**3GPP TSG-SA3 Meeting #99e *S3-201134***

**e-meeting, 11 -15 May 2020** Revision of S3-20xxxx

**Source: China Mobile**

**Title: Adding security requirements and related test cases for GVNP of type 2**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

It is proposed to add the security requirements and test cases for GVNP of type 2 into clause 5.2.5.y.

# 2 Rationale

This contribution describes the security requirements and test cases for GVNP of type 2 to mitigate the security threats described in clause 5.2.4.3.2.

# 3 Detailed proposal

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

5.2.5.y Security functional requirements and related test cases for GVNP of type 2

5.2.5.y.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 sub-clauses.

5.2.5.y.2 Security functional requirements deriving from 3GPP specifications and related test cases5.2.5.y.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.y.3 Technical baseline

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

5.2.5.y.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.y.5 Web servers

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

5.2.5.y.6 Virtualized Network devices

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

In addition, VNF shall be instantiated from trusted image. The detailed security requirements and related test cases are as following.

5.2.5.y.6.1 Instantiating VNF from trusted VNF image

*Requirement Name*: Instantiating VNF from trusted VNF image

*Requirement Description*:

 A VNF shall be initiated from a trusted VNF image which includes one or more than one images. The VNF image 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\_INSTANTIATINGVNFFROMTRUSTEDIMAGE

**Purpose:**

To test whether a VNF is instantiated from a trusted VNF image.

**Procedure and execution steps:**

**Pre-Condition:**

There are a VNF package with an incorrect digital signature, a VNF package with a correct digital signature,, and a NFVO (or simulated NFVO) on the test environment.

**Execution Steps**

**Execute the following steps:**

1. During onboarding, the tester uploads a VNF package with a correct digital signature into the NFVO. The VNF package includes a VNF image.

2. The NFVO will check the digital signature using the certificate which is included in the VNF package..

3. During onboarding, the tester uploads a VNF package with an incorrect digital signature or without a digital signature into the NFVO. The VNF package includes a VNF image.

4. The NFVO will check the digital signature using the certificate which is included in the VNF package.

**Expected Results:**

 1. In the step 2, the digital signature is validated successfully.

2. In the step 4, the digital signature is validated in failure.

**Expected format of evidence:**

Screenshots contain the result of the digital signature validation.

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