**3GPP TSG-SA3 Meeting #101-e *S3-203163***

**e-meeting, 9th – 20th November 2020** Revision of S3-20xxxx

**Source: Nokia, Nokia Shanghai Bell**

**Title: SCAS VNP: Secure Execution Environment**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***SA3 is kindly asked to approve the proposed changes in TR 33.818 v0.8.0.***

# 2 References

[1] 3GPP TR 33.818 v0.8.0 Security Assurance Methodology (SECAM); and Security Assurance Specification (SCAS); for 3GPP virtualized network products

# 3 Rationale

In current TR 33.818 v0.8.0 [1], the analysis of threats on interface between 3GPP VNF and virtualisation layer for GVNP type 1 is not quite complete. This pCR proposes additional text for the threat analysis in clause 5.2.4.2.2.3.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.4.2.2.3 Threats relating to ETSI-defined interfaces

Two of the interfaces defined in ETSI NFV specification [11] are identified as the critical assets of GVNP type 1, i.e. interface between VNF and VNFM, interface between 3GPP VNF and virtualisation layer. The threats on these interfaces are as follows.

- Threats on interface between 3GPP VNF and VNFM: an attacker can compromise a VNFM to attack a 3GPP VNF. For example, the attacker illegally terminates a 3GPP VNF or tampers with VNFD of a 3GPP VNF without authorization, resulting in DoS attack or information leak against the 3GPP VNF.

- Threats on interface between 3GPP VNF and virtualisation layer: an attacker can attack a 3GPP VNF through a compromised virtualisation layer. For example, cryptographic keys or other security critical data of a 3GPP VNF could be stolen by an attacker with access to the virtualisation layer, or the virtualized resource provided by the virtualization layer to the 3GPP VNF can be manipulated or the bootloader of Guest OS of a 3GPP VNF can be tampered by an attacker via a compromised virtualisation layer.

Editor’s Note: The threat description is to be reformulated from GVNP of type1 perspective.

Editor’s Note: The ETSI-defined interfaces shall be clarified, such as the different understanding from 3GPP defined interfaces.

Editor’s note: More threats described in 3GPP TR 33.848[9] or/and ETSI specification etc. are to be added if identified as related to the above two interfaces.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*