**3GPP TSG-SA3 Meeting #116 *S3-242374-r1***

Jeju, South Korea, 20th - 24th May 2024

**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 from GSMA OPG where 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. 3GPP TS 33.501, Annex V, provides a generic framework on user consent that allows network functions to check and retrieve user consent parameters of subscribers at the UDM. The 5GC user consent SBI is related/bound to all the data that belongs to a user and its checking may take place independently (or additionally) to the procedures giving access to an API (access token-granting procedures). While the framework was primarily introduced for network functions, it has been enhanced for also allowing trusted AFs (like in edge or capability exposure) to request user consent information.

API security for resource owner-aware northbound API access has been specified in Rel-18 TS 23.222 and TS 33.122. Further studies are ongoing in Rel-19, which also include the aspect of how to manage resource owner consent that allows an API exposure function to retrieve consent parameters.

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 23.503 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). This framework on user consent has been specified for retrieval of permanent subscription data that can be modified only by provisioning/administration means locally at the UDR. This framework describes a static handling of user consent in UDM. Hence it remains unclear, whether the same could also be used for runtime user consent (as in RNAA). Which data is still useful to retrieve from UDM/UDR when triggered by the API exposing function (AEF) needs further studying. A Rel-19 study on CAPIF RNAA aspects is ongoing in 3GPP TR 23.700-22.

So far, 3GPP TS 23.222 (CAPIF) only specifies that “The API exposing function (e.g. NEF, SCEF) acts as a resource owner consent enforcement point as specified in 3GPP TS 33.501 and interacts with the authorization function in the CAPIF core function via CAPIF-3. The API exposing function (AEF) can retrieve the resource owner consent parameters from the authorization function” at CCF which is different from UDM/UDR.

Hence, information stored in UDM/UDR and CCF shall be independent from each other to avoid conflicting scenarios. Application-related consent management should take place in CAPIF since it allows rather runtime dynamics.

Whether there could be a unified approach, has not been discussed in 3GPP, i.e. whether RNAA user consent and UDM user consent handling can be unified. But as long as the solutions are orthogonal (i.e., covering non-overlapping scenarios), it should not be an issue supporting multiple frameworks.

*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 NF to get notified if user consent information has been changed or revoked. 3GPP TS 23.502 describes how the AF can modify the content in the UDM subscription data on very specific scenarios (for instance for Expected UE Behaviour). “The AF provides one or more parameter(s) to be created or updated, or deleted in a Nnef\_ParameterProvision\_Create or Nnef\_ParameterProvision\_Update or Nnef\_ParameterProvision\_Delete Request to the NEF.” “If the AF is authorised by the NEF to provision the parameters, the NEF requests to create, update and store, or delete the provisioned parameters as part of the subscriber data via Nudm\_ParameterProvision\_Create, Nudm\_ParameterProvision\_Update or Nudm\_ParameterProvision\_Delete Request message”, and then that information (of parameter provision changes) triggers the UDM to update the parameters. Whether this mechanism is also applicable to UcSubscriptionData is under discussion, since it has been considered so far as permanent subscription data stored in the UDR.

Please see the below figure for an illustration from 3GPP TS 23.502:

|  |
| --- |
| 4.15.6.2 NEF service operations information flowFigure 4.15.6.2-1: Nnef\_ParameterProvision\_Create / Nnef\_ParameterProvision\_Update / Nnef\_ParameterProvision\_Delete request/response operations |

*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:

Processing contracts is supported by the UDM via a static approach when a subscriber is registering with the operator in general. The UDM captures generic user consent for NFs (NWDAF, EES, MDT) and whether user’s data processing is allowed or not. UDM does not capture further granularity that might be requested by an API: it does not capture information that might be requested by the API like application ID, application-related purpose, and scope.

Other Legal bases are outside the scope of 3GPP because it depends on regional laws and jurisdictions (e.g., what is considered “public interest” or “vital interest” is rather relative). 3GPP can only provide the technical mechanisms to allow fulfilment 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:

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 mechanisms to store sensitive information securely and to restrict access to those authorized. While interfacing with untrusted AFs, it is recommended to have NEF (or EES for interacting with third-party edge application servers) in place.

# 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)