**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250087-r11**

**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

### 7.2.0 General

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

It is assumed that the API invoker is onboarded to CCF-A and the target AEF is registered to a different CCF-B.

### 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 6.3.1.2 in TS 33.122 [4] will be used as baseline with the necessary enhancements (if any).

The details of how security method selection is done for the CAPIF 2/2e reference point based on the capabilities of the API Invoker and the AEF capabilities (that belongs to CCF-B) are up to 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 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:
	+ On receiving the request from the AEF, CCF-B requests the security information (AEFPSK/root CA) from CCF-A (over CAPIF-6/6e reference point).
	+ The AEF learns the access control policy from CCF-B.  If the authorization access policy at CCF-B is not enough, then CCF-B learns access control policy from CCF-A and provides it to the AEF.
* When using TLS with OAuth token:
	+ On receiving the request from the AEF, CCF-B requests the security information (e.g., root CA) from CCF-A (over CAPIF-6/6e reference point).
	+ CCF-A sends the access token request to 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].
	+ Whether CCF-A can issue an access token is to be determined during normative work.
* For the case of TLS-PSK or PKI, and TLS with OAuth token methods listed above, the specific details of how the CCF-B requests the security information of the API Invoker from the right CCF-A, i.e. where API invoker is onboarded, are up to normative work.
* For the case of TLS with OAuth token methods, how CCF-A determines to request token from CCF-B is up to the normative work.
* How CCF-B verifies that CCF-A is authorized for the service is up to normative work.
* Further details of the procedure are to be determined during normative work.

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