**3GPP TSG CT WG3 Meeting #142 *C3-253xxx***

**Goteborg, SE, 25th – 29th August, 2025 was C3-253326**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **29.222** | **CR** | **0429** | **rev** | **1** | **Current version:** | **19.3.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Finer granularity API access control |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | CAPIF\_Ph3 |  | ***Date:*** | 2025-05-29 |
|  |  |  |  |  |
| ***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-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | The stage 2 requirements in SA6 and SA3 on the support of resource and operation level access control to service APIs has been finalized during the last plenary cycle. |
|  |  |
| ***Summary of change:*** | This CR proposes a generic solution to support resource and operation level access control with future extensibility enabling to support any other level of API access control that may be needed in the future. |
|  |  |
| ***Consequences if not approved:*** | * The support of resource and operation level access control to service APIs is not defined in stage 3.
 |
|  |  |
| ***Clauses affected:*** | 5.6.2.3.2, 8.5.4.1, 8.5.4.2.6, 8.5.4.2.7, 8.5.4.2.8, 8.5.4.3.2, 8.5.6, A.6 |
|  |  |
|  | **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 does not impact the OpenAPI descriptions of the APIs. |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* \* Start of changes \* \* \* \*

##### 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 shall be of type "client\_credentials", or when the "RNAA" feature is supported, either "client\_credentials" or "authorization\_code" (applicable for both the "authorization code" and "authorization code with PKCE" grant types).

For RNAA:

- if the "authorization code" grant type is used, the request shall include the resource owner ID and the authorization code and may include the redirection URI (see also IETF RFC 6749 [23] and clause 6.5.3 of TS 33.122 [16]); and

NOTE: When the "authorization code" grant type is used for RNAA, the authorization code is obtained by the API invoker prior to the invocation of this service operation using the procedures defined in clause 4.1 of IETF RFC 6749 [23].

- if the "client credentials" grant type is used, the request shall include the resource owner ID, as defined in clause 6.5.3.1 of TS 33.122 [16].

NOTE: When the "client credentials" grant type is used for RNAA, the CCF has to verify whether the API Invoker is authorized to invoke this service operation for acquiring a token to be subsequently used while accessing a protected resource of the resource owner identified by the resource owner ID.

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 content 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 content, that includes details about the specific error that occurred.

\* \* \* \* Next changes \* \* \* \*

#### 8.5.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.5.4.1-1 specifies the data types defined specifically for the CAPIF\_Security\_API service.

Table 8.5.4.1-1: CAPIF\_Security\_API specific Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Section defined | Description | Applicability |
| AccessTokenClaims | Clause 8.5.4.2.8 | Represents the claims data structure for the access token. |  |
| AccessTokenErr | Clause 8.5.4.2.9 | Represents an error in the access token request. |  |
| AccessTokenReq | Clause 8.5.4.2.6 | Represents the access token request information. |  |
| AccessTokenRsp | Clause 8.5.4.2.7 | Represents the access token response information. |  |
| Cause | Clause 8.5.4.3.3 | Indicates the cause for revoking the API invoker's authorization to the service API. |  |
| ResOwnerId | Clause 8.5.4.2.11 | Represents the identifier of the resource owner. | RNAA |
| SecurityInformation | Clause 8.5.4.2.3 | Represents the interface details and the security method. |  |
| SecurityNotification | Clause 8.5.4.2.5 | Represents the revoked authorization notification details. |  |
| ServiceSecurity | Clause 8.5.4.2.2 | Represents the details of the security method for each service API interface. When included by the API invoker, it shall indicate the preferred method of security. When included by the CAPIF core function, it shall indicate the security method to be used for the service API interface. |  |
| OAuthGrantType | Clause 8.5.4.3.4 | Represents the OAuth grant type. | RNAA |

Table 8.5.4.1-2 specifies data types re-used by the CAPIF\_Security\_API service-based interface:

Table 8.5.4.1-2: Re-used Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Reference | Comments | Applicability |
| DurationSec | 3GPP TS 29.122 [14] | Indicates the duration in seconds. |  |
| SecurityMethod | Clause 8.2.4.3.6 | Indicates the security method (e.g. PKI). |  |
| SupportedFeatures | 3GPP TS 29.571 [19] | Used to negotiate the applicability of optional features defined in table 8.5.6-1. |  |
| Uri | 3GPP TS 29.122 [14] | Represents a URI. | RNAA |

\* \* \* \* Next changes \* \* \* \*

##### 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 | Applicability |
| grant\_type | string | M | 1 | This attribute shall contain the grant type as "client\_credentials", or when the "RNAA" feature is supported, either "client\_credentials" or "authorization\_code".(NOTE 3, NOTE 4) |  |
| client\_id | string | M | 1 | This attribute shall contain the API invoker Identifier.(NOTE 3) |  |
| resOwnerId | ResOwnerId | O | 0..1 | Contains the identifier of the resource owner.This attribute shall be present only when the access token request is used for RNAA. | RNAA |
| client\_secret | string | O | 0..1 | This attribute when present shall contain the onboarding secret which is got during API invoker onboarding.(NOTE 3) |  |
| scope | string | O | 0..1 | Contains the requested OAuth2 scope..When the "CAPIF\_Ext1" feature is not supported, it takes the following format: 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZExample: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'When the "CAPIF\_Ext1" feature is supported, it takes the following format:'3gpp#aefId1:apiName1:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,apiName2:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,…apiNameX:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue;…aefIdN:apiName1:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,apiName2:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,…apiNameZ:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue'Example 1: '3gpp#aef1:3gpp-monitoring-event:res.subscriptions,3gpp-as-session-with-qos :res.subscriptions:op.create;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management:res.transactions:op.read'Example 2: '3gpp#aef1: 3gpp-time-sync:res.subscriptions:res.configurations:op.update,3gpp-mbs-session:res.mbs-sessions:res.subscriptions:op.create'With the following definitions:- The delimiter "#" shall be used only after the discriminator "3gpp" at the beginning of the scope field.- The delimiter ":" shall be used after the AEF identifier, after the API name and after each scope level.- The delimiter "," shall be used between API names of a certain AEF.- The delimiter ";" shall be used between the last API name of the one AEF section and the next AEF section.- Within the "aefId" field, the "apiName" field, the "scopeLevelType" field and "scopeLevelValue" field, the above defined delimiters are prohibited.- The "scopeLevelType" field shall be set to either "res" (for resource-level access control) or "op" (for operation-level access control).When the "CAPIF\_Ext2" feature is supported, the content of this attribute shall be set to a list of space-delimited strings, as defined in clause 3.3 of IETF RFC 6749 [23]. |  |
| authCode | string | C | 0..1 | Contains the authorization code.This attribute shall be included only when the access token request is used for RNAA and the OAuth "authorization code" grant type is used. | RNAA |
| redirect\_uri | string | O | 0..1 | Contains the redirection URI that was used to obtain the authorization code provided within the "authCode" attribute.This attribute may be included only when the access token request is used for RNAA and the OAuth "authorization code" grant type is used.(NOTE 3) | RNAA |
| 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: When the "CAPIF\_Ext1" feature is not supported, 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", "client\_secret" and "redirect\_uri" 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 in order to keep them aligned with corresponding claims defined in IETF RFC 6749 [23] and for backward compatibility considerations.NOTE 4: The enumeration value "client\_credentials" or "authorization\_code" of the "grant\_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 changes \* \* \* \*

##### 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 8.5.4.2.8).(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 | Contains the granted OAuth2 scope.When the "CAPIF\_Ext1" feature is not supported, it takes the following format:3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZExample: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'When the "CAPIF\_Ext1" feature is supported, it takes the following format:'3gpp#aefId1:apiName1:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,apiName2:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,…apiNameX:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue;…aefIdN:apiName1:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,apiName2:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,…apiNameZ:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue'Example 1: '3gpp#aef1:3gpp-monitoring-event:res.subscriptions,3gpp-as-session-with-qos :res.subscriptions:op.create;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management:res.transactions:op.read'Example 2: '3gpp#aef1: 3gpp-time-sync:res.subscriptions:res.configurations:op.update,3gpp-mbs-session:res.mbs-sessions:res.subscriptions:op.create'With the following definitions:- The delimiter "#" shall be used only after the discriminator "3gpp" at the beginning of the scope field.- The delimiter ":" shall be used after the AEF identifier, after the API name and after each scope level.- The delimiter "," shall be used between API names of a certain AEF.- The delimiter ";" shall be used between the last API name of the one AEF section and the next AEF section.- Within the "aefId" field, the "apiName" field, the "scopeLevelType" field and "scopeLevelValue" field, the above defined delimiters are prohibited.- The "scopeLevelType" field shall be set to either "res" (for resource-level access control) or "op" (for operation-level access control).When the "CAPIF\_Ext2" feature is supported, the content of this attribute shall be set to a list of space-delimited strings, as defined in clause 3.3 of IETF RFC 6749 [23]. |
| NOTE 1: When the "CAPIF\_Ext1" feature is not supported, 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 changes \* \* \* \*

##### 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 | Applicability |
| iss | string | M | 1 | This attribute shall contain the API invoker Identifier. |  |
| scope | string | M | 1 | Contains the OAuth2 scope.When the "CAPIF\_Ext1" feature is not supported, it takes the following format:3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZExample: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'When the "CAPIF\_Ext1" feature is supported, it takes the following format:'3gpp#aefId1:apiName1:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,apiName2:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,…apiNameX:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue;…aefIdN:apiName1:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,apiName2:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue,…apiNameZ:scopeLevelType.scopeLevelValue:scopeLevelType.scopeLevelValue:…:scopeLevelType.scopeLevelValue'Example 1: '3gpp#aef1:3gpp-monitoring-event:res.subscriptions,3gpp-as-session-with-qos :res.subscriptions:op.create;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management:res.transactions:op.read'Example 2: '3gpp#aef1: 3gpp-time-sync:res.subscriptions:res.configurations:op.update,3gpp-mbs-session:res.mbs-sessions:res.subscriptions:op.create'With the following definitions:- The delimiter "#" shall be used only after the discriminator "3gpp" at the beginning of the scope field.- The delimiter ":" shall be used after the AEF identifier, after the API name and after each scope level.- The delimiter "," shall be used between API names of a certain AEF.- The delimiter ";" shall be used between the last API name of the one AEF section and the next AEF section.- Within the "aefId" field, the "apiName" field, the "scopeLevelType" field and "scopeLevelValue" field, the above defined delimiters are prohibited.- The "scopeLevelType" field shall be set to either "res" (for resource-level access control) or "op" (for operation-level access control).When the "CAPIF\_Ext2" feature is supported, the content of this attribute shall be set to a list of space-delimited strings, as defined in clause 3.3 of IETF RFC 6749 [23]. |  |
| exp | DurationSec | M | 1 | This attribute shall contain the number of seconds after which the access\_token is considered to be expired as defined in clause 4.1.4 of IETF RFC 7519 [24]. |  |
| resOwnerId | ResOwnerId | O | 0..1 | Contains the identifier of the resource owner.This attribute shall be present only when the access token is used for RNAA. | RNAA |
| NOTE: When the "CAPIF\_Ext1" feature is not supported, 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. |

\* \* \* \* Next changes \* \* \* \*

### 8.5.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8. Table 8.5.6-1 lists the supported features for CAPIF\_Security\_API.

Table 8.5.6-1: Supported Features

|  |  |  |
| --- | --- | --- |
| **Feature number** | **Feature Name** | **Description** |
| 1 | Notification\_test\_event | Testing of notification connection is supported according to clause 7.6. |
| 2 | Notification\_websocket | The delivery of notifications over Websocket is supported according to clause 7.6. This feature requires that the Notification\_test\_event feature is also supported. |
| 3 | SecurityInfoPerAPI | Indicates the support of negotiating and obtaining service API security method information per API. |
| 4 | RNAA | Indicates the support of the RNAA functionality.This feature enables the following functionalities:- Support the OAuth grant types for RNAA.- Support to convey the authorization code in access token requests to support the "authorization code" grant type for RNAA.- Support to communicate the resource owner ID for RNAA access token requests/responses.- Support to communicate the new cause codes for AEF authorization revocation. |
| 5 | CAPIF\_Ext1 | Indicates the first set of enhancements to support the Rel-19 enhancements to the CAPIF functionalities.This feature enables the following functionalities:- Support finer-granularity API access control. |
| 5 | CAPIF\_Ext2 | Indicates the first set of enhancements to support the Rel-19 enhancements to the CAPIF functionalities.This feature enables the following functionalities:- Support generic string-based OAuth scope encoding based on clause 3.3 of IETF RFC 6749 [23]. |

\* \* \* \* End of changes \* \* \* \*