**3GPP TSG- WG3 Meeting # *317***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.222** | **CR** | **0313** | **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:*** | 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:*** | | | 2023-9-22 |
|  |  | | | |  | |  | | |  |
| ***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 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-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, 8.5.4.2.6, 8.5.4.2.7, and 8.5.4.2.8 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 accessing resource of a specific resource ower via client credentials flow, the request may include the resource owner ID (i.e. the GPSI as defined in clause 6.5.3.1 of TS 33.122).

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]. According to clause 6.5.3.2 of TS 33.122 [16], if the request is sent for accessing resource of a specific resource ower via client credentials flow, the CAPIF core function shall check that the UE is accessing its own resources when API invoker is on UE. In specific, the CAPIF core function shall authenticate the UE. If the authenticated UE ID cannot be mapped to the resource owner ID, the access token request fails. If the request sent by the API invoker does not contain the resource owner ID, the CAPIF core function generates the token including the resource owner ID for the API invokers, in which the resource owner ID is identical or can be mapped to the authenticated UE ID.

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"  (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,…apiNameZ  Using 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 client credentials 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]).  If the IE contains resource owner ID, the IE takes the format of 3gpp#resource owner ID 1,aefId1:apiName1,apiName2,…apiNameX; aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ  Example: '3gpp#Zhangsan@abc.com,aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management' |
| 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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 8.5.4.2.7 Type: AccessTokenRsp

Table 8.5.4.2.7-1: Definition of type AccessTokenRsp

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| access\_token | string | M | 1 | This IE shall contain JWS Compact Serialized representation of the JWS signed JSON object containing AccessTokenClaims (see clause 8.5.4.2.c).  (NOTE 2) |
| token\_type | string | M | 1 | This IE shall contain the token type (i.e. "Bearer").  (NOTE 2, NOTE 3) |
| expires\_in | DurationSec | M | 1 | This IE when present shall contain the number of seconds after which the access\_token is considered to be expired.  (NOTE 2) |
| 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,…apiNameZ  Using 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 1)  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 client credentials 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]). If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources.  If the IE contains resource owner ID, the IE takes the format of 3gpp#resource owner ID 1,aefId1:apiName1,apiName2,…apiNameX; aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ  Example: '3gpp#Zhangsan@abc.com,aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management' |
| NOTE 1: 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 2: The "access\_token", "token\_type" and "expires\_in" attributes do not follow the related naming convention defined in clause 7.2.1. These attributes are however kept as currently defined in this specification for backward compatibility considerations.  NOTE 3: The enumeration value "Bearer" of the "token\_type" attribute does not follow the related naming convention defined in clause 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,…apiNameZ  Using 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 client credentials 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]).  If the IE contains resource owner ID, the IE takes the format of 3gpp#resource owner ID 1,aefId1:apiName1,apiName2,…apiNameX; aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ  Example: '3gpp#Zhangsan@abc.com,aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management' |
| 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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*