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

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

**Source: China Telecom**

**Title: New key issue about service API invocation authorization with resource owner consent**

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

**Agenda item: 5.19**

**Document for: Approval**

**1. Introduction**

This contribution adds new key issue#3 about service API invocation authorization with resource owner consent 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: Service API invocation authorization with resource owner consent

### Key issue details

3GPP TS 23.222 specifies that the CAPIF allows the resource owner to provide authorization to the API invocation and the API exposing function can retrieve the resource owner consent parameters from the authorization function. TR 23.700-22 “Study on CAPIF Phase 3” is studying how to enable retrieval of the resource owner consent parameters by an API exposure function from the authorization function and how to align and manage access control that is more granular than simply granted/denied for service API (e.g., service operation level, resource level, service API originator/requestor details) with the provided resource owner consent to ensure appropriate usage of resource owner consent at the enabler layer.

TS 33.122 specifies the security aspects for RNAA, including token-based authorization using OAuth 2.0 framework and procedures of authorization using client credential flow, authorization code flow and authorization code flow with PKCE.

However, the details of authorization procedures are left for stage 3, including:

- the details of access tokens used for RNAA;

- the mapping of API Invoker ID and GPSI;

- whether and how the token and/or authorization request can include resource owner ID;

- the revocation procedure for RNAA.

Besides, TR 23.700-22 “Study on CAPIF Phase 3” is studying how to enable UE-deployed API invoker accesses resources not owned by that UE. And the security aspects need to be coordinated with SA3.

### Potential security requirements

Potential security requirements for RNAA are as followed:

- The CAPIF core function shall authorize resource owner-aware northbound API invocation based on the resource owner consent;

- The CAPIF core function shall revoke API invoker authorization for RNAA;

- The CAPIF core function shall enable UE-deployed API invoker accesses resources not owned by that UE.

- The API exposing function shall retrieve the resource owner consent parameter in authorization function to determine whether API invoker is authorized to access service API for RNAA.

NOTE: Coordination with SA6 is needed.

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