**3GPP TSG-SA3 Meeting #104-e *S3-212575r3***

**e-meeting, 16 - 27 August 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: New KI on DoS to NSAC procedure**

**Document for: Approval**

**Agenda Item: 5.21 FS\_eNS2\_SEC**

# 1 Decision/action requested

***Include the KI in TR33.874***

# 2 References

[1]

# 3 Rationale

This contribution proposes a new key issue for the study.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGE (All Text Are New)\*\*\*

## 5.X Key Issue #X: DoS to NSAC procedure

### 5.1.1 Key issue details

A new Network Slice Admission Control (NSAC) procedure has been introduced in TS23.501 [2] and TS23.502 [3], where the number of registered UEs is monitored for a network slice (i.e. S-NSSAI) and a UE will be rejected to access if the number of UE registered in the requested S-NSSAI has reached its quota. However, the NSAC procedure needs to be studied further to address potential security risks, for examples:

* In the current NSAC procedure, the number of registered UE in an S-NSSAI is updated independently from other S-NSSAIs during the registration procedure. In other words, the granularity level at registration is S-NSSAI. However, it is not the case in the de-registration procedure. The numbers are only updated when the UE exits from all network slices, i.e. de-registered. Since a UE may access multiple slices, e.g. eight, the UE would still be counted against quota usage of ALL S-NSSAIs even the UE is not using some or most of slices (“idly occupied” by the UE). This may lead to the quota reached fast which does not reflect the real usage of a slice. Other legitimate UEs will suffer from DoS – “dog in the mager”. It is notable that an attacker can use legitimate UEs to launch such attacks.
* Assuming NSSAA is executed before NSAC, then if NSSAA is successful but quota has been reached, UE will be rejected. The UE has to send registration request later and go through the same NSSAA procedure again. This is a significant waste of resource (has to serve fewer UEs given the same resource) when NSSAA is required, since NSSAA requires multiple rounds of message exchanges with the home PLMN.
* The Early Admission Control (EAC) mode has been introduced where the admission control can be inactive if the number of UE bellows a preconfigured threashold. This may pose a security risk that exceeds the slice quota when a sudden increase in the slice registration requests, maliciously or accidentally.

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