**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-230337-r1***

**Electronic meeting, 16 - 20 January 2023**

**Source: Samsung**

**Title: Update of Key Issue #2**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***The contribution proposes update of KI#2 in TR 33.884***

# 2 References

[1] 3GPP TS 22.261: "Service requirements for the 5G system".

[2] S6-223489: "LS reply on CAPIF authorization roles related to FS\_SNAAPP".

# 3 Rationale

This contribution proposes to update KI#2 based on SA1 requirement and reply LS from SA6.

Following requirements are captured in TS 22.261 [1];

The 5G system shall be able to:

- provide a third-party with secure access to APIs (e.g. triggered by an application that is visible to the 5G system), by authenticating and authorizing both the third-party and the UE using the third-party's service.

- provide a UE with secure access to APIs (e.g. triggered by an application that is not visible to the 5G system), by authenticating and authorizing the UE.

- allow the UE to provide/revoke consent for information (e.g., location, presence) to be shared with the third-party.

- preserve the confidentiality of the UE's external identity (e.g. MSISDN) against the third-party.

- provide a third-party with information to identify networks and APIs on those networks.

Based on the fourth requirement, SA3 needs to consider privacy related issue while providing a method for the 5G system to identify a UE.

In addition, the reply LS from SA6 (S6-223489 [2]) states that "it is acceptable to assume that the resource owner is the UE's user, or the UE's user has been given permission by the subscriber to authorize access to the resource all scenarios considered by SA6". Therefore the following Editor's Note can be deleted;

Editor's Note: need to check with SA6 whether this is a correct interpretation of the SA6 use cases.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.2 Key Issue #2: Checking authorization before allowing access

### 5.2.1 Key issue details

Resource owners need to be able to control access to their resources. In the use cases described in TR23.700-95, the resource owner is the UE's user, or the UE's user has been given permission by the subscriber to authorize access to the resource.

### 5.2.3 Potential security requirements

1. Authn-1-ResOwner: when giving or revoking authorization, the resource owner shall be authenticated.
2. Authz-1-General: Access to resources of the resource owner via the northbound APIs shall only be allowed if the resource owner has authorized it.
3. Authz-2-App: Authorization shall be given to an application. Authentication of applications by the operating system of the UE is out of 3GPP scope.

Authz-3-OtherSub: In case it is not the resource owner triggering the AF to invoke an API, the triggerer UE of the AF shall be authorized by the resource owner to access the resource through the API.

Editor's Note: this requirement is FFS taking into consideration the reply from SA6.

1. Authz-4-Scope: The 5G system shall be able to limit the scope of API requests to resources owned by a resource owner.

Authz-5-Revoke: The resource owner shall be able to revoke authorization at any time. From then on access to resources based on the revoked authorization shall not be allowed.

The 5G system shall be able to preserve the confidentiality of the UE's external identity (i.e., MSISDN) against a third party.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*