**3GPP TSG-SA3 Meeting #108e *draft\_S3-221850-r1***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: EN resolution in solution 6 – evaluation part**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***Clarification text in order to resolve the EN in solution 6’s evaluation part.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*Resulution of Editor’s Note: How to assure by the NFc that the NFp is the original NFp which received the service request is FFS.*

*Solution details updated for resolution.*

*Corrections in evaluation.*

# 4 Detailed proposal

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

#### 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.

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

If SCP reselects NFp, the NFc can still evaluate, if the new NFp is part of the same NF Set or NF Service Set. In case of reselection, the SCP should provide the identifier of the originally selected NF Service Producer to the new, reselected NF Service Producer, which then has to include in its response both, its own NFp\_CCA and the originally selected identifier received via SCP.

\*\*\*\*\*\*\* NEXT CHANGE

### 6.6.3 Evaluation

This solution provides an approach how an NF Service Consumer can authenticate NF Service Producer, from which NF Service Consumer receives a service response, as intended NF for Service Response in indirect communication without delegated discovery and with delegated discovery.

This solution introduces Client credentials assertion or alike also for the NF Service Producer, where the assertionincludes NFp Instance ID, NFc Instance ID, and a signature using the certificate of NFp.

In indirect communication without delegated discovery, by reusing existing HTTP custom headers, it can also cover the case when SCP reselects another NF as NF Service Producer.

This solution works with assumption that the discovery results from NRF to NF Service Consumer are protected to detect any harmful modification in the middle. And it also assumes that NRF will inform NF Service Consumer about which NF Service Producers are in the NF Set or NF Service Set and that SCP only re-selects another NF Service Producer within the NF Set or NF Service Set.

NFc can only trust NFp if there has been a direct possibility to verify NFp's authenticity. This is done by proposing an assertion token such as CCA to be also used by NFp.

In indirect communication with delegated discovery, this solution requires extension of CCA and/or X.509 Certificate of NF Service Producer to include NF type of NF Service Producer.

This solution is to address KI#1 which basically assumes that the SCP and NFp are compromised or at least the SCP is compromised. It can prevent such attack when NF and NRF are mutually authenticated using TLS over direct communication without SCP being present. This means this solution does not cover the following cases:

- Delegated Discovery, Model D,

- Model C when the NF Service Consumer communicates with NRF over indirect communication via SCP.

If no NF\_p is reachable, an SCP will send an error response. An NFc cannot distinguish whether such error response has been sent by a mis-operating or compromised SCP. This is also true without this solution.

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