**3GPP TSG-SA3 Meeting #106-e *S3-220116r3***

**e-meeting, 14 – 25 February 2022**  Merger of S3-220116 and 220200

**Source: Huawei, HiSilicon, Xiaomi**

**Title: update to KI#2**

**Document for: Approval**

**Agenda Item: 5.12 FS\_** **eNS2\_SEC**

# 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

In the LS [1], SA2 has provided answers to three questions that SA3 raised before. This contribution proposes to update the KI#2 based on the answers and observations, as summarized below:

* *[SA2] 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*
* **Observation 1**: *UE usage of a user services is not considered when counting the number of UEs registered to a network slice.*
* *[SA2] The NSSAA status is kept in the UE context in AMF (also transferred between AMFs), i.e. the AMF may avoid NSSAA when NSSAA has been successful for an S-NSSAI.*

**Observation 2**: The previous NSSAA status is kept (e.g. successful) and extra NSSAA can be aoived. There should be no problem with the clarification.

* *[SA2] If needed, the operator may activate EAC mode when the current count is reaching certain operator defined threshold.*

**Observation 3**: It is up to operators to set a proper threshold to activate EAC mode, which can avoid the risk of bursting in the number of UEs attempting to register under EAC mode inactive. The threshold setting is a matter of operator deployment.

# 4 Detailed proposal

pCR

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.2 Key Issue 2: Potential security threats 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, some UEs may not have access to the slicing service when many legal UEs registered and paid for the slicing service but are not using the slices.

If EAC mode is not activated properly, there is the risk of bursting in the number of UEs attempting to register under EAC mode inactive..

### 5.2.3 Potential security requirements

No potential security requirements are identified.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

## 7.X Conclusions for KI#2

As the issue of slice usage will be handled by SA2 in Rel-18, this issue will not be studied by SA3 in Rel 17.

It is up to operators to set a proper threshold to activate EAC mode. The threshold setting is a matter of operator deployment, which does not need any specification.

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