**3GPP TSG-SA3 Meeting #104-e draft\_*S3-212931-r1***

**e-meeting, 16 - 27 August 2021**

**Source:** **Samsung**

**Title:** **Evaluation for solution 5**

**Document for: Approval**

**Agenda Item:** **5.20**

# 1 Decision/action requested

***The contribution proposes to add evaluation to solution 5***

# 2 References

[1] TR 33.875 v020 Study on enhanced security aspects of the 5G Service Based Architecture (SBA)

# 3 Detailed proposal

It is suggested to approve the following changes.

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

## 6.5 Solution #5: End-to-end integrity protection of HTTP body and method

### 6.5.1 Introduction

This solution addresses the key issue #5 (End-to-end integrity protection of HTTP messages).

The core steps of this solution are:

- Use Client credentials assertions (CCAs) based authentication as specified in TS 33.501 [2] Clause 13.3.8 for NF-NRF or/and NF-NF communication.

- Enhance the Client credentials assertions (CCAs) to include a hash of the HTTP body and HTTP method to protect the message itself.

- The receiving node (NRF or NF producer) computes the hash of the HTTP body and HTTP method and validates that it is identical to the hash received in the Client credentials assertions (CCAs).

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

Editor's Note: This solution has dependency on CT4 feedback on what SCP exactly needs to modify.

### 6.5.2 Solution details



Figure 6.5.2-1 CCA based Authentication with HTTP hash enhancement

1. NF service consumer sends a service request including a signed Client credentials assertion (CCA) token to authenticate against NF service producer or NRF as described in TS 33.501 [2] Clause 13.3.8. But for this solution it is also proposed to add an optional field in CCA to protect the part of the message itself. The added field is a hash of HTTP body and HTTP method.

2. NF service producer or NRF validates the CCA as described in 3GPP 33.501 Clause 13.3.8.3. But since one optional field is supposed to be added to the CCA, the receiving end point (NF service producer or NRF) also needs to compute the hash of the HTTP body and HTTP method and validates that it is identical to the hash received in the Client credentials assertion.

The details of the hash are proposed to be specified as following:

For computation of the hash of the HTTP body and HTTP method for inclusion into the Client credential assertion, the input S to the KDF specified in Annex B of 3GPP TS 33.220 [4] is computed as follows:

 - P0 = HTTP body;

- L0 = length of the HTTP body;

- P1 = HTTP method;

- L1 = length of HTTP method.

The input key KEY is equal to null. Note that the FC value will be allocated in the normative phase.

### 6.5.3 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 hash value of HTTP body and HTTP methods.

This solution does not handle integrity protection of HTTP headers.

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