**3GPP TSG-SA3 Meeting #116 *draft\_S3-242374-r4***

Jeju, South Korea, 20th - 24th May 2024 revision of *S3-241968*

**Title: Reply-LS on clarifications on consent management**

**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:** DocNumber(s) [Description e.g.. Draft TS 29.414 v0.1.0].
**!! WARNING !!** Do not insert the file directly as an object in this Word document.

# 1 Overall description

3GPP SA WG3 would like to provide to 3GPP SA input on the LS S3-241741/OPG\_173\_Doc\_04 from GSMA OPG, in which OPG specifically asks SA3 to respond to questions related to their new work item on privacy management.

3GPP SA3 has studied user consent and privacy in previous releases.

The purpose of the user consent framework Annex V in TS33.501(R17) 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 in some format, namely:

* TS 23.273– UE LCS Pr3GPPivacy  profile (R16), 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 by an external AF or internal AF via NEF).
* TS 32.422– MDT User Consent (R16), that apply for user consent enforcement for the mechanisms used for the control and configuration of the Trace, Minimization of Drive Test (MDT).

Hence, information stored in UDM/UDR and CCF, with respect to TS 23.273, TS 32.422, TS 23.222 and TS 33.122 should be independent from each other to avoid conflicting scenarios that can be a violation to privacy laws and regulations.

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?*

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

Answer to Q1 & Q2:

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 NF (e.g. NEF). Retrieval of permanent subscription data that can be modified only by provisioning/administration means locally at the UDR. This framework describes therefore a static handling of user consent in UDM. Hence consent framework in Annex V is not suitable for consent control in runtime at the CAPIF RNAA layer.

The CAPIF RNAA is about authorization/permission to use resources, it has different granularity, semantics (e.g. including authorized requesting AF, UE) and could be used for other purposes. CAPIF RNAA does not authorize data sharing in a lawful sense.

*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:

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 via OAM.

*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 usually depends also on legal jurisdiction (”legal basis for processing personal data”). 3GPP can only provide the technical mechanisms to enable the operators to fulfil legal aspects.

It is important to understand that the same data can be processed for different purposes and under different legal bases, but data controllers cannot swap to another legal basis to continue the consent-governed processing, when consent is revoked; if consent is revoked for a purpose, the data controller must honour the revocation.

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

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 those authorized.

# 2 Actions

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

**ACTION:** SA3 asks all 3GPP WGs in cc to take above information into account. Additionally, SA3 asks SA to consolidate and reply to GSMA OPG considering other WG’s replies.

# 3 Dates of next TSG SA WG 3 meetings

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)

SA3#118 14 - 18 October 2024 TBD (India)