**3GPP TSG-SA3 Meeting #102-e *S3-210xxx***

**e-meeting, 18 -29 January 2021** Revision of S3-210304

**Source: China Mobile**

**Title: Clarifying for types of virtualised network product class**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution clarifies types of virtualised network product class.***

# 2 References

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

# 3 Rationale

There were three types of virtualised network product class in the TR 33.818. The decoupling scenarios for the type2 and the type 3 of virtualised network product class also described. When a VNF decouples with a virtualised layer for the type 2, the virtualised layer does not be evaluated according to the 3GPP SCAS, because the SCAS for the virtualised layer is out of the 3GPP scope. Similarly, for the type 3, the SCAS for the virtualised layer and the hardware is also out of the 3GPP scope. So, we propose to only the type 1, coupling scenarios of the type2 and the type3 for vitrulised network product class are in the 3GPP scope.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the first change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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.

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: 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 componenets could be considered as internal interface.



Figure 4.1.1-2: Type2 in coupling and decoupling scenarios



Figure 4.1.1-3: Type3 in coupling and decoupling 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 virtulization 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: 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 this document.

NOTE: In order to test a 3GPP GVNP of type 1 or a 3GPP GVNP of type 2, the supporting environment (e.g. NFVI for GVNP for type 1, or hardware for GVNP for type 2) provided by the accredited test laboratory will be considered as secure enough that not impact the SCAS of GVNP. The detailed description can refer to clause 6 and clause 7.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the first change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the second change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 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. However, in decoupling scenario, a 3GPP virtualised network product can be composed by separate components from different vendors. So, vendor development process and product lifecycle process should be considered for each component of a 3GPP virtualised product when it is decoupled.

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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the second change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the third change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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 the role of vendor, there may be the other types of vendor except the traditional CT vendors and more than one vendor could be involved. 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 4.6-1 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the third change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*