**3GPP TSG-SA3 Meeting #108AdHoc-e  *S3-222909-r1***

**e-meeting, 10 – 14 October 2022**

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

**Response to: S3-221731=S3-221568 / *S6-221771***

**Release: Release 18**

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

**Source:** **3GPP TSG SA WG3**

**To: 3GPP TSG SA WG6**

**Cc:**

**Contact person: Alf Zugenmaier**

 **NTT DOCOMO**

 **zugenmai@hm.edu**

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

# 1 Overall description

SA3 would like to thank SA6 for their LS on CAPIF authorization roles related to FS\_SNAAPP.

SA3 has just started studying in TR 33.884 security aspects of the SA6 study on enhancements to the existing CAPIF functional model so that the CAPIF can support the subscriber-aware northbound API access (SNA).

Since it is mentioned in the description on SA6's LS, SA3 would like to ask whether for the current release of the standard resource owner+ in the scenarios considered by SA6 is always the user .

SA3 would like to provide the following preliminary feedback to SA6 questions. :

*1. SA6 would like to receive feedback on the solutions in the TR that are identified with SA3 dependency.*

**Answer:** SA3 will study the solutions for which SA6 has identified an SA3 dependency.

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. Especially, SA6 would like SA3 to provide feedback on the following points:*

i. *For cases where the API provider is within the PLMN trust domain, whether the authorization function in Figure 6.2.1.2.1-1 should be located inside the CAPIF core function, outside the CAPIF core function (i.e., within the API provider domain), or both options are acceptable.*

**Answer:** SA3 will study possible architectures and will provide feedback as the study progresses. In order to progress work, SA3 recommends to consider Authorization Function (AZF) as separate until the study has progressed, keeping in mind that it may be better to integrate it into the CCF, i.e. reuse CCF API definitions as much as possible for AZF.

ii. *For cases where the 3rd party API provider is outside the PLMN trust domain, whether the authorization function can be located in CAPIF core function of PLMN trust domain or in the 3rd party trust domain to address the authorization related to resource owners belonging to 3rd party API provider.*

**Answer:** This will depend on whether the 3rd party API provider trusts the PLMN to correctly perform authorization. SA3 considers scenarios in which this is not the case as out of scope for 3GPP.

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 option to retrieve authorization from subscriber upon the API invocation, as described in Solution #3.*

**Answer:** SA3 will study API authorization (based on consent from resource owner) and relationship to existing user consent mechanism taking into account near real time requirements. SA3 would prefer to postpone specification of authorization function actively contacts the resource owner for API invocation after R18.

4. *Currently, in Solution #3, the assumption is that the API provider decides which APIs require authorization from subscribers. SA6 would like clarifications on whether SA3 considers in scope of their study options for the resource owner to also provide such configuration (e.g. request authorization triggering even if not required by API provider).*

**Answer:** SA3 considers in scope of their study the security of options for the resource owner to provide such configuration, if such a functionality is required.

Furthermore there was discussion about whether currently use cases foreseen for R18 cover M2M UEs (i.e. UEs without user or user interface) for the resource owner. SA3 would like to ask SA6 to clarify this.

# 2 Actions

**To SA6**

**ACTION:** SA3 kindly requests SA6 to take the above into consideration and to provide feedback on the above question:

- Is it acceptable to assume 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?

 - Is it acceptable to postpone specification of authorization function actively contacting the resource owner for API invocation to after R18.?

 - Do use cases foreseen for R18 cover M2M UEs as resource owners?

# 3 Dates of next TSG SA WG 3 meetings

SA3#109 14 - 18 November 2022 Toulouse

SA3#109-adhoc 16 – 20 January 2023 TBD