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

Orlando, US 11 – 15 November 2024 *revision of*

**Source: Nokia**

**Title: KI5 Solution on Authenticating multiple API invokers of the same RO**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***Update to KI5 Solution on Authenticating multiple API invokers of the same RO***

# 2 References

[1] 3GPP TS 23.700-22

[2] 3GPP TS 33.700-22

# 3 Rationale

Key issue #5 of TR 33.700-22 addresses the security aspects of KI #2 in TR 29.700-22, i.e. how multiple API invokers can use one or more AEFs exposing resources related to the same Resource Owner (RO) providing the credentials. A solution was agreed in last meeting and is updated by this pCR.

In our understanding, webbrowser is a mediator and doesn’t have any processing capability. This should address the following EN.

Editor’s Note: How the solution works if ROF is web browser is ffs.

A Note to addressing the following EN has been added.

Addressing ENs.

# 4 Detailed proposal

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

### 6.X Solution: Authenticating multiple API invokers of the same RO

### 6.X.1 Introduction

This solution addresses KI#5 and is an optimization when the ROF is engaging multiple API invokers at the same UE. The ROF has a valid certificate received from the CCF which can be used for interaction between API invoker and AEF after API invoker/ROF interaction within the UE.

### 6.X.2 Solution Details

Any API Invoker of the UE that needs to get authenticated with AEF asks ROF to sign its API Invoker ID (using ROF private key). ROF provides the signd API Invoker ID with expiry time and certificate information.

When the API invoker starts the authentication process with AEF, a server-based TLS connection between AEF and API Invoker is established first. To authenticate the API invoker towards AEF, the API Invoker provides its plain API Invoker ID together with the ROF signed API Invoker ID which also includes the ROF certificate or a URI where the AEF can find the necessary details for validation.

The AEF validates the ROF certificate and validates if the plain API Invoker ID and the verified signed API Invoker ID. match. If not expired and on successful verification and match, AEF and API Invoker are authenticated.

NOTE: The solution provides a way for the ROF to give access only to its own resources to API Invokers under its control. The certificate chain of the ROF (which was issued by CCF) is enough for AEF to verify the legitimate of ROF. API Invoker Authorization to ROF resources is authomatically proven by the token.



Figure 6.X.2-1: Authentication using the ROF certificate

Alternatively, if the ROF has received a valid OpenID token during authentication between ROF and CCF, then the ROF can also provide to the API invoker the OpenID Token instead of the ROF certificate. The flow is illustrated below.



Figure 6.X.2-2: Authentication using OpenID token

Editor's Note: Not all API invokers should be be allowed to consume the resource owner data with same priority (e.g., duration/scope). So if all API invokers are going to be authenticated/authorized at once just because they are going to invoke services to access data of same resource owner, how individual authorization/data exposure of RO data works is FFS.

Editor's Note: How the ROF authenticates the API invokers and how the ROF authenticates with the CCF is FFS.

### 6.X.3 Evaluation

The solution addresses KI#5 by providing a way for the ROF to give access only to its own resources to API Invokers under its control. The certificate chain of the ROF (which was issued by CCF) is enough for AEF to verify the legitimate of ROF. API Invoker Authorization to ROF resources is authomatically proven by the token.In this solution, ROF is used to authenticate the API invoker for the CAPIF system.

The solution influences:

The behaviour of the API Invoker and ROF to generate the new token

The AEF to verify the new token type before allowing access.

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