**3GPP TSG-SA3 Meeting #102-e *S3-210311***

**e-meeting, 18 -29 January 2021** Revision of S3-21xxxx

**Source: China Mobile**

**Title: Clarifying for the security requirements and test cases in clause 5.2.5.7.7.1 and 5.2.5.7.7.2**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution clarifies the security requirements and test cases in clause 5.2.5.7.7.1 and 5.2.5.7.7.2.***

# 2 Rationale

The revised security threat has been described in 5. S3xxx. This contribution proposes to change the security requirement and test case in clause 5.2.5.7.7.1to align with the security threats.

In addition, the interface between the virtualised layer and the hardware for GVNP of type 3 is the internal interface according to 2. S3-xxxx, this contribution proposes to delete the security requirements and test cases in clause 5.2.5.7.7.2. The related threats reference for potential security functional requirements on trusted platform also be proposed to add.

# 3 Detailed proposal

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

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

All texts in clause 5.2.5.5.7.1 apply to GVNP of type 3. In addition, GVNP of type 3 has the following security requirements related to hardware resource management (e.g. prevent tampering hardware resource management information) and trusted platform which are derived from virtualisation and related test cases.

###### 5.2.5.7.7.1 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. The hardware resource configuration information and state information are sent by the hardware and forwarded by the virtualized layer to the VIM. When the VIM is compromised to change the hardware resource configuration, the hardware does not aware. The hardware should support using secure protocol (e.g. e.g SNMP v3 rather than SNMP v1) to communicate with the VIM to realize that it is communicating with the VIM who has a legal identity, and the content of the communication has the confidentiality and integrity protection.Note: the security of VIM should be guaranteed by the operator when the GVNP is deployed.

*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

**Purpose:**

To test the hardware supports using secure protocol (e.g SNMP v3 rather than SNMP v1) to communicate with the VIM.

**Procedure and execution steps:**

**Pre-Condition:**

There is a VIM (or simulated VIM), a virtualised layer (or simulated virtualised layer) on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester catches the package in the NFVI-VIM.

2. The tester checks whether the hardware resource configuration and state information in the catched package are transmitted by using secure protocol (e.g. SNMP v3).

**Expected Results:**

The hardware resource configuration and state information are transmitted by using secure protocol.

**Expected format of evidence:**

Screenshot contains the secure protocol.

###### 5.2.5.7.7.2 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].

*Threat Reference:* Threats on interface between 3GPP VNF and VNFM, in clause 5.2.4.2.2.3; Threats on interface between virtualisation layer and VIM, in 5.2.4.3.2.3.

*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.

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