**3GPP TSG-SA3 Meeting #104-e *S3-212588r1***

**e-meeting, 16 - 27 August 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: New Solution to AF authentication and authorization**

**Document for: Approval**

**Agenda Item: 5.21 FS\_eNS2\_SEC**

# 1 Decision/action requested

***Include the KI in TR33.874***

# 2 References

[1]

# 3 Rationale

This contribution proposes a new key issue for the study.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF 1st CHANGES (All Text are New) \*\*\*

## 6.Y Solution #Y: authentication and authorization for a third-party AF or an AF deployed within 3GPP systems

### 6.Y.1 Introduction

AF authentication and authorization is subject to whether the AF lies in the 3GPP system or in a third party domain. Existing but different mechanisms are chosen for the two scenarios. In case AF is a third party NF, S-NSSAI is not required at AF to prevent sensitive information leakage.

### 6.Y.2 Solution details

If an AF is deployed within the 3GPP systems, authentication and authorization is based on the mechnisms defined for SBI, Clause 13 in TS33.501 [x], where the AF is authenticated by the NRF it registered within the same PLMN. For the Oauth 2.0 based authorization, the NRF takes the role of Authentication Server and the NEF takes the role of Resource Server.

If an AF a third party NF, authentication and authorization is based on the mechnisms defined in Clause 12 in TS33.501 [x], where mutual authentication is performed between the AF and the NEF. For the Oauth 2.0 based authorization, the NEF takes both roles of Authentication Server and the Resource Server.

In order to avoid sensitive information leakage involving S-NSSAI, S-NSSAI is not sent to or made available to a third party AF. Instead, NEF keeps a mapping between S-NSSAI and ENSI (External Network Slice Inforamtion) and ENSI (instead of S-NSSAI) is available at the third party AF. The notification procedure (adapted from the clause 4.15.3.2.10 of TS 23.502 [3]) with ENSI is described as below.

### 6.Y.2.1 Number of UEs and PDU Sessions per network slice notification procedure

###

Figure 6.Y.2.1-1: Number of UEs and PDU Sessions per network slice notification procedure

0. Authentication of AF: AF is authenticated by NRF or authenticated by NEF based on description above. A token is generated for AF after authentication. It is noted that the AF token includes claim for the authorized S-NSSAI or ENSI (if AF is a third party NF).

1. To subscribe or unsubscribe for the number of UEs or the number of PDU Sessions per network slice notification with the NSACF, the AF sends Nnef\_EventExposure\_Subscribe/Unsubscribe Request (Event ID, Event Filter, Event Reporting information) message to the NEF. The Event ID parameter defines the subscribed event ID, i.e. Number of Registered UEs or Number of Established PDU Sessions. The Event Filter parameter defines the S-NSSAI for which reporting is required. If the AF is a 3GPP NF, The Event Filter parameter is S-NSSAI whereas the Event Filter parameter is ENSI if the AF is a third party NF. The Event Reporting information parameter defines the mode of reporting, i.e. threshold based reporting with included a threshold value or periodic reporting with included periodicity time interval.

2. The NEF checks whether the AF is authorised for the requested subscription 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 (NEF needs to map to S-NSSAI based on ENSI for a third party AF). The NEF forwards the request to the NSACF with Nnsacf\_SliceEventExposure\_Subscribe/Unsubscribe Request (Event ID, Event Filter, Event Reporting information). The Event Filter parameter is the mapped S-NSSAI for the third party AF.

3. The NSACF confirms with Nnsacf\_SliceEventExposure\_Subscribe/Usubscribe Response message to the NEF.

4. The NEF forwards the response from NSACF via the Nnef\_EventExposure\_Subscribe/Unsibscribe Response message to the AF. The Event Filter parameter is changed to the mapped ENSI for the third party AF.

5. When the reporting condition for a subscribed event is fulfilled, the NSACF triggers a notification towards the AF.

6. The NSACF sends the Nnsacf\_SliceEvent Exposure\_Notify (Event ID, Event Filter, Event Reporting information) message to the NEF. If the subscription is for event based notification (e.g. based on the monitored event reaching a threshold value), the Event Reporting information parameter contains confirmation for the event fulfilment. If the subscription is for periodic notification, the Event Reporting information parameter provides information for the current number of UEs registered with a network slice (e.g. represented in percentage of the maximum number of the UEs registered with the network slice) or information for the current number of PDU Sessions on a network slice (e.g. represented in percentage of the maximum number of the UEs established on the network slice) or both. It is

7. The NEF forwards the message to the AF in the Nnef\_EventExposure\_Notify (Event ID, Event Filter, Event Reporting information) message. The Event Filter parameter is changed to the mapped ENSI for the third party AF.

### 6.Y.3 Evaluation

TBC

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

\*\*\* BEGINNING OF 2nd CHANGES \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: “System architecture for the 5G System (5GS)”

[3] 3GPP TS 23.502: “Procedures for the 5G System (5GS)”

[4] 3GPP TS 23.503: “Policy and charging control framework for the 5G System (5GS); Stage 2”

[5] 3GPP TR 23.700-40: “Study on enhancement of network slicing; Phase 2”

[6] 3GPP TR 38.832: “Study on enhancement of Radio Access Network (RAN) slicing”

[x] 3GPP TS 33.501: “Security architecture and procedures for 5G system”

\*\*\* END OF 2nd CHANGES \*\*\*