**3GPP TSG-SA3 Meeting #104-e *S3-212887***

**e-meeting, 16 - 27 August 2021** Revision of S3-21xxxx

**Source: Nokia, Nokia Shanghai Bell**

**Title:**

**Document for: Approval, Information, Discussion**

**Agenda Item:**

# 1 Decision/action requested

Details on Solution #2: Authorization between NFs and SCP

# 2 References

[1] 3GPP

# 3 Rationale

*Reason for change:*

*Summary of changes:*

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES*

6.2.2 Solution details

When sending the service request to SCP in delegated discovery, the NF Service Consumer must authorize the SCP to act on its behalf. Thus, NRF needs to be provided with evidence by NFc about the SCP instance ID.

NRF knows implicit the SCP instance ID because of direct TLS between SCP and NRF, when SCP ID would be added in a SCP TLS certificate. But this still does not assure that NFc as sent its request to this SCP. Thus, authorization between NF Service Consumer and SCP, when sending the service request to SCP in delegated discovery, has to be explicit. The solution proposes to do so by enhancing the CCA by inserting either the SCP Instance ID or the SCP Domain Info in CCA\_NFc, and therefore the NF Service Consumer can authorize SCP.

NOTE: Since in model D the NF Service Consumer is delegating the discovery, as well as access token request, service request and receiving service response to SCP, the NF Service Consumer authorizes the SCP to perform these actions on its behalf.

The SCP also generates its own enhanced CCA\_SCP including its Instance ID and/or its Domain Info and sends it along with access token request and the enhanced CCA\_NFc as received from NF Service Consumer.

****

**Figure 6.2.2-1: Authorization of SCP by NFc in indirect communiation**

NFc

SCP

NRF

1. Service Request (optionally includes enhanced CCA')

**\* CCA' additionally includes Authorized SCP ID**

2. Nnrf\_AccessToken\_Get\_Request (**includes CCA' and CCA,**

CCA contains the SCP Instance ID in the subject parameter)

3. NRF analyzes the request, and authorizes the SCP

4. Nnrf\_AccessToken\_Get Response

(access token)

The NRF verifies that the Target SCP Instance ID and/or SCP Domain info present in the CCA\_NFc matches the Instance ID/Domain Info of SCP as also being part of the subject of the CCA\_SCP. A successful verification of CCA(s) by NRF ensures that the SCP has been authorized by the NF Service Consumer.

Thus, the NRF needs to know the SCP Instance ID. One way for the NRF to learn the SCP instance ID is to use direct TLS between SCP and NRF, this requires SCP ID in the SCP TLS certificate which is currently not specified in TS 33.310. Another way for the NRF to learn the SCP instance ID is by CCA\_SCP.

If authentication was successful and the NF Service Consumer is authorized based on the NRF policy and the SCP requesting the access token has been explicitly authorized by NF Service Consumer, the NRF issues an access token.

A similar solution is also applicable for authorizing SCP by NFc to request a service and receive a response from NFp on its behalf. The NFp then may perform similar verification and, in case of successful verification, can send the service response to SCP.

However, even if the TLS certificate of the NFc would mandate the usage of NFc Instance ID, another problem still needs to be solved in case the SCP selects another SCP. This is because if the NRF or the NF Service Producer do not know the SCP domain, to which the SCP belongs to, the SCP\_CCA included by NFc does not help NRF. Thus, for this reason it is suggested that the TLS certificate needs in addition to SCP Instance Id also to hold the SCP domain identifier for allowing NRF to verify that NFc authorized one SCP of a SCP domain.

If the SCP, that NF Service Consumer delegated the authorization token request to, is not serving the NF Service Consumer request by itself, but demands another SCP' to do so, then the same procedure is needed between SCP and SCP'. Hence, SCP forward the service request to SCP' with its own CCA\_SCP including into it the SCP' ID.

The verification of the CCA shall be performed by the receiving node as described in clause 13.3.8.3, but verifying that the SCP instance ID in the CCA is matching the SCP instance ID in the public key certificate used for signing the CCA. This is either done by an SCP, in case there are several SCPs in between, or by the NF Service Producer.

In practice, one would expect one to three SCPs between consumer and producer. But it needs to be noted, if the NF Service Producer wants to have verification of the full chain of trust via several SCPs, all CCAs and certificates from the NF Service Consumer and the intermediary SCPs need to be available to the NF Service Producer.

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