



GROUP SPECIFICATION

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

get full document from standards.iteh.ai

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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

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

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Executive summary	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	8
3.3 Abbreviations	8
4 Threat analysis for VNF/NS during their lifecycle	10
4.1 Introduction	10
4.2 Assets	10
4.2.1 NS Assets.....	10
4.2.2 VNF Assets	11
4.3 Threat agents	12
4.4 Threats.....	14
4.4.1 Introduction.....	14
4.4.2 VNF/NS on-boarding.....	15
4.4.3 VNF instantiation.....	17
4.4.4 VNF configuration.....	19
4.4.5 VNF during run-time	20
4.4.6 VNF termination.....	24
4.4.7 Generic Threats.....	25
5 VNF/NS On-boarding	25
5.1 Security requirements and capabilities in VNFD	25
5.1.1 NFVI Security capabilities.....	25
5.1.2 Affinity and anti-affinity rules.....	26
5.1.3 Secure computing policies for containers in VNFD	27
5.2 Security requirements and capabilities in NSD	27
5.2.1 Affinity and anti-affinity rules.....	27
5.3 Protection of VNF/NS packages and catalogues	28
5.3.1 Mitigations map	28
5.3.2 Requirements	28
5.3.2.1 VNF Package	28
5.3.2.2 NS Package	30
5.3.2.3 VNF/NS Catalogues.....	31
5.4 API Protection	32
5.4.1 Mitigations map	32
5.4.2 Requirements	32
5.4.2.1 Introduction.....	32
5.4.2.2 Os-Ma-Nfvo	32
5.4.2.3 Registration	33
5.4.2.4 API authorization server	33
6 VNF Instantiation.....	35
6.1 Mitigations map.....	35
6.2 Protection of VNF images.....	37
6.2.1 Description.....	37
6.2.2 VNF images repository protection requirements	38
6.2.3 Workload protection in VM or container requirements.....	40

6.3	Generation of VNF/VNFC instance Identity document	40
6.3.1	Description.....	40
6.3.2	Identifier generation and registration of attestation policies.....	42
6.3.2.1	Identifier generation	42
6.3.2.2	Registration of attestation policies	43
6.3.3	Attestation of VNFI/VNFCI	43
6.3.4	Generation of VNFI/VNFCI key-pair.....	43
6.3.5	Generation of VNFI/VNFCI identity document	43
6.3.6	Requirements	44
6.3.6.1	Requirements for attestation.....	44
6.3.6.2	Requirements for VNFI/VNFCI key pair generation.....	44
6.3.6.3	Requirements for VNFI/VNFCI identity document generation	44
6.4	Remote Attestation of NFVI	46
6.5	Memory Allocation	46
7	VNF Configuration	47
7.1	Injection of key-pair	47
7.2	Configuration of sensitive parameters.....	48
8	VNF during run-time.....	49
8.1	Remote attestation during run-time	49
8.2	Protection of VNF instance data.....	49
8.3	Scalability of VNF instances pinned by hardware	50
8.4	Mobility of VNF instances pinned by hardware.....	51
9	VNF termination	51
9.1	Memory clean-up	51
Annex (informative):	Change history	53
History		54

get full document from standards.iteh.ai

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
MCIOF	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.

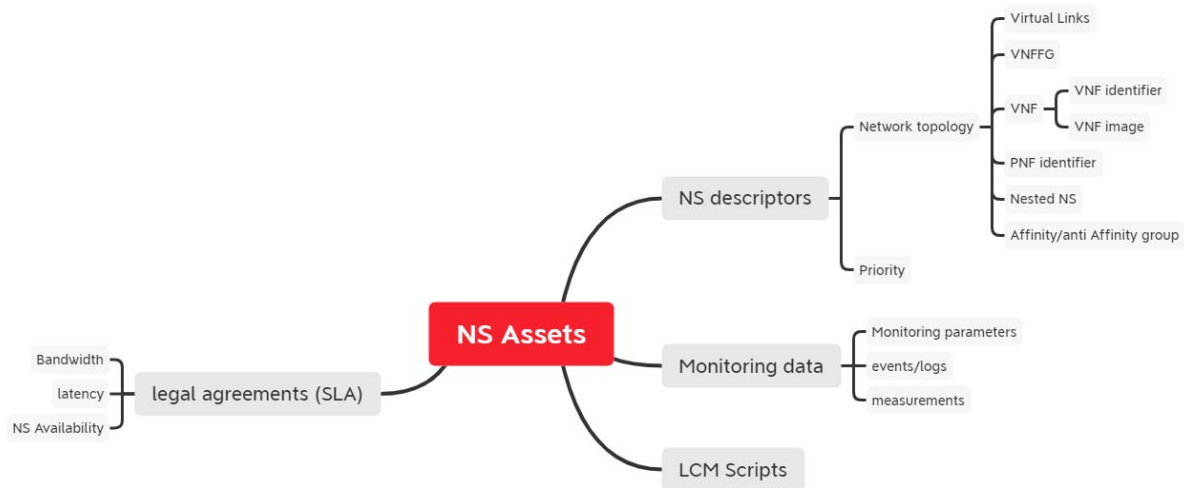


Figure 4.2.1-1: NS Assets map

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.

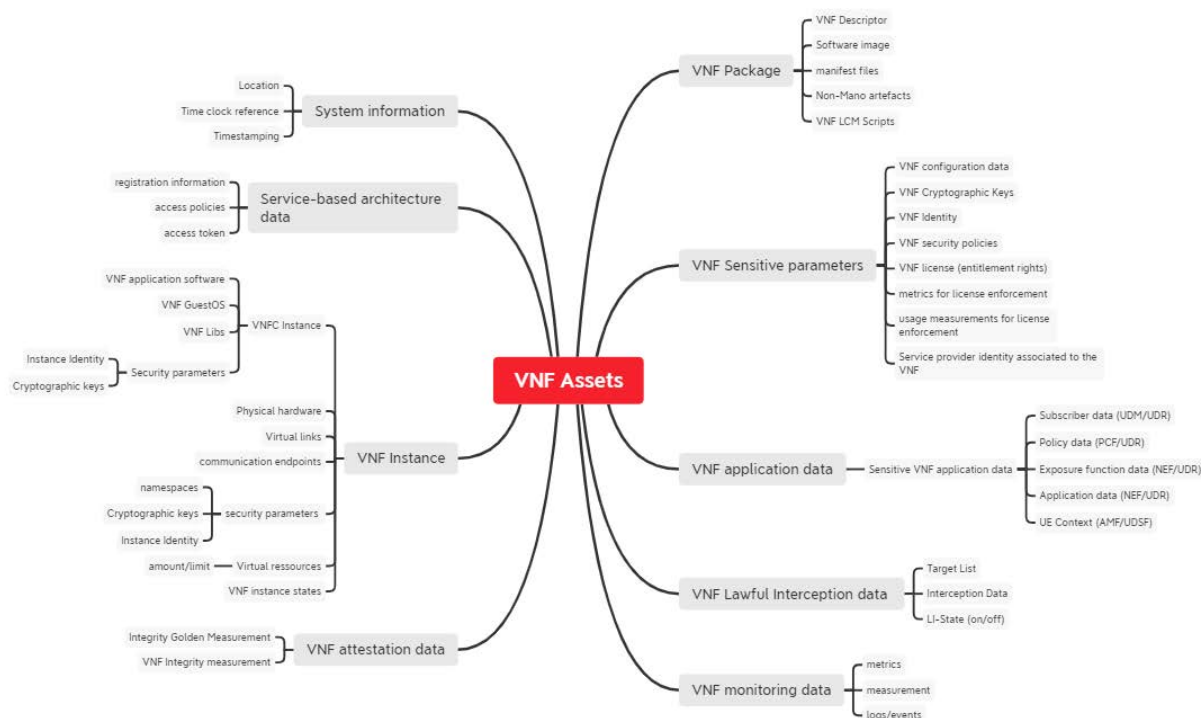


Figure 4.2.2-1: VNF Assets map

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 [1.3]. 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 3 rd 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 competitiveness, 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.