**3GPP TSG-CT WG3 Meeting #142 *C3-253228\_R1***

**Goteborg, SE, 25 - 29 August 2025**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0425** | **rev** | **-** | **Current version:** |  |  |
|  |
| *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:***  | CAPIF interconnection |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | CAPIF\_Ph3 |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** |  |
|  | *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:*** | This CR addresses the approved CR#0201on 23.222 (**S6-244551, clauses 8.25.x of 23.222**), i.e., including new service operations and information clauses for interconnection scenario. |
|  |  |
| ***Summary of change:*** | This CR adding the following functionality:- obtaining authorization for an API invoker involving another CCF- revoking authorization involving another CCF.- access control aspects.- obtaining security information involving another CCF. |
|  |  |
| ***Consequences if not approved:*** | The definition of the CAPIF\_Ph3 functionality cannot be completed in the stage 3. |
|  |  |
| ***Clauses affected:*** | 5.6.1.1, 5.6.2.1, 5.6.2.5.1, 5.6.2.5.2, 5.10.1.1, 5.10.2.1, 5.10.2.2.1, 5.10.2.2.2 |
|  |  |
|  | **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 affect any OpenAPI files. |
| ***()*** |  |
| ***This CR's revision history:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

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

#### 5.6.1.1 Overview

The CAPIF security APIs, as defined in 3GPP TS 23.222 [2], allow:

- API invokers via CAPIF-1/1e and CAPIF-6/6e reference points to (re-)negotiate the service security method and obtain authorization for invoking service APIs; and

- API exposing function via CAPIF-3/3e and CAPIF-6-6e reference points to obtain authentication information of the API invoker for authentication of the API invoker and revoke the authorization for service APIs.

\* \* \* Next change \* \* \* \*

#### 5.6.2.1 Introduction

The service operations defined for CAPIF\_Security\_API are shown in table 5.6.2.1-1.

Table 5.6.2.1-1: Operations of the CAPIF\_Security\_API

| **Service operation name** | **Description** | **Initiated by** |
| --- | --- | --- |
| Obtain\_Security\_Method | This service operation is used by an API invoker to negotiate and obtain service API security methods from the CAPIF core function. This information is used by the API invoker for service API invocations at the API Exposing Function. | API invoker |
| Obtain\_Authorization | This service operation is used by an API invoker to obtain authorization to access service APIs. | API invoker |
| Obtain\_API\_Invoker\_Info | This service operation is used by an API exposing function to obtain the authentication or authorization information related to an API invoker. | API exposing function |
| Revoke\_Authorization | This service operation is used by a service consumer to invalidate the authorization of an API invoker. | API exposing function, CCF |

Security information is generated when requested by an API invoker, and is stored in the CAPIF Core function. The information can be accessed via a resource representation URI using the API invoker ID as described in clause 8.5.2.3. The URI is provided to the API invoker in the HTTP response to the creation request (via the Obtain\_Security\_Method service operation name).

Refer to clause 9.1.2a.2 for details about verifying that the API Exposing function has the ability to authorize API invokers prior to invoking service APIs.

\* \* \* Next change \* \* \* \*

##### 5.6.2.5.1 General

This service operation is used by a service consumer to invalidate the authorization of a specified API Invoker to invoke service APIs exposed by the calling API exposing function.

\* \* \* Next change \* \* \* \*

##### 5.6.2.5.2 Invalidate authorization using Revoke\_Authorization service operation

To invalidate authorization of an API invoker for all service APIs, the service consumer shall send an HTTP DELETE message to that API invoker's resource representation URI in the CAPIF core function using the API invoker ID as specified in clause 8.5.2.3.3.2.

Upon receiving the HTTP DELETE message, the CAPIF core function shall delete the resource representation and shall notify the API invoker of the authorization invalidation using the Notification Destination URI received in the Obtain\_Security\_Method message.

The CAPIF core function shall also invalidate the previously assigned access token when the authorization of all service APIs are revoked for the API invoker.

To invalidate authorization of an API invoker for some service APIs, the service consumer shall send an HTTP POST message to that API invoker's "delete" custom resource representation URI in the CAPIF core function with a list of the service APIs that should be revoked.

Upon receiving the HTTP POST message, the CAPIF core function shall revoke the authorization of the API invoker for the indicated service APIs (e.g. it may update the list of unauthorized APIs locally); and shall notify the API invoker of the authorization invalidation using the Notification Destination URI received in the Obtain\_Security\_Method message.

In both alternatives, the CAPIF core function shall acknowledge the HTTP request from the service consumer.

NOTE: Functions from 3rd party API provider domain can also access this service operation with sufficient permissions.

\* \* \* Next change \* \* \* \*

#### 5.10.1.1 Overview

The CAPIF access control policy APIs allow a service consumer via CAPIF-3/3e and CAPIF-6/6e reference points to obtain the service API access policy from the CAPIF core function.

NOTE: Functions from 3rd party API provider domain can also access this API with sufficient permissions.

\* \* \* Next change \* \* \* \*

#### 5.10.2.1 Introduction

Table 5.3.2.1-1: Operations of the CAPIF\_Access\_Control\_Policy\_API

| **Service operation name** | **Description** | **Initiated by** |
| --- | --- | --- |
| Obtain\_Access\_Control\_Policy | This service operation is used by a service consumer to obtain the access control policy from the CAPIF core function. | API exposing function, CCF |

\* \* \* Next change \* \* \* \*

##### 5.10.2.2.1 General

This service operation is used by a service consumer to obtain the access control policy from the CAPIF core function.

\* \* \* Next change \* \* \* \*

##### 5.10.2.2.2 API exposing function obtaining access control policy from the CAPIF core function using Obtain\_Access\_Control\_Policy service operation

To obtain the access control policy from the CAPIF core function, the service consumer shall send an HTTP GET message to the CAPIF core function with the API exposing function Identifier and API identification. The GET message may include API invoker ID for retrieving access control policy of the requested API invoker as specified in clause 8.6.2.2.3.1.

Upon receiving the above described HTTP GET message, the CAPIF core function shall:

1. verify the identity of the service consumer and check if the service consumer is authorized to obtain the access control policy corresponding to the API identification;

2. if the service consumer is authorized to obtain the access control policy, the CAPIF core function shall respond with the access control policy information corresponding to the API identification and API invoker ID (if present) in the HTTP GET message; and

3. if errors occur when processing the request, the CAPIF core function shall respond to the service consumer with an appropriate error status code as defined in clause 8.6.5.

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