**3GPP TSG-SA3 Meeting #108e *draft\_S3-221855-r2***

**e-meeting, 22 - 26 August 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI4 EN resolution of sol3**

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

**Agenda Item: 5.24**

# 1 Decision/action requested

***Resolution of editor’s note in key issue #4 solution 3 is proposed.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*Solution #3 for of Key issue #4: Authorization of SCP to act on behalf of an NF or another SCP has an EN as follows:*

Editor's Note: Whether an implicit authorization of the SCP by sending the CCA to the SCP is sufficient, is ffs.

It is proposed to update to:

NOTE: Implicit authorization of the SCP using mutual TLS between NF Service Consumer and SCP is not providing e2e authorization information from the NFc to NRF or NFp.

# 4 Detailed proposal

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

6.3 Solution #3: Using existing procedures for authorization of SCP to act on behalf of an NF Consumer

6.3.1 Introduction

This solution addresses Key Issue #4 "Authorization of SCP to act on behalf of an NF or another SCP". It explains how token-based authorization and CCAs as currently specified in TS 33.501 [2] can be used to authorize the SCP to act on behalf of an NF Consumer, i.e. to request access tokens or services on behalf of the consumer. The solution relies on implicit authorization of the SCP using mutual TLS between NF Service Consumer and SCP.

### 6.3.2 Solution details

#### 6.3.2.1 Request of access token on behalf of the consumer

The SCP requests access tokens on behalf of the consumer in Scenario D (indirect communication with delegated discovery) and in Scenario C (indirect communication without delegated discovery) without mutual authentication between NF and NRF at the transport layer. The following procedure describes token requests for Scenario D, and particularly how CCAs are used to authorize the SCP to request access tokens on behalf of the NF Consumer. For Scenario C without mutual authentication between NF and NRF at the transport layer, the same principles hold.



Figure 6.3.2.1-1: Access token request of SCP on behalf of an NF Consumer

1. The NF Service Consumer sends a service request to the SCP. The consumer includes a CCA signed by the consumer. The CCA includes the NF Instance ID of the consumer. The consumer's certificate used for signing the CCA also contains the consumer's NF Instance ID.

2. The SCP sends an access token request to the NRF. The SCP includes the CCA received by the consumer in step 1.

3. The NRF verifies the CCA as described in clause 13.3.8.3 of TS 33.501 [2] and thus obtains the NF Instance ID of the consumer that signed the CCA. Besides authentication of the consumer, the CCA also implicitly authorizes the SCP to act on behalf of the NF Service Consumer.   
  
The NRF authorizes the NF Service Consumer as described in TS 33.501 [2].

4.-8. The remaining steps of the access token request and service request procedure are exactly as described in TS 33.501 [2].

#### 6.3.2.2 Service request on behalf of the consumer

The SCP requests services on behalf of the consumer in all indirect communication scenarios. The following procedure describes access token and service requests for Scenario D, and particularly how CCAs and access tokens are used to authorize the SCP to request services on behalf of the NF Consumer. For Scenario C, the same principles hold.



Figure 6.3.2.2-1: Service request of SCP on behalf of an NF Consumer

1.-4. Service request and access token request and response are performed as described in the previous clause, clause 6.3.2.1.

5. The SCP sends a service request to the NF Service Producer. The service request contains the access token and optionally the CCA received in step 1. The access token contains the NF instance ID of the NF Service Consumer.

6. The NF Service Producer validates the access token as described in TS 33.501 [2]. Because the network implements the procedures described in the previous clause, clause 6.3.2.1, the NRF has already verified that the SCP was authorized to request the access token on behalf of the NF Service Consumer. Hence the access token does not only authorize the consumer, but also implicitly authorizes the SCP to act on behalf of the NF Service Consumer.

7.-8. The remaining steps of the access token request and service request procedure are exactly as described in TS 33.501 [2].

#### 6.3.2.4 Protection of the NF consumer's CCA

The CCA is protected in transport and storage by the following methods, partly in and partly out of 3GPP scope:

- Transport protection: The CCA is protected in transport by TLS or other means, as specified in TS 33.501 [2], clause 13.1.0. Thus, it is protected between NF and SCP, and between SCP and NRF or NFp.

- Storage protection: Although CCAs are expected to be short-lived, they could be cached for a short period of time at the NF Service Consumer. Similar as for other data handled at the NF Service Consumer, e.g., sensitive UE data, storage protection mechanisms outside of 3GPP scope need to be in place.

If used according to the procedure describes in clause 6.3.2.1, only the NF Service Consumer itself, the SCP and the NRF will obtain the CCA that allows to request access tokens on behalf of the NF Service Consumer. This solution assumes, that the SCP is authorized by the NF Service Consumer to request access tokens on behalf of it, the NF Service Consumer indicates that by sending the CCA to the SCP. The NRF is itself the entity that issues access tokens for the NF Service Consumer. Hence, if used according to the procedure described in clause 6.3.2.1, only entities that are authorized by the NF Service Consumer to request access tokens on behalf of it obtain the CCA.

### 6.3.3 Evaluation

The solution addresses the threats and requirements of Key issue #4: Authorization of SCP to act on behalf of an NF or another SCP.

The solution relies on token-based authorization and CCAs as currently specified in TS 33.501 [2].

It proposes that authorization of the SCP by the CCA is implicit by sending the CCA to the SCP, i.e. by presenting the CCA\_NFc received by the NF Service Consumer, the SCP shows it is authorized to act on behalf of the Consumer and to request access tokens on behalf of it. However, authorization is not explicitly stated in the CCA. No e2e authorization information is provided from the NFc to NRF or NFp. Hence an entity that is not authorized by the NF Service Consumer but somehow has obtained a valid CCA signed by the consumer could use it to request access tokens on behalf of the consumer. Thus, in this case the NRF or the NFp can provide the service response to an unauthorized consumer.

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