**3GPP TSG-SA3 Meeting #107-e *S3-220795r2***

**e-meeting, 16 - 20 May 2022**  Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: KI#2 update - threats and requirements**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***Approve the proposed updates to KI#2 for TR33.874***

# 2 References

[1] S2-2107942 Reply LS on NSAC procedure

# 3 Rationale

This contribution proposes to update the threats and requirements clauses of KI#2 based on LS from SA2 [1]

* *SA2 would like to indicate that the UE usage of a user services is not considered when counting the number of UEs registered to a network slice*

**The threats and potential security requirements are updated based on the statement that the UE usage is not considered.**

* *If needed, the operator may activate EAC mode when the current count is reaching certain operator defined threshold.*

**The threats and potential security requirements are updated as suggested. The solution can be used to address this issue.**

# 4 Detailed proposal

pCR

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

## 5.2 Key Issue 2: DoS to NSAC procedure

### 5.2.1 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.
* The Early Admission Control (EAC) mode has been introduced where the admission control can be inactive if the number of UE bellows a pre-configured threshold. This may pose a security risk that exceeds the slice quota when a sudden increase in the slice registration requests, maliciously or accidentally.

### 5.2.2 Security threats

~~If the NSAC procedure does not reflect the real situation of the slice usage, an attacker may launch a DoS attack to legitimate users. The DoS may also happen inadvertently when many UEs do not use the slices registered.~~

If EAC mode is not activated properly, it *has the potential to ~~will~~* cause DoS to the network slices.

### 5.2.3 Potential security requirements

~~The 5G system should provide mechanisms to prevent DoS due to inconsistency between “slice registration” and “slice usage” by UEs.~~

The 5G system should prevent *a potential* DoS due to the EAC inactive mode.

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