**3GPP TSG-SA3 Meeting #108-e draft\_S3-221934-r3**

**e-meeting, 22nd – 26th August, 2022**

**Source:**  **Huawei, HiSilicon**

**Title:** **New authorization mechanism for the involved NFs in the delegated "Subscribe-Notify" scenarios**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***It is proposed to approve the change described in this document.***

# 2 References

[1] 3GPP TR 33.875: " Study on enhanced security aspects of the 5G Service Based Architecture (SBA); ".

# 3 Rationale

It is proposed to add a new authorization mechanism for the involved NFs in the delegated “Subscribe-Notify” scenarios.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

## 6.X Solution #X: Authorization mechanism for the involved NFs in the delegated “Subscribe-Notify” scenario.

### 6.X.1 Introduction

This solution addresses KI#3 on how to assure that the notification messages could be only forwarded to an authorized NF identified by its NF instance ID in the delegated “Subscribe-Notify” scenarios. This solution does not address authorization of the notification URI.

The solution is based on the authorization of NF Service Consumers for data access via DCCF specified in Annex X.2 of TS 33.501 [2]. It proposes to include two instance IDs in the access token request, allowing the NRF to check whether one NF (e.g. NF\_C) is authorized to subscription and whether another NF (e.g. NF\_A) as the proxy is allowed to request the service from the identified NF Service Producer on behalf the NF\_C. The NF Service Producer verifies the access token is valid according to these instance IDs. After successful verification, the NF Service Producer should provide the notification service. Editors Note: It is ffs how the solution works in case of notification target reselection as described in clause 6.3.1.0 of TS 23.501.

### 6.X.2 Solution details

In the “Subscribe-Notify” NF service illustration 2 (delegated scenario) specified in TS 23.501 [3], clause 7.1.2, an NF Service Consumer (e.g. NF\_C) may subscribe the service of an NF Service Producer (e.g. NF\_B) on behalf of another NF Service Consumer (e.g. NF\_A).

The Figure 6.X.2-1 describes the detailed solution for authorization mechanism for the involved NFs in the delegated “Subscribe-Notify” scenarios.



**Figure 6.X.2-1: Authorization** **mechanism for the involved NFs in the delegated “Subscribe-Notify” scenario**

1. The NF\_A decides to subscribe the service of NF Service Producer (e.g. NF\_B) on behalf of NF\_C and gets an access token from the NRF for a Service Request toward the NF\_A. The NF\_C initiates an NF service request to the NF\_A which includes the notification URI, the access\_token\_NF\_C and the CCA of NF\_C to be used for subscription.
2. The NF\_A should verify if the access token and the CCA of the NF\_C is valid and executes the service.
3. The NF\_A sends a Nnrf\_AccessToken\_Get request to NRF including the information to identify the target NF (NF Service Producer), the source NF (NF Service Consumer e.g. NF\_C), the NF Instance ID of NF\_A and the CCA\_NF\_C received at step 2.
4. The NRF should check whether the NF\_C are allowed to access the service provided by the identified NF Service Producer, and whether the NF\_A as the proxy is allowed to request the service from the identified NF Service Producer on behalf the NF\_C. The NRF authenticates NF\_C based on the CCA of NF\_C.
5. If the authorization is successful, the NRF shall then generate an access token with the identity of the NF\_A and the identity of the NF\_C, NF type of the NF Service Producer (audience), subscribe service name(s), (scope).

The NRF sends access token to the NF\_A in the Nnrf\_AccessToken\_Get response operation.

1. The NF\_A requests service to the NF Service Producer. The Service Request also consists of the CCA\_NF\_C, so that the NF Service Producer authenticates the NF \_C.
2. The NF Service Producer authenticates the NF\_C and verifies the access token to ensure that the access token is valid. After authentication and authorization is successful, the NF Service Producer assures that the NF\_A as the proxy is allowed to receive the response message on behalf the NF\_C, and executes the subscribe service.
3. The NF Service Producer should respond the NF\_A and provide the NF\_C with the notification service based on the Notification URI.

### 6.X.3 Evaluation

TBD

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