**3GPP TSG-SA3 Meeting #119 *draft\_S3-244927-r7***

Orlando, USA, 11 - 15 November 2024

**Title: Reply-LS on clarifications on consent management – Update to S3-242374**

**Response to: LS S3-241741 on clarifications on consent management from GSMA OPG**

**Release: n/a**

**Work Item: n/a**

**Source:** **3GPP SA3**

**To: 3GPP SA**

**Cc: 3GPP SA2, SA6, CT3, CT4**

**Contact person: Anja Jerichow**

 **anja dot jerichow at nokia dot com**

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

**Attachments:** none

# 1 Overall description

SA3 kindly asks SA to consider the following additional input as update proposal to SP-240551 for consideration in SA’s final LS response to OPG in response to the OPG LS SP-240527/OPG\_173\_Doc\_04 in which OPG specifically asks SA3 to respond to questions related to their new work item on privacy management.

3GPP TSG SA WG6 has specified the support of RNAA (Resource owner-aware Northbound API Access), as part of CAPIF in Rel.18 in TS 23.222, and the detailed security specification for CAPIF RNAA has been specified by SA3 in TS 33.122 (CAPIF). Recently 3GPP TSG SA WG SA6 initiated a Rel.19 study, which includes in its scope further enhancement to CAPIF for resource owner authorisation management (RNAA). GSMA OPG is invited to provide any feedback to the on-going studies captured in TR 23.700-22 (SA6) and TR 33.700-22 (SA3).

*Q1. When NEF or EES (as trusted AF) is exposing APIs using CAPIF RNAA, how is NEF or EES utilizing the UDM’s user consent information for processing authorization for API consumer/invoker?*

3GPP user consent framework, Annex V of TS 33.501: User Consent Subscription Data (UcSubscriptionData) is specified in 3GPP TS 29.503 as subscription data stored in the UDR. This data can be retrieved from UDR by UDM and from UDM by any other authorized NF (e.g., NWDAF, NEF). Permanent subscription data within this framework can be modified only by provisioning/administration means. User Consent Subscription Data is used by the NF which is deemed an enforcement point for user consent. The user consent parameters, which are bound to a SUPI/GPSI and purpose of data processing, include whether the user consent is granted or not. Annex V provides technical means to be used when it is required by regional regulations or operator’s local policy, not otherwise.

The CAPIF RNAA mechanism is about getting authorization from the resource owner for accessing protected resources per user (resource owner identifier), per application (API invoker identity), per API, and per scope and purpose (of data processing) in support of the framework. This could be used to authorize accessing privacy-related (sensitive) information. CAPIF can serve both 3GPP and non-3GPP (CAPIF) API Exposing Functions and the resource owner can be a user or a subscription owner. Rel-18 CAPIF RNAA specification only states that authorization-related information is available in the CCF. There is no further specification about the storage of the information.

Today the UDM’s user consent information stored in UDR in line with the framework specified in TS 33.501 does not provide per AF granularity. Hence, it does neither concern consent information for AF/EES applications northbound of the NEF, nor for the APIs that these applications use, nor for the scope/purpose of these used APIs.

*Q2. What is the relationship between CAPIF RNAA and UDM’s user consent information? Is there any plan/roadmap for a unified approach?*

Answer:

There is currently no relationship. Whether a unified approach related to user consent can be achieved would require additional study in 3GPP. 3GPP SA will keep GSMA OPG informed.

*Q3. For the UDM’s user consent information, are the user consent management aspects (e.g. capturing or revoking user consent from the subscriber) specified? Please illustrate.*

Answer:

Please refer to the answer to Q1. In addition, how the user consent record gets created in the first place or changed later on is not part of 3GPP specification since this depends on operator practices, e.g., if there are OAM systems, Customer Care systems, etc.

*Q4. Is there any plan/roadmap for considering other legal bases for processing personal data apart from user consent (e.g. contract, legal obligations, vital interests of the data subject, public interest, and legitimate interest [GDPR]) in a unified way?*

Answer:

Data controllers (operators) handling of personal data usually depends on legal jurisdiction ("legal basis for processing personal data"). 3GPP can only provide the technical mechanisms to enable the operators to fulfil legal aspects.

*Q5. What are the privacy considerations in 3GPP with respect to exposure of sensitive information (e.g. UE ID, location) to untrusted AFs.*

Answer:

3GPP can only provide technical mechanisms to store sensitive information securely and to restrict access to those authorized.

SA3 kindly asks SA to consider this input in their LS response to OPG.

# 2 Actions

**To 3GPP SA and SA2, SA6, CT3, CT4**

**ACTION:** 3GPP TSG SA3 asks 3GPP TSG SA to consider the above information in their reply to GSMA OPG.

# 3 Dates of next TSG SA WG 3 meetings

SA3#120 24 – 28 February 2025 Athens (Greece)