**3GPP TSG-SA3 Meeting #115 *S3-240795-r1***

**Athens, February 26 - March 01, 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.122** | **CR** | **0071** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Resolve ENs related to API invoker ID mapping | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Xiaomi | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SNAAPPY | | | | |  | ***Date:*** | | | 2024-2-05 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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 can be 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:*** | | The Editor's Note " the mapping of API Invoker ID and GPSI is left for stage 3" is documented for providing the details on how CCF checks if the UE is accessing its own resources.  If the API invoker is on UE, the CCF can obtain the authenticated API invoker ID via existing mechanisms. Then the CCF can confirm the UE is accssing its own resources if the authenticated API invoker ID is idential to the resource owner ID (i.e. the GPSI of the UE).  Therefore, the aformentioned ENs can be resolved. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The ENs about " the mapping of API Invoker ID and GPSI is left for stage 3" are removed.  The following sentence "If the authenticated API invoker ID is identical to the resource owner ID (i.e. the GPSI of the UE), CCF can confirm that the UE is accessing its own resources." is captured to provide details on how CCF checks if the UE is accessing its own resources." | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The Editor's Note about API invoker ID mapping in RNAA scenarios is not resolved. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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 the 1st 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.

- 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 by considering the authenticated API invoker ID and the resource owner ID. If the API invoker is an AF not on a UE, the check is omitted.

Editor's Note: Further details of the token are left for stage 3, this includes how to differentiate RNAA and legacy tokens

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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the 2nd 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.

Editor’s Note: Whether and how the token and/or authorization request can include resource owner ID is left to stage 3.

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

- 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 by considering the authenticated API invoker ID and the resource owner ID.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.

Editor's Note: further details of the token are left for stage 3, this includes how to differentiate RNAA and legacy tokens

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