**3GPP TSG-SA3 Meeting #121 S3-25xxxx**

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

**Source: <Your COMPANY NAME>**

**Title: Pseudo-CR on <Document TITLE>**

**Document for: Approval**

**Agenda item: x.x**

**Spec: 3GPP TS/TR <TS/TR number>**

**Version: <TS version>**

**Work Item: <Work Item>**

**Comments**

pCR to draft CR S3-251112 from SA3#120, updates in yellow

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

### 6.5.3 Authentication and authorization for RNAA

#### 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.

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.

Authorization information/authorization revocation information is transferred between the ROF and the CCF via secure CAPIF-8 reference point.

The resource owner is authenticated before being allowed to manage the resource owner authorization information.

The resource owner authenticates implicit by providing resource owner authorization information to the ROF, which allows ROF to authenticate towards the CCF.

Ressource owner authorization information / authorization revocation information is XXX…

NOTE: How to authenticate the resource owner is left to implementation.

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.

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

#### 6.5.3.B Resource owner authorization management

Editor’s Note: This clause will be updated to capture the security procedures for resource owner authorization management

Intro text about giving permission XXX

For the client credential flow, XXX

For the authorization code (or the optional PKCE) flow, the procedure and profiles are specified in clause 6.5.3.3. Furthermore, the authorization request sent through the CAPIF-8 includes the API invoker ID, i.e. the client ID as in RFC 6749 [4], clause 4.1. The authorization response sent through the CAPIF-8 includes the authorization code for the API invoker to obtain the access token from the CCF.

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