**3GPP TSG-SA3 Meeting #103-e *S3-211766***

**e-meeting, 17 - 28 May 2021**

**Source:** **Ericsson**

**Title: Evaluation of Solution #3 "Using existing procedures for authorization of SCP to act on behalf of an NF Consumer"**

**Document for: Approval**

**Agenda Item: 5.20**

# 1 Decision/action requested

***It is proposed to approve the below pCR to TR 33.875 [1]***

# 2 References

[1] 3GPP TR 33.875 "Study on enhanced security aspects of the 5G Service Based Architecture (SBA)" Release 17

# 3 Rationale

Solution #3 "Using existing procedures for authorization of SCP to act on behalf of an NF Consumer" currently does not have an evaluation.

# 4 Detailed proposal

\*\*\*\*\*\*BEGIN CHANGES\*\*\*\*\*

### 6.3.3 Evaluation

The solution addresses the threats and requirements of Key issue #4: Authorization of SCP to act on behalf of an NF or another SCP.

The solution relies on token-based authorization and CCAs as currently specified in TS 33.501 [2].

It proposes that authorization of the SCP by the CCA is implicit by sending the CCA to the SCP,.i.e. by proof of possession of CCA\_NFc, the SCP is authorized to act on behalf of an NF Service Consumer and to request access tokens. However, authorization is not explicitly stated in the CCA.

Further, the TLS connection established between NFc and SCP only mutually authenticates NFc and SCP as it mutually authenticates SCP and NRF. The CCA\_NFc sent to SCP allows SCP to authenticate the originator of the service request (NFc) against NRF, but it does not authorize SCP to contact NRF and requesting an access token on behalf of NFc.

The fact that SCP is in possession of CCA of the NF Service Consumer does not mean that NF Service Consumer has authorized that particular SCP.

NRF or NF Service Producer cannot with assurity verify that the SCP which provides the CCA of the NF Service Consumer is indeed the one SCP to which the NF Service Consumer sent its CCA. Thus, this solution does not counter a potential attack of SCP stealing a CCA and using it for requesting an access token without being requested by a NF Service Consumer.

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