|  |
| --- |
| 3GPP TR 33.818 V17.1.0 (2021-09) |
| Technical Report |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Security Assurance Methodology (SECAM);  and Security Assurance Specification (SCAS)  for 3GPP virtualised network products  (Release 17) |
|  |

|  |  |
| --- | --- |
| *5G-logo_175px* | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 10

3.3 Abbreviations 10

4 Overview 10

4.1 Introduction 10

4.1.1 Considerations on network product class when using NFV technology 10

4.1.2 Considerations on SECAM of the virtualised network products 12

4.2 Scope of a SECAM SCAS for 3GPP virtualised network products 12

4.2.1 Gap analysis 12

4.2.2 Scope of a SECAM SCAS 12

4.3 Scope of SECAM evaluation for 3GPP virtualised network products 13

4.3.1 Gap analysis 13

4.3.2 Scope of a SECAM evaluation 13

4.4 Scope of SECAM Accreditation for 3GPP virtualised network products 13

4.4.1 Gap analysis 13

4.4.2 Scope of SECAM Accreditation 14

4.5 Ultimate Output of SECAM Evaluation for 3GPP virtualised network products 14

4.5.1 Gap analysis 14

4.5.2 Ultimate Output of SECAM Evaluation 14

4.6 3GPP virtualised network products evaluation process 14

4.6.1 Gap analysis 14

4.6.2 Virtualised network product evaluation process 15

4.7 Roles in SECAM for 3GPP virtualised network products 15

4.7.1 Gap analysis 15

4.7.2 SECAM Roles Overview 15

4.7.3 Examples of instantiation of roles in SECAM 15

4.7.3.1 Introduction 15

4.7.3.2 Example: Complete self-evaluation 16

4.8 Operator security acceptance decision for 3GPP virtualised network products 16

4.8.1 Gap analysis 16

4.8.2 Operator security acceptance decision 16

4.9 SECAM Assurance level for 3GPP virtualised network products 17

4.9.1 Gap analysis 17

4.9.2 SECAM Assurance level 17

4.10 Security baseline for 3GPP virtualised network products 17

4.10.1 Gap analysis 17

4.10.2 Security baseline 17

5 Security Assurance Specification (SCAS) Creation 18

5.1 Writing process overview 18

5.2 SCAS documents structure and content 18

5.2.1 General 18

5.2.2 ToE 18

5.2.3 Generic virtualised network product model class description 18

5.2.3.1 Introduction 18

5.2.3.2 Generic virtualised network product model of type 1 19

5.2.3.2.1 Description of the GVNP model 19

5.2.3.2.2 Functions defined by 3GPP 19

5.2.3.2.3 Other functions 19

5.2.3.2.4 Operating system (OS) 19

5.2.3.2.5 Interfaces 19

5.2.3.3 Generic virtualised network product model of type 2 20

5.2.3.3.1 Description of the GVNP model 20

5.2.3.3.2 Functions defined by 3GPP 21

5.2.3.3.3 Other functions 21

5.2.3.3.4 Virtualisation layer 21

5.2.3.3.5 Interfaces 21

5.2.3.4 Generic virtualised network product model of type 3 21

5.2.3.4.1 Description of the GVNP model 21

5.2.3.4.2 Functions defined by 3GPP 22

5.2.3.4.3 Other functions 22

5.2.3.4.4 Virtualisation layer 22

5.2.3.4.5 Hardware 22

5.2.3.4.6 Interfaces 22

5.2.4 Security Problem Definition (SPD) for 3GPP virtualised network products class 22

5.2.4.1 Introduction 22

5.2.4.2 Generic assets and threats of GVNP for type 1 22

5.2.4.2.1 Generic assets of GVNP for type 1 22

5.2.4.2.2 Generic threats for GVNP of type 1 23

5.2.4.3 Generic assets and threats for GVNP of type 2 28

5.2.4.3.1 Generic assets for GVNP of type 2 28

5.2.4.3.2 Generic threats for GVNP of type 2 28

5.2.4.4 Generic assets and threats for GVNP of type 3 32

5.2.4.4.1 Generic assets for GVNP of type 3 32

5.2.4.4.2 Generic threats for GVNP of type 3 33

5.2.4.5 Generic assets and threats for network functions supporting SBA interfaces 36

5.2.5 Potential Security Requirements 36

5.2.5.1 Introduction 36

5.2.5.2 Incorporation of security requirements from existing 3GPP and ETSI specifications in current releases 37

5.2.5.3 Handling of security requirements 37

5.2.5.4 Guidelines for writing test cases 38

5.2.5.5 Potential security functional requirements and related test cases for GVNP of type 1 38

5.2.5.5.1 Introduction 38

5.2.5.5.2 Potential security functional requirements deriving from 3GPP specifications and related test cases 38

5.2.5.5.3 Technical baseline for potential general security functional requirements 38

5.2.5.5.4 Operating systems 40

5.2.5.5.5 Web servers 40

5.2.5.5.6 Network devices 40

5.2.5.5.7 Potential security functional requirements deriving from virtualisation and related test cases 41

5.2.5.5.8 Potential security requirements and related test cases to Hardening for GVNP of type 1 44

5.2.5.6 Potential security functional requirements and related test cases for GVNP of type 2 46

5.2.5.6.1 Introduction 46

5.2.5.6.2 Potential security functional requirements deriving from 3GPP specifications and related test cases 47

5.2.5.6.3 Technical baseline 47

5.2.5.6.4 Operating systems 47

5.2.5.6.5 Web servers 47

5.2.5.6.6 Virtualised Network devices 47

5.2.5.6.7 Potential security functional requirements deriving from virtualisation and related test cases 47

5.2.5.6.8 Potential Security requirements and related test cases to Hardening for GVNP of type 2 49

5.2.5.7 Potential security functional requirements and related test cases for GVNP of type 3 50

5.2.5.7.1 Introduction 50

5.2.5.7.2 Potential security functional requirements deriving from 3GPP specifications and related test cases 50

5.2.5.7.3 Technical baseline 51

5.2.5.7.4 Operating systems 51

5.2.5.7.5 Web servers 51

5.2.5.7.6 Network devices 51

5.2.5.7.7 Potential security functional requirements deriving from virtualisation and related test cases 51

5.2.5.7.8 Security requirements and related test cases to Hardening for GVNP of type 3 53

5.3 Improvement of SCAS and new potential security requirements 54

5.4 Basic vulnerability testing requirements for GVNP 54

5.4.1 Introduction 54

5.4.2 Port Scanning 54

5.4.3 Vulnerability Scanning 54

5.4.4 Robustness and Fuzz testing 54

6 Vendor development and product lifecycle processes and test laboratory accreditation 54

6.1 Overview 54

6.2 Audit and accreditation of Vendor network product development and network product lifecycle management processes 55

6.3 Audit and accreditation of test laboratories 55

6.4 Monitoring 55

6.5 Dispute resolution 55

7 Evaluation and SCAS instantiation 55

7.1 Security Assurance Specification (SCAS) instantiation documents creation 55

7.2 Evaluation and evaluation report 56

7.2.1 Network product development process and network product lifecycle management 56

7.2.2 SCAS instantiation evaluation 56

7.2.2.1 Overview 56

7.2.2.2 Content 56

7.2.2.3 Process 56

7.2.3 Security Compliance testing 56

7.2.4 Basic Vulnerability Testing 57

7.3 Self-declaration 57

7.4 Partial compliance and use of SECAM requirements in network product development cycle 57

7.5 Comparison between two SECAM evaluations 57

7.6 The evaluation of a new version 57

8 Conclusion 57

8.1 Way forward of SECAM/SCAS for 3GPP virtualised network products 57

Annex A: Change history 59

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the SECAM (Security Assurance Methodology) and SCAS (Security Assurance Specification) for 3GPP virtualised network products based on SECAM and SCAS defined in TR 33.916 [2]. It makes thorough gap analysis between current SECAM/SCAS work in TR 33.916 [2] and SECAM/SCAS work for 3GPP virtualised network products. It also identifies, defines ToE and roles of SECAM/SCAS for 3GPP virtualised network products according to deployment scenarios and decoupling ways. Based on the identified ToE and roles, the present document details the needed change or additional work to current security assurance methodology for the creation, evaluation procedure of related SCAS documents, etc. It studies new threats of the identified ToE and identifies the additional security requirements of the ToE, or/and identifies existing relevant/supporting requirements specified in ETSI NFV specifications or the equivalent. The present document also provides potential new SECAM/SCAS proposals and points out the impact to existing SECAM/SCAS documents (including TR 33.916 [2], TR 33.926 [3], TS 33.117 [4], etc.).

NOTE: SECAM/SCAS of 3GPP virtualised network products in the present document considers only the scenario that 3GPP VNF deployed in the virtual machines.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.916: "Security Assurance Methodology (SCAS) for 3GPP network products".

[3] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[4] 3GPP TR 33.117: "Catalogue of general security assurance requirements".

[5] 3GPP TS 28.500: "Management concept, architecture and requirements for mobile networks that include virtualised network functions".

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

[7] GSMA FS.16: "Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements".

[8] ETSI GR NFV-SEC 007: "Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

[9] 3GPP TR 33.848: "Study on security impacts of virtualisation".

[10] 3GPP TR 33.805: "Study on security assurance methodology for 3GPP network products (Release 12) ".

[11] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[12] ETSI GS NFV-EVE 001: "Network Functions Virtualisation (NFV); Virtualisation technologies; Hypervisor Domain Requirements Specification".

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

[14] ETSI GS NFV-IFA 019: "Network Functions Virtualisation (NFV); Acceleration Technologies; Acceleration Resource Management Interface Specification".

[15] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; VNF Descriptor and Packaging Specification".

[16] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[17] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[18] GSMA FS.14: "Network Equipment Security Assurance Scheme - Security Test Laboratory Accreditation".

[19] GSMA FS.15: "Network Equipment Security Assurance Scheme - Development and Lifecycle Assessment Methodology".

[20] GSMA FS.16: "Network Equipment Security Assurance Scheme - Development and Lifecycle Security Requirements".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**Network Functions Virtualisation Infrastructure (NFVI):** totality of all hardware and software components that build up the environment in which VNFs are deployed, as defined in ETSI GS NFV 003 [17].

**Network Functions Virtualisation 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, as defined in ETSI GS NFV 003 [17].

**Virtualised Infrastructure Manager (VIM):** functional block that is responsible for controlling and managing the NFVI compute, storage and network resources, usually within one operator's Infrastructure Domain (e.g. NFVI-PoP), as defined in ETSI GS NFV 003 [17].

**Virtual Machine (VM):** virtualised computation environment that behaves very much like a physical computer/server, as defined in ETSI GS NFV 003 [17].

**Virtualised Network Function (VNF):** implementation of an NF that can be deployed on a Network Function Virtualisation Infrastructure (NFVI), as defined in ETSI GS NFV 003 [17].

**Virtualised Network Function Component (VNFC):** internal component of a VNF providing a VNF Provider a defined sub-set of that VNF's functionality, with the main characteristic that a single instance of this component maps 1:1 against a single Virtualisation Container, as defined in ETSI GS NFV 003 [17].

**Virtualised Network Function Component Instance (VNFCI):** instance of a VNFC deployed in a specific Virtualisation Container instance. It has a lifecycle dependency with its parent VNF instance, as defined in ETSI GS NFV 003 [17].

**Virtualised Network Function Manager (VNFM):** functional block that is responsible for the lifecycle management of VNF, as defined in ETSI GS NFV 003 [17].

**VNF Package:** archive that includes a VNF descriptor, the software image(s) associated with the VNF, as well as additional artefacts, e.g. to check the integrity and to prove the validity of the archive, as defined in ETSI GS NFV 003 [17].

**virtualised network product class:** class of products that implement 3GPP defined network functionalities running on Network Function Virtualisation Infrastructure (NFVI).

**virtualised network product:** A virtualised network product is the instantiation of one or more virtualised network product class(es).

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

NFV Network Functions Virtualisation

NFVI Network Functions Virtualisation Infrastructure

NFVO Network Functions Virtualisation Orchestrator

VIM Virtualised Infrastructure Manager

VM Virtual Machine

VNF Virtualised Network Function

VNFC Virtualised Network Function Component

VNFCI Virtualised Network Function Component Instance

VNFM Virtualised Network Function Manager

# 4 Overview

## 4.1 Introduction

### 4.1.1 Considerations on network product class when using NFV technology

The definitions of network product class and network product were documented in the TR 33.916 [2]. For implementing 3GPP defined functionalities in network products, some functionalities that relate to the supporting platform (e.g. hardware components, operating system, etc.) also need to be implemented. The platform provides execution environment for 3GPP defined functionalities. For physical network products, the platform and the 3GPP defined functionalities are tightly coupled, while for virtualised network products, the platform and the 3GPP defined functionalities are decoupled. The platform of virtualised network products composes of a hardware layer and a Virtualisation layer, and is common for 3GPP defined functionalities. Concept of 3GPP VNF is defined in TS 28.500 [5]. According to the concept in [5], a 3GPP VNF is 3GPP network function(s) that runs on a Network Function Virtualisation Infrastructure (NFVI), which is the platform of virtualised network products described above.

The realistic deployment scenarios are summarized in ETSI NFV-SEC 001 [6], based on which a 3GPP network operator can deploy 3GPP defined functionalities in three modes:

- Mode 1. A network operator purchases 3GPP VNFs from its vendors and deploys it on a third party NFVI.

- Mode 2. A network operator purchases 3GPP VNFs and the Virtualisation layer (e.g. hypervisor) from its vendors, and deploys them on a third party hardware layer.

- Mode 3. A network operator purchases and deploys 3GPP VNFs, the Virtualisation layer and the hardware layer from its vendors.

NOTE: In order to implement virtualised product, some essential components besides 3GPP defined functions are also needed. Detailed description could be found in clause 5.

Each deployment mode requires the different composition of virtualised network products purchased and deployed by a network operator, which are subject to the testing and evaluation in SECAM scheme. Accordingly, the different composition of virtualised network products maps to three types of virtualised network product class as depicted in Figure 1:

- Type 1: implement 3GPP defined functionalities only

- Type 2: implement 3GPP defined functionalities and Virtualisation layer

- Type 3: implement 3GPP defined functionalities, Virtualisation layer, and hardware layer

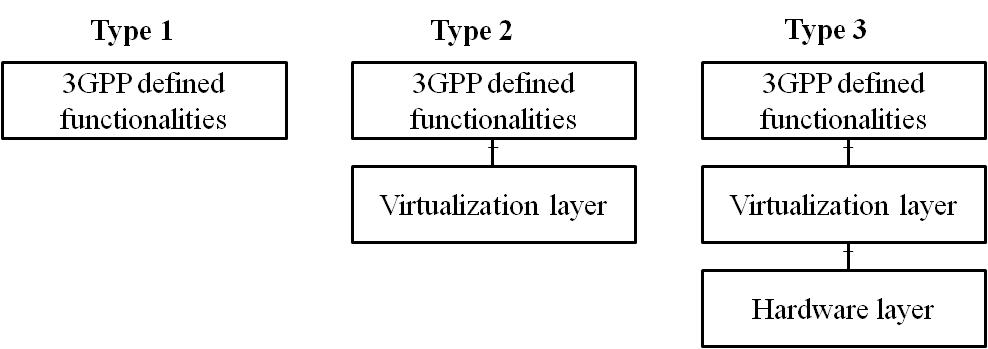


Figure 4.1.1-1: Three types of virtualised network product class

For type 2 and type 3, the.3GPP defined functionalities, the Virtualisation layer, and the hardware layer can be decoupled from each other and can be provided either by a vendor or by different vendors. In coupling scenario, the interface between components could be considered as internal interface.



Figure 4.1.1-2: Type2 in coupling scenarios

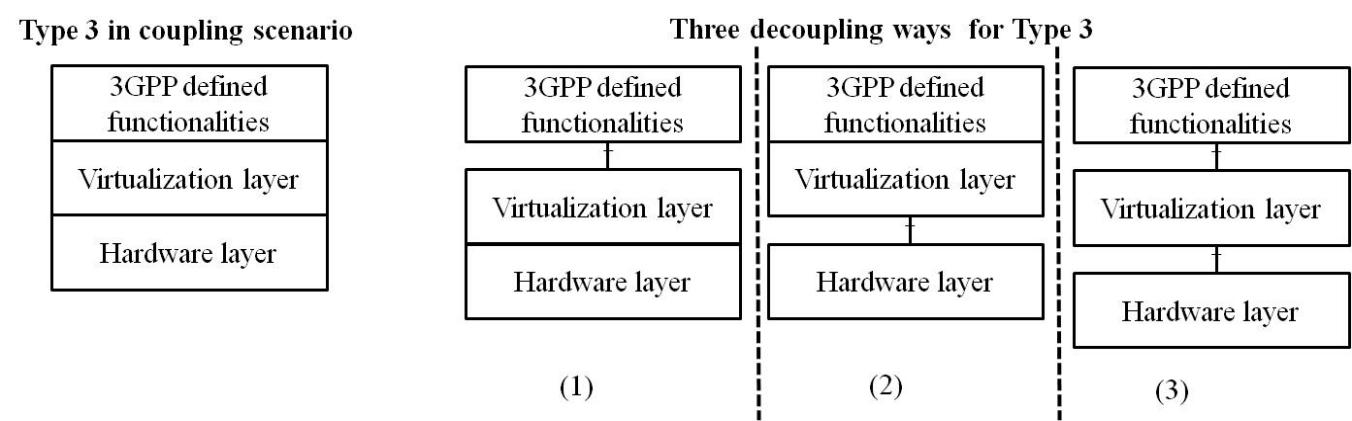


Figure 4.1.1-3: Type3 in coupling scenarios

For type 2 in the decoupling scenario as depicted in Figure 2, a network operator can purchase the 3GPP defined functionalities and the Virtualisation layer from the same or different vendors. So, it is required to assure the security of the decoupled 3GPP defined functionalities and the Virtualisation layer separately. Only decoupled 3GPP defined functionalities is in 3GPP scope. The security assurance evaluation about pure virtualisation layer is out of 3GPP scope.

For type 3 in the decoupling scenario as depicted in Figure 3, there are three decoupling ways. Like type 2 in the decoupling scenario, the security assurance requirements of the decoupled components need to be considered respectively. Only decoupled 3GPP defined functionalities in Figure 4.1.1-3 (1) and in Figure 4.1.1-3 (3) or coupled 3GPP defined functionality and virtualisation layer in Figure 4.1.1-3 (2) is in 3GPP scope. The security assurance evaluation about the others are out of 3GPP scope.

Note 1: For decoupling scenarios supporting a 3GPP GVNP, it could be considered as coupling part which is in 3GPP scope and decoupled part which is out of 3GPP scope. Only coupling part in 3GPP scope will be considered in rest of the present document.

NOTE 2: For the purpose of testing a 3GPP GVNP of type 1 or a 3GPP GVNP of type 2, NFVI for GVNP for type 1, or hardware for GVNP for type 2 are assumed to have gone through security assurance testing in the same rigorous manner that is similarly applied to the security assurance testing of any other 3GPP network product under consideration in SCAS.

### 4.1.2 Considerations on SECAM of the virtualised network products

The security assurance methodology study in TR 33.916 [2] is a general methodology and already considers virtualised network products in the design of the methodology. The biggest difference between virtualised network products and physical network products is that the former may be run on a common platform, while the latter has a private and exclusive platform. With the current SECAM as the basis, the present document aims to identify and address the gaps when applying the current SECAM to 3GPP virtualised network products as defined in clause 4.1.1.

## 4.2 Scope of a SECAM SCAS for 3GPP virtualised network products

### 4.2.1 Gap analysis

As with 3GPP physical network products, the targets of the security attack analysis need to be identified before identifying the potential attack vectors which could be used. According to the description in clause 4.1.1, three types of 3GPP virtualised network product class are defined. So, these three types of 3GPP virtualised network product class are the analysis objects of attack vectors. This is different from using 3GPP physical network product class composed of hardware, software, and interfaces as the analysis target for attack vectors. The security threat analysis and related security requirements of all these virtualised network product classes will be described in clause 5.

As the different types for 3GPP virtualised network product classes are partially inclusive, it needs to study whether it there will be substantial overlap for document writing between type 1, type 2 and type 3 SCAS of different virtualised network product classes.

The validation of evaluation performed in the past and the overall process of the validation for environment assumptions that proposed in clause 4.1 of TR 33.916 [2] can also be applied to SCAS of 3GPP virtualised network products.

### 4.2.2 Scope of a SECAM SCAS

The Security Assurance Specification (SCAS) for a given 3GPP virtualised network product class provides a description of the security requirements and associated test cases. The SCAS for a given 3GPP virtualised network product class defined in clause 4.1.1 is described below:

- For type 1 (implementing 3GPP defined functionalities only): the SCAS provides a description of the security requirements and associated test cases pertaining to 3GPP VNF.

- For type 2 (implementing 3GPP defined functionalities and Virtualisation layer): the SCAS provides a description of the security requirements and associated test cases pertaining to 3GPP VNF and Virtualisation layer together. The security assurance requirements on the interface between 3GPP VNF and Virtualisation layer is only applied in decoupling scenarios.

- For type 3 (implementing 3GPP defined functionalities, Virtualisation layer, and hardware layer): the SCAS provides a description of the security requirements and associated test cases pertaining to 3GPP VNF, Virtualisation layer and hardware layer together. The security assurance requirements on the interfaces between components of type 3 are only applied in decoupling scenarios.

Same as SECAM for 3GPP physical network products documented in TR 33.916 [2], evaluations performed in the past remain valid. The environmental assumptions which are contained in SCAS of 3GPP virtualised network products will be validated during product deployment and it's not part of SECAM.

## 4.3 Scope of SECAM evaluation for 3GPP virtualised network products

### 4.3.1 Gap analysis

The current scope of SECAM evaluation for 3GPP network products comprises the Vendor Network Product Development process evaluation, the product lifecycle process evaluation and the Network Product evaluation. Such objectives mainly focus on development and lifecycle, and they do not differentiate whether a product is physical or virtualised. Hence the scope also applies to SECAM evaluation of 3GPP virtualised network products.

The product lifecycle process of a physical network product consists of a number of processes, e.g. first commercial introduction, update, minor release, major release and end of life. The vendor network product development and lifecycle processes in these stages should comply with security requirements such as security by design, version control system, change tracking, source code review and security testing as specified in [7]. This generic product lifecycle process and the related security requirements can be applied to a virtualised network product.

### 4.3.2 Scope of a SECAM evaluation

The type of SECAM evaluation tasks in clause 4.2 of TR 33.916 [2] can be applied to 3GPP virtualised network products.

NOTE: Details of activity for the Vendor Virtualised Network Product Development process evaluation and the virtualised network product lifecycle process evaluation can be found in clause 7 of present document and the documents defined by the SECAM Accreditation Body.

## 4.4 Scope of SECAM Accreditation for 3GPP virtualised network products

### 4.4.1 Gap analysis

According to the definitions of accreditation and SECAM Accreditation Body in TR 33.916 [2], it is a general way to ensure the accuracy and recognition of the evaluation results for the network products through the accreditation and SECAM Accreditation Body. So, it can be applicable to all of the network products, regardless of whether the network product is physical network product or virtualised network product. It means, like for physical network products, the actors who perform the SECAM tasks for 3GPP virtualised network products should also be accredited by the SECAM Accreditation Body.

Table 4.4-1: Mapping between SECAM phases and involved party

|  |  |
| --- | --- |
| **SECAM tasks** | **Accredited actor** |
| Vendor Network Product Development and virtualised network product lifecycle management process | Auditor appointed by SECAM Accreditation Body |
| Compliance declaration with the accredited generic vendor development and lifecycle process requirements | Accredited vendor |
| Virtualised network product evaluation which includes Security compliance testing and Basic Vulnerability Testing | Accredited vendor or accredited third-party test laboratory |

The above tale 4.4-1 describes the accredited actor for each SECAM task for 3GPP virtualised network products. Like the SECAM Accreditation Body for the physical network products, the SECAM Accreditation Body for 3GPP virtualised network products is responsible for writing and managing the accreditation, monitoring rules and handling the dispute resolution process. But the decision on who takes the role of SECAM Accreditation Body should be made in cooperation with other SDOs such as GSMA, etc.

### 4.4.2 Scope of SECAM Accreditation

The scope of the SECAM accreditation in clause 4.3 of TR 33.916 [2] can be applied to 3GPP virtualised network products.

as GSMA shows interest on accreditation of virtualised network product when SCAS of virtualised network product is established, it is recommend to leave accreditation responsibility to GSMA.

## 4.5 Ultimate Output of SECAM Evaluation for 3GPP virtualised network products

### 4.5.1 Gap analysis

In clause 4.3.2, it is described that the type of SECAM evaluation tasks in clause 4.2 of TR 33.916 [2] can be applied to 3GPP virtualised network products, so the type of ultimate outputs from SECAM evaluation tasks for 3GPP physical network products can also be applied to 3GPP virtualised network products. It means the type of ultimate outputs from SECAM evaluation tasks for 3GPP virtualised network products includes an evaluation report of the virtualised network products, the evidence that the accredited vendor product and development lifecycle processes have been complied with for the network product, the evidence that the actors performing the evaluation tasks are accredited by the SECAM Accreditation Body.

Since the virtualised network product is delivered to the operator, the evaluation report of a virtualised network product should be examined by the operator. To maintain the fairness, the evidence of the actors which performs the evaluation tasks should be accredited by the SECAM Accreditation Body. These are the same with the evaluation report examination and the evidence of the actor accreditation for the physical network product.

### 4.5.2 Ultimate Output of SECAM Evaluation

The ultimate output of the SECAM evaluation for 3GPP virtualised network products is:

- an evaluation report demonstrating compliance of the network product with the 3GPP security assurance specifications.

- evidence to demonstrate to the test laboratory that the accredited vendor product and development lifecycle processes have been complied with for the network product. - evidence that the actors performing the evaluation tasks are accredited by the SECAM Accreditation Body. Such evidence is not required if there is consent between operator and vendor to not use the accreditation process.

Like for physical network products, the evaluation report of a virtualised network product is examined by the operator and the evidence that the actors performing the evaluation tasks are accredited by the SECAM Accreditation Body.

## 4.6 3GPP virtualised network products evaluation process

### 4.6.1 Gap analysis

The security assurance process defined in clause 4.5 of TR 33.916 [2] includes evaluating network products, outputting the evaluation report, operator's acceptance decision. A vendor also performs certification activities for network products in addition to self-declaration after outputting evaluation report. This process is a general process and can be applied to 3GPP virtualised network products.

### 4.6.2 Virtualised network product evaluation process

3GPP virtualised network product evaluation process is generally the same as 3GPP physical network product evaluation process. The security assurance process of virtualised network products describes how the operator gets assurance regarding the security of the virtualised network product.



Figure 4.6.2-1: SECAM defined Security assurance process

The figure 4.6.2-1 describes the security assurance process of the virtualised network products. The process is the same as 3GPP physical network product evaluation process. The Security Assurance Specifications (SAS(s)) in the figure refer to 3GPP SCAS specifications against which virtualised network products are evaluated.

## 4.7 Roles in SECAM for 3GPP virtualised network products

### 4.7.1 Gap analysis

According to the descriptions in clauses 4.3 and 4.4, the type of SECAM evaluation tasks and types of the accredited actors in clauses 4.2 and 4.3 of TR 33.916 [2] can be applied to the SECAM evaluation and accreditation for 3GPP virtualised network products. So, the roles involved in SECAM evaluation and accreditation described in TR 33.916 [2] can also be applied to 3GPP virtualised network products. However, there are still the following gaps:

- Vendor: there may be other types of vendor except the traditional CT vendors.

- SECAM Accreditation Body: whether GSMA can take the role or not is to be confirmed.

### 4.7.2 SECAM Roles Overview

Compared to the types of roles for 3GPP physical network products, the types of the basic roles for 3GPP virtualised network products also include vendor, test laboratory, operator, 3GPP and SECAM Accreditation Body. For SECAM Accreditation Body, it needs to be confirmed whether GSMA can take the role.

### 4.7.3 Examples of instantiation of roles in SECAM

#### 4.7.3.1 Introduction

The following clause contains an example for instantiation of roles in SECAM.

#### 4.7.3.2 Example: Complete self-evaluation

Complete self-evaluation of a 3GPP virtualised network product (e.g. vMME (MME VNF) + virtualised layer from vendor X)

This example below is similar to the SECAM defined Security assurance process in the figure 4.7.3.2-1 except that the vendor conducts all the phases of evaluation.



Figure 4.7.3.2-1: Complete self-evaluation of a 3GPP virtualised network product  
 (e.g. vMME (MME VNF) + virtualised layer from vendor X)

Evaluation results are checked by operators and dispute on evaluation results is resolved by the SECAM Accreditation Body.

## 4.8 Operator security acceptance decision for 3GPP virtualised network products

### 4.8.1 Gap analysis

In clause 4.7 of TR 33.916 [2], it was proposed that for the evaluation result of the network products, the operator decides the security acceptance through examining the network product, the security compliance testing, the basic vulnerability testing analysis reports, the self-declaration as well as the optional evidence of accreditation from the SECAM Accreditation Body. Based on the output of SECAM evaluation and the evaluation process in clauses 4.5.2 and 4.6.2, the evaluation of the virtualised network products also has the contents which are examined during operator security acceptance decision. In addition, operator security acceptance decision in clause 4.7 of TR 33.916 [2] is general process. So, it can be applied to 3GPP virtualised network products.

### 4.8.2 Operator security acceptance decision

Operator security acceptance decision for 3GPP virtualised network products is the same as those for 3GPP physical network products, i.e. operator examines the ultimate outputs of the evaluation, the self-declaration and decides if the results are sufficient according to its internal policies, etc.

## 4.9 SECAM Assurance level for 3GPP virtualised network products

### 4.9.1 Gap analysis

SECAM assurance level for 3GPP physical network products was analysed in clause 4.8 of TR 33.916 [2]. This analysis about SECAM assurance level is general and can be applicable to all of the network products, regardless of whether the network product is physical network product or virtualised network product. In addition, per network product class being considered only one SECAM assurance level could reduce the complexity of the network product evaluation. So, SECAM of the virtualised network products also considers only one assurance level per virtualised network product class.

### 4.9.2 SECAM Assurance level

Compared to SECAM assurance level for 3GPP physical network products, SECAM assurance level for 3GPP virtualised network products also considers only one assurance level per 3GPP virtualised network product class.

## 4.10 Security baseline for 3GPP virtualised network products

### 4.10.1 Gap analysis

The analysis about security baseline for network products in clause 4.9 of TR 33.916 [2] is general and is applicable for all of the network products, regardless of whether the network product is physical network product or virtualised network product. So, SECAM considers only one security baseline per virtualised network product class.

### 4.10.2 Security baseline

Compared to the security baseline for 3GPP physical network products, the security baseline for 3GPP virtualised network products also consider only one security baseline per 3GPP virtualised network product class, which is built on the entire set of security requirements, operational environment assumptions and attacker model.

# 5 Security Assurance Specification (SCAS) Creation

## 5.1 Writing process overview

The steps of a SCAS document (i.e. describing and modelling the network product class, defining the security problem, identifying the security requirements and test cases, verifying the security requirements) in clause 5.1 of TR 33.916 [2] is high level and general. So, these steps can be applied to the process of writing SCAS documents for a given virtualised network product class. However, according to the description of 3GPP virtualised network product class in clause 4.1.1, the components may be decoupled for a virtualised network product class (e.g. type2-implementing 3GPP defined functionalities and Virtualisation layer) and the security requirements on the interfaces between the components are only considered in decoupled scenario. So, when describing and modelling a given virtualised network product class, and when identifying its security requirements and test cases, it should be considered whether its components are decoupled or not.

## 5.2 SCAS documents structure and content

### 5.2.1 General

According to clause 5.1, the SCAS documents contain three parts, i.e. Virtualised Network Product Class Description, Security Problem Definition and Security Requirements (including the test cases) for any specific Network Product Class, to counteract the risks outlined by the threat analysis. Consequently SCAS documents for virtualised network products contain the following parts:

***- Network Product Class Description for virtualised network products (NPCDV):*** This clause includes the description of the virtualised network product class defined in clause 4.1.1, e.g. the physical and logical interfaces that the product class supports to interact with external entities and the major functionalities of the VNPC. This material will be contained in a 3GPP Technical Report of the 900-series.

***- Security Problem Definition (SPD):*** This clause defines the security problem that is to be addressed and the security objectives of the virtualised network product class. This material will be contained in a 3GPP Technical Reports of the 900-series.

***- Security Requirements (SR):*** This clause defines the security requirements, which may include hardening requirements, selected according to the Security Problem Definition and the requirements strictly related to the 3GPP security features implemented by the virtualised network product class, as well as the security requirements of Virtualisation aspect defined in 3GPP and ETSI NFV, etc. Requirements and test cases will be contained in one or more 3GPP Technical Specifications.

In the following clauses, detailed descriptions of NPCDV, SPD and SR for virtualised network products are provided.

### 5.2.2 ToE

The term ToE is described in clause 5.2.4.2.2.1.2 of TR 33.805 [10] that ToE is a logical and physical perimeter for the evaluation and this perimeter heavily depends on the vendor's particular version of the Network Product. The term ToE if used in a SCAS always refers to the ToE described in the SCAS instantiation. This ToE definition also can be applied to ToE of virtualised network product. According to virtualised network product classes and decoupling scenarios described in clause 4.1.1, there may be multiple ToEs for an instantiated virtualised network product class.

### 5.2.3 Generic virtualised network product model class description

#### 5.2.3.1 Introduction

According to the definition of virtualised network product class, a virtualised network product class is the class of products that implement 3GPP defined network functionalities running on Network Function Virtualisation Infrastructure (NFVI). There are three types of the classes that are described in clause 4.1.1. The generic virtualised network product model classes are described in the following clauses.

#### 5.2.3.2 Generic virtualised network product model of type 1

##### 5.2.3.2.1 Description of the GVNP model

For the virtualised network product class type 1 (i.e. implementing 3GPP defined functionalities only), the following figure 5.2.3.2.1-1 depicts the components of a generic network product model at a high level.

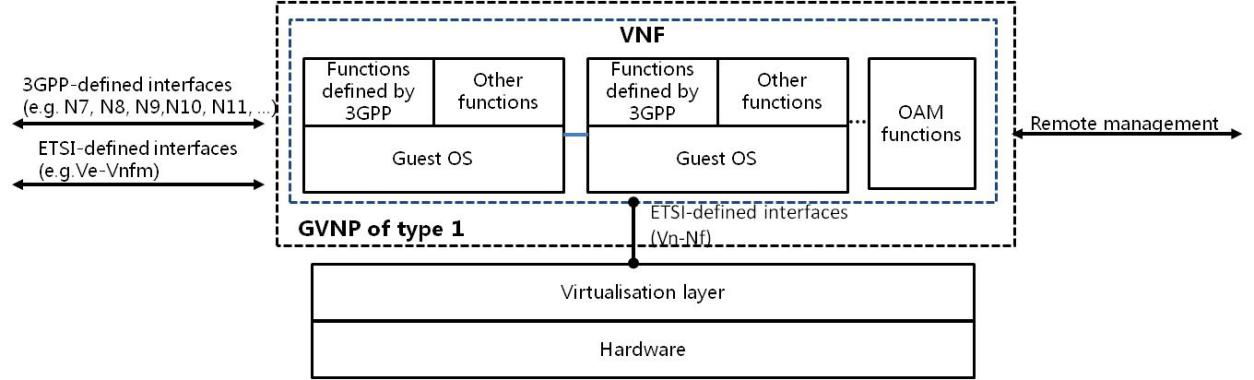


Figure 5.2.3.2.1-1: GVNP model of type 1

The components in the figure 5.2.3.2.1-1are further described in the following clauses.

##### 5.2.3.2.2 Functions defined by 3GPP

For a generic virtualised network function, it will implement 3GPP-defined functions. Unlike a generic physical network product, a 3GPP-denfined function can be deployed in multiple VMs and the feature s supported in different VM of the GVNP are up to the implementation of vendors.

To maintain generality and avoid overlap, the GVNP SCAS intends to explicitly address all GVNP functions that, if present in a GVNP, need to be evaluated and hence covered by the requirements in the GVNP SCAS.

##### 5.2.3.2.3 Other functions

A GVNP will also contain functionalities not or not fully covered in 3GPP specifications.

Examples include, but are not limited to, remote management functions.

##### 5.2.3.2.4 Operating system (OS)

The present document assumes that the functions of GVNP are implemented on multiple VMs. Each VM which is running on a common platform requires a guest operating system to run.

##### 5.2.3.2.5 Interfaces

Compared to generic physical network product, GVNP has also two types of logical interfaces, i.e. execution environment interfaces and remote logical interfaces.

The remote logical interfaces are interfaces which can be used to communicate with the GVNP from another network node and also include the remote access interfaces to the GVNP for its maintenance through e.g. an Element Management (EM), a Virtualised Network Function Manager (VNFM).

A GVNP hosts the following remote logical interfaces:

- Service interfaces that are defined in pertinent 3GPP specifications

- Service interfaces that are not defined by 3GPP

- Remote OAM interface

- Interface between EM (Element Management) and VNF which proprietary interface (see figure 5.2.3.2. 5-1)

- EMS (Element Management System) interface

- Interface defined by ETSI NFV specifications [11] and [12]:

- Interface between VNF and VNMF for GVNP lifecycle management, configuration information exchange, state information exchange necessary for network service lifecycle management, etc. This interface refers to Ve-Vnfm in the figure 5.2.3.2.5-1.

- An execution environment interface is an interface that can be used to provide the GVNP with the underlying execution environment, to guarantee hardware independent lifecycle, portability, and performance requirements of the GVNP.

A GVNP type 1 hosts the followingexecution environment interface:

- -Interface towards the underlying Virtualisation layer for execution environment provision. This interface refers to Vn-Nf in the figure 5.2.3.2.5-1.

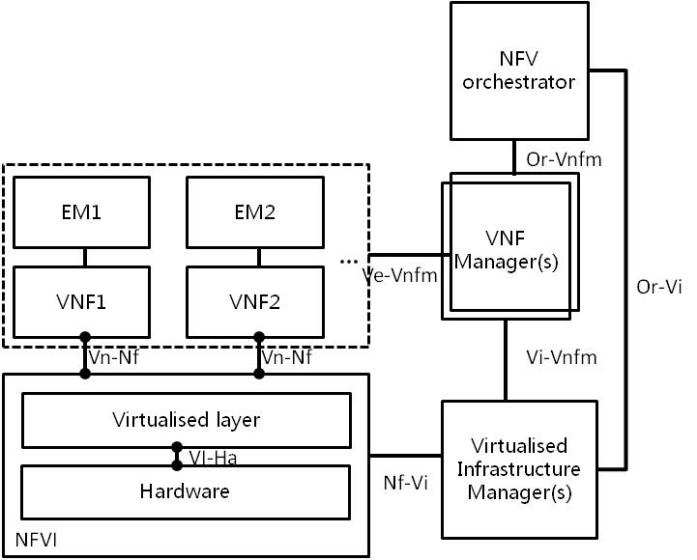


Figure 5.2.3.2.5-1: NFV reference architectural framework

#### 5.2.3.3 Generic virtualised network product model of type 2

##### 5.2.3.3.1 Description of the GVNP model

For the virtualised network product class type 2 (i.e. implementing 3GPP defined functionalities and virtualisation layer), the following figure 5.2.3.3.1-1 depicts the components of a generic network product model at a high level.

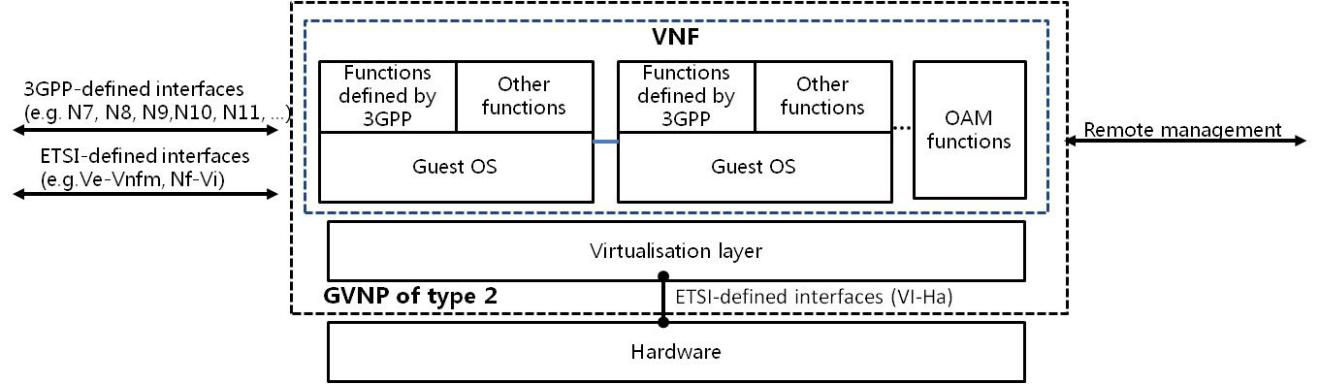


Figure 5.2.3.3.1-1: GVNP model of type 2

Compared to the GVNP model of the type 1 in figure 5.2.3.2.1-1, the GVNP model of the type 2 in the above figure has the Virtualisation layer in addition to 3GPP VNF. The VMs which deploy VNFCIs can be deployed in the multiple hosts, so there may be more than one instance of virtualisation layer that provide virtualisation resource for VNF. For simplicity, only one instance of virtualisation layer is shown in the figure 5.2.3.3.1-1. The components in the figure 5.2.3.3.1-1 are further described in the following clauses.

##### 5.2.3.3.2 Functions defined by 3GPP

All text from clause 5.2.3.2.2 applies to functions defined by 3GPP in the figure 5.2.3.3.1-1.

##### 5.2.3.3.3 Other functions

All text from clause 5.2.3.2.3 applies to other functions in the figure 5.2.3.3.1-1.

##### 5.2.3.3.4 Virtualisation layer

The virtualisation layer in a GVNP abstracts the hardware resources and decouples the VNF software from the underlying hardware. It provides the virtualisation resources (e.g. virtualised CPU, virtualised memory etc.) and the execution environment for the network functions of VNF [11]. The primary tools to realize the Virtualisation layer would be hypervisors [11]. The hypervisor can be run either directly on top of the hardware (bare metal hypervisor) or running on top of a hosting operating system (hosted hypervisor) [12]. In case of a hosted hypervisor, the Virtualisation layer includes both the hosted hypervisor and the hosting operating system.

Note: The definition of hypervisor is described in ETSI GS NFV-EVE 001 [12], i.e. the hypervisor is piece of software which partitions the underlying physical resources and creates Virtual Machines, and isolates the VMs from each other.

##### 5.2.3.3.5 Interfaces

For the GVNP model of the type 2, the Vn-Nf between VNF and the virtualised layer is an internal interface. So, in addition to the interface between the VNF and VNFM (ref. Ve-Vnfm), it has the following interface defined by ETSI NFV specifications [11] and [13]:

- Interface between the Virtualisation layer and VIM (ref. Nf-Vi) for virtualisation resource allocation, synchronization of virtualised resource state information.

- Execution environment interface (ref. VI-Ha) which towards the underlying hardware layer for execution environment creation.

The remote logical interfaces in clause 5.2.3.2.5 other than the above interfaces apply to the GVNP model of the type 2.

#### 5.2.3.4 Generic virtualised network product model of type 3

##### 5.2.3.4.1 Description of the GVNP model

For the virtualised network product class model of type 3 (i.e. implementing 3GPP defined functionalities, virtualisation layer, and hardware layer), the following figure 5.2.3.4.1-1 depicts the components of a generic network product model of type 3 at a high level.

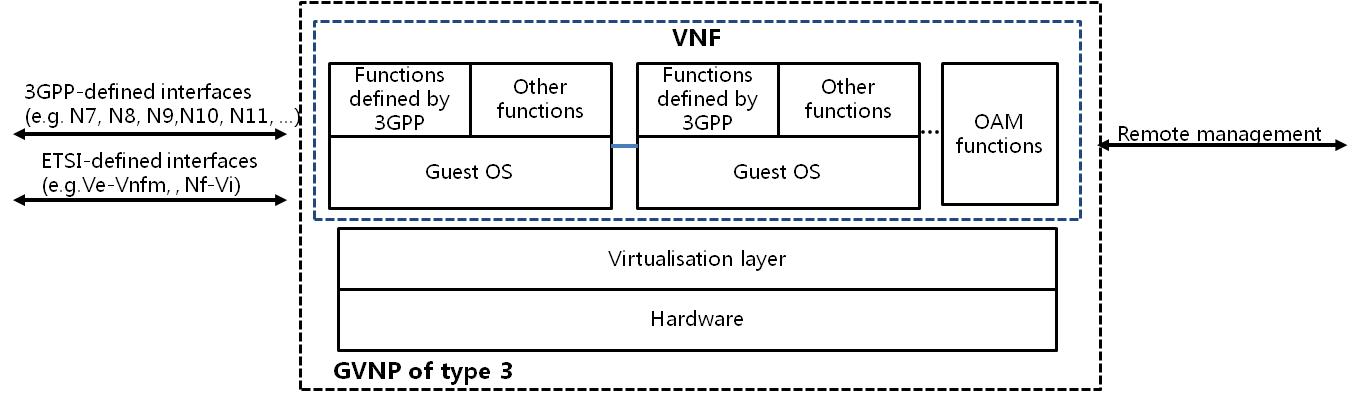


Figure 5.2.3.4.1-1: GVNP model of type 3

Compared to the GVNP model of type 2 in the figure 5.2.3.3.1-1, the GVNP model of type 3 in the above figure has hardware layer in addition to 3GPP VNF and virtualised layer. The VMs which deploy VNFCs can be deployed in the multiple hosts, so hardware layer that is shown in the figure 5.2.3.4.1-1 may consist of more than one host. The components in the figure 5.2.3.4.1-1 are further described in the following clauses.

##### 5.2.3.4.2 Functions defined by 3GPP

All text from clause 5.2.3.2.2 applies to functions defined by 3GPP in the figure 5.2.3.4.1-1.

##### 5.2.3.4.3 Other functions

All text from clause 5.2.3.2.3applies to other functions in the figure 5.2.3.4.1-1.

##### 5.2.3.4.4 Virtualisation layer

All text from clause 5.2.3.3.3 applies to virtualisation in the figure 5.2.3.4.1-1.

##### 5.2.3.4.5 Hardware

Hardware resources include computing, storage and network that provide processing, storage and connectivity to VNFs through the Virtualisation layer (e.g. hypervisor).

##### 5.2.3.4.6 Interfaces

For the GVNP model of the type 3, both interfaces (i.e. Vn-Nf and VI-Ha) are internal interfaces. So, the interfaces which are defined by ETSI NFV specification [11] just include the Ve-Vnfm and the Nf-Vi. The Nf-Vi

also includes hardware resource configuration and state information (e.g. events) exchange in addition to virtualisation resource allocation, synchronization of virtualised resource state information.

The remote logical interfaces in clause 5.2.3.2.5 other than the above interfaces apply to the GVNP model of the type 3.

### 5.2.4 Security Problem Definition (SPD) for 3GPP virtualised network products class

#### 5.2.4.1 Introduction

Clause 5.2.2 of TR 33.916 [2] describes the steps to be accomplished for the SPD part of the SCAS writing phase, principles and structures for threats and security objectives. These are general guidelines and can also be applied to SPD analysis of 3GPP virtualised network products. In addition, clause 5 of TR 33.926 [3] describes the generic assets and threats according to the structures described in TR 33.916 [2]. The following clauses describe the generic assets and threats in the course of developing 3GPP security assurance specifications for a particular virtualised network product class by referring to the generic assets and threats in TR 33.926 [3].

#### 5.2.4.2 Generic assets and threats of GVNP for type 1

##### 5.2.4.2.1 Generic assets of GVNP for type 1

The critical assets of GVNP for type 1 that need to be protected are:

- User account data and credentials (e.g. passwords, private key);

- Log data;

- Configuration data, e.g. GVNP's IP address, ports, VPN ID, Management Objects (e.g. user group, command group) etc.

- Guest Operating System, i.e. the files that make up the guest OS and its processes (code and data);

- GVNP Application;

- Sufficient processing capacity: that processing powers are not consumed close to limits;

- The interfaces of GVNP to be protected and which are within SECAM scope: for example:

- OAM interface, for remote access: interface between GVNP and OAM system

- Interface between virtualised network function (VNF) and VNFM

- Interface between VNF and virtualisation layer, for providing the execution environment to run VNF

- GVNP Software package (binary code or executable code) which includes:

- VNFD;

- VNF image and image description file;

- Configuration data (e.g. manifest file as defined in [15]).

##### 5.2.4.2.2 Generic threats for GVNP of type 1

5.2.4.2.2.1 Introduction

In clause 5.3.1 of TR 33.926 [3], the identified threats are grouped into seven categories, one covering threats relating to 3GPP-defined interfaces and the other six corresponding to the categories proposed by STRIDE. Since these seven categories are for generic 3GPP network products, they are also applicable to GVNP of type 1. In addition, GVNP of type 1 also needs to consider the threats related to ETSI-defined interfaces. As a result, there are eight categories of threats for GVPN of type 1. The following clauses describe the threats according to these security categories and use the template of threat description in clause 5.3.1 of TR 33.926 [3]. For threats descriptions of current seven categories, the present document will focus on the differences between GVNP threats and GNP threats which are described in TR 33.926 [3].

5.2.4.2.2.2 Threats relating to 3GPP-defined interfaces

For GVNP of type1 and GNP in TR 33.926 [3], the threats related to 3GPP-defined interfaces are the same. So, all texts in clause 5.3.2 of TR 33.926 [3] apply to GVNP of type 1. It means that there is no need repeat the threats relating to 3GPP-defined interfaces which are covered in 3GPP security specifications. If threats relating to 3GPP-defined interfaces are found not sufficiently covered in existing 3GPP security specifications, they need to be addressed in the SCAS for virtualised network products.

5.2.4.2.2.3 Threats relating to ETSI-defined interfaces

Two of the interfaces defined in ETSI NFV specification [11] are identified as the critical assets of GVNP type 1, i.e. interface between VNF and VNFM, interface between 3GPP VNF and virtualisation layer. The threats on these interfaces are as follows.

- Threats on interface between 3GPP VNF and VNFM: if the interface is not protected, an attacker can attack all the requests/responses sent between the VNF and the VNFM. For example, the attacker can insert, tamper or delete e.g. scaling requests, healing requests, subscribe requests, query requests and other management related requests sent from the instantiated GVNP of type 1 to the VNFM, hence the virtualised resource or relevant status information obtained by the instantiated GVNP of type 1 is not as requested. This affects the normal operation of the instantiated GVNP of type 1, and even causes DoS attacks, information leakage.

NOTE: The Virtualisation layer is out of 3GPP scope, but its protection will affect the security of the upper layer it supports. If the Virtualisation layer is compromised, the VNF on top of it could also be easily compromised. In such case, the messages sent over the VNF-VNFM interface can be manipulated by the compromised VNF, which is however not a threat coming from the VNF-VNFM interface. The analysis above focuses on the threats directly placed on VNF-VNFM interface, when it is not well protected.

- Threats on interface between 3GPP VNF and virtualisation layer: an attacker can attack an instantiated GVNP of type 1 through a compromised virtualisation layer. For example, cryptographic keys or other security critical data of an instantiated GVNP of type 1 could be stolen by an attacker with access to the virtualisation layer, or the virtualised resource provided by the Virtualisation layer to the instantiated GVNP of type 1 can be manipulated or the bootloader of Guest OS of an instantiated GVNP of type 1 can be tampered by an attacker via a compromised virtualisation layer.

5.2.4.2.2.4 Spoofing identity

5.2.4.2.2.4.1 Default Accounts

The threat in clause 5.3.3.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. The difference is that VNF is accessed through VNC (Virtual Network Console) rather than through the physical console interface, an attacker can use a default account to access a VNF via VNC.

5.2.4.2.2.4.2 Weak Password Policies

The threat in clause 5.3.3.2 of TR 33.926 [3] is generic, so it also applies to GVNP. However, the attacker using the weak password accesses GVNP through VNC (Virtual Network Console) rather than through the physical console interface.

5.2.4.2.2.4.3 Password peek

The threat in clause 5.3.3.3 of TR 33.926 [3] is generic, so it also applies to GVNP. However, the attacker using the peeked password accesses GVNP through VNC (Virtual Network Console) rather than through the physical console interface.

5.2.4.2.2.4.4 Direct Root Access

The threat in clause 5.3.3.4 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. There are no differences between direct root accesses for GVNP and GNP described in TR 33.926 [3].

5.2.4.2.2.4.5 IP Spoofing

The threat in clause 5.3.3.5 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. However, the objective of unauthorized access is a VNF, not a computer.

5.2.4.2.2.4.6 Malware

The threat in clause 5.3.3.6 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.4.7 Eavesdropping

The threat in clause 5.3.3.7 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5 Tampering

5.2.4.2.2.5.1 Software Tampering

The threat in clause 5.3.4.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. Different from traditional physical network products, as the entire GVNP is instantiated by the image(s) and other information (e.g. configuration data, software environmental parameters, licence terms information, script, manifest file, checksum, etc. as defined in [15]) within a software package, additional threats are analysed as follows:

*- Threat Name*: Software Tampering

*- Threat Category*: Tampering

- *Threat Description*: Compared with GNP software, GVNP software has additional attack surfaces, e.g. in the process of VNF package on boarding, during which the software package of a GVNP can be tampered/altered if not protected. An attacker, for example, can inject malicious code or tamper the information inside the unprotected package during on boarding. Then after the instantiation of the GVNP, the tampered code can be executed to conduct several attacks (e.g. DoS, Information Stealing, Frauds and so on).

*- Threatened Asset*: all critical assets of GVNP type 1 as listed in clause 5.2.4.2.1.

5.2.4.2.2.5.2 Ownership File Misuse

The threat in clause 5.3.4.2 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5.3 Boot tampering for GVNP of type 1

For GVNP of type 1, there is no hardware. This is different from external device boot of GNP described in clause 5.3.4.3 of TR 33.926 [3]. The threat is described as follows:

*- Threat name*: GVNP of type 1 boot tampering

*- Threat Category*: Tampering

*- Threat Description:* the GVNP bootloader may be maliciously tampered by an attacker, e.g. the attacker tampers the bootloader of GVNP through a malicious virtualisation layer.

*- Threatened Asset:* guest operating system

5.2.4.2.2.5.4 Log Tampering

The threat in clause 5.3.4.4 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5.5 OAM traffic Tampering

The threat in clause 5.3.4.5 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5.6 File Write Permissions Abuse

The threat in clause 5.3.4.6 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5.7 User Session Tampering

The threat in clause 5.3.4.7 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.6 Repudiation

5.2.4.2.2.6.1 Lack of User Activity Trace

The threat in clause 5.3.5.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7 Information disclosure

5.2.4.2.2.7.1 Poor key generation

The threat in clause 5.3.6.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.2 Poor key management

The threat in clause 5.3.6.2 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.3 Weak cryptographic algorithms

The threat in clause 5.3.6.3 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.4 Insecure Data Storage

*- Threat name*: Insecure Data Storage

*- Threat Category*: Information Disclosure

*- Threat Description:* The GVNP remotely stores sensitive data (e.g. passwords, private keys, logs) on the logical volume that the VIM allocates to the GVNP. An attacker can retrieve these data if they have been stored in an insecure way (e.g. clear text, unsalted hashes).

*- Threatened Asset*: Any sensitive data stored on the logical volume of the GVNP

5.2.4.2.2.7.5 System Fingerprinting

The threat in clause 5.3.6.5 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.6 Malware

- Threat name: Malware.

- Threat Category: Information Disclosure.

- Threat Description: A malware installed on the logical volume that the VIM allocates to the GVNP can access to the stored sensitive data (e.g. subscription data, logs).

- Threatened Asset: Any sensitive data stored on the logical volume of the GVNP.

5.2.4.2.2.7.7 Personal Identification Information Violation

The threat in clause 5.3.6.7 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.8 Insecure Default Configuration

The threat in clause 5.3.6.8 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.9 File/Directory Read Permissions Misuse

The threat in clause 5.3.6.9 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.10 Insecure Network Services

The threat in clause 5.3.6.10 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.11 Unnecessary Services

The threat in clause 5.3.6.11 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.12 Log Disclosure

The threat in clause 5.3.6.12 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.13 Unnecessary Applications

The threat in clause 5.3.6.13 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.14 Eavesdropping

The threat in clause 5.3.6.14 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.15 Security threat caused by lack of GVNP traffic isolation

The threat in clause 5.3.6.15 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.8 Denial of Service

The threats in all clauses of clause 5.3.7 for TR 33.926 [3] are generic, so they also apply to GVNP of type 1. In addition, there is DoS attack due to changing virtualisation resource that is used by GVNP. The detailed threat description is as follows:

*- Threat name*: changing virtualisation resource without authorization.

*- Threat Category*: DoS.

*- Threat Description*: There are several ways to cause a DoS attack for the GVNP: attackers having access to a compromised virtualisation layer can change the virtualisation resource used by the instantiated GVNP of type1 without authorization, or a malicious VM deployed for one instance of a VNF on a host can illegally occupy the resources of the instantiated GVNP of type1 deployed on the same host, resulting in resource limitation of the instantiated GVNP of type1, or attackers having access to a compromised VNFM can scale in a Type 1 or scale down the virtualisation resource used by a GVNP or even terminate a Type 1 instance without authorization.

*- Threatened Asset*: GVNP applications, sufficient processing capacity.

5.2.4.2.2.9 Elevation of privilege

The threats in all clauses of clause 5.3.8 for TR 33.926 [3] are generic, so they also apply to GVNP of type 1.

5.2.4.2.2.10 Threats relating to other functions

For GVNP of type 1, other functions not defined by 3GPP need to be well-documented by the vendor, including capabilities, purpose, internal interface to 3GPP defined functions, and interaction with the 3GPP defined functions. Without such documentation, all threats identified in clause 5.3.1 of TR 33.926 [3] apply.

5.2.4.2.2.11 Summary of threats for GVNP of type 1

The threats for GVNP of type 1 can be compared to TR 33.926 [3] and summarized as following:

|  |  |  |
| --- | --- | --- |
| Threat Category | Detailed threat | Comparison to TR33.926 [3] |
| Threats relating to 3GPP-defined interfaces | - | All threats can be applied. |
| Threats relating to ETSI-defined interfaces | - | New threats:   * The threats on interface between 3GPP VNF and VNFM * The threats on interface between 3GPP VNF and virtualisation layer |
| Spoofing identity | Default Accounts | Threats can be applied with difference that access through VNC instead of physical console interface. |
|  | Weak Password Policies | Same as above. |
|  | Password peek | Same as above. |
|  | Direct Root Access | Threats can be applied. |
|  | IP Spoofing | Threats can be applied with difference that objective is VNF instead of computer. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Different threats. See detail in clause 5.2.4.2.2.5.1. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tampering for GVNP of type 1 | Different threats. See detail in clause 5.2.4.2.2.5.3. |
|  | Log Tampering | Threats can be applied. |
|  | OAM traffic Tampering | Threats can be applied. |
|  | File Write Permissions Abuse | Threats can be applied. |
|  | User Session Tampering | Threats can be applied. |
| Repudiation | Lack of User Activity Trace | Threats can be applied. |
| Information disclosure | - | Different threats. See detail in clauses 5.2.4.2.2.7.4 and 5.2.4.2.2.7.6. |
| Denial of Service | - | Different threats. See detail in clause 5.2.4.2.2.8. |
| Elevation of privilege | - | All threats can be applied. |

#### 5.2.4.3 Generic assets and threats for GVNP of type 2

##### 5.2.4.3.1 Generic assets for GVNP of type 2

In addition to the critical assets for GVNP of type 1 described in clause 5.2.4.2.1, GVNP of type 2 also has the following critical assets:

- Interface between virtualisation layer and hardware, for creating an execution environment of VNFs, and collecting relevant hardware resource state information for managing the VNFs without being dependent on any hardware platform;

- Interface between virtualisation layer and Virtualised Infrastructure Manager (VIM), for resource management.

Moreover, for interface between VNF and virtualisation layer, compared to GVNP of type 1, it is an internal interface and does not be considered.

##### 5.2.4.3.2 Generic threats for GVNP of type 2

5.2.4.3.2.1 Introduction

Compared to GVNP of type 1, GVNP of type 2 has virtualisation layer besides 3GPP VNF. So the generic threats of GVNP for type 1 in clause 5.2.4.2.2 can be basically applied to GVNP for type 2. The following clauses will describe the critical threats for GVNP of type 2.

5.2.4.3.2.2 Threats relating to 3GPP-defined interfaces

Threats from clause 5.2.4.2.2.2 also apply to GVNP of type 2.

5.2.4.3.2.3 Threats relating to ETSI-defined interfaces

Since the 3GPP VNF is included in GVNP of type 2, the threats on the interface between 3GPP VNF and VNFM in clause 5.2.4.2.2.3 apply to GVNP of type 2. In addition, GVNP of type 2 also has following threats relating to ETSI-defined interfaces [11]:

- The threats on interface between virtualisation layer and hardware: an attacker can utilize the vulnerabilities of hardware (e.g. Meltdown and Spectre of CPU in host) to attack virtualisation layer and/or VNFs through this interface, resulting in information disclosure or DoS etc.

- The threats on interface between virtualisation layer and VIM: an attacker can tamper the specific assignment of virtualised resources to cause resource assignment errors or an attacker can intercept virtualised resources state information leading to information disclosure.

5.2.4.3.2.4 Spoofing identity

5.2.4.3.2.4.1 Default Accounts

The threat in clause 5.3.3.1 of TR 33.926 [3] also applies to GVNP of type 2. In addition to using default account to access GVNP, an attacker can also utilize default account to access VNF of GVNP for type 2 through VNC (Virtual Network Console).

5.2.4.3.2.4.2 Weak Password Policies

The threat in clause 5.3.3.2 of TR 33.926 [3] also applies to GVNP of type 2. In addition to using weak password to access GVNP, an attacker can also utilize weak password to access VNF of GVNP of type 2 through VNC (Virtual Network Console).

5.2.4.3.2.4.3 Password peek

The threat in clause 5.3.3.3 of TR 33.926 [3] also applies to GVNP of type 2. In addition to using peeked password to access GVNP, an attacker can also utilize peeked password to access VNF of GVNP of type 2 through VNC (Virtual Network Console).

5.2.4.3.2.4.4 Direct Root Access

The threat in clause 5.3.3.4 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.4.5 IP Spoofing

All texts from clause 5.3.3.5 of TR 33.926 [3] also apply to GVNP of type 2. The objectives of unauthorized access include VNF and virtualisation layer rather than a computer.

5.2.4.3.2.4.6 Malware

The threat in clause 5.3.3.6 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.4.7 Eavesdropping

The threat in clause 5.3.3.7 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.5 Tampering

5.2.4.3.2.5.1 Software Tampering

The threat in clause 5.2.4.2.2.5.1 of the present document for GVNP of type 1 also applies to GVNP of type 2.

5.2.4.3.2.5.2 Ownership File Misuse

The threat in clause 5.3.4.2 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.5.3 Boot tampering for GVNP of type 2

For GVNP of type 2, like the threat described in clause 5.3.4.3 of TR 33.926 [3], bootloader of guest OS and/or host OS may be maliciously tampered by an attacker when it is booted from external source. In addition, the bootloader of guest OS may also be tampered, with reference to the description in clause 5.2.4.2.2.5.3. The threat is described as follows:

*- Threat name*: GVNP of type 2 boot tampering

*- Threat Category*: Tampering

*- Threat Description:* The bootloader of host OS and guest OS for GVNP may be maliciously tampered by an attacker, e.g. the attacker compromises host OS to tamper the bootloader of guest OS, or tampers the bootloader of host OS when it is booted from external source (such as USB flash drive, memory card).

*- Threatened Asset:* guest operating system, host OS

5.2.4.3.2.5.4 Log Tampering

The threat in clause 5.3.4.4 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.4.5 OAM traffic Tampering

The threat in clause 5.3.4.5 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.4.6 File Write Permissions Abuse

The threat in clause 5.3.4.6 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.4.7 User Session Tampering

The threat in clause 5.3.4.7 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.6 Repudiation

5.2.4.3.2.6.1 Lack of User Activity Trace

The threat in clause 5.3.5.1 of TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.7 Information disclosure

The threat in all clauses of clause 5.2.4.2.2.7 also applies to GVNP of type 2.

5.2.4.3.2.8 Denial of Service

The threat in all clauses of clause 5.3.7 for TR 33.926 [3] also applies to GVNP of type 2.

As GVNP type 2 contains the Virtualisation layer in addition to GVNP type 1,in addition to considering the threats from a compromised VNFM described in clause 5.2.4.2.2.8, the Virtualisation layer of GVNP type 2 could face the threats coming from the VIM which manages it via NFVI-VIM interface. The detailed threat description is as follows:

*- Threat name*: changing virtualisation resource via a compromised VIM or unprotected NFVI-VIM interface.

- Threat Category: DoS.

- Threat Description: A VIM which manages the Virtualisation layer is responsible for assigning virtualised resource as requested. If the VIM is compromised or the NFVI-VIM interface is not securely protected, an attacker who compromised the VIM or breached the NFVI-VIM interface can change the virtualised resource used by a GVNP by manipulating the allocation of virtualised resource. For example, when an instantiated VNF is running, attackers having access to a compromised VIM or attackers breaching the insecure NFVI-VIM interface can misguide the Virtualisation layer to reduce the resource of or delete a VM on which a VNFCI is running. This can result in the reliability, availability or even illegal termination of a GVNP and hence the denial of service.

- Threatened Asset: GVNP applications, NFVI-VIM interface, sufficient processing capacity.

5.2.4.3.2.9 Elevation of privilege

The threat in all clauses of clause 5.3.8 for TR 33.926 [3] also applies to GVNP of type 2.

5.2.4.3.2.10 Threats relating to other functions

For GVNP of type 2, other functions not defined by 3GPP need be well-documented by the vendor, including capabilities, purpose, internal interface to 3GPP defined functions, and interaction with the 3GPP defined functions. Without such documentation, all threats identified in clause 5.3.1 of TR 33.926 [3] apply.

5.2.4.3.2.11 Summary of threats for GVNP of type 2

The threats for GVNP of type 2 can be compared to TR 33.926 [3] and summarized as following:

| Threat Category | Detailed threat | Comparison to TR33.926 [3] |
| --- | --- | --- |
| Threats relating to 3GPP-defined interfaces | - | All threats can be applied. |
| Threats relating to ETSI-defined interfaces | - | All threats relating to ETSI-defined interfaces of Type 1 apply here.  Additional new threats:   * The threats on interface between virtualisation layer and hardware   The threats on interface between virtualisation layer and VIM |
| Spoofing identity | Default Accounts | The threats relating to Default Accounts of Type 1 apply here. |
|  | Weak Password Policies | Same as above. |
|  | Password peek | Same as above. |
|  | Direct Root Access | Threats can be applied. |
|  | IP Spoofing | Threats can be applied with difference that objective is VNF and virtualisation layer rather than computer. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Different threats. See detail in clause 5.2.4.3.2.5.1. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tampering for GVNP of type 2 | Different threats. See detail in clause 5.2.4.3.2.5.3. |
|  | Log Tampering | Threats can be applied. |
|  | OAM traffic Tampering | Threats can be applied. |
|  | File Write Permissions Abuse | Threats can be applied. |
|  | User Session Tampering | Threats can be applied. |
| Repudiation | Lack of User Activity Trace | Threats can be applied. |
| Information disclosure | - | Different threats. See detail in clauses 5.2.4.2.2.7.4 and 5.2.4.2.2.7.6. |
| Denial of Service | - | Different threats. See detail in clause 5.2.4.3.2.8. |
| Elevation of privilege | - | All threats can be applied. |

The threats for GVNP of type 2 can be compared to GVNP of type 1 and summarized as following:

|  |  |  |
| --- | --- | --- |
| Threat Category | Detailed threat | Comparison to GVNP of type 1 |
| Threats relating to 3GPP-defined interfaces | - | All threats can be applied. |
| Threats relating to ETSI-defined interfaces | - | The threats on the interface between 3GPP VNF and VNFM apply here.  Additional new threats:   * The threats on interface between virtualisation layer and hardware * The threats on interface between virtualisation layer and VIM |
| Spoofing identity | Default Accounts | The threats relating to Default Accounts of Type 1 apply here. |
|  | Weak Password Policies | Same as above. |
|  | Password peek | Same as above. |
|  | Direct Root Access | Threats can be applied. |
|  | IP Spoofing | Threats can be applied.  Additional new threat:  - The objective of unauthorized access includes a virtualised layer in addition to a VNF. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Threats can be applied. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tampering for GVNP of type 2 | Threats can be applied here.  Additional threat:   * an attacker tampers the bootloader of host OS when it is booted from external source. |
|  | Log Tampering | Threats can be applied. |
|  | OAM traffic Tampering | Threats can be applied. |
|  | File Write Permissions Abuse | Threats can be applied. |
|  | User Session Tampering | Threats can be applied. |
| Repudiation | Lack of User Activity Trace | Threats can be applied. |
| Information disclosure | - | Threats can be applied. |
| Denial of Service | - | The DoS from a virtualised layer does not apply here.  Additional new threat:   * The DoS comes from NFVI-VIM interface. |
| Elevation of privilege | - | Threats can be applied. |

#### 5.2.4.4 Generic assets and threats for GVNP of type 3

##### 5.2.4.4.1 Generic assets for GVNP of type 3

In addition to the critical assets for GVNP of type 2 described in clause 5.2.4.3.1, GVNP of type 3 also has the following critical assets:

- Interface between hardware and Virtualised Infrastructure Manager (VIM), for Hardware resource configuration and state information (e.g. events) exchange.

Moreover, for interface between virtualisation layer and hardware, compared to GVNP of type 2, it is only considered when virtualisation layer is decoupled from hardware.

##### 5.2.4.4.2 Generic threats for GVNP of type 3

5.2.4.4.2.1 Introduction

Compared to GVNP of type 2, GVNP of type 3 has hardware besides virtualisation layer. So the generic threats of GVNP for type 2 in clause 5.2.4.3.2.1 can be basically applied to GVNP for type 3. The following clauses will describe the critical threats for GVNP of type 3.

5.2.4.4.2.2 Threats relating to 3GPP-defined interfaces

All texts from clause 5.2.4.2.2.2 also apply to GVNP of type 3.

5.2.4.4.2.3 Threats relating to ETSI-defined interfaces

Since the 3GPP VNF and the virtualised layer is included in GVNP of type 3, the threats on the interfaces between 3GPP VNF and VNFM, between the virtualised layer and the VIM that described in clause 5.2.4.2.2.3 and clause 5.2.4.3.2.3 apply to GVNP of type 3 respectively. In addition, the hardware resource configuration and state information are sent to VIM through the internal VI-Ha interface and the Nf-Vi. GVNP of type 3 also has following threats relating to the Nf-Vi interface defined by ETSI GS NFV 002 [11]:

- Threats on interface between hardware and Virtualised Infrastructure Manager (VIM) (ref. Nf-Vi): an attacker can compromise VIM to tamper with the hardware state information (e.g. deleting hardware alarm information) to affect the hardware's operation or to result in information disclosure (e.g. an attacker can get the hardware configuration from the compromised VIM. Then, the attacker can attack the hardware according to the configuration such as CPU type, memory size etc.). An attacker can also tamper or intercept the hardware resource configuration and state information if the configuration and state information are transmitted using an insecure protocol on the NFVI-VIM interface.

5.2.4.4.2.4 Spoofing identity

5.2.4.4.2.4.1 Default Accounts

The threat in clause 5.3.3.1 of TR 33.926 [3] also applies to GVNP of type 3. In addition to using default account to access GVNP, an attacker can also utilize default account to access VNF of GVNP of type 3 through VNC (Virtual Network Console).

5.2.4.4.2.4.2 Weak Password Policies

The threat in clause 5.3.3.2 of TR 33.926 [3] also applies to GVNP of type 3. In addition to using weak password to access GVNP, an attacker can also utilize weak password to access VNF of GVNP of type 3 through VNC (Virtual Network Console).

5.2.4.4.2.4.3 Password peek

The threat in clause 5.3.3.3 of TR 33.926 [3] also applies to GVNP of type 3. In addition to using peeked password to access GVNP, an attacker can also utilize peeked password to access VNF of GVNP of type 3 through VNC (Virtual Network Console).

5.2.4.4.2.4.4 Direct Root Access

The threat in clause 5.3.3.4 of TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.4.5 IP Spoofing

All texts from TR 33.926 [3] in clause 5.3.3.5 also apply to GVNP of type 3. The objectives of unauthorized access include VNF and virtualisation layer in addition to the hardware host.

5.2.4.4.2.4.6 Malware

The threat in clause 5.3.3.6 of TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.4.7 Eavesdropping

The threat in clause 5.3.3.7 of TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.5 Tampering

5.2.4.4.2.5.1 Software Tampering

The threat in clause 5.2.4.2.2.5.1 of the present document for GVNP of type 1 also applies to GVNP of type 3.

5.2.4.4.2.5.2 Ownership File Misuse

The threat in clause 5.3.4.2 of TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.5.3 Boot tampering for GVNP of type 3

All texts in clause 5.2.4.3.2.5.3 also apply to GVNP of type 3.

5.2.4.4.2.5.4 Log Tampering

The threat in clause 5.3.4.4 of TR 33.926 [3] also applies to GVNP of type3.

5.2.4.4.2.4.5 OAM traffic Tampering

The threat in clause 5.3.4.5 of TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.4.6 File Write Permissions Abuse

The threat in clause 5.3.4.6 of TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.4.7 User Session Tampering

The threat in clause 5.3.4.7 of TR 33.926 [3] also applies to GVNP of type3.

5.2.4.4.2.6 Repudiation

5.2.4.4.2.6.1 Lack of User Activity Trace

The threat in clause 5.3.5.1 of TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.7 Information disclosure

The threat in all clauses of clause 5.2.4.2.2.7 also applies to GVNP of type 3.

5.2.4.4.2.8 Denial of Service

All texts from clause 5.3.7 of TR 33.926 [3] also apply to GVNP of type 3.

Furthermore, as GVNP type 3 contains the hardware layer in addition to GVNP type 2, except considering the threats from a compromised VNFM and NFVI-VIM (Nf-Vi) interface described in clauses 5.2.4.2.2.8 and 5.2.4.3.2.8 respectively, the hardware layer of GVNP type 3 could face the threats coming from the VIM which manages it via NFVI-VIM interface. The detailed threat description is as follows:

*- Threat name*: changing hardware configuration via a compromised VIM or unprotected NFVI-VIM interface.

*- Threat Category*: DoS.

*- Threat Description*: Hardware resource configuration and state information (e.g. events) exchange is performed through NFVI-VIM interface. If the VIM is compromised or the NFVI-VIM interface is not securely protected, an attacker who compromised the VIM or breached the NFVI-VIM interface can tamper the hardware configuration and state information so that the virtualised resource supported by the hardware layer becomes unreliable. For example, attackers having access to a compromised VIM or attackers breaching the insecure NFVI-VIM interface can misguide the NFVI to detach a hardware accelerator from a VNFCI.

*- Threatened Asset*: GVNP applications, NFVI-VIM interface, sufficient processing capacity.

5.2.4.4.2.9 Elevation of privilege

The threat in all clauses of clause 5.3.8 in TR 33.926 [3] also applies to GVNP of type 3.

5.2.4.4.2.10 Threats relating to other functions

For GVNP of type 3, other functions not defined by 3GPP need to be well-documented by the vendor, including capabilities, purpose, internal interface to 3GPP defined functions, and interaction with the 3GPP defined functions. Without such documentation, all threats identified in clause 5.3.1 of TR 33.926 [3] apply.

5.2.4.4.2.11 Summary of threats for GVNP of type 3

The threats for GVNP of type 3 can be compared to TR 33.926 [3] and summarized as following:

|  |  |  |
| --- | --- | --- |
| Threat Category | Detailed threat | Comparison to TR 33.926 [3] |
| Threats relating to 3GPP-defined interfaces | - | All threats can be applied. |
| Threats relating to ETSI-defined interfaces | - | All threats relating to ETSI-defined interfaces of Type 2 apply here.  Additional new threat:  - The threats on interface between hardware and Virtualised Infrastructure Manager (VIM) |
| Spoofing identity | Default Accounts | The threats relating to Default Accounts of Type 1 apply here. |
|  | Weak Password Policies | Same as above. |
|  | Password peek | Same as above. |
|  | Direct Root Access | Threats can be applied. |
|  | IP Spoofing | The threats relating IP Spoofing of Type 2 apply here. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Different threats. See detail in clause 5.2.4.4.2.5.1. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tempering for GVNP of type 3 | Different threats. See detail in clause 5.2.4.4.2.5.3. |
|  | Log Tampering | Threats can be applied. |
|  | OAM traffic Tampering | Threats can be applied. |
|  | File Write Permissions Abuse | Threats can be applied. |
|  | User Session Tampering | Threats can be applied. |
| Repudiation | Lack of User Activity Trace | Threats can be applied. |
| Information disclosure | - | Different threats. See detail in clauses 5.2.4.2.2.7.4 and 5.2.4.2.2.7.6. |
| Denial of Service | - | Different threats. See detail in clause 5.2.4.4.2.8. |
| Elevation of privilege | - | All threats can be applied. |

The threats for GVNP of type 3 can be compared to GVNP of type 2 and summarized as following:

|  |  |  |
| --- | --- | --- |
| **Threat Category** | **Detailed threat** | **Comparison to GVNP of type 2** |
| Threats relating to 3GPP-defined interfaces | - | All threats can be applied. |
| Threats relating to ETSI-defined interfaces | - | The threats on the interfaces between 3GPP VNF and VNFM, virtualised layer and VIM apply here.  Additional new threat:  - The threats on interface between hardware and Virtualised Infrastructure Manager (VIM) |
| Spoofing identity | Default Accounts | The threats relating to Default Accounts of Type 2 apply here. |
|  | Weak Password Policies | Same as above. |
|  | Password peek | Same as above. |
|  | Direct Root Access | Threats can be applied. |
|  | IP Spoofing | The threats relating IP Spoofing of Type 2 apply here.  Additional new threat:  - The objectives of unauthorized access includes the hardware. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Threats can be applied. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tempering for GVNP of type 3 | Threats can be applied. |
|  | Log Tampering | Threats can be applied. |
|  | OAM traffic Tampering | Threats can be applied. |
|  | File Write Permissions Abuse | Threats can be applied. |
|  | User Session Tampering | Threats can be applied. |
| Repudiation | Lack of User Activity Trace | Threats can be applied. |
| Information disclosure | - | Threats can be applied. |
| Denial of Service | - | The threats from a compromised VNFM and NFVI-VIM (Nf-Vi) interface apply to here.  Additional new threat:  - the threats that comes from the VIM which manages the hardware via NFVI-VIM interface. |
| Elevation of privilege | - | Threats can be applied. |

#### 5.2.4.5 Generic assets and threats for network functions supporting SBA interfaces

Since some 3GPP defined network functions supports SBA interface, assets and threats that are believed to apply to all network functions supporting service based interfaces also should be considered.

The network functions defined by 3GPP are same for GVNP and Physical GNP. So, the generic assets and threats for virtualised network functions supporting SBA interfaces in clause 6 of TR 33.926 could be applied to all types of GVNPs in the present document.

### 5.2.5 Potential Security Requirements

#### 5.2.5.1 Introduction

According to the scope of a SECAM SCAS in clause 4.1.2, a SCAS contains security requirements and associated test cases, and may contain environmental assumptions which will be validated during product deployment. So, like GNP in TR 33.916 [2], the countermeasures deemed relevant to threat mitigation will also take the form of either:

- security requirements on the network product with associated test cases; or

- operational environment security assumptions for a given product class.

For GVNP, the operational environment security assumptions among different product classes vary greatly, for example some sensitive 3GPP functions may need to be run from special security domain (See clause 5.2.1 of TR 33.848 [9]) or may need to implement hardware (See clause 4.9 in TR 33.916 [2]) with special security requirement that make it difficult, if not impossible to be realized in a GVNP implementation or the protection of certain data may require higher level of protection due to the extreme sensitive nature of the data (e.g. lawful interception target lists). It may also be necessary to consider such assumptions during testing so that stringent security requirements can be met. Any such consideration should be well-documented as part of both the testing environment so that the validation during product deployment can be carried out and duplicated.

The Security Requirements clauses within the pertinent TS contain the security requirements identified according to the threats (see figure 5.2.5.1-1).



Figure 5.2.5.1-1: Process for deriving security requirements in a SCAS document

The security requirements include security functional requirements and hardening requirements (see clause 5.2.1). Since SECAM tasks include Basic Vulnerability Testing, basic vulnerability testing requirements are also included in security requirements of a SCAS. The types of the security requirements are same as in TR 33.916 [2].

The three types of the levels of detail for security requirements in clause 5.2.3.1.1 of TR 33.916 [2] and the relationship between these levels are generic and are also applicable to describe the level of detail of security requirements for a GVNP.

#### 5.2.5.2 Incorporation of security requirements from existing 3GPP and ETSI specifications in current releases

According to GVNP model and threat analysis, the categories of potential security functional requirements can also include the following category extension to the three categories in clause 5.2.3.2 of TR 33.916 [2]:

- Security functional requirements related to Virtualisation layer, hardware and resource isolation, among others, which may be identified in TR 33.848 [9] and ETSI specifications.

The security functional requirements in this category are within scope of SCAS and related test cases will be proposed.

#### 5.2.5.3 Handling of security requirements

A SECAM Catalogue of General Security Assurance Requirements and associated test cases is proposed in clause 5.2.3.3 of TR 33.916 [2] to prevent from writing the same security requirements from scratch several times in different network product class SCAS. This generic way is also applied to SECAM of virtualised network product class.

Since SECAM and SCAS of physical network product class are bases for SECAM and SCAS of virtualised network product class, the security requirements of a virtualised network product class will refer to the security requirements already available in the current SECAM catalogue if possible otherwise select the new ones from the agreed sources and update the Catalogue. The template for a security requirement description of virtualised network product also uses the template in current SECAM which is described in TR 33.916 [2].

#### 5.2.5.4 Guidelines for writing test cases

Some general guidelines for writing test cases (e.g. describing test case, verifiability and repeatability of test case etc.) are described in clause 5.2.3.4 of TR 33.916 [2]. These general guidelines are also used to guide writing test case of virtualised network product class.

NOTE: All the test cases in the present document do not apply to the scenarios where the tested interfaces are not standard compliant, e.g. when the VNF and VNFM are provided by the same vendor who has proprietary implementation on the interface between them.

#### 5.2.5.5 Potential security functional requirements and related test cases for GVNP of type 1

##### 5.2.5.5.1 Introduction

The present clause describes potential security functional requirements and the corresponding test cases, independent of a specific virtualised network product class of type 1. According to security threats and security requirements in the above clauses, there are threats relating to ETSI-defined interfaces and Security functional requirements related to Virtualisation layer, hardware and resource isolation etc. (see clause 5.2.4.2.2 and clause 5.2.5.2). So, the proposed potential security requirements for GVNP of type 1 are classified in three groups:

- Security functional requirements deriving from 3GPP specifications and detailed in clause 5.2.5.5.2.

- General security functional requirements which include requirements not already addressed in the 3GPP specifications but whose support is also important to ensure a network product conforms to a common security baseline detailed in clause 5.2.5.5.3, clause 5.2.5.5.4, clause 5.2.5.5.5 and clause 5.2.5.5.6.

- Security functional requirements related to Virtualisation layer, hardware and resource isolation, among others. These requirements can be called security functional requirements deriving virtualisation for simplify and detailed in clause 5.2.5.5.7.

The threat cooperation between GVNP of type 1 and physical network products are summarized in clause 5.2.4.3.2.10. Except threats relating to ETSI-definer interfaces, other threat categories can apply to threat categories for GVNP of type 1. So, the potential security requirements of the above first and second group will base on the security requirements in clause 4.2 of TS 33.117 [4] to identify the different security requirements for GVNP of type 1.

##### 5.2.5.5.2 Potential security functional requirements deriving from 3GPP specifications and related test cases

5.2.5.5.2.1 Security functional requirements deriving from 3GPP specifications – general approach

The clause 4.2.2 in TS 33.117 [4] describes the general approach taken towards security functional requirements deriving from 3GPP specifications and the corresponding test cases, independent of a specific network product class. The general approach is generic and applies to security functional requirements deriving from 3GPP specifications and the corresponding test cases of GVNP type 1.

##### 5.2.5.5.3 Technical baseline for potential general security functional requirements

5.2.5.5.3.1 Introduction

The technical baseline is a generic set of security requirements to be fulfilled by all virtualised network products.

In particular these requirements counter the security threats identified in clause 5.2.4.2.2 and they basically aim to guarantee the network product confidentiality, integrity and availability.

5.2.5.5.3.2 Protecting data and information

All text from TS 33.117 [4], clause 4.2.3.2 applies to GVNP of type 1.

5.2.5.5.3.3 Protecting availability and integrity

5.2.5.5.3.3.1 System handling during overload situations

All text from TS 33.117 [4], clause 4.2.3.3.1 applies to GVNP of type 1.

5.2.5.5.3.3.2 Boot from intended memory devices only

All text from TS 33.117[4], clause 4.2.3.3.2 applies to GVNP of type 1.

5.2.5.5.3.3.3 System handling during excessive overload situations

All text from TS 33.117 [4], clause 4.2.3.3.3 applies to GVNP of type 1.

5.2.5.5.3.3.4 System robustness against unexpected input

All text from TS 33.117 [4], clause 4.2.3.3.4 applies to GVNP of type 1.

5.2.5.5.3.3.5 Virtualised Network product software package integrity

5.2.5.5.3.3.5.0 Overview

All text from TS 33.117 [4], clause 4.2.3.3.5 applies to GVNP of type 1.

In addition, VNF package and VNF image integrity shall be validated when on board, and VNF image integrity shall be validated when in instantiated. The detailed potential security requirements and related test cases are as following.

5.2.5.5.3.3.5.1 VNF package and VNF image integrity

*Requirement Name*: VNF package and VNF image integrity

*Requirement Description*:

1) VNF package and image shall contain integrity validation value (e.g. MAC).

2) VNF package shall be integrity protected during on boarding and its integrity shall be validated by the NFVO.

*Threat Reference*: Clause 5.2.4.2.2.5.2 of the present document, "Software Tampering "; TR 33.848 [9], clause 5.18, "Key Issue 17: Software Catalogue Image Exposure"

*Test case*:

**Test Name:** TC\_VNF PACKAGE AND IMAGE­\_ INTEGRITY

**Purpose:**

1. To test whether the VNF package has been integrity protected or not.

2. To test whether the VNF image has been integrity protected or not.

**Procedure and execution steps:**

**Pre-Condition:**

- The virtualised network product document describes information regarding integrity protection of VNF package and VNF images, including details of how the integrity check is carried out, who makes the digital signatures of VNF package, what evidence is created to prove that the integrity check has been executed and what the result of the check is, etc.

- A valid VNF package and a not-valid VNF package (e.g. a tampered image in VNF package) are available.

- A valid VNF image (i.e. a correct HASH value is attached) and a not-valid VNF image (i.e. an incorrect HASH value is attached, e.g. the VNF image can be tampered when the VNF image is sent from the NFVO to the VIM or when the VNF image is stored in the image repository) are available in the image repository of VIM.

- There are NFVO and VIM, or simulated NFVO and VIM.

**Execution Steps**

Execute the following steps:

1. Review the documentation provided by the vendor describing how VNF package integrity is verified;

2. During VNF package on boarding, the tester uploads a valid VNF package into a NFVO. The NFVO verifies the integrity of the VNF package by validating the digital signature of the VNF package using the certificate of VNF vendor according to the documentation;

3. During VNF package on boarding, the tester uploads a not-valid VNF package into a NFVO. The NFVO validates the digital signature of the VNF package using the certificate of VNF vendor;

4. During VNF instantiation, the VIM selects a VNF image with a correct integrity protection value from the image repository to instantiate the VNF image.

5. During VNF instantiation, the VIM selects a VNF image with an incorrect integrity protection value from the image repository to instantiate the VNF image.

**Expected Results:**

1. The VNF package is successfully on boarded into the NFVO;

2. The not-valid VNF package is not on boarded;

3. The VNF image with a correct integrity protection value is instantiated by the VIM;

4. The VNF image with an incorrect integrity protection value is not instantiated by the VIM.

**Expected format of evidence:**

Snapshots containing the result of the VNF package on boarding and the VNF image instantiation.

5.2.5.5.3.4 Authentication and authorization

All text from TS 33.117 [4], clause 4.2.3.4 applies to virtualised network products.

5.2.5.5.3.5 Protecting sessions

All text from TS 33.117 [4], clause 4.2.3.5 applies to virtualised network products.

5.2.5.5.3.6 Logging

All text from TS 33.117 [4], clause 4.2.3.6 applies to virtualised network products.

##### 5.2.5.5.4 Operating systems

All text from TS 33.117 [4], clause 4.2.4 is generic and applies to guest operating systems for GVNP of type 1.

##### 5.2.5.5.5 Web servers

All text from TS 33.117 [4], clause 4.2.5 applies to GVNP of type 1.

##### 5.2.5.5.6 Network devices

All text from TS 33.117 [4], clause 4.2.6 applies to GVNP of type 1.

##### 5.2.5.5.7 Potential security functional requirements deriving from virtualisation and related test cases

5.2.5.5.7.1 Potential security functional requirements on GVNP lifecycle management

*Requirement Name*: GVNP lifecycle management security

*Requirement Description*:

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

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

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

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

Note: According to the definition in ETSI GR NFV 003, VNFM is responsible for the lifecycle management of VNF. The lifecycle management of VNF is set of functions required to manage the instantiation, maintenance and termination of VNF. The GVNP of type 1 is 3GPP VNF. A 3GPP VNF lifecycle management begins when the 3GPP VNF is instantiated by a VNFM after the 3GPP VNF package is delivered to the operator and uploaded to NFVO. It is different terminology with the product lifecycle management process in clause 6 that includes set of functions required to manage first commercial introduction, update, minor release, major release, end of life.

*Threat Reference*: Threats on interface between 3GPP VNF and VNFM, in clause 5.2.4.2.2.3

*Test case*:

**Test Name:** TC\_LIFECYCLE MANAGEMENT SECURITY

**Purpose:**

1. To test the VNF authenticates VNFM when VNFM initiates a communication to VNF.

2. To test the VNF establishes secure connection with the VNFM after successful authentication.

3. To test the VNF check whether VNFM has been authorized when VNFM access to VNF's API.

4. To check whether VNF logs the lifecycle management operations from VNFM.

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.

**Procedure and execution steps:**

**Pre-Condition:**

1. There is a VNFM (or simulated VNFM) in the test environment.

2. The VNF vendor's document describes how VNF authenticates/authorizes VNFM. Execution Steps

**Execute the following steps:**

1. The tester triggers the establishment of communication between the VNF and the VNFM.

2. The tester captures the communication between the VNF and the VNFM using a tool (e.g. wireshark).

3. The tester checks whether the VNF authenticates the VNFM or not according to the mechanism described in the vendor's document. For example, the VNF can use HTTPS to communicate with the VNFM, the VNF uses VNFM's certificate for authentication.

4. The tester checks whether the VNF establishes secure connection with the VNFM after successful authentication. For example, a TLS connection is established after the VNF successfully authenticates the VNFM.

5. The tester using the VNFM to access the VNF's API and checks whether the VNF authorizes the VNFM or not according to the mechanism described in the vendor's document. For example, VNF can use OAuth2.0 to authorize the VNFM. The VNF uses VNFM's token for authorization.

6. The tester checks whether the VNF logs the operations from VNFM or not.

**Expected Results:**

1. Secure communication is established between VNF and VNFM with integrity and confidentiality protection.

2. The VNFM successfully accesses the VNF's API.

3. The VNF logs the operations from VNFM.

**Expected format of evidence:**

1. Pcap traces contain the authentication and authorization processes.

2. Screenshot contains the logs.

5.2.5.5.7.2 Potential security functional requirements on executive environment provision

*Requirement Name*: secure executive environment provision

*Requirement Description*:

The VNF shall support to compare the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF can query the parsed resource state by the VNFM from the OAM. The VNF shall send an alarm to the OAM if the two resource states are inconsistent. This comparing process can be triggered periodically by the VNF, or the administrator can manually trigger the VNF to perform the comparing process.

Note: The virtualisation layer provides the execution environment for the VNF. The security of the virtualisation layer is a base of the VNF security. Whether VNFs are run on the trusted virtualisation layer or not is based on operator's decision.

*Threat Reference*: Threats on interface between 3GPP VNF and virtualisation layer, in clause 5.2.4.2.2.3.

*Test case*:

**Test Name:** TC\_SECURE EXECUTIVE ENVIRONMENT PROVISION

**Purpose:**

1. To test whether the VNF compares the owned resource state with the parsed resource state.

2. To test whether the VNF send an alarm to the OAM if the two resource states are inconsistent.

**Procedure and execution steps:**

**Pre-Condition:**

There are a VNF, a virtualisation layer (or simulated virtualisation layer), an OAM, a VNFM, a VIM (or simulated OAM, VNFM, VIM) on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester utilizes the virtualisation layer to change the resource state of VNF (e.g. change vCPU size of the VNF).

2. The tester uses the VNF to query the parsed resource state from the OAM.

3. The tester uses the OAM to query the parsed resource state of the VNF from the VNFM and send the received resource state to the VNF.

4. The tester checks whether the VNF sends an alarm to the OAM when the VNF receives the parsed resource state from the OAM and finds that the owned resource state and the parsed resource state are inconsistent.

**Expected Results:**

1. The VNF send an alarm to the OAM when the VNF receives the parsed resource state from the OAM and find that the owned resource state and the parsed resource state are inconsistent.

**Expected format of evidence:**

1. Screenshot contains the alarm on the OAM.

5.2.5.5.7.3 Instantiating VNF from trusted VNF image

*Requirement Name*: Instantiating VNF from trusted VNF image

*Requirement Description*:

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.

*Threat Reference*: TR 33.926 [3], Clause5.3.4.1, "Software Tampering "; TR 33.848, Clause5.18, "Key Issue 17: Software Catalogue Image Exposure"

*Test case*:

**Test Name:** TC\_INSTANTIATING VNF \_ TRUSTED IMAGE

**Purpose:**

To test whether the instantiating VNF from trusted VNF image.

**Procedure and execution steps:**

**Pre-Condition:**

- The virtualised network product document describes information regarding digital signature protection of VNF images, including details of how the signature check is carried out, who makes the digital signature of VNF image etc.

- One VNF package included two trusted VNF images and the VNF package carries a correct digital signature of the VNF package.

- Another VNF package included untrusted VNF image which carry wrong digital signature of VNF image and the VNF package carries a correct digital signature of the VNF package.

- There are a NFVO, or a simulated NFVO. A certificate which is used to verify the digital signature of VNF image has been configured in the NFVO. This certificate is provided by the vendor and it is issued by a CA trusted by the operator. It means the trusted VNF image is only digital signature of the VNF image is successfully verified by using the public key in the certificate issued by the CA trusted by the operator.

**Execution Steps:**

**Execute the following steps:**

1. Review the documentation provided by the vendor describing how digital signature of the VNF image is verified;

2. The tester uploads a VNF package included two trusted VNF images into a NFVO. The NFVO verifies the VNF images by validating each digital signature of the VNF image using the certificate of the VNF according to the documentation;

3. The tester uploads another VNF package included un-trusted VNF image into NFVO. The NFVO verifies the VNF image(s) by validating each digital signature of the VNF image using the certificate of the VNF according to the documentation.

Note: The digital signature validation of the image is also described in clause 5.2.5.5.3.3.5.1 VNF package and VNF image integrity, but the two test cases have the different test purposes. This test case focuses on VFN image credibility, while clause 5.2.5.5.3.3.5.1 is concerned with VNF image integrity.

**Expected Results:**

1. In the step 2, the signatures of the VNF images are successfully validated and the VNF package is successfully on boarded into the NFVO;

2. In the step 3, the signature of the un-trusted VNF image is failed to be validated and the VNF package is not on boarded into the NFVO;

**Expected format of evidence:**

Snapshots containing the result of the VNF package on boarding.

##### 5.2.5.5.8 Potential security requirements and related test cases to Hardening for GVNP of type 1

5.2.5.5.8.1 Introduction

The requirements proposed in the present clause aim to securing virtualised network products (including the network functions in service-based architecture) by reducing its surface of vulnerability. In particular the identified requirements aim to ensure that all the default virtualised network product configurations (including operating system software, firmware and applications) are appropriately set. The hardening requirements were proposed in TS 33.117 [4] are general and generally apply to GVNP of type 1. So, the potential hardening requirements for GVNP of type 1 also include four aspects, i.e. general hardening requirements (i.e. technical baseline), operating system, web server, network devices.

Compared to the physical network products, GVNP of type 1 has not hardware, but contains 3GPP functions, other functions and guest OS, it also has inter-VNF traffic and intra-VNF traffic in addition to than O&M traffic, control plane traffic and data plane traffic etc. The following clauses describe how to reduce the exposure from these new features.

5.2.5.5.8.2 Technical Baseline

5.2.5.5.8.2.1 No unnecessary or insecure services / protocols

All text from TS 33.117 [4], clause 4.3.2.1 applies to GVNP of type 1.

5.2.5.5.8.2.2 Restricted reachability of services

All text from TS 33.117 [4], clause 4.3.2.2 applies to GVNP of type 1.

5.2.5.5.8.2.3 No unused software

All text from TS 33.117 [4], clause 4.3.2.3 applies to GVNP of type 1.

5.2.5.5.8.2.4 No unused functions

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [4] clause 4.3.2.4 applies to GVNP of type 1, except the requirements and testing on hardware functions.

5.2.5.5.8.2.5 No unsupported components

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [4] clause 4.3.2.5 applies to GVNP of type 1, except the requirements and testing on hardware components.

5.2.5.5.8.2.6 Remote login restrictions for privileged users

All text from TS 33.117 [4], clause 4.3.2.6 applies to GVNP of type 1.

5.2.5.5.8.2.7 File system Authorization privileges

All text from TS 33.117 [4], clause 4.3.2.7 applies to GVNP of type 1.

5.2.5.5.8.3 Operating System

Guest OS provided by the vendors is generally based on Linux. All hardening requirements of OS in clause 4.3.3 of TS 33.117 [4] are general requirements and apply to GVNP of type 1.

5.2.5.5.8.4 Web Severs

All hardening requirements of Web Servers in clause 4.3.4 of TS 33.117 [4] are general requirements and the same for both the virtualised network product and the physical network product. So, all text from TS 33.117 [4], clause 4.3.4 applies to GVNP of type 1.

5.2.5.5.8.5 Virtualised Network Products

5.2.5.5.8.5.1 Traffic separation

All text from TS 33.117 [4], clause 4.3.5.1 applies to GVNP of type 1, except for the supporting physical separation of traffic belonging to different network domains. The detailed requirement and test case are as following.

*Requirement Name*: Traffic Separation

*Requirement Description*:

The virtualised 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. See RFC 3871 [x] for further information.

*Threat reference*: 5.2.4.2.2.7.15 Security threat caused by lack of GVNP traffic isolation.

*Test case*:

**Test Name:** TC\_TRAFFIC\_SEPARATION

Purpose:

To test whether traffic belonging to different network domains is separated.

Procedure and execution steps:

Pre-Condition:

NOTE: This test applies if the virtualised network product is meant to handle traffic from different network domains, e.g. both O&M and control plane traffic.

The virtualised network product has at least two separate logical interfaces dedicated to different network domains. Virtualised network products for which the test applies and that fail to meet this precondition fail the test by definition.

Execution Steps

Execute the following steps:

1. The tester checks whether the virtualised network product refuses traffic intended for one network domain on all interfaces meant for the other network domain, and vice versa.

2. Step 1 is to be performed for all pairs of different network domains.

Expected Results:

The two tests should be successful.

Expected format of evidence:

A PASS or FAIL.

5.2.5.5.8.5.2 Separation of inter-VNF and intra-VNF traffic

*Requirement Name*: inter-VNF and intra-VNF Traffic Separation

*Requirement Description*:

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 affect each other.

*Threat Reference: 5.2.4.2.2.7.15 Security threat caused by lack of GVNP traffic isolation*

*Test case*:

**Test Name:** TC\_TRAFFIC\_SEPARATION\_INTER-VNF\_INTRA-VNF

Purpose:

To test whether the traffics between inter-VNF traffic and intra-VNF traffic are separated.

Procedure and execution steps:

Pre-Condition:

1. There has a VNF instance on the test environment. This VNF instance has more than one VNFCI (VNF component Instance). The network between VNFCIs means intra-VNF network which is private network provided by vendor.

2. The document which describes how to separate the inter-VNF traffic with the intra-VNF traffic has been provided by the vendor. For example, the different network segments are described in the document.

3. Another VNF instance (or a simulated VNF instance) is on the test environment and can communicate with the tested VNF instance.

Execution Steps

Execute the following steps:

1. The tester checks whether the inter-VNF traffic and intra-VNF traffic are separated according the document by the vendor. For example, the tester checks whether the different network segments used by inter-VNF traffic and intra-VNF traffic respectively.

2. The tester checks whether a VNFCI refuses inter-VNF traffic on all intra-VNF interfaces. For example, the tester can send ping to all intra-VNF interfaces through an inter-VNF interface.

3. The tester checks whether a VNFCI refuses intra-VNF traffic on all inter-VNF interfaces. For example, the tester can send ping to all inter-VNF interfaces through an intra-VNF interface.

Expected Results:

In the step 1, the inter-VNF traffic and intra-VNF traffic are separated according the document by the vendor. In the step 2 and step 3, the VNFCI refuses traffic.

Expected format of evidence:

A PASS or FAIL.

#### 5.2.5.6 Potential security functional requirements and related test cases for GVNP of type 2

##### 5.2.5.6.1 Introduction

All texts from clause 5.2.5.5.1 can be basically applied to GVNP of type 2. The proposed security requirements for GVNP of type 2 are described in following clauses.

##### 5.2.5.6.2 Potential security functional requirements deriving from 3GPP specifications and related test cases

5.2.5.6.2.1 Security functional requirements deriving from 3GPP specifications – general approach

The clause 4.2.2.1 in TS 33.117 [4] also applies to security functional requirements deriving from 3GPP specifications and the corresponding test cases of GVNP type 2.

##### 5.2.5.6.3 Technical baseline

All texts from clause 5.2.5.5.3 apply to GVNP of type 2.

##### 5.2.5.6.4 Operating systems

All text from TS 33.117 [4], clause 4.2.4 also applies to guest operating systems and host operating systems for GVNP of type 2.

##### 5.2.5.6.5 Web servers

All text from TS 33.117 [4], clause 4.2.5 also applies to GVNP of type 2.

##### 5.2.5.6.6 Virtualised Network devices

All text from TS 33.117 [4], clause 4.2.6 also applies to GVNP of type 2.

##### 5.2.5.6.7 Potential security functional requirements deriving from virtualisation and related test cases

5.2.5.6.7.1 General

All texts in clause 5.2.5.5.7.1 apply to GVNP of type 2. In addition, GVNP of type 2 has the following security requirements related to virtualisation resource management, executive environment creation and VM escape which are derived from virtualisation and related test cases.

5.2.5.6.7.2 Potential security functional requirements on virtualisation resource management

*Requirement Name*: secure virtualisation resource management

*Requirement Description*:

1. To prevent a compromised VIM from changing the assigned virtualised 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, the VNF shall alert to the OAM when the VNF cannot detect a VNFC message.

2. A VNF shall log the access from the VIM.

Note: The VIM manages the virtualisation resource assignment and synchronization of virtualised resource state information. In the implementation, the VIM and the virtualisation layer are coupled and provided by one vendor, they trust each other. Whether the VIM is trust or not is based on operator's decision.

*Threat Reference:* TBA

*Test case*:

**Test Name:** TC\_SECURE VIRTUALISATION RESOURCE MANAGEMENT

**Purpose:**

1. To test whether the VNF alerts to the OAM when find the abnormal situation, e.g. a VNFCI is deleted by VIM.

2. VNF shall log the access from the VIM.

**Procedure and execution steps:**

**Pre-Condition:**

There are an OAM and a NFVO (or simulated OAM and NFVO) on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester logs to the VIM and deletes a VM of a VNF;

**Expected Results:**

1. The VNF alerts to the OAM. The alert from the VNF is found in the OAM.

2. The VNF logs the alert.

**Expected format of evidence:**

Screenshot contains the alert in the OAM and the alert in the log of the VNF.

5.2.5.6.7.3 Potential security functional requirements on executive environment creation

*Requirement Name*: secure executive environment creation

*Requirement Description*:

When an attacker tampers a driver which provided by the hardware and used to create the executive environment, the virtualisation layer shall alert the driver error to the administrator for checking the error and finding the attack at latter.

Note: Whether the hardware is trust or not is based on operator's decision to ensure the virtualisation layer and the VNF to be run on the trusted hardware.

*Test case*:

**Test Name:** TC\_SECURE EXECUTIVE ENVIRONMENT CREATION

**Purpose:**

To test the virtualisation layer alerts the driver error.

**Procedure and execution steps:**

**Pre-Condition:**

There are a virtualisation layer, a VIM (or simulated virtualisation layer, a VIM) and a host on the test environment.

**Execution Steps:**

**Execute the following steps:**

1. The tester tampers a driver on the server and implements the executive environment creation.

2. The tester checks whether the virtualisation layer alerts the driver error or not.

**Expected Results:**

The virtualisation layer alerts the driver error.

**Expected format of evidence:**

Screenshot contains the alert.

5.2.5.6.7.4 Potential security functional requirements on VM escape

*Requirement Name*: VM escape protection

*Requirement Description*:

To defence the attack that an attacker utilizes a vulnerability of a VNF to attack a virtualisation layer and then control the virtualisation layer, the virtualisation layer shall implement the following requirements:

The virtualisation 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.

*Test case*:

**Test Name:** TC\_VM ESCAPE PROTECTION

**Purpose:**

To test the virtualisation layer rejects the abnormal access from the VNF and logs the attacks from the VNF.

**Procedure and execution steps:**

**Pre-Condition:**

There are a virtualisation layer and a VNF on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester logs the VNF and makes an abnormal access (e.g. the VNF accesses the memory which is not allocated to the VNF) to the virtualisation layer.

2. The tester checks whether the virtualisation layer rejects the abnormal access from the VNF and logs the attacks.

**Expected Results:**

The virtualisation layer rejects the abnormal access from the VNF and logs the attacks.

**Expected format of evidence:**

Screenshot contains the log.

Note: The security requirements and related test cases in clause 5.2.5.6y.7.4 only considered in the decoupling scenario.

##### 5.2.5.6.8 Potential Security requirements and related test cases to Hardening for GVNP of type 2

5.2.5.6.8.1 Introduction

The purpose of hardening for GVNP of type 2 is also to reduce its surface of vulnerability. Based on the gap analysis between GVNP SECAM and GNP SECAM in clause 4, and the GVNP model of type 2 in clause 5.2.3, the GVNP of type 2 has the Virtualisation layer additional the GVNP of type 1. So, the security requirements and related test cases to hardening for GVNP of type 2 are based on the hardening requirements in TS 33.117 and the hardening requirements of GVNP for type 1.

NOTE: The only difference between for GVNP type1 and GVNP type2 in current report is about Operating System.

5.2.5.6.8.2 Technical Baseline

5.2.5.6.8.2.1 No unnecessary or insecure services / protocols

All text from TS 33.117 [4], clause 4.3.2.1 applies to GVNP of type 2.

5.2.5.6.8.2.2 Restricted reachability of services

All text from TS 33.117 [4], clause 4.3.2.2 applies to GVNP of type 2.

5.2.5.6.8.2.3 No unused software

All text from TS 33.117 [4], clause 4.3.2.3 applies to GVNP of type 2.

5.2.5.6.8.2.4 No unused functions

As GVNP of type 2 does not contain the hardware layer either, all text from clause 5.2.5.5.8.2.4 applies to GVNP of type 2.

5.2.5.6.8.2.5 No unsupported components

As GVNP of type 1 does not contain the hardware layer either, all text from clause 5.2.5.5.8.2.5 applies to GVNP of type 2.

5.2.5.6.8.2.6 Remote login restrictions for privileged users

All text from TS 33.117 [4], clause 4.3.2.6 applies to GVNP of type 2.

5.2.5.6.8.2.7 File system Authorization privileges

All text from TS 33.117 [4], clause 4.3.2.7 applies to GVNP of type 2.

5.2.5.6.8.3 Operating System

In addition to the Guest OS, the GVNP of type 2 may have host OS which is also provided by the vendor and generally based on Linux. So, all text from TS 33.117 [4], clause 4.3.3 applies to GVNP of type 2.

NOTE: Hardening requirements for Guest OS not based on Linux is not considered in the present document.

5.2.5.6.8.4 Web Severs

All text from TS 33.117 [4], clause 4.3.4 applies to GVNP of type 2

5.2.5.6.8.5 Virtualised Network Products

5.2.5.6.8.5.1 Traffic separation

All text from TS 33.117 [4], clause 4.3.5.1 applies to GVNP of type 2, except for the supporting physical separation of traffic belonging to different network domains.

5.2.5.6.8.5.2 Separation of inter-VNF and intra-VNF traffic

All text from clause 5.2.5.5.8.5.2 applies to GVNP of type 2.

#### 5.2.5.7 Potential security functional requirements and related test cases for GVNP of type 3

##### 5.2.5.7.1 Introduction

All texts from clause 5.2.5.5.1 can be basically applied to GVNP of type 3. The potential security functional requirements deriving virtualisation are detailed in clause 5.2.5.7.7.

##### 5.2.5.7.2 Potential security functional requirements deriving from 3GPP specifications and related test cases

5.2.5.7.2.1 Potential security functional requirements deriving from 3GPP specifications – general approach

The clause 4.2.2.1 in TS 33.117 [4] also applies to potential security functional requirements deriving from 3GPP specifications and the corresponding test cases of GVNP type 3.

##### 5.2.5.7.3 Technical baseline

All texts from clause 5.2.5.5.3 apply to GVNP of type 3.

##### 5.2.5.7.4 Operating systems

All text from TS 33.117 [4], clause 4.2.4 also applies to guest operating systems and host operating systems for GVNP of type 3.

##### 5.2.5.7.5 Web servers

All text from TS 33.117 [4], clause 4.2.5 also applies to GVNP of type 3.

##### 5.2.5.7.6 Network devices

All text from clause 5.2.5.5.7.3 also applies to GVNP of type 3.

##### 5.2.5.7.7 Potential security functional requirements deriving from virtualisation and related test cases

5.2.5.7.7.1 General

All texts in clause 5.2.5.6.7.1 apply to GVNP of type 3. In addition, GVNP of type 3 has the following security requirements related to hardware resource management, tampering hardware resource management information and trusted platform which are derived from virtualisation and related test cases.

5.2.5.7.7.2 Potential security functional requirements on hardware resource management

*Requirement Name*: secure hardware resource management

*Requirement Description*:

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.

*Threat Reference:* Threats on interface between hardware and Virtualised Infrastructure Manager (VIM) in clause 5.2.4.4.2.3, Denial of Service in clause 5.2.4.4.2.8

*Test case*:

**Test Name:** TC\_SECURE HARDWARE RESOURCE MANAGEMENT

**Purpose:**

To test the hardware alerts the error of the hardware resource configuration from the VIM.

**Procedure and execution steps:**

**Pre-Condition:**

There is a VIM (or simulated VIM), GVNP of type 3 on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester utilizes the VIM to make an error hardware resource configuration (e.g. error firmware upgrade).

2. The tester checks whether an alert is triggered or not.

**Expected Results:**

The hardware triggers an alert.

**Expected format of evidence:**

Screenshot contains the alert.

5.2.5.7.7.3 Potential security functional requirements on tampering hardware resource management information

*Requirement Name*: secure hardware resource management information

*Requirement Description*:

When a compromised Virtualisation 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: Whether the virtualisation layer is trust or not is based on operator's decision.

*Threat Reference:* Threats on interface between hardware and Virtualised Infrastructure Manager (VIM) in clause 5.2.4.4.2.3

*Test case*:

**Test Name:** TC\_SECURE HARDWARE RESOURCE MANAGEMENT INFORMATION

**Purpose:**

To test the hardware alerts the error of the hardware resource configuration.

**Procedure and execution steps:**

**Pre-Condition:**

There are a virtualisation layer (or simulated virtualisation layer) and a host, a VIM on the test environment.

**Execution Steps:**

**Execute the following steps:**

1. The tester tampers a received hardware resource configuration that the virtualisation layer received from the VIM.

2. The tester checks whether the hardware alerts when the tampered hardware resource configuration is implemented.

**Expected Results:**

The hardware alerts the error of the hardware resource configuration.

**Expected format of evidence:**

Screenshot contains the alert.

Note: The security requirement and related test cases in clause 5.2.5.7.7.3 is only considered in the decoupling scenario.

5.2.5.7.7.4 Potential security functional requirements on trusted platform

*Requirement Name*: trusted platform

*Requirement Description*:

The host system shall implement a Hardware-Based Root of Trust (HBRT) ((e.g. TPM, HSM)) as Initial Root of Trust [16]. The trust state of the platform shall be measured and a trusted chain shall be built [8].

*Test case*:

**Test Name:** TC\_TRUSTED PLATFORM

**Purpose:**

To test the platform is trusted.

**Procedure and execution steps:**

**Pre-Condition:**

There are a host which has been installed HBRT on the hardware and related software (e.g. host OS, Guest OS etc.).

**Execution Steps**

**Execute the following steps:**

1. The tester tampers a BIOS or a file in the host OS kernel and restart the host.

2. The tester checks whether the measurement is implemented or not.

**Expected Results:**

The measurement is implemented, the restart process is interrupted.

**Expected format of evidence:**

Measurement report or screenshot contains process stop.

##### 5.2.5.7.8 Security requirements and related test cases to Hardening for GVNP of type 3

5.2.5.7.8.1 Introduction

Based on the gap analysis between GVNP SECAM and GNP SECAM in clause 4, and the GVNP model of type 3 in clause 5.2.3, GVNP of type 3 include VNF, virtualisation and hardware, the general hardening requirements both for software and hardware in TS 33.117 apply to the GVNP of type3.

5.2.5.7.8.2 Technical Baseline

The GVNP of type 3 includes hardware and software. All the general hardening requirements from TS 33.117 [x], clause 4.3.2 applies to GVNP of type 3.

5.2.5.7.8.3 Operating System

Like GVNP of type 2, GVNP of type 3 contains Guest OS and may contain Host OS, both of which are provided by the vendor and generally based on Linux®. So, all text from TS 33.117 [4], clause 4.3.3 applies to GVNP of type 3.

NOTE: Hardening requirements for Guest OS not based on Linux is not considered in the present document.

5.2.5.7.8.4 Web Severs

All text from TS 33.117 [4], clause 4.3.4 applies to GVNP of type 3.

5.2.5.7.8.5 Network Devices

5.2.5.7.8.5.1 Traffic separation

All text from TS 33.117 [4], clause 4.3.5.1 applies to GVNP of type 3.

5.2.5.7.8.5.2 Separation of inter-VNF and intra-VNF traffic

All text from clause 5.2.5.5.8.5.2 applies to GVNP of type 3.

## 5.3 Improvement of SCAS and new potential security requirements

Vendors, operators or other bodies can propose new potential security requirements for addition to 3GPP SCASs for GVNPs if a new threat or vulnerability has been identified. This gives 3GPP the flexibility to continuously review and improve their SCASs for GVNPs.

## 5.4 Basic vulnerability testing requirements for GVNP

### 5.4.1 Introduction

The basic vulnerability testing activities such as Port Scanning, Vulnerability Scanner by the use of vulnerability scanners are the generic mechanisms to detect the exposures and vulnerabilities of both for the physical network products and the virtualised network products. Currently, the security testing tools already support vulnerability and port scanning for the virtualised network products. So, the requirements of port scanning and vulnerability scanning in clause 4.4 of the TS 33.117 [4] apply to GVNP.

The target of robustness and fuzz testing are the protocol stacks (e.g. http stack) rather than the applications. The protocol stacks supported by the NF are the same for both of virtualised and physical network products. So, all text from TS 33.117 [4], clause 4.4 applied to all types of GVNPs.

Such general requirement should be applied to fit different kinds of implementations. For example, for GVNP of type 1, as it contains VNF, BVT is applied. For GVNP of type 2, BVT can be applied for its VNF part. If its Virtualisation layer part has host OS, BVT is also applied for its Virtualisation part. For GVNP of type 3, BVT can be applied for its VNF part, Virtualisation layer part if host OS is existing, and hardware part if SNMP or similar protocol exists. All these are based on detailed implementation of specific GVNP.

### 5.4.2 Port Scanning

All text from TS 33.117 [4], clause 4.4.2 applied to all types of GVNPs.

### 5.4.3 Vulnerability Scanning

All text from TS 33.117 [4], clause 4.4.3 applied to all types of GVNPs.

### 5.4.4 Robustness and Fuzz testing

All text from TS 33.117 [4], clause 4.4.4 applied to all types of GVNPs.

# 6 Vendor development and product lifecycle processes and test laboratory accreditation

## 6.1 Overview

According to the description from clause 4.4, there is no gap between the scopes of SECAM accreditation for both physical network products and the virtualised network products. GSMA F.14, F.15 and F.16 [18], [19] and [20] described test laboratory accreditation, vendor development and product lifecycle processes and security requirements respectively. These are generic accreditation and processes. So, the processes of vendor development and product lifecycle processes and test laboratory accreditation in clause 6 of TR 33.916 [2], which provide the overview of the processes and accreditation in GSMA NESAG are apply to the virtualised network products as well.

NOTE 1: The product development and lifecycle processes as well as test laboratory accreditation procedure described in the present document needs to be revisited once GSMA SECAG publishes new methodology specifications on NESAS.

NOTE 2 : GSMA SECAG is ultimately responsible for defining the entire vendor development, product lifecycle processes, and test laboratory accreditation, including dispute resolution process. Therefore, it is the responsibility of GSMA SECAG to confirm if the current process defined in GMSA is sufficient to cover virtualised network products.

## 6.2 Audit and accreditation of Vendor network product development and network product lifecycle management processes

Vendor network product development and network product lifecycle management processes assurance requirements as well as related evaluation activities are generic in clause of TS 33.117[4], and apply to both physical network product classes and virtualised network products classes. All text from TS 33.117 [4], clause 6.2 applied to all types of GVNPs.

NOTE: According to the gap analysis in clause 4.4, who takes the role of the SECAM Accreditation Body for all types of the GVNPs, which defines end or network product development and network product lifecycle management processes assurance requirements as well as related evaluation activities, needs to be confirmed by GSMA.

## 6.3 Audit and accreditation of test laboratories

The process for audit and accreditation of test laboratories in clause 6.2 of TR 33.916[2] are generic and apply to all types of GVNPs.

## 6.4 Monitoring

All text from TR 33.916 [2], clause 6.4 applied to all types of GVNPs.

Note: To assure the GVNP security during testing process and after deployment, the hardware for GVNP for type 2, or NFVI for GVNP for type 1, which is not provided by the vendor who implements the 3GPP virtual network functions, can be assumed to comply with the monitor process in clause 6.4 of TR 33.916 [2].

## 6.5 Dispute resolution

All text from TR 33.916 [2], clause 6.5 applied to all types of GVNPs.

Note: To assure the GVNP security during testing process and after deployment, the hardware for GVNP for type 2, or NFVI for GVNP for type 1, which is not provided by the vendor who implements the 3GPP virtual network functions, can be assumed to comply with the dispute resolution process in clause 6.5 of TR 33.916 [2].

# 7 Evaluation and SCAS instantiation

## 7.1 Security Assurance Specification (SCAS) instantiation documents creation

According to gap analysis in clause 4.3, the scope of SECAM evaluation for 3GPP physical network products applies to SECAM evaluation of 3GPP virtualised network products. The SCAS instantiation of the virtualised network product also consists of a set of documents provided by the vendor to give test laboratories and operators the relevant information to understand the critical parts of the network product to be evaluated.

The content of the SCAS instantiation of the GVNP is defined and it contains details on:

- Virtualised Network Product description (e.g. software version, documentation version).

- Scope of evaluation.

- Mapping of SCAS security requirements to the virtualised network product and assets in the virtualised network product.

- References to the applicable document versions containing operational guidance in the documentation of the virtualised network product.

- Information needed to start the Security Compliance Testing, including Basic Vulnerability Testing. For GVNPs of type 1, the requirements for a NFVI supporting environment (See clause 5.9 of TR 33.848 [9]) should be included in the information. For GVNP's of type 2, the requirements of a hardware supporting environment should be included in the information.

- Details of licenses that are required for the product to operate in the scope of evaluation (if relevant).

The above document set is updated by the vendor until the testers (Security Compliance Testing, Basic Vulnerability Testing) consider they have enough and correct information to execute the required tests. Details on the content of these documents and of the update process are provided in clause 7.2.2.

## 7.2 Evaluation and evaluation report

### 7.2.1 Network product development process and network product lifecycle management

According to the descriptions in clause 4.3.2 and clause 4.5.2, the tasks and ultimate output of the GVNP evaluation is same with the physical network product evaluation. So, all text from TR 33.916, clause 7.2 basically applies to the GVNP. The following clauses will focus on the difference from clause 7.2 in TR 33.916.

### 7.2.2 SCAS instantiation evaluation

#### 7.2.2.1 Overview

Like the physical network product, SCAS instantiation evaluation of the virtualised network product is to check whether a SCAS instantiation written by a vendor is a correct instantiation of the SCAS of the network product class and whether it is a good basis for evaluating the network product.

The accredited evaluator (vendor or third-party evaluator) for security compliance testing is responsible for SCAS instantiation evaluation before it is used to evaluate virtualised network product. The evaluator confirms at least that the SCAS being instantiated for a given 3GPP virtualised network product and the virtualised network product for evaluation are consistent. According to the clause 4.3, 4.5 and 4.6, the content and the process of SECAM evaluation from TR 33.916 [2] apply to GVNP.

#### 7.2.2.2 Content

The content of the evaluation from TR 33.916 [2], in clause 7.2.2.2 applies to virtualised network products,.

#### 7.2.2.3 Process

The process from TR 33.916 [2], in clause 7.2.2.3 applies to virtualised network products. The difference is that there may be more than one vendor involved in the decoupling scenario.

### 7.2.3 Security Compliance testing

The security compliance testing in clause 7.2.3 of TR 33.916 [2] is a generic process, the inputs, outputs and activities from TR 33.916 [2], in clause 7.2.3 apply to virtualised network products. In addition, the accredited test laboratory should prepare supporting environment based on virtualised product assumption, e.g. hardware for GVNP for type 2, or NFVI for GVNP for type 1.

### 7.2.4 Basic Vulnerability Testing

According to the analyses of basic vulnerability testing requirements for GVNP, all text from TS 33.117 [4], clause 4.4 applied to all types of GVNPs. The process of BVT from TR 33.916 [2], in clause 7.2.3 is generic and applies to the virtualised network products. In addition, the test tools of BVT should support to detect the vulnerabilities in GVNP.

## 7.3 Self-declaration

All text from TR 33.916 [2], in clause 7.3 is generic and applies to the virtualised network products.

## 7.4 Partial compliance and use of SECAM requirements in network product development cycle

All text from TR 33.916 [2], in clause 7.4 is generic and applies to the virtualised network products.

## 7.5 Comparison between two SECAM evaluations

All text from TR 33.916 [2], in clause 7.5 applies to the virtualised network product.

## 7.6 The evaluation of a new version

All text from TR 33.916 [2], in clause 7.6 applies to virtualised network products.

# 8 Conclusion

## 8.1 Way forward of SECAM/SCAS for 3GPP virtualised network products

In order to ensure the security of the massive deployed virtualised 5GC network products, SECAM and SCAS for such GVNP should be considered.

It is concluded that there is no significant gap between GNP and GVNP in terms of SECAM/SCAS as identified in clause 4. However there are still some security threats and requirements specific to generic virtualised network products identified in the present document, which can serve as the basis for the SECAM and SCAS of specific virtualised network products. To continue the work, the following way forward is proposed:

- for methodology part, it is proposed to capture the methodology specific to GVNP in a new 9-series document (to pair with TR 33.916 [2]).

- for critical assets and threats: it is proposed to capture the threats and critical assets as described in clauses 5.2.3.2 and 5.2.4.2 for type 1, clauses 5.2.3.3 and 5.2.4.3 for type 2, clauses 5.2.3.4 and 5.2.4.4 for type 3 specific to virtualised network product class in a new 9-series document (to pair with TR 33.926 [3]).

- for security requirements and test cases, it is proposed to capture the requirements and corresponding test cases for GVNP as described in clause 5.2.5.5 for type 1, clause 5.2.5.6 for type 2, clause 5.2.5.7 for type 3 and clause 5.4 for general BVT test in a new document (to pair with TS 33.117 [4]).

NOTE 1: Regarding GVNP type 2, the security requirements and test cases on the interface between virtualisation layer and hardware layer, the interface between 3GPP defined functionalities and VNFM, the interface between virtualisation layer and VIM are considered. Regarding GVNP type 3, only the interface between 3GPP defined functionalities and VNFM, the interface between NFVI and VIM are considered in this present document.

NOTE 2: When run the test to GVNP type 1 and GVNP type 2, and when a test case cannot be passed, the NFVI for GVNP for type 1, or hardware for GVNP for type 2 maybe involved to find out why the test case cannot be passed. This is because the NFVI for GVNP for type 1, or hardware for GVNP for both type 1 and type 2 may not go through any security assurance testing in the same rigorous manner that is similarly applied to the security assurance testing of GVNP type 1 and GVNP type 2. 3GPP assumes the NFVI for GVNP for type 1, or hardware for GVNP for both type 1 and type 2 can demonstrate secure enough to meet the security requirement specified or will be specified in TS 33.117 [4] or other related SDO, e.g. ETSI NFV, as well as the security requirements identified is in the present document.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-06 | SA#92e | SP-210432 |  |  |  | Presented for information and approval | 1.0.0 |
| 2021-06 | SA#92e |  |  |  |  | EditHelp review and upgrade to change control version | 17.0.0 |
| 2021-09 | SA#93e | SP-210846 | 0001 | - | F | Clean up the editorial issues | 17.1.0 |