**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250087-r5**

**Online, Electronic meeting, 13 -16 January 2025**

**Source: Samsung, ZTE, China Telecom, Ericsson, Xiaomi, Nokia**

**Title: Updates to conclusion for key issue#2**

**Document for: Approval**

**Agenda item: 5.18**

**Spec: 3GPP TR 33.700-22**

**Version: 0.3.0**

**Work Item: FS\_CAPIF\_Ph3-sec**

**Comments**

This pCR proposes to update the conclusion for key issue#2 on CAPIF interconnection security.

**Proposed Changes**

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

## 7.2 Conclusion for KI #2: CAPIF interconnection security

It is assumed that the API invoker onboards to CCF-A, which is referred as onboarded CCF.

It is assumed that the target AEF connected to a different CCF-B which is referred as designated CCF (i.e., which is configured as the serving CCF for interconnection e.g., belongs to a 3rd party or a different CAPIF provider).

###  7.2.1 Conclusion for CAPIF 6/6e security

It is concluded that for CAPIF-6 and CAPIF-6e reference points, same security mechanisms specified in clauses 6.6 and 6.10 of TS 33.122 [4] for CAPIF-3/4/5 and CAPIF-3e/4e/5e reference points will be used, respectively.

### 7.2.2 Conclusion for security method negotiation

For security method negotiation procedure (as per requirement 2), clause 6.3.1 in TS 33.122 [4] can be re-used with the following enhancement:

* Target AEF provides the supported security mechanisms to its own designated CCF-B. The Security Method Request is sent from API invoker to the Onboarded CCF-A. The Onboarded CCF-A checks if the target AEF is discovered by CCF-B. The API invoker includes the designated CCF information (CCF-B ID) in the Security method request message. API invoker is provided with the designated CCF-B information by the onboarded CCF-A.
* The designated CCF-B selects a security method to be used over CAPIF-2/2e reference point for each requested AEF, taking into account the information from onboarded CCF-A, security methods that the API invoker supports over CAPIF-2/2e reference point and AEF capabilities.
* Designated CCF-B sends the selected method to the API invoker via the Onboarded CCF-A.
* Details of the procedure are to be determined during normative work.

### 7.2.3 Conclusion for API invoker authentication and authorization mechanism

For mutual authentication and authorization between API invoker (onboarded to CCF-A) and the AEF (registered to designated CCF-B), the procedures as defined in clause 6.5.2 of TS 33.122 [4] can be re-used with the following enhancement:

* When using TLS-PSK or PKI:
	+ The API invoker includes the Onboarded CCF-A ID in the Authentication Initiation request message.
	+ On receiving the request from the AEF, designated CCF-B requests the security information (AEFPSK/root CA) from the onboarded CCF-A (over CAPIF-6/6e reference point) based on the AEF ID, API invoker ID and Onboarded CCF-A ID, if the designated CCF-B doesn’t retrieve the relevant security information.
	+ The AEF learns the access control policy from the designated CCF serving the AEF to verify the API invoker authorization.
* When using TLS with OAuth token:
	+ If the onboarded CCF-A finds that the expected service/service operation/service API cannot be provided by the AEF in its domain or is previously published by designated CCF-B, the onboarded CCF-A sends the access token request to the designated CCF-B for the API Invoker requested service API information.
	+ CCF-B provides an access token to the API invoker via CCF-A as specified in clause 6.5.2.3 in TS 33.122 [4]. The AEF verifies the access token as described in 6.5.2.3 in TS 33.122 [4]. Otherwise,
* Details of the procedure are to be determined during normative work.

\* \* \* \* End of Changes \* \* \* \*