Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

Network Function Virtualization (NFV)

(As applicable to Mobile Generation Technologies)

ITSAR Number: ITSAR404042308
ITSAR Name: NCCS/ITSAR/Customer Premises Equipment/Mobile Network Based Equipment/NFV

Date of Release: 28.08.2023 Version: 1.0.0
Date of Enforcement:

MTCTE के तहत जारी:
Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification of telecommunication/ICT equipment within the country. NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sr No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Network Function Virtualization (NFV)	ITSAR404042308	1.0.0	28.08.2023	First release

Table of Contents

Scope

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) specific to NFV Infrastructure (Platform), Virtual Network Functions (both container and Virtual Machine based), Management and Network Orchestration (MANO) and Software Defined Networking (SDN). (Applicable to NFV infrastructure(platform), NFV, SDN and MANO components. All these are denoted as 'system' here).

Chapter 1 – Overview

Introduction: Traditionally, Network Functions have been bundled into bespoke hardware appliances. In contrast, network function virtualization is the deployment of these services as software modules that run on common off-the-shelf generic hardware over a hypervisor or container that controls access to hardware devices. In principle all network functions and nodes may be considered for virtualization. The greatest impetus for the NFV came from 3GPP when it proposed Service Based Architecture (SBA)for realization of 5G Core.

NFV provides the following benefits

1) OPEX and CAPEX savings due to the use of commodity hardware, the ability to share computing resources between functions, reduced energy consumption etc.
2) The operators can use the introduction of virtualized networking and cloud technologies to adopt tools similar to those used by IT industry to automate many aspects of operations and managements. This will enable operators to shorten time to market of new services and scaling of resources as per the dynamic demands.

1. NFV Technologies: The key technology used in the NFV is virtualization**.** Virtualization can be Hypervisor based or container based.

i) Hypervisor based: Hypervisor-based virtualization provides isolated environments on top of a shared pool of resources. Hypervisor is a software layer that abstracts the underlying physical resources and provides virtual machines (VM) with the full functionalities of a real system. The hypervisor is responsible for resource allocation to the VM as well as being responsible for monitoring and managing VMs through coordination with the primary OS of the underlying hardware.

There are two types of hypervisors known as Type 1 and Type 2. Pl refer Fig 1.

Type-1 Hypervisor: Also known as Bare-metal Hypervisor, it runs directly on the host machine's physical hardware. It does not need an underlying host OS because the communication to hardware resources is direct with full visibility of hardware resources.

Type-2 Hypervisor: A Type-2 hypervisor is typically installed on top of an existing OS. It is sometimes called a hosted hypervisor because it relies on the host machine's pre-existing OS to manage allocation of CPU, memory, storage, and network resources to the VM.

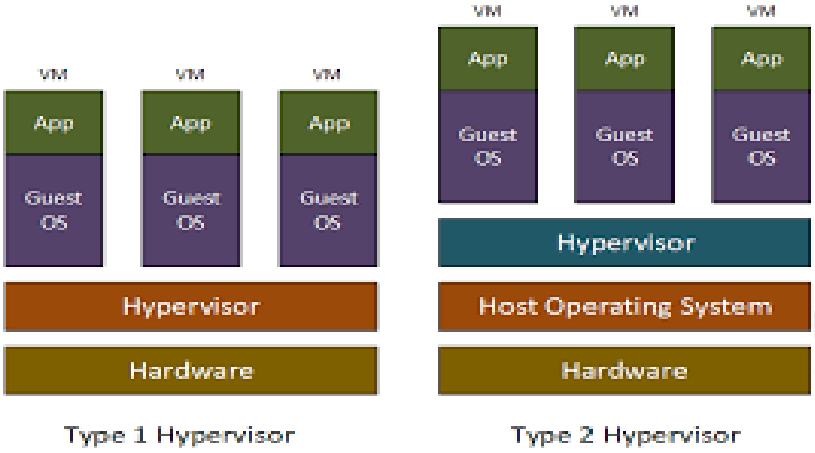

Fig 1 Type 1 and Type 2 Hypervisors

Virtual Machine (VM): A virtual machine (VM) is a type of virtualization that splits bare metal servers into numerous independent instances, each of which has its own operating system. The operating system, applications and services are all bundled into a single image that is accessed via a hypervisor, built on virtualized hardware.
A VM consists of several files that are stored on a storage device. The key files are the configuration file, virtual disk file, NVRAM setting file and log file.

ii) OS level Virtualization: OS-level virtualization represents the containerization model, which envisages that only the applications and their dependencies are integrated into a container. Each container shares the host OS kernel operating on bare metal, as well as its binaries and libraries so the applications run quickly and reliably from one computing environment to another. Containerized network function is best suited for cloud native environment and hence also called as Cloud Native Network Function (CNF)

iii) Hybrid virtualization: It is the mixture of both VMs and Containers.

iv) The Software Defined Networking (SDN) is the complementary technology which will benefit NFV implementation. The core similarity between software-defined networking (SDN) and network functions virtualization (NFV) is that they both use network abstraction. SDN seeks to separate network control functions from network forwarding functions, while NFV seeks to abstract network forwarding and other networking functions from the hardware on which it runs. SDN has three components viz. SDN application layer, SDN Control Layer and SDN infrastructure layer/Resource layer. Fig 2 below shows the concept of SDN.

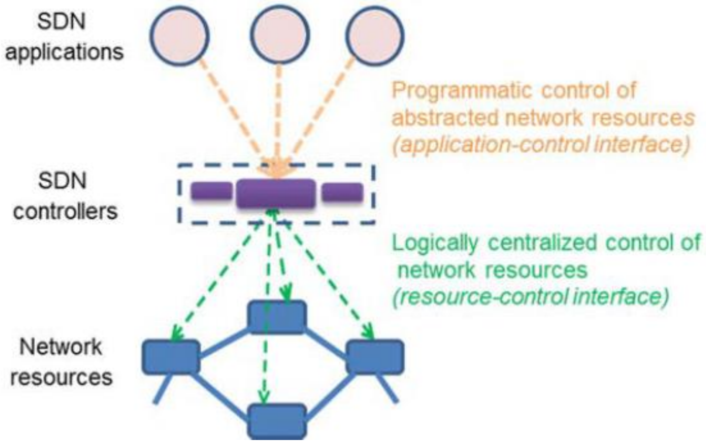
SDN applications
Programmatic control of abstracted network resources (application-control interface)
SDN controllers
Logically centralized control of network resources (resource-control interface)
Network resources

Fig 2 Concept of SDN

When SDN executes on an NFV infrastructure, SDN forwards data packets from one network device to another. At the same time, SDN's networking control functions for routing, policy definition and applications run in a VM or container somewhere on the network. Thus, NFV provides basic networking functions, while SDN controls and orchestrates them for specific uses. SDN further allows configuration and behavior to be programmatically defined and modified.
SDN can be incorporated in the NFV framework by positioning SDN resources and SDN controllers in different ways.

2. NFV Architectural Framework: The NFV architectural framework has been developed to standardize the NFV components and their service interfaces so as to ensure compatibility between different vendor implementations. ETSI has developed the NFV framework, the high-level view of which is shown in Fig 3. ETSI identifies three working domains in the NFV architecture.

i. **Virtual Network Functions (VNF)** - software implementation of network function that runs over a NFVI.
ii. **NFV Infrastructure (NFVI)** - this includes the physical resources and how these can be virtualized. NFVI supports the execution of the VNFs.

iii. **NFV Management and Orchestration (MANO)** - it includes the orchestration and lifecycle management of the physical resources and/or the software resources that support the virtualization of the infrastructure and the life cycle management of VNFs. MANO comprises of the Virtualized Infrastructure Manager (VIM), Virtualized Network Function Manager (VNFM) and NFV Orchestrator (NFVO).

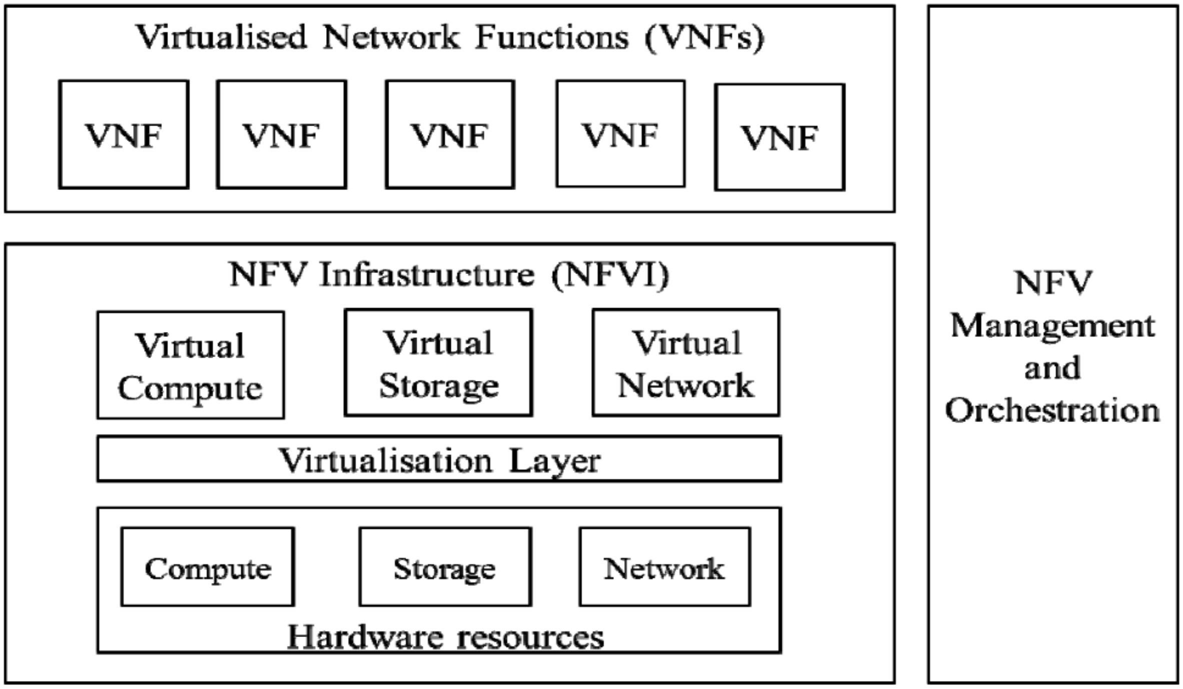

Figure 3 High level NFV Framework

The initial release of the ETSI NFV specification was predominantly dependent on hypervisor-based virtual machines (VMs) for virtualization. After the introduction of cloud native NFV, an adaptation is made in some areas as shown in the Fig 4. The cloud native here indicates the various micro services implemented as Container to realize a network services. The components of this architecture are

i. **NFV Infrastructure (NFVI):** The NFVI consists of all the hardware and software components that are contained within the environment in which VNFs are deployed. It provides virtualized computing, storage, and networking.

ii. **OSS/BSS** - Operation Support System and Business Support System of the operator.

iii. **Element Management System (EMS)**: It is responsible for the configuration, fault management, accounting, and collection of performance measurement results for the network functions provided by the VNF.

iv. **Hardware Resources:** In NFV, the physical hardware resources include computing, storage and networks that provide processing, storage, and connectivity to VNFs through the virtualization layer (Host OS, Hypervisor, CIS).

v. **Virtualized Network Function (VNF):** An implementation of an NF that can be deployed on a network function virtualization infrastructure (NFVI). VNFs are built from one or more VNF components (VNFC).

vi. **Virtualized Network Function Component (VNFC):** It is an internal component of a VNF that provides a VNF provider with a defined subset of that VNF's functionality. Its main characteristic is that a single instance of this component maps 1:1 against a single instance of an atomic deployable unit.

vii. **Virtualization layer:** It consists of two sub layers: a host OS and hypervisor (for VMs) and CIS (for containers).

viii. **Container Infrastructure Service (CIS):** The cloud-native equivalent of hypervisor is container infrastructure service (CIS), which provides all the runtime infrastructural dependencies for one or more container virtualization technologies.

ix. **Container:** It is a virtualization container using a shared operating system (OS) kernel of its host. Containers can host a VNF component (VNFC) for instance. VM-based components within NFV

x. **Hypervisor:** It is a piece of software which partitions the underlying physical resources and creates virtual machines, and isolates the VMs from each other. It is running either directly on top of the hardware (bare metal hypervisor type 1) or running on top of a hosting operating system (hosted hypervisor type 2).

xi. **Virtual Machine (VM):** It has all the ingredients (processor, memory/storage, interfaces/ports) of a physical computer or server and is generated by a hypervisor, which partitions the underlying physical resources and allocates them to VMs. Virtual machines can host a VNF component (VNFC) for instance.

xii. **NFV Orchestrator (NFVO)** - It is in charge of orchestration and management of the NFVI and software resources. It also takes care of network services in the NFVI.

xiii. **VNF Manager (VNFM)** - It is responsible for lifecycle management of VNFs (e.g. Instantiation, update, scaling, query, termination). There may be scenarios that can have multiple VNFMs may be deployed, VNFM may be deployed for each VNF or VNFM may serve multiple VNFs.

xiv. **Virtualized Infrastructure Manager (VIM)** - It comprises the functionalities that are used to control and manage the interaction of VNF with computing, storage and network resources under its authority.

xv. **Container Infrastructure Service Management (CISM):** It is a functional block that manages one or more container infrastructure services. The CISM provides mechanisms for lifecycle management of the managed container infrastructure objects, which are hosting application components as services or functions. It is a cloud-native equivalent of virtualized infrastructure manager (VIM). Kubernetes - K8s(for cloud native NFs) is a possible solution for CISM.

xvi. **NFV Security Manager (NFV SM/NSM):** NFV SM is a function that applies security policy to a virtualized network based on both predefined default policy and active analysis of information provided through security monitoring

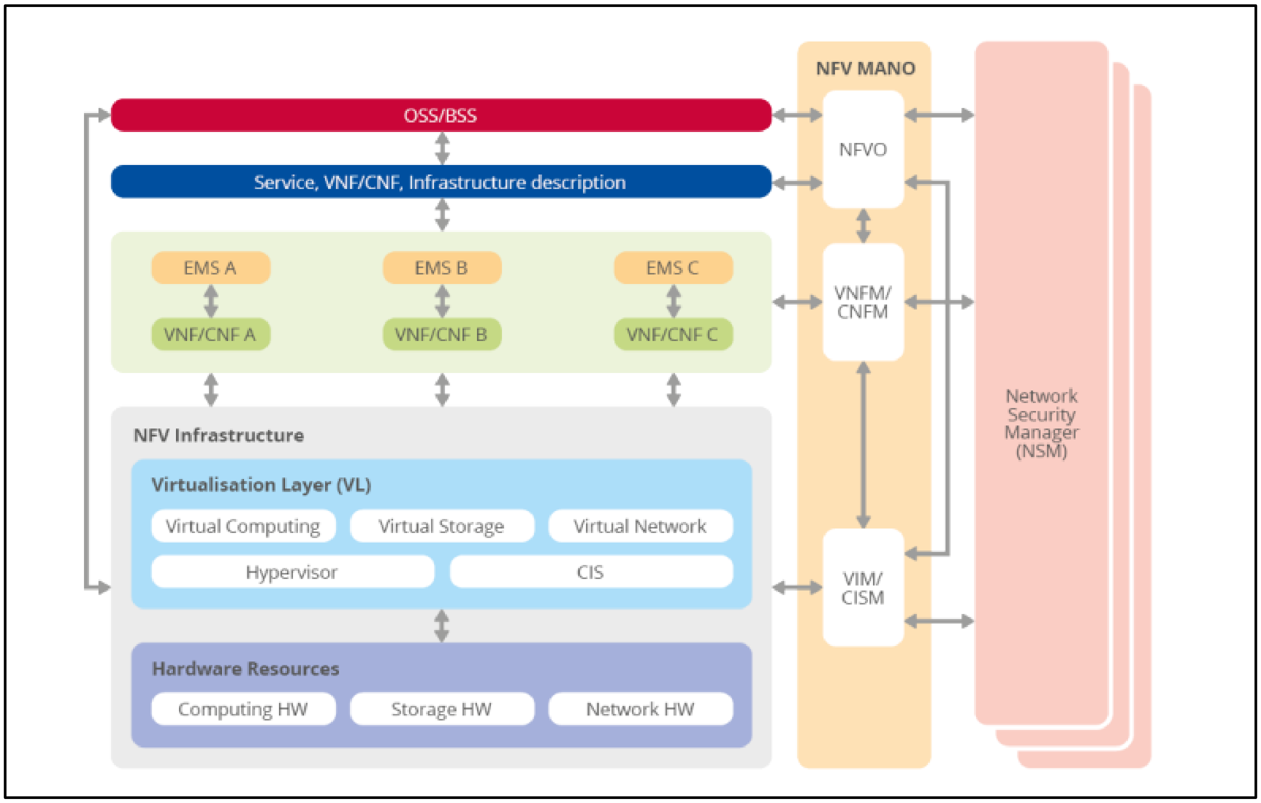

Fig 4 Adapted NFV architecture

NFV Security. Network Functions Virtualization will leverage modern technologies such as those developed for cloud computing to deliver end-end network services using the NFVI. Network function virtualization increases the attack surface. In a traditional telecom environment, it is sufficient to secure the hosts (with their operating systems), the applications running on these hosts, and the communication between these applications. With network function virtualization, it is also necessary to protect the hypervisor/CIS and its communication with the management infrastructure, and employ strict identity and access management. An unsecure hypervisor/CIS will impede adequate isolation of VMs/Containers running on the same host, inadequate identity and access management will result in compromises of the whole NFV infrastructure. With that, unauthorized parties may maliciously or accidentally impact the lifecycle of virtual machines.

A result of network function virtualization is extensive use of APIs. If as much as control of the NFV infrastructure is done programmatically, there shall be strict API access control. In particular, it is essential that there be adequate security control in place when APIs are used to provide orchestration and interaction between virtualized network functions and the underlying infrastructure.

Data protection is an essential aspect of NFV security. It covers data confidentiality, data integrity, and access control. Various data protection techniques can be deployed based on use cases.
The security requirement for NFV is covered in the subsequent chapters.

Chapter 2 – Common Security Requirements

Section 1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:
The system management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.

Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for management and maintenance.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:
The management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.4]

2.1.3 Role-based access control policy

Requirement:
The system shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that determines how users interact with domains and resources.
The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e., the specific operation command or command group (e.g View, Modify, Execute). The system shall support RBAC with minimum of 3 user roles, in particular, for OAM privilege management for System Management and Maintenance, including authorization of the operation for configuration

data and software via the network product console interface.

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.2]

2.1.4. User Authentication – Local/Remote

Requirement:
The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, enables unambiguous authentication and identification of the authorized user.
Authentication attributes include

- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.
Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported.
The same authentication credentials must not be reused on different components of platform, SDN, NFV and MANO.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:
Login to system as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to remotely.

This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the system.

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.6]

2.1.6 Authorization Policy

Requirement:
The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.
Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g. configuration and logging files).
Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications shall not be executed with administrator or system rights.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:
Users shall be identified unambiguously by the system.
System shall support the assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.
System shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.2]

2.1.8 Out of band Management

Requirement:
Management interfaces shall be secured from remote access through Out-of-band management network that is not accessible from the internet. Multi-factor authentication (MFA) shall be used for remote access through VPN.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T08]

Section 2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:
The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g. password, certificate) shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:
If the system supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services) then the communication between system and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

Note: This clause requires external authentication server for testing. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

2.2.3 Protection against brute force and dictionary attacks

Requirement:

A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in system.

Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.

Various measures or a combination of the following measures can be taken to prevent this:

i) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").

ii) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.

iii) Using an authentication attribute blacklist to prevent vulnerable passwords.

iv) Using CAPTCHA to prevent automated attempts (often used for Web applications).

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by System. An exception to this requirement is machine accounts.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

(a) The configuration setting shall be such that a system shall only accept passwords that comply with the following complexity criteria:

(i) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the system). It shall not be possible setting this absolute minimum length to a lower value by configuration.

(ii) Password shall mandatorily comprise all the following four categories of characters:

- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (e.g. @;!$.)

b) The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.

c) If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.

d) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the system.
e) When a user is changing a password or entering a new password, system /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).
Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

Additionally, pepper may be included to increase the complexity i.e password hash is a function of password, salt and pepper.

[Reference: 1) TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3
2) IETF draft-ietf-kitten-password-storage-04-BCP]

2.2.5 Inactive Session timeout

Requirement:
An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.
The system shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity.

Reauthentication of the OAM user shall be repeated following any period of inactivity lasting 15 minutes or longer.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:
If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it shall be possible to implement this function on this system.

Password change shall be enforced after initial login. (After successful authentication)
System shall enforce password change based on password management policy.
In particular, the system shall enforce password expiry. System shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed up to a certain number (Password History). The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its minimum value shall be 3.

This means that the system shall store at least the three previously set passwords. The maximum number of passwords that the system can store for each user is up to the manufacturer.
When a password is about to expire, a password expiry notification shall be provided to the user.
Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.

The system to have in-built mechanism to support this requirement.

If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.
And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the System.

The minimum password age shall be set as one day i.e recycling or flipping of passwords to immediate return to favorite password is not possible.

[Reference: 1) TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.2 2) CIS Password Policy Guide]

2.2.7 Protected Authentication feedback

Requirement:
The Authentication attribute shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "*".

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:
Predefined or default authentication attributes shall be deleted or disabled. (or changed)
Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the OEM provides instructions on how to manually change it.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:
The system shall have a function that allows a signed-in user to logout at any time. All processes under the logged-in user ID shall be terminated on logout. The network product shall be able to continue to operate without interactive sessions.

Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement:
a) The maximum permissible number of consecutive failed user account login attempts shall be configurable by the operator. The definition of the default value set at manufacturing time for the maximum number of failed user account login attempts shall be less than or equal to 8, typically 5. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user, there shall be a block delay in allowing the user to attempt login again. This block delay and the capability to set the period of the block delay, e.g., double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure shall be configurable by the operator. The default value set at manufacturing time for this delay shall be greater than or equal to 5 sec.
b) If supported, infinite (permanent) locking of an account that has exceeded the maximum permissible number of consecutive failed user account login attempts shall also be possible via configuration, with the exception of administrative accounts, which shall get only temporarily locked.

[Reference TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.5]

2.2.11 Suspend accounts on non-use

It shall be possible for the system to automatically suspend an account after 'X' days without a valid login.

Note: X may be specified by operator.

[Reference: CIS Password Policy Guide]

Section 3: Software Security

2.3.1 Secure Update

Requirement:
For software updates, the system shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.
To this end, the system has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update is originated from only these sources.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

(i) The system's Software package integrity shall be validated in the installation /upgrade stage.

(ii) The system shall support software package integrity validation via cryptographic means, e.g., digital signature, code signing certificate (valid and not time expired), and using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only. To this end, the System has a list of public keys or certificates of authorized software sources and uses the keys to verify that the software update originated from only these sources.

(iii) Tampered software shall not be executed or installed if the integrity check fails.

(iv) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in (ii) above.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).

b) Also, OEM shall submit the undertaking as below:

(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the system software which includes OEM developed code, third party software and opensource code libraries used/embedded in the system.

(ii) System software shall be free from CWE top 25, OWASP top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.

(iii)The binaries for system and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

2.3.4 Known Malware and backdoor Check

Requirement:
OEM shall submit an undertaking stating that the system is free from all known malware and backdoors as on the date of offer of system to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the system to the designated TSTL.

2.3.5 No unused software

Requirement:
Software components or parts of software which are not needed for operation or functionality of the system shall not be present.
Orphaned software components /packages shall not be present in system.
OEM shall provide the list of software that are necessary for system’s operation.
In addition, OEM shall furnish an undertaking as “System does not contain Software that is not used in the functionality of System”

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:
The system shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. The system Shall not support following services

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 and v2
- SSHv1
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD

- MOP

Any other protocols, services that are vulnerable are also to be permanently disabled.
Full documentation of required protocols and services (communication matrix) of the system and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:
The system can boot only from the memory devices intended for this purpose.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section- 4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:
The reliable time and date information shall be provided through NTP/PTP server. All elements/functions which require time stamp shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" with NTP/PTP server.

Audit logs shall be generated for all changes to time settings.

Note: RFC 8915 which proposes Network Time Security (NTS) as an extension field for the NTP version 4 is also permitted.

2.3.9 Restricted reachability of services

Requirement:
The system shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability shall be limited to legitimate communication peers.

Administrative services (e.g., SSH, HTTPS, RDP) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.2]

2.3.10 Self Testing

Requirement:
A cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error

state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

Section 4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:
Unused functions i.e the software and hardware functions which are not needed for operation or functionality of the system shall be deactivated in the system's software and/or hardware.
The list of hardware and software functions installed in the system shall match with the ones that have been mentioned and deemed necessary for the operation of the system.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:
OEM to ensure that the system shall not contain software and hardware components that are no longer supported by them or their 3rd Parties including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be given by OEM.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.5]

2.4.3 Avoidance of Unspecified mode of Access

Requirement:
System shall not contain any wireless access mechanism which is unspecified or not declared.
An undertaking shall be given by the OEM as follows:
"The system does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement:
The security event log shall be access controlled (file access rights) such that only privilege users have access to the log files.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:
The system shall log all important Security events with unique System Reference details as given in the Table below.

System shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, protocol, service or program used for access, source and destination IP addresses & ports and the outcome (success or failure) of the event.

Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event types Mandatory or optional)	**Description**	**Event data to be logged**
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the system.	Username
		Source (IP address and ports) if remote access
		Outcome of event (Success or failure)
		Timestamp
Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username,
		Timestamp,
		Length of session
		Outcome of event (Success or failure)
		Source (IP address &port) if remote access
Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username,
		Administered account,
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded,
		Value reached
		Here suitable threshold values shall be defined depending on the individual system.)
		Outcome of event (Threshold Exceeded)
		Timestamp
Configuration change (Mandatory)	Changes to configuration of the system	Change made
		Timestamp

		Outcome of event (Success or failure)
		Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the system that forces a reboot or shutdown OR where the system has crashed.	Action performed (boot, reboot, shutdown, etc.)
		Username (for intentional actions)
		Outcome of event (Success or failure)
		Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the system (e.g. shutdown)	Interface name and type
		Status (shutdown, down missing link, etc.)
		Outcome of event (Success or failure)
		Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	Administrator username,
		Administered account,
		Activity performed (group added or removed)
		Outcome of event (Success or failure)
		Timestamp.
Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	Administrator username
		Administered account
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity

		Type of event
Secure Update (Optional)	Attempt to initiate manual update, initiation of update, completion of update	User identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	Old value of time
		New value of time
		Timestamp
		origin of attempt to change time (e.g.IP address)
		Subject identity
		Outcome of event (Success or failure)
		User identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session.	User identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators (Optional)	Initiation, Termination and Failure of Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Audit data changes (Mandatory)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure)
		Subject identity

		User identity
		origin of attempt to change time (e.g.IP address)
		Details of data deleted or modified
User Login (Mandatory) and Logoff	All use of Identification and authentication mechanisms.	User identity
		Origin of attempt (IP address and port)
		Outcome of event (Success or failure)
		Timestamp

Note: The security events generated by IdAM/IAM are also acceptable.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:

(a) (i) The system shall support (preferably immediate) forwarding of security eve logging data to an external system available in redundant configuration by push or pull mechanism through redundant links.

(ii) Log functions should support secure uploading of log files to a central location or to a system external for the system.

(b) The system shall be able to store the generated audit data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit data. OEM shall submit justification document for sufficiency of local storage requirement

(c) Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only

Note: This clause requires external server for testing [c] above. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause. And also, the system shall support TLS 1.2 or above or IP Sec for ensuring secure log export.

It is recommended that all audit logs are transferred to log management platform outside the entity (NFV/SDN/MANO/Platform) to maintain their integrity and remove the risk of tampering.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.2]

2.5.4 Logging access to personal data

Requirement:
In some cases, access to personal data in a clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes, such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.5]

2.5.5 Security audit log:

Requirement:
The security audit log must not contain

1) Authentication credentials, even if encrypted (e.g password)

Access Tokens-To be masked when outputting

2) Proprietary or sensitive personal information

[Reference: GSMA NG 133 Cloud Infrastructure Reference Architecture Ver 2.0 6.3.7.3]

2.5.6 Audit Logs

Requirement:

1) All security logging mechanisms must be active from system initialization
2) Logs must be time synchronized
3) Security audit logs must be protected in transit and at rest
4) The following systems events must be logged (apart from those listed in 2.5.2)
    a) Successful and unsuccessful changes to privilege level
    b) Successful and unsuccessful security policy changes
    c) Starting and stopping of security logging
    d) Starting and stopping of processes including attempts to start unauthorized processes
    e) All command line activity performed by innate OS programs known to otherwise leave no evidence upon command completion including Power shell on windows system.

[Reference: GSMA NG 133 Cloud Infrastructure Reference Architecture ver 2.0 6.3.7.1 and 6.3.7.2]

2.5.7 Centralized log Auditing

Requirement:
All the NFV, SDN and MANO elements shall submit security events (e.g. authentication, authorization and accounting, login attempts, administration functions and configurations)

to a centralized platform, which shall monitor and analyse in real time the messages for possible attempts at intrusion.

Note: This clause requires external system for testing. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T17]

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:

The system shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

OEM shall submit to TSTL, the list of the connected entities with system and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing the communication with each entity and any other details required for verifying this requirement.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the system (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the system (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards".

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of system shall be in compliance with the respective FIPS standards (for the specific crypto algorithm).

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithm implemented inside the Crypto module of system is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the System)"

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:
a) When system is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.
b) Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.2.]

2.6.5. Protecting data and information in storage

Requirement:
a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.

b) In addition, the following rules apply for:

(i) Systems that need access to identification and authentication data in the clear/readable form e.g. in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.

(ii) Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

(iii) Stored files in the system: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:
a) Without authentication and except for specified purposes, system shall not create a copy of data in use or data in transit.
b) Protective measures shall exist against use of available system functions / software residing in system to create copy of data for illegal transmission.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**
a) System shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit. (Within its boundary).
b) Establishment of outbound overt channels such as, HTTPS, IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the System.
c) Session logs shall be generated for establishment of any session initiated by either user or system.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:
a) System shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit. (Within its boundary).
b) Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the System.
c) Session logs shall be generated for establishment of any session initiated by either user or system.

Section 7: Network Services

2.7.1 Traffic Filtering – Network Level

Requirement:
The system shall provide a mechanism to filter incoming IP packets on any IP interface.
In particular, the system shall provide a mechanism:
(a) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.
(b) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions shall be supported:

- Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
- Accept: the matching message is accepted.
- Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones.

This feature is useful to monitor traffic before its blocking.

(c) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.

(d) To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.

(e) To reset the accounting.

(f) The System shall provide a mechanism to disable/enable each defined rule.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.1]

2.7.2 Traffic Separation

Requirement:
The system shall support the physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 for further information.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.5.1].

2.7.3: Traffic Protection –Anti-Spoofing

Requirement:
The system shall not process IP Packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.3.1.1]

2.7.4 Network security

Requirement:
a) Topology hiding
All internal interfaces between VNF elements, supporting MANO platforms and IT elements (mediation, provisioning) that are not required to publicly communicate outside the operator's network, shall use private IP addresses.

b) Deploy NFVs with separate dedicated interfaces
Ideally, separate physical interfaces shall be implemented to maintain different traffic segregation in line with security zoning and X.805 principles. However, if this is not supported, then a separate logical interface and VLAN must be used to maintain security zoning.

c) Production and O&M traffic separation
O&M interfaces shall not share the same physical NIC, vNIC, distributed port group (DPG) or

port group with other production traffic types (e.g. BSS, User Plane or Signalling)

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

d) Connectivity from management to production cluster

Any connectivity between the operation and management (MANO) cluster and the production cluster shall pass through a firewall. If a virtual firewall is implemented, it shall be implemented within the management cluster.

Note 1: It is expected that MANO systems would not share the same hypervisor or CIS environment as production NFV elements.

Note 2: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

e) Network resource pools

To prevent a VM or container causing a DoS by monopolizing system and network resources, network resource pools shall be configured.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

f) Internal virtual switching control

The internal hypervisor or CIS controlled virtual IP network (vSwitch/VDS) shall be controlled to ensure a policy of positive enabling and must not support default connectivity or ‘any to any’ functionality.

g) Virtual network monitoring

In some deployments, internal network monitoring functions can be installed on the virtualization layer. If these are installed, the functions must be restricted to the administrator only and shall not provide a mechanism for compromising the security of the hypervisor or CIS or other VMs or containers.

Additionally, any operation of this type of monitoring functionality shall generate an alarm to the VIM and be recorded in the audit logs.

h) VLAN and VXLAN zoning

A comprehensive set of common VLAN and VXLANs must be created across each NFVi to ensure traffic separation and security zoning requirements.

Note: VLAN and VXLAN zoning shall ensure that clear vendor separation is maintained.

Only VLAN and VXLANs necessary to support VNFs hosted on a cluster shall be configured on the 'leaf' and 'spine' switching layers. The VLAN IP infrastructure shall follow existing segmentation and zoning rules with the use of firewalls or other security controls to provide protection between zones.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

The hardware firewall appliances shall to be used to provide boundary protection when connecting to untrusted or semi-trusted networks (e.g. internet or GRX).

i) Dedicated network infrastructure
If a third party XaaS provider is being used then the dedicated local 'leaf' switching infrastructure supporting only the operator VNFs shall be provided to ensure segregation from other tenants.
Additionally, dedicated spine switches shall be provided.

j) Protect all OAM traffic
Link security shall be provided through the use of native traffic encryption such as HTTPS, SFTP, SNMP v3 or using TLS or IPsec tunnelling protocols.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T21]

Section 8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

Requirement:
The system shall have protection mechanism against Network level and Application-level DDoS attacks.
The system shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

- For example, potential protective measures include:
- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application

- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:
The system shall act in a predictable way if an overload situation cannot be prevented. System shall be built in this way that it can react on an overload situation in a controlled way. However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that System cannot reach an undefined and thus potentially insecure, state.

OEM shall provide a technical description of the System's Over Load Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements e.g. RAN)

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]

2.8.3 Manipulated packets that are sent to an address of the network device shall not lead to an impairment of availability

Requirement:
The system shall not be affected in its availability or robustness by incoming packets from other network elements that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of the System. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.
Examples of such packets are:

- Mass-produced TCP packets with a set SYN flag to produce half-open TCP connections (SYN flooding attack).
- Packets with the same IP sender address and IP recipient address (Land attack).

- Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
- Fragmented IP packets with overlapping offset fields (Teardrop attack).
- ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IPv4 packets (Ping-of-death attack).
- Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.6.2.2]

Section 9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:
It shall be ensured that externally reachable services of system are reasonably robust when receiving unexpected input.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.4]

2.9.2 Port Scanning

Requirement:
It shall be ensured that on all network interfaces of system, only documented ports on the transport layer respond to requests from outside the system.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:
The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide remediation plan.

Sl No	CVSS Score	Severity	Remediation
1	9.0-10.0	Critical	To be patched immediately
2	7.0-8.9	High	To be patched within a month
3	4.0-6.9	Medium	To be patched within three months
4	0.1-3.9	Low	To be patched within a year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Reference 1: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.3
Reference 2: GSMA NG 133 Cloud Infrastructure Reference Architecture]

Section 10: Operating System

2.10.1 Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions.
b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop the system from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the system.
system shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet too Big	Permitted	N/A
N/A	135	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

The system shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e., do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

N/A: Not Applicable

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

Requirement:

The system shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:

Each system account shall have a unique identification with appropriate non-repudiation controls.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.2.2]

2.10.5 OS Hardening - Minimized kernel network functions

Requirement:

Kernel-based network functions not needed for the operation of the network element shall be deactivated. In particular, the following ones shall be disabled by default:

1. IP Packet Forwarding between different interfaces of the network product.
2. Proxy ARP
3. Directed broadcast
4. IPv4 Multicast handling
5. Gratuitous ARP messages

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.2]

2.10.6 No automatic launch of removable media

Requirement:
The system shall not automatically launch any application when a removable media device is connected.
[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.3]

2.10.7 External file system mount restrictions

Requirement:
If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in the system in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.
OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g. USB drive, CD ROM etc.) for data transfer.

[Reference– TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.6]

2.10.8 File-system Authorization privileges

Requirement:
The system shall be designed to ensure that only users that are authorized to modify files, data, directories, or file systems have the necessary privileges to do so.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.2.7]

2.10.9 SYN Flood Prevention

Requirement:
The system shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.4]

2.10.10 Handling of IP options and extensions

Requirement:
IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all

packets with enabled IP options or extension headers shall be filtered.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.2.4.1.1.3]

Section 11: Web Servers

This entire section of the security requirements is applicable if the system supports **web management interface.**

2.11.1 HTTPS

Requirement:
The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:
Access to the webserver (for both successful as well as failed attempts) shall be logged by system.
The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL shall be included whenever possible.
- Status code of web server response

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:
The system shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
System shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:

No system web server processes shall run with system privileges.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:
HTTPS methods that are not required for system operation shall be deactivated.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:
All optional add-ons and components of the web server shall be deactivated if they are not required for system operation.

In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.4]

2.11.7 No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:
If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

Requirement:
If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:
If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:
Access rights for system’s web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.8]

2.11.11 No default content

Requirement:
Default content that is provided with the standard installation of the system's web server shall be removed.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.9]

2.11.12 No directory listings

Requirement:
Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

Requirement:
The HTTPS header shall not include information on the version of the system's web server and the modules/add-ons used.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:
User-defined error pages and Error messages shall not include version information and other internal information about the system web server and the modules/add-ons used. Default error pages of the system web server shall be replaced by error pages defined by the OEM.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:
File type or script-mappings that are not required for system operation shall be deleted.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:
Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the system web server's document directory.
In particular, the system web server shall not be able to access files which are not meant to be delivered.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.14]

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:
If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.
[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.15]

2.11.18 HTTP User session

Requirement:
To protect user sessions, system shall support the following session ID and session cookie requirements:

1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
2. The session ID shall be unpredictable.
3. The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
4. In addition to the Session Idle Timeout, system shall automatically terminate sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.
5. Session IDs shall be regenerated for each new session (e.g., each time a user logs in).
6. The session ID shall not be reused or renewed in subsequent sessions.
7. The system shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.
8. Where session cookies are used the attribute 'HttpOnly' shall be set to true.
9. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
10. Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
11. The system shall not accept session identifiers from GET/POST variables.
12. The system shall be configured to only accept server generated session ID.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.3]

Section 12: Other Security requirements

2.12.1 Remote Diagnostic Procedure – Verification

Requirement:

If the system is providing Remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user.

All activities performed by the remote user are to be logged with the following parameters:

1. User id
2. Time stamp
3. Interface type
4. Event level (e.g. CRITICAL, MAJOR, MINOR)
5. Command/activity performed and
6. Result type (e.g. SUCCESS, FAILURE).
7. IP Address of remote machine

2.12.2 No System Password Recovery

Requirement:

No provision shall exist for System / Root password recovery.

2.12.3 Secure System Software Revocation

Requirement:

Once the system software image is legally updated/upgraded with New Software Image, it shall not be possible to roll back to a previous software image.

In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls.

System shall support a well-established control mechanism for rolling back to previous software image.

2.12.4 Software Integrity Check –Installation

Requirement:

System shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only.

Tampered software shall not be executed or installed if integrity check fails.

2.12.5 Software Integrity Check – Boot

Requirement:

The system shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” to the expected reference value.

2.12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

System shall support the mechanism to verify both the physical and logical interfaces exist in the product.
Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

2.12.7 No Default Profile

Requirement:
Predefined or default user accounts (other than Admin/Root) in system shall be deleted or disabled.

Chapter 3 Specific Security Requirements

Part 1 NFV Infrastructure (Platform)

This part presents the NFV infrastructure(platform) specific security requirements. NFV infrastructure, here does not include virtualization layer. Kindly refer to Fig 5 below for different security domains

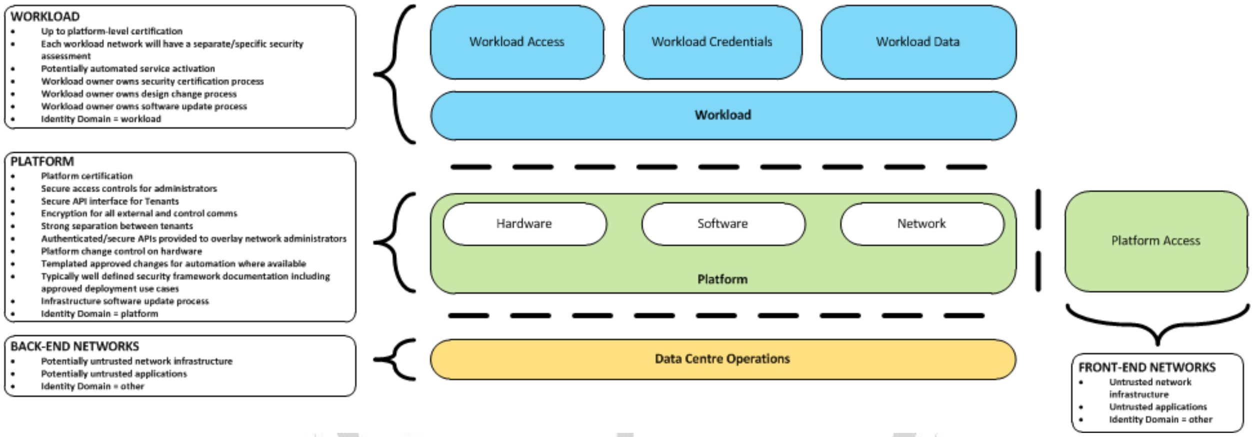
WORKLOAD
Up to platform-level certification
Each workload network will have a separate/specific security assessment
Potentially automated service activation
Workload owner owns security certification process
Workload owner owns design change process
Workload owner owns software update process
Identity Domain = workload
PLATFORM
Platform certification
Secure access controls for administrators
Secure API interface for Tenants
Encryption for all external and control comms
Strong separation between tenants
Authenticated/secure APIs provided to overlay network administrators
Platform change control on hardware
Templated approved changes for automation where available
Typically well defined security framework documentation including approved deployment use cases
Infrastructure software update process
Identity Domain = platform
BACK-END NETWORKS
Potentially untrusted network infrastructure
Potentially untrusted applications
Identity Domain = other
Workload Access
Workload Credentials
Workload Data
Workload
Hardware
Software
Network
Platform
Platform Access
Data Centre Operations
FRONT-END NETWORKS
Untrusted network infrastructure
Untrusted applications
Identity Domain = other

Fig 5 Security Domain

Cloud Infrastructure: A generic term covering NFVI, IaaS and CaaS capabilities - essentially the infrastructure on which a Workload can be executed.
Platform here include hardware, software and network that supports workloads i.e cloud infrastructure with all its hardware and software components.
Workload: An application (for example VNF, or CNF) that performs certain task(s) for the users. In the Cloud Infrastructure, these applications run on top of compute resources such as VMs or Containers.
Front-End Networks: to get access from internet and virtual/physical network used by carriage networks
Back-end networks: Datacenter operations access to the platform and subsequently, workloads.

3.1.1 Launch Environment

Requirement:
The hypervisor that is launched shall be part of a platform and an overall infrastructure that contains:
(a) hardware that supports an Measured Launch Environment (MLE) with standards-based cryptographic measurement capabilities and storage devices and

(b) an attestation process with the capability to provide a chain of trust starting from the hardware to all hypervisor components. Moreover, the measured elements shall include, at minimum, the core kernel, kernel support modules, device drivers, and the hypervisor's native management applications for VM Lifecycle Management and Management of Hypervisor. The chain of trust shall provide assurance that all measured components have not been tampered with and that their versions are correct (i.e., overall boot integrity). If the chain of trust is to be extended to guest VMs, the hypervisor shall provide a virtual interface to the hardware-based MLE.

[Reference: NIST SP 800-125A REV. 1 Security Recommendations for server-based Hypervisor platforms]

3.1.2 CPU Pinning

Requirement:
When a VM instance is created, the vCPUs are, by default, not assigned to a particular host CPU. Certain workloads require real-time or near real-time behavior viz., uninterrupted access to their cores. For such workloads, CPU pinning shall be possible to bind an instance's vCPUs to a particular host' cores or SMT threads.

Note: It is possible for OEM to demonstrate this clause with an example of CPU pinning.

[Reference: GSMA NG.133 - Cloud Infrastructure Reference Architecture]

3.1.3 Workload Placement

Requirement:
Affinity Rule: It specifies workloads that shall be hosted on the same computer node.
Non-Affinity Rule: It specifies workloads that shall not be hosted on the same computer node.
It shall be possible to segregate workloads based on server groups (affinity and non-affinity groups)
Note: It should be possible for OEM to demonstrate this clause with examples

[Reference: GSMA NG.133 - Cloud Infrastructure Reference Architecture]

3.1.4 SR-IOV and DPDK Considerations

Requirement:
Acceleration techniques like DPDK, SR-IOV usually bypasses security protections. Measures shall be taken to ensure security when these technologies are employed to accelerate network packet processing.

Note: OEM shall give the list of measures which shall be verified

3.1.5 Isolation

Requirement:

The physical management interfaces like Baseband Management Controller, integrated lights out (iLO) etc shall use a dedicated network which is separate from virtualization fabric network.

3.1.6 Top of the Rack (ToR) Switches

Requirement:
The ToR switches shall be programmed to limit the VLAN/VXLANs used by hosts within the rack to only those virtual networks made accessible to the hosts.

3.1.7 Hardware-Based Root of Trust (HBRT)

Requirement:
a) The host system shall include an HBRT or Trusted Platform Module (TPM) as Initial Root of Trust. The HBRT shall be based on hardware-based TPM or equivalent hardware root of trust (e.g., Secure Element including TPM functionalities, HSM including TPM functionalities).

b) The host system HBRT shall be able to provide isolated instances of the HBRT capabilities for individual workloads.

c) The host system HBRT shall include a hardware-based compute engine to be used by the workloads for cryptographic and security functionality.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 8.10]

3.1.8 Core Hardware -HBRT

Requirement:

(a) The HBRT shall be both physically and electronically tamper-resistant.
(b) The HBRT shall be both physically and electronically tamper-evident.
(c) The HBRT physical and software interfaces between the HBRT and other hardware components of the host system to which it directly communicates shall be protected from eavesdropping, manipulation, replay or similar attacks.
(d) The level of resistance against attacks of the HBRT shall be verifiable and trustable using a certification process.
(e) It shall be possible to restrict the booting procedure if assistance from the HBRT is not available or the HBRT currently does not contain valid cryptographic material.
(f) Any tampering to the HBRT shall lead to detectable degradation of its function.
(g) The HBRT shall be physically protected such that any attempts to remove or replace the HBRT shall cause physical damage to both the HBRT and host system hardware to which the HBRT is attached, rendering both inoperable.

(h) The HBRT shall be (physically and/or logically) bound to the host system, so that any attempt to remove the HBRT will be detected and prevent normal operation of the host system.

(i) The HBRT shall include an Immutable Unique Identification value physically linked to the physical root of trust that can be used as identification of the platform. This value shall be stored in a shielded location protected from unauthorized use and disclosure.

(j) The HBRT shall provide capabilities to allow itself to be part of an attestation function.

(k) The host system shall have a mechanism to discover the tampered/non-tampered status of the HBRT.

(l) The host system shall have an interface to provide authorized external services with information about the tampered/non-tampered status of the HBRT.

(m) The host system shall provide a mechanism to report to authorized external services when tamper events occur.

Note: OEM shall submit an undertaking along with Explanatory Note

[Reference: ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 5.1]

3.1.9 Chain of Trust (CoT)

Requirement:

a) The chain of trust (CoT) is a method for maintaining valid trust boundaries by applying a principle of transitive trust. Each firmware module in the system boot process is required to measure the next module before transitioning control. Once a firmware module measurement is made, it is required to immediately extend the measurement value to a root of trust for storage, such as an HSM register, for attestation at a later point in time

b) Static Root of Trust for Measurement (SRTM) begins with measuring and verifying the integrity of the BIOS firmware. It then measures additional firmware modules, verifies their integrity, and adds each component's measure to an SRTM value. The final value represents the expected state of boot path loads. SRTM stores results as one or more values stored in PCR storage. In SRTM, the CRTM resets PCRs 0 to 15 only at boot.

The host system shall support static root-of-trust measurement for hardware-based remote attestation.

c) In Dynamic Root of Trust for Measurement (DRTM), the RTM for the running environment is stored in PCRs starting with PCR 17. The host system shall support dynamic root-of-trust measurement for hardware-based remote attestation.

d) The chain of trust rooted in hardware shall be extended to the OS kernel and its components to enable cryptographic verification of trusted boot, system images, container runtimes and container images and so on. Chain of trust across hardware, operating system, hypervisor, VM, and container shall be ensured. Using a Trusted Platform Module (TPM), as a hardware root of trust, measurements of platform components, such as firmware, bootloader, OS kernel, shall be securely stored and verified.

[Reference: GSMA NG.126 - Cloud Infrastructure Reference Model]

3.1.10 Remote attestation

Requirement:
a) The remote attestation (RA) technique can be used to remotely verify the trust status of an NFV platform. ETSI suggests leveraging hardware security module (HSM), trusted platform module (TPM) and virtual TPM/HSM (vTPM/vHSM) to provide trusted protection for VNFs. These modules are used to shelter integrity measurements (i.e. hash values), cryptographic keys and certificates that are required to empower remote attestation of VNF components. Indeed, remote attestation guarantees the integrity of VNF instances at load time.
It shall be possible to attest a VNF through the full attestation chain from the hardware layer through the virtualization layer to the VNF layer.

b) Attestation of a platform’s integrity shall be linked to the application layer and possible for other functions to query. If platform attestation fails, the VNF shall not be allowed to run.

c) Attestation of the VNF shall be performed prior to deployment or network integration and during operations.

Scenarios aimed to establish specific trust between NFV stakeholders:

(1) measurement of VM during launch,
(2) protected VM launch on a trusted NFVI,
(3) measurement of VM during launch and while in use,
(4) remote attestation of secret storage,
(5) secure VM migration between two trusted NFVIs.

[Reference: 1) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T9] 2) ETSI GR NFV-SEC 018 NFV Security Report on NFV Remote Attestation Architecture]

3.1.11 Asset Tagging and Trusted Location

Requirement:
It shall be possible to assign specific labels for each server in the cloud infrastructure to enforce isolation of critical workloads and remotely attest each server’s measurement and label against policies, feeding the results into a policy orchestrator to report, alert, or enforce rules based on events.

[Reference: NISTIR 8320A Hardware-Enabled security]

3.1.12 Trusted computing technologies

Requirement:

a) Silicon-based security functionality (for example Intel TXT, SGX, AMD SEV or ARM Trust zone) shall be implemented with a TPM that stores measurements of the entire hypervisor or CIS stack and boot process to provide a trusted hardware platform.

This measure shall be applied to:

i) blade clusters supporting VNF that support security critical functions; for example, lawful interception, customer access credential (HSS), security key management (AuC) or that have external traffic interfaces directly accessed by third parties or customers (Internet, GRX)

ii) all other MANO and VNF blade clusters to improve base platform security and reduce the complexity of affinity rules and hardware cluster of differing security trust levels.

b) A mechanism shall be in place to identify any attempt to physically remove the TPM from a system board. If physical tampering has been identified the blade server shall be considered compromised and no longer be used to support VNFs.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T15]

3.1.13 Local or removable blade storage – SAN protection (applicable if SAN is used)

Requirement:

(a) Local storage protection

(b) If local blade storage is supported, then it shall not store sensitive information such that its theft or removal would enable an attacker to gain a copy of the stored data.

(c) Mutual authentication between VMs or containers and SA

(d) Mutual authentication shall be implemented between each VM or container and its associated SAN storage using CHAP (e.g. DH-CHAP, FCPAP).

(e) SAN data protection in transit

(f) The sensitive data in transit between NFV and SAN shall be protected using encapsulated security payload (ESP), as specified by the fiber channel protocol (FC-SP) or equivalent.

(g) SAN physical blade interface

(h) Separate physical interface module shall be used on each blade or rack mounted server for connectivity to the SAN. Any SAN connectivity shall not share common IP interface with other operational traffic.

(i) SAN storage protection

The SAN storage shall protect against tampering and any ability to create unauthorized local copies of any of the stored data.

In the event of tampering or unauthorized copying, an alarm and log event shall be generated recording what data has been copied and which user initiated the action.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T20]

3.1.14 Key Management System

Requirement:
a) The host system shall implement a key management system which includes key generation, key storage, key deletion and cryptographic processing with the following requirements:
i) The cryptographic material shall be stored in a shielded location, protected against eavesdropping and physical and environmental tampering.
ii) The key generation processing shall be protected against eavesdropping and physical and environmental tampering.
iii) The key management system shall include an access right management to the sensitive data.
iv) The key management system shall ensure a complete deletion of outdated keys under deletion request.
v) The key management system shall be scalable and ensure a high availability service.
vi) The key management system shall be remotely manageable to allow evolution, security strengthening, and countermeasure deployment of the system.

b) The host system shall provide cryptographically separated secure environments to different applications.

Note: This clause requires key management system for testing. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 5.1]

3.1.15 Server boot hardening

Requirement:

The server boot process must be trusted. For this purpose, the integrity and authenticity of all BIOS firmware components must be verified at boot. Secure Boot based on Unified Extensible Firmware Interface must be used. By verifying the signatures of all BIOS components, Secure Boot will ensure that servers start with the firmware expected and without malware insertion into the system.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v1.0 Section: 6.3.1.1]

3.1.16 De-provisioning workloads

Requirement:

a) The host system shall provide

i) the capability to perform a secure wipe of storage at the request of authorized external services.

ii) a mechanism by which authorized external services can confirm the completion of the secure wipe operation.

iii) a mechanism to ensure that storage which is in the process of a secure wipe cannot be re-allocated until that operation is successfully completed.

iv) a mechanism to perform a secure wipe, at the time of de-provisioning, of any and all files associated with a workload.

Note: This is normally triggered by application layer.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.7]

3.1.17 Dealing with failure

Requirement:

(a) The host system shall be booted with debug options off by default.

(b) It shall make a record when debug options are turned on, and a specific log entry shall be created. This record shall be unalterable without a power-off or reboot of the host system.

(c) It shall have an interface to provide authorized external services with information about the state of its debug options, including their historical state since boot.

(d) It shall provide a mechanism to report to authorized external services when a change in debug status occurs.

(e) Requirements relating to failure conditions:

i) The host system shall have an interface to provide authorized external services with information related to failures or replacement of its components.

ii) The host system shall provide a mechanism to report to authorized external services when failures occur.

Note: External Services may be requested by Remote Attestation Server or Trust Broker

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.8]

3.1.18 Direct access to memory

Requirement:
The host system shall be able to deny direct access to memory to particular hardware resources.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 8.12]

3.1.19 Function and Software

Requirement:
a) Infrastructure must be implemented to perform at least the minimal functions needed to operate the Cloud Infrastructure.

Regarding software:

i) Only that software which is required to support the functions shall be installed.
ii) Any unnecessary software or packages shall be removed.
iii) Where software cannot be removed, all services to it shall be disabled.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture v1.0 section: 6.3.1.4]

3.1.20 System Hardening

Requirement:

a) The Platform must maintain the specified configuration.
b) All systems part of Cloud Infrastructure must support password rules defined in Chapter 2.
c) All servers part of Cloud Infrastructure must support a root of trust and secure boot.
d) The Operating Systems of all the servers part of Cloud Infrastructure must be hardened by removing or disabling unnecessary services, applications and network protocols, configuring operating system user authentication, configuring resource controls, installing and configuring additional security controls where needed, and testing the security of the Operating System
e) The Platform must support Operating System level access control.
f) The Platform must support Secure logging. Logging with root account must be prohibited when root privileges are not required.
g) All servers part of Cloud Infrastructure must be Time synchronized with authenticated Time service.
h) All servers part of Cloud Infrastructure must be regularly updated to address security vulnerabilities.
i) The Platform must support Software integrity protection and verification and must scan software artefacts and manifests.

j) The Cloud Infrastructure must support encrypted storage, for example, block, object and file storage, with access to encryption keys restricted based on a need to know. Controlled Access Based on the Need to Know.

k) The Cloud Infrastructure should support Read and Write only storage partitions (write only permission to one or more authorized actors).

l) It must be ensured that only authorized actors have physical access to the underlying infrastructure.

m) The Platform must ensure that only authorized actors have logical access to the underlying infrastructure.

n) Any change to the Platform must be logged as a security event, and the logged event must include the identity of the entity making the change, the change, the date and the time of the change.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.1]

3.1.21 Platform and Access

Requirement:

a) The Platform must support authenticated and secure access to API, GUI and command line interfaces.

b) The Platform must support Traffic Filtering for workloads (for example, Fire Wall).

c) The Platform must support Secure and encrypted communications, and confidentiality and integrity of network traffic.

d) The Cloud Infrastructure must support authentication, integrity and confidentiality on all network channels.

e) The Cloud Infrastructure must segregate the underlay and overlay networks.

f) The Cloud Infrastructure must be able to utilize the Cloud Infrastructure Manager and identity lifecycle management capabilities

g) The Platform must implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control).

h) The Platform must be able to assign the Entities that comprise the tenant networks to different trust domains

i) The Platform must support creation of Trust Relationships between trust domains.

j) For two or more domains without existing trust relationships, the Platform must not allow the effect of an attack on one domain to impact the other domains either directly or indirectly.

k) The Platform must not reuse the same authentication credential (e.g., key-pair) on different Platform components (e.g., on different hosts, or different services).

l) The Platform must protect all secrets by using strong encryption techniques, and storing the protected secrets externally from the component.
Note: OEM shall enable the feature to access the protected secrets stored externally from the component which shall be testable.

m) The Platform must provide secrets dynamically as and when needed.
Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

n) The Platform shall use Linux Security Modules(applicable for Linux Platform) such as SEL inox to control access to resources.

o) The Platform must not contain back door entries (unpublished access points, APIs, etc.).

p) Login access to the platform's components must be through encrypted protocols such TLS v1.2 or higher

q) The Platform must provide the capability of using digital certificates that comply with X.509 standards issued by a trusted Certification Authority.

r) The Platform must provide the capability of allowing certificate renewal and revocation.

s) The Platform must provide the capability of testing the validity of a digital certificate (CA signature, validity period, non-revocation, identity).

t) The Cloud Infrastructure architecture shall rely on Zero Trust principles to build a secure by design environment

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.2]

3.1.22Workload Security

Requirement:

a) The Platform must support Workload placement policy.

b) The Cloud Infrastructure must provide methods to ensure the platform’s trust status and integrity (e.g. remote attestation, Trusted Platform Module).

c) The Platform must support secure provisioning of workloads.

d) The Platform must support Location assertion.

e) The Platform must support the separation of production and non-production Workloads.

f) The Platform must support the separation of Workloads based on their categorisation.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.4]

3.1.23 Image security on cloud Platform

Requirement:

In order to maintain Images securely the following requirements shall be followed

a) Images must be scanned to be maintained free from known vulnerabilities.
b) Images must not be configured to run with privileges higher than the privileges of the actor authorized to run them.
c) Images must only be accessible to authorized actors.
d) Image Registries must only be accessible to authorized actors.
e) Image Registries must only be accessible over secure networks that enforce authentication, integrity and confidentiality.
f) Image registries must be clear of vulnerable and out of date versions.
g) Images must not include any secrets. Secrets include passwords, cloud provider credentials, SSH keys, TLS certificate keys, etc.
h) CIS Hardened Images shall be used whenever possible.
i) Minimalist base images shall be used whenever possible.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.5]

3.1.24 Lifecycle management Security on cloud

Requirement:

The following aspects of lifecycle management shall be fulfilled

a) The Platform must support Secure Provisioning, Availability, and Deprovisioning (Secure Clean-Up) of workload resources where Secure Clean-Up includes tear-down, defense against virus or other attacks through signature-based AV scan.
b) The Cloud Operator must implement and strictly follow change management processes for Cloud Infrastructure, Cloud Infrastructure Manager and other components of the cloud, and Platform change control on hardware.
c) The Cloud Operator shall support automated templated approved changes.
d) The Platform must provide logs and these logs must be regularly monitored for anomalous behavior.
e) The Platform must verify the integrity of all Resource management requests.
f) The Platform must be able to update newly instantiated, suspended, hibernated, migrated and restarted images with current time information.
g) The Platform must be able to update newly instantiated, suspended, hibernated, migrated and restarted images with relevant DNS information.

h) The Platform must be able to update the tag of newly instantiated, suspended, hibernated, migrated and restarted images with relevant geolocation (geographical) information.
i) The Platform must log all changes to geolocation along with the mechanisms and sources of location information (i.e. GPS, IP block, and timing).
j) The Platform must implement Security life cycle management processes including the proactive update and patching of all deployed Cloud Infrastructure software.
k) The Platform must log any access privilege escalation.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.6]

3.1.25 Confidentiality and Integrity protection on Platform

Requirement:
The following requirements shall be fulfilled for Confidentiality and Integrity protection on Platform

a) The Platform must support Confidentiality and Integrity of data at rest and in transit.
b) The Platform must support Confidentiality and Integrity of data related metadata.
c) The Platform must support Confidentiality of processes and restrict information sharing with only the process owner (e.g., tenant).
d) The Platform must support Confidentiality and Integrity of process-related metadata and restrict information sharing with only the process owner (e.g., tenant).
e) The Platform must support Confidentiality and Integrity of workload resource utilization (RAM, CPU, Storage, Network I/O, cache, hardware offload) and restrict information sharing with only the workload owner (e.g., tenant).
f) The Platform must not allow Memory Inspection by any actor other than the authorized actors for the Entity to which Memory is assigned (e.g., tenants owning the workload), for Lawful Inspection, and by secure monitoring services.
g) The Cloud Infrastructure must support tenant networks segregation.
h) For sensitive data encryption, the key management service shall leverage a Hardware Security Module to manage and protect cryptographic keys.

[Reference: 1) GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.3 2) NSA-CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

3.1.26 Protection of data at rest

Requirement:
The following requirements shall be met

a) All data persisted to primary, replica, or backup storage shall be encrypted.

b) It must be ensured that all forms of data at rest are protected using strong cryptographic algorithms with strong integrity protection as prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” Only.

c) User authentication related to access to data at rest shall use multi-factor authentication or Public Key Infrastructure (PKI) based certificate authentication.

d) Backup storage can incorporate data integrity protection measures like a write once and read many approaches.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part III: Data Protection (2021), Section-Protection of Data-at-rest]

3.1.27 Protection of data in use

Protecting and securing cloud data while *in use*, also referred to as *confidential computing*, utilizes hardware-enabled features to isolate and process encrypted data in memory so that the data is at less risk of exposure and compromise from concurrent workloads or the underlying system and platform.

A *trusted execution environment (TEE)* is an area or enclave protected by a system processor. Sensitive data like cryptographic keys, authentication strings, or data with intellectual property and privacy concerns can be preserved within a TEE, and operations involving these data can be performed within the TEE, thereby eliminating the need to extract the secrets outside of the TEE. A TEE also helps ensure that operations performed within it and the associated data cannot be viewed from outside, not even by privileged software or debuggers. Communication with the TEE is designed to only be possible through designated interfaces, and it is the responsibility of the TEE designer/developer to define these interfaces appropriately. A good TEE interface limits access to the bare minimum required to perform the task.

A hardware-mediated execution enclave is defined as an area of process space and memory within a system environment within a computer host which delivers confidentiality and integrity of instructions and data associated with that enclave. This enclave is protected from eavesdropping, replay and alteration attacks as the programs within the enclave are executed. An enclave is considered capable of executing processes, and executable code can be loaded into it. Encrypted data and code in the TEE is unavailable to other applications, the BIOS, operating systems, kernels, administrators, cloud vendors, and hardware components except CPUs. TEE-based confidential computing collaborates with sandboxed containers to isolate malicious applications and protect sensitive data.

Requirement:
The following requirements shall be met

a) The host system shall provide workloads access to hardware-mediated execution enclaves (HMEE).

b) The host system shall make use of hardware-mediated execution enclaves when protecting its own sensitive processes
c) The host system shall provide the ability for authorized actors to perform a secure wipe of sections of memory in the HMEE.
d) The host system shall provide workloads with isolated enclaves.

[Reference: 1) NSA-CISA Security Guidance for 5G Cloud Infrastructures Part III: Data Protection (2021), Section-Protection of Data-in-use 2) ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 8.9]

3.1.28 Workload Provisioning

Requirement:

a) The host system shall have an interface to provide authorized external services with information about its ability to prohibit host or hypervisor memory deduplication techniques that allow for sharing of memory pages between workloads.
b) The host system shall provide a mechanism to disable host or hypervisor memory deduplication techniques that allow for sharing of memory pages between workloads.
c) The host system shall disable host or hypervisor memory deduplication techniques that allow for sharing of memory pages between workloads by default. Where a capability is disabled, it shall not be possible re-enable it without a host system reboot.
d) The host system shall allow appropriately authorized parties to specify that certain memory types or locations (e.g. volatile vs non-volatile, on-blade vs off-blade) are not used for particular workloads.
e) The host system shall allow appropriately authorized parties to specify that only certain memory types or locations (e.g. volatile vs non-volatile, on-blade vs off-blade) are used for particular workloads
f) The host system shall provide the ability to prohibit local caching of binary images for workloads.
g) The host system shall have an interface to provide authorized external services with information about its ability to prohibit binary image caching.
h) The host system shall have an interface to provide authorized external services with information about its ability to provide perform secure provisioning of workloads.
i) The host system shall have an interface to provide authorized external services with information about its ability to provide secure de-provisioning of workloads.
j) The host system shall have an interface to provide authorized external services with information about its ability to block migration of workloads.
k) The host system shall provide secure provisioning of workloads.
l) The host system shall provide secure de-provisioning of workloads.

Note: External services may be requested by Remote Attestation Server or Trust Broker

[Reference: ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Sec 6.2]

Infrastructure as a Code

Infrastructure as a Code (IaaC) (or also called Infrastructure as Code, IaC) refers to the software used for the declarative management of cloud infrastructure resources.

3.1.29 Secure Design and Architecture

Requirement:

a) Threat Modelling methodologies and tools shall be used during the Secure Design and Architecture stage triggered by Software Feature Design trigger. Security Control Baseline Assessment shall be performed during the Secure Design and Architecture stage triggered by Software Feature Design trigger.

b) Security Control Baseline Assessment shall be performed during the Secure Design and Architecture stage triggered by Software Feature Design trigger

Note: OEM shall submit an undertaking

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.9]

3.1.30 Secure Code Stage

Requirement:

The code shall be secured by adhering to the below mentioned requirements

a) Static Application Security Testing must be applied during the Secure Coding stage triggered by Pull, Clone or Comment trigger.

b) Software Composition Analysis shall be applied during Secure Coding stage triggered by Pull, Clone or Comment trigger

c) Source Code Review shall be performed continuously during the Secure Coding stage.

d) Integrated SAST via IDE Plugins shall be used during the Secure Coding stage triggered by Developer Code trigger.

e) SAST of Source Code Repo shall be performed during the Secure Coding stage triggered by Developer Code trigger.

Note: OEM shall submit an undertaking

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.10]

3.1.31 Continuous Build, Integration and Testing Stage

Requirement:

The following requirements shall be met during Build, Integration and Testing Stage

a) Static Application Security Testing shall be applied during the Continuous Build, Integration and Testing stage triggered by Build and Integrate trigger.
b) Software Composition Analysis shall be applied during the Continuous Build, Integration and Testing stage triggered by Build and Integrate trigger.
c) Image Scan must be applied during the Continuous Build, Integration and Testing stage triggered by Package trigger.
d) Dynamic Application Security Testing shall be applied during the Continuous Build, Integration and Testing stage triggered by Stage & Test trigger
e) Fuzzing shall be applied during the Continuous Build, Integration and testing stage triggered by Stage & Test trigger.
f) Interactive Application Security Testing shall be applied during the Continuous Build, Integration and Testing stage triggered by Stage & Test trigger.

Note: OEM shall submit an undertaking

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.11]

3.1.32 Continuous Delivery and Deployment Stage

Requirement:

The following requirements shall be met during Delivery and Deployment Stage

a) Image Scan must be applied during the Continuous Delivery and Deployment stage triggered by Publish to Artifact and Image Repository trigger.
b) Code Signing must be applied during the Continuous Delivery and Deployment stage triggered by Publish to Artifact and Image Repository trigger.
c) Artifact and Image Repository Scan shall be continuously applied during the Continuous Delivery and Deployment stage.
d) Component Vulnerability Scan must be applied during the Continuous Delivery and Deployment stage triggered by Instantiate Infrastructure trigger.

Note: OEM shall submit an undertaking

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.12]

3.1.33 Runtime Défense and Monitoring

Requirement:

The following requirements shall be met during runtime

a) Component Vulnerability Monitoring must be continuously applied during the Runtime Defense and Monitoring stage and remediation actions must be applied for high severity rated vulnerabilities.
b) Runtime Application Self Protection shall be continuously applied during the Runtime Defense and Monitoring stage.
c) Application testing and Fuzzing shall be continuously applied during the Runtime Defense and Monitoring stage.
d) Penetration Testing shall be continuously applied during the Runtime Defense and Monitoring stage.

Note: OEM shall submit an undertaking

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.13]

3.1.34 Software integrity protection and verification

Requirement:

a) The host system shall verify the provenance and integrity of all instances and versions of software components before installing them.

b) It shall refuse to install all software that fails verification against the policies held by the host system.

c) It shall verify the integrity of software components before execution.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 8.14]

3.1.35 Communications security

Requirement:

The host system shall use one or more of the following methods for communications security:

a) TLS (minimum version 1.2) and IPSec, employing cryptographic primitives prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”, with client and server authentication required.
b) The host system shall not employ anonymous TLS.

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 8.6]

3.1.36 Cryptographic primitives

Requirement:

The host system shall support the specified key length as per Table1 of the latest document, “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”

[Reference: ETSI GS NFV-SEC 012 V3.1.1 section 6.5]

3.1.37 Monitoring of resource usage at both VNF infrastructure (VNFI) and level of guest VNFs

Requirement:
Monitoring shall be put in place at both the infrastructure level and the level of guest VNFs. These two layers will require interfaces with the management & orchestration system to consume monitoring information, then act on it accordingly.

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.5.5]

3.1.38 Identity API Access Control

Requirement:
API access shall have some policy-based mechanism to maintain access control.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.8]

3.1.39 Time Synchronization

Requirement:
Given that token expiration is a component of Identity and Access Management, time synchronization among the servers is critical and hence shall be implemented.

Note: This clause requires IAM for testing. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.
[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.10]

3.1.40 Compute Isolation

Requirement:
The compute hosts in an availability zone can be further organized in terms of aggregates. The compute hosts in the same aggregate share a set of attributes (such as a tenant or a hardware capability) defined by administrators.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 11]

3.1.41 Assurance checks from Management and Operations domain

Requirement:
The Management and Operations domain which will have control over the service catalog holding the VNF Package, and shall make assurance checks on it.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 5.2.3.1.1]

3.1.42 Lifetime of entities

Requirement:
It is important that the lifetime of Management and Orchestration entities shall be long, relative to the lifetime of entities which they control, such as VNFs, and VNFCIs.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 5.3.2]

3.1.43 Provisioning/Deployment

Requirement:

(a) Regarding the provisioning of servers, switches, routers and networking, tools must be used to automate the provisioning eliminating human error.

(b) The deployment tool is a sensitive component storing critical information (deployment scripts, credentials, etc.).

The following rules must be applied:

i) The boot of the server or the VM hosting the deployment tool must be protected

ii) The integrity of the deployment images must be checked, before starting deployment

iii) The deployment must be done through dedicated network (e.g., VLAN)

iv) When the deployment is finished, the deployment tool must be turned-off, if the tool is only dedicated to deployment. Otherwise, any access to the deployment tool must be restricted.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture v1.0 Section: 6.3.6.1]

3.1.44 Confidentiality and Integrity of communications

Requirement:

a) It is essential to secure the infrastructure from external attacks. To counter this threat, API endpoints exposed to external networks shall be protected by either a rate-limiting proxy or web application firewall (WAF), and shall be placed behind a reverse HTTPS proxy.

b) It shall be ensured that integrity and confidentiality of all network communications (internal and external) by using Transport Layer Security (TLS) protocol Ver 1.2 or above.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture v 1.0]

3.1.45 Securing 3rd Party Hosting Environments

Requirement:

a) Sensitive information of virtualized NFs shall be confidentiality protected when using a 3rd party environment (e.g., NFVI).

b) Third party hosting environments that support virtualized 3GPP NFs shall meet 3GPP virtualization security requirements and to enable operators to meet legal/regulatory requirements.
c) The system shall be able to monitor the attestation of 3rd party hosting environments.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

[Reference: 1)3GPP 33.848-17.1.0 V.0.11.0 Section 5.21 2) ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.9 3) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T29]

3.1.46 Isolation of VM's/Containers (VM and Hypervisor Breakout)

Requirement:

a) The NFVI shall provide security isolation to minimize the impact of and detect hypervisor/VM breakout on a virtualized 3GPP NF.
b) The system shall prevent and detect attacks that breakout from an attacked VNF through the virtualization layer to any other VNF or any other location.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.22]

3.1.47 Front end access Security

Requirement:
Front-end network security at the application level will be the responsibility of the workload, however the platform must ensure the isolation and integrity of tenant connectivity to front-end networks.

[Reference: GSMA NG 126 Ver 3.0 Section 7.4.3]

3.1.48 Backend access Security

Requirement:
The integrity of resources management requests coming from a higher orchestration layer to the Cloud Infrastructure manage shall be validated and verified.

[Reference: GSMA NG 126 Ver 3.0 Section 7.4.2]

3.1.49 Secure hardware resource management

Requirement:

The VIM manages the hardware resource configuration and state information exchange. When the VIM is compromised to change the hardware resource configuration, an alert shall be triggered by the hardware. The administrator can check the alert and find the attack at latter.

Note: This clause is applicable to GVNP Type 3

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.7.7.2]

Part 2 Virtualization Security

(Applicable for both Hypervisor based VM with its VNF and CIS based Container with its CNF)

3.2.1 Application of hardening policies

Requirement:

The following shall be met

The hypervisor or CIS shall be hardened to allow only the minimum services and processes necessary to operate VMs or containers, and all other services shall be removed by default.

As a minimum, the following configuration changes must be made among others:

a) remove all unused features;

b) when a VM or container is deleted, the virtual disk shall be zeroed to prevent an attacker reconstructing the contents of the VM or container disk;

c) disable the ability to connect external devices to VMs or containers (e.g., CD, serial and parallel ports);

d) make sure a VM does not have the ability to run with the full OS privilege level and can only operate at guest level; this can be controlled using Intel VT-x and AMD-V extensions;

e) make sure each VM or container has a predefined set of restricted resources to ensure one VM or container cannot impact the resources and performance of another in the same hypervisor or CIS;

f) disable the ability of a VM to initiate ‘disk shrinking’;

g) enable persistent disk mode;

h) restrict the visibility of one VM or container to detect another VM or container existing on the same host;

i) use zoning and LUN masking to segregate SAN activity with each VM having unique authentication credentials;

   Note: This clause is applicable only when SAN is used

j) remove direct access to the O&M functionality of the hypervisor or CIS for management only through a secure connection from the VIM; however, this may not always be operationally feasible, so the hypervisor or CIS installation shall limit access to the hypervisor or CIS ‘root’ operating system to either:

i) a dedicated O&M interface supporting a secure protocol (e.g. TLS 1.2 or above) with only an IP address,

ii)ACL restriction on which domain can connect successfully;

k) only allow 'root' access from the local terminal (LMP);

l) where a hardware manufacturer provided monitoring tools that are implemented on the hypervisor or CIS or they utilize embedded support for industry standard protocols such as Common Information Model (CIM), these functions must be installed and operated on the hypervisor or CIS with limited privileges.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P12]

3.2.2 Strong password policy

Requirement:
A strong complex password as per clause 2.4 of CSR shall be configured for each hypervisor or CIS 'root' account and secured in a safe location with physical and procedural controls on its access and use.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P09]

3.2.3 Hypervisor/CIS protection

Hypervisor or CIS introspection can be used to scrutinize software running inside VMs or containers to find abnormal activities. Using introspection capabilities, the hypervisor's or CIS's functionalities are enhanced, enabling it, among other things, to monitor network traffic, access files in storage, and to execute read memory. Hypervisor or CIS introspection APIs are powerful tools to perform deep VM or container analysis and potentially increase VM or container security. However, they can also be used as an exploit that makes it possible to break and bypass the isolation between VMs or containers and the hypervisor or CIS.

The hypervisor or CIS must enforce network security policies. This includes, but is not limited to, ensuring that;

a) VMs or containers are isolated from each other,
b) VMs or containers are prevented from accessing each other's memory spaces,
c) keys used to encrypt memory are also under hypervisor or CIS control,
d) hypervisors or CISs are not allowed to write directly to memory,
e) hypervisors or CISs are not allowed to bypass normal memory access controls and security within the VM or container,
f) hypervisors or CISs are not allowed to change data within a VNF at run-time

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T07]

3.2.4 Isolation of VM's (VM and Hypervisor Breakout)

Requirement:

a) The NFVI shall provide security isolation to minimize the impact of and detect hypervisor/VM breakout on a virtualized 3GPP NF.

b) The system shall prevent and detect attacks that breakout from an attacked VNF through the virtualization layer to any other VNF or any other location.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.22]

3.2.5 Data synchronicity through network

Requirement:

In a virtualized environment, flexible and low cost (both in money and resource terms) security monitoring agents can be easily inserted around multiple VNFs across the network, which could allow an attacker to identify the different messages making up a single procedure.

a) The virtualized 3GPP NFs shall be protected from distributed monitoring attacks. The system shall dynamically assign VNF resources (e.g. memory address) to prevent long-term data leakage and exposure and protect network resources.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.25]

3.2.6 VNF Protection

Requirement:

a) Protection of VNFs

i. It shall be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts.

ii. Binding shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.

iii. The system shall manage (e.g. assign or log bindings) key storage and confidential data in a manner that provides protection against data compromise.

iv. Sensitive data shall only be decrypted or handled in an unencrypted format in VNFs on trusted and well-known hosts.

v. It must be possible to control whether untrusted or less trusted VNFs are allowed to run on the same host as VNFs in a higher trust domain.

vi. It must be possible to further restrict VNFs on a single host depending on whether they handle decrypted sensitive data.

vii. The system shall prevent and detect unauthorized or unintended data manipulation and leakage (e.g. modification of VNF images, instantiating parallel VM(s) or container(s) on the same physical CPU).

b) Securing internal VNF communication

Where a NFV is composed on multiple VNFs the vendor shall demonstrate how it protects the internal communication of its NFV, as it transits between VMs or containers.

c) Protection of stored data

i) It shall be ensured that any security critical (including LI), customer privacy or confidentiality related information is stored securely on any shared or local storage (e.g. SAN, SSD).

ii) Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” shall only be used for protecting this data.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T19]

3.2.7 VNF Image validation and protection

Requirement:

a) A VNF Package is composed of several components such as, for example, VNFD, software images, scripts, etc. During the on-boarding of the VNF package, a validation of the package shall be performed. The validation shall be a procedure that verifies the integrity of the VNF package. A package is certified by performing acceptance testing and full functional testing against the VNF including configuration, management, and service assurance.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

b) VNF images can be cryptographically signed and verified during launch time. This can be achieved by setting up some signing authority and modifying the hypervisor or CIS configuration to verify an image’s signature before they are launched.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

c) The software package and the artefacts within the package of a VNF shall have their integrity protected by the vendor’s (OEM’s) signature. The software package and the artefacts within the package of a VNF and the software catalogue holding its image shall have their integrity protected after onboarding. The software package and the artefacts within the

package of a VNF containing sensitive information must support the protection of confidentiality.
Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause..

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T2]

3.2.8 The IDAM (Identity and Access Management)

Requirement:
a) The mobile networks shall assign unique identities to all elements that will communicate to other elements in the mobile network.
Before allowing access to a resource, each network element shall authenticate and authorize the entity requesting access.
Where possible, identities shall be assigned using Public Key Infrastructure X.509 certificates from a trusted certificate authority (CA) rather than username/ password combinations.
b) If username/password is used, multi-factor authentication (MFA) shall be enabled to reduce the risk of compromise.
c) The mobile network shall provide automated mechanisms for credential management.
d) Where possible, use certificate pinning or public key pinning to provide additional identity assurance when authentication is dependent upon multiple CAs.
e) All access to resources shall be logged.
f) Analytics for detecting potentially malicious resource access attempts shall be deployed and run regularly.
g) Applications and workloads shall be explicitly authorized to communicate with each other using mutual authentication. Due to the ephemeral nature of cloud computing, key rotation and lifespan need to be frequent and short to maintain the demands of high-velocity capabilities and control and limit the blast radius in case of credential compromise.
h) For the client and server to bi-directionally verify identity via cryptography, all workloads must leverage mutual/two-way transport authentication.
i) Authentication and authorization must be determined independently (decision point) and enforced (enforcement point) within and across the environment.
j) Authorization for workloads are granted based on attributes and roles/permissions for which they have been assigned. It is strongly recommended organizations use both Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) to provide granular authorization enforcement in all environments and throughout their workload lifecycle. Such a posture can enable defense in- depth, where all workloads are able to accept, to consume, and to forward the identity of the end user for contextual or dynamic authorization. This can be achieved through the use of identity documents and tokens.

[Reference: 1) NSA-CISA Security Guidance for 5G Cloud Infrastructures Part I: Prevent and Detect Lateral Movement (2021) 2) CNCF Cloud Native Security Whitepaper Ver 2.0]

3.2.9 The Mobile Cloud Software shall be kept up-to-date and free from known vulnerabilities

Requirement:

a) Software repositories for known vulnerabilities and out-of-date versions shall be regularly scanned using one or more software scanning tools or services.

b) Third-party applications and libraries that are integrated into the network-slicing infrastructure shall be regularly monitored for publicly reported vulnerabilities.

c) The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide a remediation plan.

Sl No	CVSS Score	Severity	Remediation
1	9.0-10.0	Critical	To be patched immediately
2	7.0-8.9	High	To be patched within a month
3	4.0-6.9	Medium	To be patched within three months
4	0.1-3.9	Low	To be patched within a year

d) Zero-day vulnerabilities shall be remediated immediately or as soon as practically possible.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part I: Prevent and Detect Lateral Movement (2021) Reference 2 : GSMA NG 133 Cloud Infrastructure Reference Architecture]

3.2.10 Availability

Requirement:

It shall be possible to replicate virtual machine/ containers into various zones and clusters to achieve high availability.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 9]

3.2.11 Token Generation

Requirement:

The parameters relevant to the token, i.e., lifespan and key length shall be configurable during the token generation.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.2.2]

3.2.12 Token Verification

Requirement:
Validation of the received token shall be carried out before the provision of the requested service.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.2.3]

3.2.13 Token Transport

Requirement:
Token in transit to the authentication manager need to be protected.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 5.6]

3.2.14 The software package must be checked for integrity during installation

Requirement:
Each individual artifact in a VNF Package shall have a cryptographic signature when it is stored in the NFV-MANO catalogue(s):

i) The VNF provider's signature on individual artifacts in a VNF Package shall be stored by NFV-MANO.

[Reference: ETSI NFV-SEC021v2.6.1 VNF - GS, Section 5.1]

3.2.15 Key Management and security within migrated images

Requirement:
When images are migrated, regardless of the vehicle for accomplishing the migration, they shall possess the same MAC addresses, CPU ID, and other hardware signatures that they possessed prior to the migration.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 4.4.3.3.2]

3.2.16 Logging

Requirement:
The logging module shall provide standard features, such as a common set of logging levels for classifying the logged events, log file rotation, and runtime logging configuration.

[Reference: ETSI GS NFV-SEC 002 V1.1.1 Section 10.1]

3.2.17 Event Notification

Requirement:

Generation of event notifications shall be provided as it can serve as a basis for purposes such as accounting, security monitoring, troubleshooting, and auditing.

[Reference: 1) ETSI GS NFV-SEC 002 V1.1.1 Section 10.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T17]

3.2.18 Encrypted Storage

Requirement:

i)Persistent volume shall be encrypted as per Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)"

ii) The encryption of ephemeral volume is optional.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 7.1]

3.2.19 Policies for workload placement in Retained data

Requirement:

Retained Data collection, storage and query shall only take place within the country.

An undertaking in this regard shall be submitted.

[Reference: ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.5]

3.2.20 Platform backup

Requirement:

The storage for backup must be independent of storage offered to tenants.

[Reference: GSMA NG.133 Cloud Infrastructure Reference Architecture managed by OpenStack v 1.0 Section: 6.3.6.3]

3.2.21 Validating the Topology of Virtualized Network Functions

Requirement:

a) The topology of the Virtualized Network functions needs to be validated to ensure that the connectivity of the whole network, including all its virtualized functions meets its security policy.

b) It also needs to be verified that any unauthorized connectivity shall not be present and that it cannot be added by any unauthorized party.

[Reference– ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.1.2]

3.2.22 Ensure disconnectedness between many parts of an infrastructure network

Requirement:
Without any Virtualized forwarding Functions running, there must not be any connectivity between each partitioned network (core or customer networks).

[Reference– ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.1.1]

3.2.23 Security Groups

Requirement:
Security groups mechanism shall be present that tenants can use to control network traffic from and to virtual machines or network interfaces. A security group is defined by a set of rules. A rule consists of specific conditions (mainly pertaining to the type, source, and destination of traffic) and the action (e.g., drop, reject, or accept) to be taken if the conditions are satisfied.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.1]

3.2.24 Anti-Spoofing

Requirement:
Support to anti-spoofing of MAC addresses, IP addresses, ARP messages, and DHCP messages shall be present.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.2]

3.2.25 Network Address Translation

Requirement:
Support for the private IP address to communicate with a host on the public network shall be provided.

[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.3]

3.2.26 Network Isolation

Requirement:
Traffic separation of various tenants shall be ensured.
[Reference– ETSI GS NFV-SEC 002 V1.1.1 Section 8.4]

3.2.27 OS-level access control

Requirement:

OS-level access controls need to be implemented to provide mechanisms for supporting access control security policies on Operating System processes.

[Reference: ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Section 6.3]

3.2.28 The networking within the Mobile cloud shall be securely configured

Requirement:
Service Meshes shall be used to protect node-to-node traffic.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part I: Prevent and Detect Lateral Movement (2021)]

3.2.29 Lock down communications among isolated network functions

Requirement:
Mobile networks shall ensure that all communication sessions on an NF's control plane, user plane, management plane, and through the cloud infrastructure are authenticated using the identities provisioned from the Identity and Authorization session. For example, these sessions could use mutually-authenticated TLS v1.2+ where the X.509 certificates are the identities that are authenticated.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part I: Prevent and Detect Lateral Movement (2021)]

3.2.30 VNF Deployment

Requirement:
Minimum baseline security controls and hardening measures shall be configured for new VNF deployments. This can be done in many ways such as using pre-hardened golden images, deployment time configuration, etc. Such controls include fully implemented access control rules and ensuring that any unused ports, features, insecure protocols, or services are disabled

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T04]

3.2.31 Software compliance and integrity preservation

Requirement:

a) A software checksum (hash or signature) shall be created by the vendor/OEM during NFV and a supporting NFVI (e.g., host OS, hypervisor or CIS, SDN Controllers) software compilation that can be validated with a corresponding checksum created during any testing and validation process operated by the operator or a third party.
b) TEE is an important enabler for that goal. Tamper-proofing techniques shall be enabled for the preservation of software integrity by causing an altered software to fail.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

c) The concept of trusted execution and the associated technologies (e.g. Intel SGX enclave) shall be provided that make certain that even a malicious host OS or operator cannot tamper or inspect any managed payload memory space.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

[Reference: ENISA NFV Security in 5G – Challenges and Best Practices (February 2022) BP-T10]

Other Security Requirements

3.2.32 Security By Design

Requirement:

a) The security-by-design concept shall be used to address the protection of NFV resources and components at design time through the integration of security mechanisms. This shall concern the hardware layer, the virtualization layer, MANO and VNFs.

b) Secure software development lifecycle (SDLC) principles shall be used to avoid vulnerabilities and thus contribute to developing NFV software applications and services in a secure manner.

c) The use of Dev Sec Ops methodology shall be promoted. The Dev SecOps process aims at merging the security discipline within DevOps, thus considering security in every stage of the development process. By having security and development teams working together early in the development lifecycle, security naturally finds itself in the product by design.

Note: OEM shall submit an undertaking

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P14]

3.2.33 Open-Source Software

Requirement:

a) Open-source code must be inspected by tools with various capabilities for static and dynamic code analysis

b) The CVE (Common Vulnerabilities and Exposures) must be used to identify vulnerabilities and their severity rating for open-source code part of Cloud Infrastructure and workloads software.

c) Critical and high severity rated vulnerabilities must be fixed in a timely manner as defined in Ch 2.9.2

d) A dedicated internal isolated repository separated from the production environment must be used to store vetted open-source content.

[Reference: GSM Association NG 126 Cloud Infrastructure Reference Model Version 3.0 Section 7.10.8]
Note: OEM shall submit an undertaking

3.2.34 Secure update management

Requirement:
The process must consider the ability to update the cryptographic algorithms and to adapt to upcoming 4G/5G security challenges. Updates must be applied in a timely manner to protect against hardware or software bugs and security flaws, including those which are newly found.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P06]

3.2.35 Restrictions on installing applications

Requirement:
It shall not be possible to install a VNF application into the operational NFV environment without validation and approval by the operator.

Note: This can be a manual control process but it is expected that additional technical security controls will be adopted that allow only signed code to be installed in the NFV infrastructure
[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-P07]

Common Security Requirements related to 3GPP (4G/5G) Network Functions:

3.2.36 Establishment of trust domains for Network Functions
Requirement:

The trust domains of 3GPP network functions shall be identified. Security policies shall be applied depending on those trust domains. The system shall manage each trust domain separately. The system shall manage (e.g., define, enforce) the security policies for each trust domain independently.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.2]

3.2.37 Confidentiality of sensitive data

Requirement:
The sensitive information of a virtualized 3GPP NF is not exposed through the virtualization layer. The system shall manage (e.g., define, enforce) the permission control at the virtualization layer between NFs and/or sub-NFs.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.3]

3.2.38 Availability of Network Functions

Requirement:

a) Virtualized 3GPP NFs, particularly those which are critical to the operation and security of the network, will have access to the required resources for their availability or functionality when sharing resources with other VNFs.

b) The system shall manage the utilization, traffic distribution, and overload control of the NFs and sub-NFs to ensure availability for key network processes.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.4]

3.2.39 Common Software Environment

Requirement:

a) The software vulnerability in one virtualized 3GPP NF does not affect other virtualized 3GPP NFs using the same software platform.

b) Network interfaces shall be locked down so that they only accept a restricted number of expected protocols.

c) Network management shall be secured and shall only be allowed from authorized devices and/or networks.

d) Multi-factor authentication shall be used to log into administrator accounts.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.5]

3.2.40 Data Location and Lifecycle

Requirement:

a) The privacy sensitive information of a virtualized 3GPP NF is protected from being leaked out of the country.

b) The sensitive information of a virtualized 3GPP NF is protected during its lifecycle process to avoid leakage of the information to other VNFs reusing the storage resource.

c) All privacy sensitive data shall be encrypted when at rest and when in transit. Security policy which restricts where certain types of data can reside shall be defined and implemented by TSPs.

d) When VNF moves from one host to another or when VNF is terminated, the system shall ensure that resources, privacy sensitive data, and/or keys are fully cleared.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.6]

3.2.41 Function Isolation

Requirement:

a) The virtualization platform prevents one function from inspecting the memory of other functions.

b) Delegated administrator roles shall be used, with roles which could give a user or administrator the ability to inspect the memory of functions only used in exceptional circumstances

c) The system shall manage reference point-based security and service-based security between VNF functional "boxes".

d) Confidentiality protection shall be provided to protect information traveling between memory locations in a single or multiple logical memory block.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.7]

3.2.42 Keys and Confidential Data

Requirement:

a) It shall be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts.

b) Binding shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.

c) The system shall manage (e.g., assign/log bindings) key storage and confidential data in a manner that provides protection against data compromise.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.12]

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.2.43 Attestation at 3GPP Function level

Requirement:

a) It shall be possible to attest a virtualized 3GPP NF through the full attestation chain from the hardware layer through the virtualization layer to the VNF layer.

b) Attestation of a platform's integrity shall be linked to the application layer and possible for other functions to query. If platform attestation fails the virtualized 3GPP NF shall not be allowed to run.

c) Attestation of the VNF shall be performed prior to deployment/network integration and during operations.

d) Attestation of the VNF shall be done at the hardware, virtualization, and NF layers. The system shall manage VNF attestation.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.14]

3.2.44 IP layer vs Application layer Security

Requirement:

a) The security mechanisms in upper layers higher than the common virtualization platform layer (e.g. hypervisor) can provide virtualized 3GPP NFs the same protection as in physical NFs.

b) The system shall be able to communicate security policies to the hypervisor(s) to protect NF resource selection.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.24]

3.2.45 Secure Management APIs

Requirement:

a) The system shall be able to support a single 3GPP-defined security level, for all APIs (including the 3GPP layer, NFV layer, and NFVI layer) within a 3GPP network.

b) The system shall be able to support 3GPP-defined API access restrictions for specific NFs, NF components, and network slices.

[Reference 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.29]

3.2.46 Secure executive environment creation

Requirement: When an attacker tampers a driver which provided by the hardware and used to create the executive environment, the virtualization layer shall alert the driver error to the administrator for checking the error and finding the attack at latter.
Note: This clause is applicable to GVNP Type 2/3;

[Reference: 3GPP TS 33.818 v17.1.0 Section 5.2.5.6.7.3]

3.2.47 VM escape protection

Requirement:

a) To defend against the attack that an attacker utilizes a vulnerability of a VNF to attack a virtualization layer and then control the virtualization layer, the virtualization layer shall implement the following requirements:
i) The virtualization shall reject the abnormal access from the VNF (e.g. the VNF accesses the memory which is not allocated to the VNF) and log the attacks.

Note: This clause is applicable to GVNP Type 2/3

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.6.7.4]

3.2.48 Secure hardware resource management information

Requirement:
When a compromised Virtualization layer tampers the hardware resource configuration which is received from the VIM to result in the configuration error of the hardware, the hardware shall trigger an alert. The administrator can check the alert and find the attack at latter.
Note: This clause is applicable to GVNP Type 3
[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.7.7.3]

3.2.49 Unnecessary Hypervisor services

Requirement:
Unused services must be identified and disabled. Disable all hypervisor services such as clipboard- or file-sharing between the guest OS and the host OS unless they are needed. Disconnect unused virtual hardware in each guest OS.

[Reference: ENISA Security Aspects of Virtualization (Feb 2017) HY-05, OS-06]

3.2.50 Hypervisor boot configuration choice

Requirement:
The hypervisor shall have a boot configuration choice to disallow the use of non-certified drivers.
[Reference: ENISA Security Aspects of Virtualization (Feb 2017), HY-14, Pg-63]

3.2.51 Management of hypervisor platform

Requirement:

a) VM configuration management tools shall have the capability to compile logs and alert administrators when configuration changes are detected in any VM that is being monitored.
b) The access control solution for VM administration shall have a granular capability, both at the permission assignment level and the object level (i.e., the specification of the target of the permission can be a single VM or any logical grouping of VMs based

on function or location). In addition, the ability to deny permission to some specific objects within a VM group (e.g., VMs running workloads of a particular sensitivity level) in spite of having access permission to the VM group shall exist

[Reference: NIST SP 800-125A REV. 1 Security Recommendations for Server-based Hypervisor Platforms]

3.2.52 Hypervisor Security

Requirement:

The following must be met

a) Synchronize the virtualized infrastructure to a trusted authoritative time server.
b) Disable all hypervisor services such as clipboard- or file-sharing between the guest OS and the host OS unless they are needed. Each of these services can provide a possible attack vector. File sharing can also be an attack vector on systems where more than one guest OS share the same folder with the host OS.

[Reference: NIST Special Publication 800-125 Guide to security for full virtualization technologies]

Part 2 (A)Virtual Machine

This part presents the Virtual Machine specific security requirements.

3.2A.1 Traffic separation

Requirement:
The virtualized network product shall support logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.8.5.1]

3.2A.2 Secure crash measures for VMs running on hypervisors

Requirement:
The following clauses must be satisfied:

a) Hypervisors need to ensure that in the event of the crash of a VNF component instance, all file references, hardware pass-through devices, and memory are safe from access by unauthorized entities.

b) If the application running within the VM crashes, but not the VM itself, the hypervisor needs to ensure that no changes to the existing authorizations are made.

NOTE: The hypervisor might be unaware that the application within the VM has crashed.

c) In the event of a crash, arrangements need to be made for the relevant NFV instance to wipe the remote storage (e.g. the VNF Manager might instruct the Virtualization Infrastructure Manager to request this).

d) If the VNF component instance is using swap storage, it needs to be marked as such and the hypervisor ought to wipe it in the event of a crash.

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.4]

3.2A.3 Memory Introspection

Requirement:
a) An NFV environment shall use a virtualization platform which prevents one function from inspecting memory of other functions.

b) Delegated administrator roles shall be used to ensure that administrators do not have the ability to inspect memory of functions except under exceptional circumstances such as for network forensics.

c) The system shall manage the hypervisor to enforce network security policies. This includes, but is not limited to, ensuring that: -

i. VMs are isolated from each other
ii. Applications shall be prevented from accessing each other's memory spaces,
iii. VMs shall be prevented from accessing the memory of another VM,
iv. Keys used to encrypt the memory shall be kept under hypervisor control,
v. Hypervisors shall not be allowed to write directly to memory,
vi. Hypervisors shall not be allowed to bypass normal memory access controls and security within the VNF/VM,
vii. Hypervisors shall not be allowed to change data within a 3GPP VNF at run-time.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.8]

3.2A.4 Direct Execution of commands from Guest VMs

Requirement:

a) Gold standard must be defined for VMs of all types, and VM Images that do not conform to the standard shall not be allowed to be stored in the VM Image server or library. Images in the VM Image library shall be periodically scanned for outdated OS versions and patches, which could result in a drift from the standard.
b) Every VM Image stored in the image server shall have a digital signature attached to it as a mark of authenticity and integrity, signed using trustworthy, robust cryptographic keys.
c) Permissions for checking into and out of images from the VM Image library shall be enforced through a robust access control mechanism and limited to an authorized set of administrators. In the absence of an access control mechanism, VM image files shall be stored in encrypted devices that can only be opened or closed by a limited set of authorized administrators with passphrases of sufficient complexity.
d) Access to the server storing VM images shall always be through a secure protocol such as Transport Layer Security (TLS).

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

[Reference: NIST SP 800-125A REV. 1 Security Recommendations for Server-based Hypervisor Platforms]

3.2A.5 VM Lifecycle Management

Requirement:
During VM live migration, a secure authentication protocol must be employed; the credentials of the administrator performing the migration are passed only to the destination host; the migration of memory content and processor state takes place over a secure network connection; and a dedicated virtual network segment is used in both source and destination hosts for carrying this traffic.

[Reference: NIST SP 800-125A REV. 1 Security Recommendations for Server-based Hypervisor Platforms]

3.2A.6 Network Segmentation

Large overlay-based virtual networking deployments shall include either centralized or federated SDN controllers using standard protocols for configuration of overlay modules in various hypervisor platforms.

[Reference: NIST Special Publication 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection]

Part 2 (B) Container

This part presents the container specific security requirements.

3.2B.1 Container breakout

Requirement:

a) The virtualization layer must provide capabilities to limit the impact on co-hosted containers caused by a rogue container escaping its isolation. One of the commonly practiced security controls is to enforce strict resource limits on container usage, which helps in preventing resource starvation due to an attack by a rogue container.

b) The virtualization layer must enforce the principle of 'least privilege' which ensures that no containers run with a privilege higher than what is actually required.

[Reference: 1) 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.27 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022) BP-T31]

3.2B.2 Container Platform Integrity

Requirement:
The following shall be implemented to ensure the integrity of the container platform

a) The Kubernetes cluster shall be hardened against known attacks through suitable configurations. The Container Platform's Kubernetes cluster shall be hardened by following security guidelines and by running appropriate tools.
b) Opening up direct access to worker nodes shall not be resorted.
c) Worker node subnets shall be on private subnets (no access to the Internet) unless explicitly required (e.g., web server).
d) Container platform information and verified firmware and configuration measurements that are retained within an attestation service shall be used for policy enforcement. It shall also be possible to label worker nodes in the database with key value attributes

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

3.2B.3 Launch Time Integrity

Requirement:

Before launching a container, it must be verified that the underlying container platform is trusted. This verification includes ensuring that monitoring and other runtime controls and policies are active.

After assuring the integrity of the container platform, the integrity of each container must be verified before launch. The container shall be loaded from a trusted images source.

After launching the container, the container's execution shall be securely monitored according to the policies specific to the container and container platform. The stack shall be constantly monitored using analytics or other means that provide ongoing proof of the secure state of the stack as containers are launched and terminated.

Container encryption/decryption of images on Trusted Platforms: The ability to encrypt the workload images can provide at-rest cryptographic isolation to help protect consumer data and intellectual property. When the runtime node service receives the launch request, it can detect that the image is encrypted and make a request to retrieve the decryption key. This request can be passed through an attestation service to a key broker with proof that the platform has been attested. The key broker can then verify the attested platform report and release the key back to the Cloud Service Provider and node runtime services. At that time, the node runtime can decrypt the image and proceed with the normal workload execution. The disk encryption kernel subsystem can provide at-rest encryption for the workload on the platform.

a) It should be possible to run containers in TEEs to reduce the attack surface for containers.

Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

3.2B.4 Container Image Hygiene

Requirement:
The following best practices shall be implemented

(a) Multi-stage builds shall be used to create minimal images. Container images shall be devoid of build tools and other extraneous binaries.
(b) Container images shall be regularly scanned for any vulnerabilities
(c) Container shall not run as root.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part IV: Ensure Integrity of Cloud Infrastructure (2021)]

3.2B.5 Securely Isolate Network Resources (Pod Security)

Requirement:

a) Pods with containers configured to run as privileged shall be rejected using the technical controls and policies provided by the container orchestration platform.
b) Container shall not allow processes to run as root
c) Container orchestration platforms shall provide technical controls and policies to prevent privilege escalation.
d) Container orchestration platforms shall provide technical controls and policies to restrict directories used by host Path and ensure that those directories are read only.
e) Critical Containers shall be cryptographically isolated using TEEs

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.
[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources, 2021]

3.2B.6 Runtime security

Requirement:
Permitted syscalls shall be restricted to an allow-list to decrease the application's attack surface.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources,2021]

3.2B.7 Real-time threat detection and incident response

Requirement:
a) Attestation services shall be used to verify configuration policy and container metrics (e.g., hash of files, time to execute a module) at both boot and run times.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources,2021]

3.2B.8 Good container security hygiene

Requirement:
Pod Spec shall be used to set limits to help minimize resource contention and mitigate the risk arising from poorly written or compromised applications that consume an excessive number of resources. Also setting a resource quota or creating a limit range can force the use of limits on a namespace.

[Reference: NSA-CISA Security Guidance for 5G Cloud Infrastructures Part II: Securely Isolate Network Resources, 2021]

3.2B.9 Software Catalogue Image Exposure

Requirement:

a) The software package and the artefacts within the package of a virtualized NF and the software catalogue holding its image shall be integrity protected after its onboarding.
b) The software package and the artefacts within the package of a virtualized NF containing sensitive information shall support confidentiality protection.
c) Software package and artefacts within the package of a virtualized NF shall be bound to a specific network after onboarding, such that unauthorized software cannot be instantiated even if it has valid vendor certificate.

[Reference: 1) 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.18 2) ETSI NFV-SEC021v2.6.1 VNF - GS, Section 5.1]

3.2B.10 Container related

Requirement:
The following must be satisfied

a) Vulnerabilities within the runtime software: The container runtime must be carefully monitored for vulnerabilities, and when problems are detected, they must be remediated quickly.
Note: OEM shall enable feature/provide capability so that runtime vulnerability can be detected.
b) It should be possible to use a combination of existing network level devices and more app-aware network filtering tool which dynamically generate the rules to filter this traffic based on the specific characteristics of the apps running in the containers.”
Note: OEM shall support/ enable this.

c) Compliance with container runtime configuration standards shall be automated. It shall also be ensured that containers are run with the default profiles provided by their runtime and shall consider using additional profiles for high-risk apps

d) App vulnerabilities: Additional tools shall be implemented that are container aware and designed to operate at the scale and change rate typically seen with containers. These tools shall be able to automatically profile containerized apps using behavioral learning and build security profiles for them to minimize human interaction.

e) Rogue containers: Separate environments for development, test, production, and other scenarios, each with specific controls to provide role-based access control for container deployment and management activities shall be used. All container creation shall be associated with individual user identities and logged to provide a clear audit trail of activity

[Reference: NIST Special Publication 800-190 (September 2017)]

3.2B.11 Host OS related

Requirement:
Organizations shall use container-specific OS which is read only OS with other services disabled.

a) Shared kernel: Container workload shall be grouped onto host by its sensitivity level. Improper user access rights: All authentication to the OS shall have feature of audit, login anomalies shall be monitored, and any escalation to perform privileged operations shall be logged.

b) Host file system tampering: It must be ensured that containers are run with the minimal set of file system permissions required. In no case shall containers be able to mount sensitive directories on a host's file system, especially those containing configuration settings for the operating system.

c) Disparate data sensitive workloads shall not be allowed to be run on the same OS kernel.

[Reference: NIST Special Publication 800-190 (September 2017)]

3.2B.12 Resource Requests and Limits

Requirement:
It shall be possible to apply different object level resource requests and limits via c groups so as to prevent rogue workloads exhausting the node and cluster level resources.

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

3.2B.13 Audit Log Analysis

Requirement:

a) The log systems in cloud native architecture shall support

i) Granular audit configuration and filtering for workloads

ii) In addition, it shall be interoperable so that advanced filtering to prevent overloads in downstream processing is possible.

iii) It shall be possible to generate actionable audit events that correlate/contextualize data from logs into "information" that can drive decision trees/incident response.

b) It shall be possible to detect non-compliant violations based on a pre-configured set of rules that filter violations of the organization's policies. It shall also be possible to API auditing that filters for a specific set of API Groups or verbs.

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

3.2B.14 Control Plane Authentication and Certificate Root of Trust

Requirement:

a) The orchestrator administrators shall configure all orchestrator control plane components to communicate via mutual authentication and certificate validation with a periodically rotated certificate in addition to existing control plane hardening.

b) The Issuing Certificate Authority (CA) can be a default orchestrator CA or an external CA. Particular attention shall be given by the administrators to protect the CA's private key.

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

3.2B.15 Service Mesh implementation

Requirement:

To effectively ensure secure communications between services in cloud native environments, organizations shall implement a service mesh to eliminate implicit trust within and across workloads, achieved through data-in-motion encryption.

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

3.2B.16 Storage

Requirement:

Cloud Native Storage covers a broad set of technologies that are bucketed into presented storage and accessed storage. Presented storage is storage made available to workloads such as volumes and includes block stores, file systems and shared file systems. Access storage is storage that is accessed via an application API, and includes object stores, key value stores, and databases.

a) Storage systems contain a data access interface that defines how applications or workloads store or consume data that is persisted by the storage system or service. This interface *shall* be protected by access controls, authentication, authorization, and potentially encryption in transit.
b) Storage systems also contain a control plane / management interface which is typically an API and shall be protected by authentication and TLS. In general, the control interface is only accessed via a service account by an orchestrator or service broker

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

3.2B.17 Principle of Least Privilege

Requirement:
Mandatory Access Control (MAC) implementations (e.g. SELinux and App Armor) can limit the privileges beyond those set to the container or namespace.

Additionally, they provide container isolation at the host level to prevent container breakout or pivoting from one container to another, to escalate privileges beyond those permitted by the access control in place.

[Reference: CNCF Cloud Native Security Whitepaper Ver 2.0]

Part 2(C) VNF_CNF Related

(Wherever VNF or CNF is explicitly mentioned, those clauses are applicable for those VNF or CNF. Otherwise, the clauses are applicable for both VNF and CNF)

3.2C.1 VNF/CNF network security profile

Requirement:
a) Each VNF/CNF supporting VNFC functions shall have a predefined network security profile describing its requirements for vNICs, ports, port group, VLANs and the requirement for internal VXLAN connections.
b) The security profile shall also define the vNIC firewall rules related to protocols (port numbers) that need to be supported on each VLAN or VXLAN connection. There shall never be a requirement for all ports to be open, particularly on external standard-based interfaces (e.g. GTP).

Note: This clause requires support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.2C.2 Protection from buffer overflows

Requirement:

The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by OEM.

[Reference: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.5]

3.2C.3 Data at rest storage

Requirement:

All subscriber data removed from the data at rest and the storage shall be cleaned.

[Reference: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-at-rest]

Note: Cleaned here means overwrite storage by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

3.2C.4 VNF/CNF Startup

Requirement:

VNF/CNF startup shall include a secure boot process.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.19]

Note: This clause requires support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.2C.5 Trusted Time Source

Requirement:

The VNF/CNF shall synchronize with trusted time source.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.20]

Note: This clause requires support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

3.2C.6 VNF/CNF integration with authentication and authorization services

Requirement:

The VNF/CNF shall integrate with the operator's authentication and authorization services, e.g., IDAM (Identity Access Management). Limiting the number of repeated failed login attempts (configurable) reduces the risk of unauthorized access via password guessing (Bruce force attack). The restriction on the number of consecutive failed login attempts (“lockout_failure_attempts”) and any actions post such access attempts (such as locking the account where the “lockout duration” is left unspecified) shall abide by the operator’s policies.

[Reference: 1) ONAP - VNF API security requirements, October 2022 2) GSMA NG.133 Cloud Infrastructure Reference Architecture v 1.0 section: 6.3.2.2]

Note: This clause requires support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

3.2C.7 VNF/CNF Host Spanning

Requirement:

a) All control plane data in transit between hosts shall be sent over an encrypted and authenticated channel using the protocols as prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR).”.

b) User plane traffic between hosts should be protected.

c) The system shall prevent and detect unauthorized VNF/CNF host spanning.

[Reference: 3GPP TR 33.848-0.11.0 Section 5.15]

3.2C.8 Input validation

Requirement:

a) The VNF/CNF must implement the following input validation controls:
   i) Size (length) of all input shall be checked.
   ii) Large-size input that can cause the VNF/CNF to fail shall not be allowed. If the input is a file, the VNF /CNF API must enforce a size limit.
   iii) Input that contains content or characters inappropriate to the input expected by the design shall not be permitted. Inappropriate input, such as SQL expressions shall not be allowed.

[Reference: ONAP- VNF API security requirements, October 2022]

3.2C.9 Key Management and security within cloned images

Requirement:

Cloned images shall not possess cryptographic key pairs utilized by their original image. Propagation of two or more images with the same key pairs immediately cancels out the notion of utilizing key pairs for the purpose of establishing identity.

[Reference: ETSI GS NFV-SEC 003 V1.1.1 Section 4.4.3.3.1]

3.2C.10 Encrypting VNF/CNF volume/swap areas

Requirement:

a) The VNF/CNF volumes shall be secured by encrypting them and storing the cryptographic keys at safe locations. TPM or HSM modules can be used to securely store these keys.
   Note: This clause requires support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

b) VM or Container or container swap areas shall be encrypted.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP-T14]

3.2C.11 Encrypted Data Processing

Requirement:

a) Sensitive data shall only be decrypted or handled in an unencrypted format in VNFs/CNFs on trusted and well-known hosts.
   Note: This clause requires support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

b) It shall be possible to further restrict VNFs/CNFs on a single host depending on whether they handle decrypted sensitive data.

c) These controls shall be verified by secure hardware backed attestation of the health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.

d) The system shall prevent and detect unauthorized data manipulation and leakage (e.g., modification of VNF/CNF images, instantiating parallel VM(s) on same physical CPU).

[Reference: 3GPP TR 33.848-0.11.0 Section 5.16]

3.2C.12 GVNP Life Cycle Management Security

Requirement:

a) VNF shall authenticate VNFM when VNFM initiates a communication to VNF.

b) VNF shall be able to establish securely protected connection with the VNFM.

c) VNF shall check whether VNFM has been authorized when VNFM access VNF's API.

d) VNF shall log VNFM's management operations for auditing.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.1]

Note: This test case is optional when the VNF and VNFM belongs to the same VNF vendor. If the VNF and VNFM belongs to the same VNF vendor and the interface between VNF and VNFM is proprietary interface, the API level authorization is not needed

3.2C.13 Instantiating VNF from trusted VNF image

Requirement:
A VNF shall be initiated from one or more trusted images in a VNF package. The VNF image(s) shall be signed by an authorized party. The authorized party is trusted by the operators.

[Reference: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.3]

3.2C.14 Inter-VNF and intra-VNF Traffic Separation

Requirement:
The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated to prevent the security threats from the different networks affecting each other.

[Reference: 3GPP TS 33.818-17.1.0 Section 5.2.5.5.8.5.2]

3.2C.15 Security functional requirements on virtualization resource management

Requirement:

a) To prevent a compromised VIM from changing the assigned virtualized resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, and the VNF shall alert the OAM when the VNF cannot detect a VNFC message.
b) A VNF shall log the access from the VIM.

[Reference: 3GPP TS 33.818 v17.1.0 Section 5.2.5.6.7.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022)]

3.2C.16 VNF package and VNF image integrity

Requirement:

1) VNF package and the image shall contain integrity validation value (e.g. MAC).
2) VNF package shall be integrity protected during onboarding and its integrity shall be validated by the NFVO.

[Reference: 3GPP TS 33.818- 17.1.0 Section 5.2.5.5.3.3.5.1 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T2]

3.2C.17 Secure crash measures for VMs running on hypervisors

Requirement:

In the event of a crash, the hypervisor must wipe the local storage that is no longer required. (e.g. the VNF Manager might instruct the Virtualization Infrastructure Manager to request this).

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.4]

3.2C.18 Proper image management of VM images must be done

Requirement:

Images shall be carefully protected against unauthorized access, modification, and replacement by both systems and human actors.

a) Small number of images must be kept.
b) Images must be kept updated to avoid known vulnerability exploits.
c) Cryptographic checksum protection must be used to detect unauthorized changes to images and snapshots.
d) Strict control around access, creation and deployment of images/instances must be implemented. Such activities must be recorded for audit purposes.

[Reference: ENISA Security Aspects of Virtualization (Feb 2017) G-07, PG 37, OS-01, OS-02]

3.2C.19 Secrets in NF Container/VM Image

Requirement:

The VNF/CNF images shall not be packaged with embedded secrets such as passwords or credentials, or any other critical configuration data.

[Reference: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.28]

3.2C.20 Container image authorization

Requirement:

Public cloud service provider shall give an undertaking that geo-fencing has been enabled so that container images can only run on particular platforms.

[Reference: CNCF CLOUD NATIVE SECURITY WHITEPAPER Ver 2.0]

3.2C.21 Security Management and Orchestration

Requirement:
NFV orchestrator shall be designed incorporating the security and trust requirements of the NFVI. The orchestration and management of security functions requires integration by enabling interaction among the security orchestrator, the VNFM, and the element management systems (EMS). This type of protection can be achieved by setting scaling boundaries in the VNFD or network service descriptor (NSD), for example, and having the NFVO enforce these restrictions to protect from attacks such as a DNS amplification attack.

Secure management and administration of the NFVI and NFV-MANO is critical for the security of a virtualized network. The following describe the basic principle for such secure management which shall be met
a) Internal components within VNFs are not able to directly connect to entities or management functions outside of the network trust domain, except via interfaces that are explicitly part of the VNF security design.

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T8]

Part 3-SDN

This part presents the SDN specific security requirements.

3.3.1 Mutual authentication within SDN

Requirement:
There must be mutual authentication between the controller and the switching/routing entities in SDN.

[Reference: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.1.3.1.1]

3.3.2 Centralized Log Auditing

Requirement:
All the SDN elements shall submit security events (e.g. authentication, authorization and accounting, login attempts, administration functions and configurations etc) as defined in Log table in Ch 2.5.2 to a centralized platform, which shall monitor and analyses in real time the messages for possible attempts at intrusion.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T17]

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.3.3 Software compliance and integrity preservation

Requirement:
A software checksum (hash or signature) shall be created by the OEM/vendor during SDN Controller software compilation that can be validated with a corresponding checksum (hash or signature) created during any testing and validation process operated by the operator or a third party.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T10]

3.3.4 OS hardening

Requirement:
The OS of SDN elements shall be hardened to allow only the minimum services and processes necessary to operate and all other services shall be removed by default.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-P12]

3.3.5 Host Security

Requirement:
SDN elements shall be hosted on secure server.

3.3.6 SDN controller and associated SDN communications

Requirement:
An SDN controller shall always communicate with its associated SDN resources using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: ETSI GS NFV-EVE 005 Section 6.1, REC#1]

3.3.7 Prevent attacks via forwarding plane

Requirement:
There shall be mechanisms to prevent attacks mounted via the Forwarding Plane against SDN switches and controllers. OEMs shall submit the list of measures taken to prevent reconnaissance attacks, DoS and resource exhaustion attacks and vulnerability exploits.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#1]

3.3.8 Prevent attacks via control network

Requirement:

a) There shall be mechanisms to mitigate attacks from the control network. TLS shall be used to protect integrity.
b) There shall be High-Availability (HA) controller architecture.
c) The configuration of secure and authenticated administrator access to controllers shall be enabled.
d) Role-Based Access Control policies shall be implemented for controller administrators.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#2]

Note on c) and d): These clauses require support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.3.9 Prevent attacks via SDN controller's Application Control Interface

Requirement:

a) There shall be mechanisms to mitigate attacks via the SDN Controller's Application Control Interface such as

TLS 1.2 or higher shall be used to secure northbound communications and secure controller management.

b) The SDN systems shall be configured to validate flows in network device tables against controller policy.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#3]

3.3.10 Prevent attacks via virtualized environment

Requirement:

There shall be mechanisms to mitigate attacks against controllers and switches via the Virtualized environment. OEMs shall submit the list of measures taken to prevent such attacks.

[Reference: ETSI GS NFV-EVE 005 Section 6.2, REC#4]

3.3.11 Northbound Applications

Requirement:

a) Northbound applications, including the orchestrators, shall not be assigned admin level access to the controllers.
b) The identity of northbound applications shall be confirmed through certificates.

3.3.12 SDN security management

Requirement:

a) The controls below shall be applied if message bus technology for communication between SDN elements is used.
   i) A strong mechanism to authenticate the integrity of messages must be deployed between the 'publisher' and 'producer' over the message bus.
   ii) No messages shall be accepted or processed by the message broker or 'consumer' systems from unknown, 'fake' or unauthenticated users.
   iii) The communications shall be secured using TLS 1.2 and above security or certificates where supported (e.g. Kafka).
   iv) The message bus shall be monitored for any unauthenticated messages or 'fake' or default usernames and a security alarm raised for investigation.

b) The security functionality shall be deployed that identifies potential attacks on any SDN elements. Any security functionality shall provide automated alarms and the ability to change the network or element configuration to mitigate the attack.

c) A high availability architecture shall be implemented for key SDN components (e.g. SDN Controllers) to ensure operational service is maintained. The design shall include primary and secondary IP links with, where possible, diverse routing to allow for single point of network failure.

d) Any changes to network, service and virtual environments shall be restricted to the orchestrator. The SDN Controller and the VNFM/CNFM and VIM/CISM shall have additional controls applied to them to restrict such access for normal operation. Restricting the SDN Controller and the VNFM/CNFM and VIM/CISM will prevent the application of rules and changes that may break policy and rules during deployment of service templates.

e) The orchestration layer and SDN must be architected so that SDN networks and NFV environments are not operationally dependent on the orchestration or MANO layer to maintain operating services under circumstances that may render the orchestration platform unavailable.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T22]

Part 4 MANO

This part presents the MANO specific security requirements.

3.4.1 Instantiation of MANO components

Requirement:

The MANO system shall allow instantiation of MANO components and managed entities, the NFVIs, only at explicit geographic locations. It may be enforced through attribute-based access control and attribute based or multi-factor authentication (where location is one of the behavioral factors).

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.2 Identity verification shall be done at the Receiver end in MANO Architecture

Requirement:

Relying parties shall not allow any actions from received data before successfully identifying and verifying the location of the relied upon party. The possible countermeasure is to deploy the multi-attribute authentication and authorization schemes.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.3 Monitoring in VIM

Requirement:

Stored VM images shall be monitored to determine if any unauthorized modification, deletion or insertion has occurred. The requirement calls for proof of integrity of the data stores used for VM images and when combined with the data transfer integrity services.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.4 Message handling in MANO

Requirement:

The transmitter of a message shall provide means that will allow for the determination of any modification, deletion, insertion, or replay has occurred. The transmitting party shall enable a complete message and session integrity service.

[Reference– ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.5 Data Transfer in MANO

Requirement:

Data transferred over any internal interface of MANO shall be protected using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference– ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.6 Identity verification in MANO

Requirement:

The receiving party shall not allow any actions from received data before successfully identifying and verifying the identity and location of the transmitting party. This requirement shall eliminate most elements of masquerade and when placed alongside access control schemes shall also eliminate most forms of privilege escalation.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.7 The client and authorization servers shall mutually authenticate

Requirement:
NFV-MANO APIs shall only allow themselves to be accessed by authorized users. One solution for authorizing access is the use of OAuth2.0 with access token. The client shall authenticate the resource server and vice versa. Mutual authentication is done by the transport layer protection and is required.

[Reference: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T23, BP-P1]

3.4.8 Authentication of the Request Originator

Requirement:
Before accepting the token as valid, the resource server shall authenticate the originator of the request as the legitimate owner of the token. The token is bound to the subject through the subject Identifier, which ensures that the token has been provided for this consumer.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.9 Requirements for client credentials

Requirement:

a) The client credentials shall be stored in a secure and tamper-resistant location or stored encrypted with the key protected in a tamper-resistant location.
b) The client credentials shall not be included in the source code and software packages.
c) The client credentials shall be installed in the client in a secure way, eliminating any possibility of gaining access to these credentials during installation.
d) The client credentials shall be possible for the authorization server to revoke the client credentials.

[Reference: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T23]

3.4.10 Access Token shall be signed

Requirement:

The access token shall be signed to detect manipulation of the token or production of fake tokens. Access tokens shall be secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS). It shall be possible to encrypt the content of the access token.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.11 Format of Access Token

Requirement:
The access token shall be defined in a standard format (SAML or JWT).

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.12 Access tokens shall have limited lifetimes

Requirement:
The access token shall include a claim for the expiration time (expiration).

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.13 Access tokens shall be restricted to a particular number of operations

Requirement:
There shall be a restriction on the number of operations that an access token can perform in order to mitigate the replay attack by a malicious client.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.14 Access token shall be bound to the intended resource server.

Requirement:
The access token shall include a claim for the NF Instance Id of the Service Producer (audience). By using token binding, a client can enforce the use of a specified external authentication mechanism with the token.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.15 Tokens shall be bound to the client ID

Requirement:
The access token shall include a claim for the NF Instance Id of the Service Consumer (subject) which is the "Client ID."

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.16 Token Revocation

Requirement:
Token Revocation shall be possible. Unbound tokens shall not be used under any circumstance. The authorization server shall provide a mechanism for token revocation. If not, the lifetime of the Access token shall be kept very short, or the access token shall be single use. If a scheme to bind access tokens to the underlying transport layer relies on non-standard extensions, and those extensions are not available, the system shall fail securely, preventing a bid-down attack.

[Reference: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.4.17 Orchestrator node trust

Requirement:

a) Orchestration platforms shall be configured to provide features that create a secure environment for all the apps they run.

b) Orchestrators shall ensure that nodes are securely introduced to the cluster, have a persistent identity throughout their lifecycle, and can also provide an accurate inventory of nodes and their connectivity states.

c) A compromised node must be able to be isolated and removed from the cluster without disrupting or degrading overall cluster operations.

d) Orchestrators that provide mutually authenticated network connections between cluster members and end-to-end encryption of intra-cluster traffic shall be deployed.

[Reference: NIST Special Publication 800-190 [September 2017]

3.4.18 Logging in MANO

Requirement:
The receiver of a message shall be able to determine if any of modification, deletion, insertion, or replay has occurred. This requirement provides for a closed loop message and session integrity service.

[Reference: ETSI GS NFV-SEC 014 V3.1.1 Section 6]

3.4.19 MANO Access Control and Management

Requirement:

a) The MANO components shall support a high-level of role granularity to ensure appropriate levels of privilege can be assigned to all users to protect key processes and the integrity of data.

b) All OAM access shall be controlled through a centralized single sign-on or PAM solution with all access (success and failure) recorded in the audit log mechanism. Multi-factor authentication shall be used to log into administrator accounts.

c) All administration and management shall only be permitted from known, attested devices and multi-factor authentication shall be enforced.

d) The confidentiality and data integrity of all messages must be ensured, e.g. by using a transport-layer mechanism, such TLS 1.2 and above, on each interface.

e) The authorization server database used to authenticate the user and store associated user credentials, access tokens and refresh tokens must be stored in a tamper resistant location (e.g. HSM).

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T23]

Note: b) and e) The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.4.20 Security Management and Orchestration

Requirement:

a) Secure management and administration of the NFVI and NFV-MANO is critical for the security of a virtualized network. The following describe the basic principles for such secure management which shall be met

b) Administration of the NFVI is only available over mutually authenticated, encrypted and integrity protected channels or APIs.

c) All channels or APIs are separated from each other and use separate credentials.

d) NFV-MANO and NFVI administrators are only provided with the privileges and accesses required to carry out their role.

e) NFV-MANO and NFVI administrators do not have access to workloads running within the virtualized environment.

f) Functions that manage the administration and security of the NFVI (e.g., MANO) are physically separate and do not run on the same NFVI as the NFs they manage.

g) Ensure that there is physical/logical separation of the management network from other networks.

h) Management networks shall not pass through any virtualized Forwarding Functions.

[Reference: 1) ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T8]

3.4.21 Hardware Security

Requirement:

Separate dedicated hardware shall be used to provide independent NFV management (MANO) and service clusters (NFV). In addition, separated clusters shall be used to provide MANO and NFVI.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T16]

3.4.22 Centralized log auditing

Requirement:
All the MANO elements shall submit security events (e.g. authentication, authorization and accounting, login attempts, administration functions and configurations) to a centralized platform, which shall monitor and analyze in real time the messages for possible attempts at intrusion.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T17]

3.4.23 VIM connectivity to virtualization layer

Requirement:
a) The connectivity between the VIM and the virtualization layer shall support a secure access protocol (e.g. IPSec, TLS) to protect against the eavesdropping of password information. It is also required that the secure access shall support mutual authentication before allowing any O&M connectivity.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T24]

3.4.24 Recovery and reinstallation

Requirement:
Recovery mechanisms in NFV must ensure the following:
The NFVI must be restored completely, with all configurations and settings adjusted correctly. This includes controller nodes pointing to the right set of components, settings reloaded with correct parameters, and full inter-operability restored. Of particular importance is restoring the interoperation between NFV, SDN, and MANO systems, in an automated way, without the need for human intervention to reconfigure these systems to become functional again.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T25]

3.4.25 Deploying VM/Container of different trust levels

Requirement:
The VIM shall be configured to ensure that VMs or containers of differing trust levels are not deployed on the same physical host or blade and that VMs or containers requiring a

‘hardware root of trust’ cannot be installed on a physical host or blade that does not fully support trusted boot and TPM.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T26]

3.4.26 NFVO Security Management

Requirement:

(a) A mutual authentication mechanism shall exist between the NFVO, VIM and EMS platforms to provide a level of trust and to ensure only the authorized NFVO can make requests to the VIM and EMS platforms and vice versa.

(b) The NFVO shall provide internal workflow rules to prevent accidental changes to the NFVI and NFV services that could have an impact on service delivery.

(c) A mechanism shall exist to provide configuration roll-back in the event of any unauthorized or accidental service changes.

(d) The NFVO shall create and maintain a comprehensive audit log of all service changes including the identity of the user making each change.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T27]

3.4.27 VNF deletion or relocation

Requirement:

a) The NFVO shall only relocate or retire a VNF after backup and storage of critical data such as encryption keys or subscriber information to ensure this data is not lost during migration or restructuring of the network. This also applies when a request to relocate or retire a VNF comes from the EMS.

b) The NFVO shall only relocate or retire a VNF after having validated that the security and affinity policies can be and will be applied upon reintroduction of the element either in the same or a new location. This validation must take into account both operator and regulatory requirements.

c) The NFVO shall only relocate or retire a VNF after its operational state is no longer depended upon by other VNFs. In the event of a VNF being attacked or compromised it shall be possible to isolate the VNF from the production environment and restore the VNF to a state prior to the attack.

d) It shall also be possible to take a snapshot of the affected VNF to allow for security investigation and analysis.

[Reference: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T5]

Annexure-I

Definitions

1. Anti-Spoofing: Anti Spoofing is a technique for identifying and dropping packets that have a false source address
2. Application Programming Interface: This interface can be thought of as a contract of service between two applications
3. Atomic deployable unit: An instance of an atomic deployable unit is represented by a single VM for hypervisor-based virtualization or represented by one or a set of OS containers for CIS (Container Infrastructure Service) based virtualization.
4. Availability: The network availability is the average percentage of time during which the network is performing its intended function.
5. ABAC: Attribute-based access control (ABAC), also known as policy-based access control for IAM, defines an access control paradigm whereby a subject's authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment attributes.
6. Chain of trust: It is used to infer trust in the measurement data of the software component that represents the last link of the chain
7. Confidentiality: The state of keeping or being kept secret or private.
8. Confidential system internal data: that contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).
9. Firewall: A firewall is a network security device that monitors traffic to or from the network.
10. Generic virtualized network product model (GVNP) Type 1: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0
11. Generic virtualized network product model (GVNP)Type 2: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0
12. Generic virtualized network product model (GVNP)Type 3: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0
13. Host path: In Kubernetes, a host Path volume means mounting a file or a directory from the node's host inside the pod. A Kubernetes host path is one of the volumes supported by Kubernetes.
14. Host system: collection of hardware, software and firmware making up the system which executes workloads
15. Hypervisor: A software which acts as a bridge in between the Virtual Machines and the Host machine. It converts all the operations from the Virtual Machines so that they will be executable on the Host Machine CPU.

16. Least Trusted Domain (LTD): The Less Trusted Domain (LTD) contains resources that can be managed without the risk of compromising sensitive information, since these functionalities are offloaded to the MTD.
17. More Trusted Domain (MTD) contains resources (network, storage, processing) where sensitive functions can be offloaded.
18. Namespace: In Kubernetes, namespaces provide a mechanism for isolating groups of resources within a single cluster.
19. Network Functions Virtualization (NFV): principle of separating network functions from the hardware they run on by using virtual hardware abstraction
20. Network Functions Virtualization Infrastructure (NFVI): totality of all hardware and software components that build up the environment in which VNFs are deployed.
21. Network Functions Virtualization Infrastructure (NFVI) components: NFVI hardware resources that are not field replaceable, but are distinguishable as COTS components at manufacturing time.
22. Network Functions Virtualization Infrastructure Node (NFVI-Node): physical device[s] deployed and managed as a single entity, providing the NFVI Functions required to support the execution environment for VNFs.
23. Network Function Virtualization Infrastructure Point of Presence (NFVI-PoP): N-PoP where a Network Function is or could be deployed as Virtual Network Function (VNF)
24. Network Functions Virtualization Management and Orchestration (NFV-MANO): functions collectively provided by NFVO, VNFM, and VIM
25. Network Functions Virtualization Management and Orchestration Architectural Framework (NFV-MANO Architectural Framework): collection of all functional blocks (including those in NFV-MANO category as well as others that interwork with NFV-MANO), data repositories used by these functional blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFV.
26. Network Functions Virtualization Orchestrator (NFVO): functional block that manages the Network Service (NS) lifecycle and coordinates the management of NS lifecycle, VNF lifecycle (supported by the VNFM) and NFVI resources (supported by the VIM) to ensure an optimized allocation of the necessary resources and connectivity
27. Network Interface Controller (NIC): device in a compute node that provides a physical interface with the infrastructure network.
28. Network operator: operator of an electronics communications network or part thereof. An association or organization of such network operators also falls within this category.
29. Network Point of Presence (N-PoP): location where a Network Function is implemented as either a Physical Network Function (PNF) or a Virtual Network Function (VNF)

30. Network Service: composition of Network Function(s) and/or Network Service(s), defined by its functional and behavioral specification.
31. Network Service Orchestration: subset of NFV Orchestrator functions that are responsible for Network Service lifecycle management
32. Network Service Provider: type of Service Provider implementing the Network Service
33. Overlay Networks: A software-defined networking component included in most orchestrators that can be used to isolate communication between applications that share the same physical network
34. Personal data: “personal data” means any data about an individual who is identifiable by or in relation to such data;
35. Physical Network Function (PNF). Refers to the legacy network appliances on proprietary hardware.; implementation of a NF via a tightly coupled software and hardware system
36. Physical Network Function Descriptor (PNFD): template that describes the connectivity requirements of Connection Point(s) attached to a Physical Network Function.
37. Platform: A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.
38. Pods: Pods are the isolated environments used to execute 5G network functions in a 5G container centric or hybrid container/virtual network function design and deployment.
39. Pod Spec: PodSpec includes a set of fields that specify the user and/or group to run the application.
40. Post-incident analysis: post-incident analysis is the checking of various logged measurements to establish details of the attack, i.e. the mode and method of attack, the time of the attack, the identities or locations of attackers.
41. Relying Parties: An entity that relies upon the subscriber’s authenticator(s) and credentials or a verifier’s assertion of a claimant’s identity, typically to process a transaction or grant access to information or a system. An entity that relies upon the subscriber’s credentials, typically to process a transaction or grant access to information or a system
42. Sensitive Data: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
43. Syscall: The system call is the fundamental interface between an application and the Linux kernel.
44. TEE: A Trusted Execution Environment (TEE) is an area in memory protected by the processor in a computing device. Hardware ensures confidentiality and integrity of

code and data inside a TEE. The code that runs in the TEE is authorized, attested, and verified.

45. Virtual Machine (VM): virtualized computation environment that behaves very much like a physical computer/server; A virtual machine (VM) is an isolated computing environment created by abstracting resources from a physical machine
46. VM Image: A Virtual Machine Image is a fully configured Virtual Machine used to create a VM for deployment.
47. Virtual Network: virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity
48. Virtualized Network Function (VNF): implementation of an NF that can be deployed on a Network Function Virtualization Infrastructure (NFVI)
49. Virtualized Network Function Component (VNFC): internal component of a VNF providing a VNF Provider a defined subset of that VNF's functionality, with the main characteristic that a single instance of this component maps 1:1 against a single Virtualization Container
50. VNF Image: It is a fully configured Network Function which is used to deploy the network function in a virtualized environment.
51. Virtualized Network Function Instance (VNF Instance): run-time instantiation of the VNF software, resulting from completing the instantiation of its components and of the connectivity between them, using the VNF deployment and operational information captured in the VNFD, as well as additional run-time instance-specific information and constraints.
52. VNF Package: VNF Package is a ZIP file including VNFD, software images for VM, and other artifact resources such as scripts and config files
53. Worker nodes: Worker nodes within the Kubernetes cluster are used to run containerized applications and handle networking to ensure that traffic between applications across the cluster and from outside of the cluster can be properly facilitated.
54. Workload: component of the NFV architecture that is virtualized in the context of a particular deployment

Annexure-II

Acronyms

5GC	-	5G Core Network
5GMM	-	5GS Mobility Management
5GS	-	5G System
5GSM	-	5G Session Management
ACL	-	Access Control List
ARP	-	Address Resolution Protocol
AUSF	-	Authentication Server Function
AUTS	-	Authentication failure message with synchronization failure
CIoT	-	Cellular Internet of things
CIS	-	Center for Internet Security
CLI	-	Command Line Interface
CP	-	Control Plane
DAST	-	Dynamic Application Security Testing
DDoS	-	Distributed Denial of Service
DHCP	-	Dynamic Host Configuration Protocol
DL	-	Downlink
EM	-	Element Manager
EPS	-	Evolved Packet Core
EPS	-	Evolved Packet System
EMM	-	Evolved Mobility Management
gNB	-	5G Next Generation base station
GTP-C	-	GPRS Tunneling Protocol Control Plane
GTP-U	-	GPRS Tunneling Protocol User Plane
GUI	-	Graphical User Interface
GUTI	-	Global Unique Temporary Identifier
HBRT	-	Hardware Based Root of Trust
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
IaaC	-	Infrastructure as a Code
ICMP	-	Internet Control Message Protocol
IDE	-	Integrated Development Environment
IE	-	Information Element
IP	-	Internet Protocol
ISO-OSI	-	International organization of Standardization – Open System Interconnection
JSON	-	JavaScript Object Notation
MAC	-	Media access control

MANO	-	Management and Orchestration
NAS	-	Non-Access Stratum
N1A0	-	Null Security Algorithm
NF	-	Network Function
NFV	-	Network Function Virtualization
NFVI	-	Network Functions Virtualization Infrastructure
NFVO	-	Network Function Virtualization Orchestrator
NG	-	Next Generation
ng-eNB	-	Next Generation e-NodeB
NG-RAN	-	Next Generation Radio Access Network
O&M	-	Operations and Maintenance
OAM	-	Operations Administration Maintenance
OS	-	Operating System
OSS/BSS	-	Operation Support System/Business Support System
PDU	-	Protocol Data Unit
PKI	-	Public key infrastructure
PNF	-	Physical Network Function
RAM	-	Random Access Memory
RES	-	Response
RFC	-	Request for Comments
RRC	-	Radio Resource Control
S-NSSAI	-	Single - Network Slice Selection Assistance Information
SAML	-	Security Assertion Markup Language
SAST	-	Static Application Security Testing
SBI	-	Service Based Interfaces
SCA	-	Software Composition Analysis
SDN	-	Software defined networking
SEAF	-	Security Anchor Function
SMT	-	Simultaneous Multithreading
SUCI	-	Subscription Concealed Identifier
TEE	-	Trusted Execution Environment
UE	-	User Equipment
UL	-	Uplink
URL	-	Uniform Resource Locator
UUID	-	Universal Unique Identifier
VIM	-	Virtualized Infrastructure Manager
VM	-	Virtual Machine
VNF	-	Virtual Network Function
VNFD	-	Virtual Network Function Descriptor
VNFM	-	Virtual Network Function Manager

Annexure-III

List of Undertaking to be furnished by the OEM for NFV security Testing Submissions

1. Source code security assurances (against test case 3.3)
2. Know malware and backdoor check (against test case 3.4)
3. No unused software (against testcase 3.5)
4. No unsupported Components (against test case 4.2)
5. Avoidance of unspecified mode of access (against test-case 4.3)
6. Cryptographic module security assurance (against test case 6.2)
7. Cryptographic Algorithms implementation Security Assurance (against test 6.3)
8. Core hardware – HBRT (against test case 3.1.8)
9. Secure design and Architecture (against test case 3.1.31)
10. Secure code stage (against test case 3.1.32)
11. Continuous build, integration and against testing (against test case 3.1.33)
12. Continuous delivery and deployment stage (against test case-3.1.34)
13. Runtime defense and monitoring (against test case 3.1.35)
14. Security by design (against test case-3.2.32)
15. Open-source software. (against test case-3.2.33)
16. Container image authorization (against test case-3.2C.20)

Annexure-IV

References

1. 3GPP TS 33.818 V17.1.0 (2021-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products (Release 17).
2. 3GPP TR 33.848 V0.11.0 (2022-02) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects; Study on Security Impacts of Virtualization (Release 17).
3. ETSI GS NFV-SEC 001 V1.1.1 (2014-10) "Network Functions Virtualization (NFV); NFV Security; Problem Statement"
4. ETSI GS NFV-SEC 002 V1.1.1 (2015-08) "Network Functions Virtualization (NFV); NFV Security; Cataloguing security features in management software"
5. ETSI GS NFV 003 V1.3.1 (2018-01) Network Functions Virtualization (NFV); Terminology for Main Concepts in NFV.
6. ETSI GS NFV-SEC 006 V1.1.1 (2016-04) Network Functions Virtualization (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns.
7. ETSI GR NFV-SEC 009 V1.2.1 (2017-01) Network Functions Virtualization (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration.
8. ETSI GS NFV-SEC 010 V1.1.1 (2016-04) Network Functions Virtualization (NFV); NFV Security; Report on Retained Data problem statement and requirements.
9. ETSI GS NFV-SEC 012 V3.1.1 (2017-01) Network Functions Virtualization (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components.
10. ETSI GS NFV-SEC 013 V3.1.1 (2017-02) Network Functions Virtualization (NFV) Release 3; Security; Security Management and Monitoring specification
11. ETSI GS NFV-SEC 014 V3.1.1 (2018-04) Network Functions Virtualization (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points.
12. ETSI GR NFV-SEC 018 V1.1.1 (2019-11) Network Functions Virtualization (NFV); Security; Report on NFV Remote Attestation Architecture.
13. ETSI GS NFV-SEC 021 V2.6.1 (2019-06) Network Functions Virtualization (NFV) Release 2; Security; VNF Package Security Specification.
14. ETSI GS NFV-SEC 022 V2.8.1 (2020-06) Network Functions Virtualization (NFV) Release 2; Security; Access Token Specification for API Access.
15. ETSI GS NFV-EVE 005 V1.1.1 (2015-12) Report on SDN Usage in NFV Architectural Framework.

16. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES “Part I: Prevent and Detect Lateral Movement 2021”
17. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES “Part II: Securely Isolate Network Resources”
18. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021)
19. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES (2021) “Part IV: Ensure Integrity of Cloud Infrastructure”
20. NIST Special Publication 800-125B (March 2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection.
21. NIST Special Publication 800-125 Guide to Security for Full Virtualization Technologies.
22. NIST Special Publication 800-190 Application Container Security Guide.
23. ONAP VNF API Security Requirements
24. ENISA Security aspects of virtualization FEBRUARY 2017.
25. ENISA NFV SECURITY IN 5G Challenges and Best Practices FEBRUARY 2022.
26. GSMA NG 133 Cloud Infrastructure Reference Architecture managed by OpenStack v 1.0, Feb 2022.
27. GSMA NG 126 Cloud Infrastructure Reference Model Version 3.0
28. CNCF _Cloud-Native-Security-whitepaper-May2022-v2