**3GPP TSG-SA3 Meeting #107e AdHoc *S3-221376-r1***

**e-meeting, 27 June - 1 July 2022**

**Source: Huawei, HiSilicon**

**Title: New KI on NSAC**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

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

# 2 References

[1] 23.700-41 Study on enhancement of network slicing; Phase 3

# 3 Rationale

The contribution proposes a new key issue to study security aspects related to Network Slice Admission control (NSAC). This is also a continuation of an inconclusive key issue in Rel-17 of TR33.874.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF 1st CHANGES \*\*\*

## 5.X Key Issue #X: network slice admission control (NSAC)

### 5.X.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.

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

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