**3GPP TSG-SA3 Meeting #121 S3-251232**

**Gothenburg, SWEDEN, 7 - 11 April 2025**

**Source: Nokia, Huawei**

**Title: Baseline pCR against Draft CR KI1.3 from pre-discussion on Finer level of authorization**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS/TR 33.122 / Living Draft CR S3-251231**

**Version: 3.122 v19.0.0**

**Work Item: CAPIF\_Ph3\_Sec**

**Comments**

Baseline pCR against draft CR S3-251231 (was S3-251114 from SA3#120)

\* \* \* First Change \* \* \* \*

## 6.Y Authorization for finer level service API access

Finer level service API access allows the CCF to limit service operations and customize the allowed resources (HTTP methods) per service operation.

Finer level of feature refers to the API feature and the possibility to authorize for a feature different granularities: e.g. the location API may provide course, medium or fine location. Another finer level of a feature can be the bundling of service operations.

Note: Feature level is determined by stage 3.

To enable finer level service API access, the access token request via CAPIF-2 includes the indication of the requested service and resources at the respective granularity. For RNAA, the request also includes the GPSI of the UE.

The CCF verifies the API invoker ID and the requested level of finer authorization granularity, if available. If verification was successful, CCF creates and sends an access token back to the API invoker including finer level authorization information.

NOTE 1: An an example for finer level granularity the access token can include: Resource Owner ID (if the API Invoker is part of the UE), operations (e.g. retrieve, create, etc), features (e.g. feature 1, feature 2, etc) and resources (e.g. resource 1, resource 2, etc).

\* \* \* Next Change \* \* \* \*

#### 6.5.3.1 General

The authorization function shall obtain the necessary permission from the resource owner for allowing the API invoker to access a northbound API.

The authorization function shall support finer level authorization as specified in TS 23.222 [X].

The ROF may support finer level authorization as specified in TS 23.222 [X].

RNAA shall use token-based authorization using OAuth 2.0 framework with the following roles:

- The API invoker has the role of the OAuth 2.0 client.

- The CCF has the role of the OAuth 2.0 authorization server, i.e., providing the access token used for RNAA.

- The AEF has the role of the resource server.

The access tokens used for RNAA shall contain the resource owner ID.

The resource owner may be the user of the UE or the owner of the subscription depending on the use case and regulations.The resource owner ID is specified as the GPSI of the corresponding UE if the resource is related to a UE.

NOTE: The present document does not specify the resource owner.

The access token shall include the resource owner ID and the API invoker ID. The resource owner ID is the GPSI. The API invoker ID binds the token to the API invoker. To avoid privacy issues, GPSI should be different from MSISDN, SUPI etc.

The AEF shall check if the token includes *resOwnerId* claim, which includes resource owner ID, to identify that it is a token used in RNAA.

AEF shall do the authorization check of the API invocation request for accessing the resources of the resource owner. AEF checks the request against the token, including:

1) checking the token integrity and

2) checking whether the GPSI (if present) in the API invocation request is compliant with the resource owner ID in the access token. As the token includes resource owner ID, there is no need for additional UE authentication in API invocation. Moreover, the token should be able to restrict the API invoker to a specific resource (e.g., location, QoS, PDN connectivity status) of the resource owner.

For OAuth 2.0 flows involving redirection, authentication between CCF/AUF and UE should be performed after API Invoker redirects the UE to CCF/AUF.

In case of an external AF (i.e., not the application on the UE) being the API invoker, for mutual authentication of API invoker AF and API exposing function, the authentication methods of clause 6.4 and clause 6.5.2 are reused.

For authorization, the following OAuth 2.0 flows may be used:

- Client credential flow (according to RFC 6749 [4]),

- Authorization code flow (according to RFC 6749 [4]), or

- Authorization code flow with PKCE (according to RFC 7636 [11]).

CCF shall indicate the selected flows to the API invoker.

CCF shall give service authorization which subscribers or users can use RNAA.

For selecting the authorization method, the procedure as specified in clause 6.3.1.2 is used with the following RNAA specific additions. The API invoker shall include in the Security Method Request the supported RNAA authorization flows. The CCF shall determine the RNAA authorization flow based on the RNAA capabilities of the CCF, AEF, and API invoker. The API invoker shall use the determined RNAA authorization flow in the subsequent communication with the CCF and AEF.

NOTE: In the present document, only a UE accessing its own resources is considered if the API invoker is on a UE.

\* \* \* End of Changes \* \* \* \*