**3GPP TSG-SA3 Meeting #108e *S3-222247-r1***

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

**Source: CableLabs**

**Title: Selective End of End Protection of HTTP Request and Response in Indirect Communication**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***It is requested to approve the pCR.***

# 2 References

[1] 3GPP TR 33.875. Study on Security aspects for 5G Service Based Architecture (SBA)

# 3 Rationale

This pCR proposes a solution for KI#5 in TR 33.875. It allows an NF to verify the integrity of selected attributes in a service request or response consumer.

Instead of protecting the integrity of entire request or response, which has impact on the functioning of SCP based on the feedback from CT, this solution proposes to protect only selected fields that are considered critical and should not be modified by any intermediate entities such as SCP.

Further, to avoid complexity of signalling which attributes are to be integrity protected inline request or response, this solution proposes to use static configuration to indicate which attributes require integrity protection.

# 4 Detailed proposal

## 6.Y Solution #Y: Selective End of End Protection of HTTP Request and Response in Indirect Communication

### 6.Y.1 Introduction

This solution addresses KI#5.

It allows an NF to verify the integrity of selected attributes in a service request or response consumer. It requires the use of CCA and Server Credential Assertion (SCA) so that a recipient NF has access to the public key certificate of a sending NF. The solution does not propose any change to CCA or SCA.

Instead of protecting the integrity of entire request or response, which has impact on the functioning of SCP based on the feedback from CT, this solution proposes to protect only selected fields in a request or response that are considered critical and should not be modified by any intermediate entities such as SCP. Note there is a trade-off. The more of the message is protected, the fewer attacks are possible, but there is also a higher risk that the SCP may need to modify integrity protected parts of the message.

Further, to avoid complexity of signalling which attributes are to be integrity protected inline request or response, this solution proposes to use static configuration to indicate which attributes require integrity protection.

### 6.Y.2 Solution details

Each NF, either NF Service Consumer or NF Service Producer, is provided with a static integrity protection policy, describing which attributes or information elements within a service request or service response require integrity protection. For example, AUSF and UDM may be configured with the security policy requiring the integrity protection of authentication method, and authentication vector.

Based on the security policy, an NF creates one (or more) JWT tokens for the information elements in a service request or service response that require integrity protection. The JWT token is digitally signed by the private key of the NF. The JWT token may be included in an information element in a service request or service response, or in an HTTP header.

The public key certificate of the sending NF that is required to verify a received JWT token is communicated to a receipt NF in CCA or SCA.

When a recipient NF receives a service request or service response, it checks its security policy to see if any information elements in the received service request or service response require integrity protection. If yes, it extracts and verifies the JWT token to ensure that protected information elements have not been tampered with.

Editor’s Note: how to mitigate replay of a JWT token is FFS.

### 6.Y.3 Evaluation

TBD