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

**Goteborg, Sweden, 7 – 11 April 2025**

**Source: Xiaomi**

**Title: Pseudo-CR on authorizing the API invoker on one UE to access resources related to another UE**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS 33.122**

**Version: 19.0.0**

**Work Item: CAPIF\_Ph3\_sec**

**Comments**

This contribution provides guidance for authorizing the API invoker on one UE to access resources related to another UE

\* \* \* Start of the 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, the CCF shall check that the UE is accessing its own resources. 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.

NOTE X: To authorize the API invoker on one UE to access resources related to another UE, the CCF authorizes the API invoker based on authorization information available in the CCF.

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

NOTE Y: To authorize the API invoker on one UE to access resources related to another UE, the CCF authorizes the API invoker based on authorization information provided by the resource owner.

\* \* \* End of the Change \* \* \* \*