**3GPP TSG-SA3 Meeting #101-e *S3-210315r5***

**e-meeting, 9 -20 Novenber 2021** Revision of S3-210315

**Source: China Mobile**

**Title: proposal for way forward**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution adds conclusion into clause 8.***

# 2 Rationale

At present, massive virtualized network equipments (like vAMF, vUDM etc.)have been deployed in commercial 5G core networks . In order to ensure the security of such virtualized network products, SECAM and SCAS for GVNP of 5GC shall be developed. Although there is no significant gap between GNP and GVNP in terms of SECAM/SCAS as identified in clause 4, there are still some security threats and requirements specific to generic virtualized network products identified in the present document, the SECAM and SCAS of GVNP in this document only apply to the virtualized 5GC netwok products.

This contribution adds way forward.

# 3 Detailed proposal

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

# 8 Conclusion

## 8.2 Way forward of SECAM/SCAS for 3GPP virtualized network products

In order to ensure the security of the massive deployed virtualized 5GC network products, SECAM and SCAS for such GVNP should be considered.

It is concluded that there is no significant gap between GNP and GVNP in terms of SECAM/SCAS as identified in clause 4. However there are still some security threats and requirements specific to generic virtualized network products identified in the present document, which can serve as the basis for the SECAM and SCAS of specific virtualized network products. To continue the work, the following way forward is proposed:

- for methodology part, it is proposed to capture the methodology specific to GVNP in a new 9-series TR (to pair with TR33.916[2]).

- for critical assets and threats: it is proposed to capture the threats and critical assets as described in clause 5.2.3.2/5.2.4.2 for type1, clause 5.2.3.3/5.2.4.3 for type2, clause 5.2.3.4/5.2.4.4 for type3 specific to virtualized network product class in a new 9-series TR (to pair with TR33.926 [3]).

- for security requirements and test cases, it is proposed to capture the requirements and corresponding test cases for GVNP as described in clause 5.2.5.5 for type1, clause 5.2.5.6 for type2, clause 5.2.5.7 for type3 and clause 5.4 for general BVT test in a new TS (to pair with TS 33.117 [4]).

NOTE1: Regarding GVNP Type2, the security requirements and test cases on the interface between virtualization layer and hardware layer, the interface between 3GPP defined functionalities and VNFM, the interface between virtualization layer and VIM are considered. Regarding GVNP Type 1, only the interface between 3GPP defined functionalities and VNFM, the interface between NFVI and VIM are considered in this present document.

NOTE2：When run the test to GVNP type 1 and GVNP typ2, and when a testcase cannot be passed, the NFVI for GVNP for type 1, or hardware for GVNP for type 2 maybe invlvoed to find out why the testcase cannot be passed. This is because the NFVI for GVNP for type 1, or hardware for GVNP for both type 1 and type 2 may not go through any security assurance testing in the same rigorous manner that is similarly applied to the security assurance testing of GVNP type 1 and GVNP typ2. The NFVI for GVNP for type 1, or hardware for GVNP for both type 1 and type 2 can demostrate secure enough to meet the security requirement specified or will be specified in other related SDO, e.g. ETSI NFV, as well as the security requirements identified is not in the present document.

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