**3GPP TSG-SA3 Meeting #121 draft\_S3-251720-r1**

**Goteborg, Sweden, 7 - 11 April 2025**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.122** | **CR** | ***draft*** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Security procedures for CAPIF interconnection |
|  |  |
| ***Source to WG:*** | Samsung, China Telecom, Nokia, Nokia Shanghai Bell, Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | CAPIF\_Ph3\_sec |  | ***Date:*** | 2025-02-21 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-19 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | This draftCR proposes normative texts for security procedures for CAPIF interconnection based on the conclusions made in TR 33.700-22. |
|  |  |
| ***Summary of change:*** | This draftCR will capture the security procedures for CAPIF interconnection |
|  |  |
| ***Consequences if not approved:*** | Security procedure for CAPIF interconnection is not specified |
|  |  |
| ***Clauses affected:*** | 6.X (new), 6.X.1 (new), 6.X.2(new), 6.X.3(new) |
|  |  |
|  | **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's revision history:*** | S3-251116 |

\* \* \* 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, that 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 [xx], 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 clause 6.X.3.1, 6.X.3.2 and 6.X.3.3.

Editor’s Note: Security procedure for CAPIF RNAA interconnection is FFS.

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

Editor’s Note: How the API invoker knows that it should send the CCF-B ID to AEF of CCF-A is FFS.

Editor’s Note: How the API invoker knows that certain service APIs are offered by different CCF is FFS.

* The API invoker shall include the API invoker ID and may include the CCF-B ID (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.

Editor’s Note: Whether CCF-B ID to be included as a mandatory or optional IE in the authentication initiation request is FFS. If included whether it is a sensitive information against AEF in different domain and how to resolve it is FFS.

NOTE: If CCF-B ID is included in the authentication initiation request message, the CCF-A can use the CCF-B ID to identify the onboarded CCF of the API invoker. If CCF-A has the information about the API invokers onboarded to CCF-B then the CCF-B ID is not included the authentication initiation request message.

Editor’s Note: Whether communicating with other CCFs to identify the API invoker’s onboarded CCF is FFS.

* The AEF 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 may include the CCF-B ID.
* 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 ID.
* If the CCF-A does not have security information, 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.

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

Editor’s Note: For AEFPSK identification, if AEF details are sufficient or service API information is needed is FFS.

* The CCF-B shall provide the security information related to the chosen security method to the CCF-A.
* The CCF-A shall provide the received security information to the AEF.
* The AEF sends the authorization information request to CCF-A. CCF-A sends the response for authorization information request to the AEF. The AEF performs authorization based on the obtained authorization information.

Editor’s Note: Whether CCF-A will have sufficient information to authorize the API invoker or it needs additional information from CCF-B is FFS.

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

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 provides the security information (API invoker's root CA certificate) to the AEF via CCF-A, for the AEF to validate the API invoker's certificate.

Editor’s Note: Whether communicating with other CCFs to identify the API invoker’s onboarded CCF is FFS.

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

Editor’s Note: How the API invoker knows that it should send the CCF-B information to AEF of CCF-A is FFS.

Editor’s Note: How the API invoker knows that certain service APIs are offered by different CCF is FFS.

* 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.

Editor’s Note: Further which CCF provides the access token and how rest of the procedure works is FFS. Forwarding an access token request means to make the onoboarding secret public to the CCF-A. If this is wanted is FFS.

* 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.

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

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