ETSI TR 133 936 V18.0.1 (2024-05)

5G;
Security Assurance Methodology (SECAM)
for 3GPP virtualized network products
(3GPP TR 33.936 version 18.0.1 Release 18)

Reference
DTR/TSGS-0333936vi01

Keywords
5G,SECURITY

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

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

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

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 defines the complete Security Assurance Methodology (SECAM) evaluation process (evaluation, relation to SECAM Accreditation Body, roles, etc.) as well as the components of SECAM that are intended to provide the expected security assurance for virtualized network product. It will thus describe the general scheme providing an overview of the entire scheme and explaining how to create and apply the Security Assurance Specifications (SCASs). It will detail the different evaluation tasks (vendor network product development and network product lifecycle management process assessment, Security Compliance Testing, Basic Vulnerability Testing and Enhanced Vulnerability Analysis) and the different actors involved. Enhanced Vulnerability Analysis is outside the scope of the present release of SECAM. The present document will help all involved parties to have a clear understanding of the overall process and the covered threats.

In another aspect, compared to [2], present document shows specific methodology to virtualized network product in addition.

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 TS 28.500: "Management concept, architecture and requirements for mobile networks that include virtualised network functions".

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

[5] 3GPP TR 33.927: "Security Assurance Specification (SCAS); threats and critical assets; in 3GPP virtualized network product classes".

[6] 3GPP TS 33.527: "Security Assurance Specification (SCAS); for 3GPP virtualized network products".

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

[8] Void

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

[10] GSMA FS.15: "Network Equipment Security Assurance Scheme - Development and Lifecycle Assessment Methodology v.2.2".

[11] GSMA FS.46: "NESAS Audit Guidelines v.2.0".

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

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].

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].

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 virtualized network products, the platform and the 3GPP defined functionalities are decoupled. The platform of virtualized network products composes of a hardware layer and a Virtualization layer, and is common for 3GPP defined functionalities. Concept of 3GPP VNF is defined in TS 28.500 [3]. According to the concept in [3], a 3GPP VNF is 3GPP network function(s) that runs on a Network Function Virtualization Infrastructure (NFVI), which is the platform of virtualized network products described above.

The realistic deployment scenarios are summarized in ETSI NFV-SEC 001 [4], 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.

Each deployment mode requires the different composition of virtualized 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 virtualized network products maps to three types of virtualized network product class as depicted in Figure 1:

- Type 1: implement 3GPP defined functionalities only
- Type 2: implement 3GPP defined functionalities and Virtualization layer
- Type 3: implement 3GPP defined functionalities, Virtualization layer, and hardware layer

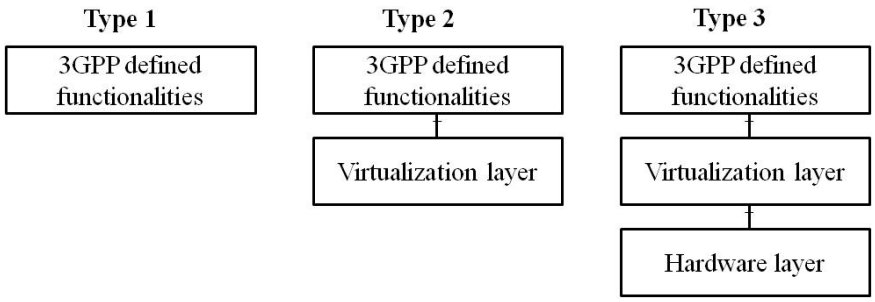

Figure 4.1.1-1: Three types of virtualized network product class

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.

4.1.2 Considerations on SECAM of the virtualized network products

The security assurance methodology study in TR 33.916 [2] is a general methodology and already considers virtualized network products in the design of the methodology. The biggest difference between virtualized 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 virtualized network products as defined in clause 4.1.1.

Editor's note: The text maybe revisited after update of TR33.916[2].

4.2 Scope of a SECAM SCAS for 3GPP virtualized network products

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. 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 virtualized network product classes will be described in TR 33.927 [5] and TS 33.527 [6] respectively.

The Security Assurance Specification (SCAS) for a given 3GPP virtualized network product class provides a description of the security requirements and associated test cases. The SCAS for a given 3GPP virtualized network product class 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.

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 virtualized network products will be validated during product deployment and it is not part of SECAM.

4.3 Scope of SECAM evaluation for 3GPP virtualized 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 apply to a type 1 virtualized network product.

4.4 Scope of SECAM Accreditation for 3GPP virtualized network products

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 is applicable to all of the network products, regardless of whether the network product is physical network product or virtualized network product. It means, like for physical network products, the actors who perform the SECAM tasks for type 1 of 3GPP virtualized 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 virtualized 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
Virtualized network product evaluation which includes Security compliance testing and Basic Vulnerability Testing	Accredited vendor or accredited third-party test laboratory

Consequently, according to table 4.4-1, SECAM can take different forms, depending on who performs security compliance testing and who performs Basic Vulnerability Testing.

SECAM is intended to enable self-evaluation where the vendors evaluate their network products if they have the proper accreditation for that.

The responsibility for writing and managing the accreditation and monitoring rules is taken by a SECAM Accreditation Body. The SECAM Accreditation Body's role also includes the handling of the dispute resolution process.

The decision on who takes the role of SECAM Accreditation Body should be made in cooperation with other SDOs such as GSMA, etc. It is recommended to leave accreditation responsibility to GSMA.

Even if it describes the complete process, including evaluation by accredited actors under SECAM Accreditation Body control and Security Assurance Specifications (SCAS) writing, SECAM does not preclude 3GPP SCAS security requirements and tests cases being used directly by mutual consent between vendors and operators without the accreditation process in place if it so desires. This ensures that the 3GPP SECAM work is not held up by delays in deliverables under the responsibility of external bodies, or by conflicting requirements in different countries (e.g. relating to accreditation).

The presence of a SECAM Accreditation Body as defined above is highly desirable in order to ensure a wide recognition of evaluation results and to have a working dispute resolution process available. Having a SECAM Accreditation Body also avoids the need for each operator to set up a one to one trust relationship with every vendor regarding their testing methods and skills.

Validity of accreditation is defined by the SECAM Accreditation Body.

4.5 Ultimate Output of SECAM Evaluation for 3GPP virtualized network products

The ultimate output of the SECAM evaluation for type 1 of 3GPP virtualized 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 type 1 of virtualized 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 virtualized network products evaluation process

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 applies to 3GPP virtualized network products.

The security assurance process of type 1 of virtualized network products describes how the operator gets assurance regarding the security of the virtualized network product.

4.7 Roles in SECAM for 3GPP virtualized network products

The roles involved in SECAM evaluation and accreditation described in TR 33.916 [2] also apply to type 1 of 3GPP virtualized network products, i.e. vendor, test laboratory, operator, 3GPP and SECAM Accreditation Body. The clause 4.6.1 of TR 33.916 [2] also applies to GVNP.

This example below of complete self-evaluation is similar to the SECAM defined Security assurance process in the figure 4.7-1 except that the vendor conducts all the phases of evaluation.

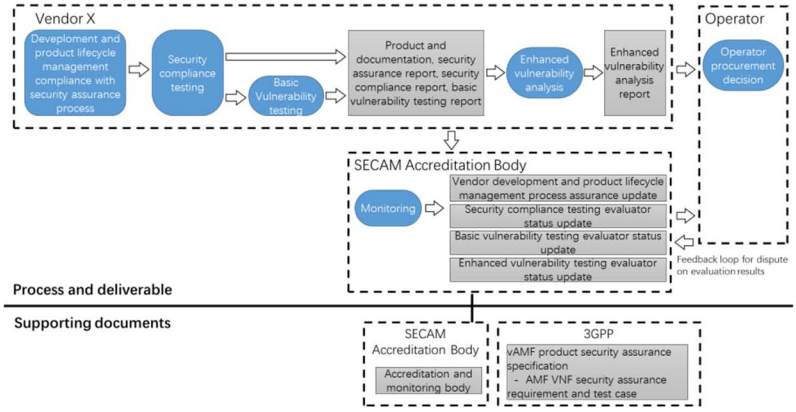

Figure 4.7-1: Complete self-evaluation of a 3GPP virtualized network product (e.g. vAMF (AMF VNF) from vendor X)

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 virtualized network products

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. In addition, operator security acceptance decision in clause 4.7 of TR 33.916 [2] is general process. So, operator security acceptance decision for type 1 of 3GPP virtualized 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 virtualized network products

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 applicable to all of the network products, regardless of whether the network product is physical network product or virtualized 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 virtualized network products also considers only one assurance level for type 1 of virtualized network product class.

4.10 Security baseline for 3GPP virtualized network products

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 virtualized network product. So, SECAM considers only one security baseline for type 1 of virtualized 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 Introduction

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 apply to the process of writing SCAS documents for a given virtualized network product class. According to the description of 3GPP virtualized network product class in clause 4.1, there are three types of the virtualized network product classes, when describing and modelling a given virtualized network product class, the type of the given virtualized network product class should be considered.

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.

5.2 SCAS documents structure and content

5.2.1 General

According to clause 5.1, the SCAS documents contain three parts, i.e. Virtualized 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 virtualized network products contain the following parts:

- ***Network Product Class Description for Virtualized network products (NPCDV):*** This clause includes the description of the virtualized network product class defined in clause 4.1.x, 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 virtualized 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 virtualized network product class, as well as the security requirements of Virtualization aspect defined in 3GPP and other standard organization like ETSI NFV, etc. Requirements and test cases will be contained in one or more 3GPP Technical Specifications.

In the following clauses, detailed descriptions of SCAS parts SPD and SR for virtualized network products are provided.

5.2.2 Security Problem Definition (SPD)

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 virtualized network products.

5.2.3 Security Requirements

5.2.3.1 Introduction

According to the scope of a SECAM SCAS in clause 4.2, 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 or may need to implement hardware (See clause 4.9 in TR 33.916 [2]) with special security requirement that make it difficult. 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 5.2.3.1-1).

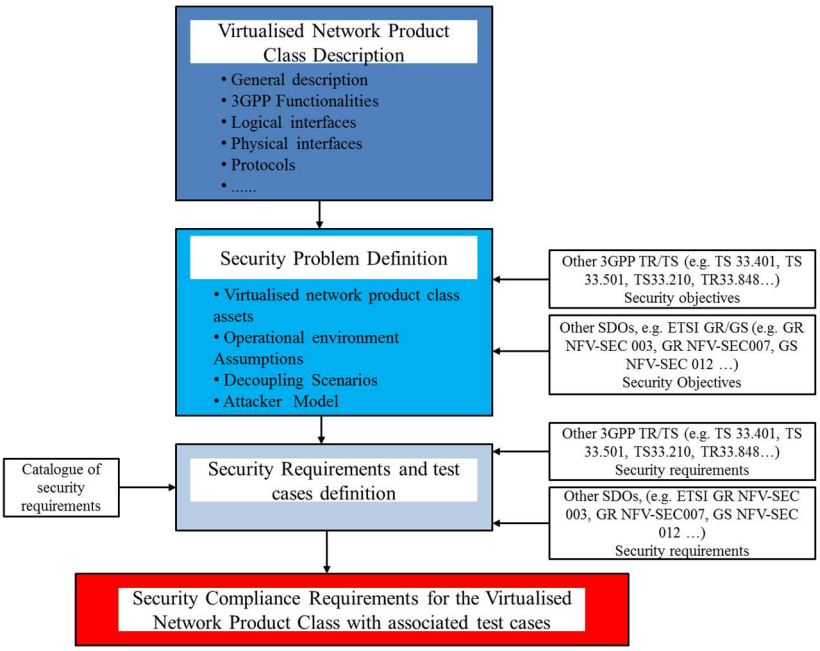

Figure 5.2.3.1-1: Process for deriving security requirements in a SCAS document

The security requirements include security functional requirements and hardening requirements. 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.

5.2.3.2 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 virtualization layer, hardware and resource isolation, among others, which may be identified in ETSI specifications etc..

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

5.2.3.3 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 virtualized network product class.

Since SECAM and SCAS of physical network product class are bases for SECAM and SCAS of virtualized network product class, the security requirements of a virtualized 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 virtualized network product also uses the template in current SECAM which is described in TR 33.916 [2].

5.2.3.4 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 virtualized 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.

5.3 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 generic virtualized network product

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 virtualized network products. Currently, the security testing tools already support vulnerability and port scanning for the virtualized network products. So, the existing general requirements of port scanning and vulnerability scanning apply to all types of 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 virtualized and physical network products. So, the existing general requirements of robustness and fuzz testing apply to GVNPs.

6 Vendor development and product lifecycle processes and test laboratory accreditation

6.1 Overview

According to the description from clause 4.4, the scope of SECAM accreditation described in TR 33.916 [2] is applicable to all of the network products, regardless of whether the network product is physical network product or virtualized network product. GSMA FS.14, FS.15 and FS.16, FS.46 [9], [10] [11] and [7] 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 NESASG are apply to type 1 of virtualized network products as well.

Editor's note: The product development and lifecycle processes as well as test laboratory accreditation procedure described in the present document needs to be revisited once GSMA NESASG publishes new methodology specifications on NESAS.

NOTE: GSMA NESASG 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 NESASG to confirm if the current process defined in GSMA is sufficient to cover type 1 of virtualized network products.

The final choices and rules for the accreditation and monitoring rules are under the responsibility of the SECAM Accreditation Body. It is recommended to leave accreditation responsibility to GSMA. This clause outlines what is in scope of the SECAM Accreditation Body.

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

Since the scope of SECAM accreditation described in TR 33.916 [2] is applicable to all of the network products, the evaluation of the security relevant part of the Vendor virtualized network product development and virtualized network product lifecycle management processes is also done as part of the vendor accreditation process by the SECAM Accreditation Body.

Vendor virtualized network product development and virtualized network product lifecycle management processes assurance requirements as well as related evaluation activities generic to all network product classes are defined by the SECAM Accreditation Body. The vendor will define their own processes and describe them in written format. During an audit, the processes will be evaluated and their application on development activities in practice will be verified. An accreditation will be awarded, if the requirements are met.

As described in clause 6.2 of TR 33.916 [2], lifecycle management of virtualized network products also consists of establishing discipline and control in the updates of virtualized network product during its development and maintenance. Lifecycle management controls are important during normal improvement of virtualized network product as well as for vulnerability/security flaw remediation (documentation used to track vulnerability/security flaw, remediation procedure with relation to corrective actions for each identified vulnerability/security flaw…). The vendor accreditation for virtualized network product development and virtualized network product life cycle management processes will provide assurance for these aspects in SECAM.

In addition, for type 1 of virtualized network products, a VNF is instantiated through a series of operations, such as parsing VNF package files, parsing VNFD, instantiating VMs, etc, after a type 1 of virtualized network products (i.e. a VNF package and related softwares, etc.) to a operator delivered by a vendor. The VNF instance can be updated, migrated and deleted, scaled-in, scale-down etc., by VNFM. These processes is called VNF life cycle management defined in ETSI GS NFV 003 [12], it is different from the lifecycle management process of virtualized network products. Its audit and accreditation are out of scope in 3GPP.

The Vendor virtualized network product development and virtualized network product lifecycle management processes assessment does not necessarily apply only to a single virtualized network product. Vendors can submit their generic

virtualized network product development and virtualized network product lifecycle management processes or a subset of them for auditing and accreditation. Generic virtualized network product development and virtualized network product lifecycle management processes are usually used during development of all or some products of the same vendor. As different virtualized network product development and virtualized network product lifecycle management processes could be utilized within the organization of one vendor, e.g. due to mergers or acquisitions, vendors could obtain and hold accreditation for different generic virtualized network product development and virtualized network product lifecycle management processes.

Once the vendor obtains accreditation and as long as the accreditation has not expired, vendors are allowed to produce development process compliance declarations for the "virtualized network product development and virtualized network product lifecycle management processes compliance validation" task on their own.

At the beginning of a SECAM evaluation of a product, the Vendor will have to provide a development process compliance declaration to the compliance tester containing a rationale showing that the generic accredited process was effectively applied in the virtualized network product development and virtualized network product lifecycle management of the virtualized network product under evaluation.

Requirements and accreditation procedures for vendor development lifecycle process and product lifecycle maintenance process accreditation are specified in [10].

6.3 Audit and accreditation of test laboratories

The process for audit and accreditation of test laboratories in clause 6.3 of TR 33.916 [2] are generic and apply to all types of GVNPs.

For type 1 of virtualized network products, to assure the GVNP security during testing process, in addition to assessing the skills of the vendors or third-party test laboratories, the compliance to Test methodology, the SECAM Accreditation Body also needs to accredit the security declaration for NFVI supporting environment (i.e. NFVI for GVNP for type 1) of vendor's or third-party test laboratories.

6.4 Monitoring

All text from TR 33.916 [2], clause 6.4 applied to type 1 of GVNPs.

NOTE: To assure the GVNP security during testing process and after deployment, NFVI for type 1 of GVNP, 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 type 1 of GVNPs.

NOTE: To assure the GVNP security during testing process and after deployment, NFVI of type 1 for GVNP, 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

As described in clause 4.3, the scope of SECAM evaluation for 3GPP physical network products applies to SECAM evaluation of 3GPP virtualized network products. The SCAS instantiation of the virtualized 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 type 1 for GVNP is defined and it contains details on:

- Virtualized Network Product description (e.g. software version, documentation version).
- Scope of evaluation.
- Mapping of SCAS security requirements to the virtualized network product and assets in the virtualized network product.
- References to the applicable document versions containing operational guidance in the documentation of the virtualized 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 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 7.2.1.

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 and clause 4.5, 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 of type 1. The following clauses will focus on the difference from clause 7.2 in TR 33.916 [2].

The description about network product development process and network product lifecycle management in clause 7.2.1 of TR 33.916 [2] applies to type 1 of virtualized network products. In addition, the Vendor Virtualized Network Product Development and virtualized network product lifecycle management process self-evaluation report for the type 1 of virtualized network product under evaluation, which is provided by the vendor, can also contain the security declaration for NFVI supporting environment (i.e. NFVI for GVNP for type 1).

7.2.2 SCAS instantiation evaluation

7.2.2.1 Overview

Like the physical network product, SCAS instantiation evaluation of the virtualized 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 virtualized network product. The evaluator confirms at least that the SCAS being instantiated for a given type 1 of 3GPP virtualized network product and the virtualized network product for evaluation are consistent. According to the clauses 4.3, 4.5 and 4.6, the content and the process of SECAM evaluation from TR 33.916 [2] apply to GVNP of type 1.

7.2.2.2 Content

The content of the SCAS instantiation evaluation from TR 33.916 [2], in clause 7.2.2.2 is generic and applies to type 1 of virtualized network products.

In addition, what the network product description provides is described from TR 33.916 [2], in clause 7.2.2.2.1, a compatibility description (such as which types of virtualization platforms VNF can be deployed on) can also be included in the type 1 of virtualized network product description, to facilitate the preparation of the NFVI supporting environment in the test phase.

7.2.2.3 Process

The process from TR 33.916 [2], in clause 7.2.2.3 applies to type 1 of virtualized network products.

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 virtualized network products. In addition, the accredited test laboratory should prepare supporting environment, i.e. NFVI for GVNP for type 1.

7.2.4 Basic Vulnerability Testing

The process of BVT from TR 33.916 [2], in clause 7.2.3 is generic and applies to the virtualized network products. In addition, the test tools of BVT should support to detect the vulnerabilities in GVNP of type 1.

7.3 Self-declaration

Like self-declaration of a physical network products, after the evaluation process is finished, the vendors review all the evaluation results of the type 1 for virtualized network products and give a declaration of their product. All text from TR 33.916 [2], in clause 7.3 is generic and applies to the virtualized network products.

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

The basic principles for partial compliance and use of SECAM requirements in network product development cycle is described in clause 7.4 of [2]. It also applies to the evaluation of type 1 for virtualized network products.

7.5 Comparison between two SECAM evaluations

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

7.6 The evaluation of a new version

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

Annex A:
Change history

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
2022-02	SA3-106e						0.2.0
2022-08	SA3-108e					Merge approved contributions: S3-222407, S3-222408, S3-222409, S3-222410, S3-222411, S3-222157, S3-222412, S3-222413, S3-222166, S3-222169, S3-222414, S3-222415, S3-222416, S3-222417, S3-222176, S3-222177	0.3.0
2022-11	SA3-109	S3-224096				Merge approved contributions: S3-224080, S3-224081, S3-224082, S3-223461, S3-223553, S3-223554, S3-223555, S3-224083, S3-223564, S3-223572, S3-223575, S3-224084, S3-223633	0.4.0
2023-02	SA3-110	S3-231466				Merge approved contribution: S3-231098	0.5.0
2023-03	SA#99	SP-230131				Presented for information and approval	1.0.0
2023-03	SA#99					Upgrade to change control version	18.0.0
2023-03	SA#99					EditHelp review	18.0.1

History

Document history		
V18.0.1	May 2024	Publication