ETSI GS NFV-SEC 003 V1.1.1 (2014-12)

Network Functions Virtualisation (NFV);
NFV Security;
Security and Trust Guidance

Disclaimer

This 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-SEC003

Keywords

NFV, security

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

Intellectual Property Rights

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

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

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

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

1 Scope

The present document has been developed to describe the security and trust guidance that is unique to NFV development, architecture and operation. Guidance consists of items to consider that may be unique to the environment or deployment. Supplied guidance does not consist of prescriptive requirements or specific implementation details, which should be built from the considerations supplied.

Guidance is based on defined use cases, included in the present document, that are derived from the Security Problem Statement and are unique to NFV. Relevant external guidance will be referenced, where available.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

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

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

2.2 Informative references

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

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

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

[i.1] Popek and Goldberg 1974 paper: "Formal Requirements for Virtualizable Third Generation Architectures".

[i.2] CSA CloudTrust.

[i.3] GS NFV-SWA 001: "Network Functions Virtualisation (NFV); Virtual Network Function Architecture".

3 Abbreviations

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

ABAC	Attribute-Based Access Control
API	Application Programming Interface
BIOS	Basic Input Output System
CA	Certificate Authority

CDN	Content Distribution Network
CLI	Command Line Interface
CPU	Central Processing Unit
CPUID	CPU Identifier
CSA	Cloud Security Alliance
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMA	Direct Memory Access
DNA	DeoxyriboNucleic Acid
DNS	Domain Naming Service
DoS	Denial of Service
DPI	Deep Packet Inspection
DRM	Digital Rights Management
EM	Element Manager
EMS	Element Management System
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
GTP-C	GPRS Tunnelling Protocol-Control
GTP-U	GPRS Tunnelling Protocol-User Data Tunneling
GUI	Graphical User Interface
HSM	Hardware Security Module
HSS	Home Subscriber Server
HVM	Hardware Virtual Machine
IAM	Identity and Access Management
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IO	Input/Output
IP	Intellectual Property
IT	Information Technology
LI	Lawful Intercept
LUN	Logical Unit Number
MAC	Media Access Control
MANO	Management and Orchestration
MME	Mobile Management Entity
NE	Network Element
NF	Network Function
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFVO	Network Function Virtualization Orchestrator
NIC	Network Interface Card
NTP	Network Time Protocol
OA&M	Operations, administration and management
OS	Operating System
PKI	Public Key Infrastructure
RADIUS	RADIUS protocol
RAM	Random Access Memory
RBAC	Rights-Based Access Management
SDN	Software Defined Networking
SIP	Session Initialization Protocol
SSAE	Statement on Standards for Attestation Engagements
SVA	Security Virtual Appliance
SWA	Software Architecture
TBOOT	Trusted Boot
TOR	Top of Rack
TPM	Trusted Platform Module
TXT	Trusted eXecution Technology
UEFI	Unified Extensible Firmware Interface
UUID	Unique Universal IDentifier
VA	Virtual Appliance
VIM	Virtual Infrastructure Manager
VLAN	Virtual LAN (Local Access Network)
VM	Virtual Machine

VMM	Virtual Machine Monitor
VNF	Virtual Network Function
VNFC	Virtual Network Function Component
VNFCI	Virtual Network Function Component Instance
VNFD	Virtual Network Function Descriptor
VNFM	Virtual Network Function Manager
VoLTE	Voice over LTE
VPC	Virtual Private Cloud
vSwitch	virtual Switch
VTPM	Virtual Trusted Platform Module

4 Network Function Virtualisation Security

4.1 NFV High-Level Security Goals

Security is Embedded in NFV DNA

Security is defined as the state of being protected (secured) as well as those measures applied to achieve/maintain/validate protection.

The dynamic nature of Network Function Virtualisation demands that security technologies, policies, processes and practices are embedded in the genetic fabric of NFV.

Additional high-level security goals for NFV include:

- Establish a secured baseline of guidance for NFV operation, while highlighting optional measures that enhance security to be commensurate with risks to confidentiality, integrity and availability.
- Define areas of consideration where security technologies, practices and processes have different requirements than non-NFV systems and operations.
- Supply guidance for the operational environment that supports and interfaces with NFV systems and operations, but avoid redefining any security considerations that are not specific to NFV.

NOTE: NFV security considerations are very similar to hypervisor-based virtualisation security considerations in their architecture and interfaces. However, security architects and operations managers are instructed to consider use cases beyond hypervisor-based constructs to include cloud orchestration, virtual appliances and empower future innovations.

4.2 NFV Security Use Case Summaries

The following use cases describe the need for security within the VNF, between VNFs and secured interfaces and interchanges external to the VNF. The use cases are summarized for brevity, highlighting important security functions and considerations unique to NFV.

4.2.1 Intra-VNFSec: Security within Virtual Network Functions

Within the VNF, security measures and processes are required for VNF operations, for contained VNFC operations, and for secured interface with external assets and services. Specifically, this clause describes the use cases that are unique within a VNF.

4.2.1.1 VNFC-Specific Security Use Cases

Sensitive authentication data in workloads

NFV workloads routinely possess sensitive authentication data used for authenticating the workload, its processes and users. This sensitive authentication data can consist of passwords, private keys, cryptographic certificates, tokens and other secrets. This data should be protected during all phases of the NFV security and trust lifecycle and should be considered highly dynamic in nature, with updates likely during instantiation, hibernation/suspension, and VNF retirement. NFV workloads containing sensitive authentication data reside within and may be described as VMs, VAs, VNFs and VNFCs. Guidance for this use case should describe the processes, procedures and technologies unique to NFV that would satisfy the use case, pointing to external best practices where available.

Function and capability authorization control for VNFs

There are many functions and capabilities that will be provided by various parts of a VNF and various different entities within NFV may request that these functions and capabilities are employed. It is not always appropriate to provide authorization for an entity to access these, even when the same entity has previously done so. Authorization for use of these functions and capabilities may be controlled by a number of techniques and across a number of variables, including identity, trust, joint or delegated decision making and API security.

Guidance for this use case should describe the key technologies for use in the context of authorization control for VNFs, and how they may be used within an NFV context.

4.2.1.1.1 VNFC Creation

The creation of a VNFC will require updates to networking, credentialing, encryption, licensing, configuration and other settings unique to the new VNFC that impact security. Creating a VNFC can be accomplished in one of the following ways:

- The instantiation of a newly-defined VNFC.
- The instantiation of a VNFC with pre-configured state the cloning of an existing VNFC.

Guidance for these use cases should describe update and verification processes and procedures, virtual asset tracking and audit records.

4.2.1.1.2 VNFC Deletion

The retirement and deletion of a VNFC and its VNFCIs will require updates to networking, credentialing, encryption, licensing, configuration and other settings unique to VNFC removal that impact security. When requests for secured wipe and verified destruction are made, the actions taken should be forensically sound. When a VNFC is to be made unavailable, for re-use or re-creation, deletion of all possible instances (VNFCIs) should be verified across backups and archives, cloned images and other copies.

Guidance for this use case should describe update and verification processes and procedures, virtual asset tracking and audit records. Asset management should ensure certificate revocation and updates of IP whitelisting/blacklisting.

4.2.1.1.3 VNFC Configuration and Package Management

The updates to a VNFC and associated VNFCIs include patching, updating, new/modified software packages and configuration changes. These changes can include:

- Patching of the operating system, drivers and virtual machine components.
- Adding dynamic updates to the configuration (DNS, DHCP, etc.).
- Management of virtual machines and virtual appliances, including security virtual appliances.
- Updates to event-based configuration guidance, such as whitelists and blacklists.
- New versions of application software, software frameworks (e.g. Java) and software components.

Guidance for this use case should describe update and verification processes and procedures.

4.2.1.1.4 VNFCI Migration

Migrating a VNFCI is desired for maintenance of underlying VNF infrastructure, failover in the event of VNF infrastructure failure and disaster recovery in the event of a site failure condition. Migrations are often performed as "live migrations" that should not incur downtime to the operations of the VNFC when correctly functioning.

Migration concerns include memory reuse, feature parity, configuration compatibility and service availability.

4.2.1.1.5 VNFC Operational State Changes

Operational state changes (planned and unplanned/intentional or unintentional) can significantly affect VNFC security. A partial list of operational state changes includes:

- Hibernation, sleep, resumption, abort, restore, suspension.
- Power-on and power-off (either physical or virtual).
- Instantiation, whether pre-configured or not.
- Patching and maintenance.
- High-availability, recovery and data-in-motion changes during live migration.
- Integrity verification failure, crash and OS compromise.
- Retirement and termination.

Guidance for this use case should describe integrity verification processes and procedures including logging and audit.

4.2.1.1.6 VNFC Topology Changes

Topology changes that affect the security of the VNFC can result in loss of communication, unintended traffic flows, loss of intended traffic flows and other issues including:

- Network IP address and VLAN updates.
- Service chaining.
- Failover and disaster recovery.

Guidance for this use case should describe awareness of topology changes and resiliency.

4.2.1.1.7 VNFC Scale-Up and Scale-Down

The scale-up and scale-down of a VNFC affect sizing and can alter the memory, storage and processing requirements, resulting in differences in class of service, monitoring thresholds, performance thresholds and backups. Scale-up and scale-down are also referred to as vertical scalability.

Guidance for this use case should describe architectural and operational changes associated with increased/decreased requirements for the VNFC due to scale-up/scale-down.

4.2.1.1.8 VNFC Scale-In and Scale-Out

Scale-in and scale-out of a VNFC affects multiple resources (e.g. services and communications) that spread the VNFC workload, resulting in differences in class of service, monitoring thresholds, performance thresholds, networking and backups. Scale-in and scale-out are also referred to as horizontal scalability.

Guidance for this use case should describe architectural and operational changes associated with increased/decreased requirements for the VNFC due to scale-in/scale-out, as well as dependencies between systems utilized for scalability.

4.2.2 Infra-VNFSec: Security between Virtual Network Functions

Virtual Network Functions that communicate directly with each other have special security needs, as network-level security enforcement is often not inherent in the communication path. Characteristics include:

- Secured orchestration for and between VNF domains.
- Flows are often not through firewalls or other network policy enforcement points.
- Virtual Appliances and Security Virtual Appliances need to be configured to be part of the traffic flow.
- Service chaining capabilities need to be enforced, if available.
- Requires strong VNF-VNF security measures and individual VNF resiliency to attack.

4.2.3 Extra-VNFSec: Security external to Virtual Network Functions

The security of VNFs is reliant on the security of the physical infrastructure, environment and external services. The following use cases identify key issues external to the VNF that directly impact VNF and VNFC security.

Regulatory and jurisdictional impact on NFV deployments

NFV deployments will exist, as current telecommunications services do, in a regulatory and jurisdictional environment. The virtualisation of network functions leads to new requirements both on the VNFs themselves and on the management and orchestration components with which they are controlled. Issues include Lawful Intercept, Auditing and Service Level Agreements, and although there are many similarities to existing practise, the advent of NFV brings some changes.

In addition, future NFV deployments may increasingly be spread across borders, leading to multiple sets of requirements being placed on operators. The ability to administer services across borders and to migrate services in real-time between different jurisdictions presents further challenges.

The trust and security document will identify key legal and regulatory issues and address appropriate processes and technologies.

Authentication, Authorization and Accounting for NFV

NFV deployments will be complex, with multiple administrative domains within the same deployment, for example:

- NFVI - comprising:
    - Network(s)
    - Hypervisor
    - Compute
    - Storage
- SDN
- Service network
- VNFM
- Orchestration

The authentication, authorization and accounting requirements across these domains will be different, some having regulatory requirements, for instance. In addition, there will be a mix of human and system entities requiring services.

In some deployments, there will be requirement for external parties - such as other operators - to be able to access and administer parts of the NFV deployment, and this will also include access to authentication, authorization and accounting services.

Although each NFV deployment will be different, there will be some common technologies, features and best practices. The trust and security document will identify and describe these.

4.3 NFV External Operational Environment

These are items of consideration for the external operational environment that are unique to supporting Network Function Virtualisation. Included are physical security, hardware, services, policies and practices.

4.3.1 External Physical Security Guidance

A referenced standard for physical security should be described and documented to support NFV needs. This may include facility (i.e. SOC2, SSAE 16) specialized hardware (i.e. FIPS, TPM) and other considerations that are relied upon for NFV for confidentiality, integrity availability and audit.

4.3.2 External Hardware Guidance

- Discuss Trusted Computing Base.
- Include the use of physical taps as required for Lawful Intercept.
- Describe VNF usages of FIPS and HSM.
- Other hardware advantages? Requirements?

4.3.3 External Service Guidance

4.3.3.1 DNS

Ensure the ability to update newly instantiated, suspended, hibernated, migrated and restarted images with relevant DNS information.

4.3.3.2 IP Addressing, DHCP and Routing

Ensure the ability to update newly instantiated, suspended, hibernated, migrated and restarted images with relevant IP addressing, including routing tables, route health information and whitelists/blacklists. A VNF that is acting as a router or DHCP server should be validated before routes and addressing updates are propagated.

4.3.3.3 Time Services and NTP

Ensure the ability to update newly instantiated, suspended, hibernated, migrated and restarted images with current time and time zone information. Log all changes to time, date and time zone. Log changes to time server source.

4.3.3.4 Geolocation

Ensure the ability to update newly instantiated, suspended, hibernated and restarted images with relevant geolocation information. Log all changes to geolocation along with the mechanisms and sources of location information (i.e. GPS, IP block, and timing).

- Discuss Geolocation sources.

4.3.3.5 Security Visibility and Testing

This clause encompasses all of the facilities outside of NFV used for security monitoring, vulnerability scanning, penetration testing, and NFV security monitoring and reporting.

- External visibility into VNF and VNFC.
- External components of Introspection services Monitoring, Logging, Reporting, Analytics and Auditing.