**3GPP TSG-SA3 Meeting #119 S3-245239**

Orlando, US 11 – 15 November 2024 *revision of S3-244932*

**Source: Nokia**

**Title:** **Update to KI2 Solution 14 on Authentication in CAPIF interconnect when API invoker has not included CCF information**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

*Update to Solution on authentication aspect in CAPIF interconnect querying different CCFs*

# 2 References

[1] 3GPP TS 23.700-22

[2] 3GPP TS 33.700-22

# 3 Rationale

*Update to KI#2 solution on CAPIF interconnect needed. Aspect of querying different CCFs.*

*Evaluation has been provided.*

# 4 Detailed proposal

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

## 6.14 Solution #14: Authentication aspect in CAPIF interconnect when API invoker has not included CCF information

### 6.14.1 Introduction

This solution is addressing KI#2 on security aspects for CAPIF interconnect, specifically the authentication and authorization aspect between API invoker and AEF if in different security domains, when API invoker does not provide its CCF details. In this case, AEF needs to first query CCF(s) to gain the necessary security details for authentication with the API invoker.

An API invoker registered at CCF-B wants to authenticate to an AEF (registered at CCF-A) to consume its API services. CCF-B and CCF-A are associated. Hence it knows the security method of AEF to enable an API invoker to access the API service (via CAPIF-1/e). The solution describes how the AEF in one security domain and the API invoker in the other security domain are enabled to establish a security session using TLS-PSK in the interconnect case. Specifically, it is addressed how to handle the case if the Authentication Initiation Request from APIInvoker does not include the source CCF details towards the AEF.

### 6.14.2 Solution details

#### 6.14.2.1 Summary

Prior to the authentication, CCF-B and API invoker have obtained the security method TLS-PSK that allows to authenticate to the AEF, and any security information related to this security method. 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 and requests security information of API invoker from the CCF-A where it is registered, mentioning the APIInvokerID. AEF needs to request security information of the APIInvoker from CCF-B. However, if CCF-B is connected to multiple CCFs and the AEF associated to CCF-A has no knowledge yet, that the APIInvoker is associated to CCF-B, it first needs to send an APIInvoker ownership query to the CCFs it is collaborating with.

Hence, since CCF-A does not know the API invoker, CCF-A needs to find the correct CCF (CCF-B) first. It therefore forwards the APIInvokerID to all interconnected CCFs. One of these CCFs responds (i.e. CCF-B) by confirming that it possesses information about the APIInvokerID. CCF-A gets the APIInvoker information including the AEFPSK from CCF-B that confirmed about the knowledge of APIInvokerID information and authenticates the API invoker to AEF.

#### 6.14.2.2 Information flow



**Figure 6.14.2.2-1: Information flow to allow establishment of TLS-PSK in interconnect**

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 derive 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.

Step 5: AEF requests security information from CCF-A.

Step 6,7: CCF-A sends ApIInvokerID Ownership Query to all its interconnected CCFs (in the figure CCF-B and CCF-C).

Step 8: CCF-B responds to APIInvokerID Ownership Query request confirming that the APIInvokerID belongs to it.

Step 9: CCF-A requests the security information from CCF-B and optionally provides CCF-A ‘s information.

Step 10: CCF-B sends the response by providing AEF-PSK to CCF-A.

Step 11: CCF-A sends the response to AEF.

Step 12: AEF sends the Authentication Initiation Response to APIInvoker.

Step 13: TLS connection is established between APIInvoker and AEF using AEFPSK.

### 6.14.3 Evaluation

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 addresses the 1st requirement of KI#2 by enabling the AEF to gain security information for API invoker authentication through querying CCF(s) when API invoker does not provide its CCF details. In this case, AEF contacts the CCF-A it is registered with, CCF-A sends ApIInvokerID Ownership Query to all its interconnected CCFs. The CCF, to which the API Invoker belongs to responses (here CCF-B) and CCF-B onboard the API invoker responds security information related to TLS-PSK.

The CCF-A query is based on the API invoker ID received. Uniqueness of the API invoker ID in interconnection scenarios needs to be assured.

The solution introduces additional communication between interconnected CCFs to share security information.

Editor’s Note: Further evaluation is ffs.

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