**3GPP TSG-SA3 Meeting #119 S3-245234**

Orlando, US 11 – 15 November 2024 *revision of S3-244929*

**Source: Nokia**

**Title: Update to KI1.3 Solution 29 on scope enhancements for finer granular access**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***Update to KI1.3 Solution on scope enhancements for finer granular access***

# 2 References

[1] 3GPP TS 23.700-22

[2] 3GPP TS 33.700-22

# 3 Rationale

*KI1.3 requires solutions for finer granular access.*

*The following editor notes where addressed respectively by NOTE 1 and 2*

Editor's note: Granularity details to be added.

Editor's note: The inclusion of resource owner identifier is proposed to be a scope parameter which is creating a misalignment with Rel-18, where it is captured in a claim. FFS how to handle.

# 4 Detailed proposal

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

## 6.29 Solution #29: Enhancing authorization through finer granularity access token

### 6.29.1 Introduction

This solution is addressing KI#1.3 to enhance finer granularity authorization by reusing already existing mechanisms available in CAPIF ecosystems and is based on 23.700-22 Solution 9 as selected by conclusion. I.e. to support RNAA, the CCF checks whether the API invoker is permitted to access the requested service API based on the API invoker's subscription information and resource owner consent using more granular information about API invoker in the context of RNAA.

In short: A Resource Owner, registered to a CAPIF instance, wants to provide its consent to an API Invoker to access its own resources. In this context, the CCF and AEF should be able to correctly identify the owner of the resource and authorize the access request based on their knowledge.

### 6.29.2 Solution details

#### 6.29.2.1 Summary

The solution proposes a way to enhance current OAuth2 based authorization mechanisms, both at CCF and AEF, to allow a finer granularity access control.

NOTE 1: A finer granularity can include: Resource Owner ID, operations (e.g. retrieve, create, etc), features (e.g. feature 1, feature 2, etc) and resources (e.g. resource 1, resource 2, etc).

After authentication between the CCF and the API Invoker, the latter will include the required additional information to CCF during the Access token Request. The API Invoker will include in the scope parameter more authorization details that allow to distinguish both the resource owner and the resources that API Invoker intends to access. This will allow the CCF to verify if the resource owner allowed this specific API Invoker to access the requested resources.

When the verification is completed, the CCF will include the authorization details, with the new granularity, into the access token returned to the API Invoker.

The previously provided access token will allow the AEF to correctly authorize, or deny, the request by the mechanism already available to AEF. AEF must be able to verify the details for finer granularity access control.

NOTE 2: The inclusion of resource owner identifier is proposed to be a scope parameter while in Rel-18 RO id is part of claim. Granularity is not specified in Rel-18. The solution proposes that a Rel-19 RNAA token is including the RO id and granularity details in scope and leaving empty the Rel-18 resOwenrId. This allows to distinguish between Rel-19 and Rel-18. It is done by purpose to distinguish between RO id in claims in Rel-18 and to avoid backward compatibility problems.

.

#### 6.29.2.2 Information flow



1. CAPIF-1e authentication and secure session establishment is performed as specified in subclause 6.3.1 of 33.122.

2. After successful establishment of TLS session over CAPIF-1e, the API invoker shall send an Access Token Request message to the CAPIF core function with the enhanced scope.

NOTE 1: the enhanced scoped will include all the required additional details necessary for granular authorization, such as Resource owner ID, operation features and/or resources.

3. The CAPIF core function shall verify the Access Token Request message per OAuth 2.0 [4] specification, by verifying the required scope at the finer granularity required by the API Invoker.

4. The CAPIF core function shall generate an access token with the detailed scope containing finer granularity and return it in an Access Token Response message.

5. The API invoker authenticates to the AEF by establishing a TLS session with the API exposing function based on the choosed authentication method

6. With successful authentication to the AEF, the API invoker shall initiate invocation of a 3GPP northbound API with the AEF. The access token received from the CAPIF core shall be sent along with the northbound API invocation request as per OAuth 2.0 [4].

7. The API exposing function shall validate the access token. If validation of the access token is successful, the AEF shall verify the API invoker's Northbound API invocation request against the authorization claims in access token, ensuring that the API Invoker has access permission for the requested service API.

NOTE 2: the verification procedure should be enanched to verify the additional fields inserted in the access token from CCF.

8. After successful verification of the access token and authorization claims of the API invoker, the requested northbound API shall be invoked, and the appropriate response shall be returned to the API invoker.

### 6.29.3 Evaluation

The solution addresses the requirements of KI#1.3 by allowing to insert the required finer granularity as part of the token Request and the access token itself.

The solution affects:

* The API invoker, who will need to modify the access token request.
* The CCF which will need to understand the new fields and verify the perimission of the API invoker
* The AEF which will need to verify the new enhanced scope.

Editor's Note: Further evaluation is TBD.

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