**3GPP TSG-SA3 Meeting #117 draft\_S3-242xxx-r4**

Maastricht, Netherlands 19 - 23 August 2024

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

**Title: Key issue on security of resource owner consent 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 consent 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 consent management over CAPIF-8 reference point

### 5.X.1 Key issue details

This key issue identifies and addresses the security aspects of resource owner consent management over CAPIF-8 referenct point studied in TR 23.700-22 [X] with KI #1.

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

However, the security mechanism for managing resource owner consent with authorization function in CAPIF core function over CAPIF-8 was not specified. 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 consent 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.

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

Mutual authentication between the authorization function in CAPIF core function and the resource owner shall be supported.

NOTE: Coordination with SA6 is needed.

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