**3GPP TSG-CT WG3 Meeting #131 *C3-235156***

**Chicago, United States, 13 - 17 November, 2023 (revision of C3-235156)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.222** | **CR** | **0314** | **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 securitymethod data type for 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 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:*** | | According to clause 6.5.3 of TS 33.122, in resource owner-aware northbound API access (RNAA) scenarios, two new security methods (i.e. authorization code flow, PKCE in clause 6.5.3 of TS 33.122) are utilized between API invoker and AEF.  However, currently, SeurityMethod data type defined in clause 8.2.4.3.6 of TS 29.222 only covers traditional security methods including Security method 1 (Using TLS-PSK), Security method 2 (Using PKI), Security method 3 (TLS with OAuth token) as described in 3GPP TS 33.122.  Without adding the new data type, the RNAA feature that relies on new authorization flows can not be supported by the CAPIF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add new datatype in clause 8.2.4.3 of TS 29.222. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The RNAA feature that relies on new authorization flows can not be supported by the CAPIF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.5.4.1, 8.5.4.2.3, 8.5.4.3.x, 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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 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. |  |
| 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. |  |
| AuthorizationFlow | Clause 8.5.4.3.x | Represents the authorization flows to support RNAA | RNAA |

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

##### 8.5.4.2.3 Type: SecurityInformation

Table 8.5.4.2.3-1: Definition of type SecurityInformation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| interfaceDetails | InterfaceDescription | O | 0..1 | Details of the interface (NOTE) |  |
| aefId | string | O | 0..1 | AEF identifier (NOTE) |  |
| apiId | string | C | 0..1 | API identifier.  If API invoker supplies this IE in the PUT request, CCF shall respond back with this IE and its associated security information. | SecurityInfoPerAPI |
| prefSecurityMethods | array(SecurityMethod) | M | 1..N | Security methods preferred by the API invoker for the API interface |  |
| selSecurityMethod | SecurityMethod | O | 0..1 | Supplied by the CAPIF core function, it indicates the selected security method for the API interface. If it is not provided, it means no common supported security method by the API invoker and the AEF, or the selected security method is not allowed by the local policy in the CAPIF core function. |  |
| authenticationInfo | string | O | 0..1 | Authentication related information |  |
| authorizationInfo | string | O | 0..1 | Authorization related information |  |
| authorizationFlow | AuthorizationFlow | O | 0..1 | The authorization flows to support RNAA as defined in clause 6.5.3 of TS 33.122 [16]. | RNAA |
| NOTE:      Only one of the attributes "aefId" or "interfaceDetails" shall be included. | | | | | |

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

##### 8.5.4.3.x Enumeration: AuthorizationFlow

Table 8.5.4.3.x-1: Enumeration AuthorizationFlow

|  |  |  |
| --- | --- | --- |
| Enumeration value | Description | Applicability |
| CLIENT\_CREDENTIALS\_FLOW | Client credentials flow as described in clause 6.5.2 of TS 33.122 [16]. |  |
| AUTHORIZATION\_CODE\_FLOW | Authorization code flow defined in clause 6.5.3 of TS 33.122 [16]. |  |
| AUTHORIZATION \_CODE\_FLOW\_WITH\_PKCE | Authorization code flow with PKCE defined in clause 6.5.3 of TS 33.122 [16]. |  |

\* \* \* Next 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. |
| x | RNAA | Indicates the support of resource owner awareness authorization. |

\* \* \* 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

authorizationFlow:

$ref: '#/components/schemas/AuthorizationFlow 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

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'

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.

AuthorizationFlow:

anyOf:

- type: string

enum:

- CLIENT\_CREDENTIALS\_FLOW

- AUTHORIZATION\_CODE\_FLOW

- AUTHORIZATION\_CODE\_FLOW\_WITH\_PKCE

- type: string

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