**3GPP TSG-SA3 Meeting #101-e *S3-203130***

**e-meeting, 9 -20 Novenber 2020** Revision of S3-20xxxx

**Source: China Mobile**

**Title: Adding hardening requirements for GVNP of type 2**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution adds hardening requirements for GVNP of type 2 into clause 5.2.5.6.x.***

# 2 References

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

# 3 Rationale

Based on the gap analysis between GVNP SECAM and GNP SECAM in clause 4, and the GVNP model of type 2 in clause 5.2.3, the GVNP of type 2 has the virtualization layer additional the GVNP of type 1, this contribution proposes security requirements and related test cases to hardening for GVNP of type 2 based on the hardening requirements in TS 33.117 and the hardening requirements of GVNP for type 1.

# 4 Detailed proposal

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

5.2.5.6.x Security requirements and related test cases to Hardening for GVNP of type 2

5.2.5.6.x.1 Introduction

The purpose of hardening for GVNP of type 2 is also to reduce its surface of vulnerability. Based on the gap analysis between GVNP SECAM and GNP SECAM in clause 4, and the GVNP model of type 2 in clause 5.2.3, the GVNP of type 2 has the virtualization layer additional the GVNP of type 1. So, the security requirements and related test cases to hardening for GVNP of type 2 are based on the hardening requirements in TS 33.117 and the hardening requirements of GVNP for type 1.

5.2.5.6.x.2 Technical Baseline

5.2.5.6.x.2.1 No unnecessary or insecure services / protocols

All text from TS 33.117 [4], clause 4.3.2.1 applies to GVNP of type 2.

5.2.5.6.x.2.2 Restricted reachability of services

All text from TS 33.117 [4], clause 4.3.2.2 applies to GVNP of type 2.

5.2.5.6.x.2.3 No unused software

All text from TS 33.117 [4], clause 4.3.2.3 applies to GVNP of type 2.

5.2.5.6.x.2.4 No unused functions

As GVNP of type 2 does not contain the hardware layer either, all text from clause 5.2.5.5.8.2.4 applies to GVNP of type 2.

5.2.5.6.x.2.5 No unsupported components

As GVNP of type 1 does not contain the hardware layer either, all text from clause 5.2.5.5.8.2.5 applies to GVNP of type 2.

5.2.5.6.x.2.6 Remote login restrictions for privileged users

All text from TS 33.117 [4], clause 4.3.2.6 applies to GVNP of type 2.

5.2.5.6.x.2.7 Filesystem Authorization privileges

All text from TS 33.117 [4], clause 4.3.2.7 applies to GVNP of type 2.

5.2.5.6.x.2.8 Summary

There is no difference between for GVNP type1 and GVNP type2 in current specification.

5.2.5.6.x.3 Operating System

In addition to the Guest OS, the GVNP of type 2 may have host OS which is also provided by the vendor and generally based on Linux. So, all text from TS 33.117 [4], clause 4.3.3 applies to GVNP of type 2.

Editor’s Note: Hardening requirements for Guest OS not based on Linux are FFS.

5.2.5.6.x.4 Web Severs

All text from TS 33.117 [4], clause 4.3.4 applies to GVNP of type 2

5.2.5.6.x.5 Virtualized Network Products

5.2.5.6.x.5.1 Traffic separation

All text from TS 33.117 [4], clause 4.3.5.1 applies to GVNP of type 2, except for the supporting physical separation of traffic belonging to different network domains.

5.2.5.6.x.5.2 Separation of inter-VNF and intra-VNF traffic

All text from clause 5.2.5.5.8.5.2 applies to GVNP of type 2.

5.2.5.6.x.5.3 Separation of infrastructure management traffic and VNF traffic related to service

All text from clause 5.2.5.5.8.5.3 applies to GVNP of type 2.

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