**3GPP TSG-SA3 Meeting #105-e *S3-213918r1***

e-meeting, 8 - 19 November 2021 Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: update to KI#1**

**Document for: Approval**

**Agenda Item: 5.18 FS\_** **eNS2\_SEC**

# 1 Decision/action requested

***Approve the proposed conclusions to KI#3 for TR33.874***

# 2 References

[1] TR33.874

# 3 Rationale

This contribution is to address the following EN

Editor's Note: Whether the AF is considered to be within the 3GPP operator domain (according to TS 33.501 [7], clause 12) or not is FFS.

In the last meeting (#104-bis), sending ENSI to AF from NEF was made optional. It was found as in the EN that it would have an impact to the current trust models. The current models are

**Model A = trusted AF (AF deployed by PLMN, or AF trusted by PLMN)**

**Model B = untrusted AF (AF not trusted by PLMN)**

Note: both trusted and untrusted AFs could be authenticated and authorized between AF and NEF (or interact with 5GC NFs through NEF)

The pCR revise the solution to align with exiting trust model

# 4 Detailed proposal

pCR

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

### 6.1.2.2 Number of UEs and PDU Sessions per network slice status retrieval by AF procedure



Figure 6.1.2.2-1: Number of UEs and PDU Sessions per network slice status retrieval by AF procedure

1. To retrieve information about the number of the UEs registered with a network slice or the number of the PDU Sessions established on a network slice or both, the AF sends Nnef\_SliceStatus\_Retrieval Request (Event ID, Event Filter) message to the NEF.

The Event ID parameter defines the information to be reported, i.e. the number of registered UEs with a network slice or the number of the PDU sessions with a network slice or both. The Event Filter parameter defines the S-NSSAI for which reporting is required. If the AF is a trusted NF, The Event Filter parameter is S-NSSAI whereas the Event Filter parameter is ENSI for an untrusted AF.

NOTE: If AF is from the 3rd party that belongs to a different security domain than the operator, i.e. untrusted AF by the operator, ENSI shall be used to meet the requirement for AF in clause 5.9.2.3, TS 33.501[7].

2. The NEF checks whether the AF is authorised based on the AF token. It needs to check whether the token claims matches the AF’s identity and the Event Filter parameter. If authorised, the NEF may query the NRF to find the NSACF responsible for the requested S-NSSAI. The authorization check by NEF needs to make sure the AF is allowed to access the S-NSSAI.

The NEF shall map to S-NSSAI from ENSI for a untrusted AF. The authorization check by NEF needs to make sure the AF is allowed to access the S-NSSAI.

3. The NEF forwards the request to the NSACF with Nnsacf\_SliceStatus\_Retrieval Request (Event ID, Event Filter).

4. The NSACF returns the Nnsacf\_SliceStatus\_Retrieval Response (Event ID, Event Filter, Event Reporting information) message to the NEF, as in TS23.502 [3].

5. The NEF forwards the message to the AF in the Nnef\_SliceStatus\_Retrieval Response (Event ID, Event Filter, Event Reporting information) message. The Event Filter parameter is changed to the mapped ENSI for the untrusted AF.

### 6.1.3 Evaluation

This solution addresses the key issue #3 by optionally storing a mapping between an S-NSSAI and ENSI in NEF. An untrusted AF is configured with ENSI instead of S-NSSAI to avoid sensitive information leakage.

NOTE: the mapping between an S-NSSAI and ENSI is only configured for untrusted AF.

 This solution is in line with the SA2 defined procedures for the AF to get access to the network slice quota information.

The NSACF services, i.e. “Nnsacf\_SliceEventExposure\_Subscribe/Unsubscribe” and “Nnsacf\_SliceEventExposure\_Notify” are not affected and can be kept as is in TS23.502 [3].

Optionally, the corresponding NEF services may be updated with the different Event Filter values.

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