**3GPP TSG CT WG3 Meeting #135 *C3-243542***

**Hyderabad, IN, 27 - 31 May, 2024** *(Revision of C3-243169)*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.3* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.222** | **CR** | **0350** | **rev** | **1** | **Current version:** | **18.5.0** |  |
|  | | | | | | | | |
| *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:*** | API Invoker authorization | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | CT3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SNAAPP | | | | |  | ***Date:*** | | | 2024-05-20 |
|  |  | | | |  | |  | | |  |
| ***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-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)  Rel-20 (Release 20)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The Clause 8.23.3 of TS 23.222, specifies the information elements in Revoke API Invoker Authorization request message. Cause value is included in this request message indicating the cause for revoking the authorization. However, it is not clear on the behaviour of the CCF with the presence of cause value. For instance, when the API invoker’s subscription with API provider is invalid, the the CCF should revoke its authorization on other AEFs of the API provider. CCF behaviour has to be clarified.  The above was discussed as proposed in SA6 CR (S6-241295) during SA6#60 meeting. And, companies in SA6 opinioned to implement the cause value and the related behaviour in stage-3.  Based on the above conclusion, this CR proposes cause value (not valid subscription) and the clarifies the related behaviour based on the cause value (invalid subscription, overlimit usage), for Revoke\_Authentication service operation of CAPIF\_Security API. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Cause value for not valid subscription. CCF revoking the authorization on other AEFs based on the cause value. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | CCF behaviour for authorization revocation request is ambigious with the presence of cause value. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.5.4.3.3, A.6 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | This CR proposes backward compatible change to CAPIF\_Security\_API Open API specification file. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

##### 8.5.4.3.3 Enumeration: Cause

Table 8.5.4.3.3-1: Enumeration Cause

|  |  |  |
| --- | --- | --- |
| Enumeration value | Description | Applicability |
| 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. |  |
| AUTHORIZATION\_ISSUE | The revocation of the authorization of the API invoker is due to API Invoker not being authorized anymore by the API Provider. | RNAA |
| OTHER\_REASON | The revocation of the authorization of the API invoker is due to other reason. | RNAA |

\*\*\* Second Change \*\*\*

### 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. |

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

# A.6 CAPIF\_Security\_API

openapi: 3.0.0

info:

title: CAPIF\_Security\_API

description: |

API for CAPIF security management.

© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

version: "1.3.0-alpha.4"

externalDocs:

description: 3GPP TS 29.222 V18.5.0 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

grantType:

type: array

items:

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

minItems: 1

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

- authorization\_code

client\_id:

type: string

resOwnerId:

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

client\_secret:

type: string

scope:

type: string

authCode:

type: string

redirect\_uri:

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'

resOwnerId:

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

required:

- iss

- scope

- exp

ResOwnerId:

type: object

description: >

Represents the identifier of the resource owner.

properties:

gpsi:

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

anyOf:

- required: [gpsi]

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

- AUTHORIZATION\_ISSUE

- OTHER\_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.

- AUTHORIZATION\_ISSUE:

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

not being authorized anymore by the API Provider.

- OTHER\_REASON:

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

OAuthGrantType:

anyOf:

- type: string

enum:

- CLIENT\_CREDENTIALS

- AUTHORIZATION\_CODE

- AUTHORIZATION\_CODE\_WITH\_PKCE

- type: string

description: >

This string provides forward-compatibility with future extensions to the enumeration and

is not used to encode content defined in the present version of this API.

description: |

Indicates the supported authorization flow (e.g. client credentials flow, authorization code flow, etc.) to the API invoker.

Possible values are:

- CLIENT\_CREDENTIALS: Indicate that the grant type is is client credentials flow.

- AUTHORIZATION\_CODE: Indicate that the grant type is authorization code.

- AUTHORIZATION\_CODE\_WITH\_PKCE: Indicate that the grant type is authorization code with PKCE.

\*\*\* End of Change \*\*\*