificate is signed by the subsequent certificate in the file, ending in a root Certificate Authority certificate

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.3] and the following apply:

CA	Certificate Authority
CP	Certificate Policy
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root CA

4 Rationale and approach for the use of public key certificates

4.1 Scope

The present document provides a guide to the use of Public Key Infrastructures (PKI) for the purpose of distributing Public Key Certificates (PKC) as applicable to the ETSI ISG NFV for the support of Public Key Cryptography in authenticating, authorizing and encrypting links between objects in NFV.

Each operator should develop Certificate Policy in accordance with their regional and national requirements. The present document assumes that the reader is generally familiar with Digital Signatures, PKIs, and core ETSI NFV specifications. The present document is consistent with the Internet X.509 Certificate Policy and Certification Practices Framework as defined in IETF RFC 3647 [i.14]. The certificate policy defines the structure of PKI.

NOTE: The PKIs described in the present document are privately managed, thus non-private (non-permissioned) PKIs are out of scope of the present document.

4.2 PKI Participants

4.2.0 Introduction

An NFV PKI can be implemented as a multi-tier hierarchy with a Root Certification Authority (RCA) at tier 1. There may be many certificate chains anchored by the RCA. Identified chains can be organized functionally and might include NFVI, VNF, MANO, and Support (such as OSS/BSS). A representative certificate hierarchy is shown in figure 4.2.0-1. The fewer tiers there are in the hierarchy, the smaller attack surface is, at the cost of limiting the number of trust domains.

The end-entity certificate, its private key, and all sub-CA certificates for a given CA chain should be installed on the device (hardware resource or software element, as appropriate). During authentication messaging exchange (using TLS or similar protocol) the end-entity and all sub-CA chain certificates should be sent to the other end point.

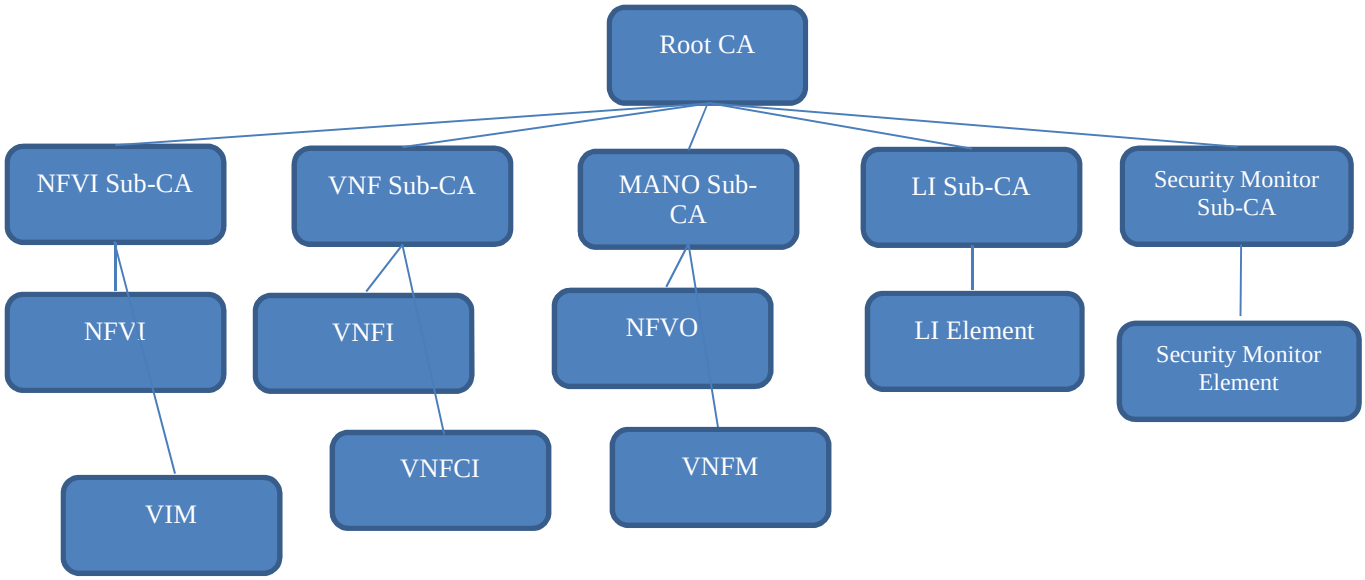

Figure 4.2.0-1: ETSI NFV PKI Certificate Hierarchy

Support of multiple roots is possible and when used it is expected to be specified by the operator. To anchor trust, certificates issued in ecosystems comprised of multiple roots have to be verifiable (chainable) to the corresponding root. This may be accomplished by cross signing certificates or allowing subscribers to honour multiple roots. This may provide ecosystem supply chain benefits at the risk of a substantially increased PKI attack surface. Furthermore, PKI operations of either deploying multiple valid chains or executing cross signing while achieving security over time has proven difficult.

PKI participants can include registration authorities, subscribers, relying parties, and auditors. PKI participants are described below.

4.2.1 Certificate Authorities

The entities called Certificate Authorities (CAs) are the heart of the ETSI NFV PKI. The CA is an aggregate term encompassing the collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to Subscribers or other CAs. The CAs are responsible for:

- Implementing and maintaining a Certificate Policy (CP).
- Issuing compliant certificates.
- Delivery of certificates to Subscribers in accordance with the CP and other documents such as a Subscriber Agreement.
- Revocation of certificates.
- Generation of key pairs, protection, operation, and destruction of CA private keys.
- CA certificate lifecycle management ensure that all aspects of the CA services, operations, and infrastructure related to certificates issued under the CP are in fact compliant to the CP.
- Facilitating as a trusted party the confirmation of the binding between a public key and the identity, and/or other attributes, of the "Subject" of the certificate.

Sub-CAs are operated by designated sub-CA service providers and issue end-entity device certificates to subscribers.

4.2.2 Registration Authorities

Registration authorities (RAs) are entities that enter into an agreement with a CA to collect and verify each Subscriber's identity and information to be entered into the Subscriber's certificates. The RA performs its function in accordance with the CP and will perform front-end functions of confirming the identity of the certificate applicant, approving or denying certificate applications (manual) or requests (dynamic), requesting revocation of certificates, and managing account renewals.

4.2.3 Subscribers

The Subscriber is an organization or process acting on behalf of an organization identified in a Digital Certificate Subscriber Agreement (DCSA). The Subscriber is responsible for completing the certificate application or request. The CA relies on the RA to confirm the identity of the Certificate Applicant and either approves or denies the application or request. If approved, the RA communicates to the CA, and the Subscriber can then request certificates.

Subscribers are expected to comply to both CP requirements and any additional certificate management practices that govern the Subscribers' request for certificates and for handling the corresponding private keys. The Subscriber agrees to be bound by its obligations through execution of the DCSA between the Subscriber and the RA, and any other applicable agreements.

Technically, CAs are also Subscribers of certificates within a PKI, either as a Root CA issuing a self-signed certificate to itself, or as a sub-CA. However, in the present document, Subscriber apply only to the organization requesting device certificates, including those Subscribers who may have arranged to have a sub-CA operated onsite at their facility.

4.2.4 Relying Parties

Relying Parties validate the binding of a public key to a Subscriber's name in a device certificate. The RP is responsible for deciding whether or how to check the validity of a certificate by checking the appropriate certificate status information. The RP can use the certificate to verify the integrity of a digitally signed message, to identify the initiator of a communication, to attest the validity of a device setting or software component, or establish confidential communications with the holder of the certificate. For instance, an NFVi resource can use the device certificate presented by a Support server providing a firmware update and validate the signature of the signed firmware.

4.2.5 Auditors

PKI participants compliance to the CP may be verified by a third party authority.

4.3 Mapping of secure relationships to NFV reference points

The NFV reference architectural framework as defined in ETSI GS NFV 002 [i.2] identifies a number of named reference points and the set of allowed entities that communicate via them. Any of these entities or components may benefit by having a certificate and associated and protected private key to execute cryptographic security functions with other terminating entities.

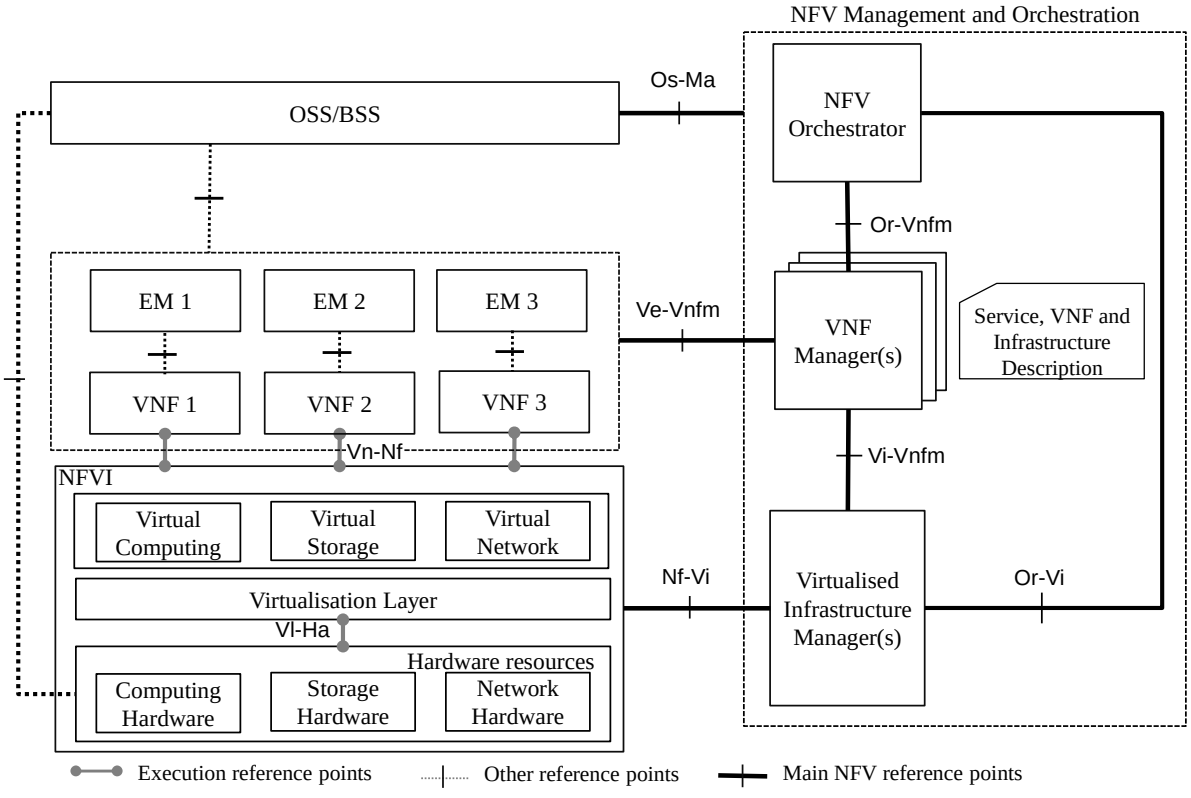

Figure 4.3-1: NFV reference architectural framework

The means by which participants are connected in the PKI is expected to be specified either using online or off-line processes. Furthermore, the Sub-CAs and RAs may exist within the MANO functionality or OSS/BSS environment. Online CA connectivity should be proxied probably via the OSS/BSS. This may facilitate on-line enrolment for certificate issuance in accordance with Enrolment of Secure Transport (EST, IETF RFC 7030 [i.16]) and IETF RFC 8295 [i.21]) or Simplified Certificate Enrollment Protocol (SCEP IETF RFC 8894 [i.20]).

Table 4.3-1: Reference points and Functional Entities they link

Reference point classification	Reference point	PKI applicability	Terminating entities	
Main NFV reference points	**Os-Ma**	**Yes**	**MANO**	**OSS/BSS**
	Ve-Vnfm	Yes	VNF-Manager	EM or VNF
	Nf-Vi	Yes	VIM	NFVI
	Or-Vi	Yes	VIM	NFV Orchestrator
	Vi-Vnfm	Yes	VIM	VNF-Manager
	Or-Vnfm	Yes	VNF-Manager	NFV Orchestrator
Execution refence points	Vi-Ha	NA	Hardware resources	Virtualisation layer
	Vn-Nf	Yes	VNF	NFVI
Other reference points	Not specified	Yes	EM	VNF
	Not specified	Yes	OSS/BSS	EM/VNF
	Not specified	Yes	OSS/BSS	HW resources
NOTE: Vi-Ha is shown here as not applicable simply because it does not appear there is a technical solution (instruction set or other implementation) to allow a VNFI/VNFCI to cryptographically challenge the hardware on which it is being installed. This is a gap as this capability would be useful.				

4.4 Use Cases for the use of certificates in NFV

The benefit to using PKI is the ability to establish security associations between any entity within the domain of the PKI. Security associations are application of security principles to each of the reference points implemented in NFV. The security principles addressable by PKI includes authentication, encryption, and signing. Transport Layer Security (TLS) as specified by IETF RFC 8446 [i.15] provides support for authentication, encryption, and message authentication (signing). File or image signing can also be supported by PKI and may be useful in NFV for distribution of images, packages, and configuration files.

Reference points may be applied between both trusted and untrusted entities. This may apply to multi-tenant or multi-operator environments or to high risk functions within a single-tenant and single-operator environment (such as security monitoring or lawful intercept functions). These use cases and how authentication, encryption, and signing are applied become the primary security association use cases in application of PKI. The criticality of benefit of these capabilities are shown as high, medium, and low in the following tables. The present document is informative, but the intent of the criticality is to indicate the priority of actions: to be mandated (high), to be highly recommended (medium), and to be given careful consideration (low) be done. Also, the use case model here does not imply that PKI and use of PKC are the only way to achieve authentication, encryption, and signing.

Table 4.4-1: PKI trusted use case mapping to NFV reference points

Reference point	Authentication	Encryption	Signing/message authentication
Os-Ma	High	Medium	Low
Ve-Vnfm	High	Medium	Low
Nf-Vi	High	Medium	Low
Or-Vi	Medium	Low	Low
Vi-Vnfm	Medium	Low	Low
Or-Vnfm	Medium	Low	Low
Vi-Ha	NA	NA	NA
Vn-Nf	Medium	NA	NA
EM-VNF (not specified)	High	Medium	Low
OSS/BSS-EM/VNF (not specified)	High	Medium	Low
OSS/BSS-NFVi (not specified)	High	Medium	Low

Table 4.4-2: PKI untrusted use case mapping to NFV reference points

Reference point	Authentication	Encryption	Signing/message authentication
Os-Ma	High	High	Medium
Ve-Vnfm	High	High	Medium
Nf-Vi	High	High	Medium
Or-Vi	High	High	High
Vi-Vnfm	High	High	High
Or-Vnfm	High	High	High
Vi-Ha	NA	NA	NA
Vn-Nf	High	NA	NA
EM-VNF (not specified)	High	Medium	Medium
OSS/BSS-EM/VNF (not specified)	High	Medium	Medium
OSS/BSS-NFVi (not specified)	High	Medium	Medium

While the uses above focus on security associations to support reference points explicitly included on the ETSI NFV reference architecture, any interface connecting to an NFV component can similarly implement authentication, encryption, and signing. Moreover, while authorization in context of role-based or attribute-based access controls are not explicitly treated here, use of PKI credentials rather than traditional user or process identities may provide for greater confidence policy assertions. Moreover, network wide attestation may be similarly possible.

4.5 Considerations for PKC validation

4.5.1 Certificate path building and chain validation

When a PKC is received by an application (e.g. during TLS negotiation), in order for the entity proffering the certificate to be trusted and for the relying party to trust any assertions made in the PKC, the relying party is required to validate the PKC by means of verifying the signature of the certificate with the known public key of the PKC issuer, and verifying the validity of the PKC. Details of steps that should be taken to validate the certificate are outlined in clause 4.5.1.

Any decision to act on the content of a valid PKC is independent of the validity of the PKC, however an invalid PKC should in most circumstances be discarded and any information asserted by the key in the PKC should not be acted on.

A certificate chain (or certificate path) is validated from the end-entity certificate (i.e. the certificate of the entity that the relying party is authenticating or connecting to), through to the root acting as the Trust Anchor of all PKCs in the PKI. The relying party may accept the validity of the end-entity certificate at any stage in the tree, e.g. if any intermediate certificate is considered as "fresh" validation of the chain may be chosen to stop when validation checks reach the first fresh and valid point in the certificate chain.

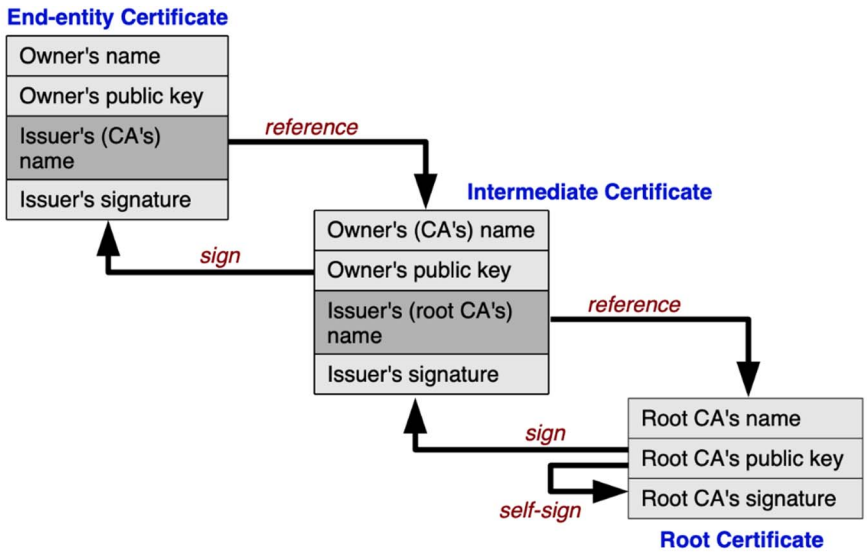

Figure 4.5.1-1: Conventional PKI structure
(from https://upload.wikimedia.org/wikipedia/commons/d/d1/Chain_of_trust.svg)

The following steps provide a guide to implementing certificate path building and validation. At minimum, a relying party needs to make checks consistent with the relying party's Certification Policy which should include the following technical steps (as defined in the Recommendation ITU-T X.509 [i.13]:

a) Check that the signature on the certificate is properly formatted and can be cryptographically verified by using the public key present in the issuer's PKC.

b) Check that the current date and time is within the validity period of the certificate. In particular check that the *notBefore* value is before the time at which the certificate is checked and that the *notAfter* value is after the time at which the certificate is checked.

c) Check that the value of the Issuer field of the certificate matches the value of the Subject field of the issuer's PKC.

d) Check that the *basicConstrains* extension is present in the issuer's PKC and that the value of the CA field is set to *TRUE*. Also, if the *pathLenConstraints* value of the extension is set, check that its value is present and set higher or equal to the current level of the certificate in the chain minus one. For example, in a three-level hierarchy (i.e. End-Entity - level 0, Intermediate CA - level 1, and Root CA - level 2), the value in the Intermediate CA's certificate (if present) should be equal to or greater than 0. For the Root CA's certificate, the value should be greater than or equal to 1. In order to provide flexibility, the *pathLenConstraints* is usually not present in Root CA's certificates.

e) Check for the presence of *authorityKeyIdentifier* extension. If present, and the *keyIdentifier* field is set, check that its value matches the *subjectKeyIdentifier* extension's value in the next certificate in the chain (if present). The values in these extensions are usually calculated by using the Method 1 as described in IETF RFC 5280 [i.17].

f) Check that the *keyUsage* extension in the next certificate in the chain supports certificate signing (i.e. the *keyCertSign* bit is set).

The PKIs may add attribute certificates to the PKC contents. The relying party may be required, in that case, to check for the presence of specific Object Identifiers (OID) in the *certificatePolicies* extension. Relying parties with specific policy requirements (such as subscribers' authentication servers or UE identifiers) should have a list of acceptable policy identifiers that should be used to verify the identifiers present in the certificates. In that case, the relying party should process the extension as follows:

a) Check that the *certificatePolicies* extension is present in the certificate. The value of this extension is a set of *certificatePolicy* values that should be check against the values set in the CP (if present). In particular, for each of the values, the relying party should check that:

   - The required values of the *certPolicyId* field are present. For example, if the CP mandates for a specific value (*1.3.6.1.4.1.XXXX.YYY.ZZZ*) to be present in EE or Sub-CA certificates, the relying party should retrieve the content of the *certPolicyId* field of the *certificatePolicy* and check it against the required value.

   - Although the use of *policyQualifiers* is discouraged as it might introduce interoperability issues, if the *policyQualifiers* field in the *certificatePolicy* extension is set, then the relying party should process the values according to their types as described in IETF RFC 5280 [i.17]. The detailed processing of these values is out of the scope of the present document.

To continue the chain building process, the relying party should repeat the steps above until one trusted certificate is reached.

5 Use cases for the use of certificates in NFV

5.1 VNF certificate use case

5.1.0 Introduction to use cases

VNFs are implemented with one or more VNFCs, which are internal component of a VNF providing a defined sub-set of that VNF's functionality, with the main characteristic that a single instance of this component (i.e. VNFCI) maps 1:1 against a single Virtualisation Container. A VNF instance composed of various VNFCIs could have multiple logical identities, each of which is represented by a certificate, to communicate with different peers. In all of the use cases below, there is a pre-condition that a pre-established relationship exists between the communicating peers and the CA/RA respectively. It is anticipated that multiple CA/RAs will be used for different parts of the NFVI and different Network Services. Some will be private to the infrastructure or tenant and others may use external public CA/RA for example VNF transport connections between Network Operators.

5.1.1 Use case #1: VNF management connection

A VNF instance should be configured and managed by both VNFM and EM, while it needs to be identified in order to be managed and configured. With the precondition that the VNFCI does not have a pre-established relationship with either the VNFM or EM, in order to ensure the security of this management path, a secure connection between a VNFCI and its corresponding VNFM or EM requires a VNFCI to have one or more certificates provisioned to attest its identity to the VNFM or EM to establish a secure connection between them.

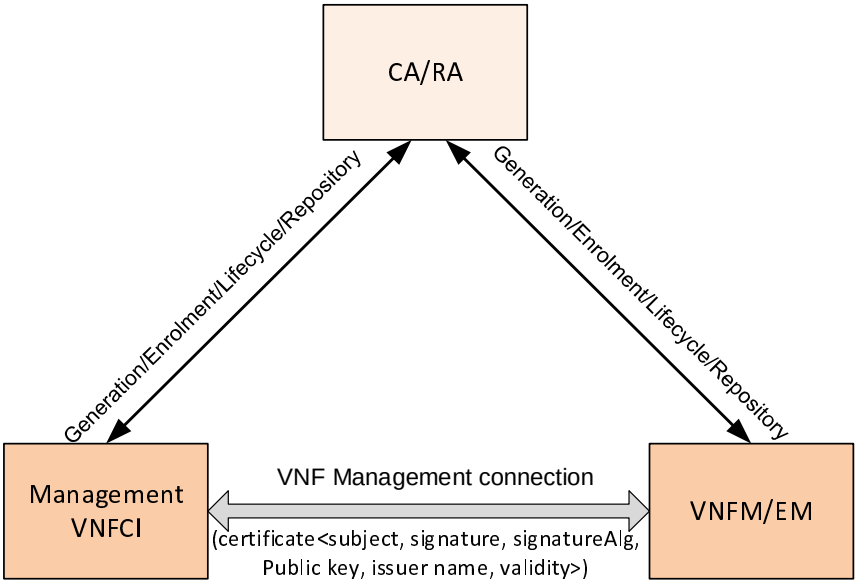

Figure 5.1.1-1: Use case#1 VNFCI management connection

Actors: VNFCI, VNFM/EM, CA/RA.

In this use case, VNFCI and VNFM or EM are validated by CA/RA and get the certificate(s) issued by CA/RA respectively. VNFCI sends its certificate to VNFM or EM, in which the attributes such as <subject, signature, signatureAlg, public key, issuer name, validity, etc.> are included. And VNFM/EM can verify VNFCI's identity via the certificate. And vice versa, VNFCI can validate VNFM/EM's identity in a similar fashion.

5.1.2 Use case #2: VNF transport connection

The VNFCI has the requirement to communicate with other entities, including other VNFCIs, PNFs, etc. With the precondition that the VNFCI does not have a pre-established relationship with either the VNFM or EM, a secure connection (e.g. IPsec) between the VNFCI and the peer or a SeGW requires a VNFCI to have one or more certificates provisioned to attest its identity to the communication peers or SeGWs to establish secure connections between them.

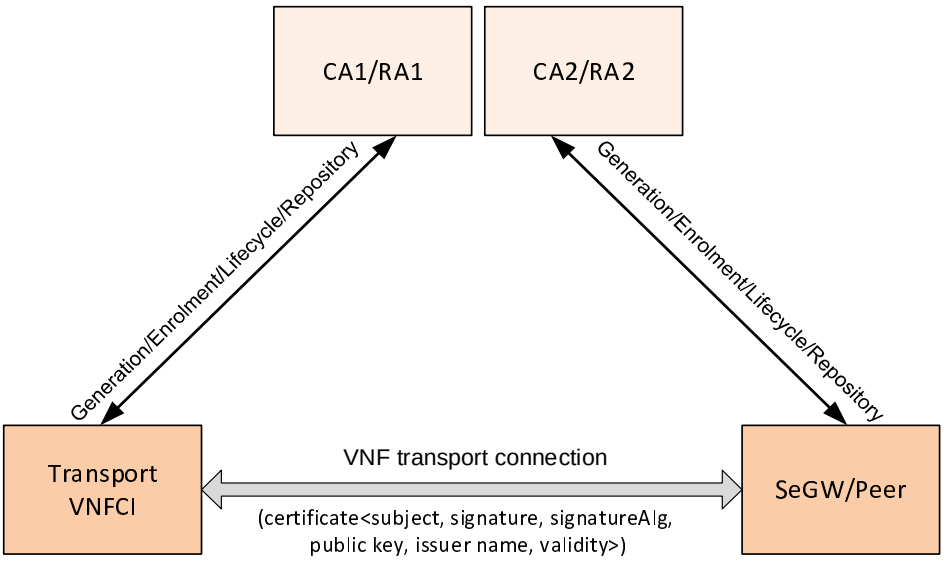

Figure 5.1.2-1: Use case#2 VNFCI transport connection

Actors: VNFCI, CA1/RA1, SeGW/Peer, CA2/RA2.

In this use case, VNFCI is validated and gets the certificate(s) issued by CA1/RA1, and SeGW/Peer gets the certificate(s) issued by CA2/RA2. CA1/RA1 and CA2/RA2 may be the same in some situations. VNFC sends its certificate to SeGW/Peer, in which the attributes such as <subject, signature, signatureAlg, public key, issuer name, validity, etc.> are included. And SeGW/Peer can verify VNFCI's identity via the certificate. And vice versa, VNFCI can validate SeGW/Peer's identity in a similar fashion.

5.2 MANO certificate use case

As entities with longer lifetime, MANO functional blocks (including NFVO, VNFM and VIM) need to communicate with each other, as well as with OSS/BSS, VNF, EM or NFVI. A secure connection (e.g. TLS) between the MANO and the peer requires a MANO functional block to have one or more certificates provisioned to attest its identity to the communication peer to establish a secure connection between them.

5.3 OSS/BSS/EM certificate use case

As traditional functional blocks, OSS/BSS need to communicate with EM and NFVO respectively, and OSS/BSS need to communicate with OSS/BSS, VNF and VNFM respectively. A secure connection (e.g. TLS) between these traditional functional blocks and the peer requires OSS/BSS or EM to have one or more certificates provisioned to attest its identity to the communication peer to establish a secure connection between them.

6 Analysis

6.1 General

In order to eliminate or mitigate risks against attacks such as spoofing, tampering and information disclosure, secure connection can be established on all the interfaces introduced by NFV scenario. IPsec and TLS mechanisms are widely deployed to protect the communication between two entities using certificates.

In NFV scenario, the functional blocks to be issued certificates include:

NFV-MANO functional blocks and VNFCI

The NFV-MANO functional blocks and VNFCI should employ certificates which can be used in order to establish secure connections between them.

Other functional blocks

OSS/BSS employs certificates in order to establish secure management connections with NFVO.

EM employs certificates in order to establish secure management connections with VNF or VNFM.

NFVI (i.e. the control & admin agents in NFVI), employs certificate(s) in order to establish secure connections with VIM.

6.2 Deployment scenarios

It is stated in NFV Requirements (ETSI GS NFV 004 [i.4]) that the NFV framework (ETSI GS NFV 002 [i.2]) is expected to implement appropriate security countermeasures to address protection of data transmitted via shared network resources and protection of new interfaces exposed by the interconnectivity among NFV architectural components (e.g. hardware resource, VNFs and management systems). In order to realize the authentication, data confidentiality and integrity protection, some cryptographic security algorithms may be employed.

Clause 5.1 of the ETSI GS NFV-SEC 001 [i.8] describes seven deployment scenarios:

- Monolithic Operator.
- Network Operator Hosting Virtual Network Operators.

- Hosted Network Operator.
- Hosted Communications Providers.
- Hosted Communications and Application Providers.
- Managed Network Service on Customer Premises.
- Managed Network Service on Customer Equipment.

Multi-tenant is a key factor in several of these scenarios. Because different providers and operators create different administrative domains, while each certificate applies to a specific security domain, multi-tenant scenarios need to be considered for certificate deployment.

It is possible to differentiate two identified administrative domains as defined in ETSI GS NFV-MAN 001 [i.5] for deployment scenarios, although additional administrative domains may exist. The two domains are by default separate PKIs:

- **Infrastructure Domain:** The Infrastructure Domain provides virtualised infrastructure resources such as computing, networking and storage or a composition of those resources via a service abstraction to a Tenant Domain, and is responsible for the management and orchestration of those resources.
- **Tenant Domain:** The Tenant Domain provides VNFs, and combinations of VNFs into Network Services, and is responsible for their management and orchestration, including their functional configuration and maintenance at application level.

By applying this two administrative domains approach to the seven NFV deployment scenarios in ETSI GS NFV-SEC 001 [i.8] using the NFV reference architectural framework as defined in ETSI GS NFV 002 [i.2], it is possible to envision associated certificate management scenarios.

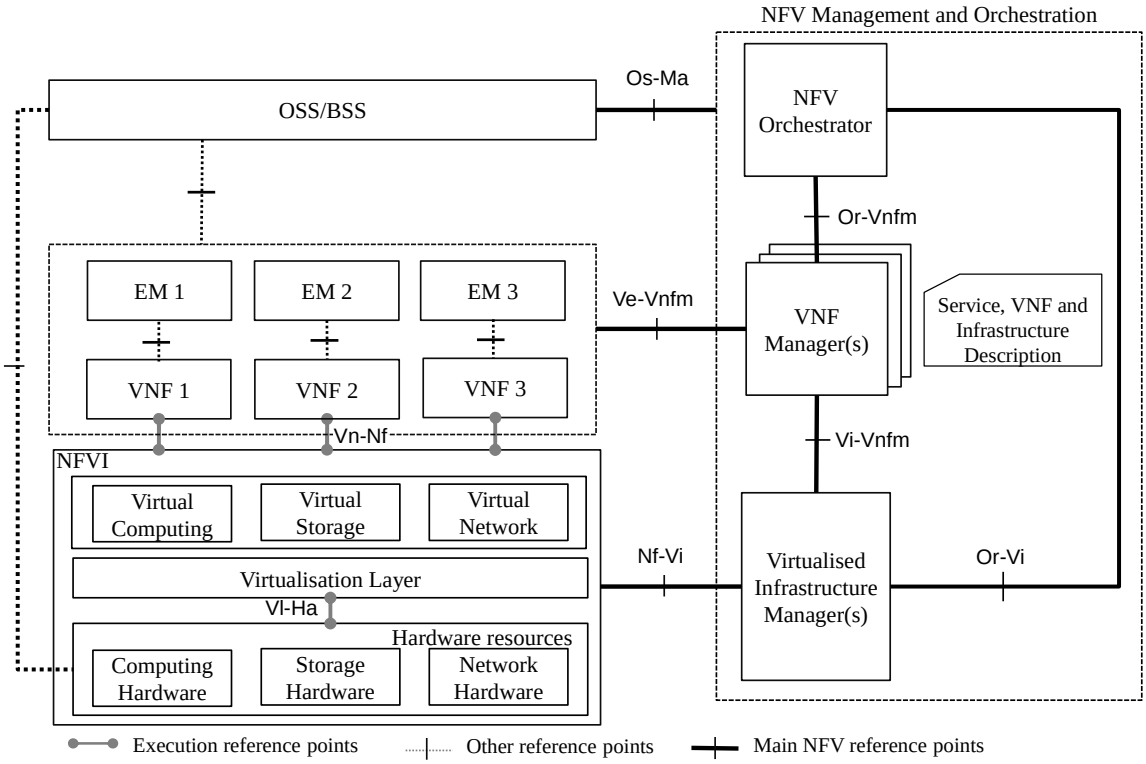

Figure 6.2-1: NFV reference architectural framework (ETSI GS NFV 002 [i.2])

Monolithic Operator

The same organization that operates the virtualised network functions deploys and controls the hardware and hypervisors they run on and physically secures the premises in which they are located.

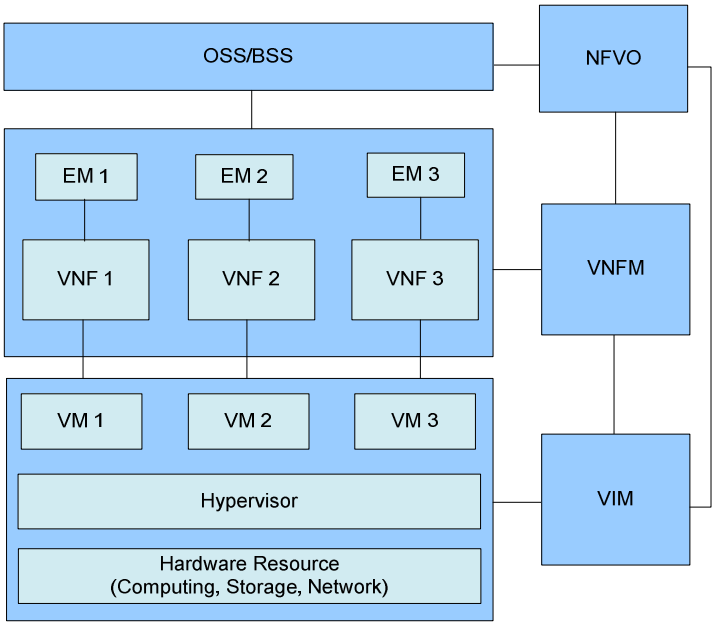

Figure 6.2-2: Deployment scenario 1

In this scenario, the entire NFV network is operated by one operator. This is the simplest deployment scenario. Since there is only one administrative domain, all the needed certificates can be issued by the CA of the network operator domain.

Network Operator Hosting Virtual Network Operators

The network operator hosts VNFs for itself and other virtual network operators, within the same facility.

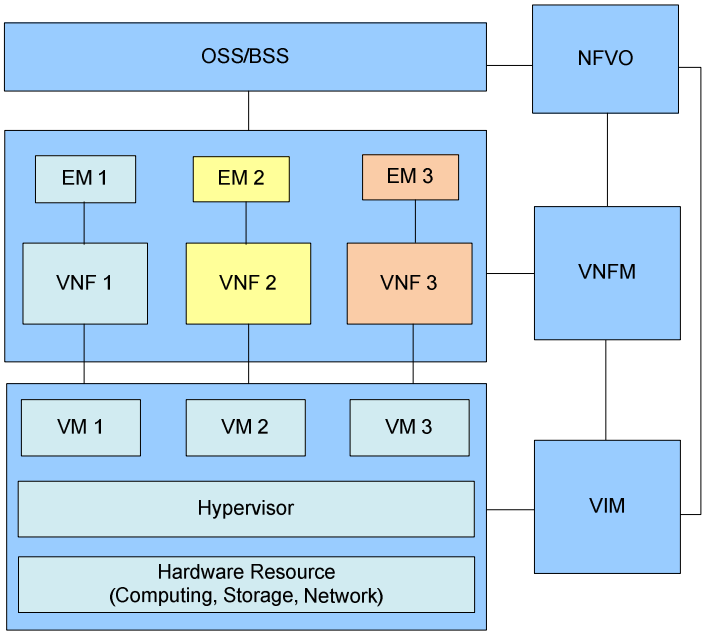

Figure 6.2-3: Deployment scenario 2

In this scenario, since VNF 1, VNF 2 and VNF 3 belong to different network operators respectively, the certificates issued to VNF 1, VNF 2 and VNF 3 should reside in different administrative domains.

Hosted Network Operator

An IT services organization operates the computer hardware, infrastructure network and hypervisors on which a separate network operator runs virtualised network functions.

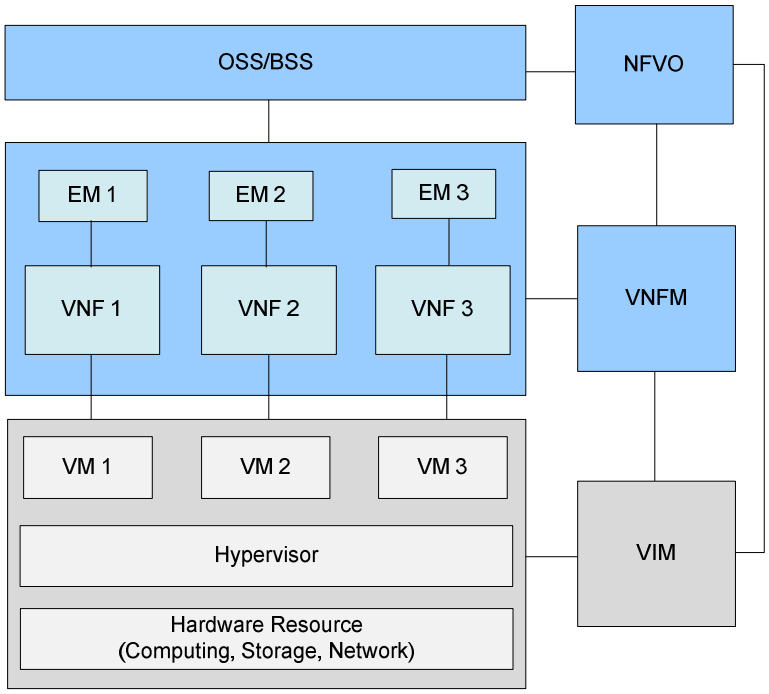

Figure 6.2-4: Deployment scenario 3

In this scenario, since the infrastructure and the above VNFs are provided and operated by different providers/operators, the certificates issued to the entities in Infrastructure Domain and Tenant Domain may reside in different administrative domains.

Hosted Communications Providers

This scenario is similar to the Hosted Network Operator scenario, except the IT services organization hosts multiple communications providers.

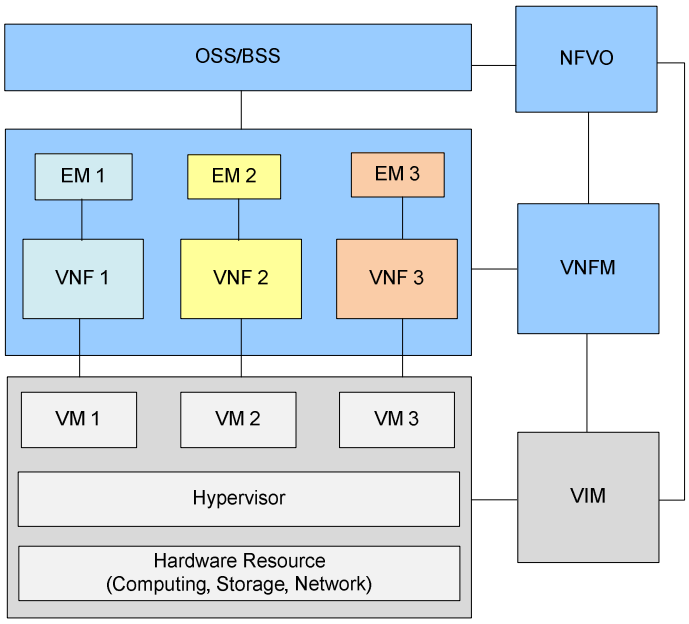

Figure 6.2-5: Deployment scenario 4

In this scenario, because infrastructure, VNF 1, VNF 2 and VNF 3 belong to different providers/operators respectively, the certificates issued to the entities in Infrastructure Domain and Tenant Domain may reside in different administrative domains.

Hosted Communications and Application Providers

This scenario is similar to the Hosted Communications Providers scenario, except servers in a data centre facility are offered to the public for deploying virtualised applications. Similarly, the certificates issued to the entities in Infrastructure Domain and Tenant Domain may reside in different administrative domains.

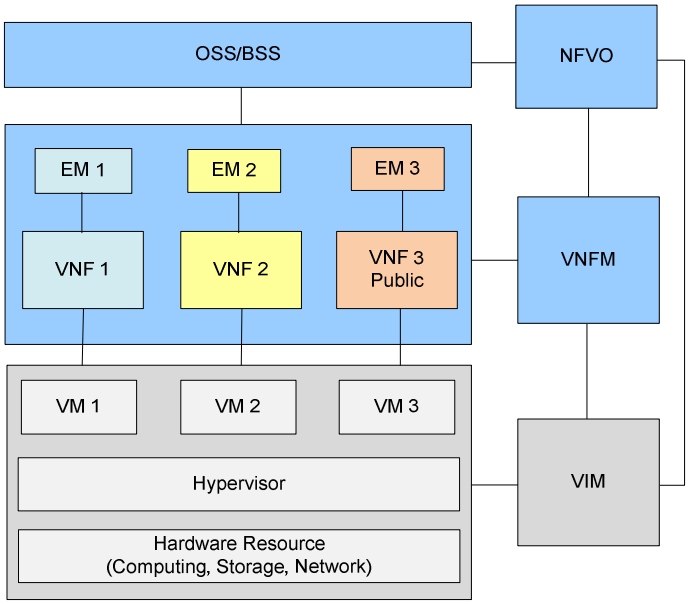

Figure 6.2-6: Deployment scenario 5

Managed Network Service on Customer Premises

In this scenario, a network operator runs virtualised network functions on its own generic server hardware located on a customer's premises and physically secured by the customer, normally under a contractual agreement between the network operator and the customer.

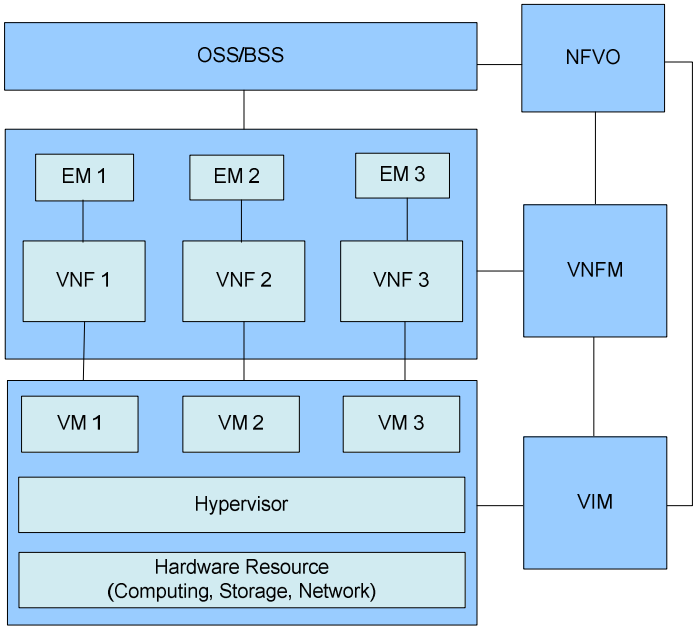

Figure 6.2-7: Deployment scenario 6

Because there is no impact on certificate deployment if the building belongs to network operator or customer, the certificate issuance is the same as that of a Monolithic Operator, i.e. all the needed certificates can be issued by the CA of the network operator domain.

Managed Network Service on Customer Equipment

This scenario is similar to the Managed Network Service on Customer Premises scenario, except the computer hardware is supplied and operated by the customer rather than the network operator.

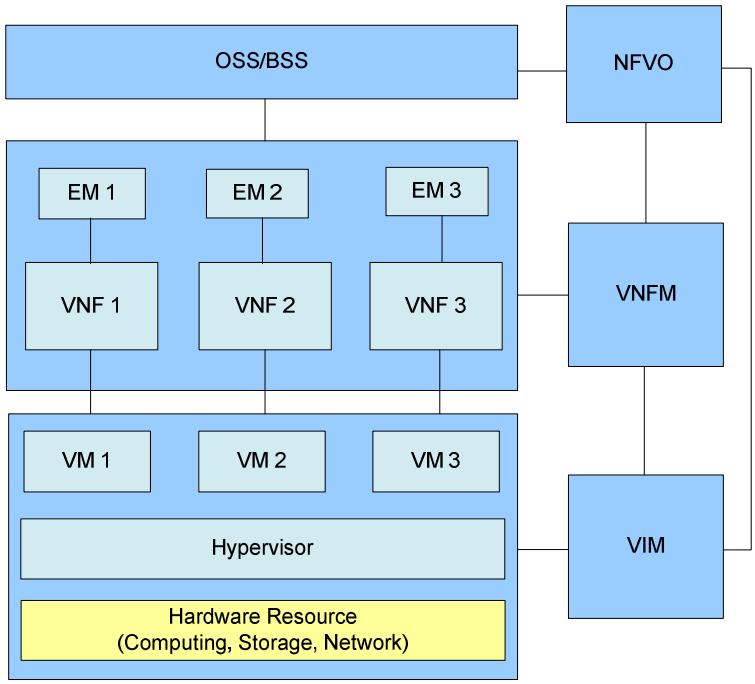

Figure 6.2-8: Deployment scenario 7

There may be a requirement to configure certificates for Lights-out Management (i.e. deploying a form of out-of-band management often using a dedicated management channel to allow monitoring and management of network-attached equipment regardless of whether the machine is powered on, or whether an operating system is installed or functional), which will be within the hardware management domain which is out of scope of the present document. The certificate issuance is similar to a Hosted Network Operator, i.e. the certificates issued to the hardware management domain and the entities in the Infrastructure and Tenant Domains may reside in different administrative domains.

7 Certificate management framework

7.1 Certificate hierarchy

Considering that the certificates may be deployed at two or more layers, however, the introduction of NFV brings new certificate deployment and management issues. A multi-layered certificate mechanism is desirable for NFV framework. The vertical layers that certificates need to be deployed could be as follows.

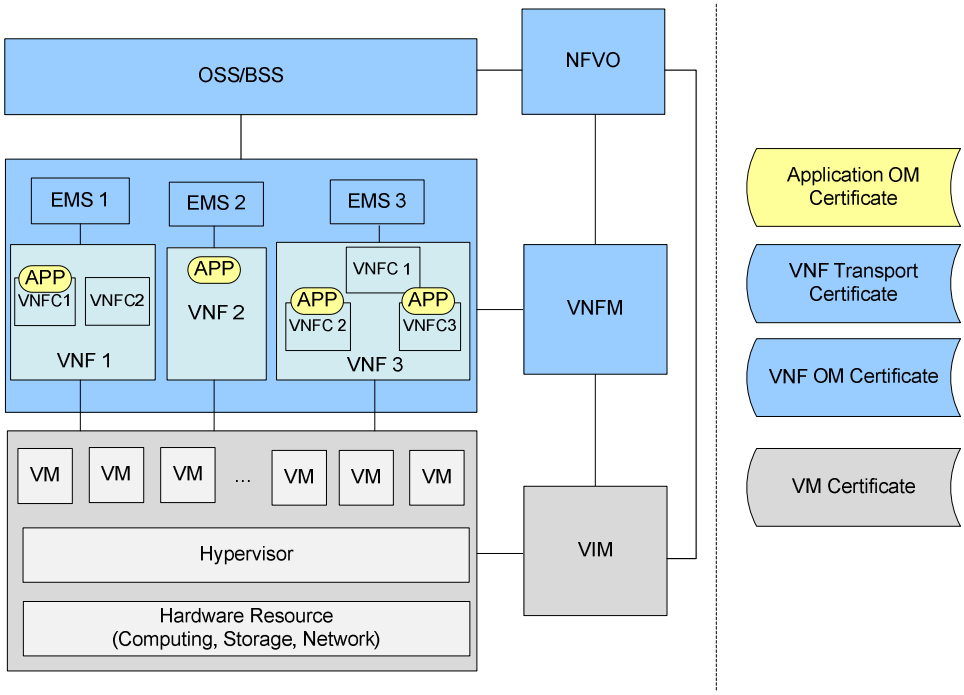

Figure 7.1-1: NFV hierarchy

- **Applications Environment Layer:** It provides orchestration and management functionality to application software or even 3rd party software installed on VNFs. It supports a flexible and efficient multi-tenancy run-time and hosting environment for Applications by providing both VNFaaS and VNPaaS facilities, allowing 3rd Party Application develops different degrees of control over processing power, memory, storage or operating system support. At this layer, each VNF can be configured with OM certificate(s) in order to manage the software installed on VNFs.

- **Execution Environment Platform Layer:** It provides the basic VNF functionalities. At this layer, each VNF can be configured with certificate(s) corresponding to the Tenant domain as defined by MANO.

- **Infrastructure Platform Layer:** It provides the hardware resources for the platform (e.g. CPU, memory, storage, acceleration devices, input/output devices, etc.) together with the supporting operating system and virtualisation (hypervisor) software. At this layer, each VM can be configured with certificate(s) corresponding to the Infrastructure domain as defined by MANO.

Meanwhile, the horizontal layers could be defined between a variety of functionalities within the same layer, e.g. between VM and VIM, between VNF and VNFM, and between two VNFs hosted by the same or different operators.

At all these layers, each layer has a corresponding peer for function management, and each function at one layer may have a peer to communicate with. Certificates are needed to perform authentication to all the management protocols and peer-to-peer telecommunication protocols.

In the NFV multi-layered environment, the certificates need to be deployed at multiple layers, so it is quite complicated to consider where and how to deploy the certificates, and how to manage all the certificates deployed in different layers and different functionalities. The certificate management also needs to be embedded to the service procedures and make the trust relationship configurable and can be passed on reliably.

7.2 Certificate category

The above layering approach gives rise to corresponding certificate categories:

- **Application OM certificates:** It is used to establish management connection in order to perform management operations on VNFCIs.

- **VNFCI certificates:** It includes two types of certificates as below:
  - **VNFCI transport certificates:** It is configured to each VNFC instance which has the external communication requirement. It is used to establish secure connection with other peer entities (e.g. VNFCIs).
  - **VNF OM certificates:** It is used to establish management connection between VNFCI and VNF management entities (e.g. VNFM and EMS) in order to perform management operations to VNFCIs.
- **VM certificates:** It is configured to each VM in Infrastructure domain. It is used to establish management connection with VIM to perform management operations to VM.

Considering secure communication requirement on the new interfaces exposed by the interconnectivity among management systems, the MANO entities should also be configured with certificates to establish secure connection with the peer entities:

- **MANO certificates:** Each MANO entity will have a certificate which is used to establish management connection with VM or VNF hosted on the VM. Moreover, secure connection can also be established between MANO entities in order to ensure secure communication.

Some other management entities such as EMS also need to be configured with certificates in order to establish secure management links with VNFs. Because they are not new entities introduced by NFV scenario, no special description is needed to address this in the present document.

Due to the virtualisation, the introduction of NFV has a great impact on the deployment of VM certificate at Infrastructure Platform Layer and VNF certificate at Execution Environment Platform Layer. Compared to the traditional physical devices, the virtualisation makes VM and VNF creation much more dynamic. Therefore, the present document aims to address the basic certificate management issues at Infrastructure Platform Layer and Execution Environment Platform Layer when a VNF is instantiated initially.

8 NFV certificate lifecycle management

8.1 Certificate generation

8.1.1 Initial Credential

8.1.1.1 Key pair generation

8.1.1.1.1 Option 1: NFVI generates key pair

This option uses a key pair generation mechanism implemented by NFVI to generate the key pair. For this option, the VNFI acquires the key pair from the injection of the NFVI. Therefore, the MANO (NFVO & VNFM & VIM) does not know VNFI's private key. This key pair generation procedure is depicted in figure 8.1.1.1.1-1.

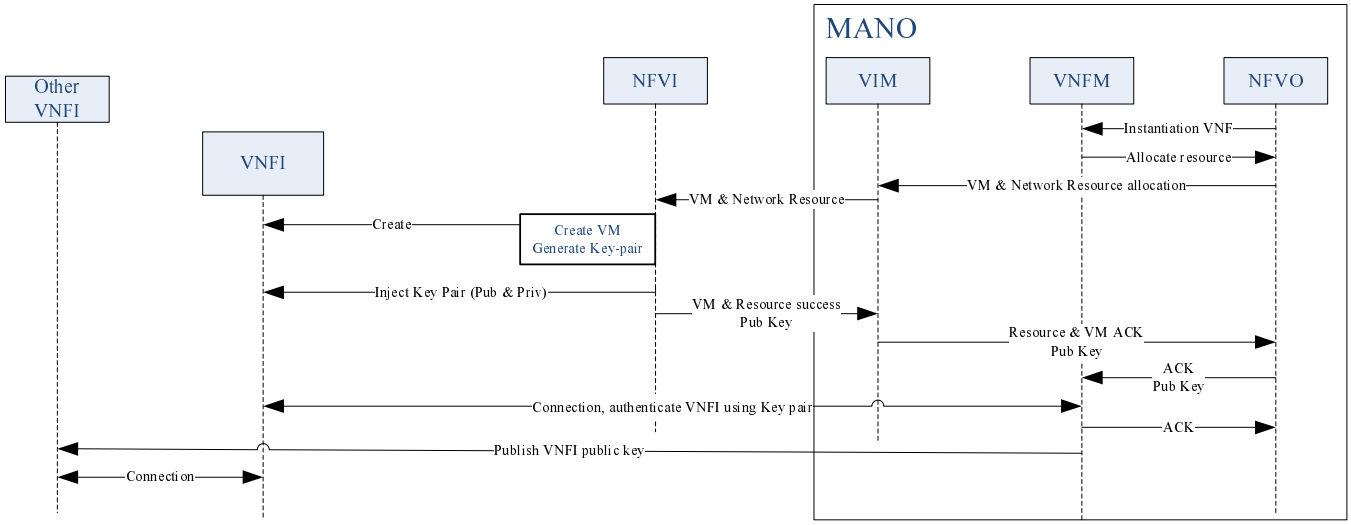

Figure 8.1.1.1.1-1: NFVI generate key pair procedure

1) NFVO calls VNFM to instantiate the VNF.
2) VNFM calls the NFVO for resource allocation.
3) NFVO requests allocation of resources to the VIM (VMs and network resources).
4) VIM forwards the resources allocation requests to NFVI.
5) NFVI generates the key pair and inject the key pair into the secure storage of the created VNFI (securely deleting the private key from its own storage). Meanwhile, NFVI confirms the successful instantiation VNFI back to the VIM, providing the VNF-ID and the public key as well.
6) VIM forwards the resources allocation response back to NFVO along with the public key.
7) NFVO acknowledges the completion of the resource allocation back to VNFM along with the public key.
8) VNFM establish trust relationship with the VNFI and configures the VNFI. Then VNFM acknowledges the completion of the VNFI instantiation back to the NFVO.
9) VNFM publishes the public key provided by NFVI.
10) Finally, the other network elements can establish trust relationship with the VNFI.

As the private key is only known to NFVI and the VNFI, the risk of the private key exposure is reduced.

8.1.1.1.2 Option 2: HMEE generates key pair

This option uses a key pair generation mechanism implemented by HMEE to generate the key pair. For this option, HMEE is a secure part of the VNFI. NFVI cannot access the authentication function or read HMEE data. This key pair generation procedure is depicted in figure 8.1.1.1.2-1.

NOTE 1: A Hardware-Mediated Execution Enclave (HMEE) is defined as an area of process space and memory within a system environment within a computer host which delivers confidentiality and integrity of instructions and data associated with that enclave. See ETSI GS NFV-SEC 009 [i.10], clause 6.16.

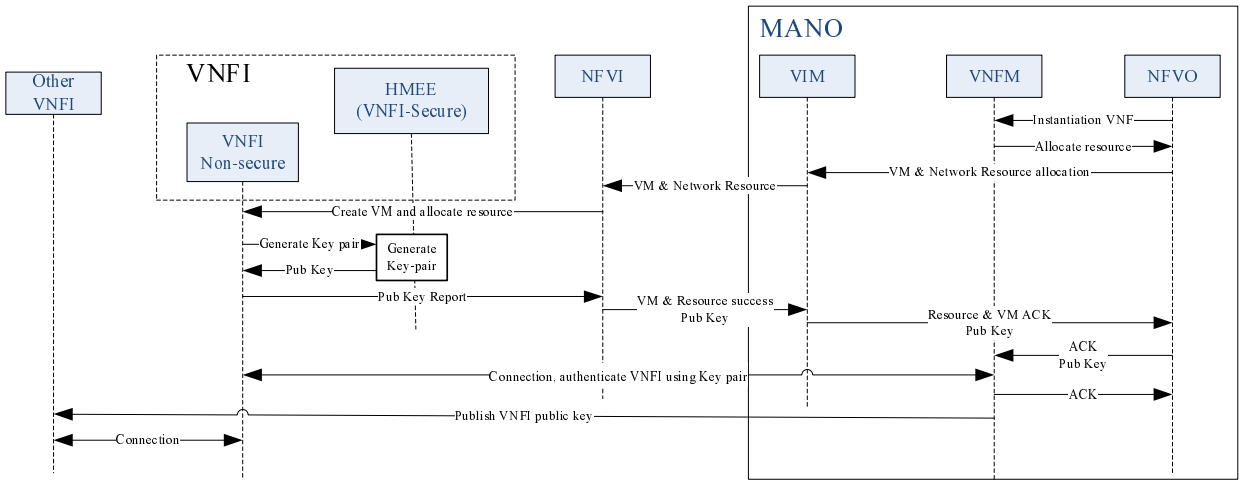

Figure 8.1.1.1.2-1: HMEE generate key pair procedure1

1) NFVO calls VNFM to instantiate the VNF.

2) VNFM calls the NFVO for resource allocation.

3) NFVO requests allocation of resources to the VIM (VMs and network resources).

4) VIM forwards the resources allocation requests to NFVI.

5) NFVI creates the VNFI with a HMEE protecting the sensitive part of the VNFI.

NOTE 2: The precise details of the creation and communication with the HMEE is outside the scope of the present document.

6) VNFI sends the key pair generation request message to HMEE.

7) The HMEE generates the key pair and reports the public key back to VNFI.

8) VNFI informs NFVI of the public key provided by HMEE.

9) NFVI confirms the successful initialization VNFI back to the VIM, providing the VNF-ID and the public key as well.

10) VIM forwards the resources allocation response back to NFVO along with the public key.

11) NFVO acknowledges the completion of the resource allocation back to VNFM along with the public key.

12) VNFM establish trust relationship with the VNFI and configures the VNFI. Then VNFM acknowledges the completion of the VNFI instantiation back to the NFVO.

13) VNFM publishes the public key provided by VNFI.

14) Finally, the other network elements can establish trust relationship with the VNFI.

As the private key is stored in the trust environment during the whole lifecycle, the risk of private key exposure does not exist.

8.1.1.1.3 Option 3: HSM generates key pair

This option uses a key pair generation mechanism implemented by HSM to generate the key pair created using an ETSI GS NVF-SEC 012 [i.11] compliant random number generator. The HSM is linked to the HMEE where the VNFI is implemented through a secure channel established after a mutual authentication process. For this mutual authentication process, the public key of the HSM is expected to be loaded in the HMEE and the hardware (e.g. CPU) root certificate from which the HMEE certificate is generated is expected to be loaded in the HSM. How the public key of the HSM is introduced in the HMEE, and how the hardware root certificate is introduced in the HSM is out of scope of the present document.

NOTE 1: Hardware Secure Module (HSM) is defined in ETSI GS NFV-SEC 009 [i.10], clause 6.20.

NOTE 2: In the procedure described below, the VNFI contains a single component and is equivalent to a VNFCI.

The key pair generation procedure is depicted in figure 8.1.1.1.3-1.

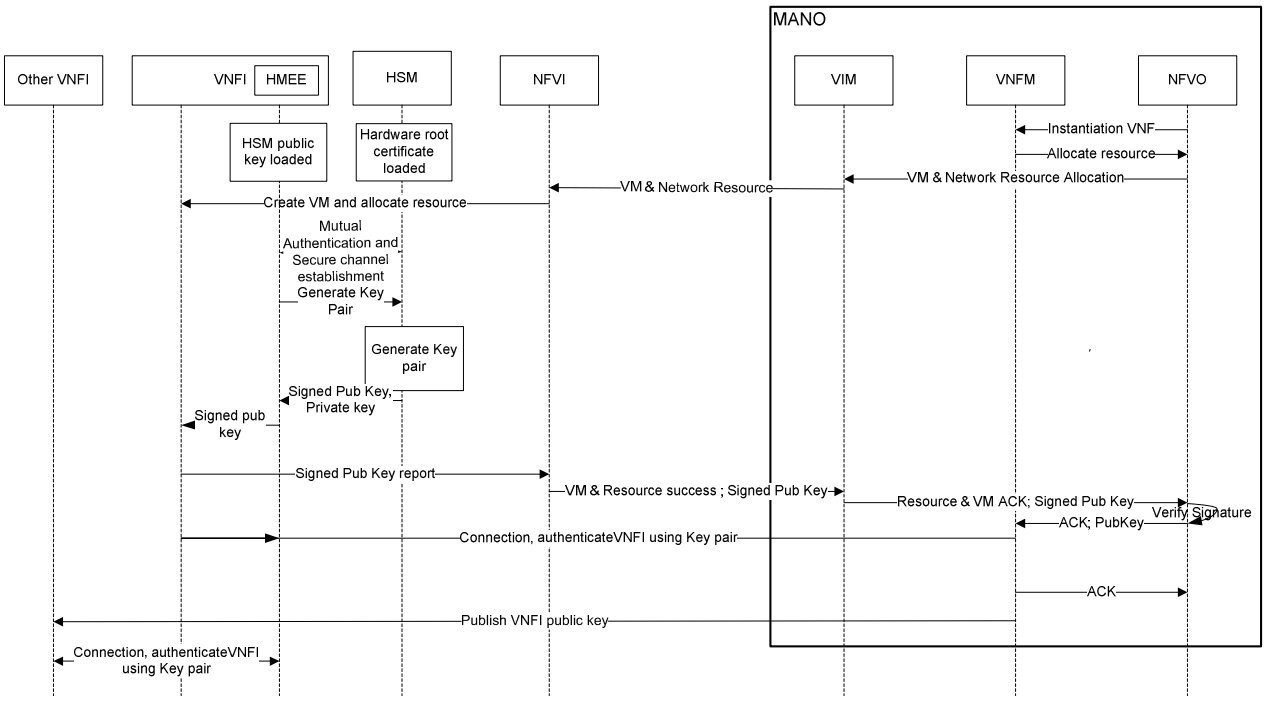

Figure 8.1.1.1.3-1: HSM generate key pair procedure

1) The public key of the HSM is introduced in the HMEE and the hardware root certificate is introduced in the HSM.

2) NFVO calls VNFM to instantiate the VNF.

3) VNFM calls the NFVO for resource allocation.

4) NFVO requests allocation of resources to the VIM (VMs and network resources).

5) VIM forwards the resources allocation requests to NFVI.

6) NFVI created the VNFI with a HMEE.

7) Mutual Authentication process between the HMEE and the HSM is done and a secure channel is established between HSM and HMEE.

8) VNFI through the HMEE sends the key pair generation request message to HSM.

9) The HSM generates the key pair and reports the signed public key and private key back to the HMEE. The public key is signed with the HSM key and the certificate may contain some other information (as the hash, version, etc.) of the VNFI.

10) VNFI informs NFVI of the signed public key provided by HSM.

11) NFVI confirms the successful initialization VNFI back to the VIM, providing the VNF-ID and the signed public key as well.

12) VIM forwards the resources allocation response back to NFVO along with the signed public key of the VNFI.

13) NFVO verifies the certificate of the signed public key and acknowledges the completion of the resource allocation back to VNFM along with the public key. The signature gives assurance to the NFVO on the key pair quality generated by a reliable source and information in the certificate assurance on version, integrity of the code of VNFI and the implementation of the VNFI in a HMEE.

14) VNFM establish trust relationship with the VNFI and configures the VNFI. Then VNFM acknowledges the completion of the VNFI instantiation back to the NFVO.

15) VNFM publishes the public key provided by VNFI.

16) Finally, the other network elements can establish trust relationship with the VNFI.

As the private key is stored in the trust environment during the whole lifecycle, the risk of private key exposure does not exist.

8.1.2 VNFCI Certificate

8.1.2.0 Introduction to VNFCI certificate issuance

A VNFCI certificate is issued by operator CA after a VNFCI is successfully instantiated. It is requested by the VNFCI that takes the initial credential as proof to an Operator CA. Automated Certificate Management can be performed using a number of well defined protocols, such as CMPv2 [i.18], SCEP [i.20] and EST [i.16]. In the following certificate enrolment procedure EST will be used.

The certificate configured to VNF should be aimed at VNFCI which has the communication requirement with external entities. Some options are listed for the formal certificate issuance as shown below.

All the following EST certificate enrolment procedures are in line with the specification of IETF RFC 7030 [i.16].

8.1.2.1 Option 1: VNFCI generates key pair, constructs and signs certificate request

This option uses a certificate enrolment mechanism implemented directly by VNFCI itself to request a certificate from Operator CA.

For this option, the VNFCI generates a public-private key pair, constructs and signs the certificate request message. VNFCI needs to use the initial credential to request formal certificate issued by Operator CA according to the certificate enrolment procedure. Operator CA verifies the VNFC's identity using the initial credential.

It is assumed that all CA certificates that are not explicitly required have been removed from the VNF image. The operator root CA certificate could be added to the VNF package during onboarding, or transferred to the VNFCI either during instantiation or in the previousinitial credential procedure. As defined by ETSI TS 133 310 [i.19], the protection of the operator root CA certificate during provisioning may be based on operator security policy. If an operator root CA certificate provisioned prior to the EST protocol run is available the VNFCI uses it. If no operator root CA certificate is provisioned at all then the VNFCI cannot continue with the certificate enrolment procedure.

This EST enrolment procedure is depicted in figure 8.1.2.1-1.

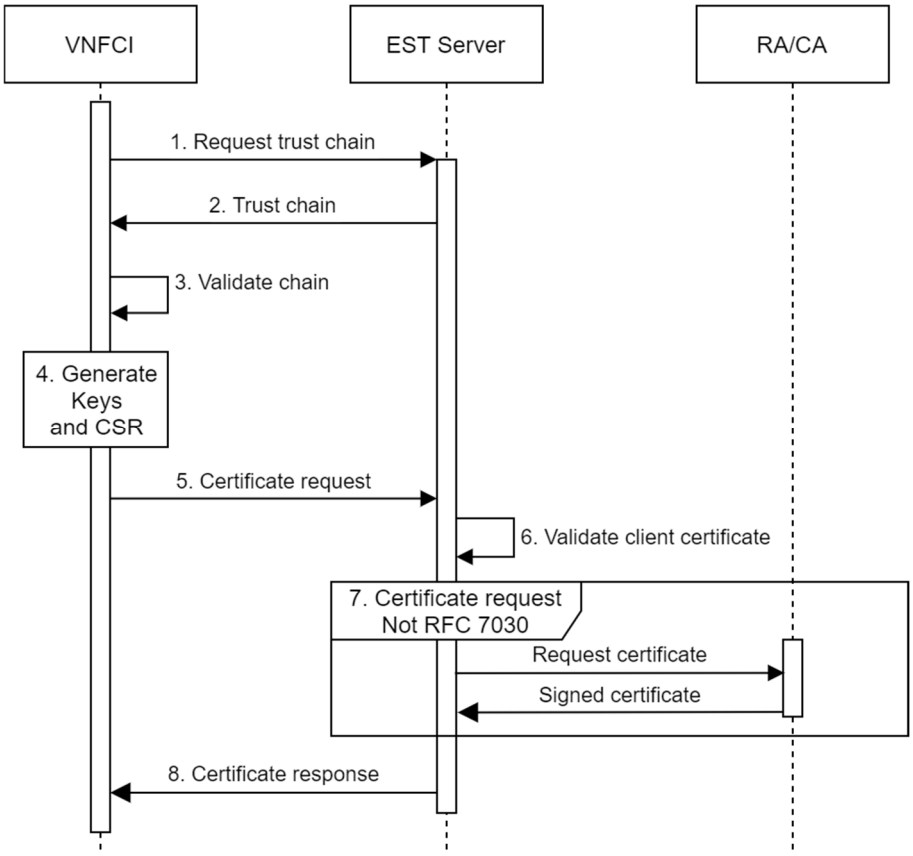

Figure 8.1.2.1-1: Direct VNFCI certificate enrolment procedure

1) After the successful instantiation, by the indication of certificate installed during instantiation, the VNFCI initiates a TLS connection to the Operator Certificate Enrolment Server and requests the trust chain (all intermediate and root CA certificates). The VNFCI verifies the Operator certificate against the Operator root CA certificate and abandons the connection if they do not verify.

2) The Operator Certificate Enrolment Server returns the trust chain containing all of the Operator RA/CA certificates.

3) The VNFCI verifies the trust chain against the Operator root CA certificate and abandons the certificate request if they do not verify.

4) The VNFCI generates a public-private key pair and constructs the Certificate Signing Request to be certified by the Operator RA/CA.

5) The VNFCI sends the Certificate Signing Request message to Operator Certificate Enrolement Server to request a certificate. The initial credential is used as the client certificate to authenticate the message to the Operator Certificate Enrolement Server.

6) Operator Certificate Enrolement Server verifies the connection based on the initial credential. If the verification is successful, it requests the certificate from the Operator RA/CA.

7) Operator Certificate Enrolment Server requests the certificate be signed by the Operator RA/CA. The Operator RA/CA responds to the enrolment request, providing the new certificate.

8) The Operator Certificate Enrolment Server then returns the signed certificate to the VNFCI, verifies the received message, and if successful, installs the received certificate.

Additional policy could be applied to enhance the security, such as invalidating the initial credential once VNFCI installs a formal certificate successfully.

NOTE: This initial credential can be used for all VNFCIs, or just for a Master VNFCI (e.g. first VNFCI established during the instantiation procedure) which can be a longer-lived entity compared to other VNFCs in a VNF.

8.1.2.2 Option 2: VNFCI generates key pair, constructs certificate request, and VNFM signs certificate request

This option uses a certificate enrolment agent mechanism to leverage a VNFC instance to obtain its certificate issued by Operator CA with the help of VNFM that acts as an agent of the VNFCI.

For this option, the VNFCI generates public-private key pair, and constructs the public key certificate request message. VNFCI sends the certificate request message to the VNFM, using the initial credential to request a formal certificate issued by Operator CA. VNFM authenticates the message based on the initial credential, then acts as an agent to request a formal certificate The VNFM uses its certificate to authenticate with the Operator Certificate Enrolment Server to request the certificate be signed. The Operator Certificate Enrolment Server request the certificate from the Operator CA according to the certificate enrolment procedure. Operator CA issues VNFCI the formal certificate and sends it to VNFCI via the Operator Certificate Enrolment Server and VNFM.

It is assumed that all unnecessary CA certificates have been removed from the VNF image. The operator root CA certificate could be added to the VNF package during onboarding, or transferred to VNFCI either during instantiation or in the previous initial credential procedure. As defined by ETSI TS 133 310 [i.19], the protection of the operator root CA certificate during provisioning may be based on operator security policy. If an operator root CA certificate provisioned prior to the EST protocol run is available the VNFCI uses it. If no operator root CA certificate is provisioned at all then the VNFCI cannot continue with the certificate enrolment procedure.

This enrolment procedure is depicted in figure 8.1.2.2-1.

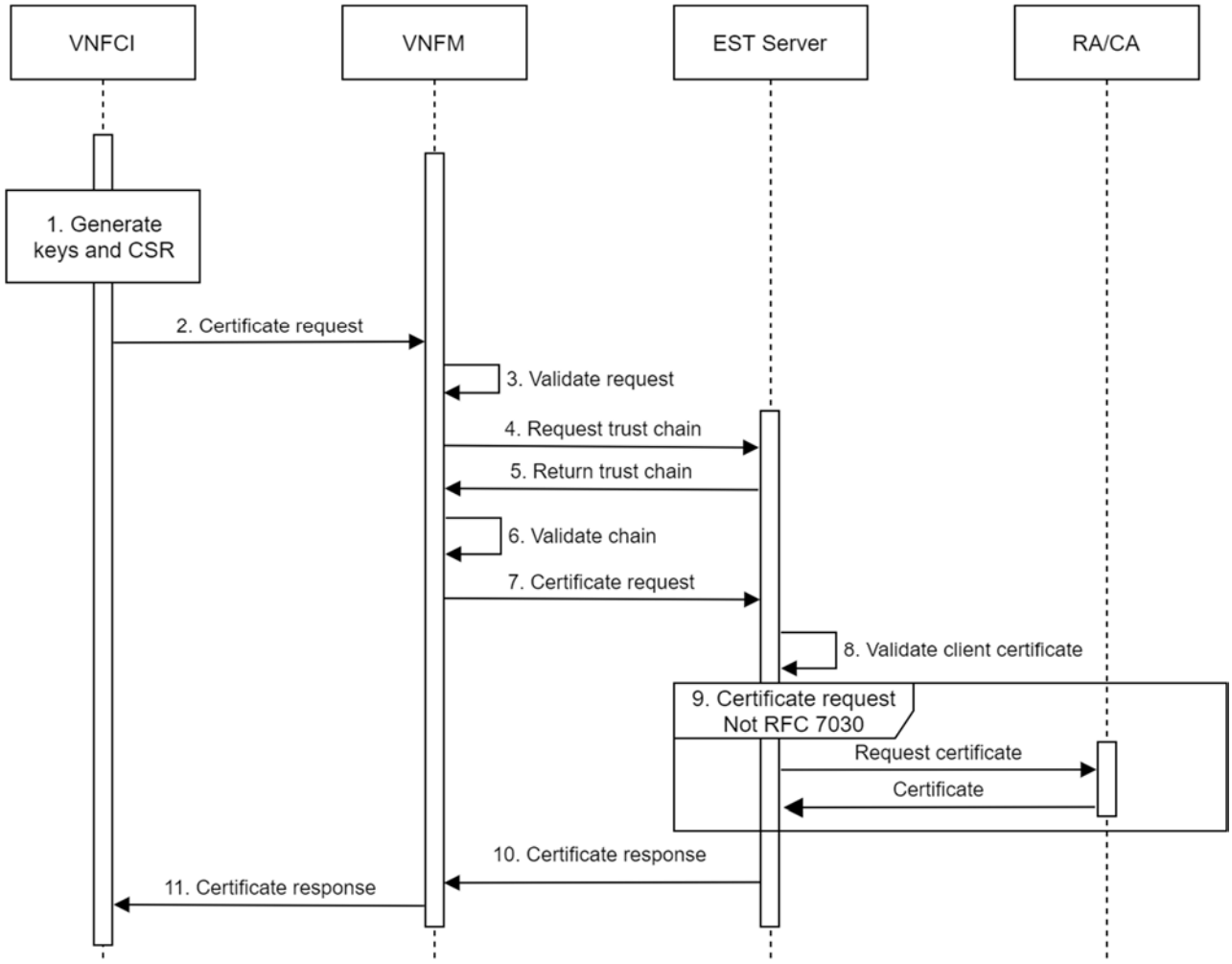

Figure 8.1.2.2-1: VNFCI certificate agent enrolment procedure

1) After the successful instantiation, by the indication of certificate installed during instantiation, the VNFCI generates a public-private key pair to be certified by the Operator RA/CA.

2) The VNFCI constructs and sends Certificate Request message to VNFM to request a certificate, providing the generated public key. In this message the initial credential is used to authenticate the message by VNFM.

3) Based on the initial credential, VNFM verifies the Certificate Request message. If the verification is successful, VNFM acts as an agent of the VNFCI.

4) The VNFM initiates a TLS connection to the Operator Certificate Enrolment Server and requests the trust chain (all intermediate and root CA certificates). The VNFM verifies the Operator certificate against the Operator root CA certificate and abandons the connection if they do not verify.

5) The Operator Certificate Enrolment Server returns the trust chain containing all of the Operator RA/CA certificate.

6) The VNFM verifies the trust chain against the Operator root CA certificate and abandons the certificate request if they do not verify.

7) The VNFM sends the Certificate Signing Request message to the Operator Certificate Enrolment Server to request a certificate. The VNFM certificate is used as the client certificate to authenticate the message to the Operator Certificate Enrolment Server.

8) Operator Certificate Enrolment Server verifies the connection based on the VNFM certificate. If the verification is successful, it requests the certificate from the Operator RA/CA.

9) Operator Certificate Enrolment Server requests the certificate be signed by the Operator RA/CA. The Operator RA/CA responds to the enrolment request, providing the new certificate.

10) The Operator Certificate Enrolment Server then returns the signed certificate to the VNFM.

11) The VNFM verifies the Certificate Response message, and constructs and forwards Certificate Response message back to the VNFCI. The VNFCI verifies the received message, if successful, installs the received certificate.

NOTE: Authentication of VNFCI using the initial credential can be performed either by VNFM or by RA/CA, since both VNFM and RA/CA share the secret information. The above procedure assumes this authentication is performed by VNFM.

Additional policy could be applied to enhance the security, such as invalidating the initial credential once VNFCI installs a formal certificate successfully.

8.1.2.3 Option 3: HSM generates key pair, constructs and signs certificate request

This option uses an HSM to obtain a certificate issued by Operator CA on behalf of a VNFCI. This could be particularly advantages for highly dynamic (rapidly scaling in/out) or short lived VNFCIs. The HSM in this clause is considered to be more feature rich than a basic HSM that can only handle basic certificate queries.

For this option, a key pair generation mechanism implemented by an HSM is used to generate the key pair, using an ETSI GS NFV SEC 012 [i.11] compliant random number generator, and constructs the public key certificate request message on behalf of the VNFCI. The HSM uses its certificate to authenticate with the Operator Certificate Enrolment Server to request the certificate be signed. The Operator Certificate Enrolment Server request the certificate from the Operator CA according to the certificate enrolment procedure. Operator CA issues the formal certificate and sends it to the HSM. When instantiated the VNFCI is linked to the HSM through a secure channel established after a mutual authentication process. For this mutual authentication process, the public key of the HSM is expected to be loaded in the VNFCI and the initial credential is expected to be loaded in the HSM. How the public key of the HSM is introduced in the VNFCI, and how the initial credential is out of scope of the present document.

It is assumed that MANO will request the creation of several key pairs and certificates for VNFC scale out. The HSM will be responsible for the secure key pair/certificate creation and destruction.

This enrolment procedure is depicted in figure 8.1.2.3-1.

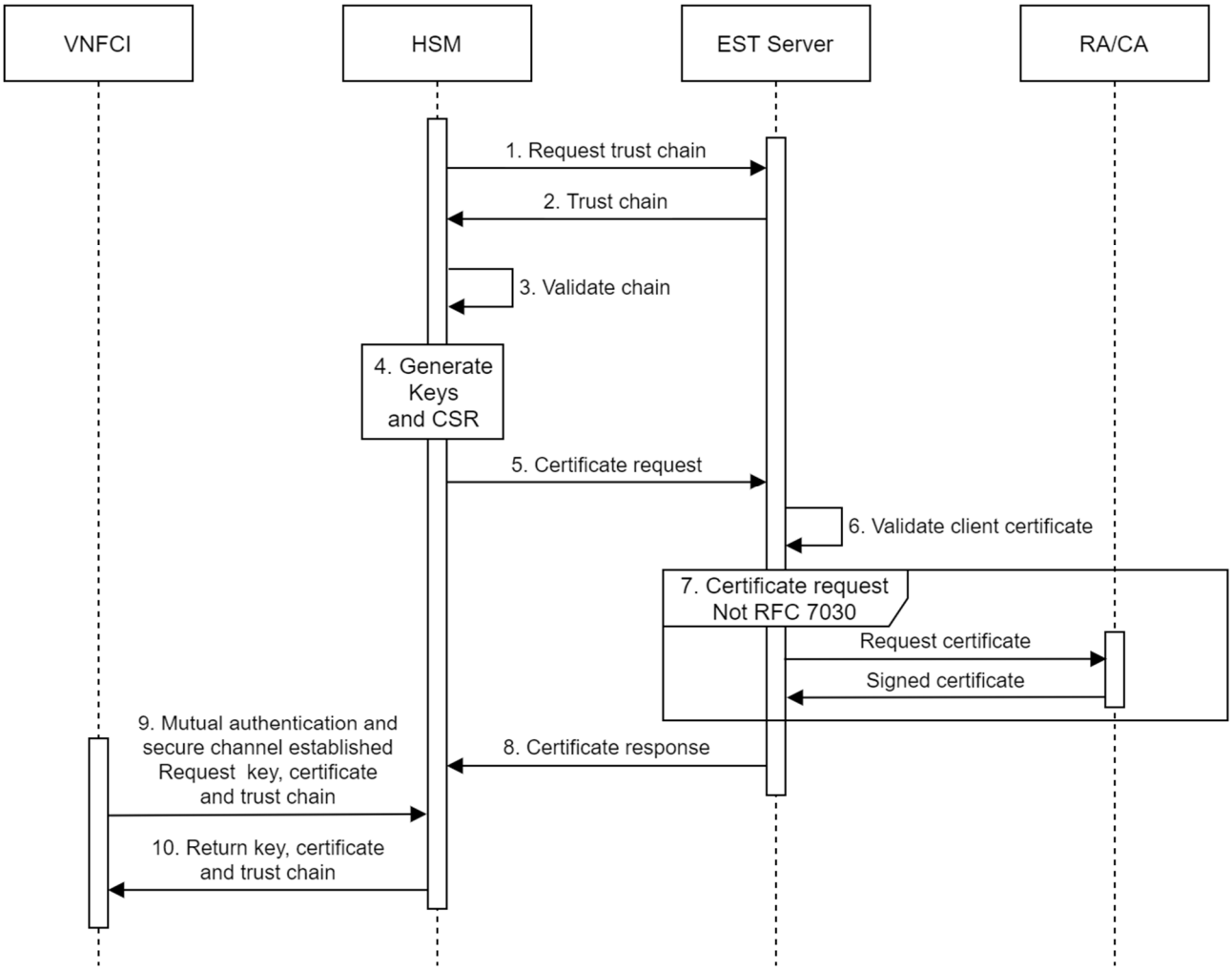

Figure 8.1.2.3-1: HSM certificate enrolment for VNFCI procedure

1) The HSM initiates a TLS connection to the Operator Certificate Enrolment Server and requests the trust chain (all intermediate and root CA certificates). The HSM verifies the Operator certificate against the Operator root CA certificate and abandons the connection if they do not verify.

2) The Operator Certificate Enrolment Server returns the trust chain containing all of the Operator RA/CA certificates.

3) The HSM verifies the trust chain against the Operator root CA certificate and abandons the certificate request if they do not verify.

4) The HSM generates a public-private key pair to be certified by the Operator RA/CA and constructs the Certificate Signing Request.

5) The HSM sends the Certificate Signing Request message to the Operator Certificate Enrolment Server to request a certificate. The HSM certificate is used as the client certificate to authenticate the message to the Operator Certificate Enrolment Server.

6) Operator Certificate Enrolment Server verifies the connection based on the HSM certificate. If the verification is successful, it requests the certificate from the Operator RA/CA.

7) Operator Certificate Enrolment Server requests the certificate be signed by the Operator RA/CA. The Operator RA/CA responds to the enrolment request, providing the new certificate.

8) The Operator Certificate Enrolment Server then returns the signed certificate to the HSM. Where it is stored until the VNFC is instantiated.

9) After the successful instantiation, by the indication of certificate installed during instantiation, the VNFCI creates a mutually authenticated and secure channel to the HSM and requests a private key, signed certificate and the trust chain.

10) Based on the initial credential, the HSM verifies the request message. If the verification is successful, the HSM returns the keys, certificate and trust chain to the VNFCI.

NOTE: Steps 9 and 10 could be performed any number of times as the VNFCI is instantiated and terminated throughout its lifecycle.

Additional policy could be applied to enhance the security, such as invalidating the initial credential once VNFCI installs a formal certificate successfully.

8.2 Certificate update

A certificate is updated as a new certificate issuance before the current certificate expires, that may also include name update, attribute update, public key update, expiration update, etc. Certificate update can initiate by VNFCI or by VNFM on behalf of the VNFCI.

All of the previously mentioned certificate management protocols (CMP [i.18], SCEP [i.20] & EST [i.16]) have certificate renewal procedures. Once the CA has issued a formal certificate for the VNFCI, the VNFCI is able to authenticate either directly or through the agent of VNFCI (i.e. VNFM) for any subsequent updates with that certificate. The PKI should support either case for certificate update.

If the public-private key pair needs to be updated, either VNFCI or NFVI could generate the key pair, which is determined by implementation.

9 NFV Certificate Management

9.0 Introduction

All NFV functional blocks should configure certificates, including MANO entities, VNFCI, VNFI and some other O&M entities (e.g. EMS and OSS/BSS). Manual and automatic configurations are common ways used in certificate deployment. In order to support the requirement that the NFV framework incorporates mechanisms for automation of operational and management functions automation, the clauses below focus on automatic mechanisms for certificate management.

9.1 MANO and other functional blocks

The MANO functional blocks defined by ETSI GS NFV 002 [i.2] include:

- NFV Orchestrator (NFVO).
- VNF Manager (VNFM).
- Virtualised Infrastructure Manager (VIM).

Furthermore, some other functional blocks, such as EM and OSS/BSS, are entities exchanging information with NFV-MANO functional blocks or VNFs to perform management operation. Therefore, they are also described here.

Since MANO and other O&M functional blocks (i.e. EM and OSS/BSS) are long-lived entities, the certificate deployment is similar with the traditional non-virtualised entities, e.g. by manual or automatic configuration.

9.2 Tenant domain

9.2.1 VNF certificate

9.2.1.0 Introduction

The certificate in VNF is for the logical functions of VNF. This clause discusses the certificate management and the relationship between certificate lifecycle and VNF lifecycle.

9.2.1.1 ID and certificate management in VNF

One VNF could have several functionalities and several logical interfaces, and one VNF could have several identities for different functionality, for different communication interface. According to the policies, different interfaces/functionalities could be assigned either same ID or different IDs. The ID and the functionalities/interfaces/communication-sessions could be a multiple-to-multiple mapping, as shown in figure 9.2.1.1-1.

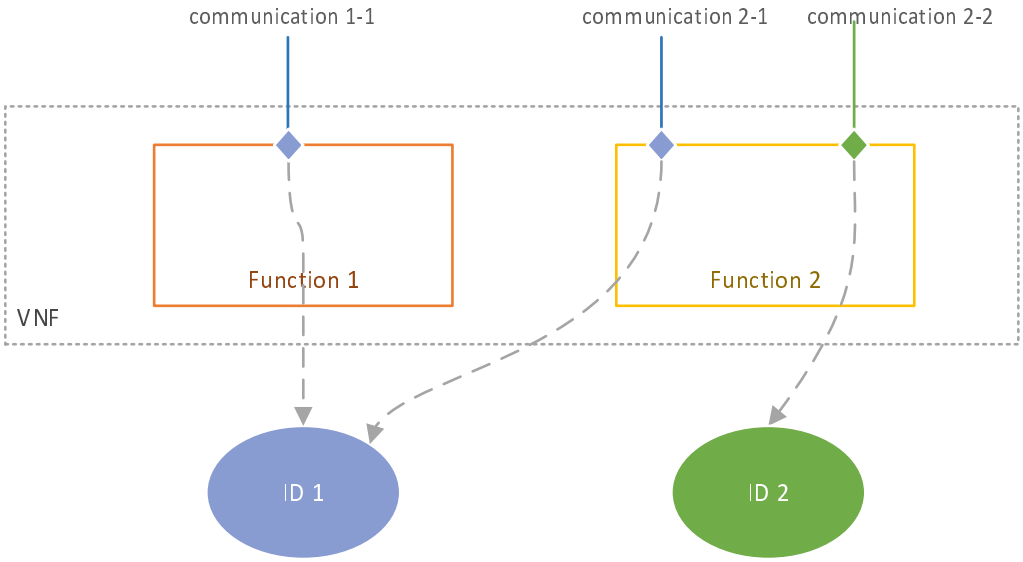

Figure 9.2.1.1-1: Mapping between function and ID

For example, the Mobility Management Entity (MME) in 3GPP network may connect to EMS, to eNodeB, to Serving Gateway (SGW), to other MME belonging to the same or different operators. All those connections could use the same ID or use different IDs in different interfaces.

A VNF consists of several VNF components (VNFC). A VNF instance (VNFI) is composed by several VNFC instances (VNFCI). A VNFC could be instantiated to multiple VNFCI.

A VNFCI refers to one realization of a defined VNFC. As defined in ETSI NFV 003 [i.3] a VNFCI corresponds to one virtualisation container (for example OS container or VM).

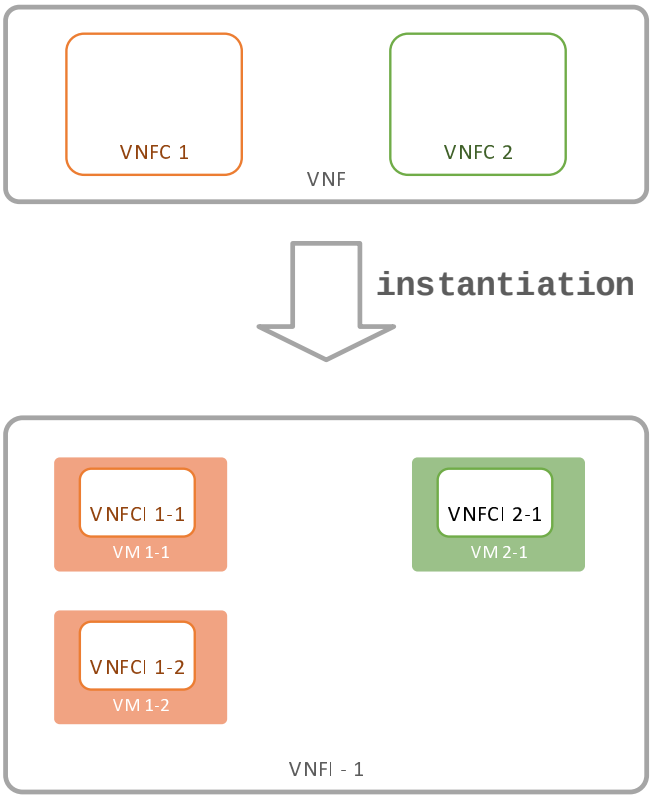

Figure 9.2.1.1-2: VNF instantiation: one VNFC could have multiple VNFCI

The ID in one VNF could be assigned to multiple functions, and each function could have multiple instances (VNFCI). Therefore, one ID will have multiple users, i.e. multiple VNFCI. There could be different policies for the binding between credential and ID. In the present document, the credential(s) bound to one ID are the certificate and the corresponding private key. The policies are:

P1. One ID have multiple credentials, each VNFCI using unique credential.

P2. One ID have one credential, all the VNFCI using same credential for one ID.

P3. One ID have multiple credentials, some of them are unique and some of them are bound to multiple VNFCI.

In case P2, the VNF only applies one certificate from CA/RA, for one ID. In case P1 and P3, the VNF needs to apply multiple certificate from CA/RA, for one ID. It is not restricted that one ID is bound to one certificate. IETF RFC 5280 [i.17] says:

"A CA MAY issue more than one certificate with the same DN to the ***same subject entity****."*

The *subject entity* equals to the ID being discussed in the present document.

The operator can select the policy. However, it should be emphasized that *issuing multiple certificate to the same entity* is an optional feature for the CA capacity.

One certificate for one ID

Figure 9.2.1.1-3 shows an example for the policy "one certificate one ID".

NOTE: This policy does not mean the certificate has to have multiple copies rather that in virtual environments, there are solutions that do not need to copy the certificate into each VNFCI.

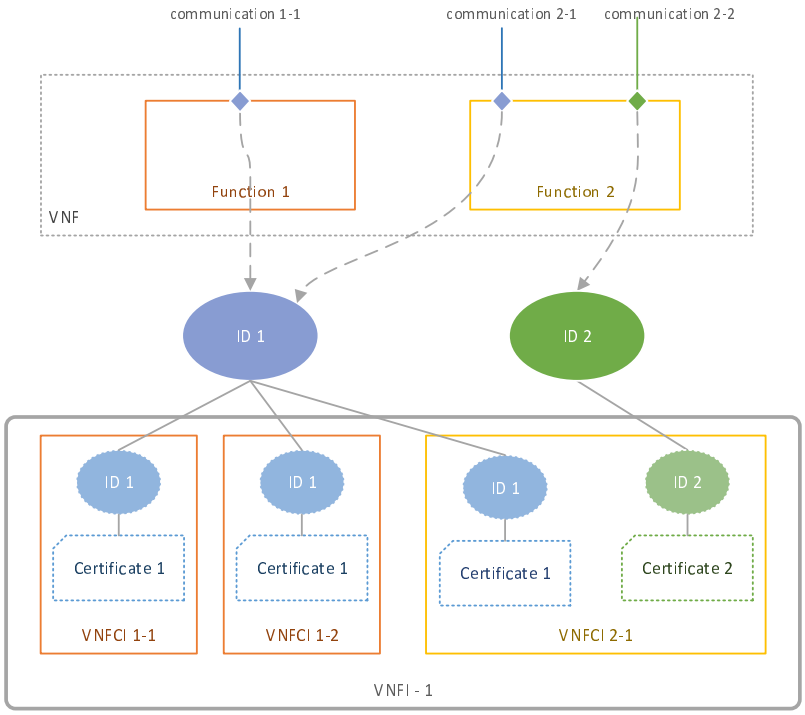

Figure 9.2.1.1-3: Example of certificate sharing

The traditional network NE has a secure internal physical environment. The communication between the components of one NE is typically regarded as a secure zone. The private key and certificate could be used by multiple components, that is, multiple physical boards. If only the private key is not disclosed on the network communication, the share is considered as safe.

In the virtual environment, the NE is distributed in the virtual environment and there is no physical boundary for internal communication. If the private key has multiple copies, the risk of key disclosure is increased: transferring the private key faces communication attack, and, multiple copy or multiple access means one copy disclosure will pose a threat to all VNFCI using that certificate. Therefore, sharing private key and certificate should be actively discouraged unless carefully implemented.

Table 9.2.1.1-1 lists the requirement of implement certificate sharing in one VNF.

Table 9.2.1.1-1: Requirement of implement certificate sharing in one VNF

	Risk	Mitigation
Confidential	• Disclosure of private key in communication • Storage and memory hack to get private key	• Communication encryption when private key is transmitted • Storage encryption in all VNFCI storing private key • Storage encryption in network or platform storage
Integrity	• Storage modification	• Storage integrity protection in all VNFCI storing private key • Storage integrity protection in network or platform storage
Access control	• Spoofing to get private key copy • Communication message modification/replay	• Communication & storage authentication and authorization • Communication integrity protection
Audit	• Repudiation	• Log
Availability	• DOS or DDOS (happens each request)	• Security domain for internal communication in VNF

A secure zone should be built for the private key storage and transmission on the network. In the case of a VNF instance, the VNF instance is itself a trust domain, and any VNFCIs which make up the VNF instance are therefore within the boundary of that trust domain. In general, that any communications and shared storage between those VNFCIs are expected to be protected at the level of the VNF instance, to maintain the trust boundary. However, some VNFCIs may be more sensitive than other therefore groups of one or more VNFCI within the VNF instance may have additional communications and shared storage security requirements. There may, of course, be different levels of trust domains, including some with multiple VNFs. A trust domain is not congruent to the shared domain of a private key.

Unique certificate for each ID in each VNFCI

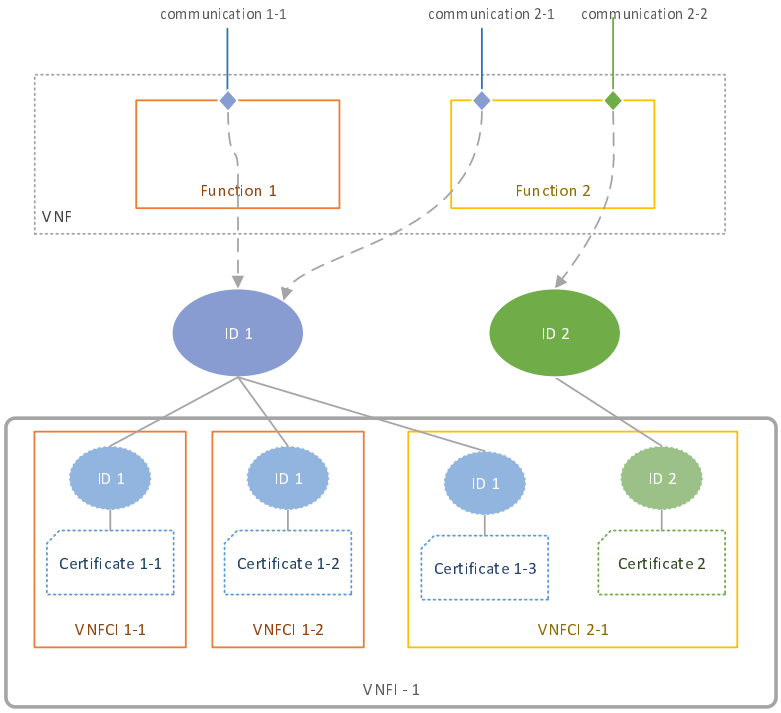

Figure 9.2.1.1-4: Example of unique certificate for each VNFCI

This policy has a significant advantage: the private key is held in each VNFCI and no inter-VNFCI communication to transfer any private keys. The life cycle of the certificate is along with the container VM lifecycle. When one instance is created on a new VM, e.g. VNF instantiation and scaling out, a new certificate is applied from CA. When one instance is terminated on a VM, e.g. VNF termination and scaling in, the certificate that stored on the VM is revoked from CA. When one instance is terminated and recreated in another location, e.g. VNF migration, the certificate in the old VM is revoked and a new certificate is applied for the instance in the new VM.

For the non-certificate sharing case, multiple certificates for one subject entity brings some complexities for management, because the "subject name" and "public key" is a one to many mapping. The only unique index in the certificate is the "issuer + serial number". This leads to the management complexity as follows:

a) Complexity in operation and maintenance, e.g.:

   i) Complex to configure the mapping between certificates and the functions, between certificates and function instances.

   ii) Configuration change or software upgrade may cause certificate application, update or revocation.

b) Complexity for certificate management function in VNF. The certificate lifecycle management should be distributed in all VNFCI that uses the certificate. Each VNFCI should support or partly support certificate initial application, update and revocation. At least, the private key generation, certificate application file generation and signature should be supported.

c) Complexity and inefficiency to NFV dynamic orchestration. Each time the NFV scales and each time the NFV container migrates, the certificate is expected to be either initially applied or revoked. The application and revoke are network communication and will lead to time latency for the orchestration.

d) Complexity in updating/revoking a certificate. The CA/RA workload is increased and the CA/RA is expected to support an "optional feature" in IETF standard, i.e. *A CA MAY issue more than one certificate with the same DN to the **same subject entity.***

9.2.1.2 Certificate lifecycle and VNF lifecycle

Certificates have their lifecycles, i.e. certification applying, certificate update and certificate revocation, as discussed in clause 8. A VNF has its lifecycle, i.e. VNF instantiation, scaling, update, upgrade and termination. If a certificate is assigned to one or multiple VNFCI, this certificate's lifecycle will have interaction to the VNF lifecycles. For example, one or multiple certificates should be applied from CA when the VNF instantiation is operated, and the corresponding certificates should be revoked from CA when one VNF instance is terminated.

The relation between VNF operation and VNF certificate management can be summarized in figure 9.2.1.2-1. Although the VNF migration is not purely a VNF operation, it is listed in this figure since this operation impacts the certificate lifecycle. In case of non-shared case, certificate management only happens between VNF and CA, as discussed in clause 8. In case of certificate sharing case, the certificate storage and sharing are also impacted by the VNF management.

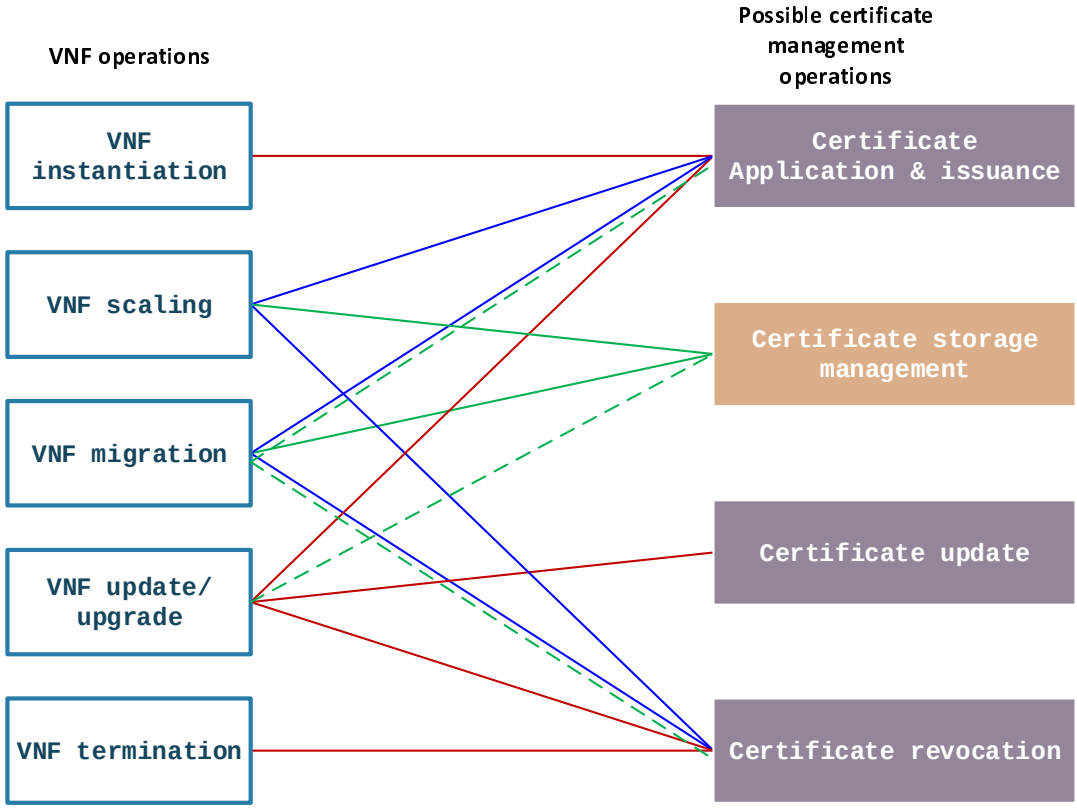

Figure 9.2.1.2-1: The relation between VNF status and VNF certificate operations

In figure 9.2.1.2-1, the green line is applicable in "certificate sharing case" or where a VNFCI's certificate is held in an HSM, the blue line is applicable to "non-certificate sharing case", and the red line is applicable to both cases. The dashed green line is optional in some implementations or some cases.

The following clause will explain figure 9.2.1.2-1 case by case.

9.2.1.3 VNF instantiation

When an VNF is instantiated, all the certificate required are applied for from the Operator CA. If the policy P1 (non-sharing) is deployed, each VNFCI should apply for its certificate from the Operator CA, even if they are assigned to the same ID. If policy P2 (certificate sharing) is deployed, only one certificate application is proceeded, normally by the "certificate-managing VNFCI". Other VNFCI shares the private key and certificate via various solutions.

9.2.1.4 VNF scaling

During the lifecycle of a VNF, the VNF Management functions may monitor KPIs of a VNF, if such KPIs were captured in the deployment template. The management functions may use this information for scaling operations. Scaling may include changing the configuration of the virtualised resources (scale up, e.g. add CPU, or scale down, e.g. remove CPU), adding new virtualised resources (scale out, e.g. add a new VM), shutting down and removing VM instances (scale in).

The scaling action and corresponding certificate operations as shown in table 9.2.1.4-1.

Table 9.2.1.4-1

VNF scaling action	Possible VNF certificate operations (certificate sharing)	Possible VNF certificate operations (certificate not sharing)
Scale UP: increase virtualised resource, e.g. add CPU or memory **Scale down:** release virtualised resources from existing instances, e.g. remove CPU	The resource change is transparent to certificate storage and usage.	The resource change is transparent to certificate storage and usage.
Scale out: add new virtualised resources, e.g. add a new VM instances	**certificate storage management:** assign the certificate copy or access right to the newly created VNFCI.	**Certificate initialization:** newly created VNFCI applies for new certificate from the Operator CA.
Scale in: release some virtualised resources, e.g. shut down and remove VM instances	**certificate storage management:** remove the certificate copy or access right from the obsoleted VNFCI.	**Certificate revocation:** the certificate used by obsoleted VNFCI is revoked from the Operator CA, by the VNFCI itself or by the certificate management function in VNFCI, or by the manager NE.

9.2.1.5 VNF migration

VNF instance or part of VNF instance change the resources, e.g. the container VM. See table 9.2.1.5-1 for details.

Table 9.2.1.5-1

VNF migration	Possible VNF certificate operations (certificate sharing)	Possible VNF certificate operations (certificate not sharing)
VNF or part of VNF change the resources, e.g. the container VM	• If the certificate-managing VNFCI is not migrated, change the share assignment: remove the copy or assign the access right to the new VNFCI and remove the copy or the access right from the obsoleted VNFCI. • If the communication for context migration is safe, the certificate could be copied from old resources to new resources. • If the sharing is via network storage, just re-mount the storage. • Otherwise, apply the the Operator CA for a new certificate for all migrated VNFCI and revoke the certificate used by obsoleted VNFCI.	Apply to the Operator CA for a new certificate for each migrated VNFCI.

9.2.1.6 VNF update/upgrade

VNF update/upgrade supports VNF software and/or configuration changes of various complexities, including addition of new functions, removal of current functions and modification of current functions. The function addition may need certificates and the function removal may obsolete certificate. The addition, removal and the modification may need to change some contents of existing certificate, e.g. the Key-usage or the validity period. The VNF certificate management should have corresponding actions in accordance with the VNF changes. See table 9.2.1.6-1 for details.

Table 9.2.1.6-1

VNF update/upgrade	Possible VNF certificate operations (certificate sharing)	Possible VNF certificate operations (certificate not sharing)
Add new function that need certificate	• If required certificate is not available in VNFI, apply for a new one, otherwise. • If required certificate exists in VNFI, but the contents does not satisfy the requirement, update the certificate and manage the sharing, otherwise. • If required certificate exists in VNFI, manage the sharing.	• If required certificate is not available in VNFCI, apply for a new one, otherwise. • If required certificate exists in VNFCI, but the contents does not satisfy the requirement, update the certificate and manage the sharing.
Remove a function that was assigned a certificate	• If the certificate is required by other function, manage the sharing. • If the certificate is not required by other function, revoke it.	• Revoke the certificate.
Change the function related to a certificate	• If the certificate does not satisfy the requirement of the function change, update it. • if the certificate is no longer needed by other functions in this VNFI, change the sharing or revoke it. • if the certificate is still used by other functions in this VNFI, check the contents of certificate. If the contents of the certificate need change, update it.	• If the certificate does not satisfy the requirement of the function change, update it. • if the certificate is no longer needed by other functions in this VNFCI, revoke it. • if the certificate is still used by other functions in this VNFCI, check the contents of certificate. If the contents of the certificate need change, update it.
Add or Remove a function without communication requirement	Change is transparent to certificate storage and usage.	Change is transparent to certificate storage and usage.

9.2.1.7 VNF termination

NFV Orchestrator can receive a request to terminate an existing VNF instance. This request may be triggered by OSS or MANO. In this case, VNFI or MANO or OSS should invoke certificate revocation for the VNFI before it is gracefully terminated. If VNFI is terminated abnormally, the MANO or OSS should initiate a certificate revocation procedure as soon as it detects the abnormality of VNFI.

It is highly recommended to securely clear the local or network storage of the private key and the certificate before termination. The clearing could be done by VNF, if it is gracefully terminated, or by MANO if the VNFI is abnormally terminated. The clearing is very important because the PKI relies on Certificate Revocation List (CRL) or Online Certificate Statis Protocol (OCSP) to prevent certificate misuse or abuse of revoked certificates. As the CRL is periodically updated, an attack could success between the CRL update gaps, if someone could get the copy of private key and the certificate file.

9.3 Certificate Provisioning

In the traditional NE, certificates and associated keys could be provisioned by:

1) Manually copying the private key and certificate via USB.

2) Connect to the local maintenance port and copy certificate.

3) The NE is provisioned with a device certificate issued by vendor or by third- party entity:

   a) this certificate is used as the NE certificate;

   b) using this certificate as an initial credential to apply a new certificate.

4) The NE is provisioned with some credentials, e.g. token or pre-shared key, and the new certificate is applied using this credential to access CA.

All of those solutions could be implemented for the NFVI creation, e.g. provisioning the certificate for the switches, routers and the host OS, etc. If the VM is created to have direct access right to the physical interfaces, e.g. USB port or Ethernet port, those solutions are applicable for VNF layer certificates provisioning.

In VNFI layer, solution 1 is not applicable, because neither the USB interface nor the manual operations are available in most cases. Solution 2 is not applicable, because the local maintenance port is not available in most cases. The device certificate (solution 3) is no longer available, since the vendor only delivers software package to the operator. The VM and the NE are created on virtual resources, and therefore solution 3 is not applicable. The solution 4 requires provisioning credentials via USB or local maintenance interface, thus it is not applicable for virtual environment.

Provisioning certificate in NFV needs to be automated and manual operations avoided as much as possible. Some of the possible solutions have been discussed in clause 8.1. The main philosophy is injecting credentials to the instance. If the credentials are certificate, they could be used as the formal certificate or they could be as the temporary credential to apply formal certificates from the Operator CA. It could be the VNFM or VIM to do the injection.

9.4 Trust chain management

Certificate management systems have to be validated by VNFs, which can be realized by provisioning a root CA certificate, trust chain or Pre-Shared Key (PSK) in to those VNFIs. The root CA certificate or PSK can be provisioned during onboarding or the instantiation procedure. And VNFIs can use this provisioned information to validate the PKI system.

VNF should maintain a trust chain of Operator CA certificates (containing certificate for all intermediate and root CA's) to validate the certificates issued by the Operator CA. The trust chain may be provisioned in the VNF during the VNF instantiation procedure, or be obtained using certificate management protocol, e.g. EST [i.16].

If the root CA certificate is provisioned during the instantiation procedure, it should be configured by VNFM and securely transmitted via VIM and NFVI, then injected to the VNFI.

If the root CA certificate is provisioned using a certificate management protocol, there should be some mechanism to ensure VNFI can trust the CA's identity, e.g. a PSK is shared between VNF and CA in order to validate that CA in the subsequent certificate management protocol requests for the VNFI.

9.5 Client certificate distribution

Where a TLS protected API relies on certificate-based client authentication (where the producer/server requests the consumer/client transmit a certificate within the TLS handshake) effective and secure distribution of the client certificate is required.

It may be possible for API producers to use mechanisms/options, within the certificate automation protocol (for example EST Extensions [i.20]) or some other mechanism, to retrieve and validate the client certificate automatically. Further details for automatic certificate distribution are not defined in the present document.

10 Recommendations

10.1 Overview

Clause 10 provides recommendations related to the certificate management for NFV derived from the certificate management framework, certificate lifecycle management and NFV certificate management descriptions in clauses 7, 8 and 9 respectively, as well as based on the use cases and approach defined in clauses 4 and 5. Recommendations encompass the identification of potential new requirements, covering certain aspects or required functionality.

Recommendations are categorized in and elaborated as follows:

- General (refer to clause 10.2);
- Functional security (refer to clause 10.3);
- Reference points and/or interfaces (refer to clause 10.4); and

- Descriptors and other information/data model artefacts (refer to clause 10.5).

NOTE: There are some identifiable PKIs structures for the management of certificates associated with the VNF lifecycle for which some of these recommendations are not applicable (see the considerations in clause 10.5). While it is desirable to have a unified PKI solution as suggested by these recommendations, real deployment scenarios may require different PKI arrangements in order to ensure guarantees of trust domain separation.

10.2 General recommendations

The present clause provides recommendations focusing on generic and framework aspects.

Table 10.2-1 provides recommendations related to general aspects of certificate management.

Table 10.2-1: General recommendations related to certificate management

Identifier	Recommendation description
Gen.Cert.001	It is recommended that a generic requirement be specified to support automated certificate management for the NFV Architectural Framework.
Gen.Cert.002	It is recommended to specify requirements for supporting automated certificate lifecycle management, i.e. creation, update and revocation of certificate.
Gen.Cert.003	It is recommended to specify requirements for supporting different certificate types for the establishment of a secure connection between peer entities, i.e. between applications of VNFC (VNFC certificate defined by clause 6.2 of ETSI NFV-SEC 021 [i.22]), between VNFC and NFV-MANO/EM (VNF OM certificate), between NFV-MANO functional blocks (NFV-MANO certificate).
Gen.Cert.004	It is recommended to extend requirements specification defined in clause 6 of ETSI NFV-SEC 021 [i.22] for supporting certificate types and roles to verify and check the integrity of signed Packages, i.e. VNF Package, SW image, VNF Snapshot Package, and NS Package.
Gen.Cert.005	It is recommended to specify requirements for the management of information required to distribute certificates, i.e. FQDN of end points and sub Cas certificates.

NOTE: The present document does not cover package signing and it is associated certificate management.

10.3 Functional recommendations

The present clause provides recommendations focusing on functional aspects of the functional blocks identified in the NFV Architectural Framework.

Table 10.3-1 provides recommendations related to functional security aspects of NFVO.

Table 10.3-1: Recommendations related to functional security aspects of NFVO

Identifier	Recommendation description
Nfvo.Cert.001	It is recommended to specify a functional requirement related to the establishment of secure connections between the NFVO and its peer entities using NFV-MANO certificate and the sub CAs certificate of the peer entity provided by Operator Certificate Enrolment Server.
Nfvo.Cert.002	It is recommended to specify a functional requirement related to the re-establishment of secure connections between the NFO and its peer entities using an updated NFV-MANO certificate and sub CAs certificate provided by Operator Certificate Enrolment Server without interruption of NFV-MANO services provided by the NFVO.

Table 10.3-2 provides recommendations related to functional security aspects of VNFM.

Table 10.3-2: Recommendations related to functional security aspects of VNFM

Identifier	Recommendation description
Vnfm.Cert.001	It is recommended to specify a functional requirement for the VNFM related to the management of the VNF instance certificates (i.e. VNFC certificate, VNF OM certificate and sub CAs certificate) including, requesting, distributing, updating and deleting the certificates.
Vnfm.Cert.002	It is recommended to specify a functional requirement for the VNFM related to the request process of issuing a VNF certificate and VNF OM certificate of the VNF instance to Operator Certificate Enrolment Server during VNF LCM for the VNF instance. See note.
Vnfm.Cert.003	It is recommended to specify a functional requirement for the VNFM for the distribution of the VNF certificate, VNF OM certificate and sub CAs certificate provided by Operator Certificate Enrolment Server to the VNF instance.
Vnfm.Cert.004	It is recommended to specify a functional requirement for the VNFM to support updating the VNF certificate VNF OM certificate and sub CAs certificate provided by Operator Certificate Enrolment Server to the VNF instance.
Vnfm.Cert.005	It is recommended to specify a functional requirement for the VNFM to support establishment of a secure connection with peer entities using NFV-MANO certificate and sub CAs certificate provided by Operator Certificate Enrolment Server.
Vnfm.Cert.006	It is recommended to specify a functional requirement for the VNFM to support re-establishment of secure connection with peer entities using an updated NFV-MANO certificate and sub CAs certificate provided by Operator Certificate Enrolment Server without interruption of NFV-MANO services provided by the VNFM.
NOTE: Timing for issuing the certificate at other than VNF LCM is not addressed in the present document, e.g. issuing VNF provider certificate before packaging, certificate expiration, certificate revocation.	

Table 10.3-3 provides recommendations related to functional security aspects of VIM.

Table 10.3-3: Recommendations related to functional security aspects of VIM

Identifier	Recommendation description
Vim.Cert.001	It is recommended to specify a functional requirement for the VIM to support receiving a VNF certificate and a VNF OM certificate from the VNF instance during VNF LCM.
Vim.Cert.002	It is recommended to specify a functional requirement for the VIM to support providing a VNF certificate and a VNF OM certificate to VNFM.
Vim.Cert.003	It is recommended to specify a functional requirement for the VIM to support injecting or updating the VNF certificate, VNF OM certificate and sub CAs certificate provided by an Operator Certificate Enrolment Server to the VNF instance via VNFM.
Vim.Cert.004	It is recommended to specify a functional requirement for VIM to support establishing a secure connection with peer entities using a NFV-MANO certificate and sub CAs certificate of the peer entity provided by Operator Certificate Enrolment Server.
Vim.Cert.005	It is recommended to specify a functional requirement for VIM to support re-establishing the secure connection with peer entities using an updated NFV-MANO certificate and sub CAs certificate provided by Operator Certificate Enrolment Server without interruption of MANO services provided by the VIM.

Table 10.3-4 provides recommendations related to functional security aspects of WIM.

Table 10.3-4: Recommendations related to functional security aspects of WIM

Identifier	Recommendation description
Wim.Cert.001	It is recommended to specify a functional requirement for the WIM to support establishing a secure connection with peer entities using a NFV-MANO certificate and a sub CAs certificate of the peer entity provided by Operator Certificate Enrolment Server.
wim.Cert.002	It is recommended to specify a functional requirement for the WIM to support re-establishment of the secure connection with peer entities using updated NFV-MANO certificate and sub CAs certificate provided by Operator Certificate Enrolment Server without interruption of NFV-MANO services provided by the WIM.

NOTE 1: The requirements for the WIM are not specifically addressed in the present document.

Table 10.3-5 provides recommendations related to functional security aspects of CISM.

Table 10.3-5: Recommendations related to security aspects of CISM

Identifier	Recommendation description
Cism.Cert.001	It is recommended to specify a functional requirement for the CISM to support establishment of a secure connection with peer entities using a NFV-MANO certificate and a sub CAs certificate of the peer entity provided by Operator Certificate Enrolment Server.
Cism.Cert.002	It is recommended to specify a functional requirement for CISM to support re-establishment of the secure connection with peer entities using updated NFV-MANO certificate and a sub CAs certificate provided by Operator Certificate Enrolment Server without interruption of NFV-MANO services provided by the CISM.

NOTE 2: The requirements for the CISM are not addressed in the present document.

Table 10.3-6 provides recommendations related to functional security aspects of CIR.

Table 10.3-6: Recommendations related to functional security aspects of CIR

Identifier	Recommendation description
Cir.Cert.001	It is recommended to specify a functional requirement for CIR to support establishing a secure connection with peer entities using NFV-MANO certificate and sub CAs certificate of the peer entity provided by Operator Certificate Enrolment Server.
Cir.Cert.002	It is recommended to specify a functional requirement for CIR to support re-establishment of the secure connection with peer entities using an updated NFV-MANO certificate and sub CAs certificate provided by Operator Certificate Enrolment Server without interruption of NFV-MANO services provided by CIR.

NOTE 3: The requirements for the CIR are not specifically addressed in the present document.

Table 10.3-7 provides recommendations related to functional security aspects of NFVI.

Table 10.3-7: Recommendations related to functional security aspects of NFVI

Identifier	Recommendation description
Nfvi.Cert.001	It is recommended to specify a functional requirement for NFVI to support key-pair generation and injection of the key pair into a VNF instance.
Nfvi.Cert.002	It is recommended to specify a functional requirement for CIR to support re-establishment of the secure connection with peer entities using an updated NFV-MANO certificate and sub CAs certificate provided by Operator Certificate Enrolment Server without interruption of NFV-MANO services provided by CIR.

Table 10.3-8 provides recommendations related to functional aspects of Operator Certificate Enrolment Server.

Table 10.3-8: Recommendations related to functional aspects of Operator Certificate Enrolment Server

Identifier	Recommendation description
Cm.Cert.001	It is recommended to specify a functional requirement for Operator Certificate Enrolment Server to support managing all types of the certificate lifecycle.
Cm.Cert.002	It is recommended to specify a functional requirement for Operator Certificate Enrolment Server to support distributing all types of certificates and trust chains (all intermediate and root CA certificates) to MANO functional blocks.
Cm.Cert.003	It is recommended to specify a functional requirement for Operator Certificate Enrolment Server to support providing FQDN and authorization to enable certificate management.

10.4 Reference points and/or interfaces recommendations

The present clause provides recommendations focusing on the definition and specification of interfaces on the various NFV-MANO defined reference points and NFV-MANO services.

Table 10.4-1 provides recommendations related to Os-Ma-nfvo reference point.

Table 10.4-1: Recommendations related to the Os-Ma-nfvo

Identifier	Recommendation description
OsMaNfvo.Cert.001	It is recommended to specify an interface requirement for the NS LCM to provide interface endpoint of the Operator Certificate Enrolment Server used to manage the VNF certificate and the VNF OM certificate.
OsMaNfvo.Cert.002	It is recommended to specify an interface requirement to exchange NFV-MANO certificates.
OsMaNfvo.Cert.003	It is recommended to specify an interface requirement to authenticate certificate-based clients by retrieving and validating client certificates.

Table 10.4-2 provides recommendations related to Or-Vnfm reference point.

Table 10.4-2: Recommendations related to the Or-Vnfm

Identifier	Recommendation description
OrVnfm.Cert.001	It is recommended to specify an interface requirement for VNF LCM in order to support providing an interface endpoint of Operator Certificate Enrolment Server to manage VNF certificates and VNF OM certificates.
OrVnfm.Cert.002	It is recommended to specify an interface requirement to support authentication of a certificate-based client by retrieving and validating the client certificate.

Table 10.4-3 provides recommendations related to the Ve-Vnfm reference point.

Table 10.4-3: Recommendations related to the Ve-Vnfm

Identifier	Recommendation description
VeVnfm.Cert.001	It is recommended to specify an interface requirement for VNF LCM to support providing an interface endpoint of the Operator Certificate Enrolment Server to manage VNF certificate and VNF OM certificate.
VeVnfm.Cert.002	It is recommended to specify an interface requirement for VNF Configuration to enable setting and modifying a VNF certificate and a VNF OM certificate.
VeVnfm.Cert.003	It is recommended to specify an interface requirement for the VNFM to support establishment of a secure connection to the authorized VNF instance using the initial credentials of the VNF instance.
VeVnfm.Cert.004	It is recommended to specify an interface requirement to support authentication of certificate-based client by retrieving and validating the client certificate.

Table 10.4-4 provides the recommendations related to Vi-Vnfm reference point.

Table 10.4-4: Recommendations related to the Vi-Vnfm

Identifier	Recommendation description
ViVnfm.Cert.001	It is recommended to specify an interface requirement related to virtual resource management for injecting and updating a VNF certificate and a VNF OM certificate.
ViVnfm.Cert.002	It is recommended to specify an interface requirement related to virtual resource management for exchanging public keys, VNF certificates and VNF OM certificates.
ViVnfm.Cert.003	It is recommended to specify an interface requirement to support authentication of certificate-based clients by retrieving and validating client certificates.

NOTE: The present document allows both the Ve-Vnfm and Vi-Vnfm to be used for the provision or modification of the VNF and VNF OM certificates. Any restriction or recommendations of Ve-VnFM vs Vi-Vnfm would depend on the actual implementation or subsequent normative NFV certificate management specifications.

Table 10.4-5 provides recommendations related to the NFV-MANO management interfaces.

Table 10.4-5: Recommendations related to the NFV-MANO management interfaces

Identifier	Recommendation description
ManoMgmt.Cert.001	It is recommended to specify an interface requirement for NFV-MANO management to support exchanging NFV-MANO certificates and sub CAs certificates.
ManoMgmt.Cert.002	It is recommended to specify an interface requirement for NFV-MANO management to support updating NFV-MANO certificates and sub CAs certificates.
ManoMgmt.Cert.003	It is recommended to specify an interface requirement to support authentication of certificate-based clients by retrieving and validating client certificates.

10.5 Various considerations for certificate automation, trust handling and PKI structures

10.5.1 Concepts

The present clause describes certificate management options for OS container-based VNFs. Some of these considerations could be extended to address VM-based VNFs.

NOTE: In the present clause 10.5 and unless specified otherwise, the sets of terms *consumer/producer* and *client/server* are used interchangeably when referring to public-key certificate owners.

As stated in ETSI GS NFV-SEC 023 [i.23], a VNF or VNFC designed to be deployed and managed on Container Infrastructure Service instances (CIS) is represented by a containerized workload running on OS containers. Existing de-facto standard container infrastructure management systems consider managing containerized workloads at a granularity which is higher than on a single container level. A set of OS containers that are tightly coupled to run in the same execution environment (i.e. on the same CIS instance) and designed to be scheduled together, is defined as the smallest manageable workload object. A VNFC instance is assumed to be 1:1 mapped to such a smallest manageable unit of a containerized workload. The CISM manages and exposes Managed Container Infrastructure Objects (MCIOs).

An MCIO whose declarative descriptor specifies compute/storage infrastructure resource requests represents such smallest manageable unit and is assumed to be 1:1 mapped to a VNFC. A CISM instance manages multiple containerized workloads in a cluster of CIS instances.

As described in ETSI GS NFV-IFA 040 [i.24], namespaces are abstract NFV object for OS container management and orchestration representing a logical grouping for a particular set of identifiers, resources, policies and authorizations within the scope of a cluster of CIS instances. Therefore, one (or several) namespaces are shared between the VNFCs part of a VNF.

10.5.2 Certificate categories

It is assumed that a VNFI requires inter-VNFCI TLS communications to deliver its services. Such intra-VNFI TLS sessions (between VNFCIs) are assumed to employ certificates for end-point (mutual) authentication.

NOTE 1: For example, 3GPP has specified the certificate profile for the client and server certificates (i.e. for the service consumer and service producers) in the SBA architecture. A 3GPP Network Function (NF) could face several options when deciding the certificate usage, for example:

1) the NF could get one certificate that can be used as client as well as server certificate; or

2) there might be one client certificate for consuming interfaces and one certificate for all the service producing interfaces (referred to as 1+1 assumption); or

3) the latter service producing end points might get each one its own server certificate (referred to as 1+N assumption).

The specification allows all three of these approaches. Nonetheless, having a combined client and server certificate is often considered unsafe. Figure 10.5.2-1 illustrates the other two options.

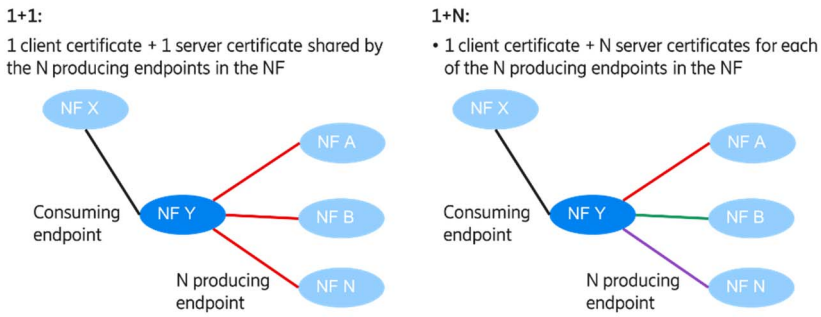

Figure 10.5.2-1: 1+1 and 1+N assumptions for SBA certificates

A VNFI realization implemented using an OS container technology has four layers of certificates associated with it:

1) The management layer includes certificates necessary for the secure configuration of the VNFI. Several certificates are needed for the management layer that connect management functions to the managed elements.

The "VNFCI transport certificate" is of 2 types:

2) Certificate(s) for intra-VNFI secure communication. For example, such certificates are necessary if TLS is relied upon for the secure communication between VNFCIs of the VNFI, with scope limited to the VNFI. And

3) Certificate(s) for inter-VNFI secure communication (e.g. for 3GPP NFs communications relying on TLS).

4) The CIS cluster control plane layer includes certificates related to the CIS cluster control plane components which communicate over mutually authenticated TLS sessions.

NOTE 2: Certificate categories 2 and 4 are not detailed in Clause 7.2 and recommendations for their management are not captured in clause 10.

NOTE 3: The number of certificates per VNF (application) is based on how the VNF is realized, on scaling assumptions and on how it interconnects with other VNFs in the same NS or slice. It is not surprising to find tens of different VNFCI transport certificates associated with a VNFI realization (and several others at management layers) in complex deployments such as 3GPP SBA NFs. These number estimates are per network slice. Furthermore, if OAuth 2.0 is deployed, then additional certificates for token verification are expected.

Figure 10.5.2-2 illustrates a high-level view of different certificate layers.

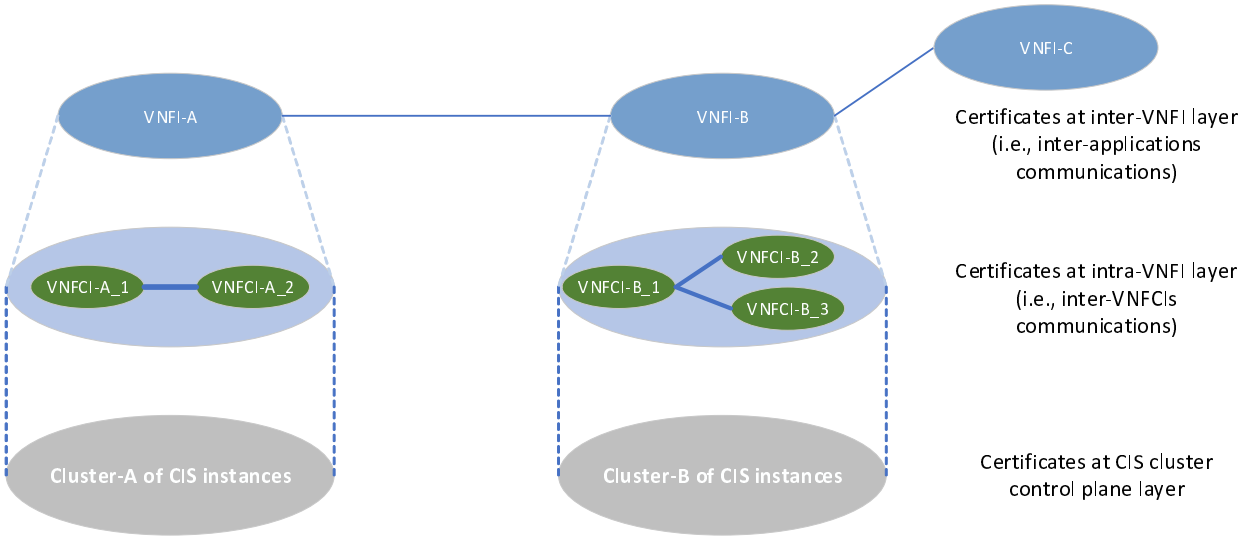

Figure 10.5.2-2: Three layers of interfaces where certificates are used. CIS cluster control plane, Intra-VNFI, and Inter-VNFI layers

Figure 10.5.2-3 illustrates one alternative of PKI arrangement showing how the certificates for all the endpoints may come from a central CA via application specific Certificate Management Functions (see clause X+1.4) that are configured through the management system, which contains the knowledge of the topology of endpoints requiring certificates and provides the certificate automation logic towards the CA.

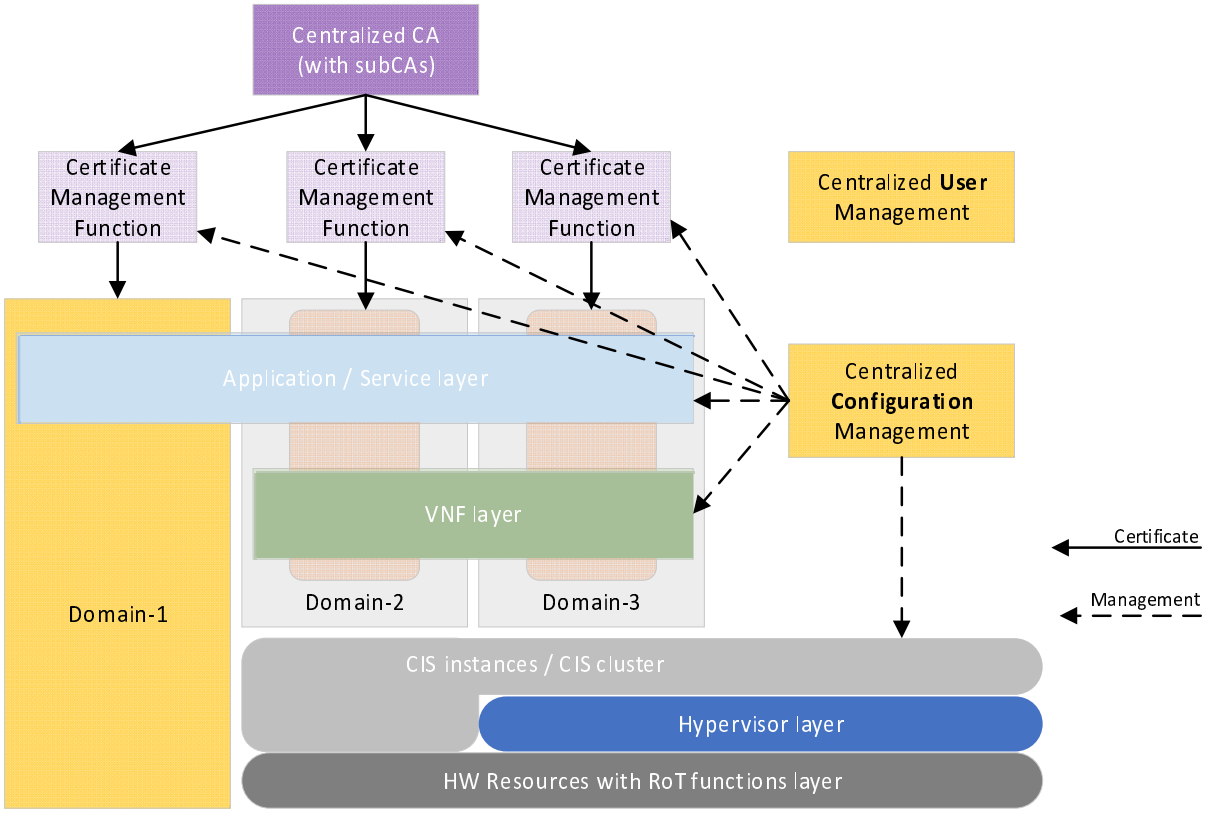

Figure 10.5.2-3: High-level view showing CA components

NOTE 4: Figure 10.5.2-3 illustrates a Certificate Management Function per domain (see clause 10.5.4 for its roles). This does not preclude other deployments where the same Certificate Management Function can be used for multiple domains based on the security policy. Figure 10.5.2-3 shows the use of a centralized CA. Nonetheless, a complex system such as 5G is expected to use more than one CA.

10.5.3 Trust assumptions

As stated in clause 9.2.1.1, the VNF instance is itself a trust domain and any VNFCIs which make up the VNF instance are therefore within the boundary of that trust domain.

NOTE 1: A VNF instance may also be subdivided into sub-security domains and be part of a larger security domain.

In a given trust domain, the tenant is given controls over the origins of VNFCIs certificates. The cloud provider empowers the tenant with various controls over service deployments implementing attestation and authentication of the execution environments where the secrets for the secure (TLS) connections are stored.

The consequences of this model is that the cloud provider should facilitate, at the discretion of the tenant, the ability for tenants to control the certificates at VNFCI transport (both inter-VNFI and intra-VNFI local to the CIS cluster) and management layers. Attestation should be used to bind the VNFCIs protection environments to the secure HW with Root-of-Trust (RoT) functions.

Certificates at the CIS cluster control plane layer, for the TLS sessions between the internal CIS control plane components, may be added under the tenant's control. Nonetheless, typical IT deployments leave the CIS control plane bring its own cluster internal CA for certificate management of these components. This CA can also be added as a sub-CA using manual procedures. There are three options for the CIS cluster control plane layer certificate management:

1) Option-1: uses a CA functionality internal to the CIS cluster control plane to act as an independent CA.

2) Option-2: uses a CA functionality internal to the CIS cluster control plane to act as a sub-CA to the operator root CA.

3) Option-3: uses the operator root CA directly.

Option-1 is usually employed although it has the apparent disadvantage from a management perspective, i.e. if external management functions need to interact with the CIS clusters. In this case, the CISM function should support the TLS SNI extension functionality which allows actors that use a certificate from an external PKI to connect to a cluster API Server for management purposes.

NOTE 2: For Option-1, Kubernetes® [i.25] being the de-facto CISM standard for these releases, the latest published versions of the reference Kubernetes® [i.25] API support the TLS SNI extension. For Option-2, certificate partial chain verification is not properly implemented by Kubernetes® API to distinguish if certificates come from a specific -. As a consequence, certificates created under a sub-CA for, say, cluster B will be accepted in cluster A if clusters A and B have sub-CAs that share the same root CA. In Option-3 the operator root CA can exercise control of who is given access to Kubernetes® [i.25] layers by management actors. However, Option-3 might be problematic with regards to performance and reliability.

10.5.4 Proposed PKI Structure

In order to manage the four categories of certificates listed in Clause X+1.2 according to the previous trust assumptions, the following PKI structure is proposed, illustrated in Figure X+1.4-1:

- For VNF management operations, such as VNFM interactions, the management layer may own either a local separated CA or a sub-CA of the Tenant CA.

- At intra-VNFI layer, the TLS secure communications confined to the CIS cluster and internal to VNFI should rely on an internal-to-VNF CA, which is separated from the tenant CA and from external-to-cluster CA hierarchy.

NOTE 1: Many open-source TLS implementation lack proper partial chain verification. As such, employing a common root CA among different clusters increases the risk of setting up TLS sessions with VNFCIs which are not supposed to be accessible from outside the cluster. Therefore, setting up an internal-to-VNF CA for certificates with scope confined to the VNFI trust domain diminishes this risk in addition to not exposing the VNFI internal topology externally.

NOTE 2: The private key for the internal-to-VNF CA should be protected during runtime and at rest if the key is persistent or backed-up.

- At inter-VNFI layer, the TLS communications rely on certificates issued by a Tenant CA or sub-CAs. This CA or sub-CA is typically external to the CIS cluster where the VNFI is instantiated.

- The CIS cluster control plane layer considers a local independent CA generated at (cluster) instantiation, as per Option-1 above. CISM management interface is likely to be consumed from outside the cluster, hence the TLS SNI extension is necessary to be supported.

NOTE 3: This CA is independent and not part of the overall PKI created under the operator root CA.

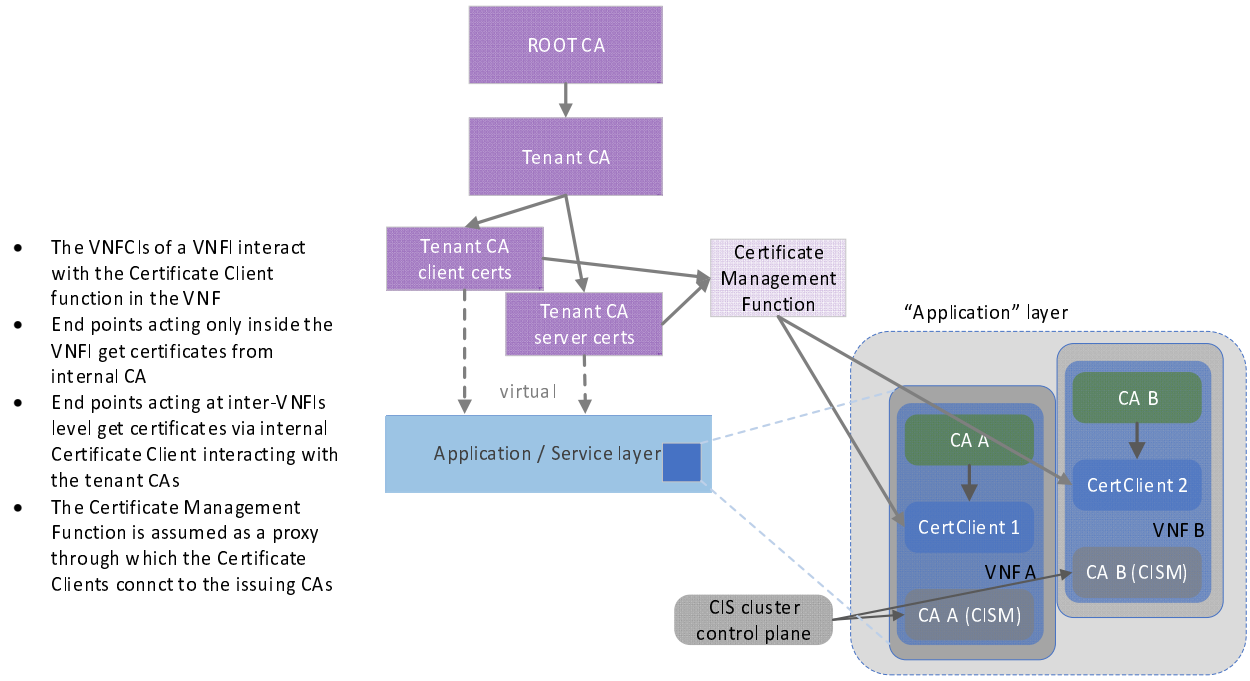

Figure 10.5.4-1: Certificate Client and Certificate Management Function in cooperation to provide certificates

The following two functions are identified:

1) Certificate Client instantiated at CIS cluster level.

2) Certificate Management Function through which the Certificate Clients get certificates issued by a Tenant CA or sub-CAs.

The Certificate Client has the following roles:

- Handles certificate issuing for TLS secure communications at intra-VNFI layer (Figure 10.5.2-2). For example, the Certificate Client receives certificate signing requests and interacts with an internal-to-VNF CA, thus acting as an RA.

- Interacts with the Certificate Management Function for certificates needed to secure TLS external communications with peers outside the cluster namespace.

NOTE 4: A CIS cluster may have several Certificate Clients, e.g. one for "consumers" and another one for "producers".

The Certificate Management Function has the following roles:

- Acts as a proxy between tenant CA and Certificate Clients to coordinate and monitor life-cycle management of certificates at inter-VNFI layer (Figure 10.5.2-2).

- Automates the entity registration per VNF and configures their Certificate Clients.

NOTE 5: The Certificate Management Function can mediate the interactions with a Certificate Enrolement Server (e.g. EST Server or CMPv2).

11 Conclusion

The present document introduces four use cases related to the provisioning and managing of certificates. Based on the detailed analysis of these use cases, gaps are identified with reference to the existing specifications, while relevant recommendations are also proposed. These recommendations highlight the expectation to perform additional normative specification work and to update existing normative specification documents. The scope of analysis cover the following aspects:

1) Potential architectural options for the placement of Operator Certificate Enrolment Server within the NFV-MANO architecture highlighting the need to enhance the NFV-MANO reference points and functional blocks.

2) Information modeling analysis that highlights the gaps with respect to the NFV information model and runtime information.

Based on the above scope of analysis, recommendations have been derived that are grouped in the following four categories:

1) General recommendations focusing on higher-level and framework aspects.

2) Recommendations focusing on functional security aspects of the functional blocks identified in the NFV Architectural Framework.

3) Recommendations on the definition and specification of interfaces on each reference points and/or interfaces.

The proposed recommendations encompass the identification of potential new requirements, which should form the basis of the development of a new normative specification, while filling the gaps in the existing ones.

History

Document history		
V1.1.1	January 2019	Publication
V1.2.1	July 2021	Publication