ETSI GS NFV-SEC 025 V1.1.1 (2026-04)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV);
Security;
Secure End-to-End VNF and NS management specification

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/NFV-SEC025

Keywords
access control, cybersecurity, NFV, NFVI, security, trust

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Executive summary

The present document defines detailed security requirements and capabilities to enable secure end-to-end management of Virtualized Network Functions (VNFs) and Network Services (NS). It includes provisions for attestation of the NFV system, secure configuration, mobility and scalability of VNFs, considering multi-tenant environments, and supports both VM and container-based architectures to ensure robust security throughout the NFV lifecycle.

1 Scope

The present document defines the capabilities to enable a secure End-to-End management of VNF and NS, starting from the VNF/NS on-boarding, instantiation and configuration, mobility scalability during the run time and termination of VNF/NS.

For this aim, the present document includes in particular:

- Detail security requirements and capabilities that are candidates for the enhancement of the NSD and VNFD.
- Definition of the attestation for the entire NFV system (including the multi-tenant case) and the VNF use of attestation to assess the security level and capability of the NFVI platform and NFV-MANO.
- Mobility and scalability of VNFs that are pinned by hardware (e.g. HMEE, HSM).
- The secure configuration of VNFs, including the key pair injection.
- Memory allocation for sensitive VNFs.

Both VM and OS container architectures will be considered.

2 References

2.1 Normative references

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

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

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

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

[1] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

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

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

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

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

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

[7] ETSI GS NFV-SOL 013: "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; Specification of common aspects for RESTful NFV MANO APIs".

[8] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[9] ETSI GS NFV-SEC 022: "Network Functions Virtualisation (NFV) Release 4; Security; Access Token Specification for API Access".

[10] ETSI GS NFV-SEC 023: "Network Functions Virtualisation (NFV) Release 5; Security; Container Security Specification".

[11] OASIS KMIP SPEC: "Key Management Interoperability Protocol Specification Version 2.1".

[12] ETSI GS NFV-SEC 020: "Network Functions Virtualisation (NFV); Security; Identity Management and Security Specification".

[13] ETSI GS NFV-SEC 024: "Network Functions Virtualisation (NFV) Security; Security Management Specification".

[14] OASIS PKCS #11 SPEC: "Cryptographic Token Interface Base Specification" Version 3.1.

[15] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[16] ISO/IEC 27001:2022: "Information security, cybersecurity and privacy protection — Information security management systems — Requirements".

[17] NIST SP 800-53 Rev. 5: "Security and Privacy Controls for Information Systems and Organizations".

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

[19] IETF RFC 9711 "The Entity Attestation Token (EAT)".

[20] ETSI GS NFV-SEC 026: "Network Functions Virtualisation (NFV) Release 5; Security; Isolation and trust domain specification".

2.2 Informative references

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

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

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

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

[i.2] ETSI GS NFV-SEC 006: "Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns".

[i.3] "ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G)", November 2019.

[i.4] NIST SP 800-125: "Guide to Security for Full Virtualization Technologies", January 2011.

[i.5] NIST SP 800-125A Rev1: "Security Recommendations for Server-based Hypervisor Platforms", June 2018.

[i.6] NIST SP 800-125B: "Secure Virtual Network Configuration for Virtual Machine (VM) Protection", March 2016.

[i.7] Fraunhofer AISEC report: "Threat analysis of container-as-a-service for network function virtualization", November 2017.

[i.8] 5G Americas: "The Evolution of Security in 5G: A "slice" of Mobile Threats", July 2019.

[i.9] ETSI NFV FVI Platform Capability Registry.

[i.10] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; VNF Descriptor and Packaging Specification".

[i.11] ETSI GS NFV-IFA 014: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Network Service Templates Specification".

[i.12] ETSI GR NFV-EVE 018: "Network Functions Virtualisation (NFV) Release 5; Evolution and Ecosystem; Report on Multi-tenancy in NFV".

[i.13] ENISA: "NFV Security in 5G: Challenges and Best Practices" 2022.

[i.14] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV) Release 4; Security; VNF Package Security Specification".

[i.15] ETSI GS NFV-SOL 004: "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; VNF Package and PNFD Archive specification".

[i.16] ETSI GS NFV-SOL 007: "Network Functions Virtualisation (NFV) Release 4; Protocols and Data Models; Network Service Descriptor File Structure Specification".

[i.17] ETSI GR NFV-IFA 039: "Network Functions Virtualisation (NFV) Release 5; Architectural Framework; Report on Service Based Architecture (SBA) design".

[i.18] SPIFFE: Universal identity control plane for distributed systems; CNCF Incubating Project.

[i.19] SPIRE: About SPIRE; CNCF Incubating Project.

[i.20] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310 version 18.5.0 Release 18)".

[i.21] ETSI GR NFV-SEC 018: "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".

[i.22] NIST FIPS 140-2 Security Requirements for Cryptographic Modules, May 2001.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

API authorization server: logical function that implements the authorization server functionality as defined in IETF RFC 6749 [8] as a standalone physical server or logical entity

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AMF	Access and Mobility Function
API	Access Point Identifier
CA	Certification Authority
CIR	Container Image Registry
CIS	Container Infrastructure Services

CISM	Container Infrastructure Service Management
CPU	Central Processing Unit
CSP	Certification Service Provider
DF	Deployment Flavour
DPU	Data Processing Unit
DRTM	Dynamic Root of Trust for Measurement
EM	Element Manager
GPU	General Purpose Processor
HBRT	Hardware Based Root of Trust
HMEE	Hardware Mediated Execution Enclave
HRoT	Hardware Root of Trust
HSM	Hardware Security Module
ID	Identity Document
IoT	Internet of Things
JSON	JavaScript Object Notation
KMIP	Key Management Interoperability Protocol
LCM	Life Cycle Management
LoA	Level of Assurance
MCIOP	Managed Container Infrastructure Object Package
MNO	Mobile Network Operator
NEF	Network Element Function
NFVI	Network Function Virtualisation Infrastructure
NFVO	Network Functions Virtualisation Orchestrator
NIC	Network Interface Card
NRF	Network Repository Function
NS	Network Service
NTP	Network Time Protocol
NUMA	Non Uniform Memory Access
OAM	Operations, Administration, and Maintenance
OSS	Operations Support Systems
PCF	Policy Control Function
PKCS	Public Key Cryptographic Standard
PoP	Point of Preference
PTP	Precision Time Protocol
PVID	Primary Verifiable Identity Document
RA	Registration Authority
RBAC	Role Based Access Control
RoT	Root of Trust
SLA	Service-Level Agreement
SM	Security Manager
SUE	System Under Evaluation
TLS	Transport Layer Security
TPM	Trusted Platform Module
TVRA	Threat Vulnerability and Risk Analysis
UDM	Unified Data Management
UDR	User Data Repository
UDSF	Unstructure Data Storage Function
UE	User Equipment
URI	Uniform Resource Identifier
VBS	Virtual Block Storage
VID	Verifiable Identity Document
VIM	Virtualised Infrastructure Management
VL	Virtual Link
VM	Virtual Machine
VNF	Virtualised Network Function
VNFC	Virtualised Network Function Component
VNFCI	Virtual Network Function Component Instance
VNFD	Virtualised Network Function Descriptor
VNFI	Virtual Network Function Infrastructure
VNFM	Virtualised Network Function Manager

4 Threat analysis for VNF/NS during their lifecycle

4.1 Introduction

Before analysing the way to protect the NS and the VNF during their lifecycle, it is important to identify the threats affecting the NS and the VNF.

For this identification of threats, it is essential first to know the critical assets of NS and VNF (clause 4.2), consisting of anything that has value for an organization (for business or to fulfil legal obligations) and needs to be protected, and secondly to identify the threat agents (clause 4.3), the entities that can adversely act on the asset.

During the lifecycle of the VNF or NS, the list of assets evolves, including, during the on-boarding, the information contained in the VNF package and adding later some identifiers, cryptographic keys and runtime environment when it is instantiated, and then adding the data, monitoring data, generated during the run-time.

The associated threats for each of the lifecycle steps are identified in clause 4.4.

This threat analysis uses the TVRA method described in ETSI TS 102 165-1 [i.1] and the format found in the annex A of ETSI GS NFV-SEC 006 [i.2].

4.2 Assets

4.2.1 NS Assets

At the NS level, the network topology, describing constituents of the NS, their communication links, their affinity or anti-affinity rules is an important asset. For example, the use of an out-of-date version of a VNF that is part of the NS, and including a security threat in its software, could have an impact on the NS security; protection of the identification of the constituents of the NS is needed.

In the same way, the affinity/anti-affinity rules may be used to group the sensitive VNFs together to run in an NFVI-PoP protected with a high level of protection. These rules also need to be protected.

The priority description defines the priority in case of congestion on the underlying physical links and is used to resolve conflicts in case of resource shortage. This priority information needs to be protected to ensure that resources for critical communications are not pre-empted during resource allocation.

Monitoring data, such as metrics, measurements and events, is also information that shall be protected.

And the LCM scripts associated with some events are also some assets to be protected as they have an impact on the orchestration of the NS when an event is raised. Modification in the scripts may have an impact on, e.g. the NS service continuity.

The service provider may have legal obligations to fulfil e.g. provide a network service on a slice with a service level agreed with his customer. The SLA is an asset that the service provider needs to protect (e.g. bandwidth, latency, availability).

The NS Assets mapping depicted in figure 4.2.1-1 lists the identified assets at the NS level.

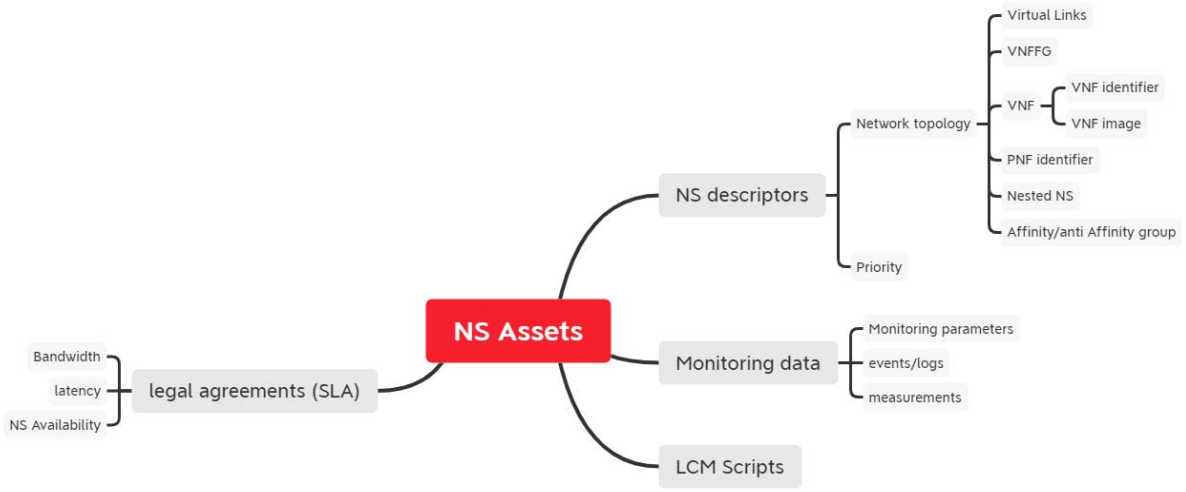

Figure 4.2.1-1: NS Assets map

4.2.2 VNF Assets

At the VNF level, the VNF Package contains some assets to be protected, e.g. some descriptors, the software, the manifest files and non-MANO artefacts files, the LCM scripts associated to some events.

After instantiation of the VNF there are some sensitive parameters that shall be protected, e.g. cryptographic keys, VNF instance identity, security policies, data associated to the VNF for the license management and enforcement (e.g. Service Provider Id).

Some data related to the service-based architecture are also some sensitive data, e.g. the VNF registration information, access policies and access token used to control access to the API of the VNF.

After instantiation, the VNF instance with the guest OS, libs, the virtual links, the VNFC instance included in the VNF instance, the security and configuration parameters need to be protected.

The VNF data used for the attestation process, such as the VNF integrity measurement and integrity golden measurement that are used by the attestation server to check the integrity of the VNF software, are also assets.

Some VNFs use as input a time clock reference, timestamping or location information that need to be trustable information (e.g. digital signing and certificate verification, license enforcement, timestamping of events, lawful Interception). Any manipulation of time reference invalidates signing processes, certificate validation and exposes organizations to compliance problems, legal challenges and compromise the security of the NFV system. Time reference, timestamping information and location are assets for the VNF.

During the run-time of the VNF, the sensitive application data generated by the application stored in the permanent storage or in transit, the lawful interception data, the VNF monitoring information (e.g. metrics, measurements, events) and the VNF instance states are also important assets that shall be protected.

Examples of such sensitive application data are:

- Subscriber data managed by UDM and UDR Network Functions
- Policy data managed by PCF and UDR Network Functions
- Exposure function data managed by NEF and UDR Network Functions
- Application data, such as those managed by NEF and UDR Network Functions
- UE Context managed by AMF and UDSF Network Functions

The VNF Assets mapping depicted in figure 4.2.2-1 lists the identified assets at the VNF level.

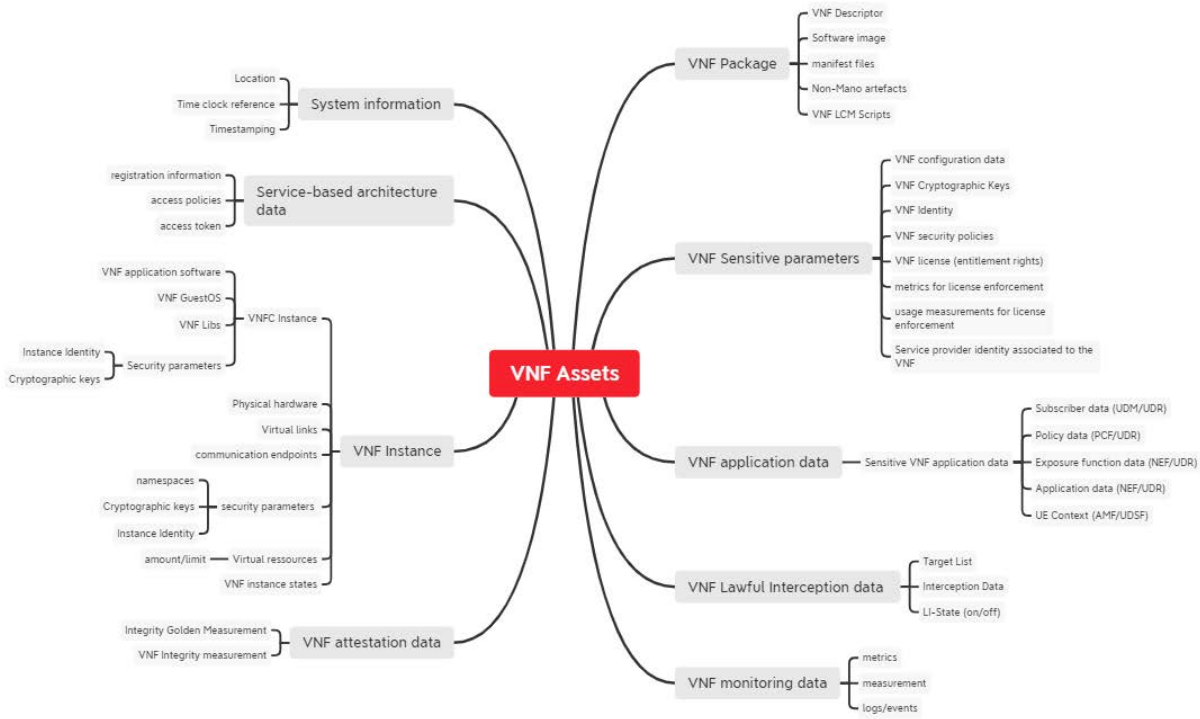

Figure 4.2.2-1: VNF Assets map

4.3 Threat agents

A list of threat agents for the 5G network landscape is given in clause 6 of the ENISA Threat landscape for 5G networks [i.3]. These threat agents apply also for the NFV environment. The threat agents groups in this report are the following:

- Cyber criminals
- Insider including employees (own, third parties)
- Hostile state actors
- Hacktivists
- Cyber warriors
- Cyber-terrorists
- Corporations
- Script Kiddies
- Inadvertent attacker

The means by which these threat agents attack the system have evolved, and they may use powerful Cyber Threat Intelligence based on Artificial Intelligence to attack the NFV system. The threat agent may have legitimate access to the network that could facilitate the attack.

The 5G infrastructure that will be used by various applications with a critical and vital impact on society, will concentrate the efforts of the cyber-criminals and cyber-terrorists.

The 5G has a great importance to the sovereignty of the nation-states and then will be the target of attacks sponsored by states, and in particular in a situation of cyber war. A hostile state actor may even instrument the attack at the physical layer, influencing 5G component manufacturers to introduce backdoors into their designs.

Table 4.3-1 lists the threat agents and, for each, describes the target, motivation and capabilities of the threat agent. The table also gives a link to the associated threats described in clause 4.4.

Table 4.3-1: Threat agents list

Threat agents			
Item	**Threat-Agent name**	**Description (Target/motivation/capabilities)**	**Associated Threats**
Threat-Agent.1	Cyber criminals	Target: Industries, government, operators, organizations, individuals. The 5G networks will connect various industries and governments that are the target of the cyber criminals. Attacks towards the Network virtualization system of operator to enter the various target is a possible channel to reach their goal. The cyber criminals have legitimate access to the network that could ease their attack. Capabilities: The cyber criminals may use a very powerful system (e.g. using artificial intelligence).	
Threat-Agent.2	Insider, including employees (own or 3rd parties)	Target: Industries, organizations, operators. The insider may be paid by another organization to mount some attacks using their knowledge and their access to the system. The number of insiders may be important due to the number of 3rd parties involved in the 5G system (VNF providers, Infrastructure manufacturers, component designers, etc.). Capabilities: The threat agent uses his knowledge of the system and his legitimate access to the system.	
Threat-Agent.3	Hostile state actor	Target: other country for economic or political reasons, Industries. The motivation of the nation-states' agents is mostly espionage against other countries. The nation-state may influence third parties involved in the network system (e.g. component designers) to instrument their products for this espionage. Capabilities of the hostile state actor are significant and may use a very powerful system (e.g. using artificial intelligence).	
Threat-Agent.4	Hacktivists	Target: Industries, organizations, operators. The motivation of hacktivists is to draw attention to their cause that are in general protestation against political or geopolitical decisions affecting national or international matters. They are active in disclosing some confidential information involving their target. Capabilities are in general relatively low as they belong to associations that are not motivated by the monetization in their attacks. But they are able to gain a legitimate access to the network which could ease the attack.	Threats:
Threat-Agent.5	Cyber warriors	Target: Other country for geopolitical reasons. The cyber wars is the new way the states is using to maintain their dominance, independence and sovereignty. The soldiers will use the 5G networks for their missions, increasing the attractiveness of this technology as a target of attacks and positioning the 5G network as a high critical infrastructure to protect. The cyber warriors have both the defender and offender roles. Capabilities of the nation state are significant and may use very powerful system (e.g. using artificial intelligence).	

Threat agents			
Item	**Threat-Agent name**	**Description (Target/motivation/capabilities)**	**Associated Threats**
Threat-Agent.6	Cyber terrorists	Target: individuals, industry. The 5G infrastructure is used by a vast amount of applications with a critical and vital impact on the society. For example in the autonomous driving, an attack on the system could be setup remotely to cause accidents with vital impact on individuals. An attack also on energy supplier infrastructure may cause also large damage at the national level. Capabilities of the terrorist organizations may be important.	
Threat-Agent.7	Corporation	Target: other corporation (industries, operators, etc.). The main motivation of such threat agent is economical and the competiveness, tracking new services deployed by competitors and a potential use of patents. Capabilities could be important but balanced with the benefit derived. The Threat agent use his high knowledge of the system to mount the attack.	
Threat-Agent.8	Script Kiddies	Target: operators, application providers. The main motivation of this threat agents is gaining a free access to resources (e.g. gaming). The attack is set-up on the devices that the threat agent owned at home (IoT devices, mobile phone, etc.). Capabilities are low but the threat agent has a legitimate access to the network and can mount the attack on his personal device at home.	
Threat-Agent 9	Inadvertent attacker	Target: any exposed system element. Devoid of motivation, but takes an action that somehow damages a part of the system (e.g. switches off a power source or damages a cable).	
Threat-Agent 10	Physical external event	This agent may be natural, such as flooding or any other threat of physical "force majeure" including geological/extreme weather/exceptional physical natural events or may be other presence of other high risks industries in the physical vicinity of the NFV system (e.g. Oil or Gas). Target: any exposed system element. Capability of creating damages to all or a part of the system without any intention of doing so.	

4.4 Threats

4.4.1 Introduction

The complexity and the extension of attack surface of a virtualized environment increase the difficulty to list, in an exhaustive manner, the security threats to which the NS/VNF assets are exposed during the lifecycle of NS/VNF. For this activity of threat analysis, some reports have been used to help the identification of the largest number of these threats:

- ENISA Threat Landscape [i.3]
- NIST SP 800-125 [i.4]
- NIST SP 800-125Ar1 [i.5]
- NIST SP 800-125B [i.6]
- Fraunhofer AISEC report [i.7]

- 5G Americas [i.8]

Only threats concerning the VNF and NS in an NFV environment have been listed. They have been sorted with the lifecycle steps concerned by the threat:

- VNF/NS on-boarding
- VNF instantiation
- VNF configuration
- VNF during run-time
- VNF termination

The threats are listed in tables, where the threat is named and described, the corresponding threat agents are listed and the assets concerned by the threat are identified. Then the last column of the tables gives a link in the document to the possible requirements to mitigate the threat.

4.4.2 VNF/NS on-boarding

Table 4.4.2-1 lists the threats on VNF/NS assets during the on-boarding of VNF/NS. For further details, see clause 5 of the present document.

Table 4.4.2-1: Threats during VNF/NS on-boarding

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
On-boarding -Threat 1	A threat agent gains access to the Os-ma-nfvo interface and on-boards a malicious VNF in NFV-MANO. This VNF could be used to attack the other VNF or NFVI and/or gain access to sensitive data.	Cyber criminals, insiders, cyber warriors, cyber terrorists, hostile state actors, hacktivists, corporations, script kiddies	VNF application data, VNF sensitive parameters, VNF lawful interception data, some VNF Instance assets	Verify the operation of the VNF in a sandboxed, firewalled lab before allowing the operation of the VNF.
On-boarding -Threat 2	A threat agent gains access to the Os-ma-nfvo interface and uploads a malicious VNF as a new version of a VNF constituent of a legitimate NS. This VNF is used to attack the other VNF in the same namespace/security domain and/or gain access to sensitive data.	Cyber criminals, insiders, cyber warriors, cyber terrorists	Some VNF instance assets including guestOS, libs, VNF application data, VNF sensitive parameters	Vendor and Operator Signed VNF package.
On-boarding -Threat 3	A threat agent acting as an operator gains access to the Os-ma-nfvo and on-boards a malicious NS containing malicious VNFs that will attack the network functions of other tenants.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation	VNF application data, VNF sensitive parameters, VNF lawful interception data, some VNF Instance assets	Isolation and roles (RBAC) between tenants, orchestration and on-boarding is required.

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
On-boarding -Threat 4	A threat agent acting as a man in the middle on the Os-Ma-Nfvo interface and e.g. prevents the VNF software update to exploit a known security flaw in the VNF software.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Inadvertent attacker	VNF application data, VNF sensitive parameters, VNF lawful interception data, some VNF Instance assets	End to end encryption and authentication of API.
On-boarding -Threat 5	Malicious entity in NFV-MANO that gains access to the NS and VNF Descriptors. This attack could be through inclusion of concealed software within legitimate NFV-MANO itself. Some example of attacks may be: • Other corporation could have access to network topology of a competitor and track new services deployed by this competitor. • An attacker may change the NS descriptor and substitute a VNF by a malicious one that will further attack the other VNF or sensitive data. • The attacker may change the priority of the NS to perform DoS attacks • The attacker may change the NS/VNF LCM scripts and provoke damage on the service (e.g. disruption of the service).	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation, Hostile state actor	Network topology, priority, NS LCM scripts, VNF Package assets, NS SLA	Isolation and roles (RBAC) between tenants, orchestration and on-boarding is required. Vendor and Operator Signed VNF package.
On-boarding -Threat 6	Malicious entity in NFV-MANO that gains access to the software image registry. This attack could be through inclusion of concealed software within legitimate NFV-MANO itself. Malicious access to the registry could be a read access or read/write access, deletion of the registry. Example of attacks may be: • Injection of malicious image or modification of legitimate VNF software image that could result in an attack on other VNF instances. • An attacker may use a read access to the registry to find exploitable security flaw in the software to perform additional attack. • DoS attack.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation, Script kiddies	VNF Software image, other VNF instance assets	Isolation and roles (RBAC) between tenants, orchestration and on-boarding is required. Vendor and Operator Signed VNF package.
On-boarding -Threat 7	Privileged user abuse with access to the software image registry.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation	VNF Software image, other VNF instance assets	Access control to the registry, multi factor token for critical operations.
On-boarding -Threat 8	Malicious entity in NFV-MANO that gains access to the VNF Package integrity verification process to bypass this verification. This attack could be through inclusion of concealed software within legitimate NFV-MANO itself. This attack allows the on-boarding of VNF packages that have been modified and that may contain malicious software, or modified descriptors.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation	Network topology, priority, NS LCM scripts, VNF Package assets, other VNF instance assets, NS SLA	Access control to NFV-MANO, multi-factor token for critical operations. Verification process to be executed within an HMEE.
On-boarding -Threat 9	Compromised private keys and algorithms used for code signing due to poor key protection/management/design which would undermine the security of code signing process.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation	VNF Software image, other VNF instance assets	Signing keys held within an HSM.

4.4.3 VNF instantiation

Table 4.4.3-1 lists the threats on VNF assets during the instantiation of VNF. For further details, see clause 6 of the present document.

Table 4.4.3-1: Threats during VNF instantiation

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Instantiation.1	Malicious VIM that counterfeit a legitimate one and instantiate malicious VNFs, misconfigures the VNF (e.g. misconfiguration of its security domain). This attack could be through inclusion of concealed software within legitimate VIM. This attack allows the instantiation of malicious VNFs that will attack legitimate VNFs sharing the same NFVI.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF application data, VNF sensitive parameters, VNF lawful interception data, some VNF Instance assets	
Instantiation.2	Malicious VIM that allocates virtual resources for fake instances, abusing the cloud computational resources of the NFVI and provoking DoS attacks to other Network functions sharing the resources.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF Instance virtual resources, NS SLA	
Instantiation.3	Malicious Identity provider for the VNF instances, able to reuse the same identity for several VNFs over time with the same key pair without knowledge or authorization of MANO. A malicious VNF instance is able to abuse the authentication process and interact with other network functions.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF application data, VNF sensitive parameters, VNF lawful interception data, some VNF Instance assets	
Instantiation.4	Malicious attacker abuses privileged user account and accesses to the VNF instances Identity registry allowing a malicious VNF instance to abuse the authentication process.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF application data, VNF sensitive parameters, VNF lawful interception data, some VNF Instance assets	
Instantiation.5	Malicious NFVI that counterfeit legitimate one and instantiate a malicious VNF image, GuestOS or Libs. This attack could be through inclusion of concealed software within legitimate NFVI.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF application data, VNF sensitive parameters, VNF lawful interception data, some VNF Instance assets	
Instantiation.6	Malicious NFVI that allocates virtual resources for fake instances, abusing the cloud computational resources of the NFVI and provoking DoS attacks to other Network functions sharing the resources.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF Instance virtual resources, NS SLA	
Instantiation.7	Malicious Authorization server or inclusion of concealed software within the legitimate Authorization server that is able to modify the access control policies to API and allows API access to malicious entities. Access to the API allows the malicious entities to have access to VNF sensitive parameters and sensitive VNF application data.	Cyber criminals, insiders, cyber warriors, cyber terrorists	Service-based architecture data assets, VNF sensitive parameters, sensitive VNF application data, lawful Interception data	

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Instantiation.8	Malicious entity in MANO that uses e.g. Privileged user abuse and gains access to the service-based architecture registry and modifies the e.g. API access policies or counterfeit the registration server.	Cyber criminals, insiders, cyber warriors, cyber terrorists	Service-based architecture data assets, VNF sensitive parameters, sensitive VNF application data, lawful Interception data	
Instantiation.9	Malicious Attestation server that accepts illegitimate VNFs to be instantiated or accepts malicious NFVI software, allowing these illegitimate software to launch other attacks.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets	
Instantiation.10	Compromised private keys used by attestation server due to poor key protection/management which would undermine the security of attestation process.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets, NS SLA	
Instantiation.11	Malicious Attestation server that systematically rejects the attestation report and provoke an outage in the network.	Cyber criminals, insiders, cyber warriors, cyber terrorists	NS SLA, VNF sensitive parameters	
Instantiation.12	Malicious entity using e.g. Privileged user abuse and gains access to integrity golden measurements registry. It could result in the positive verification of an illegitimate VNF or the rejection of legitimate VNF.	Cyber criminals, insiders, cyber warriors, cyber terrorists	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets, NS SLA	
Instantiation.13	Inclusion of concealed hardware or software in the low layers of NFVI that counterfeit the RoT for measurement and/or the RoT for reporting of the attestation process.	Insiders, Hostile state actor	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets, NS SLA	
Instantiation.14	Exploitation of hardware or software vulnerabilities in the RoT for measurement and/or the RoT for reporting of the attestation process.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Hostile state actor	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets, NS SLA	

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Instantiation.15	Exploitation of hardware or software vulnerabilities in NFVI computing resources to instantiate illegitimate software that will mount side channel attacks on sensitive network functions (e.g. in HMEE).	Cyber criminals, insiders, cyber warriors, cyber terrorists, Hostile state actor	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets	
Instantiation.16	Exploitation of software vulnerability in hypervisor and/or CIS that allows a malicious VNF to be instantiated in the same security domain of another legitimate VNF owned by another tenant.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Hostile state actor	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets, NS SLA	
Instantiation.17	Exploitation of software vulnerability in VIM and/or CISM that allows a malicious VNF to be instantiated in the same security domain of another legitimate VNF owned by another tenant.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Hostile state actor	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets, NS SLA	

4.4.4 VNF configuration

Table 4.4.4-1 lists the threats on VNF assets during the configuration of VNF. For further details, see clause 7 of the present document.

Table 4.4.4-1: Threats during VNF configuration

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Config.1	Privileged user abuse with access to the configuration parameters registries (e.g. Cryptographic keys, security parameters, Identities, etc.).	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	VNF sensitive parameters assets	
Config.2	Compromised authentication private keys due to poor protection/management which would undermine the authentication process of VNFs, VNFM, VIM, NFVO.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	VNF cryptographic keys	
Config.3	Malicious VNFM that gains access to configuration parameters, LCM scripts, and misconfigures the VNF through the EM, runs malicious LCM scripts.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	Some VNF Instance assets, VNF application data, VNF sensitive parameters	

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Config.4	Malicious entity acting as a man in the middle between VNFM and VNF/EM to get access to configuration parameters.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	Some VNF Instance assets, VNF application data, VNF sensitive parameters	
Config.5	Malicious entity acting as a man in the middle between NFVI and VIM to get access to sensitive configuration parameters (e.g. cryptographic keys, VNF Identity, etc.)	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	VNF Instance security parameters, VNF sensitive parameters	
Config.6	Malicious entity acting as a man in the middle between NFVI and SM to change sensitive configuration parameters (e.g. Lawful Interception data).	Cyber criminals, insiders, cyber terrorists, hostile state actor	VNF lawful interception data, VNF sensitive parameters	
Config.7	When hypervisor is used to provision the public/private key pairs in the VNF/VNFC instances, a malicious NFVI/hypervisor has access to the private key and may process a leakage of this private asymmetric key (with associated public key). This attack could be through inclusion of concealed software within legitimate NFVI. The private/public key pair may be used by an illegitimate VNF to pass off as a legitimate one, connect to a VNF and get some sensitive data from it.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	VNF cryptographic keys, VNF application data, VNF sensitive parameters	
Config.8	Use of a weak algorithm which would undermine the authentication process of VNFs, VNFM, VIM, NFVO, etc.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	VNF cryptographic keys	

4.4.5 VNF during run-time

Table 4.4.5-1 lists the threats on VNF assets during run-time. For further details, see clause 8 of the present document.

Table 4.4.5-1: Threats during VNF run-time

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Runtime-1	Inclusion of concealed or unauthorized software in NFVI to gain access to the boot procedure and to launch other malicious software (e.g. illegitimate hypervisor, drivers, API) that could be used for further attacks on the VNFs and sensitive data.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters, NS SLA	

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Runtime-2	Inclusion of concealed or modified hardware in NFVI to exploit hardware/software vulnerabilities and to mount attacks on sensitive data (e.g. secure enclaves).	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters, NS SLA	
Runtime-3	Malicious VNF, that gains access to physical/logical storage at rest of other legitimate VNFs and extracts sensitive information (e.g. Authentication, authorization and accounting credentials), that it is not authorized to have.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF application data, VNF lawful Interception data, VNF sensitive parameters,	
Runtime-4	Malicious VNF, that gains access to physical/logical storage at rest of other legitimate VNFs and modifies some data to provoke a failure.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters, NS SLA	
Runtime-5	Malicious VNF, that gains access to physical/logical storage at rest of other legitimate VNFs to change the access control policies at the application level e.g. NRF data. Accessing to the SBA registration data (NRF data and registry) allows an attacker to registered malicious VNF in the core network that will further access to sensitive assets or allows the attacker to expose malicious APIs.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters, NS SLA	
Runtime-6	Malicious software in the NFVI that abuses the computational resources and causes the DoS attacks.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation	NS SLA	
Runtime-7	Malicious software in the NFVI that exploits hypervisor vulnerability to gain access, to trespass slice and VNF isolation and disclose data from other tenants.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters, NS SLA	

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Runtime-8	Malicious entity in the VIM that manipulates the resources orchestration for the VNFs and compromises the network function or slices separation and compromises the priorities of network services.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, inadvertent attacker	NS SLA	
Runtime-9	Malicious or misconfigured/buggy VNF that is able to communicate to other legitimate VNF and floods the communication link with requests that compromise the availability of the legitimate VNF and provoke localized saturation of the network.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, inadvertent attacker	NS SLA	
Runtime-10	Malicious VNF or injection of concealed software in NFVI that gains access to the network traffic and is able to mount a traffic sniffing attack on the data in transit and gain access to sensitive information.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters	
Runtime-11	Malicious software in NFVI gains access to the network traffic and is able to modify/falsify/inject data in transit.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters, NS SLA	
Runtime-12	Malicious software in the NFVI, VIM, SM gains access to the monitoring data for listening to sensitive MNO data or modifying them to create a failure in the network management system.	Corporation, insiders, cyber terrorists, hostile state actor	VNF monitoring data, VNF lawful Interception data, NS SLA	
Runtime-13	Malicious software in NFVI that modifies the license entitlement rights for a VNF to gain a perpetual right or extend the entitlement rights to the VNF software or conversely remove license entitlement rights or provoke additional requests for new license entitlement rights.	Corporation	VNF Licenses, NS SLA	
Runtime-14	Injection of concealed software in NFVI that modifies data used for license enforcement (e.g. time, location, resource usage) to gain a perpetual right or extend the entitlement rights for a VNF or conversely decease license entitlement right or provoke additional requests for new license entitlement rights.	Corporation	VNF licenses, NS SLA	
Runtime-15	Malicious VNF or injection of concealed software in NFVI that gains access to security sensitive function (e.g. Lawful Interception) sensitive data, intercept these data during transit, modify the data during transit or at rest in the data storage.	Cyber terrorists, hostile state actor, insider	VNF Lawful Interception data, VNF application data, VNF sensitive parameters	

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Runtime-16	Exploitation of known security weakness in a network function.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters, NS SLA	
Runtime-17	Compromised private keys used by VNF due to poor key protection/management or weak algorithm which would undermine the security of VNF authentication or application processes.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF cryptographic keys	
Runtime-18	Abuse of administration rights of the NFVI or NFV MANO environment to get access to the management of the NFV environment, including the virtualization layer. Sensitive data of a legitimate VNF could leak to other illegitimate VNF.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters	
Runtime-19	VNF that monopolises the virtual resources of a host reducing the availability for other VNFs that share the physical resources (due to poor VNF resources segregation).	Corporation, insiders, cyber terrorists	NS SLA, VNF instances resources	
Runtime-20	Malicious software that gain access to the VNF states storage during VNF move or resilience, and is able to modify the state of this VNF.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF States, NS SLA	
Runtime-21	unintended mis-configuration of the VNF instance that undermine the VNF processes	Inadvertent attacker	VNF application data, VNF sensitive parameters, NS SLA	
Runtime-22	External attack from malicious devices such as IoT device or smartphone, that cause excessive access requests to the network and create an overload of some VNFs resources.	Cyber criminals, insiders, cyber warriors, cyber terrorists, hacktivists, corporation, script kiddies, inadvertent attacker, hostile state actor	NS SLA	
Runtime-23	Attacker that is able to activate a licensed feature inside one or more VNF.	Corporation, hostile state actor, cyber criminals, insiders	VNF Licenses	

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Runtime-24	Malicious software in NFVI or MANO that manipulates the system clock, time reference or timestamping information and invalidates the signing processes, certificate validation processes, license enforcement processes and timestamping of events.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actor	VNF application data, VNF licenses, time clock reference, timestamping	
Runtime-25	Malicious software in NFVI or MANO that manipulates the geo-location information and invalidates e.g. the license enforcement processes and exposes lawful interception system to compliance and legal problems.	Cyber criminals, insiders, cyber warriors, cyber terrorists, corporation, hostile state actors	VNF application data, VNF licenses, VNF lawful Interception data, location	
Runtime-26	Malicious software in NFVI or MANO that manipulates the service provider Identity associated with the VNF and invalidates the license management enforcement process for the licenses locked to this service provider.	insiders, corporation	Service Provider ID, VNF licenses	

4.4.6 VNF termination

Table 4.4.6-1 lists the threats on VNF/NS assets when VNF is terminated or for any VNF that has released resources e.g. after a move or a scaling process. For further details, see clause 9 of the present document.

Table 4.4.6-1: Threats during VNF termination or releasing of VNFI resources

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Termination-1	A malicious VNF is instantiated in NFVI to access to data not erased from a terminated VNF or any VNF that has released resources. Data could include application data, cryptographic keys.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation, Hostile state actor	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters	
Termination-2	Abuse of resource allocation in VIM or NFVI to allocate to a malicious VNF the virtual resources released from a terminated VNF or from a VNF that has released resources after a move or a scaling process.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation, Hostile state actor	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters	
Termination-3	Inclusion of concealed software in NFVI to prevent the deletion/erasure of data and states of the VNF that has been terminated.	Cyber criminals, insiders, cyber warriors, cyber terrorists, Corporation, Hostile state actor	VNF Instance assets, VNF application data, VNF lawful Interception data, VNF monitoring data, VNF sensitive parameters	

4.4.7 Generic Threats

Table 4.4.7-1 lists the generic threats against VNF/NS assets.

Table 4.4.7-1: Generic Threats

Threat				
Item	**Description of threat**	**Threat Agent**	**Assets concerned**	**Mitigation Requirements**
Generic-1	Physical attacks on data centres or antennas, which will result in the unavailability of the network service	Hacktivist, Cyber terrorists, Hostile state actor, Physical external event	NS SLA, Physical hardware	Data Centre physical security should comply with international standards such as ISO/IEC 27001:2022 [16] & NIST SP 800-53 [17].
Generic-2	Exploitation of weak user authentication allowing abuse. This privileged user abuse could imply several threats during the VNF lifecycle steps (see threats during instantiation, configuration,…)	Cyber criminals, insiders, cyber warriors, cyber terrorists, Hostile state actor	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets	Use of certificate based authentication and multi-factor authentication.
Generic-3	Physical access to NFVI (especially in MEC environment) to inject malware or get access to sensitive data through physical interface ports (e.g. NIC, USB).	Cyber criminals, insiders, cyber warriors, cyber terrorists, Hostile state actor	VNF sensitive parameters, sensitive VNF application data, lawful Interception data, VNF instance assets	Data Centre physical security should comply with international standards such as ISO/IEC 27001:2022 [16] & NIST SP 800-53 [17]. Use of certificate-based authentication and multi-factor authentication.

5 VNF/NS On-boarding

5.1 Security requirements and capabilities in VNFD

5.1.1 NFVI Security capabilities

Some VNF providers make use of underlying NFVI platform capabilities in order to accelerate performance and optimize throughput of their VNF products. In order to ensure a proper instantiation and placement of the VNF by the VIM and ensure proper operation of the VNF, ETSI-NFV has defined:

- a way to describe the specific NFVI capability requirements in the VNF descriptor;
- a NFVI Platform Capability Registry [i.9], giving the capabilities of the underlying hardware infrastructure resources.

The registry is defined to specify capabilities that are generic to all NFVI platform components, and capabilities that are NFVI vendor specific.

Five categories has been specified in this registry: CPU, MEMORY, STORAGE, NETWORK, LOGICAL NODE.

In the same way, some VNF requires additional security features on the NFVI platform to operate properly ensuring an adequate level of security. The NFVI Platform Capability Registry may be extended to describe NFVI security capabilities, and the VNFD metadata may be extended to describe the specific security requirements for the VNF/VNFC.

Table 5.1.1-1 below gives the security features that could be required by a VNF or VNFC.

Table 5.1.1-1: security capabilities per categories

Category	Security Capability	Permitted values
CPU	HMEE	SGX, SEV, TDX, etc. version number
	Hyper-threading control (ON/OFF/Disallow)	
	Technology type	e.g. NUMA
	GPU	Type, version
MEMORY	Secure release	
STORAGE	Transparent encryption	Using Self key generation or external key
	Secure release	
NETWORK	Hardware encryption	
	Data Processing Unit (DPU)	
LOGICAL NODE	Localization group (datacentre, physical resources)	
VIRTUALIZATION LAYER	Syscall filtering	Seccomp
PLATFORM	Crypto-Accelerator	
	Key storage	
	Random generator entropy	
	Attestation	
	RoT	
	Time precision	NTP, PTP

It shall be possible to describe the security requirements in the VNFD at the VNF component level. Example one VNF with a VNFC for LI functionality that needs an execution in a HMEE. The other components running in classic Virtualization containers.

The security requirements of a VNF in the VNFD may be sensitive information that the VNF Provider want to keep confidential, and for which an integrity check is needed.

The security capability of an NFVI in the registry is also information that needs protection.

5.1.2 Affinity and anti-affinity rules

Some VNFs require specific isolation of a VNFC relative to other VNFCs and the placement of the VNFC by the VIM shall take into account such a requirement. Clause 6.2.5 of ETSI GS NFV-IFA 011 [i.10] gives a requirement for VNFD metadata relative to this placement control in the VNF_PACK.META.012:

- The VNFD shall support a description of metadata about placement of virtualisation containers relative to each other.

One possible solution proposed is the use of affinity and anti-affinity rules.

The anti-affinity groups defined in ETSI NFV-IFA specifications provide a mechanism to tell the VIM necessary isolation needs. Affinity and anti-affinity rules and local affinity and anti-affinity rules can be defined by the constituents of VNFs by the service provider, as described in ETSI GS NFV-IFA 011 [i.10].

Clause 5.8.2.2 of ETSI GR NFV-EVE 018 [i.12] explains how the affinity and anti-affinity groups can be used for virtual resource isolation.

Table 5.1.2-1 Affinity Policy

Policy	VM Group	Host	Zone
Intra-group affinity	Same VM group	Same host	Same zone
Inter-group affinity	Different VM group	Same host	Same zone

Table 5.1.2-2 Anti-Affinity Policy

Policy	VM Group	Host	Zone
Intra-group anti-affinity	Same VM group	Different host	Same zone
Inter-group anti-affinity	Different VM group	Different host	Same zone

5.1.3 Secure computing policies for containers in VNFD

As described in clause 6.1.4 of ETSI GS NFV-SEC 023 [10], some filtering of the system calls may be setup to limit the effect of container escape attacks. The filters should be defined to allow just enough capabilities for a correct execution of the VNF/VNFC, as an allowed list of system calls that are permitted and will depend on the VNF/VNFC. The policies (allowed list) may be defined as a JSON file (e.g. Docker™) and the granularity is the container. The policies file for the container shall be included in the VNF Package in the MCIOP or a separate security file.

It shall be defined in the IFA specifications how to include these secure computing policies in the VNF package.

The allowed list of syscalls shall be defined in the VNF Package (or VNFD), measures shall be taken to prevent its deletion, see clause 5.3.2.1 Req-VnfPackage-1 to Req-VnfPackage-4 of the present document.

NOTE: Inclusion of policies in MCIOP or in a separate security file in the VNF package is for future study. Docker™ defines such policies using JSON. How this could be used within NFV-MANO is for future study.

When the syscalls allowed list is empty (e.g. in the JSON file), all syscalls are blocked. However, it is possible with Docker™ to run a container without a policies file. In this case, a default profile is used. When the policies file exists, it shall not be possible to circumvent its use. The policies file and default profile are sensitive assets to be protected and deletion of these files shall be prevented

To enable a zero-trust architecture, the following requirements apply:

- When no policies file or no default profile exists for the container, all syscalls shall be blocked.
- The default profile shall have an empty list of allowed syscalls, blocking all syscalls by default. This default profile can be further updated to conform with operator policy by making the default restrictive in terms of allowed system calls.

Optionally, a NFV-MANO policies file may be used applying to several containers configured by NFV-MANO.

To apply more permissive policies to a container than allowed by the optional NFV-MANO policies file or the default profile, a specific policies file shall be included in the VNF Package for this container.

It shall be defined in IFA spec how the profile file is provided to the CIS to configure the seccomp feature.

5.2 Security requirements and capabilities in NSD

5.2.1 Affinity and anti-affinity rules

At the NS level, there could be a requirement on the placement of a VNF instance relative to other instances of the same constituent VNF, and relative to other constituent VNFs. Clause 5.3 of ETSI GS NFV-IFA 014 [i.11] gives requirements for Network Service Deployment flavour relative to this placement control of VNFs and VLs constituents of the NS:

- NST_NSF003: An NS DF description shall enable describing affinity and anti-affinity rules between the different instances of a constituent VNF.
- NST_NSF004: An NS DF description shall enable describing affinity and anti-affinity rules between the constituent VNFs.
- NST_NSF006: An NS DF description shall enable describing affinity and anti-affinity rules between the different instances of a constituent VL.

- NST_NSF007: An NS DF description shall enable describing affinity and anti-affinity rules between the constituent VLs

The anti-affinity groups defined in ETSI NFV-IFA specifications provide a mechanism to tell the VIM the necessary isolation needs. Affinity and anti-affinity rules can be defined for the constituents of NSs and NS instances by the service provider when designing network services, see ETSI GS NFV-IFA 014 [i.11]. The local affinity or anti-affinity rules are defined between VNF instances created from the same VNF profile.

Clause 5.7.2.2 of ETSI GR NFV-EVE 018 [i.12] explains how the affinity and anti-affinity groups can be used for virtual resource isolation.

Table 5.2.1-1: Set of allowed rules for affinity and anti-affinity

Rule ID	Description	Source
NST_NSF003	An NS Deployment Flavour (DF) description shall enable describing affinity and anti-affinity rules between different instances of the same constituent VNF.	ETSI GS NFV-IFA 014 [i.11], clause 5.3
NST_NSF004	An NS DF description shall enable describing affinity and anti-affinity rules between the constituent VNFs.	ETSI GS NFV-IFA 014 [i.11], clause 5.3
NST_NSF005	An NS DF description shall enable describing affinity and anti-affinity rules between different instances of a constituent VL.	ETSI GS NFV-IFA 014 [i.11], clause 5.3
NST_NSF006	An NS DF description shall enable describing affinity and anti-affinity rules between the constituent VLs.	ETSI GS NFV-IFA 014 [i.11], clause 5.3

5.3 Protection of VNF/NS packages and catalogues

5.3.1 Mitigations map

Figure 5.3.1-1 gives a map of the mitigations for the VNF/NS packages and catalogues to address on-boarding threats.

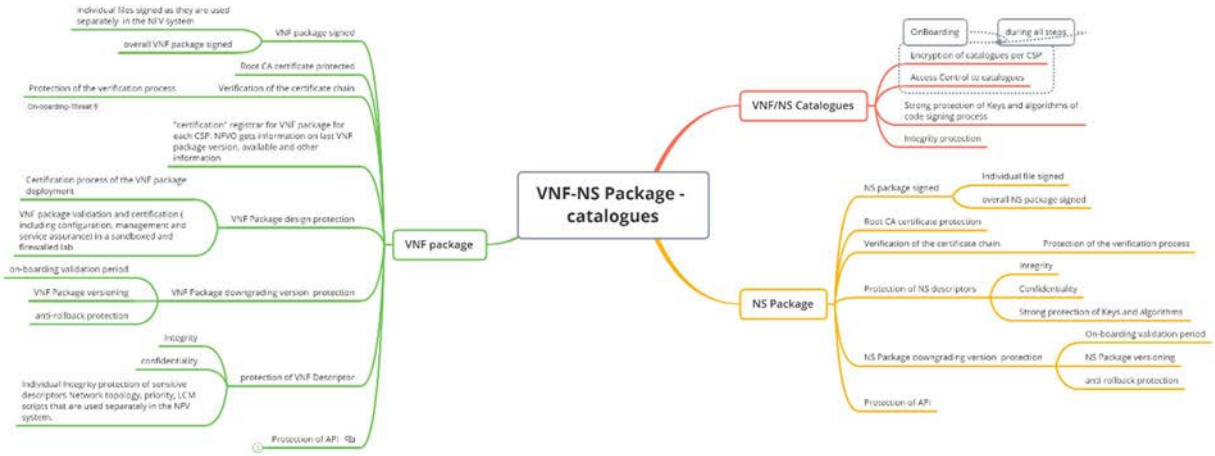

Figure 5.3.1-1: mitigations for the VNF/NS packages and catalogues to address on-boarding threats

5.3.2 Requirements

5.3.2.1 VNF Package

Table 5.3.2.1-1 gives the requirements concerning the VNF package and the associated threats they address.

Table 5.3.2.1-1: VNF Package requirements

Requirement ID	Requirement	Associated threat	Comments
Req-VnfPackage-1	Each individual artifact in a VNF package shall have a cryptographic signature produced by the VNF Provider when it is stored in the NFV-MANO catalogue.	On-boarding-threat.1, On-boarding-Threat 2, On-boarding-Threat 5	ENISA Best Practice: BP-T2 (see [i.13]). This Requirement is already addressed by ETSI GS NFV-SEC 021 [i.14].
Req-VnfPackage-2	Additionally, if the service provider policy mandates signing an artifact, this service provider's signature on this individual artifact(s) shall be stored as well.	On-boarding-threat.1, On-boarding-Threat 2, On-boarding-Threat 5	The present Requirement is already addressed by ETSI GS NFV-SEC 021 [i.14].
Req-VnfPackage-3	Additionally, the VNF package shall support an integrity protection of the overall VNF package as defined in clause 5.1 of ETSI GS NFV-SOL 004 [i.15].	On-boarding-threat.1, On-boarding-Threat 2, On-boarding-Threat 5	ENISA Best Practice: BP-T2 (see [i.13]). This requirement is already addressed by clause 5.1 of ETSI GS NFV-SOL 004 [i.15].
Req-VnfPackage-4	The integrity of the VNF Package and the authenticity of the issuer shall be verified during the on-boarding.	On-boarding-threat.1, On-boarding-Threat 2, On-boarding-Threat 5	
Req-VnfPackage-5	The root CA certificate shall be stored in a tamper-resistant storage.	On-boarding-Threat 8	
Req-VnfPackage-6	The VNF Package integrity check shall include the verification of the entire certificate chain.	On-boarding-Threat 8	
Req-VnfPackage-7	The VNF Package shall not be on-boarded unless its integrity is verified.	On-boarding-Threat 8	
Req-VnfPackage-8	The NFVO should be able to get information of the "certified" VNF package (last version and other information) for each CSP (e.g. in a registrar).	On-boarding-threat.1, On-boarding-Threat 2, On-boarding-threat 4	
Req-VnfPackage-9	The VNF Package design and validation shall be handled securely.	On-boarding-threat.1	
Req-VnfPackage-10	The VNF package deployment process (i.e. verification of the VNF package content, signature of the VNF package, up to the on-boarding in NFV-MANO) shall be certified and verified.	On-boarding-threat.1	ENISA Best Practices: BP-T4 (see [i.13]). The process of VNF deployment is clearly defined within the VNF provider company and verified for each VNF deployment with a proof of verification. see clause 5.5 of ETSI GS NFV-IFA 011 [i.10].
Req-VnfPackage-11	The VNF package validation and certification (including the configuration, management and service assurance) process shall be executed in a sandboxed and firewalled lab.	On-boarding-threat.1	ENISA Best Practice: BP-T2 (see [i.13]).
Req-VnfPackage-12	The VNF Package should contain means to check during the on-boarding that the VNF package is a fresh VNF package (e.g. use of certificate lifetime).	On-boarding-threat 4	Where feasible, a short-lived signing certificate can be used to enforce that the VNF package has been signed recently.
Req-VnfPackage-13	The VNF Package should contain an anti-rollback protection (e.g. versioning, Certificate Revocation List) to prevent the VNF Package from downgrading to an older version (for exception see comment).	On-boarding-threat 4	By default, the on-boarding process should reject a downgrading version of the VNF Package unless an administrator's action is taken to authorize the on-boarding of that specific package.

Requirement ID	Requirement	Associated threat	Comments
Req-VnfPackage-14	The VNF descriptor shall be protected in integrity after the on-boarding and signature stored in the catalogue along with the descriptor.	On-boarding-threat.5	ENISA Best Practice: BP-T2 (see [i.13]). This Requirement is already addressed by ETSI GS NFV-SEC 021 [i.14].
Req-VnfPackage-15	The VNF descriptor, software image and artefacts in the VNF package should be bound to the communication service provider that enabled the on-boarding of this VNF package to avoid unauthorized instantiation from another tenant (e.g. signature using CSP keys).		ENISA Best Practice: BP-T2 (see [i.13]). This Requirement is already addressed by ETSI GS NFV-SEC 021 [i.14] as an option depending on service provider policies. This is specifically recommended for NFV-MANO, enabling multi-tenancy.
Req-VnfPackage-16	The software image and artefacts in the package containing sensitive information shall support confidentiality protection.	On-boarding-threat.5	ENISA Best Practice: BP-T2 (see [i.13]). This requirement is already addressed by ETSI GS NFV-SOL 004 [i.15].
Req-VnfPackage-17	The sensitive descriptors, such as Network topology, priority, LCM scripts, and software image that are used separately in the NFV system, shall be integrity protected individually and the signature shall be stored or transmitted along with the data to enable verification of integrity.	On-boarding-threat.5	For example, the LCM scripts transmitted to the VNFM are signed (by the VNF vendor or CSP) to ensure that the scripts have not been tampered with. Very important as well for software images.
Req-VnfPackage-18	The interface used for the on-boarding of the VNF Package (Os-Ma-Nfvo) shall be protected (see specific requirement for the API protection).	On-boarding-Threat 1, On-boarding-Threat 2, On-boarding-Threat 3, On-boarding-Threat 4	
Req-VnfPackage-19	The catalogue of descriptor, artefact and VNF software shall be protected (see specific requirement for VNF/NS Catalogues).	On-boarding-Threat 3, On-boarding-Threat 9	ENISA Best Practice: BP-T2 (see [i.13]).

5.3.2.2 NS Package

Table 5.3.2.2-1 gives the requirements concerning the NS package and the associated threats they address.

Table 5.3.2.2-1: NS Package requirements

Requirement ID	Requirement	Associated threat	Comments
Req-NSPackage-1	Each NS package file contained in the NS package shall be signed by the CSP.	On-boarding-Threat 5	
Req-NSPackage-2	Additionally the overall NS package shall support an integrity protection as defined in clause 5.1 of ETSI GS NFV-SOL 007 [i.16].	On-boarding-Threat 5	
Req-NSPackage-3	The integrity of the NS Package and the authenticity of the issuer shall be verified during the on-boarding.	On-boarding-threat.1, On-boarding-Threat 2, On-boarding-Threat 5	
Req-NSPackage-4	The root CA certificate shall be stored in a tamper-resistant storage.	On-boarding-Threat 8	
Req-NSPackage-5	The NS Package integrity check shall include the verification of the entire certificate chain.	On-boarding-Threat 8	
Req-NSPackage-6	The NS Package shall not be on-boarded unless its integrity is verified.	On-boarding-Threat 8	

Requirement ID	Requirement	Associated threat	Comments
Req-NSPackage-7	The NFVO shall be able to get information of the "certified" NS package (last version and other information) for each CSP (e.g. in a registrar).	On-boarding-threat.1, On-boarding-Threat 2, On-boarding-threat 4	
Req-NSPackage-8	The NS Package design and validation shall be handled securely.	On-boarding-threat.1	
Req-NSPackage-9	The NS package deployment process (i.e. verification of the NS package content, signature of the NS package, up to the on-boarding in NFV-MANO) shall be certified and verified.	On-boarding-threat.1	
Req-NSPackage-10	The NS package validation and certification (including the configuration, management and service assurance) process shall be executed in a sandboxed and firewalled lab.	On-boarding-threat.1	
Req-NSPackage-11	The NS Package should contain an on-boarding validation period (e.g. certificate validity period used for NS Package signature) to ensure the NS Package is on-boarded or updated with the last up-to-date NS package.	On-boarding-threat 4	
Req-NSPackage-12	The NS descriptor shall be protected in integrity after the on-boarding.	On-boarding-threat.5	
Req-NSPackage-13	The NFV-MANO shall support confidentiality protection of the NS descriptors.	On-boarding-threat.5	
Req-NSPackage-14	The NFV-MANO shall support a strong protection of keys and algorithms.	On-boarding-Threat 9	
Req-NSPackage-15	The interface used for the on-boarding of the NS Package (Os-Ma-Nfvo) shall be protected (see specific requirement for the API protection).	On-boarding-Threat 1, On-boarding-Threat 2, On-boarding-Threat 3, On-boarding-Threat 4	
Req-NSPackage-16	The catalogue of descriptor of the NS package shall be protected (see specific requirement for VNF/NS Catalogues).	On-boarding-Threat 3, On-boarding-Threat 9	

5.3.2.3 VNF/NS Catalogues

Table 5.3.2.3-1 gives the requirements concerning the VNF/NS catalogues and the associated threats they address.

Table 5.3.2.3-1: VNF/NS catalogues requirements

Requirement ID	Requirement	Associated threat	Comments
Req-Catalogue-1	The VNF and NS packages in the catalogues shall be encrypted and signed per CSP, when NFV-MANO is multi-tenant.	On-boarding-Threat 3	ENISA Best Practice: BP-T2 (see [i.13])
Req-Catalogue-2	An access control to the catalogues shall be implemented.	On-boarding-Threat 3	ENISA Best Practice: BP-T2 (see [i.13])
Req-Catalogue-3	The NFV-MANO shall support a strong protection of keys and algorithms for the code signing process.	On-boarding-Threat 9	
Req-Catalogue-4	The catalogues shall be protected in integrity, and integrity shall be verified regularly.	On-boarding-Threat 1, On-boarding-Threat 2, On-boarding-Threat 3, On-boarding-Threat 5.	

5.4 API Protection

5.4.1 Mitigations map

Figure 5.4.1-1 below gives, in the form of a map, the list of mitigations to address the threats on the Os-Ma-Nfvo API during the on-boarding of VNF/NS packages, threats listed in clause 4.4.2.

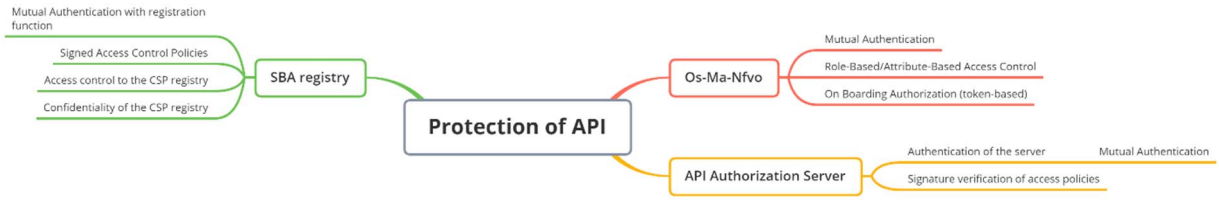

Figure 5.4.1-1: Mitigation map for the protection of Os-Ma-Nfvo API

5.4.2 Requirements

5.4.2.1 Introduction

The requirements on interfaces supported by the reference point of MANO's entities have been defined in ETSI GS NFV-IFA 005 [1], ETSI GS NFV-IFA 006 [2], ETSI GS NFV-IFA 007 [3], ETSI GS NFV-IFA 013 [5], ETSI GS NFV-IFA 008 [4] and ETSI GS NFV-IFA 010 [6] and shall be supported.

ETSI GS NFV-SOL 013 [7] has defined a solution for the protection of API based on OAuth2.0 protocol as defined in IETF RFC 6749 [8].

ETSI GS NFV-SEC 022 [9] includes a threat analysis concerning the access token and defines associated requirements for the mitigation of such threats and shall be supported when the protection of API is based on OAuth 2.0 protocol.

5.4.2.2 Os-Ma-Nfvo

Table 5.4.2.2-1 below lists the requirements on the Os-Ma-Nfvo reference point, associated with the threats listed in clause 4.4.2 and to the mitigations listed in the map of clause 5.4.1.

Table 5.4.2.2-1: Requirements on Os-Ma-Nfvo reference point

Requirement ID	Requirement	Associated threat	Comments
Req-API-1	The Os-Ma-Nfvo reference point shall support mutual authentication to validate the authenticity of the consumer and producer.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-API-2	NFVO shall verify authenticity of the consumer of the Os-Ma-Nfvo reference point.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3.	
Req-API-3	OSS/BSS shall verify authenticity of the producer of the Os-Ma-Nfvo reference point, before the on-boarding of VNF/NS package.	On-boarding-Threat 4.	
Req-API-4	The Os-Ma-Nfvo reference point shall support an access control model (e.g. Role-Based Access Control).	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3.	
Req-API-5	The NFVO shall verify that the consumer of the Os-Ma-Nfvo reference point is authorized to consume the API.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3.	Access control to API is addressed by ETSI GS NFV-SEC 022 [9]

5.4.2.3 Registration

The API capabilities registration function, as listed in Table 5.4.2.3-1, provides specific requirements on registering the functionalities and capabilities of APIs to enable secure and manageable API usage aligned with mitigating threats identified in clause 4.4.2. These requirements ensure that entities using the API have visibility and control over what API operations are exposed and how they are accessed.

This API registration function is a specialized subset of the broader NFV-S data registration framework outlined in ETSI GR NFV-IFA 039 [i.17]. The data registration superset in ETSI GR NFV-IFA 039 [i.17] encompasses comprehensive metadata and lifecycle management of all NFV system components, including descriptors, monitoring data, performance metrics, and security-related attributes.

Table 5.4.2.3-1: Requirements on API registration function and associated requirements on an entity that uses it

Requirement ID	Requirement	Associated threat	Comments
Req-Registration-1	A service exposing an interface shall register the access control policies and discovery policies for its API in a registry.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-Registration-2	A mutual authentication shall be processed before the registration of the API.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-Registration-3	The access control policies and discovery policies shall be signed.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-Registration-4	The registration function shall validate the access control policies against other policies of the NFV system for that service.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-Registration-5	The registration function shall restrict access to the access control policies to authorized management party(ies)	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-Registration-6	The registration function shall support the capability to encrypt the data in the registry using negotiated key and algorithm to or from an authenticated and authorized tenant.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-Registration-7	Any client wishing to consume a service shall register itself (including role and attributes) with the registration function.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	Need some initial client registration using e.g. one time token

Since the policy registry controls secure access to system critical security function, it is assumed that the registry is adequately secured against unauthorized access to the registry. The details of the necessary security mechanisms to secure the registry are outside the scope of the present document. The security policy registry may be a sub-set of the API capability registry (as described in ETSI GR NFV-IFA 039 [i.17]) or may be a separate registry depending on implementation security requirements.

Supporting real-time policy updates is essential for NFV deployments, where security postures need to be agile and responsive. This involves secure communication channels for policy changes, Role-Based Access Controls (RBAC) to limit who can initiate updates, and synchronization mechanisms to propagate changes across distributed components. Incorporating these capabilities ensures that the NFV security framework remains robust and adaptable and being able to manage security risks during the entire service lifecycle.

5.4.2.4 API authorization server

Table 5.4.2.4-1 below lists the requirements on the API authorization server, associated with the threats listed in clause 4.4.2 and to the mitigations listed in the map of clause 5.4.1.

Table 5.4.2.4-1: Requirements on API authorization server

Requirement ID	Requirement	Associated threat	Comments
Req-ApiAuth-1	Mutual authentication shall be processed between the authorization server and the entity that request authorization to access an API.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-ApiAuth-2	The authorization server shall be responsible for verifying the integrity of the overall policy registry (integrity of all policies not just the integrity of individual policies themselves).	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	
Req-ApiAuth-3	The authorization server shall verify the integrity of the access control policies in the registry for the API, before assessing the authorization to access the API and before issuing the authorization token to the API consumer.	On-boarding-Threat 1; On-boarding-Threat 2; On-boarding-Threat 3; On-boarding-Threat 4.	

6 VNF Instantiation

6.1 Mitigations map

The figure 6.1-1 gives a map of the mitigations for the threats during the VNF instantiation process.

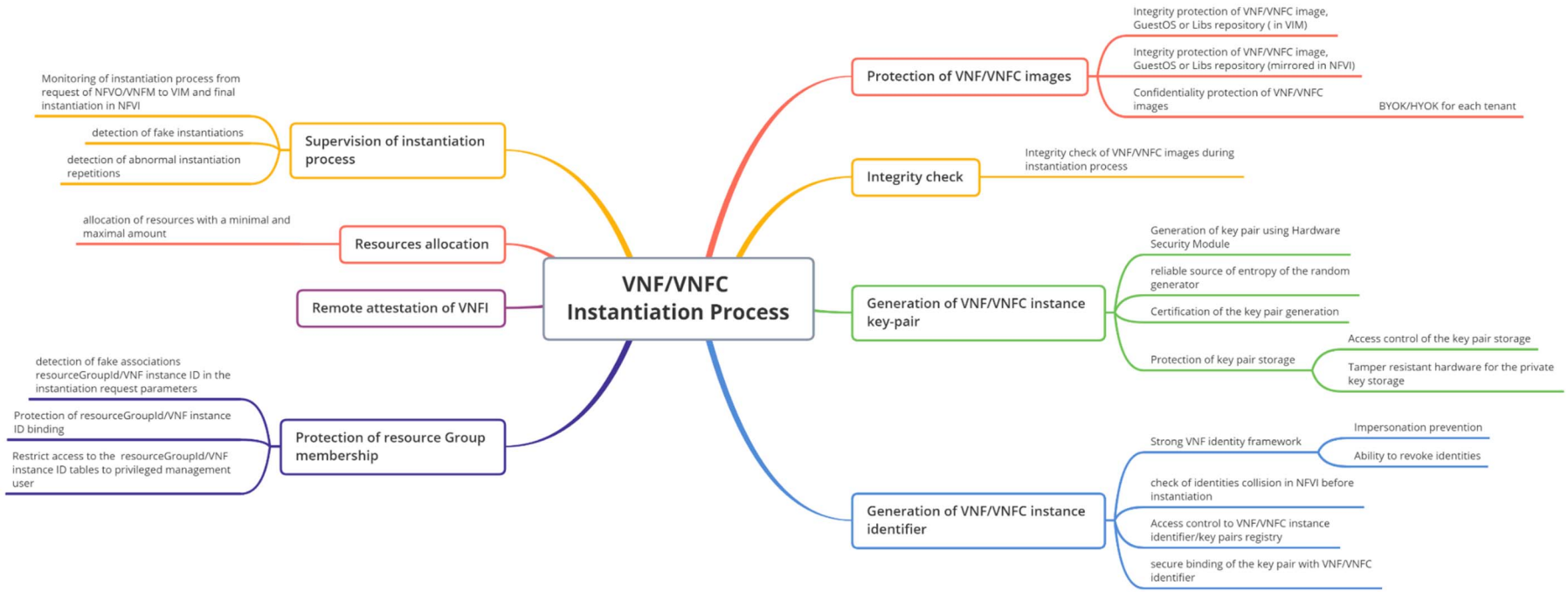

Figure 6.1-1: Mitigations for the threats during the VNF instantiation process

Figure 6.1-2 gives a map of protections from malicious NFV entities during the VNF instantiation process.

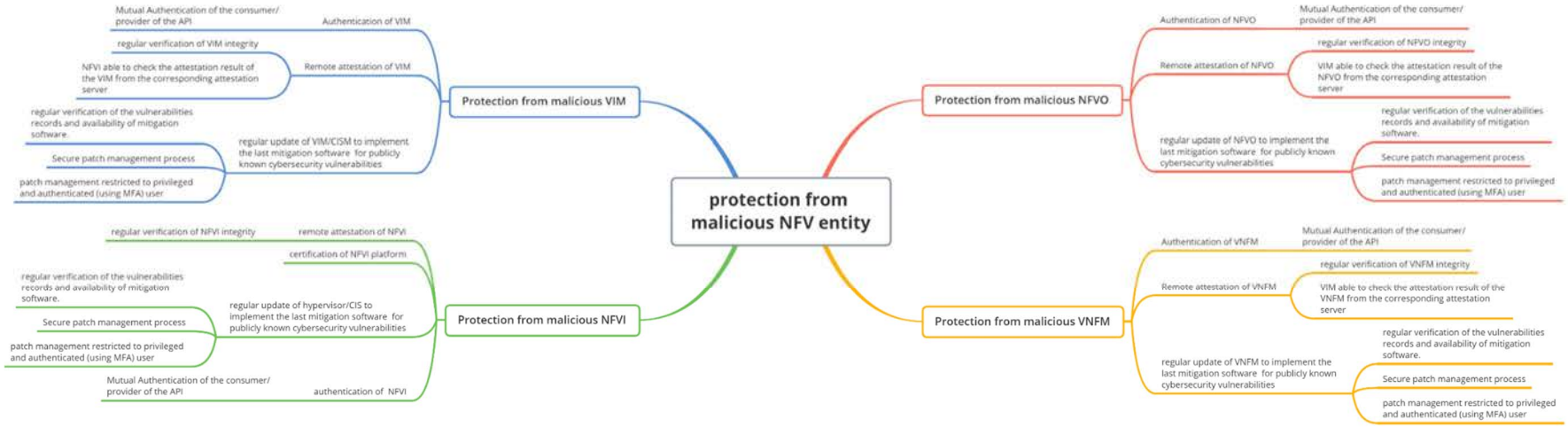

Figure 6.1-2: Protection from malicious NFV entities

Figure 6.1-3 gives a map for additional mitigations related to the NFVI integrity protection using secure boot, root of trust and remote attestation.

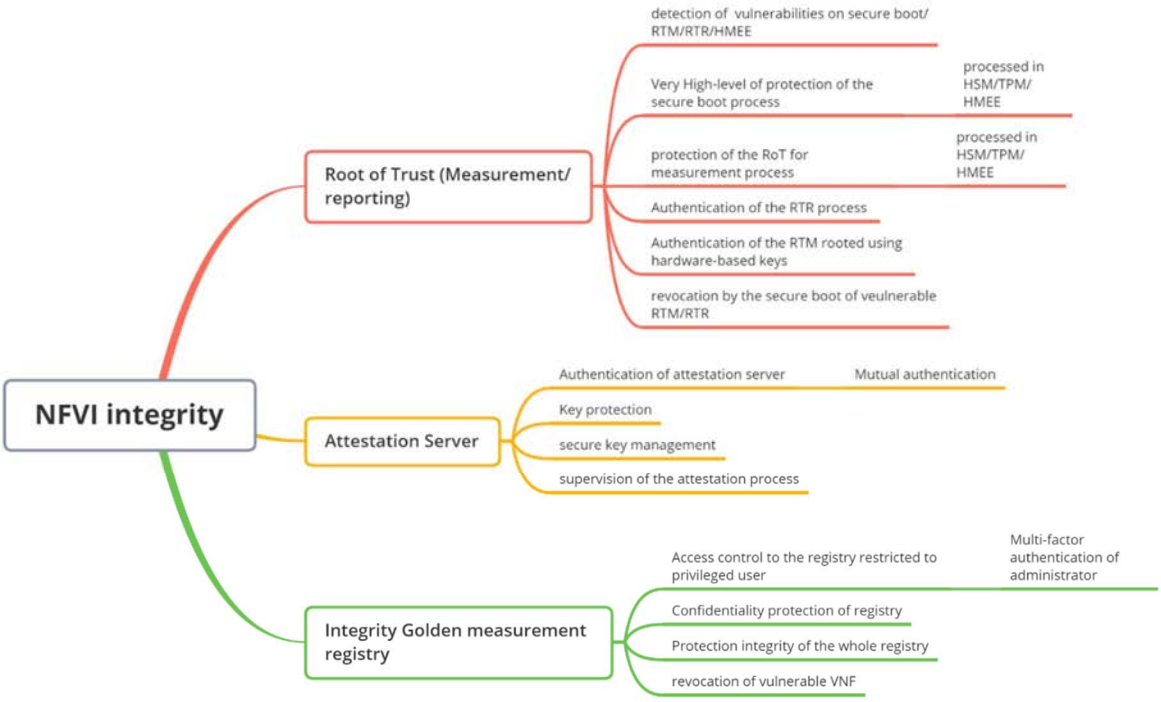

Figure 6.1-3: Mitigations for the threats related to NFVI integrity protection

6.2 Protection of VNF images

6.2.1 Description

The VNF images are highly sensitive assets that could be very easily tampered in the NFV system, where they are stored or during a transfer from the repository to the compute node (VM or container). The VNF images are stored in different locations in the system:

- In the VNF package catalogue.
- In the VNF images repository either in VIM or CIR and/or in the NFVI where the VNF images are mirrored allowing fast instantiation and scaling processes.
- In the VM or container.
- In the snapshots storage.

A VNF package is, in general, owned and the on-boarding/update is controlled by a specific Communication Service Provider and may be associated with a specific network. However, there could be some multi-tenancy use-cases where a VNF package is shared by several tenants. Specific details on this use-case can be found in ETSI GR NFV-EVE 018 [i.12] and ETSI GS NFV-SEC 026 [20].

A binding to a specific CSP and/or specific network service of the VNF package after the on-boarding and of the VNF image in the repositories is necessary such that a VNF image cannot be instantiated on behalf of an unauthorized CSP even if the vendor signature is valid. CSP-specific VNF image repositories or snapshots, where the VNF images are protected in integrity using signature with CSP certificate and with an access control, are a solution to envisage.

There are sensitive VNFs (e.g. LI VNFs) for which the software is a sensitive asset and may contain other sensitive information. An unencrypted VNF image provides information to the attacker. For these VNFs a confidentiality protection shall be possible. This confidentiality protection shall be possible and controlled by the CSP, everywhere the VM software is stored, including in the VM/Container. It shall be possible for the Communication Service Provider to control the key management and to bring or hold its own key for this VNF image encryption in repositories and for VM/Container encryption.

These sensitive VNF, that need a specific protection during the run-time, are typically instantiated in an HMEE. It shall be possible to bring, in the HMEE, the key that has been used to encrypt the software image to decrypt the image before the software starts. A solution for this use-case is described in clause 5.3.5 of ETSI GS NFV-SEC 026 [20]. In the solution, a key management system, controlled by the tenant, provides the encryption key for the encryption of the workload image, and after a successful attestation of the content of HMEE, provides the decryption key (wrapped with a public key of the HMEE) to decrypt the software image and to allow its execution.

The following clauses give requirements for the protection of VNF images:

- In the VNF images repository either in VIM or CIR and/or in the NFVI where the VNF images are mirrored allowing fast instantiation and scaling processes.
- In the VM or container.

Clause 5.3.2.1 of the present document gives the requirements concerning the protection of the VNF package catalogue.

Clause 8 of the present document gives the requirements concerning the protection of the VNF snapshots stored during the run-time of the VNF.

6.2.2 VNF images repository protection requirements

Table 6.2.2-1 gives the requirements concerning the VNF images repositories. These requirements apply for the VNF images repositories in VIM and in NFVI where the VNF images are mirrored allowing fast instantiation and scaling processes.

Table 6.2.2-1: VNF images repositories requirements

Requirement ID	Requirement	Associated threat	Comments
Req-images-repository-1	The repositories shall support CSP signing/CSP provided integrity protection of VNF images to avoid the instantiation of VNF images on behalf of unauthorized party.	Instantiation.1, Instantiation.5	ENISA Best Practice: BP-T2 (see [i.13]). It is important to pinpoint which root certificate shall be used to sign images at storage and to verify the signatures at instantiation and start-up.
Req-images-repository-2	The VNF images integrity shall be verified during launch time by the hypervisor or Container Infrastructure Service (CIS).	Instantiation.1, Instantiation.5	NOTE: Not all hypervisors are known to support VM image signature validation at VM image booting. The support of VM image validation at instantiation should be known in advance. Not only the hypervisor could be responsible of this aspect. The security policy dictates whether the instantiation may happen without validation.

Requirement ID	Requirement	Associated threat	Comments
Req-images-repository-3	NFV-MANO and NFVI shall support the VNF images encryption in the repositories using CSP specific key(s) and Key management.	Instantiation.1, Instantiation.5	Not all layers of the OS container-based VNF images may need encryption.
Req-images-repository-4	The root key from requirement Req-images-repository-3 shall be protected in a tamper resistant module such as HSM.	Instantiation.1, Instantiation.5	
Req-images-repository-5	The tamper resistant module storing key(s) shall be certified e.g. FIPS 140-2 [i.22] Level 3.	Instantiation.1, Instantiation.5	
Req-images-repository-6	The need for encryption and key management used shall be configurable per CSP/per VNF image. The encryption/decryption process used shall be defined per CSP/per VNF image.	Instantiation.1, Instantiation.5	Encryption/decryption process may change and evolve over time and therefore more than one alternative may become of interest. Also, different encryption/decryption process may be defined to best suit the VNF image protected. (Different type of data, within the image encrypted, may call for different encryption method).
Req-images-repository-7	When encryption of VNF images is used, the encryption of VNF image shall be done before the signing of the VNF image, to enable an integrity verification without any need for decryption.	Instantiation.1, Instantiation.5	
Req-images-repository-8	Interface with the key management system shall be done through a standardized protocol. At least Key Management Interoperability Protocol (KMIP) as defined by OASIS KMIP SPEC [11] shall be supported	Instantiation.1, Instantiation.5	
Req-images-repository-9	An access control to the VNF images repositories shall be implemented to avoid instantiation of the VNF on behalf of unauthorized party.	Instantiation.1, Instantiation.5	ENISA Best Practice: BP-T2 (see [i.13]).
Req-images-repository-10	The NFV-MANO and NFVI shall support a strong protection of keys and algorithms for the code signing and encryption process	Instantiation.1, Instantiation.5	
Req-images-repository-11	The images repository shall be protected in integrity, and integrity shall be verified regularly.	Instantiation.1, Instantiation.5	NIST SP 800-125 [i.4].
Req-images-repository-12	Administrative access privilege to the VNF images repository shall be protected through a strong access control mechanism.	Instantiation.1, Instantiation.5	NIST 800-125A Rev.1 [i.5].
Req-images-repository-13	Access control for administrator accounts shall support Multi-Factor Authentication.	Instantiation.1, Instantiation.5	
Req-images-repository-14	Administrative access to the VNF images repository shall be done through a secure protocol.	Instantiation.1, Instantiation.5	NIST 800-125A Rev.1 [i.5]
Req-images-repository-15	The image repository shall support house cleaning functionality to delete the out-of-date images (e.g. old versions, images no more used).	Instantiation.1, Instantiation.5	

6.2.3 Workload protection in VM or container requirements

Table 6.2.3-1 gives the requirements concerning the workload protection in the VM or container.

Table 6.2.3-1: Workload protection in VM or container requirements

Requirement ID	Requirement	Associated threat	Comments
Req-Workload-1	The hypervisor and/or CIS shall support the VM or container encryption.	Instantiation.5	
Req-Workload-2	The hypervisor and/or CIS shall support the encryption granularity down to per VM or per Container.	Instantiation.5	
Req-Workload-3	The hypervisor and/or CIS shall support an external key management controlled by the CSP.	Instantiation.5	
Req-Workload-4	Interface with the key management system shall be done through a standardized protocol. At least Key Management Interoperability Protocol (KMIP) as defined by OASIS KMIP SPEC [11] shall be supported.	Instantiation.5	
Req-Workload-5	The key management system shall use a tamper resistant module such as HSM.	Instantiation.5	
Req-Workload-6	The tamper resistant module storing the key(s) shall be certified e.g. FIPS 140-2 [i.22] Level 3.	Instantiation.5	
Req-Workload-7	After the hypervisor/CIS has used the key to decrypt the workload, it shall delete any local copy of the key.	Instantiation.5	

6.3 Generation of VNF/VNFC instance Identity document

6.3.1 Description

The main purposes of VNF instance identity are as described in ETSI GS NFV-SEC 020 [12]: the distinction, the discovery, attachment and trust. Using a trustworthy identity of the VNF instance or VM/Container's workloads in NFV is essential as it is used for authentication (proving that a service is what it says it is), for authorization (controlling who can access a service) and for confidentiality (keeping data exchanged between services secret).

"*An improper verification of identity and location of transmitting party on internal interfaces*" is one of the vulnerabilities (VUL5) listed by ENISA report [i.13]. ENISA proposes, as best practices, and in the conclusion of this report to develop a strong identity framework.

For a natural person, an identity document (e.g. passport , ID card, etc.) is used to prove their identity. The trust in the identity document, such as the passport, is established because there is an implicit trust in the authority that issues the identity document and there is a way to verify that the document originates from that authority. The identity document contains also attributes from the person that are used to authenticate the person that presents the identity document, such as picture, fingerprint pattern, physical attributes such as height, eye colour.

In the same way, in a highly distributed environment such as NFV, and to enable zero-trust architecture in such a multi-tenant environment, workloads in the NFV system should have trustworthy digital identity documents, verifiable with cryptographic techniques and including attributes bound to the VNFI/VNFCI, inherent to the workload. Some attributes have been listed in ETSI GS NFV-SEC 020 [12], such as: TYPE, timestamp of the instantiation step, geolocation of the data centre, LoA, identification of the MANO entities involved in the instantiation of the workload.

These identity attributes of the VNF instance are asserted during the attestation process of the VNFI/VNFCI, and the corresponding identity identifier is included in the digital identity document when attestation is successful.

After successful attestation of VNFI/VNFCI, key material that will be usable for communication with this workload is generated by a key pair generator (e.g. a Hardware Security Module) and certificate signed by the relevant certificate authority, and the certificate included in the digital identity document.

With this digital identity document, authentication, confidentiality and integrity, authorization, observability, and metering are possible.

Attestation process of the VNFI/VNFCI, and key generation is part of the VNFI/VNFCI identity generation process.

The VNF Bootstrapping Service as defined in ETSI GS NFV-SEC 024 [13], that is used for attestation, for the generation of VNF credentials, for the validation of VNF policies and to securely identifies the VNF is the corresponding process defined by ETSI-NFV.

To allow secure communication between services that are in different trust domains, and therefore be able to validate the identities across multiple trust domains, the collection of public keys in use for the identity generation in the SM of one trust domain shall be shared with the SM of the other trust domain. This is what is called the federation in the figure 6.3.1-1.

Figure 6.3.1-1 shows the architecture for the identity generation with an embedded Security Agent.

Figure 6.3.1-2 shows the architecture for the identity generation with an adjunct Security Agent.

An example of trustworthy identity document generation is provided by the open-source SPIFFE [i.18] /SPIRE [i.19] technology. The SPIRE Agent is equivalent to the VBS Agent of the figures 6.3.1-1 and 6.3.1-2 and the SPIRE Server is equivalent to the VNF boot-strapping Service described in the figures 6.3.1-1 and 6.3.1-2.

NOTE: ETSI TS 133 310 [i.20] describes the certificate management for Service Based Architecture within 3GPP.

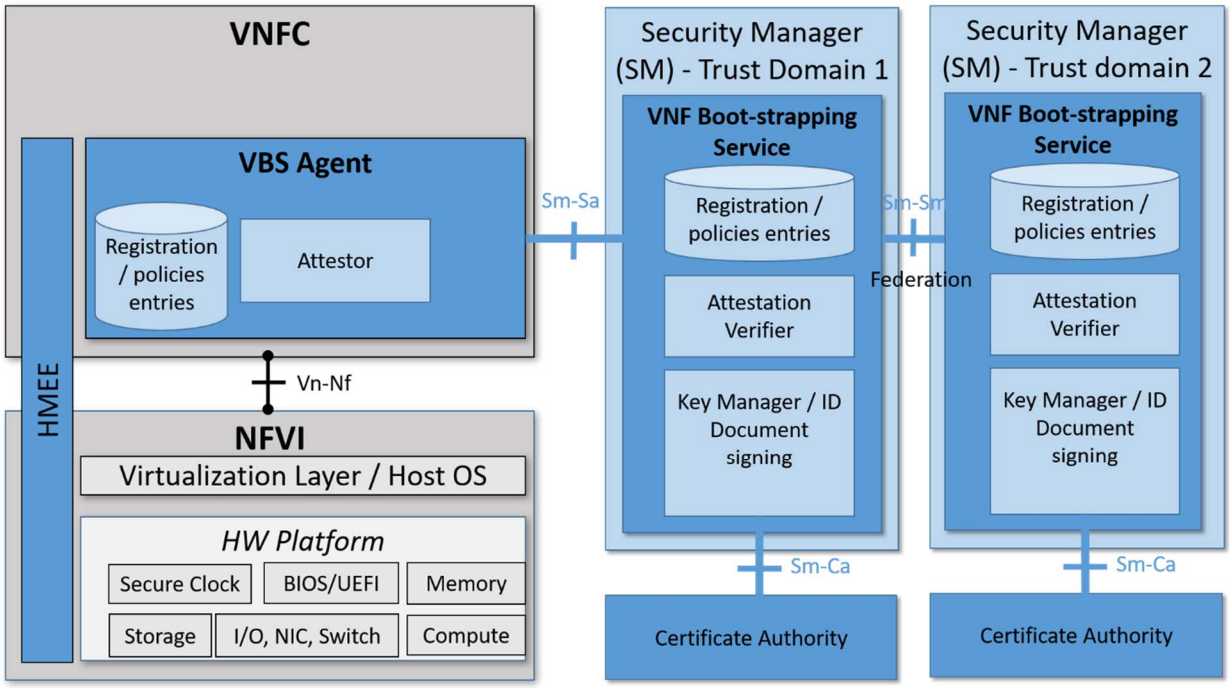

Figure 6.3.1-1: Identity Generation with an embedded SA

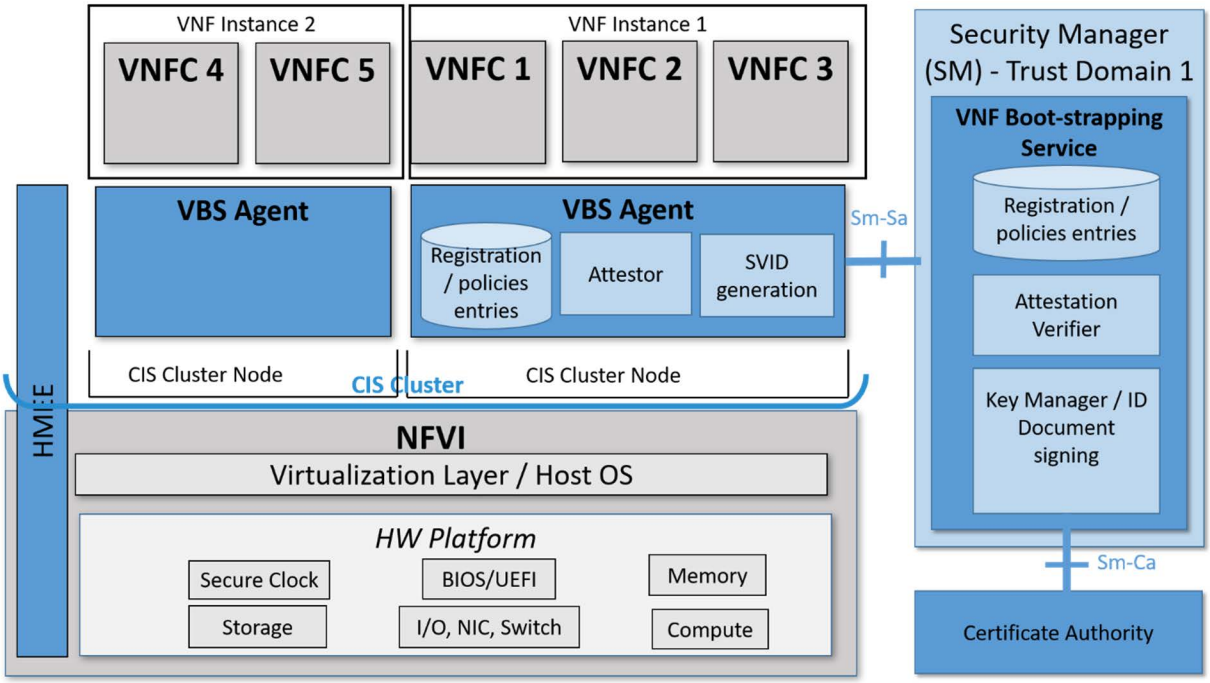

Figure 6.3.1-2: Identity Generation with an adjunct SA

The steps for the generation of the identity document are the following:

1) Generation of an identifier and registration of attestation policies.

2) Attestation of the workload and check against the registration (golden measurement) and policies entries for this workload.

3) Generation of key material.

4) Generation of the signed identity document.

6.3.2 Identifier generation and registration of attestation policies

6.3.2.1 Identifier generation

ETSI GS NFV-IFA 007[3] defines "create VNF identifier", a VNF lifecycle management operation that creates a VNF instance identifier and an associated instance of a VnfInfo information element, identified by that identifier. This operation returns an output parameter that is the VNF Instance Identifier just created: VnfInstanceId. This identifier is an URI parameter.

The identity of the VNF/VNFC instances shall uniquely identify the instance across heterogeneous environments and organizations, within a global scope and be interpretable consistently regardless of the context.

In a heterogeneous environment and distributed architecture, there could be some services defined with a SPIFFE scheme (some cloud providers use this Identity scheme for their instance), but also other schemes. The Identity scheme shall be identifiable in the identity of the VNF instances.

The VNF instances are instantiated within a trust domain. Identifying the trust domain in the VNF instance identity allows an easy mapping with the authority managing the trust domain and issuing the identities within this trust domain and with the set of cryptographic keys associated to this authority. The trust domain is an identity namespace.

The VNF instances' identities shall be used, interpretable and verifiable across multiple security domains.

ETSI GS NFV-SEC 020 [12] defines the VNF instance Identity as a Uniform Resource Identifier (URI) as defined by IETF RFC 3986 [15], identifying the identity scheme, the trust domain, and taking the VNFInstanceIdentifier as the last path element.

As described in clause 6.3.1 of the present document, the VNF bootstrapping Service in the Security Manager may be the authoritative entity that generates the VNF/VNFC instance identity. This service uses the VnfInfo metadata to generate the path information of the Identity, according to policies associated with this trust domain.

6.3.2.2 Registration of attestation policies

Security threads linked to registering attestation policies include risks to privacy, integrity, and trust. One key threat is the potential for relying parties to link different attestations from the same user, disturbing user privacy through profiling or tracking. Furthermore, data breaches exposing attestation evidence may also allow attackers to track users.

Monitoring systems in identity governance may trigger re-attestation if suspicious activities or policy violations are detected, preventing unauthorized access. However, secure integration of these triggers is essential to avoid security gaps.

Attestation relies on Trusted Execution Environments and secure hardware; attacks on CPU firmware can undermine attestation validity or cause data leakage.

Attestation data shall be stored in encrypted, tamper-proof storage with strict access controls. Related lifecycle management, including creation, expiration, and revocation, ensures data integrity.

6.3.3 Attestation of VNFI/VNFCI

The attestation of Virtual Network Function Instances (VNFI) and Virtual Network Function Component Instances (VNFCI) is a fundamental for NFV security to verify the integrity and trustworthiness of both the virtualized network functions and the underlying infrastructure. The attestation ensures a trust chain from the physical hardware trust anchor through the virtualization platform to the VNFCI where each layer is in a verified state based on the trust of the lower layers.

The VNFCI attestation focuses on the virtualized environment where the VNF software runs, such as virtual machines or containers, the separation from VNFCI attestation and underlying NFVI node attestation (physical hardware, firmware, platform) is essential because the VNFCI may be operated independently from the NFVI node and other components. Hence, ETSI GS NFV SEC 020 [12] attestation is separated between the NFVI node and the VNFCI.

The attestation process itself is performed according to ETSI GS NFV-SEC 024 [13]. It involves remote attestation protocols where a verifier requests cryptographic evidence from the attested components. These protocols support different levels of assurance, such as load-time versus runtime attestation, and local versus remote attestation, depending on the security requirements and environment.

6.3.4 Generation of VNFI/VNFCI key-pair

The generation of key pairs for Virtual Network Function Instance (VNFI) and Virtual Network Function Component Instance (VNFCI) involves a flexible and secure process according to the needs of the NFV deployment. In general key pairs can be generated by different trustworthy entities depending actual deployment scenario. These entities include the NFVI itself, a HMEE (Hardware-based Module or Environment Entity), or a HSM (Hardware Security Module).

The generated key pair may be either signed locally by the VNFCI or the Virtual Network Function Manager (VNFM) or NFV Orchestrator (NFVO). A Certification Authority (CA) or Registration Authority (RA) issues a certificate that bind the public key to the VNFCI identity including related standard attributes and potential extensions like authority key identifiers.

These certificates are fundamental for enabling mutual authentication between VNFCI, VNFM/EM (Element Manager), and other NFV entities, or for establishing secure communication channels such as TLS or IPsec.

The lifecycle management of these certificates and keys is an integral part of the NFV security framework spanning from enrolment, renewal to final revocation.

6.3.5 Generation of VNFI/VNFCI identity document

The generation of identity documents for Virtual Network Function Instance (VNFI) and Virtual Network Function Component Instance (VNFCI) within the ETSI NFV framework is based on the creation a Primary Verifiable Identity Document (VID/PVID) in format of X.509 certificate. as outlined in ETSI GS NFV-SEC 020 [12]. The attestation process itself involves remote attestation protocols where a verifier requests evidence (e.g. cryptographic proofs) from component being attested as defined in ETSI GS NFV-SEC 024 [13].

As described in ETSI GS NFV-SEC 020 [12] the attestation results and claims are incorporated into the X.509 certificate by leveraging the Subject Directory Attributes extension, as specified in IETF RFC 5280 [18]. This includes attestation measurements, cryptographic evidence, reflecting the integrity state of the VNFI or VNFCI along with other claims, such as issue at time (iat) of the attestation and location information, being structured according to IETF RFC 9711 [19].

The Primary Verifiable Identity Document (VID/PVID) identity document enables any relying party to verify that a robust attestation process has been successfully executed and securely bound to the entity's identity before granting access or establishing communication with the VNFI or VNFCI. Hence, the VID/PVID document acts as a critical trust anchor for VNFI and VNFCI entities also in zero trust-zones and shall be verifiable and understandable by other entities in a distributed environment.

6.3.6 Requirements

6.3.6.1 Requirements for attestation

Table 6.3.6.1-1 gives the requirements concerning the VNFI/VNFCI attestation.

Table 6.3.6.1-1: VNFI/VNFCI attestation requirements

Requirement ID	Requirement	Associated threat	Comments
Req-attestation-1	Authentication of attestation server especially also done by mutual authentication.		
Req-attestation-2	Key protection for attestation server.		
Req-attestation-3	Secure key management of attestation keys.		
Req-attestation-4	Supervision and secure execution of the attestation process.		

6.3.6.2 Requirements for VNFI/VNFCI key pair generation

Table 6.3.6.2-1 gives the requirements concerning the VNFI/VNFCI key pair generation.

Table 6.3.6.2-1: VNFI/VNFCI key pair generation requirements

Requirement ID	Requirement	Associated threat	Comments
Req-Key-pair-generation-1	The generation of key pair shall be done by using Hardware Security Module or Hardware-based Module or Environment Entity.		
Req-Key-pair-generation-2	Reliable source of entropy of the random generator.		
Req-Key-pair-generation-3	Certification of the key pair generator.		
Req-Key-pair-generation-4	For key protection itself an access control of key pair storage is required.		
Req-Key-pair-generation-5	The keys shall be stored in tamper resistant hardware storage for private key protection.		

6.3.6.3 Requirements for VNFI/VNFCI identity document generation

Table 6.3.6.3-1 gives the requirements concerning the VNFI/VNFCI identity document generation.

Table 6.3.6.3-1: VNFI/VNFCI identity document generation requirements

Requirement ID	Requirement	Associated threat	Comments
Req-Identity-generation-1	Identity identification of workload shall support zero-trust principles.		
Req-Identity-generation-2	Identity identification shall be verifiable and understandable by any entity in the distributed environment.		
Req-Identity-generation-3	Identity identification of workload shall be globally unique in an heterogeneous environment.		
Req-Identity-generation-4	Identity identification of workload shall be interpretable consistently regardless the context.		
Req-Identity-generation-5	In heterogeneous environment and distributed architecture, the Identity scheme shall be identifiable in the identity identification of the workload for a proper interpretation.		
Req-Identity-generation-6	The trust domain of the workload shall be identifiable in the identity identification of the workload allowing federation of trust domains.		
Req-Identity-generation-7	Identity documents shall be standardized.		
Req-Identity-generation-8	Each VNFC instance constituting the VNF instance shall have an identity document.		
Req-Identity-generation-9	Identity document shall be generated after a successful verification against identity attributes inherent to the workload and configured as registration entries for the workload (attestation process).		
Req-Identity-generation-10	Identity document shall be verifiable cryptographically.		
Req-Identity-generation-11	Identity document shall be bound to VNF instance workload attributes inherent to the workload.		
Req-Identity-generation-12	The list of possible attributes inherent to the workload identity shall be flexible to include CSP specific attributes, open to the diversity of environments, and extensible.		
Req-Identity-generation-13	The assertions about workload's identity shall be issued by a trustable process and shall not be issued by the workload itself.		
Req-Identity-generation-14	The identity document shall include key material of the workload that enable a secure communication with the workload.		
Req-Identity-generation-15	The process that generates the identity document shall be a highly protected process.		
Req-Identity-generation-16	The identity document shall be signed using a certified security module (e.g. FIPS 140-2 Level 3 HSM) trusted by the certificate authority of the trust domain.		
Req-Identity-generation-17	The interface with the certified security module used for identity document signing shall support at least the PKCS #11 protocol [14].		
Req-Identity-generation-18	The identity document shall be provided to the workload through a secure communication channel.		

Requirement ID	Requirement	Associated threat	Comments
Req-Identity-generation-19	The VBS agent may serve one VNFC in a container (embedded agent as defined in ETSI GS NFV-SEC 024 [13]) or may be node specific and serve multiple containers in a node (adjunct agent as defined in ETSI GS NFV-SEC 024 [13]).		

6.4 Remote Attestation of NFVI

The remote attestation process for NFV Infrastructure (NFVI), as outlined in ETSI GR NFV-SEC 018 [i.21], focuses on establishing a chain of trust from the underlying hardware layer up through the hypervisor platform to the Virtual Network Functions (VNFs). This process ensures that each layer and component in the NFV stack is in a trustworthy state before being considered secure. The attestation is performed for each layer and the final attestation result of a layer is independent of the underlying used HW or software.

The attestation starts at the physical hardware layer, including all hardware chips and their associated firmware. Next, the entire software stack of the hypervisor platform is attested, encompassing the operating system and hypervisor components. After the hypervisor platform is verified as trustworthy, the related NFVI layer, including virtualized hardware resources, is considered trusted and the VNF layer is attested. The attestation of the VNF layer involves attesting the VM on which the VNF runs and the software packages providing the VNF functionality.

Even though the Remote Attestation procedure itself is standardized, the used TEEs forming the Hardware Root of Trust (HRoT) differentiate concerning the measurement they take on the Attester/the System Under Evaluation (SUE).

As a consequence, the used hardware platform impacts the remote attestation procedure consequentially, it is important that the attestation is separated between the NFVI node and the VNFCI attestation result captured in the PVID/VID ETSI GS NFV-SEC 020 [12].

During the attestation, measurements are performed from the various layers (hardware, hypervisor, VM/VNF). These measurements are stored securely, typically within a tamper-resistant security module associated to the HRoT.
A quoting enclave generates an attestation report that includes these measurements, which is signed with the key to the quoting enclave for integrity protection and finally sent to a remote attestation server i.e. the verifier.

The verifier checks the report against known reference values (golden measurements) to determine trustworthiness.

Different attestation scopes can be applied depending on requirements, from attesting just hardware and virtual platform (hypervisor + VM) to attesting VNF software packages running inside the VM.

The attestation of a NFVI/VNFCI is based on a layered remote attestation process that establishes a robust trust chain in NFV environment via the NFVI, by verifying each component's integrity through cryptographic measurements and secure reporting, it ensures that network services are built on trusted infrastructure and software stacks.

6.5 Memory Allocation

Memory allocation in NFVI faces multiple challenges, including performance degradation, overhead, and fragmentation. Security risks accompany these challenges, with virtualization layers exposing the infrastructure to potential attacks. Multi-tenancy awareness in NFV orchestration ensures memory resource separation between different tenants to maintain isolation boundaries. The continuous monitoring and logging of memory usage or access helps detect abnormal activity.

These security-focused memory management practices mitigate risks like privilege escalation, data leakage through shared memory, and virtual machine escape attacks, supporting the confidentiality and integrity of critical network functions running in a virtualized environment. Proper planning and enforcement of these protections in the NFVI prevents from exploiting vulnerabilities associated with memory allocation in shared infrastructure.

Memory allocation for sensitive VNFs requires additional measures to ensure strict isolation and protection from unauthorized access. These requirements for memory allocation for sensitive VNFs in NFVI are described in ETSI GS NFV-SEC 026 [20] to ensure strong isolation and security for sensitive workloads.

Hence, sensitive VNFs often run on dedicated or isolated NFVI resources to prevent interference or data leakage from other VNFs sharing the infrastructure. Encrypting memory regions allocated to these VNFs prevents from exposing sensitive information or protects data even in case of malicious access attempts. Access control mechanisms, such as role-based access control, restrict memory access only to authorized VNFs or users. Spatial partitioning, where fixed memory quotas are allocated to each partition to prevent resource depletion and cross-tenant interference, ensures strong isolation and security for sensitive workloads within NFVI memory allocation Cache and CPU partitions complement memory partitioning to provide comprehensive resource isolation down to hardware levels. Key management and secure handling of encryption keys are essential for maintaining the confidentiality and integrity of memory partitions.

Highly sensitive VNFs also benefit from Trusted Execution Environments (TEEs), which provide hardware-supported memory protection and secure processing.

NFVI memory allocation and management of sensitive workloads requires multi-tenant trust domain separation, resource isolation, and hardened protection layers suitable for sensitive VNFs deployed on the NFVI platforms ensuring data privacy and security throughout the memory lifecycle.

7 VNF Configuration

7.1 Injection of key-pair

The process of the injection of key-pairs in VNFs shall address several security concerns. When hypervisors are used to provision public/private key pairs for VNFs or VNFC instances, a compromised NFVI or malicious hypervisor can gain access to private keys, potentially leaking them through concealed malicious software. Leaked private keys can be exploited by illegitimate VNFs masquerading as legitimate ones by using said keys, allowing unauthorized connection and extraction of sensitive data. Also, key pairs at rest need to be protected by tamper-resistant storage. Furthermore, the use of weak cryptographic algorithms during the key pair generation or management process undermines the authentication mechanisms across VNFs, VNFM, VIM, and NFVO, increasing vulnerability to attacks. In delegation mode, the security of key pairs is crucial, requiring secure deletion of private keys after distribution to prevent unauthorized access. Secure transmission channels shall be maintained to prevent man-in-the-middle attacks intercepting key material between components.

Table 7.1-1: injection of key pair requirements

Requirement ID	Requirement	Related Threat	Comments
Req-key-pair injection-1	VNFM shall protect key pairs at rest and during use within tamper-resistant storage for VNF OAM and VNFCI certificates.	Compromise of VNF OAM and VNFCI private keys	Critical to safeguard private keys to maintain confidentiality and integrity during key lifecycle.
Req-key-pair injection-2	VNFM shall securely generate, manage, and delete private keys during VNFCI certificate request and installation in delegation mode.	Leakage or unauthorized access to private keys during key handling	Ensures private keys do not remain accessible post-injection, reducing key exposure risk.
Req-key-pair injection-3	VNFM shall use secured and authenticated channels when passing certificates and keys to VNFs during configuration.	Man-in-the-middle attacks intercepting key pairs during injection	Encrypting communications prevent interception and tampering by malicious entities.
Req-key-pair injection-4	VNF package artifacts and VNFD files shall have signature verification to ensure integrity and authenticity.	Injection of tampered or malicious VNF packages with false keys	Protects against use of unauthorized or malicious key pairs embedded in VNF packages.
Req-key-pair injection-5	VNFM shall operate in delegation mode with strict control over keypair handling, signing requests, and coordination with CMF/CA.	Unauthorized generation, use, or distribution of keypairs	Enforces proper certificate lifecycle procedures aligned with trusted authorities.

Requirement ID	Requirement	Related Threat	Comments
Req-key-pair injection-6	Hypervisor and NFVI integrity shall be maintained to prevent malicious software from accessing private keys during key provisioning.	Malicious NFVI/hypervisor leaking private keys	Infrastructure security controls and attestation help prevent insider attacks on key material.
Req-key-pair injection-7	Use only strong cryptographic algorithms for key pair generation and management to avoid weak authentication processes.	Use of weak or compromised algorithms undermining key-security	Following latest cryptographic standards avoids vulnerabilities from algorithmic shortcomings.

7.2 Configuration of sensitive parameters

The configuration of sensitive parameters during VNF setup involves serious risks related to privileged user abuse, insider threats, and malicious components. Privileged users with access to configuration parameters, registries, cryptographic keys, security parameters, and identities may abuse their rights to cause damage or extract sensitive information. Malicious VNF management entities that have access to configuration parameters, lifecycle management scripts, or Element Manager (EM) functions can misconfigure VNFs or execute harmful scripts and cause damage to the entire system. Man-in-the-middle (MitM) attackers can intercept or alter sensitive parameters exchanged between VNFM and VNF/EM, between NFVI and VIM, or between NFVI and Service Manager, potentially changing critical parameters such as lawful interception data or VNF identities. Strong authentication, access control, encryption, and audit mechanisms are essential to protect the integrity and confidentiality of sensitive configuration parameters throughout the lifecycle.

Table 7.2-1: Configuration of sensitive parameters requirements

Requirement ID	Requirement	Related Threat	Comments
Req-configuration of sensitive parameters-1	Operators should implement strong access control and limit privileges to prevent abuse by privileged users.	Privileged user abuse with access to configuration parameters	Essential to enforce the least privilege principle to minimize insider risk.
Req-configuration of sensitive parameters-2	Continuous monitoring and auditing of privileged access is required to detect and prevent misuse.	Privileged user abuse	Real-time monitoring helps quickly detect suspicious privileged activities.
Req-configuration of sensitive parameters-3	Require validation and authorization of LCM scripts to prevent malicious reconfiguration.	Malicious VNFM misconfiguring VNFs with harmful LCM scripts	Script signing and validation prevent execution of unauthorized changes.
Req-configuration of sensitive parameters-4	Strong authentication and session protection for EM access shall be enforced.	Malicious VNFM or insider attacks via EM	Multi-factor authentication and session timeout improve security.
Req-configuration of sensitive parameters-5	Use encrypted and authenticated channels (e.g. TLS) to secure management communications.	Man-in-the-Middle (MitM) attacks interception configuration parameters	TLS encryption protects the confidentiality and integrity of data in transit.
Req-configuration of sensitive parameters-6	Enforce secure channel protocols and endpoint authentication to prevent data interception and alteration.	MitM attacks between NFVI and VIM	Mutual authentication between endpoints prevents impersonation attacks.
Req-configuration of sensitive parameters-7	Encrypt and authenticate data exchanges, ensuring integrity during transport.	MitM attacks altering lawful interception or sensitive configuration parameters	Mutual authentication between endpoints prevents impersonation attacks.
Req-configuration of sensitive parameters-8	Apply RBAC and multifactor authentication to restrict access to authorized personnel only.	Unauthorized access to management interfaces due to weak controls	Consistent access enforcement.

Requirement ID	Requirement	Related Threat	Comments
Req-configuration of sensitive parameters-9	Validate all inputs and filter out malicious payloads before execution.	Injection of malicious configuration or commands	Input validation reduces risks of command injection and malware infection.
Req-configuration of sensitive parameters-10	Maintain detailed logs of configuration activities to enable forensic analysis and compliance.	Lack of audit and traceability	Logs shall be securely stored to prevent tampering and support audits/analysis.
Req-configuration of sensitive parameters-11	Conduct proactive log analysis to identify suspicious activities and incidents promptly.	Insider threats or compromised credentials undetected	Advanced analytics improve detection of subtle or complex attack patterns.
Req-configuration of sensitive parameters-12	Define and test incident response plans specifically for configuration parameter breaches.	Delayed or inadequate breach handling	Regular drills ensure readiness and effective breach containment.

8 VNF during run-time

8.1 Remote attestation during run-time

Remote attestation is a critical process where the integrity of a running Virtual Network Function (VNF) instance is verified by a trusted verifier. The verifier challenges the VNF using a nonce to ensure freshness of the attestation, requiring the VNF to provide a cryptographic quote via an HBRT (e.g. TPM, HSM, etc.), providing cryptographic functions and root-of-trust. This quote reflects the current software state of the VNF instance, attesting that it matches a known good configuration. Alongside this quote, the VNF provides measurement logs, such as hashes of loaded executables and system components, which the verifier checks against a whitelist/golden values to ensure no unauthorized changes have occurred. This continual attestation process verifies the trustworthiness of the VNF during its entire lifecycle, protecting against malicious tampering or unauthorized modifications.

Table 8.1-1: VNF during run-time requirements

Requirement ID	Requirement	Related Threat	Comments
Req-RA-during-run time-1	Verify VNF integrity via remote attestation using a hardware chip-generated cryptographic quote		Ensures VNF software matches a known good state through cryptographic proof during runtime
Req-RA-during-run time-2	Provide measurement logs of software components for verification by a trusted verifier		Measurement logs help correlate the quote with the actual software components loaded
Req-RA-during-run time-3	Ensure continuous periodic attestation to confirm VNF trustworthiness throughout lifecycle		Detects unauthorized changes during the VNF operational run time

8.2 Protection of VNF instance data

The protection of VNF data at run-time is ensured by binding VNF instances to trusted hosts using hardware-based sealing mechanisms and resource control. Specialized hardware like an HBRT (e.g. TPM, HSM, etc.) provide cryptographic functions and a hardware-based root of trust, which enhances secure storage and platform integrity.

This involves pinning virtual CPUs to physical CPUs to reduce attack surface and verifying the integrity of VNF images and configurations through cryptographic hashes. Trusted or measured/attested boot technologies ensure that only platforms with known-good firmware, hypervisors, and kernels run the VNF. These protections prevent rogue administrators or attackers from executing compromised VNFs or accessing sensitive data. Continuous monitoring, periodic attestation, and hardware-rooted security features like Dynamic Root of Trust for Measurement (DRTM) reinforce these protections by enforcing runtime integrity and confidentiality of the VNF instances.

Table 8.2-1: VNF instance data requirements

Requirement ID	Requirement	Related Threat	Comments
Req-protection VNF instance-1	Seal VNF instance data via an HBRT (e.g. TPM, HSM, etc.) binding to trusted hosts		Ensures VNF only runs on trusted hardware
Req-Protection VNF instance-2	Pin virtual CPUs to physical CPUs for resource control and reduced attack surface		Restricts VM execution environment to reduce the risk of CPU-based attacks
Req-Protection VNF instance-3	Verify the integrity of VNF images and runtime configurations using cryptographic hashes		Prevents running tampered or unauthorized VNF images
Req-Protection VNF instance-4	Enforce Hardware-based security (HRoT) and employ a trusted or measured boot to verify firmware, hypervisor, and OS integrity before VNF start		Builds a root of trust anchored in hardware

8.3 Scalability of VNF instances pinned by hardware

Scalability for VNFs pinned to hardware involves both scale-up (vertical scaling) and scale-out (horizontal scaling) strategies within the constraints imposed by hardware resource binding. Scale-up requires increasing resources like virtual CPUs and memory on the pinned hardware to improve performance, but this is limited by the physical capacity of the host. Scale-out is achieved by deploying multiple VNF instances or clusters, each pinned to specific hardware CPUs, allowing distributed processing and higher throughput. Effective CPU pinning enhances cache affinity and reduces latency, which supports better scalability. Orchestration tools dynamically allocate resources and balance load among pinned instances to prevent performance bottlenecks and ensure scalability objectives are met efficiently without violating hardware pinning constraints.

Table 8.3-1: scalability of VNF instances pinned by hardware requirements

Requirement ID	Requirement	Related Threat	Comments
Req-scalability of VNF-1	Enable scaling up VNF resources (CPU, memory) within pinned hardware constraints		Scaling up improves performance linearly until hardware resource limits are reached
Req-scalability of VNF-2	Support scaling out by instantiating multiple VNF clusters pinned CPUs		Used when scale-up reaches limits; clustering may introduce communication and synchronization overhead
Req-scalability of VNF-3	Optimize CPU pinning and memory locality to improve cache efficiency		Proper resource affinity reduces latency and improves throughput for data plane intensive VNFs
Req-scalability of VNF-4	Use automated orchestration for dynamic resource allocation among pinned VNFs		
Req-scalability of VNF-5	Load balancing across pinned VNF instances to maintain performance		

8.4 Mobility of VNF instances pinned by hardware

Mobility of VNFs pinned to hardware focuses on the ability to migrate VNFs between physical hosts while preserving the benefits of hardware pinning. This includes maintaining CPU and memory bindings post-migration to retain performance gains. Secure migration is critical, requiring integrity checks and trusted attestation of VNFs before and after transfer to prevent tampering or unauthorized changes. Minimizing performance-loss/OOS-time and latency during migration ensures continuity of service. Synchronization of VNF state and data across hosts is necessary to avoid inconsistencies or loss during the migration process. Together, these capabilities enable flexible and secure movement of VNFs between trusted physical infrastructures, supporting dynamic network service delivery without compromising pinned hardware performance advantages.

Table 8.4-1: mobility of VNF instances pinned by hardware requirements

Requirement ID	Requirement	Related Threat	Comments
Req-mobility of VNF-1	Support live migration of VNFs across hosts maintaining CPU pinning		
Req- mobility of VNF-2	Ensure trusted attestation and integrity during migration		
Req- mobility of VNF-3	Minimize downtime and latency in migration operation		
Req- mobility of VNF-4	Maintain consistent hardware resource bindings post-migration		
Req- mobility of VNF-5	Synchronize VNF state and data accurately across migration		

9 VNF termination

9.1 Memory clean-up

There are critical risks related to memory cleanup during VNF termination. If memory is not properly cleaned up, it leads to memory leaks where allocated memory remains unreleased. This causes the VNF process to consume more and more memory over time, eventually exhausting system memory and swap space. Consequences include degraded performance, system slowdowns, VNF crashes, or even NFV infrastructure instability, harming overall service availability.

Moreover, improper cleanup can leave sensitive data in memory regions, which, in shared NFV infrastructure, are exposed to risks. Security vulnerabilities arising from incomplete memory removal in VNFs primarily include risks of data leakage, unauthorized data access, and privilege escalation. When memory is not fully cleaned upon VNF termination, even sensitive information such as user data, credentials, or cryptographic keys may remain accessible in the residual memory. This creates an opportunity for attackers or other VNFs sharing the same physical infrastructure to exploit these remnants to access confidential information without authorization.

Incomplete memory cleanup can also lead to side-channel attacks where attackers infer sensitive data by analysing memory usage patterns or stale data. Additionally, poorly managed memory may allow malicious actors to escalate privileges or inject malicious code by exploiting leftover or corrupted data structures in memory.

Moreover, in virtualized infrastructures, improper isolation combined with remaining memory exposure increases the risk of cross-tenant attacks, where one compromised VNF or tenant can affect others by gaining unauthorized access to their sensitive data through leftover memory artifacts.

Table 9.1-1: VNF termination/memory clean-up requirements

Requirement ID	Requirement	Related Threat	Comments
Req-VNF termination-1	Proper memory de-allocation and graceful VNF termination	Memory leaks leading to system performance degradation and instability	Allow to release resources properly and freeing allocated memory
Req-VNF termination-2	Memory complete cleaning upon VNF termination	Leftover sensitive data remains accessible, risking data leakage and cross-tenant attacks in case of shared memory	Critical for confidentiality and sensitive workloads; prevents other VNFs or tenants from accessing leftover data
Req-VNF termination-3	OS-level cleanup on process termination	Partial cleanup if only threads are terminated; memory might remain allocated	Process termination fully releases memory, but individual termination may not
Req-VNF termination-4	VNF orchestrator validation of cleanup	Incomplete cleanup can cause cascading faults in NFV infrastructure	Orchestrators shall ensure VNFs clean up properly before deletion
Req-VNF termination-5	Prevention of side-channel attacks	Residual memory data can be exploited to infer sensitive information	Requires thorough memory cleaning and secure termination practices
Req-VNF termination-6	Avoidance of privilege escalation via memory	Attackers may exploit leftover data or corrupted structures to escalate privileges	Enforces need for comprehensive memory safety measures

Annex (informative): Change history

Date	Version	Information about changes
04-2020	v0.0.1	First draft as baseline
07-2020	V0.0.2	Implementation of the following contributions accepted during the SEC#168 and SEC#169 meetings: NFVSEC(20)000057r1_SEC025_Threat_Analysis_Introduction NFVSEC(20)000058r4_SEC025_Threat_Analysis_Assets NFVSEC(20)000059r3_SEC025_Threat_Analysis_Threat_Agents NFVSEC(20)000063_SEC025_Threat_Analysis_Threat_Introduction NFVSEC(20)000064r1_SEC025_Threat_Analysis_On_Boarding_Threats
08-2020	V0.0.3	Implementation of the following contributions accepted during the SEC#170 meeting: NFVSEC(20)000069r1_SEC025_application_data_Asset NFVSEC(20)000074_SEC025_Threat_Analysis_adding_reference
09-2020	V0.0.4	Implementation of the following contributions accepted during the SEC#172 meeting: NFVSEC(20)000065r2_SEC025_Threat_Analysis_Instantiation_Threats NFVSEC(20)000070r1_SEC025_Threat_Analysis_Configuration_Threats NFVSEC(20)000071r1_SEC025_Threat_Analysis_Runtime_Threats
09-2020	V0.0.5	Implementation of the following contributions accepted during the SEC#173 meeting: NFVSEC(20)000072r1_SEC025_Threat_Analysis_VNF_Termination_Threats NFVSEC(20)000073r2_SEC025_Threat_Analysis_Generic_Threats NFVSEC(20)000085_SEC025_New_VNF_Assets NFVSEC(20)000086r1_SEC025_add_runtime_threats
12-2020	V0.0.6	Implementation of the following contribution accepted during the SEC#178 meeting: NFVSEC(20)000113r1_SEC025_Additional_Threat_and_Threat_Agent
09-2021	V0.0.7	Implementation of the following contribution accepted during the SEC#194 meeting: NFVSEC(21)000070r2_SEC025_Security_capabilities
01-2022	V0.0.8	Implementation of the following contribution accepted during the SEC#201 meeting: NFVSEC(21)000091r3_SEC025_Protection_VNF_NS_Packages
02-2022	V0.0.9	Implementation of the following contribution accepted during the SEC#204 meeting: NFVSEC(21)000098r2_SEC025_API_Protection
03-2022	V0.0.10	Implementation of the following contribution accepted during the SEC#204 meeting: NFVSEC(22)000009r1_SEC025_VNF_instantiation_mitigation_maps
04-2022	V0.0.11	Implementation of the following contribution accepted during the SEC#207 meeting: NFVSEC(22)0000021r2_SEC025_Seccomp_capability
05-2022	V0.0.12	Implementation of the following contribution accepted during the SEC#209 meeting: NFVSEC(22)000026r3_SEC025_VNF_images_Protection
07-2022	V0.0.13	Implementation of the following contribution accepted during the SEC#213 meeting: NFVSEC(22)000036r2_SEC025_VNF_instance_Identifier_generation
10-2023	V0.0.14	Implementation of the following contribution accepted during the SEC#242 NFVSEC(23)000202r1_SEC025_VNF_instance_identifier_generation
12-2023	V0.0.15	Implementation of the following contribution accepted during the SEC#244 NFVSEC(23)000235_NFV-SEC_025_Editorial_Updates
09-2024	V0.0.16	Implementation of the following contribution accepted during the SEC#270 NFVSEC(24)000156r1_SEC025_VNF_NS_Onboarding_Threat_Mitigations
10-2024	V0.0.17	Implementation of the following contribution accepted during the SEC#272 NFVSEC(24)000183r1_SEC025_update_VNF_image_protection
06-2025	V0.0.18	Implementation of the following contribution accepted during SEC#290 NFVSEC(25)000040r1_SEC025_proposed_resolution_to_a_number_of__editor_s_notes
09-2025	V0.0.19	Implementation of the following contributions accepted during SEC#292, SEC#293 and SEC#296 NFVSEC(25)000100_SEC025_section_6_3_3_Attestation NFVSEC(25)000106_SEC025_section_6_3_6_Requirements NFVSEC(25)000105r1_SEC025_section_6_4_remote_Attestation_of_NFVI NFVSEC(25)000112_SEC025_section_6_5_Memory_Allocation
10-2025	V0.0.20	Implementation of the following contributions accepted during SEC#299 and SEC#300 NFVSEC(25)000136_SEC025 section 7 VNF configuration NFVSEC(25)000137r1_SEC025 section 8 VNF during runtime NFVSEC(25)000138r1_SEC025 section 9 VNF termination NFVSEC(25)000145_SEC025 specification clean up

History

Version	Date	Status
V1.1.1	April 2026	Publication