**3GPP TSG-SA3 Meeting #108e *draft\_S3-222806-r3***

**e-meeting, 10 – 14 October 2022 was *draft\_S3-221851-r2***

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI1 analysis on NFp authentication in indirect communication**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

*Proposal for KI#1 conclusion on NFp authentication in indirect communication.*

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

Even if not all cases can be covered, it appears as an improvement to allow the optional inclusion of a token such as CCA for the producer side such that a NF Service Consumer would have the option to validate if the NF sending the response is the producer that NFc has selected by itself or if it is a producer of the same NF Set or NF Service Set as indicated in the OAuth token received from NRF.

Analysis is proposed along these lines.

# 4 Detailed proposal

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

*\*\*\*\* in clause 7 Conclusions*

## 7.1 KI#1: Authentication of NRF and NF Service Producer in indirect communication

### 7.1.1 Analysis

The key issue addresses the scenario of an intermediary such as a standalone SCP to be compromised. In this case, the NF Service Consumer is not able to verify if the NRF response or the NF Service Producer response has been received by a legitimate entity. However, it also needs to be considered that reselection of the NF Producer by the SCP can be a desired feature.

3 solutions are presented to cover this key issue.

Solution #1 and extended solution #6 are based on using the concept of CCA for the NF Service Producer or the SCP, i.e., similar to the CCA used for the NF Service Consumer as specified in 3GPP TS 33.501 [2]. Such a token is introduced to allow a client to validate the sender of a response directly, even if an SCP is in between.

Solution #1 has a limited scope as provided in the respective evaluation part in clause 6.1.

Solution #6 superseeds solution #1, overcoming some of the limits of solution#1 in case of Model C, also addressing the scenario of reselection of the target NF.

The optional inclusion of such a token including a NF Set Id allows a NF Service Consumer to validate if the NF sending the response is the producer that NFc has selected by itself or if it is a producer of the same NF Set or NF Service Set as indicated in the OAuth token received from NRF. The token cannot be used, if SCP has applied reselection of NFp outside of an NF Set.

Solution #6 addresses Model C with direct TLS between NF consumer and NRF for discovery. It does not address Model D or Model C without direct TLS between NF consumer and NRF for discovery. It requires that the NF Service Consumer has knowledge about which NF Service Producers are in the NF Set of the producer.

Editor's Note: Solution #13 analysis is FFS.

Editor's Note: FFS how to address the following questions: what should the NFc do if the response comes from another entity than the intended producer.  Should the NFc assume that the SCP has reselected the producer and accept the response? Or should the NFc reject the response?

Editor's Note: It needs to be clarified what are the cases of compromised SCP and whether they are addressed by the proposed solutions.

### 7.1.2 Conclusion

TBD

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