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

Maastricht, Netherlands 19 - 23 August 2024

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

**Title: New key issue for accessing UE resources by an application on another UE**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***It is proposed to add the following key issue to the TR 33.700-22.***

# 2 References

[1] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[2] 3GPP TS 23.700-22: "Study on CAPIF Phase 3".

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

# 3 Rationale

As from clause 6.5.3.1. in TS 33.122 [1], (for Release 18) the scope of an API invoker on a UE in Resource owner-aware northbound API access (RNAA) is limited to accessing its own resources only, i.e., resource owner is a user of the UE hosting the API invoker that can authorize the API access.

TS 23.700-22 [2] has a key issue to study that case in Release 19. Security aspects need to be studied. This document proposes a key issue to TR 33.700-22 [3] to study security aspects of that enhancement.

# 4 Detailed proposal

It is proposed to approve the following change to TR 33.700-22 [3].

\*\*\* 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".

[Z] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs"

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

## 5.X Key Issue #X: Authorizing API invoker on one UE accessing resources owned by another UE

### 5.X.1 Key issue details

This key issue addresses the security aspects of TR 23.700-22 KI #6.

It studies the security aspects for the case that API invoker(s) are deployed on the UE and can access resources (hosted in the network) related to another UE (e.g., application client on UE is fetching location of another UE or setting QoS for PDU sessions of another UE), in accordance with TR 23.700-22 [X].

As specified in 3GPP TS 23.222 [Z], the API invoker may be deployed in any of the following ways:

a. API invoker may be deployed as AF on the UE (i.e. 3rd party application).

b. API invoker may be deployed as AF on the UE supporting several other 3rd party applications deployed on the UE.

c. API invoker may be deployed on the network as AF.

According to TS 33.122 [Y] of Rel-18 Resource Owner-Aware Northbound API Access (RNAA), an API invoker deployed on a UE is only authorized to request resources owned by its own UE.

This key issue covers the security aspects necessary to support API invoker(s) deployed on one UE to request access to resources owned by other UEs.

### 5.X.2 Security threats

Without a proper security mechanism, unauthorized API invokers can access to resources related to a UE, which potentially results in sensitive information leakage and unauthorized modification to the resources accessed by northbound APIs.

### 5.X.3 Potential security requirements

An authentication and authorization mechanism should be supported to allow the case of accessing resources related to a UE by an application residing on another UE.

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

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.

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