**3GPP TSG-SA3 Meeting #122 draft\_S3-252037-r1**

**Fukuoka, Japan, 19 – 23 May 2025**

**Source: Samsung, Xiaomi, China Telecom, Nokia, Nokia Shanghai Bell, Lenovo, CATT**

**Title: Updates to security procedure for CAPIF interconnection**

**Document for: Approval**

**Agenda item: 4.22**

**Comments**

This pCR proposes to update the security procedure for CAPIF interconnection in living document [S3-251890](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_122_Fukuoka/Docs/S3-251890.zip).

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

## 6.X Security procedures for CAPIF interconnection

### 6.X.1 General

The CAPIF provider A and CAPIF provider B host the CAPIF in their trust domains as specified in clause 6.2.2 in TS 23.222 [3]. The designated CAPIF core function of the CAPIF provider A interconnects with the designated CAPIF core function of the CAPIF provider B over CAPIF-6/6e interface.

The following clauses 6.X.2 and 6.X.3 detail security aspects of the scenario where, the API invoker is onboarded to CCF-B of the CAPIF provider B and the target AEF is registered to CCF-A of CAPIF provider A.

### 6.X.2 Security method negotiation

For security method negotiation procedure in CAPIF interconnection, clause 6.3.1.2 shall be followed with the following enhancement:

* The API invoker shall send the security method request to the CCF-B.
* In case where CCF-B is in possession of the security method(s) as specified in clause 8.25.3.1 of TS 23.222 [3], CCF-B shall select a security method to be used over CAPIF-2/2e reference point for each AEF based on the access scenarios and AEF capabilities.
* In case where CCF-B is not in possession of the security method(s), based on the AEF details received from the API invoker, CCF-B identifies the CCF-A where the AEF is registered and sends the request to CCF-A to either get the supported list of security method(s) of AEF or to get a selected security method. The request to CCF-A shall include AEF details and may include the API invoker ID and security method supported by API invoker (e.g., to enable CCF-A to select the security method). The CCF-A shall provide to CCF-B either the list of supported security methods of AEF or the selected security method. If the list of supported security methods of AEF is received, the CCF-B shall select a security method to be used over CAPIF-2/2e reference point for each AEF based on the access scenarios and AEF capabilities.
* The CCF-B shall send Security Method Response message to the API invoker indicating the selected security method for each AEF.

### 6.X.3 Authentication and authorization procedure

For the mutual authentication between the API invoker onboarded to CCF-B in CAPIF provider B and AEF registered to the CCF-A in CAPIF provider A, the procedures as defined in clause 6.5.2 shall be followed with the enhancements as specified in this clause .NOTE: It is assumed authorization information is available at the CCF-A.

#### 6.X.3.1 Method 1: Using TLS-PSK

The authentication procedure in clause 6.5.2.1 shall be followed with the following enhancements for CAPIF interconnect:

* The API invoker shall send the authentication initiation request message to the target AEF in CAPIF provider domain A for CAPIF interconnection. Based on the AEF details available at the API invoker, which indicates the AEF belongs to CCF-A, the authentication initiation request message shall include the information for identification of the CCF-B.
* [modified texts from Nokia] The API invoker in CAPIF provider domain B shall include the API invoker ID in the authentication initiation request message sent to the target AEF-A in CAPIF provider domain A for CAPIF interconnection.
* Based on the AEF-A details available at the API invoker which indicates the AEF belongs to CCF-A, the API invoker shall include the CCF-B ID (CAPIF core function the API invoker is onboarded to) in the authentication initiation request message.

NOTE: Whether CCF-B ID is sensitive against the AEF and how to address it if necessary are not addressed in the present document.

NOTE: CCF-B ID reveals that the API Invoker is accessing API services from a different CAPIF provider domain.

* The AEF in CAPIF provider domain A shall request for security information (AEFPSK) from CCF-A to perform authentication and secure connection establishment with the API invoker, if the AEF does not have a security information. The request shall include the API invoker ID and the CCF-B ID.
* When CCF-A receives the request message for security information from the AEF, CCF-A fetches the security information related to the chosen security method (TLS-PSK: AEFPSK), based on API invoker ID and CCF-B ID.
* If the CCF-A does not have security information of the API invoker locally available, CCF-A shall request the security information from CCF-B over CAPIF-6/6e reference point based on the received API invoker ID, and the available AEF details (including the service API interface information). The CCF-B shall provide the TLS-PSK related security information (AEFPSK) to CCF-A.

NOTE: The CCF-A can check the received API Invoker ID and CCF-B ID based on the information locally available to contact the right CCF-B to fetch the security information.

* The CCF-A shall provide the received security information to the AEF.
* After sending the authentication initiation response, API invoker in CAPIF provider domain B and AEF in CAPIF provider domain A establish a TLS connection using the security information obtained.
* After successful authentication of API invoker and AEF, the AEF shall obtain the authorization information from CCF-A. If CCF-A does not have sufficient information for authorization, CCF-A shall fetche additional information related to the API invoker from CCF-B based on the business relationship. The AEF performs authorization based on the obtained authorization information.

#### 6.X.3.2 Method 2: Using PKI

[from Nokia] The authentication procedure in clause 6.5.2.2 shall be followed with the following enhancements for CAPIF interconnect to establish a dedicated secure session over CAPIF-2e using mTLS:

The API invoker onboarded to CCF-B and the AEF registered to CCF-A shall follow the procedure in subclause 6.X.3.1 with the following adaptation to establish dedicated secure session over CAPIF-2e using TLS based on certificate based mutual authentication.

* For fetching the security information related to the chosen security method (TLS-PKI) the CCF-B includes only the API invoker ID.
* The CCF-B shall provide the security information (API invoker's root CA certificate) to the AEF via CCF-A, for allowing the AEF to validate the API invoker's certificate.

#### 6.X.3.3 Method 3: TLS with OAuth Token

The authentication procedure in clause 6.5.2.3 shall be followed to establish a dedicated secure session between API invoker and CCF-B of the API provider domain B over CAPIF-2e using mTLS.

The authorization procedure in clause 6.5.2.3 shall be followed with the following enhancements:

* The API invoker shall send the access token request message to the onboarded CCF-B, CCF-B determines that the service API requested is provided by the AEFs in CAPIF provider domain A. In interconnection scenario, the parameter ‘scope’ in Access token request message is required.
* The CCF-B sends the access token request message with API Invoker ID, list of service API information of AEF (according to Annex C.3.2 for the client\_id and scope) to the CCF-A in CAPIF provider domain A. In interconnection scenario, the Onboard\_secret is not included in the access token request message to the CCF-A. In interconnection scenario, the parameter ‘scope’ in Access token request message is required. The CCF-A generates and provides an access token specific to the API invoker and returns it in an Access Token Response message to the API invoker via CCF-B as specified in clause 6.5.2.3.
* On CAPIF-2e, the API invoker authenticates to the AEF by establishing a TLS session with the AEF as specified in clause 6.X.3.1 or 6.X.3.2.
* With successful authentication to the AEF on CAPIF-2e, the API invoker shall initiate invocation of a 3GPP northbound API with the AEF including the access token in northbound API invocation request as per OAuth 2.0. The AEF verifies the integrity of the access token by verifying the CCF’s signature to validate the access permission for the requested service API as specified in clause 6.5.2.3.

[CCA based text changes from Nokia pCR]

* The API invoker shall send the access token request message to the onboarded CCF-B. Since the discovered service API is provided by a different CAPIF provider domain, the API invoker shall provide a client credential assertion token to allow for authentication of the API Invoker ID by CCF and AEF of the other CAPIF provider domain.
* CCF-B determines that the service API requested is provided by an AEF in CAPIF provider domain A and sends the access token request message to CCF-A in CAPIF provider domain A. If the Onboard\_secret is included in the access token request to CCF\_B, it shall be removed before forwarding the request to CCF-A.
* CCF-A authenticates the API invoker. If the CCA is included, CCF-A may verify the API invoker identity. If successfully authenticated, CCF-A generates an access token specific to the API invoker and provides it in an Access Token Response message to the API invoker via CCF-B.
* On CAPIF-2e, the API invoker authenticates to the AEF by establishing a TLS session.
* If successfully authenticated to the AEF, the API invoker shall initiate the invocation of a 3GPP northbound API request with the AEF including the OAuth 2.0 access token in the request.
* AEF verifies the integrity of the access token by verifying CCF-A's signature to validate the access permission for the requested service API as specified in clause 6.5.2.3.

Editor’s Note: Whether CCF-A will have sufficient information to authenticate the API invoker before including API invoker ID into the access token is FFS.

#### 6.X.3.4 Authentication and Authorization for RNAA

[from ZTE: Option 1]

In CAPIF RNAA interconnection, the API invoker is onboarded to CCF-B of the CAPIF provider B and the target AEF is registered to CCF-A of CAPIF provider A. The ROF in CAPIF provider domain B connects with CCF-A of CAPIF provider A.

For authorization and authorization in CAPIF RNAA interconnection, clause 6.5.3 shall be followed with the following enhancement:

- For authorization, the CCF-A has the role of the OAuth 2.0 authorization server, i.e., providing the access token used for RNAA. The CCF-A shall indicate the selected flows to the API invoker. The CCF-A shall give service authorization which subscribers or users can use RNAA.

- For revocation, the CCF-A can initiate the Authorization Revocation Request message as defined in clause 8.23.4 of TS 23.222 [3] with additional information to identify the RNAA-related revoked token. The CCF-B provides notification message to the API invoker after token revocation.

[From Samsung: Option 2]

Authentication and authorization for RNAA as specified in clause 6.5.3, in TS 33.122 shall be re-used. The CCF-A (AEF registered CCF) has the role of the OAuth 2.0 authorization server, i.e., providing the access token used for RNAA.

In case of an external AF (i.e., not the application on the UE) being the API invoker, for mutual authentication of API invoker AF and API exposing function, the authentication methods for interconnection as specified in clause 6.X.3.1 and clause 6.X.3.2 can be reused.

For authorization, the OAuth 2.0 flows as specified in clause 6.5.3.1 is applicable and shall be re-used.

For selecting authorization method, the procedure defined in clause 6.X.2 shall be followed. The API invoker shall include the supported RNAA authorization flows in the Security Method Request. In case where CCF-B is not in possession of the RNAA authorization flow, CCF-B sends the request to CCF-A to either get the supported list of RNAA authorization flows or to get a selected RNAA authorization flows. The CCF-A shall provide either the list of supported RNAA authorization flows or the RNAA authorization flows to the API invoker via CCF-B. The CCF-A/B shall determine the RNAA authorization flow based on the RNAA capabilities of the CCF-A, AEF, and API invoker. The API invoker shall use the determined RNAA authorization flow in the subsequent communication with the CCF-A and AEF.

For revocation, the CCF-A shall initiate the revocation and procedure as defined in clause 6.5.3.4 can be re-used. The CCF-A via CCF-B notifies the the API invoker after token revocation.

[from Xiaomi: Option 3]

Clause 6.X.3.3 can be reused to support client credentials flow in RNAA scenarios.

For authorization code (optional PKCE) flow in RNAA scenarios, the clause 6.X.3.3 can be reused with the following additional enhancements related to the authorization request message.

* The API invoker shall send the authorization request message to the onboarded CCF-B, CCF-B determines that the service API requested is provided by the AEFs in CAPIF provider domain A.
* The CCF-B sends the authorization request message to the CCF-A in CAPIF provider domain A.

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