|  |
| --- |
| 3GPP TR 33.927 V0.2.0 (2022-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Service and System Aspects;Security Assurance Specification (SCAS) ;threats and critical assets ;in 3GPP virtualized network product classes;(Release 18) |
|   |
|  | 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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.© 2022, 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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Generic Virtualized Network Product (GVNP) class description 7

4.1 Overview 7

4.2 Minimum set of functions defining the GNP class 7

4.3 Generic network product model 7

5 Generic assets and threats 7

5.1 Introduction 7

5.2 Critical assets 7

5.3 Threats 7

6 Generic assets and threats for network functions supporting SBA interfaces 7

# Foreword

This clause is mandatory; do not alter the text in any way other than to choose between "Specification" and "Report".

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 drafting the TS/TR, pay particular attention to the use of modal auxiliary verbs! TRs shall not contain any normative provisions.

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.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The present document captures the virtualized network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The present document contains generic aspects that are believed to apply to more than one network product class. In another aspect, present document defines different types of virtualized network products compared to only one type defined in [2].

# 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 33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

[3] 3GPP TR 33.936: "Security Assurance Methodology (SECAM) for 3GPP virtualized network products".

[4] 3GPP TR 23.501: " System architecture for the 5G System (5GS) Stage 2".

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

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

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or abbreviations.

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP TR 21.905 [1].

Definition format (Normal)

**<defined term>:** <definition>.

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

GVNP Generic Virtualized Network Product

NFVI Network Functions Virtualization Infrastructure

VM Virtual Machine

SCAS Security Assurance Specification

OAM Operation and Management

NFVO Network Functions Virtualization Orchestrator

VIM Virtualized Infrastructure Manager

VNFM Virtualized Network Function Manager

EM Element Management

NFV Network Functions Virtualization

# 4 Generic Virtualized Network Product (GVNP) class description

Editor’s Note: The structure of sub-clause follows the structure of TR33.926

## 4.1 Overview

A 3GPP generic virtualized network product class defines a set of functions that are implemented on that product, which includes, but not limited to minimum set of common 3GPP functions for that product covered in 3GPP specifications, other functions and softwares not covered by 3GPP specifications, as well as interfaces to access that product. A generic type 1 of virtualized network product may also include software, and OS components that the product is implemented on. The current document describes the threats and the critical assets in the course of developing 3GPP security assurance specifications for a particular network product class.

NOTE: Considering the situation that type 2 and/or type 3 of virtualized product class are dependent of pre-mature specifications from other standard organization, only type 1 of virtualized product class are specified in present document.

**Applicability of the GVNP security assurance specification to products:** Assume a telecom equipment vendor wants to sell a product to an operator, and the latter is interested in following the Security Assurance Methodology as described in TR 33.936[3], then, before evaluation according to TR 33.936[3] in a testing laboratory can start, it first needs to be determined which security assurance specifications written by 3GPP apply to the given product.

Different with 3GPP GNP defined in TR33.926[2], based on different implementation, 3GPP VNP will be categorized as 3 types. As a result, a type 1 of 3GPP Virtualized Network Product may be composed with software (e.g. operating system, drivers, applications, services, protocols), and interfaces (e.g. console interfaces and O&M interfaces) that allow the 3GPP network product to be managed and configured locally and/or remotely. A GVNP is a 3GPP network product.

**GVNP Security Assurance Specification (GVNP SCAS):** The GVNP SCAS provides descriptions of the security requirements (which are including test cases) pertaining to type 1 of generic virtualized network product class.

**Need for a GVNP network product model:** This minimum set of functions listed in clause 4.2 is exclusively meant as a membership criterion for the GVNP Class. It is not meant to restrict the functionality of a GVNP, nor the scope of the present document in any way. On the contrary, it is clear that GVNPs will contain many more functions than those from the minimum set listed in clause 4.2, and the GVNP will contain requirements relating to functions not contained in this minimum set. Some of these functions, beyond the minimum set, can be found from various 3GPP specifications, but by far not all these functions. This implies that there is a need to describe the functions that cannot be found from 3GPP specifications in some other way before the GVNP can be written so that the GVNPs can make reference to this description. This description is the GVNP model, cf. clause 4.3.

EXAMPLE 1: 3GPP specifications do not describe a local management interface, but GVNPs will have to take it into account, so a local management interface needs to be part of a GVNP model.

EXAMPLE 2: A GVNP sometimes says e.g.: "Authentication events on the local management interface shall be logged." This implies the presence of a logging function. The logging function is not part of the defining minimum set of functions from clause 4.2. If a product implements this minimum set, but no logging function, then this just means that the product is a GVNP, but will fail the evaluation against the GVNP SCAS.

The GVNP models are further used in clauses 5 and 6 in various ways, e.g. the critical assets can point to parts of the GVNP model, threats and requirements can refer to interfaces shown in the GVNP model, etc.

## 4.2 Minimum set of functions defining the GNP class

According to TR 33.936 [3], a virtualized network product class is a class of products that all implement a common set of 3GPP-defined functionalities. This common set is defined to be the list of functions contained in pertinent 3GPP specifications, such as clause 5 of 3GPP TS 23.501 [4].

4.3 Generic virtualized network product model

4.3.1 Introduction

A virtualized network product class is the class of products that implement 3GPP defined network functionalities running on Network Function Virtualization Infrastructure (NFVI). The realistic deployment scenarios are summarized in ETSI NFV-SEC 001 [x], 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 Virtualization 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 Virtualization layer and the hardware layer from its vendors.

NOTE: In order to implement virtualized product, some essential components besides 3GPP defined functions are also needed.

As a result, it defines type 1 of GVNP which is implement 3GPP defined functionalities only

NOTE: Considering the situation that type 2 and/or type 3 of virtualized product class are dependent of pre-mature specifications from other standard organization, only type 1 of virtualized product class are specified in present document.

****

**Figure 4.3-1:** **Type 1 of virtualised network product class**

The rest part of device could be seen as a supporting environment and is not considered in scope of those types.

NOTE: For the purpose of testing a 3GPP GVNP of type 1, NFVI for GVNP for type 1 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.

The generic virtualized network product model classes are described in the following clauses.

4.3.2 Generic virtualized network product model of type 1

4.3.2.1 Description of the GVNP model

For the virtualized network product class type 1 (i.e. implementing 3GPP defined functionalities only), the following figure 4.3-2 depicts the components of a generic virtualized network product model at a high level.

****

**Figure 4.3-2: GVNP model of type 1**

The components in the figure 4.3-2 are further described in the following clauses.

4.3.2.2 Functions defined by 3GPP

For a generic virtualized network function, it will implement 3GPP-defined functions. Unlike a generic physical network product defined in [2], 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.

4.3.2.3 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.

4.3.2.4 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.

4.3.2.5 Interfaces

Compared to generic physical network product defined in [2], 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 Virtualized 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 4.3-3)

- EMS (Element Management System) interface

- Interface defined by ETSI NFV specifications [5] and [6]:

- Interface between VNF and VNFM 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 4.3-3.

- 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 Virtualization layer for execution environment provision. This interface refers to Vn-Nf in the figure 4.3-3.

****

**Figure 4.3-3: NFV reference architectural framework**

# 5 Generic assets and threats

Editor’s Note: This clause will describe Generic assets and threats for virtualized network product. The structure of sub-clause follows the structure of TR33.926.

## 5.1 Introduction

## 5.2 Critical assets

Editor’s Note: This clause will describe critical assets for each kind of GVNP.

## 5.3 Threats

Editor’s Note: This clause will describe threats for each kind of GVNP.

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

Editor’s Note: Although there is no difference between virtualized network product and physical network product in SBA aspect, it is also specified in present document for integrity coverage on assets and threats.

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA3-106e |  |  |  |  | Create draft version on skeleton and scope | 0.1.0 |