**3GPP TSG-SA3 Meeting #115Adhoc-e *S3-241265-r1***

**Online, 15th -19th April 2024**

**Source: Nokia, Nokia Shanghai Bell, ZTE**

**Title: Resolution of EN concerning including OAM attacks in the study**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***It is requested to approve the pCR***

# 2 References

# 3 Rationale

This pCR proposes to remove the EN concerning scoping the OAM as in scope of the study. SA5 is responsible for this OAM interface which implies that it’s not in scope of SA3. Therefore, it cannot be studied in SA3.

The pCR further introduces a few editorial changes.

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

# 4 Overview

NPN can be hosted by a PLMN. NPN customers can request dedicated NFs to be deployed in the customer premises for performance and privacy reasons.

The focus of the study is divided into two parts:

- Provide security to the PLMN from the attacks that may be initiated by the PNI-NPN.

- Provide security to PNI- NPN functions from attacks that may be initiated by the PLMN.

Public Network Integrated NPNs are NPNs made available via PLMNs e.g. by means of dedicated DNNs, or by one (or more) Network Slice instances allocated for the NPN. Therefore, NFs which may reside within PNI-NPN Network Slice instances may require interfaces which cross the operational domains between PNI-NPNs and PLMNs. In addition, AFs which reside within a PNI-NPN DNNs operational domain may require interfaces which cross the operational domains between PNI-NPNs and PLMNs.

The creation, modification, and termination of a Network Slice Instance (NSI) are supported by Management Services provided by the 5G management systems. Therefore, NFs which provide NSI Management Services may cross the operational domains between PNI-NPNs and PLMNs. The security of management interface is not in the scope of this study.

NFs which reside in the PNI-NPN operational domain may require interfaces which cross the trust boundary between PNI-NPN and PLMN. Therefore, these interfaces require security controls to mutually protect the NFs which reside in the PLMN operational domain and in the PNI-NPN operational domain.

Editor’s Note: Whether interface between customer’s AFs and 5G core network of this study is FFS,

Figure 4-1 and Figure 4-2 demonstrate two example PNI-NPNs with dedicated NFs deployed in the customer premises.

Figure 4-1 PNI-NPN with dedicated UPF deployed in the customer premises

For scenario 1, as depicted in Figure4-1, dedicated UPF is deployed in the customer premises, the other NFs are deployed in the operator premises. The interface between the dedicated UPF in the customer premises and NFs in the operator premises is N4.

Figure 4-2 PNI-NPN with dedicated UPF and part of CP functions deployed in the customer premises

For scenario 2, as depicted in Figure 4-2, dedicated UPF and part of CP functions are deployed in the customer premises. The interface between the dedicated NFs in the customer premises and the NFs in the operator premise is SBA interface. Examples of dedicated CP functions that are likely to be hosted by NPN in the customer premises are as below:

- AMF.

- SMF.

SA1 has captured the scenarios and added requirements in clause 8.2 of TS 22.261[2], which is:

*“The 5G system shall enable a PLMN to host an NPN without compromising the security of that PLMN.*

*NOTE: Dedicated network entities of NPN can be deployed in customer premises that are outside the control of the PLMN operator.”*

**\*\*\*\*** END OF CHANGE **\*\*\*\***