**3GPP TSG- WG3 Meeting # *316***

**Xiamen, China, 9 - 13 October, 2023**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.222** | **CR** | **0312** | **rev** |  | **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:***  | Authorization code flow for resource owner-aware northbound API access |
|  |  |
| ***Source to WG:*** | CT3 |
| ***Source to TSG:*** | Xiaomi |
|  |  |
| ***Work item code:*** | SNAAPP |  | ***Date:*** | 2023-09-22 |
|  |  |  |  |  |
| ***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 6.5.3.3 of TS 33.122, in resource owner-aware northbound API access (RNAA) scenarios, the authorization code flow defined in clause 4.1 of RFC 6749 is reused. Therefore, the following enhancements should be adopted to support the authorization code flow.In RNAA scenarios, the resource owner client is introduced in the service architecture. However, in TS 29.222, the service architecture is not updated.In RNAA scenarios, the access token shall include the resource owner ID. However, in TS 29.222, the token does not contain the resource owner information.According to clause 6.5.3.3 of TS 33.122, the authorization code flow defined in clause 4.1 of RFC 6749 is reused. To enable the API invoker to access resources of a specific resource owner via authorization code flow, the API invoker needs to obtain the authorization code before requesting the access token. However, in TS 29.222, there is no existing authorization code realted service operation.Moreover, as described in clause 4.1 of RFC 6749, the API invoker needs to send the authorization code to the CAPIF core function when it requests the access token. However, in TS 29.222, there is no authorization code information in the token related service operation.This results in CAPIF not supporting the authorization code flow for RNAA.This contribution focuse on the parts other than that for obtaining the Authorization\_Code. |
|  |  |
| ***Summary of change:*** | Add the resource owner ID in the accesstokenreq and accesstokenresp data types.Add the authorization code in the accesstokenreq data type. |
|  |  |
| ***Consequences if not approved:*** | This results in CAPIF not supporting the authorization code flow for RNAA. |
|  |  |
| ***Clauses affected:*** | 4.2, 5.6.2, 8.5.2.3.4, 8.5.4.2 |
|  |  |
|  | **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's revision history:*** |  |

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

## 4.2 Service Architecture

3GPP TS 23.222 [2], clause 6 specifies the functional entities and domains of the functional model, which is depicted in Figure 4.2-1, in detail.



Figure 4.2-1: CAPIF Functional Model

CAPIF-1 and CAPIF-1e reference points connect an API invoker inside the PLMN Trust Domain and an API invoker outside the PLMN Trust Domain respectively, with the CAPIF core function.

CAPIF-2 and CAPIF-2e reference points connect an API invoker inside the PLMN Trust Domain and an API invoker outside the PLMN Trust Domain respectively, with the API exposing function.

CAPIF-3 reference point connects an API exposing function inside the PLMN Trust Domain with the CAPIF core function.

CAPIF-4 reference point connects an API publishing function inside the PLMN Trust Domain with the CAPIF core function.

CAPIF-5 reference point connects an API management function inside the PLMN Trust Domain with the CAPIF core function.

NOT 1E: The API exposing function, API publishing function and API management function are part the API provider domain which can be implemented by the Service Capability Exposure Function (SCEF) and/or the Network Exposure Function (NEF).

NOTE 2: The functional model described in this specification applies to both PLMN(s) and to SNPN(s).

3GPP TS 23.222 [2], clause 6 specifies functional model for the CAPIF to support 3rd party API providers, which is depicted in Figure 4.2-2 in detail



Figure 4.2-2: Functional model for the CAPIF to support 3rd party API providers

The CAPIF core function in the PLMN trust domain supports service APIs from both the PLMN trust domain and the 3rd party trust domain having business relationship with PLMN Trust Domain. The API invokers may exist within the PLMN trust domain, or within the 3rd party trust domain or outside of both the PLMN trust domain and the 3rd party trust domain.

CAPIF-3e reference point connects an API exposing function outside PLMN Trust Domain with the CAPIF core function.

CAPIF-4e reference point connects an API publishing function outside PLMN Trust Domain with the CAPIF core function.

CAPIF-5e reference point connects an API management function outside PLMN Trust Domain with the CAPIF core function.

CAPIF-7 and CAPIF-7e reference points connect API exposing functions within PLMN Trust Domain and outside PLMN Trust Domains respectively. 3GPP TS 23.222 [2] specifies functional model for interactions between API exposing functions.

NOTE: CAPIF-7 reference point is not represented in the Figure 4.2-2 which is aligning to TS 23.222 [2].

3GPP TS 23.222 [2], clause 6 specifies functional model to support CAPIF interconnection, which is depicted in Figure 4.2-3 in detail.



Figure 4.2-3: CAPIF interconnection functional model

CAPIF-6 and CAPIF-6e reference points connect two CAPIF core functions located in the same or different PLMN trust domains, respectively. The reference points allows API invokers of a CAPIF provider to utilize the service APIs from the 3rd party CAPIF provider or another CAPIF provider within trust domain.

Figure 4.2-4 shows the functional security architecture of CAPIF when Resource owner-aware northbound API access is supported. The authorization function itself is a part of the CCF. The Oauth client and the CCF shall communicate using https.



Figure 4.2-4: CAPIF supporting RNAA functional

Editor's note: the above figure will need alignment with SA3 and SA6.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next 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" or "authorization\_code". The grant type shall be set as " authorization\_code " when API invoker uses authorization code flow. The grant type shall be set as "client\_credentials" when API invoker uses client credentials flow.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 accessing resource of a specific resource ower via authorization code flow, the request shall include the authorization code.

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.

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

##### 8.5.4.2.6 Type: AccessTokenReq

Table 8.5.4.2.6-1: Definition of type AccessTokenReq

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| grant\_type | string | M | 1 | This IE shall contain the grant type as "client\_credentials" or "authorization\_code".The grant type shall be set as "authorization\_code" when API invoker uses authorization authorization code flow.The grant type shall be set as "client\_credentials" when API invoker uses client credentials flow.(NOTE 3, NOTE 4) |
| client\_id | string | M | 1 | This IE shall contain the API invoker Identifier.(NOTE 3) |
| client\_secret | string | O | 0..1 | This IE when present shall contain the onboarding secret which is got during API invoker onboarding.(NOTE 3) |
| scope | string | O | 0..1 | This IE when present shall contain a list of AEF identifiers and its associated API names for which the access\_token is authorized for use.It takes the format of 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZUsing delimeter "#" after the discriminator "3gpp", ":" after AEF identifier, "," between API names and ";" between the last API name of the previous AEF identifier and the next AEF identifier. (NOTE 2) Example: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'If the authorization code flow is selected, this IE when present may contain resource owner ID (i.e. the GPSI as defined in clause 6.5.3.1 of TS 33.122 [16]). |
| Authorization\_code | string | M | 1 | This IE when present shall contain authorization code. |
| NOTE 1: This data structure shall not be treated as a JSON object. It shall be treated as a key, value pair data structure to be encoded using x-www-urlencoded format as specified in clause 17.13.4.1 of W3C HTML 4.01 Specification [22].NOTE 2: The scope may contain more space-delimited strings which further add additional access ranges to the scope, the definition of those additional strings is out of the scope of the present document.NOTE 3: The "grant\_type", "client\_id" and "client\_secret" attributes do not follow the related naming convention defined in subclause 7.2.1. These attributes are however kept as currently defined in this specification for backward compatibility considerations.NOTE 4: The enumeration value "client\_credentials" of the "grant\_type" attribute does not follow the related naming convention defined in subclause 7.2.1. This enumeration is however kept as currently defined in this specification for backward compatibility considerations. |

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

##### 8.5.4.2.8 Type: AccessTokenClaims

Table 8.5.4.2.8-1: Definition of type AccessTokenClaims

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| iss | string | M | 1 | This IE shall contain the API invoker Identifier. |
| scope | string | M | 1 | This IE shall contain a list of AEF identifiers and its associated API names for which the access\_token is authorized for use.It takes the format of 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZUsing delimeter "#" after the discriminator "3gpp", ":" after AEF identifier, "," between API names and ";" between the last API name of the previous AEF identifier and the next AEF identifier. (NOTE)Example: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'If the authorization code flow is selected, this IE when present may contain resource owner ID (i.e. the GPSI as defined in clause 6.5.3.1 of TS 33.122). |
| exp | DurationSec | M | 1 | This IE shall contain the number of seconds after which the access\_token is considered to be expired. |
| NOTE: The scope may contain more space-delimited strings which further add additional access ranges to the scope, the definition of those additional strings is out of the scope of the present document. |

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