**3GPP TSG-CT WG3 Meeting #131 *C3-235155***

**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, 8.5.4.2.6, 8.5.4.2.8, 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 introduces a backward compatible feature in CAPIF\_Security\_API. |
|  |  |
| ***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.

 \* \* \* 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) |
| resource\_owner\_id | string | O | 1 | This IE shall contain the resource owner ID.(NOTE x) |
| 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' |
| 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.NOTE x: The resource\_owner\_id is only applicable to the RNAA feature. |

 \* \* \* 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' |
| exp | DurationSec | M | 1 | This IE shall contain the number of seconds after which the access\_token is considered to be expired. |
| resource\_owner\_id | string | O | 1 | This IE shall contain the resource owner ID. |
| 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.NOTEx: The resource\_owner\_id is only applicable to the RNAA feature. |

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

# A.6 CAPIF\_Security\_API

openapi: 3.0.0

info:

 title: CAPIF\_Security\_API

 description: |

 API for CAPIF security management.

 © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

 All rights reserved.

 version: "1.3.0-alpha.2"

externalDocs:

 description: 3GPP TS 29.222 V18.1.0 Common API Framework for 3GPP Northbound APIs

 url: https://www.3gpp.org/ftp/Specs/archive/29\_series/29.222/

servers:

 - url: '{apiRoot}/capif-security/v1'

 variables:

 apiRoot:

 default: https://example.com

 description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222.

paths:

 /trustedInvokers/{apiInvokerId}:

 get:

 parameters:

 - name: apiInvokerId

 in: path

 description: Identifier of an individual API invoker

 required: true

 schema:

 type: string

 - name: authenticationInfo

 in: query

 description: >

 When set to 'true', it indicates the CAPIF core function to send the

 authentication information of the API invoker. Set to false or omitted otherwise.

 schema:

 type: boolean

 - name: authorizationInfo

 in: query

 description: >

 When set to 'true', it indicates the CAPIF core function to send the

 authorization information of the API invoker. Set to false or omitted otherwise.

 schema:

 type: boolean

 responses:

 '200':

 description: >

 The security related information of the API Invoker based on the request

 from the API exposing function.

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/ServiceSecurity'

 '307':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/307'

 '308':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/308'

 '400':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/400'

 '401':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/401'

 '403':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/403'

 '404':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/404'

 '406':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/406'

 '414':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/414'

 '429':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29122\_CommonData.yaml#/components/responses/default'

 put:

 parameters:

 - name: apiInvokerId

 in: path

 description: Identifier of an individual API invoker

 required: true

 schema:

 type: string

 requestBody:

 description: create a security context for an API invoker

 required: true

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/ServiceSecurity'

 callbacks:

 notificationDestination:

 '{request.body#/notificationDestination}':

 post:

 requestBody:

 required: true

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/SecurityNotification'

 responses:

 '204':

 description: No Content (successful notification)

 '307':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/307'

 '308':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/308'

 '400':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/400'

 '401':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/401'

 '403':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/403'

 '404':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/404'

 '411':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/411'

 '413':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/413'

 '415':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/415'

 '429':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29122\_CommonData.yaml#/components/responses/default'

 responses:

 '201':

 description: Successful created.

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/ServiceSecurity'

 headers:

 Location:

 description: >

 Contains the URI of the newly created resource, according to the structure

 {apiRoot}/capif-security/v1/trustedInvokers/{apiInvokerId}

 required: true

 schema:

 type: string

 '400':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/400'

 '401':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/401'

 '403':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/403'

 '411':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/411'

 '413':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/413'

 '414':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/414'

 '415':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/415'

 '429':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29122\_CommonData.yaml#/components/responses/default'

 delete:

 parameters:

 - name: apiInvokerId

 in: path

 description: Identifier of an individual API invoker

 required: true

 schema:

 type: string

 responses:

 '204':

 description: No Content (Successful deletion of the existing subscription)

 '307':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/307'

 '308':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/308'

 '400':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/400'

 '401':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/401'

 '403':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/403'

 '404':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/404'

 '429':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29122\_CommonData.yaml#/components/responses/default'

 /trustedInvokers/{apiInvokerId}/update:

 post:

 parameters:

 - name: apiInvokerId

 in: path

 description: Identifier of an individual API invoker

 required: true

 schema:

 type: string

 requestBody:

 description: Update the security context (e.g. re-negotiate the security methods).

 required: true

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/ServiceSecurity'

 responses:

 '200':

 description: Successful updated.

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/ServiceSecurity'

 '307':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/307'

 '308':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/308'

 '400':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/400'

 '401':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/401'

 '403':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/403'

 '404':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/404'

 '411':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/411'

 '413':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/413'

 '415':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/415'

 '429':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29122\_CommonData.yaml#/components/responses/default'

 /trustedInvokers/{apiInvokerId}/delete:

 post:

 parameters:

 - name: apiInvokerId

 in: path

 description: Identifier of an individual API invoker

 required: true

 schema:

 type: string

 requestBody:

 description: Revoke the authorization of the API invoker for APIs.

 required: true

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/SecurityNotification'

 responses:

 '204':

 description: Successful revoked.

 '307':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/307'

 '308':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/308'

 '400':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/400'

 '401':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/401'

 '403':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/403'

 '404':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/404'

 '411':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/411'

 '413':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/413'

 '415':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/415'

 '429':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29122\_CommonData.yaml#/components/responses/default'

 /securities/{securityId}/token:

 post:

 parameters:

 - name: securityId

 in: path

 description: Identifier of an individual API invoker

 required: true

 schema:

 type: string

 requestBody:

 required: true

 content:

 application/x-www-form-urlencoded:

 schema:

 $ref: '#/components/schemas/AccessTokenReq'

 responses:

 '200':

 description: Successful Access Token Request

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/AccessTokenRsp'

 '307':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/307'

 '308':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/308'

 '400':

 description: Error in the Access Token Request

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/AccessTokenErr'

 '401':

 description: Unauthorized

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/AccessTokenErr'

 '403':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/403'

 '404':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/404'

 '411':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/411'

 '413':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/413'

 '415':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/415'

 '429':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29571\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29571\_CommonData.yaml#/components/responses/default'

components:

 schemas:

 ServiceSecurity:

 type: object

 description: >

 Represents the details of the security method for each service API interface.

 When included by the API invoker, it indicates the preferred method of security.

 When included by the CAPIF core function, it indicates the security method to be

 used for the service API interface.

 properties:

 securityInfo:

 type: array

 items:

 $ref: '#/components/schemas/SecurityInformation'

 minimum: 1

 notificationDestination:

 $ref: 'TS29122\_CommonData.yaml#/components/schemas/Uri'

 requestTestNotification:

 type: boolean

 description: >

 Set to true by API invoker to request the CAPIF core function to send a

 test notification as defined in in clause 7.6. Set to false or omitted otherwise.

 websockNotifConfig:

 $ref: 'TS29122\_CommonData.yaml#/components/schemas/WebsockNotifConfig'

 supportedFeatures:

 $ref: 'TS29571\_CommonData.yaml#/components/schemas/SupportedFeatures'

 required:

 - securityInfo

 - notificationDestination

 SecurityInformation:

 type: object

 description: Represents the interface details and the security method.

 properties:

 interfaceDetails:

 $ref: 'TS29222\_CAPIF\_Publish\_Service\_API.yaml#/components/schemas/InterfaceDescription'

 aefId:

 type: string

 description: Identifier of the API exposing function

 apiId:

 type: string

 description: API identifier

 prefSecurityMethods:

 type: array

 items:

 $ref: 'TS29222\_CAPIF\_Publish\_Service\_API.yaml#/components/schemas/SecurityMethod'

 minItems: 1

 description: Security methods preferred by the API invoker for the API interface.

 selSecurityMethod:

 $ref: 'TS29222\_CAPIF\_Publish\_Service\_API.yaml#/components/schemas/SecurityMethod'

 authenticationInfo:

 type: string

 description: Authentication related information

 authorizationInfo:

 type: string

 description: Authorization related information

 required:

 - prefSecurityMethods

 oneOf:

 - required: [interfaceDetails]

 - required: [aefId]

 SecurityNotification:

 type: object

 description: Represents the revoked authorization notification details.

 properties:

 apiInvokerId:

 type: string

 description: String identifying the API invoker assigned by the CAPIF core function.

 aefId:

 type: string

 description: String identifying the AEF.

 apiIds:

 type: array

 items:

 type: string

 minItems: 1

 description: Identifier of the service API

 cause:

 $ref: '#/components/schemas/Cause'

 required:

 - apiInvokerId

 - apiIds

 - cause

 AccessTokenReq:

 format: x-www-form-urlencoded

 description: Represents the access token request information.

 properties:

 grant\_type:

 type: string

 enum:

 - client\_credentials

 client\_id:

 type: string

 client\_secret:

 type: string

 resource\_owner\_id:

 type: string

 scope:

 type: string

 required:

 - grant\_type

 - client\_id

 AccessTokenRsp:

 type: object

 description: Represents the access token response information.

 properties:

 access\_token:

 type: string

 description: >

 JWS Compact Serialized representation of JWS signed JSON object (AccessTokenClaims)

 token\_type:

 type: string

 enum:

 - Bearer

 expires\_in:

 $ref: 'TS29122\_CommonData.yaml#/components/schemas/DurationSec'

 scope:

 type: string

 required:

 - access\_token

 - token\_type

 - expires\_in

 AccessTokenClaims:

 type: object

 description: Represents the claims data structure for the access token.

 properties:

 iss:

 type: string

 scope:

 type: string

 exp:

 $ref: 'TS29122\_CommonData.yaml#/components/schemas/DurationSec'

 resource\_owner\_id:

 type: string

 required:

 - iss

 - scope

 - exp

 AccessTokenErr:

 type: object

 description: Represents an error in the access token request.

 properties:

 error:

 type: string

 enum:

 - invalid\_request

 - invalid\_client

 - invalid\_grant

 - unauthorized\_client

 - unsupported\_grant\_type

 - invalid\_scope

 error\_description:

 type: string

 error\_uri:

 type: string

 required:

 - error

 Cause:

 anyOf:

 - type: string

 enum:

 - OVERLIMIT\_USAGE

 - UNEXPECTED\_REASON

 - type: string

 description: >

 This string provides forward-compatibility with future

 extensions to the enumeration but is not used to encode

 content defined in the present version of this API.

 description: |

 Indicates the cause for revoking the API invoker's authorization to the service API.

 Possible values are:

 - OVERLIMIT\_USAGE:

 The revocation of the authorization of the API invoker is due to the overlimit

 usage of the service API

 - UNEXPECTED\_REASON:

 The revocation of the authorization of the API invoker is due to unexpected reason.

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