**3GPP TSG-SA WG3 Meeting #117 S3-24xxx**

**Maastricht, Netherlands, 19th – 23th Aug 2024**

**Source: China Telecom**

**Title: New key issue about CAPIF interconnection**

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

**Agenda item: 5.19**

**Document for: Approval**

**1. Introduction**

This contribution adds new key issue#1 about CAPIF interconnection in TR 33.700-22.

**2. Reason for Change**

This contribution provides the key issue needed to be considered in SA3.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TR 33.700-22.

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

## Key issue #X: CAPIF interconnection

### Key issue details

TS 23.222 defines an architectural model for the CAPIF interconnection which allows API invokers of a CAPIF provider to utilize the service APIs from the 3rd party CAPIF provider and other CAPIF core function within the same CAPIF provider. TS 23.222 specifies some information, like service API information, shareable information, which is transferred between CCFs via CAPIF-6/6e. Besides, CCFs coordinate to authenticate and authorize service API access for the AEF service API(s) exposed via CAPIF-6/6e, which is studied in TR 23.700-22 “Study on CAPIF Phase 3” now.

However, the security mechanisms supporting CAPIF interconnection are still not specified in R18, which may pose security risks such as information leakage and unauthorized access. So it is worth studying it to mitigate the risks.

### Potential security requirements

Potential security requirements for CAPIF interconnection are as followed:

- Authenticating and authorizing service API access for the AEF service API(s) exposed via CAPIF-6/6e shall be supported;

NOTE: Coordination with SA6 is needed.

- The transport of messages over the CAPIF-6 and CAPIF-6e reference points shall be integrity protected.

- The transport of messages over the CAPIF-6 and CAPIF-6e reference points shall be protected from replay attacks.

- The transport of messages over the CAPIF-6 and CAPIF-6e reference points shall be confidentiality protected.

- Mutual authentication between the CAPIF core functions shall be supported.

- The CAPIF core function shall be able to authorize the other CAPIF core functions to publish and manage the service API information via CAPIF-6/6e.

\* \* \* Next Change \* \* \* \*