**3GPP TSG-SA3 Meeting #103-e *draft\_S3-212123-r4***

e-meeting, 17 - 28 May 2021

**Title: LS on User consent**

**Response to:**

**Release: Rel-17**

**Work Item: UC3S**

**Source: SA3**

**To: SA2**

**Cc:**

**Contact person:**

**Name:** Anja Jerichow

**Email Address:** anja(dot)jerichow(at)nokia(dot)com

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

**Attachments:**

# 1 Overall description

SA3 would like to inform SA2 on the work status of user consent study in TR 33.867 regarding user consent and revocation.

In the context of eNA, data is processed for specific purposes and provided to external applications. Thus, a solution for user consent is important to have in Rel-17 along with the normative eNA feature currently progressed by SA2. SA3 has so far identified key issue #2 on “User consent for UE data collection” and key issue #3 "Modification or revocation of user consent" in TR 33.867, for which solutions are needed.

SA3 would like to mention: all mechanisms for user consent need to be specified as "may" since requirements vary across regulatory environments. It is not in the remit of SA3 to decide in detail with data (raw data, analytics reports, models, etc.) might be subject to user consent in certain legal jurisdictions, therefore, below requirements and recommendations are for "data subject to user consent".

SA3 would like to provide the following comments on SA2 conclusions in KI#15 User consent for UE data collection/analysis:

\*\*\*\*\*\* **Comments below related to telco / company view to be deleted below \*\*\*\*\*\***

|  |  |  |
| --- | --- | --- |
| **23.700-91 conclusions on KI#15 User consent for UE data collection/analysis** | | **SA3 comments** |
| a) | UDR (via UDM services) holds the user consent for user related data **which is provisioned by MNO as a user subscription information.**  **Comments from telco**  Need to have an agreement, **where** to store the user consent  Whether new service for tracking to be discussed 🡪Not to be part of Nudm\_SDM service.  Can we agree on UDM storing! OK.  Clarify provisioned/managed (more than one time provision) by MNO as a user subscription information.  Tracking (see e)  checking the UC? Where to put the policy enforcement point. | **Proposed response per LS**  There is general agreement in SA3 that UDR (via UDM services) holds the user consent for user related data which is stored as a user subscription information.  Nokia: since already user consent is provided by UDR via UDM in MDT case, it is useful to have a similar mechanisms for other use cases, thus, it is recommended that for UE data collection and analytics, the UDR (via UDM services) holds the user consent  Huawei: we are fine that UDR (via UDM services) holds the user consent. However, the services should be extensible so that the services can cover other user consent scenario, e.g. MEC.  Ericsson: Okay. UDM/UDR manages already user consent for other services as subscription data and it should be OK to manage consent for other services/UCs, preferably in a generic way.  Mind though that considering user consent “as a user subscription information (in UDM)” implies making use of the existing services for Subscription Data Management, i.e., Nudm\_SDM. This includes the possibility for an NF consumer to Get user consent data and Subscribe to get Notifications of changes of user consent data from UDM.  In other words, the Nudm\_SDM service does not support any tracking functionality as discussed in bullet e). The requirements for such tracking functionality will determine the service and the NF exposing such service. |
| b) | A service provider (external to MNO domain) may use NEF parameterProvision\_Update service to update or to revoke the user consent to the UDM/ UDR (when applicable).  **Comments from telco**  Third party should not manage operator UE subscription database  Separation of User consent mgmt., i.e. **separate by operator / AF (i.e. each legal entity has its own responsibility)**  **🡪 technical separation**  User consent for data input by ext AF – such consent shall be managed by this AF i.e. each one is responsible for its own parts.  If data comes from AF (controller), then the MNO is only the processor. Controller always has to manage. | **Proposed response per LS**  A service provider (external to MNO domain, i.e. a third party), should not be able to manage/modify the operator's UE subscription database. However, the UDM/UDR can hold as part of the UE subscription database technically separated user consent information, one used by external parties, one used by the MNO, such that it can be assured that only the correct legal entity can update or revoke user consent. The data controller is the one also managing the data, e.g. if an AF stores data in UDM/UDR, from a legal point of view it must be also be the AF managing user consent related data.  Nokia: allowing an external entity to update or revoke user consent in UDM/UDR **may result in new security risks** and is therefore not recommended  Huawei: this is much relying on difference service security requirements, and should be extensible for kinds of services. This is one possible way to update and modify user consent. Since there is some existing mechanism for AF authentication and authorization, **we don't see any new security risk**.  Ericsson: Not okay for now. Needs to be further studied. The issue is whether we are allowing a company quite far down on the supply chain to be able to dictate the actions for those higher up, in essence changing the position of the controller/processor relationship. Issues could arise from an improper data subject check or **demanding data deletion based on consent when a different legal basis has been used.** |
| c) | Alternatively, the user consent parameter **may be configuredby MNO** in the UDM/UDR (when applicable).  **Comments from telco**  Unclear term. Configured ???  Write/manage? (what is meant that an operator receives user consent and e.g. OAM takes user consent infos provided and updates the subscription database accordingly) | **Proposed response per LS**  It is useful to allow an operator to manage user consent parameters in the UDM/UDR, i.e. the data provided by user consent need to be written in the subscription database.  Nokia: It is useful to allow an operator to configure user consent parameters in the UDM/UDR.  Huawei: agree with Nokia.  Ericsson: Okay. |
| d) | Another option is the ASP configures the ASP's Application in UE to provide input data only if user consent is obtained.  **Comments from telco**  ASP shall configure in UE, provide the input, out of scope | **Proposed response per LS**  SA3 would like to point out that "configuration of ASP's application in UE to provide input data only if user consent is obtained" is not in the remit of 3GPP scope.  Nokia: Configuration by application service providers is out of scope in 3GPP.  Huawei: out of 3GPP scope, but can be an alternative.  Ericsson: Okay. |
| e) | A functionality to be provided to support **tracking the distribution and usage** of any user related information that may be subject to user consent.  NOTE 1: Whether the functionality described in bullet item e) is hosted by NWDAF, DCCF (and possible interactions with DRF) or as a standalone NF is decided in normative phase in alignment with SA WG3 feedback.  **Comments from telco**  SA3 requirement on tracking is needed. Who/Where is doing the tracking (SA2 topic???) NOTE 1 – SA2 responsible   * Revocation needed   if SA3 wants to develop solution, we need SA2 architecture   * feedback on tracking   Models (maybe later release?)  But analytics reports??? R17  Tracking to be done by data controller??? How to otherwise do the revocation? Controller need to know which processor to contact.  What should be tracked? Entities, who have a copy of the data.  For this NF ids need to be known.  🡪 tracking of any user related information that may be subject to user consent.  Are analytics reports (mobility report single UE) are subject to UC?  This depends on regulations. But we need to provide the possibility to revoke. | **Proposed response per LS**  SA3 agrees that a functionality to support tracking is needed. TR 33.866 also includes a potential security requirement on this. Where this functionality is hosted, is up to SA2 decision.  Nokia: It is proposed to host this service in UDM/UDR, as already user consent information is stored there, and thus different user consent for different use cases would be all in one place.  A new standalone NF seems to be not necessary for tracking the distribution and usage of user related information, when UDM already holds subscriber data and subscription details.  Huawei: We need more time to investigate details. But in general, we are fine to **introduce a functionality to support tracking NFs** who are using data subject to user consent.  Ericsson: Not okay for now. Needs to be further studied. SA3 first needs to define requirements on tracking. **Then how to achieve** that (with UDM or new NF) can be left **to SA2**. So, SA3 should indicate that requirements are not yet defined by SA3 and will come back later. |
| f) | The functionality described in bullet item e) subscribes to the UDM/UDR to receive notifications for any changes in the user consent.  **Comments from telco**  Depends on decision, **where** to host (SA2 issue) | **Proposed response per LS**  Whether the functionality to be defined in SA2 needs to subscribe to notifications for changes in the user consent depends on where it is hosted. When hosted in UDM/UDR, this is obsolete.  Nokia: this is not needed, if hosted by UDM/UDR.  Huawei: Huawei: We need more time to investigate this issue. But in general, we are fine to introduce a functionality to support tracking NFs who are using data subject to user consent.  Ericsson: Same comment as in (e). |
| g) | If a requested data is subject to user consent, the NWDAF and/or the functionality described in e) may check the user consent from the UDM/UDR before the data collection.  NOTE 2: This does not preclude that also other entities (e.g. AMF or SMF) to check availability of user consent with UDM/UDR.  **Comments from telco**  Mention that SA3 has 2 solutions in TR (policy enforcement) – SA3 continuous to study | **Proposed response per LS**  SA3 TR 33.866 has currently 2 potential solutions recorded, whether user consent checking is done by NWDAF or by the data provider has not been decided so far. SA3 will report on this later.  Nokia: Checking user consent from UDM/UDR should be supported by any NF.  Huawei: Agree with Nokia.  Ericsson: Not okay for now. Needs to be further studied. This is premature. SA3 has not decided if the consent checking is done by NWDAF or data provider. SA3 and will come back later. |
| h) | User consent for the user data provided by a data source to a data consumer may have a **validity time.** On expiry of this validity time, the user data should be either **deleted or the user consent for this data to be renegotiated**.  **Comments from telco**  Anonymized data is not PII  Data subject to user consent – requ. on deletion needed  Renegotiation? Also ok to have. | **Proposed response per LS**  SA3 agrees that providing a validity time of user consent seems to be useful as it allows to reduce the amount of tracked data. Deletion and renegotiation are important to have. Note, only for data that is subject to user consent, a requirement on deletion and renegotiation exists. Anonymized data is not considered as personal identifiable data anymore.  Nokia: Providing a validity time of user consent seems to be useful as it allows to reduce the amount of tracked data. It then is the responsibility of the entity that stores user consent that data can be wiped after the validity time passed.  Huawei: Agree with Nokia.  Ericsson: Okay but must be clarified that only \*raw\* or personally identifiable data is under the scope. |
| i) | (Subject to applicability of Data Protection Regulations) in case of user consent revocation at UDM/UDR, NWDAF deletes the related user data and terminates the data collection from the corresponding source NF.  **Comments from telco**  Optional to support and to use  Use phrases such as “If consent is required, then it shall …” | **Proposed response per LS**  SA3 agrees on the principle of user revocation. It is currently discussed in SA3. SA3 will define necessary mechanisms and/or requirements and will inform SA2.  Nokia: Since different regulations can provide different requirements on user consent revocation, it is important to allow for revocation.  Huawei: Agree with Nokia.  Ericsson: Okay in principle. We should clarify that 3GPP can only specify "may" for everything related to consent. "shall" shall not be used because of different regulations. |
| j) | (Subject to applicability of Data Protection Regulations) in case of **user consent revocation** (at UDM/UDR), the functionality described in bullet item e) may send a request to NWDAF service consumer(s) to delete the related user data/ analytics.  **Comments from telco**  SA3 to commit on req. arch in SA2 scope, but pls keep SA3 informed  Where policy is enforced, this is different from deletion/revocation request  Enforcement is where the data has been propagated too (e.g. AMF).  Policy enforcement points & data operator  Pol. Enf. For data collection – data collector or data processor? Mention to SA2.  NWDAF need to know which entity? | **Proposed response per LS**  SA3 agrees with the requirement that in case of user consent revocation, it must be possible to delete related user data and related data analytics subject to user consent. Since the architectural design is in scope of SA2, please inform SA3 on the specified solution. Please note, that it is important to decide where the policy enforcement point is, i.e., the policy may be enforced at a different network function than the one requesting deletion and revocation. It must be clearly stated, who is the data collector and who is the data processor.  Nokia: In case of user consent revocation it must be possible to delete related user data and related data analytics.  Huawei: Agree. In case of user consent revocation, it is a way to delete the related user data/analytics immediately.  Ericsson: Have to wait for agreement on (e). |
| k) | (Subject to applicability of Data Protection Regulations) in case of user consent revocation (at UDM/UDR), NWDAF service consumer(s) may delete the related user data/analytics on request (refer to bullet item j) or on expiry of validity time (refer to bullet item h). | **Proposed response per LS**  NWDAF service consumers shall delete the related user data/analytics subject to user consent on request or expiry in line with regulatory jurisdiction.  Nokia: A requirement in line with the conclusion should be added. I.e. NWDAF service consumer(s) may delete the related user data/analytics on request or on expiry of validity time.  Huawei: Agree. In case of user consent revocation, it is a way to delete the related user data/analytics passively.  Ericsson: Same comment as (i). |

# 2 Actions

**To SA2**

**ACTION:** SA3 asks SA2 to take this information into account to allow progressing normative work on user consent and user consent revocation in TS 23.288.

# 3 Dates of next TSG SA WG 3 meetings

SA3#103Bis-e 5 - 9 July 2021 Electronic meeting (TBC)

SA3#104-e 16 - 27 August 2021 Electronic meeting