**3GPP TSG-SA3 Meeting #108e *draft\_S3-221848-r3***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: EN resolution in KI1 - threat clarification**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***EN resolution in KI1 - threat clarification and editorial updates.***

# 2 References

[1] 3GPP TS 33.875

# 3 Rationale

*The EN on detailing the threats is resolved. Editorial changes in the key issue details are proposed.*

# 4 Detailed proposal

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

5.1 Key issue #1: Authentication of NRF and NF Service Producer by the NF Service Consumer in indirect communication

5.1.1 Key issue details

When SCP is present, the TLS between an NF Service Consumer and NRF/NF Service Producer can be split into at least two segments (NFc-SCP, SCP-NRF or SCP-NFp). In this case, the NF Service Consumer (NFc) and NRF or NFc and NF Service Producer (NFp) do not directly authenticate each other via TLS.

Client Credentials Assertion (CCA) has been specified to allow NRF or another NF to directly authenticate an NF Service Consumer in the presence of an SCP, but direct authentication of the NRF or NF Service Producer by the NF Service Consumer has not been addressed in indirect communication. The key issue will investigate solutions allowing the NF Service Consumer to directly authenticate the NRF/NF Service Producer in indirect communication.

NOTE: It needs to be taken into account that producer reselection by SCP can be a desired feature.

5.1.2 Security threats

The request by the NF Service Consumer could be forwarded by SCP to an unintended NF.

The request by the NF Service Consumer could be forwarded within the validity of an authorization token more than one request could be sent to the same NF, which could result in a deny of service attack. In indirect communication scenarios an NF Service Consumer cannot verify whether the service response was sent by a legitimate NF or NRF. NFc can only authenticates the SCP, but not NFp or NRF. Thus, an NF Service Consumer could receive service responses from an unintended NF.

5.1.3 Potential security requirements

The 5GS should provide a mechanism that allows an NF Service Consumer to authenticate an NRF or an NF Service Producer during an indirect communication with them via an SCP.

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