**3GPP TSG-SA3 Meeting #99e *S3-201137***

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

**Source: China Mobile**

**Title: Adding security functional requirements deriving virtualisation and related test cases for GVNP of type 3**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

It is proposed to add the Ssecurity functional requirements deriving virtualisation and related test cases for GVNP of type 3 into clause 5.2.5.z.7.

# 2 Rationale

This contribution describes the security functional requirements deriving virtualisation and related test cases for GVNP of type 3 and adds these requirements into clause 5.2.5.z.7.

# 3 Detailed proposal

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

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

[4] 3GPP TR 33.117: "Catalogue of general security assurance requirements"

[5] 3GPP TS 28.500: "Management concept, architecture and requirements for mobile networks that include virtualized network functions"

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

[7] GSMA Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process

[8] ETSI GR NFV-SEC 007: "Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments"

[9]3GPP TR 33.848: "Study on security impacts of virtualisation"

[10] 3GPP TR 33.805: "Study on security assurance methodology for 3GPP network products (Release 12) "

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

[12] ETSI GS NFV-EVE 001: “Network Functions Virtualisation (NFV); Virtualisation technologies; Hypervisor Domain Requirements Specification”

[13] ETSI GS NFV-IFA008: "Network Functions Virtualisation (NFV); Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification"

[14] ETSI GS NFV-IFA019: "Network Functions Virtualisation (NFV); Acceleration Technologies; Acceleration Resource Management Interface Specification"

[x] ETSI GS NFV-SEC 012: “Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components”\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the first change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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

5.2.5.z.7 Security functional requirements deriving from virtualisation and related test cases

All texts in clause 5.2.5.x.7 apply to GVNP of type 3. In addition, GVNP of type 3 has the following security requirements related to hardware resource management, tampering hardware resource management information and trusted platform which are derived from virtualisation and related test cases.

5.2.5.z.7.1 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. When the VIM is compromised to change the hardware resource configuration, an alert shall be triggered by the hardware. The administrator can check the alert and find the attack at latter.

*Threat Reference:* TBA

*Test case*:

**Test Name:** TC\_SECURE HARDWARE RESOURCE MANAGEMENT

**Purpose:**

To test the hardware alerts the error of the hardware resource configuration from the VIM.

**Procedure and execution steps:**

**Pre-Condition:**

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

**Execution Steps**

**Execute the following steps:**

1. The tester utilizes the VIM to make an error hardware resource configuration.

2. The tester checks whether an alert is triggered or not.

Editor’s note: The detailed error hardware resource configuration is ffs.

**Expected Results:**

 The hardware triggers an alert.

**Expected format of evidence:**

Screenshot contains the alert.

5.2.5.z.7.2 Security functional requirements on tampering hardware resource management information

*Requirement Name*: secure hardware resource management information

*Requirement Description*:

When a compromised virtualization layer tampers the hardware resource configuration which is received from the VIM to result in the configuration error of the hardware, the hardware shall trigger an alert. The administrator can check the alert and find the attack at latter.

Note: The operators should check whether the virtualisation layer is trust or not.

*Test case*:

**Test Name:** TC\_SECURE HARDWARE RESOURCE MANAGEMENT INFORMATION

**Purpose:**

To test the hardware alerts the error of the hardware resource configuration.

**Procedure and execution steps:**

**Pre-Condition:**

There are a virtualisation layer (or simulated virtualisation layer) and a host, a VIM on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester tampers a received hardware resource configuration that the virtualisation layer received from the VIM.

2. The tester checks whether the hardware alerts when the tampered hardware resource configuration is implemented.

**Expected Results:**

 The hardware alerts the error of the hardware resource configuration.

**Expected format of evidence:**

Screenshop contains the alert.

Note: The security requirement and related test cases in clause 5.2.5.z.7.2 is only considered in the decoupling scenario.

5.2.5.z.7.3 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 [x]. The trust state of the platform shall be measured and a trusted chain shall be build [8].

*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 screenshop contains process stop.

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