**3GPP TSG-SA3 Meeting #108e *S3-221802***

**e-meeting, 22 - 26 August 2022**

**Source: Huawei, HiSilicon**

**Title: update to KI#3**

**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 to update KI#3 to include security threats and requiremnts.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF 1st 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.

### 4.3.2 Security threats

If a mischievious 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 other VPLMNs

If an attacker employs legitimate UEs to register for a slice but not to use the slice services, fewer other UEs will be allowed to use the slice. This will cause an underutilized slice and denial of services to those UEs rejected due to quota reached.

If the updated NSAC procedures are not secured, an attacker may temper the signalling or access sensitive information without authorization.

### 4.3.3 Potential security requirements

The 5G system should secure the NSAC procedures ~~in support of multiple NSACF.~~ in support of improved network control of the UE behaviour and multiple NSACF

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

\*\*\* END OF 1st CHANGES \*\*\*