**3GPP TSG-SA3 Meeting #121 S3-25xxxx-r5**

**Goteborg. SWEDEN, 7 - 11 April 2025**

**Source: Samsung, Xiaomi**

**Title: Security procedure for CAPIF interconnection**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS 33.122**

**Version: 18.4.0**

**Work Item: CAPIF\_Ph3\_sec**

**Comments**

This pCR is proposed to draft CR S3-251116 from SA3#120, it proposes detailed procedure for CAPIF interconnection security.

\* \* \* 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 [xx]. 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 details 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

The API invoker and the CCF-A shall negotiate a security method that shall be used by the API invoker and the AEF for CAPIF-2e interface authentication and protection. After successful mutual authentication on CAPIF-1e interface, based on the API invoker's subscribed service APIs, access scenarios (whether the API invoker access the AEF prior to service API invocation or upon the service API invocation) and AEF capabilities, the CCF-A shall select the security methods and send the selected security methods to the API invoker.

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. The API invoker shall include AEF details and the CAPIF-2/2e security capability information in the security method negotiation request to the CCF-B.
* Based on the AEF details received from the API invoker, CCF-B identifies the CCF-A where the AEF is registered and forwards the request to CCF-A.
* The CCF-A shall select a security method to be used over CAPIF-2/2e reference point for each AEF, considering the information received from CCF-B, access scenarios and AEF capabilities.
* The CCF-A shall send Security Method Response message to the API invoker via CCF-B, 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 clause 6.X.3.1 and 6.X.3.2.

#### 6.X.3.1 Method 1 or 2: TLS-PSK or PKI

* Based on the service API discovery information received from CCF-A via CCF-B, the API invoker determines the requested services APIs are provide by the AEF in CAPIF provider domain A.
* The API invoker shall include the API invoker ID, the CCF-B information (CAPIF core function the API invoker is onboarded to) in the authentication initiation request message sent to the target AEF in CAPIF provider domain A for CAPIF interconnection.
* The AEF shall request for security information from CCF-A to perform authentication and secure interface 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 information.
* When the CCF-A receives the request message from the AEF for security information, the CCF-A fetches security information based on API invoker ID and the CCF-B information. If it has no security information, the CCF-A shall request the security information (AEFPSK/root CA) from CCF-B over CAPIF-6/6e reference point based on the received API invoker ID and CCF-B information.

Editor’s Note: How the API exposing function authorizes the API invoker's service API invocation request in interconnection scenario is FFS.

6.X.3.2 Method 3: TLS with OAuth Token

* 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.
* The CCF-A provides an access token to the API invoker via CCF-A as specified in clause 6.5.2.3. The access token is specific to the AEF in CAPIF provider domain A and signed by the CCF-A as per IETF RFC 7515 [zz].
* On CAPIF-2e, the API invoker authenticates to the AEF by establishing a TLS session with the AEF. The API invoker shall include the API invoker ID and CCF-B information in the authentication initiation request message sent to CCF-A via CCF-B to the target AEF in CAPIF provider domain A.
* If the AEF does not have a security information, AEF shall request for security information from CCF-A to perform authentication and secure interface establishment with the API invoker. The request shall include the API invoker ID and the CCF-B information.
* When the CCF-A receives the request message from the AEF for security information, the CCF-A fetches security information based on API invoker ID and the CCF-B information. If it has no security information, the CCF-A shall request the security information from CCF-B over CAPIF-6/6e reference point based on the received API invoker ID and CCF-B information.
* The AEF shall validate the access token. The AEF verifies the integrity of the access token by verifying the CCF’s signature. If validation of the access token is successful, the AEF shall verify the API invoker's Northbound API invocation request against the authorization claims in access token, ensuring that the API Invoker has access permission for the requested service API.

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