**3GPP TSG-SA WG6 Meeting #49-e S6-221114**

**e-meeting, 16th – 25th May 2022 (revision of S6-22xxxx)**

**Title: LS on CAPIF authorization roles related to FS\_SNAAPP**

**Response to:**

**Release: Release 18**

**Work Item: Study on application enablement aspects for subscriber-aware northbound API access (FS\_SNAAPP)**

**Source:** **3GPP TSG SA WG6#49-e**

**To: 3GPP TSG SA WG3**

**Cc:**

**Contact person: Yuji Suzuki**

 **yuuji.suzuki.rm@nttdocomo.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** **Draft TR 23.700-95 v1.3.0**

# 1 Overall description

SA6 has been studying in TR 23.700-95 the enhancements to the existing CAPIF functional model so that the CAPIF can support the subscriber-aware northbound API access (SNA), a scenario in which the northbound API invocation requires the API invoker obtaining the user’s (i.e. resource owner’s) consent before being allowed to access the resource.

The SA6 study has taken into account both use cases of obtaining user’s consent while the user is online as well as enabling the user to provide in-advance consent as a matter of convenience (i.e. not to get bothered with consent pop up screen while online) as well as enabling offline type of use case (i.e. enabling the App server making API calls while the user is not actively engaged on the UE).

In the SA6 study, we assume that, in CAPIF, the API invoker may be different from the resource owner, and that the AEF exposes the protected resources related to the resource owner. This is a major change in assumption, as the existing CAPIF specification in TS 33.122 assumes that the API invoker performs the functions of the resource owner (as highlighted in green below).

The CAPIF functional models are being enhanced to accommodate the aforementioned additional feature (i.e. obtaining user consent both for online and offline use cases prior to API invocation).

|  |
| --- |
| As per OAuth 2.0 [4], the CAPIF core function shall perform the functionalities of the Authorization and token protocol endpoints, the API invoker shall perform the functions of the resource owner, client and redirection endpoints functionalities, while the API exposing function shall perform the resource server functions. The API invoker client (Client endpoint) shall be registered as a confidential client type with an authorization grant type of ‘client credentials'. The access token shall follow the profile described in annex C. |

As part of the FS\_SNAAPP study while taking into account TS 33.122 and the specified OAuth 2.0 CAPIF functional security model, the following key architectural points stood out:

a. The OAuth 2.0 authorization server (enabling Authorization and token protocol endpoints) should generally be in the same domain as the resource server function. Thus, the OAuth 2.0 authorization server is expected to be in the API provider domain of the 3rd party trust domain if the user’s resource being accessed is within the span of control of the 3rd party (i.e. user’s resource is outside of PLMN).

b. When the API provider domain is within the PLMN trust domain, the functionalities of the OAuth 2.0 authorization server (enabling Authorization and token protocol endpoints) reside in the CAPIF core function.

c. According to the descriptions in TS 33.122, the 3rd party API provider may use the authorization functionalities of the CAPIF core function even when the API provider domain is within the 3rd party trust domain, at least when the CAPIF uses the client credential flow. Thus, in the current specification, the API provider in the 3rd party domain may choose whether it implements the authorization mechanisms by itself (as shown in the point a above, and this is out of 3GPP's scope) or it relies on the CAPIF core function's authorization functionalities.

Based on the analyses above, SA6 would like to get the following feedbacks from SA3:

1. SA6 would like to know if the points a-c listed above are aligned with SA3’s perspective.

2. Clause 6.2 of TR 23.700-95 contains potential functional models for SNAAPP. SA6 would like SA3 to assess the functional models and provide feedback on their viability (for two cases where the API provider domain is within and outside the PLMN trust domain).

3. Currently, in TS 33.501 Annex V, the user consent data are stored in the UDM/UDR as subscription data (an in-advance consent). SA6 would like to get SA3’s view for the online user consent check option (the user consent is checked upon the API invocation) in FS\_SNAAPP study.

# 2 Actions

**To SA3**

**ACTION:** SA6 asks SA3 to provide feedback on the above questions.

# 3 Dates of next TSG SA WG 6 meetings

SA6#49-bis-e 22nd June – 1st July 2022 e-meeting

SA6#50 22nd August – 26th August 2022 meeting