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

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

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.122** | **CR** | ***draft*** | **rev** | **-** | **Current version:** | **18.4.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Draft CR for authorizing API invoker on one UE accessing resources related to another UE |
|  |  |
| ***Source to WG:*** | Xiaomi |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | CAPIF\_Ph3\_Sec |  | ***Date:*** | 2025-3-17 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | This draft CR provides mechanism for authorizing API invoker on one UE accessing resources related to another UE. |
|  |  |
| ***Summary of change:*** | Clauses 6.5.3.2 and 6.5.3.3 are updated to capture the security procedures of authorizing API invoker on one UE accessing resources related to another UE. |
|  |  |
| ***Consequences if not approved:*** | CAPIF cannot authorize API invoker on one UE accessing resources related to another UE.  |
|  |  |
| ***Clauses affected:*** | 6.5.3.2, 6.5.3.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

Start of 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.

Editor’s note: 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 2: 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 and the CCF will not check if the UE is accessing its own resources.

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

Editor's note: 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 and the CCF will not check if the UE is accessing its own resources.

End of Changes