**3GPP TSG-SA3 Meeting #119 S3-24XXXX**

Orlando, US 11 – 15 November 2024 *revision of S3-244931*

**Source: Nokia**

**Title: Update to KI2 Solution 13 on authentication aspect in CAPIF interconnect requesting security information from another CCF**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

*Update to Solution on authentication aspect in CAPIF interconnect requesting security information from another CCF*

# 2 References

[1] 3GPP TS 23.700-22

[2] 3GPP TS 33.700-22

# 3 Rationale

*Update to Solution on authentication aspect in CAPIF interconnect requesting security information from another CCF.*

*The NOTE in step 4 address the following EN*

Editor's Note: The need of the APIInvoker to provide the CCF address is ffs.

# 4 Detailed proposal

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

## 6.13 Solution #13: Requesting security information from another CCF in order to authenticate using TLS-PSK in CAPIF interconnect

### 6.13.1 Introduction

This solution is addressing KI#2 on security aspects for CAPIF interconnect, specifically the authentication aspect between API invoker and AEF if in different security domains.

### 6.13.2 Solution details

#### 6.13.2.1 Summary

CCF-B and API invoker have obtained the security method that allows to authenticate to the AEF, and any security information related to the security method TLS-PSK. Hence, CCF-B and API invoker can derive AEFPSK based on the AEF’s API service details.

AEF receives an Authentication Initiation Request from APIInvoker, which includes the CCF-B information where the API invoker is registered. AEF requests security information of API invoker from the CCF-A it is registered with, mentioning the APIInvokerID and the CCF-B Information. CCF-A forwards the APIInvokerID to CCF-B which responds to CCF-A with the AEFPSK, which is forwarded to AEF.

API invoker and AEF authenticate using AEFPSK with the knowledge that CCF-B confirmed the APIInvokerID information.

#### 6.13.2.2 Information flow

 

**Figure B.X.2.2-1: Information flow to allow authenticating API invoker to AEF in a different security domain**

Step 1: APIInvoker gets the AEF details using Obtains\_Security method from CCF-B

Step 2: Mutual authentication based on client and server certificates shall be established using TLS between the API invoker and the CCF-B.

Step 3: APIinvoker and CCF-B derives AEF-PSK based on TLS master key used in step 2.

Step 4: APIInvoker sends Authentication Initiation Request to AEF based on AEF details received in step 1 and CCF-B information.

NOTE X: The CCF-B information (address) is required so that CFF-A, when contacted by the AEF, can forward the Request Security information to the correct interconnected CCF (CCF-B). AEF needs to transmit CCF-B information to CCF-A to allow CCF-A to retrieve the PSK security information from CCF-B.

Step 5: AEF requests security information from CCF-A by passing the CCF-B’s information received in step 4 along with APIInvokerID.

Step 6,7: CCF-A based on CCF-B’s information received requests security information from CCF-B.

Step 8: CCF-B sends the response by providing AEF-PSK to CCF-A.

Step 9: CCF-A sends the response to AEF.

Step 10: AEF sends the Authentication Initiation Response to APIInvoker.

Step 11: TLS connection is established between APIInvoker and AEF using AEF-PSK.

Editor's Note: How to perform API invoker authentication using TLS-PKI is FFS.

### 6.13.3 Evaluation

TBD

The solution addresses the 1st requirement of KI#2 by enabling the AEF to request security information related to the security method TLS-PSK from the CCF-B via CCF-A based on the CCF-B’s information and the APIInvokerID. The AEF is registered with the CCF-A and the API invoker in onboard to the CCF-B.

The solution is providing a method for AEF in a second domain to verify the security information, e.g., AEFpsk, used by an API invoker from the first domain.

The solution introduces:

* minor changes in the communication between API Inovker and AEF.
* additional communication between interconnected CCFs to share security information.

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