**3GPP TSG-SA3 Meeting #108e *draft\_S3-221856-r1***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI4 conclusion on authorization of SCP to act on behalf of another SCP**

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

**Agenda Item: 5.24**

# 1 Decision/action requested

***Conclusion on key issue #4 on authorization of SCP to act on behalf of another SCP.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

# 4 Detailed proposal

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

*\*\* under 7. Conclusions*

7.4 KI#4: Authorization of SCP to act on behalf of an NF or another SCP

7.4.1 Analysis

One of the main 5G security features is the usage of OAuth 2.0 to authorize service requests. In indirect communication scenarios, however, an SCP is not explicitly authorized, it could request a service or a token without the knowledge of the NF Service Consumer (NFc).

2 solutions (Sol#2 and Sol#3) have been proposed, mandating the usage of CCA, by which the NFc can at least "implicitly authorize" the SCP. This achieves a minimum level of trust, but cannot avoid the threat described in clause 5.4.2 within the validity time of the CCA, i.e. that "SCP can send a service request and receive a valid service response on behalf of NF Service Consumer", even though the NF Service Consumer has not authorized the SCP”. Thus, CCA validity time need to be chosen very carefully to minimize this possibility.

Solution #3 argues that existing mechanisms are sufficient: a NF sending a request (with its CCA) to SCP, implicitly authorises SCP against NRF to process this request. The limit of this solution is that the CCA can be stolen or misused and, without NFc having requested a service, NRF could provide an access token to SCP or NFp could provide a service to SCP.

Solution #2 proposes to include the SCP identifier (i.e., either SCP Instance and/or Domain info) in the CCA generated by the NF Service Consumer. Thus, only the SCP, which SCP Identifier is included in the CCA from NFc is able to get a response from NRF to its request. This ensures that the CCA cannot be misused by a MitM and thus achieves an additional level of trust, when the CCA is more than once usuable. This however comes with a trade-off, since it impacts existing implementation (CCA generation by NFc and NRF handling of CCA). Further, if more than one SCP is in the path, with this solution SCP needs to create its own CCA including the SCP identifier from the requesting SCP in order to keep the chain of trust.

A conclusion to this key issue therefore needs to weight the level of security and trust achieved against the impact of suggested enhancements to the current release.

Another aspect, which requires further analysis is whether explicit authorization of the SCP would be needed. NRF can only authorize NFs. NRF neds to trust that any request forwarded by SCP was initiated by a NFc. Thus, in general only implicit authorization of SCP by the NF Service Consumer is possible with the current solutions proposals based on CCA.

In summary, whether an explicit mean to authorize a standalone SCP is needed has been debated.

Different views exist. If the SCP is standalone, it would serve several NFs. SCP needs to request access tokens for many different NFs and and distribute service responses to several different NF Service Consumers. Solution #2 provides an additional level of security.

Whether to go for Sol#2 or Sol#3 is a trade of between security enhancement versus complexity added. If CCA is supported, the optional inclusion of an SCP identifier (SCP instance or SCP domain identifier) in the CCA is recommended, to allow NRF to authenticate SCP as the one (or as part of the SCP domain) selected by the NF Service Consumer. In addition, secure transport and storage security can be applied where CCAs are stored and transported.

7.4.2 Conclusion

It is concluded that CCA can optionally include the SCP instance or SCP domain identifier, if available. Normative updates are needed.

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