**3GPP TSG-SA3 Meeting #108e-AdHoc *S3-222549r4***

**e-meeting, 10 - 14 October 2022** merger of 2549 and 2832

**Source: Huawei, HiSilicon, Nokia**

**Title: New key issue on multiple NSACFs**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***Approve the new KI proposal to eNS3 TR33.886***

# 2 References

[1]

# 3 Rationale

The contribution proposes a new key issue to study the slice admission control when multiple NSACFs are deployed in HPLMN and VPLMN.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES \*\*\*

## 4.3 Key Issue #3: network slice admission control (NSAC)

### 4.3.1 Key issue details

The network slice admission control (NSAC) issues were studied in Rel-17. It has been agreed in Rel-18 to enhance NSAC features with the following features:

- improved network control of the UE behaviour

- support deploying multiple NSACF

In both cases, better UE admission control is aimed to match the allocated quota. However, potential issues of Denial of service (DoS) attacks to legitimate UEs when the additional features are added to the access control mechanism. The information of actual UE / PDU session usage by a slice, or misinformation provided by malicious UEs or mischievous NFs may not be reflected based on current solutions. For example, a NSACF in a VPLMN updating the number of registered UEs or PDU sessions independently may not provide trusted information to the home NSACF. Another example is when a UE not using a network slice is still counted against quota usage of S-NSSAIs where it is registered. It is notable that an attacker can use legitimate UEs to launch such attacks.

In the TR23.700-41 [3], the issue of how to support network slice admission control (NSAC) involving multiple service areas is being studied, together with multiple solutions accepted. The general assumption is that multiple NSACFs are required, either centralized or distributed. In a roaming scenario, it is assumed that the NSAC may be controlled by an NSACF in the VPLMN or an NSACF in the HPLMN.

However, in a roaming scenario, the information reported by the NSACF in the VPLMN is not verified when it is reported to the HPLMN, i.e. there is no proper home control and a misinformation provided by VPLMN may have negative impact to the slices in other service areas, either in HPLMN or other VPLMN.

The security control in different serving areas/PLMNs could be different. For example. the security measure in some service areas is not as strict as what in other areas, attack surface in PLMN of one region may be higher than other regions, etc. The compromised/malicious NSACFs (for solution#13) in some high risky serving areas/networks may trigger DoS or other attacks on the home network, e.g., the compromised/malicious (local/distributed) NSACFs in a risky service area may fake the case that the number of registration UEs/PDU sessions is reaching the maximum number, and send Nnsacf\_NSAC\_NumberUpdate\_Request to the Primary NSACF for new quota. The Primary NSACF may allocate more quota to the NSACF in compromised serving area/network while decrease the quota of other “lower load” area. Finally, the service of other serving areas/networks could be impacted as the global maximum number may be exhausted by the compromised/malicious NSACFs. As the attack complexity is relatively low while the availability impact could be high, the risk on the system could be high.

### ~~4.3.2 Security threats~~

### ~~The malicious/compromised NSACF(s) in specific area(s) of a PLMN with low security protection may continuously send fake message primary NSACF to indicate the number of registration UEs/PDU sessions is reaching the maximum number, that may cause the primary NSACF to re-distribute the quotas of maximum number of registration UEs/PDU sessions to NSACFs in serving areas, finally impact the service of other benign serving areas.~~

~~If an NSACF in a VPLMN overstates its quota usage to the home NSACF handling the total quota, it may cause reduced quota and denial of servie for UEs in HPLMN or other VPLMNs. If an NSACF in a VPLMN understates its quota usage to the home NSACF handling the total quota, it may cause quota being exceeded and depletion of the system resources.~~

### ~~4.3.3 Potential security requirements~~

~~The 5G system shall provide means for verifying the report from an NSACF in VPLMN.~~

~~The 5G System shall provide a means for preventing the quota of maximum of registration UEs/PDU sessions of a network slice being exhausted by malicious/compromised NSACF(s).~~

\*\*\* END OF CHANGES \*\*\*