**3GPP TSG-SA3 Meeting #117 draft\_S3-242xxx-r3**

Maastricht, Netherlands 19 - 23 August 2024

**Source: Xiaomi (?), Nokia (?), China Telecom (?), Ericsson**

**Title: Key issue on security of resource owner permission management**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***It is proposed to approve this key issue to TR 33.700-22.***

# 2 References

1. 3GPP TR 33.700-22: "Study on security aspects of CAPIF Phase3"

# 3 Rationale

It is proposed to approve this key issue for TR 33.700-22 [1] to study potential solutions for resource owner authorization management.

# 4 Detailed proposal

\*\*\* Start of the first Change \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[X] 3GPP TR 23.700-22: "Study on CAPIF Phase 3".

[Y] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

\*\*\* Start of the second Change \*\*\*

## 5.X Key Issue #X: Security of resource owner permission management

### 5.X.1 Key issue details

This key issue identifies and addresses the security aspects of resource owner permission management studied in TR 23.700-22 [X] with KI #1.

As from clause 6.5.3. in TS 33.122 [Y], (for Release 18) three authorization flows are introduced to be used as potential procedures in RNAA enhanced CAPIF. These are client credentials, authorization code and authorization code with PKCE. Client credentials flow generally becomes applicable when the authorization is preconfigured in the authorization server by an out of band mechanism. The authorization code and authorization code with PKCE require online user interaction. The case where there is no preconfigured authorization information and the authorization permission from the user can only be obtained by an out of band mechanism is not addressed. New authorization mechanism(s) need to be studied to address that case.

CAPIF-8 reference point was introduced to CAPIF for the interaction between the authorization function and resource owner. For resource owner permission management, the resource owner communicates with the authorization function in the CAPIF core function over CAPIF-8.

The security mechanism for managing resource owner permission with the functionalities over CAPIF-8 reference point is out of scope of the Rel-18 of the specification. Security mechanism for this reference point needs to be studied.

### 5.X.2 Security threats

Without integrity protection for CAPIF-8 reference point, messages over the CAPIF-8 reference point can be modified by attackers.

Without confidentiality protection for CAPIF-8 reference point, messages over the CAPIF-8 reference point can be sniffed by attackers.

Without the anti-replay attack mechanism for CAPIF-8 reference point, messages over the CAPIF-8 reference point can be replayed by attackers.

Without the resource owner authentication, malicious resource owner can impersonate victim resource owner to do resource owner permission management.

### 5.X.3 Potential security requirements

The transport of messages over the CAPIF-8 reference point should be integrity protected.

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

The transport of messages over the CAPIF-8 reference point should be confidentiality protected.

Authorization server should be able to authenticate the resource owner.

The resource owner should be able to authenticate the authorization server.

CAPIF should support a set of secure authorization mechanisms, which addresses possible different use cases.

NOTE: Coordination with SA6 is needed.

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