**3GPP TSG- WG3 Meeting #**

**Chicago, United States, 13 - 17 November, 2023 (revision of C3-235155)**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.222** | **CR** | **0313** | **rev** | **2** | **Current version:** | **18.3.0** |  |
|  |
| *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:***  | Update authorization obtaining part to support resource owner-aware northbound API access |
|  |  |
| ***Source to WG:*** | CT3 |
| ***Source to TSG:*** | Xiaomi |
|  |  |
| ***Work item code:*** | SNAAPP |  | ***Date:*** | 2023-11-3 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | As referring to clause 6.5.3.1 of TS 33.122, in resource owner-aware northbound API access (RNAA) scenarios, the access token shall include the resource owner ID.According to clause 6.5.3.2 of TS 33.122, to enable the API invoker to access the resources of a specific resource owner via client credentials flow, the token request may include the resource owner ID.However, currently, AccessTokenReq, AccessTokenRsp, and AccessTokenClaims data types in TS 29.222, which relate to the authorization flow, do not contain resource owner ID information. Currently, clause 5.6.2.3.2 of TS 29.222 only provides authorization procedure without involving UE ID checking. However, in RNAA scenarios, as described in clause 6.5.3.2 of TS 33.122, the CCF shall check that the UE is accessing its own resources if the API invoker is on a UE. Without updating the authorization part, the CAPIF cannot support the RNAA feature. |
|  |  |
| ***Summary of change:*** | Add the resource owner ID in the accesstokenreq and accesstokenresp data types.Add the requirement and methods of checking UE is accessing its own resources. |
|  |  |
| ***Consequences if not approved:*** | CAPIF cannot support the RNAA feature. |
|  |  |
| ***Clauses affected:*** | 5.6.2.3.2 |
|  |  |
|  | **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 requires a backward compatible feature in CAPIF\_Security\_API covered in TS29.22 CR#0312. |
|  |  |
| ***This CR's revision history:*** |  |

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

##### 5.6.2.3.2 Obtain authorization using Obtain\_Authorization service operation

To obtain authorization information from the CAPIF core function to invoke service APIs, the API invoker shall perform the functions of the resource owner, client and redirection endpoints as described in clause 6.5.2.3 of 3GPP TS 33.122 [16].

The API invoker shall send a POST request to the "Token Endpoint", as described in IETF RFC 6749 [23], clause 3.2. The "Token Endpoint" URI shall be:

{apiRoot}/capif-security/v1/securities/{securityId}/token

where {securityId} is the API invoker identifier and represents the "Individual trusted API invoker" resource created during obtain security method, as described in clause 5.6.2.2.

The body of the HTTP POST request shall indicate that the required OAuth2 grant must be of type "client\_credentials". The "scope" parameter (if present) shall include a list of AEF identifiers and its associated API names the API invoker is trying to access (i.e., the API invoker expected scope). If the request is sent for client credentials flow in RNAA scenarios, the request may include the resource owner ID (i.e. the GPSI as defined in clause 6.5.3.1 of TS 33.122 [16]).

The API invoker may use HTTP Basic authentication towards this endpoint, using the API invoker identifier as "username" and the onboarding secret as "password". Such username and password may be included in the header or body of the HTTP POST request.

On success, "200 OK" shall be returned. The payload body of the POST response shall contain the requested access token, the token type and the expiration time for the token. The access token shall be a JSON Web Token (JWT) as specified in IETF RFC 7519 [24]. The access token returned by the CAPIF core function shall include the claims encoded as a JSON object as specified in clause 8.5.4.2.8 and then digitally signed using JWS as specified in IETF RFC 7515 [25] and in Annex C.1 of 3GPP TS 33.122 [16].

The digitally signed access token shall be converted to the JWS Compact Serialization encoding as a string as specified in clause 7.1 of IETF RFC 7515 [25].

If the access token request fails at the CAPIF core function, the CAPIF core function shall return "400 Bad Request" status code, including a JSON object in the response payload, that includes details about the specific error that occurred.

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