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

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

**Source: China Telecom**

**Title: New key issue about onboarding resource owner to CAPIF**

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

**Agenda item: 5.19**

**Document for: Approval**

**1. Introduction**

This contribution adds new key issue#2 about onboarding resource owner to CAPIF 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: Onboarding resource owner to CAPIF

### Key issue details

Based on RNAA architecture specified in TS 23.222, the CAPIF allows the resource owner to provide authorization to the API invocation. The resource owner utilizes the resource owner client to interact with the authorization function in the CAPIF core function via CAPIF-8. TR 23.700-22 “Study on CAPIF Phase 3” is studying resource owner consent management now. However, how to identify the resource owner and secure the resource owner consent transmission was not specified in Rel-18. It provides an opportunity for malicious resource owners to attack the CAPIF core function via CAPIF-8. For example, the attack message may be sent to the CAPIF core function to affect service API invocation authorization, or the resource owner consent stored in the authorization function may be tampered with or leaked. Onboarding resource owner to CAPIF and securing the CAPIF-8 are worth to be studying.

### Potential security requirements

Potential security requirements for RNAA are as followed:

- The CAPIF core function shall authenticate the resource owner's onboarding request;

- The CAPIF core function shall authenticate the resource owner's offboarding request;

NOTE: Coordination with SA6 is needed.

- The transport of messages over the CAPIF-8 reference points shall be integrity protected.

- The transport of messages over the CAPIF-8 reference points shall be protected from replay attacks.

- The transport of messages over the CAPIF-8 reference points shall be confidentiality protected.

- Privacy of the 3GPP user over the CAPIF-8 reference points shall be protected.

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