**3GPP TSG-SA Meeting #104 SP-240732**

**Shanghai, PRC, 18-21 June 2024**

**Title: [DRAFT] Reply LS on clarifications on consent management**

**Response to:** **LS on clarifications on consent management from GSMA OPG (SP-240527)**

**Release: Rel.18**

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

**To: GSMA OPG**

**Cc: 3GPP SA WG2, 3GPP SA WG3, 3GPP CT WG4, 3GPP CT WG3, 3GPP TSG SA WG6**

**Contact person: Alessio Casati**

**alessio.casati@nokia.com**

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

**Attachments:** None

# 1 Overall description

3GPP TSG-SA thanks GSMA OPG for their LS on clarifications on consent management.

3GPP TSG SA would like to clarify that 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. Additionally, 3GPP TSG SA WG SA6 has initiated a Rel.19 study on CAPIF (FS\_CAPIF\_Ph3 in [SP-231357](https://www.3gpp.org/ftp/TSG_SA/TSG_SA/TSGS_102_Edinburgh_2023-12/Docs/SP-231357.zip)), which includes in its scope further enhancement to CAPIF for user consent management (RNAA). GSMA OPG is invited to provide any feedback to the on-going study captured in TR [23.700-22](https://www.3gpp.org/dynareport/23700-22.htm).

3GPP TSG SA would like to inform that the purpose of the user consent framework Annex V in TS 33.501 is for providing technical means to manage subscriber permissions at the operator domain such that Network Functions of the 3GPP system can request or can be provisioned/configured with subscriber-related data in accordance with local laws and regulations. These permissions are stored in UDM/UDR.

In addition, it is worth mentioning that there are two other specifications that also handle consent, namely:

- TS 23.273– UE LCS Privacy profile, that apply for user consent enforcement in the 5G System Location Services (i.e., UE LCS privacy feature). This includes the enforcement of user consent for LCS services in GMLC and NEF (when location services are accessed via NEF).

- TS 32.422– MDT User Consent, that apply for user consent enforcement for the mechanisms used for the control and configuration of the Trace, Minimization of Drive Test (MDT).

UE LCS Privacy profile and MDT User Consent information are stored in UDM/UDR.

In addition to above comments, the following answers are provided to the received questions.

**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 TSG SA Answer**: see answers in Q2.

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

**3GPP TSG SA Answer:** User Consent Subscription Data (UcSubscriptionData) is specified in 3GPP TS 29.503 as permanent subscription data stored in the UDR. This data can be retrieved from UDR by UDM and from UDM by any other authorized Network Function (e.g. NEF). Permanent subscription data can be modified only by provisioning/administration means at the UDR..

The CAPIF RNAA is about subscriber’s authorization/permission to a requesting AF enabling the AF to access subscriber resources. The consent mechanism enabled by RNAA, has different granularity in support of different use cases for exposure of subscriber related network resources via APIs. In Rel.18, only a UE accessing its own resources is considered if the requesting AF is on a UE.

At present these two mechanisms are independent of one another. ~~A unified approach could be investigated in 3GPP in a contribution driven manner.~~

**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.

**3GPP TSG SA Answer:** 3GPP TS 33.501, Annex V describes the user consent framework and mentions revocation in the context of informing/notifying on any changes done on the subscription details. Hence, it allows a Network Function to get notified if user consent information has been changed or revoked in UDM/UDR. In addition, for instance, according to 3GPP specifications (e.g. TS 23.502), the user consent is checked by the UDM for MSISDN exposure where the user consent is managed by the MNO. However, the user consent management (e.g., capturing or revoking user consent from the subscriber) is not specified.

**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?

**3GPP TSG SA Answer:** Data controllers (operators) handling 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.

**3GPP TSG SA Answer:** Whether exposure to an untrusted AF is allowed, may depend on operator policy or also on legal jurisdiction and hence is not handled by 3GPP. 3GPP can only provide technical mechanisms to store sensitive information securely and to restrict access to authorized consumers.

# 2 Actions

**To GSMA OPG**

**ACTION**: 3GPP TSG SA asks GSMA OPG to consider the above information

# 3 Dates of next TSG SA WG6 meetings

3GPP SA#105 September 10th -13th "2024 Melbourne, Australia

3GPP SA#106 December 10th -13th "2024 Madrid, Spain