**3GPP TSG-SA3 Meeting #122 draft\_S3-252075-r1**

**Fukuoka, Japan, 19 – 23 May 2025 merger of S3-252075 and S3-252215**

**Source: Xiaomi, Nokia**

**Title: pCR against Living CR on Cross UE authorization**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS 33.122**

**Version: 19.0.0**

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

**Comments**

The key points of this contribution are list as follows.

* To support the cross UE authorization scenarios, this contribution changes the NOTE text into normative text.
* Since the checking depends on the authorization information provided by the resource owner, the statement “If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources.”is changed to “If the API invoker is on a UE and the authorization information provided by the resource owner relates to the same UE, the CCF shall check that the UE is accessing its own resources.”
* Last but not least, since the existing RNAA flows are reused to support cross UE authorization, the CIBA flow related EN is automatically resolved.

\* \* \* First 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.

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.

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

#### 6.5.3.2 Authorization using oauth client credential flow

If client credential flow is used for authorization of the API invoker by the AEF, the procedures in RFC 6749 [4] shall be followed with the following profile:

- The access token request message may include the resource owner ID.

NOTE 1: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

NOTE 2: The mapping of API Invoker ID and GPSI is left for stage 3.

- The CCF shall check whether the API invoker is entitled to consume the API and allowed to access the resources of the resource owner, by using authorization information available in the CCF.

- If the API invoker is on a UE and the authorization information provided by the resource owner relates to the same UE, the CCF shall check that the UE is accessing its own resources. The API invoker on one UE if attempts to access resources related to another UE the CCF will not check that the UE is accessing its own resources. To authorize the API invoker on one UE to access resources related to another UE via client credentials flow, the CCF authorizes the API invoker based on authorization information provided to the CCF.

If the API invoker is an AF not on a UE, the check is omitted.

NOTE 3: How to get the authorization from the resource owner and store it in the CCF is out of scope of the present document.

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

#### 6.5.3.3 Authorization using authorization code (optional PKCE) flow

If authorization code flow, optionally with PKCE, is used by the AEF for authorization of the API invoker, the procedures in RFC 6749 [4] and optionally RFC 7636 [11] shall be followed, with the following profile:

- The authorization token and/or authorization request may include the resource owner ID.

NOTE 1: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

NOTE 2: The mapping of API Invoker ID and GPSI is left for stage 3.

- The resource owner dynamically authorizes the API invoker to access the resource owner's resources as described in RFC 6749 [4] and optionally RFC 7636 [11].

- If the API invoker is on a UE and the authorization information provided by the resource owner relates to the same UE, the CCF shall check that the UE is accessing its own resources. The access token shall contain the resource owner ID (i.e., GPSI) and the API invoker ID. The API invoker on one UE if attempts to access resources related to another UE the CCF will not check that the UE is accessing its own resources. To authorize the API invoker on one UE to access resources related to another UE via authorization code (optional PKCE) flow, the CCF authorizes the API invoker based on authorization information provided beforehand by the resource owner and available at the execution time of issuing the authorization code. If the API invoker is an AF not on a UE, the check is omitted.

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