**3GPP TSG-SA3 Meeting #108e *S3-221904-r2***

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

**Source: CableLabs, Nokia, Nokia Shanghai Bell**

**Title: Authentication of NF Producer 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#1 in TR 33.875 to allow an NF consumer to authenticate NF producer in indirect communication before the NF consumer sends its service request to the NF producer. Since a service request may contain sensitive information, e.g., SUPI, it is important for the authentication of NF producer to occur before the an actual service request being sent to the producer.

This property is consistent with HTTPS/TLS in which a client certificate with client information is sent to the server only after the authentication of a server certificate, and an HTTPS request is sent to the server only after the authentication of the server in TLS.

# 4 Detailed proposal

## 6.Y Solution #Y: Authentication of NF Service Producer in Indirect Communication

### 6.Y.1 Introduction

This solution addresses KI#1.

This solution proposes a simple authentication procedure which allows an NF service consumer or any other entity (e.g., an delegated SCP) to authenticate an NF service producer before sending an actual service request. This ensures that an actual service request with request parameters, some of which may be sensitive (e.g., SUPI), is only sent to an NF service producer that has already been authenticated.

This property is consistent with the behaviour of HTTPS/TLS in which a client certificate with client information is sent to the server only after the authentication of a server certificate, and an HTTPS request is sent to the server only after the authentication of the server in TLS.

This simple authentication procedure can be executed by an NF service consumer or by an SCP which has been delegated by an NF service consumer to perform service discovery and re-selection on its behalf.

### 6.Y.2 Solution details

A Client (e.g., an NF Service Consumer) first performs the service discovery to obtain information about an NF Service Producer (e.g., NF Service Producer Instance ID). Before the Client sends a service request to the NF Service Producer, it performs the following procedure to obtain a Server Credentials Assertion (SCA) from the producer. Similar to CCA, which allows to verify the identity of a consumer, SCA allows to verify the identity of the producer.

This procedure can be performed by an NF Service Consumer to verify the identity of an NRF or an NF Service Producer. For example, it can be performed to verify the identity of an NRF before an NF Service Consumer sends an access token request to an NRF.

In delegated discovery, this procedure can be performed by an NF Service Consumer before sending an actual service request. This procedure will trigger the SCP to perform the first service discovery and eventually return the SCA to the NF Service Consumer. Alternatively, if a delegated SCP is trusted by an NF Service Consumer to verify the identity of an NF Service Producer, an SCP will perform this procedure on the behalf of NF Service Consumer to verify the identity of an NF Service Producer before it forwards a service request from an NF Service Consumer to the NF Service Producer.

Editor’s Note: It is for further study whether the threats and security requirements are addressed if the SCP performs the procedure on behalf of the NF Service Consumer.

When a re-selection of an NF Service Producer is performed, this procedure can be re-performed against the newly selected NF Service Producer.

Editor’s Note: It is for further study whether re-performing the procedure after reselection addresses the key issue threats and requirements.



Figure 6.Y.2-1 Authentication Procedure for NF Service Producer in Indirect Communication

1. A client (e.g., an NF service consumer or an SCP) sends an HTTP request to a server (e.g., an NRF or an NF serviced producer) to obtain its Server Credentials Assertion (SCA). This HTTP request can be a simple HTTP Get request to a well-known resource (e.g., /SCA) or a service request (e.g., NFp\_SCA\_Get\_Request) without any requesting parameter. This ensures that no client information is exposed to the server in such request.

2. The SCP forwards the request (NFp\_SCA\_Get\_Request, or HTTP Get) to from the Client to the Server.

3. The Server (e.g. an NRF or an NF service producer) receives the request and generates Server Credential Assertion (SCA). The SCA has the same format as CCA and includes the identity of the server (e.g., NF service producer instance ID) and associated proof, which allows the verification of the server identity.

4. The Server sends the SCA in the response (e.g., NFp\_SCA\_Get\_Response or HTTP response) back to the SCP. The response may include an indicator to request for the CCA from the Client.

5. The SCP forwards the response including the SCA back to the Client.

6. The Client verifies the SCA cryptographically and then verifies the server identity (e.g., NF service producer Instanace ID) in the SCA against the corresponding identity of server where a service request is to be sent.

### 6.Y.3 Evaluation

TBD