**3GPP TSG-SA3 Meeting #108-e draft\_S3-221933-r1**

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

**Source:**  **Huawei, HiSilicon, Nokia, Nokia Shanghai Bell**

**Title:** **Resolving EN in solution #6**

**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 remove the following EN: Editor’s Note: How to assure by the NFc that the NFp is origianl NFp which received the service request is FFS by adding the CCA of NFc as input for the generation of CCA of NF Service Producer, the NFc could assure that the CCA of the NF Service Producer is received from the NFp which received the CCA of the NF Service Consumer.

# 4 Detailed proposal

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

#### 6.6.2.1 For indirect communication without delegated discovery procedure



Figure 6.6.2.1-1: With mutual authentication between NF and NRF at the transport layer

**Discovery of the NF Service Producer:**

0. When a NF Service Consumer discover a NF Servcie Producer for a service, NRF provides information of target NF set and candidate target NF instance IDs belonging to the target NF set.

The NF set information in the discovery response from NRF to NF consumer needs to be end to end integrity protected, by e.g. TLS or solution to Key Issue #5, so that the SCP cannot modify the NF set information in the discovery response.

**NF Service Consumer authorization:**

1-2. After mutual authentication between NF Service Consumer and NRF at the transport layer, the NF Service Consumer and NRF perform the "Access token request before service access" procedure. If the NF Service Consumer has already discovered the NF Service Producer, it can also perform the "Access token request for a specific NF Service Producer/NF Service Producer instance" procedure.

**Service Request:**

4. Among the candidates NF instances list, the NF Service Consumer may select an NF instance for a Service Request. And the NF Service Consumer keep the list of candidate NF instances and NF set for verification of expected Service Response.

After acquiring an access token from the NRF, a NF Service Consumer may send a Service Request to the SCP. The service request includes the access token and CCA of the NF Service Consumer.

The service request includes the 3gpp-Sbi-Routing-Binding header and/or 3gpp-Sbi-Discovery header in order to specify target NF Service Producer and/or target NF Set, so that the SCP is instructed to perform the NFp reselection within the scope of NF Set.

5. An SCP forward a Service Request to the NF Service Producer. If needed, the SCP may reselect another NF Service Producer belonging to the same NF set.

**Service Response:**

6-7. After receiving a Service Request, the NF Service Producer may verify the Service Request and may respond with a Service Response with CCA of the NF Service Producer. CCA of NF Service Producer includes NF instance ID of NF Service Producer and NF instance ID of NF Service Consumer.

8-9. When receiving a Service Response, the NF Service Consumer may verify whether the NF instances ID of NF Service Producer which sends the Service Response is in the list of candidate NF instances for the Service Request.

#### 6.6.2.2 For indirect communication with delegated discovery



Figure 6.6.2.2-1: for indirect communication with delegated discovery

1. The NF Service Consumer sends a service request to the SCP. The service request shall include NF service discovery factors such as target NF type and the NF Service Consumer's CCA as defined in clause 13.3.8.

2. The SCP may perform a NF discovery operation with the NRF using NF service discovery factors received in step 1.

3. (same with step 3 in subclause 13.4.1.3.2 TS33.501.) The SCP sends an access token request (Nnrf\_AccessToken\_Get Request) to the NRF. The access token request includes parameters as defined in clause 13.4.1.1. The access token request may include the NF Service Consumer's CCA if received in Step 1.

4. (same with step 4 in subclause 13.4.1.3.2 TS33.501.) The NRF authenticates the NF Service Consumer using one of the methods described in clause 13.3.1.2. If NF Service Consumer authentication is successful and the NF Service Consumer is authorized based on the NRF policy, the NRF issues an access token as described in clause 13.4.1.1. The NRF uses the NF Service Consumer instance ID as the subject of the access token.

5. (same with step 5 in subclause 13.4.1.3.2 TS33.501.) The NRF sends the access token to the SCP in an access token response (Nnrf\_AccessToken\_Get Response).

6. (same with step 6 in subclause 13.4.1.3.2 TS33.501.) The SCP sends the service request to the NF Service Producer. The service request includes an access token (i.e., received in Step 1, received in Step 5, or previously cached), and may include the NF Service Consumer's CCA if received in Step 1.

7. (same with step 7 in subclause 13.4.1.3.2 TS33.501.) The NF Service Producer authenticates the NF Service Consumer by one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1.

8. If the validation of the access token is successful, the NF Service Producer may respond with a Service Response with CCA of the NF Service Producer. CCA of NF Service Producer may include NF type and NF instance ID of NF Service Producer and NF instance ID of NF Service Consuer.

9. The SCP forwards the service response to the NF Service Consumer. The SCP may include the access token in the service response to NF Service Consumer for possible re-use in subsequent service requests.

10. When receiving a service response, the NF Service Consumer may verify whether the NF Service Producer belongs to the target NF type and authenticate NF Service Producer using CCA and X.509 certificate of the NF Service Producer, and may verify whether the CCA of the NF Service Consumer in the CCA of NF Service Producer is the same with the CCA of the NF Service Consumer sent in Step 1.

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 provides 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.

\*\*\* 2nd CHANGE \*\*\*

#### 6.6.2.3 Client credentials assertion of NF Service Producer

CCAs shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures based on JSON Web Signature (JWS) as described in RFC 7515 [45].

The CCA of NF Service Producer may include:

- the NF instance ID of the NF Service Producer;

- the NF set information of the NF Service Producer;

- the NF instance ID of the NF Service Consumer;

- The NF type of the NF Service Producer;

- The CCA of the NF Service Consumer received in the service request message;- A timestamp and an expiration time, and

The NF Service Consumer shall digitally sign the generated CCA based on its private key as described in RFC 7515 [45]. The signed CCA shall include one of the following fields:

- the X.509 URL (x5u) to refer to a resource for the X.509 public key certificate or certificate chain used for signing the client authentication assertion, or

- the X.509 Certificate Chain (x5c) include the X.509 public key certificate or certificate chain used for signing the client authentication assertion.

\*\*\* 3rd 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 a token alike also for the NF Service Producer. The assertion includes 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 reselect 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 the 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 cover the 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, but needs to be addressed.

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