**3GPP TSG-SA3 Meeting #108e *draft\_S3-221857-r1***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Key Issue 5 EN resolution solution 4**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***Resolution of editors note in solution 4 (KI5 on e2e integrity protection)***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*The following editor’s notes in solution 4 need resolution. The following is proposed and implemented in this pCR.*

Editor's Note: Backwards compatibility with Rel-16 NF producers supporting only existing CCA is ffs.

🡪 For backwards compatibility with Rel-16 a new resource name for Rel-18 API can be used. Text updated in -r1 to:

" NOTE: To avoid backward compatibility issues and allow to distinguish between releases, a new API URI with the respective release version can be used."

Editor's Note: If not the hash but the whole message or headers is included, impact on throughput needs to be considered and is ffs.

🡪 Transform into text: If not the hash but the whole message or header is included, impact on the throughput is expected.

Editor's note: It is ffs how the SCP can perform necessary message modifications, if the (hash of the) whole service request is included in CCA.

🡪 The assumption is that the SCP does not need to modify messages. This is already covered by the NOTE.

Editor's Note: CT4 feedback is needed on which headers are not subject to modification, mediation, or alteration by the SCP and can be delivered as is to the other far end of the indirect communication.

🡪 It is proposed to cover this by conclusion text (different pCR).

Editor's Note: It is ffs if a keyed hash is necessary and if yes how the key is obtained or derived.

🡪 Transformed into a NOTE: A keyed hash value not necessary, because the hash is signed digitally in the CCA.

🡪 By this, the last sentence in the evaluation part can be deleted.

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE*

6.4 Solution #4: Service request authenticity verification in indirect communication

6.4.1 Introduction

This solution addresses the KI#5.

6.4.2 Solution details

This solution allows the NF Service Producer to verify that a service request of the NF Service Consumer received via SCP has not been modified.

In case of CCA is used for authentication, the service request received by NRF or NF Service Producer can be verified as the one to be originally sent by the NF Service Consumer. This would guarantee that in indirect communication no intermediary can modify the service request unrecognized.

NOTE: To avoid backward compatibility issues and allow to distinguish between releases, a new API URI with the respective release version can be used.

For this, the CCA is enhanced with a new payload value for 'service request verification' and a protected header list.

- The 'service request verification' (SRV) includes the service request message (or a hash of it) as one of the payload values. If not the hash but the whole message or header is included, impact on the throughput is expected.

- The protected header list (HL) includes custom headers that shall be integrity protected and thus not be modifiable undetected by SCP.

If present, the NF Service Producer or the NRF can verify whether these data included in the CCA are matching the service request as sent by the NF Service Consumer. I.e. the NF Service Producer verifies that the data included in the payload is matching the service request received together with the CCA. The receiver also verifies that the headers in the protected header list are not modified.

Since CCA is digitally signed by the NF Service Consumer, thus the recipient can verify that the service request received from SCP is the original one as provided by the NF Service Consumer. The additional SRV payload provides authenticity of the service request.

NOTE: This solution assumes that an SCP does not need to modify service request details for providing its service of delegated discovery and access token request to NRF or transferring a service request to the NF Service Producer. If there are headers that need to be modified by SCP/Proxy, then those headers cannot be considered as payload of SRV. The NF Service Consumer provides in this case a separate list of headers (HL) to explicitly state what is covered under SRV. The destination endpoint (NRF or NF) can take them in consideration while verifying the received data.

In detail:

- NF Service Consumer creates a service request and creates a keyed hash value about those parts of the service request, that are not to be modifiable by the SCP, and generates CCA including a 'service request verification' (SRV) payload with the keyed hash value. If necessary, a protected HL is included.

NOTE: A keyed hash value is not necessary, because the hash is signed digitally in the CCA.

- NRF, after verifying the authenticity of NF Service Consumer by checking the CCA, it checks SRV, i.e. it verifies the authenticity of the service request by creating a hash of the service request and comparing it with the received SRV value. It also verifies that the headers in the protected HL are not modified.

- NF Service Producer, after receiving an access token and CCA/SRV from the SCP, it verifies the NF Service Consumer by checking the CCA, it checks whether the NF instance id for which the access token was provided, matches the identity in CCA and it verifies the authenticity of the service request by creating a hash of the service request and comparing it with the received SRV value. It also verifies that the headers in the protected HL are not modified.

6.4.3 Evaluation

This solution provides an approach how an NF Service Producer can verify that a service request of the NF Service Consumer received via SCP has not been modified.

This solution extends Client credentials assertion to include new payload value for service request verification and a protected header list.

When the service request verification includes whole service request message, which may double the size of the message and may impact on system throughput.

When the service request verification includes hash value of service request message, additional information should be transmitted to the NF Service Producer to inform HTTP headers and order among HTTP headers which should be considered in calculation of hash value.

When SCP appends HTTP standard header(s) such as Via header and Authenticate header, in this solution, NF Service Producer cannot recognize those headers should not be considered in calculation of hash as those are added by SCP and NF Service Producer will fail to calculate correct hash value of HTTP message.

*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE*