ETSI GR NFV-SEC 005 V1.1.1 (2019-01)

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

DGR/NFV-SEC005

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

This Group 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] ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[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] ETSI GS NFV-SWA 001: "Network Functions Virtualisation (NFV); Virtual Network Functions Architecture".

[i.7] ETSI GS NFV-INF 001: "Network Functions Virtualisation (NFV); Infrastructure Overview".

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

[i.9] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[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] IETF RFC 4809: "Requirements for an IPsec Certificate Management Profile".

[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)".

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

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
CSR	Certificate Signing Request
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.

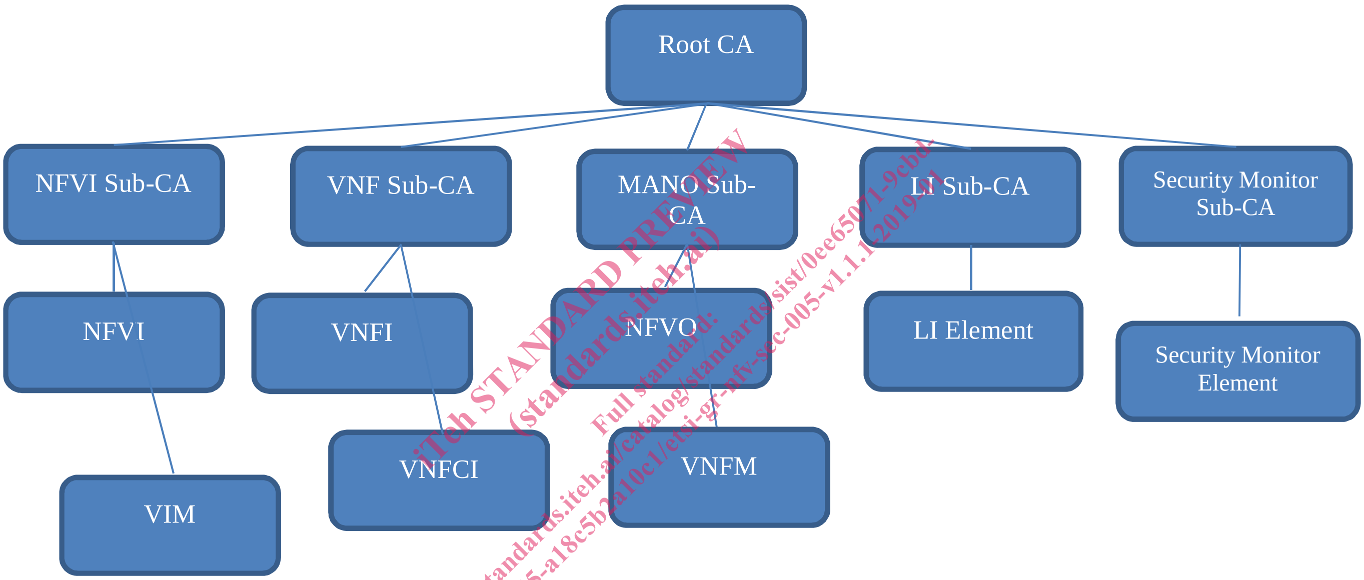

Figure 4.2.0-1: ETSI NFV PKI Certificate Hierarchy

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 identify, 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.

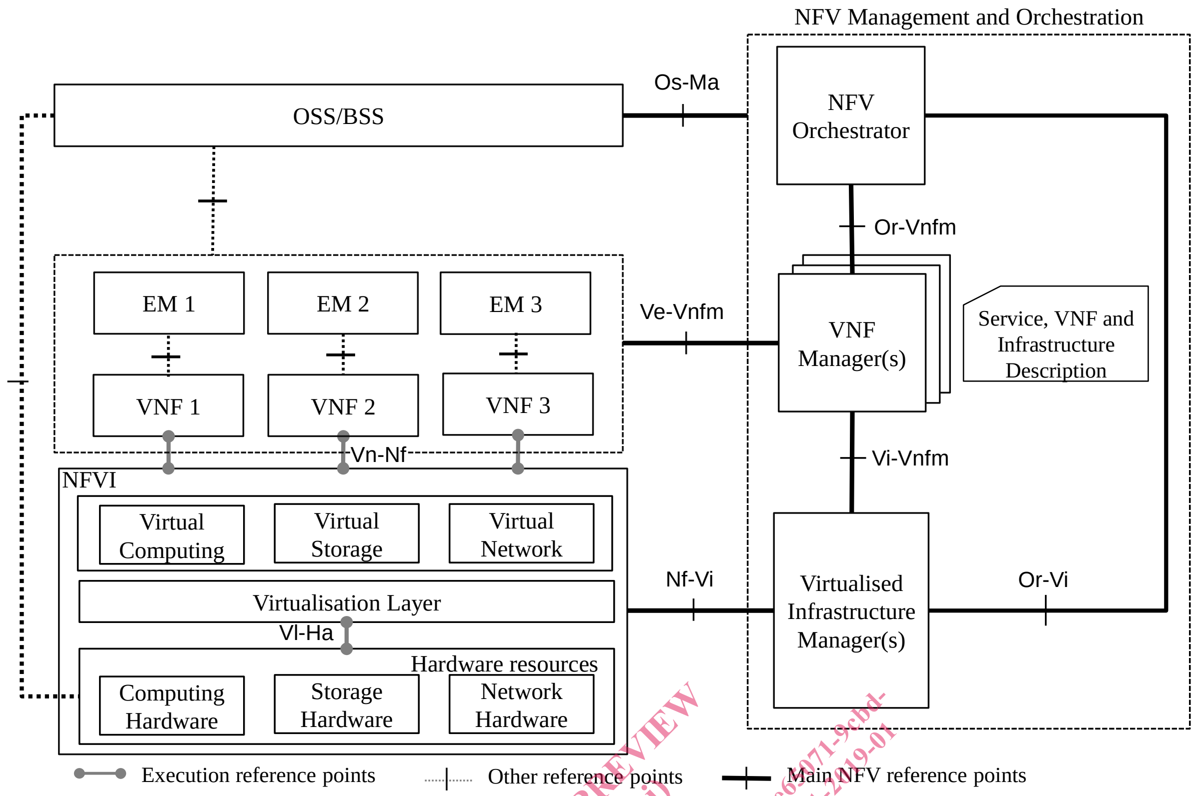

Figure 4.3-1: NFV reference architectural framework

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.17]).

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	VMF-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	Network Function
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 principals to each of the reference points implemented in NFV. The security principals addressable by PKI including 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 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.