**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250087-r3**

**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 CCF-A.

### It is assumed that CCF-B is connected with the target AEF. 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

The precondition for authentication between entities of different domains is to have a common security method selected. The API Invoker of one domain needs to know the security method supported by the AEF of another domain for providing interconnection security.

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 CCF-B. The Security Method Request is sent from API invoker to CCF-A. CCF-A checks if the target AEF is discovered by CCF-B. (CCF-B ID)
* 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 CCF-A and AEF capabilities.
* CCF-B sends the selected method to the API invoker via the 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 (on-boarded to CCF-A) and the AEF (registered to 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 CCF-A ID in the Authentication Initiation request message.
	+ Received the request from the AEF, CCF-B requests the security information (AEFPSK/root CA) from CCF-A (over CAPIF-6/6e reference point) based on the AEF ID, API invoker ID and CCF-A ID, if CCF-B doesn’t retrieve the relevant security information.
	+ The AEF learns the access control policy from the CCF serving the AEF to verify the API invoker authorization.
* When using TLS with OAuth token:
	+ If 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 CCF-B, CCF-A sends the access token request to the CCF-B.
	+ 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 \* \* \* \*