**3GPP TSG-SA3 Meeting #105-e *draft\_S3-220168-r3***

**e-meeting, 14 - 25 February 2022 (revision of S3-yyxxxx)**

**Source: Huawei, HiSilicon**

**Title: New SID on Study of Enhancement of User Consent for 3GPP Services**

**Document for: Approval**

**Agenda Item: 4.18**

3GPP™ Work Item Description

Information on Work Items can be found at
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study of Enhancement of Security aspects on User Consent for 3GPP Services

Acronym: FS\_eUC3S

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-18

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | X |  |
| No |  |  |  |  |  |
| Don't know | X | X | X |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a Study Item

{Tick one box. "**Feature** / **Building Block** / Work Task" form a hierarchical structure. E.g. no Building Block can be proposed without a corresponding parent Feature. The full structure of all existing Work Items is shown in the 3GPP Work Plan in ftp://ftp.3gpp.org/Information/WORK\_PLAN}

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 930006 | Security aspects on User Consent for 3GPP services | UC3S\_SEC |

**Dependency on non-3GPP (draft) specification:**

# 3 Justification

In R17, SA3 has defined in 3GPP TS 33.501 a general framework applicable to any feature required to handle user consent. The framework includes storage requirements for the UDM as well as generic services for user consent check and revocation. For any such feature, the framework requires the identification, in the standards, of a special NF called the user consent enforcement entity. This has been already done for features such as eNA and MEC in R17.

However, the case that the enforcement entity and UDM belong to different legal domains, i.e. subject to different regulations, has not been considered since for both eNA and MEC roaming scenarios were not included so far. Nevertheless in R18, for these features roaming is to be taken into consideration, e.g. as documented in SP-211330 for R18 eNA, "WT#2.2: Whether and how to support data and analytics exchange in roaming case (including network sharing)", and in SP-211316 for R18 MEC, "WT1 Improvements to roaming, to support access to EHE in a VPLMN."

Another case that was not addressed is about RAN endorsing the role of the enforcement entity. It seems now that many use cases and features would require investigating this, e.g. SON/MDT, NTN, etc. In particular for NTN, SA3 has already replied to an LS from RAN2 in S3-214349 stating that "SA3 has not yet studied how this user consent handling can be used specifically for the NTN use case.".

In SA6, a related R18 study was approved in SP-210476 (SNAAP). The objectives of this study include one related to user consent: "Clarify user consent aspect within CAPIF procedures". Some solutions are already captured in the corresponding 3GPP TR 23.700-95 which does actually include a NOTE emphasizing that the final procedure and requirement are to be specified by SA3.

Further, in Rel-18, more items are expected to deal with user data which requires user consent handlng, e.g. AIML, EEC operations.

Between, current user consent mechanism has the following limitations:

- Current user consent relies on static mechanism, i.e. subscription information in UDM, and there is no procedure to update user consent via interaction with user

- As more applications are available, it will be harder to preconfigure user consent setting for all applications.

- In EDGE, many applications may request privacy data of the same UE and it may be a burden to UDM.

- Consent should have granular definition for enhanced privacy protection (e.g. network can share location info to Application Server-1 when user is in location-y)

Therefore, the continuation of the user consent work is required in SA3 not only to cover the issue described above but also any R18 feature expected to deal with user consent and to address the above mentioned Rel-17 limitations.

# 4 Objective

The aim of this study is to investigate potential enhancements of 5GS that would enable broader use cases in relation with user consent.

The following aspects are in the scope of the study:

1. Investigating the potential issues and solutions in case that enforcement point and UDM belong to different legal entity, e.g. roaming, etc.

2. Investigating the potential issues and solutions in case that enforcement point is RAN.

3. Investigating the potential solutions for dynamic user consent management with user interaction.

4. Identifying target use cases which is relevant to above objectives, e.g. NTT, SNAAP, etc..

NOTE 1: This study will identify use cases which is relevant to the objectives, and produce the general requirements and solutions based on those investigation. The concluded procedures for specific use cases will be finally specified in this use case’s work item.

NOTE 2: Principles, regulations, and definitions related to privacy, which are recognized differently in each different country or area, are taken into account when deriving the concept of user consent for 3GPP users.

NOTE 3: Even where solutions exist to obtain user consent, collection and exposure of user sensitive data should be minimized and identification of the users should only be allowed where critical to the operation of the related feature.

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
|  Internal TR | TR 33.8XX | Enhancement of Security aspects on User Consent for 3GPP Services | TSG#96 | TSG#98 |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| N/A | N/A | N/A | N/A |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Rong Wu, Huawei, Raina.wu@HUAWEI.COM

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

SA2, SA6 and RAN3 may need to be consulted during the SA3 study with respect to use cases and scenarios that require User Consent.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Huawei |
| HiSilicon |
| China Telecomn |
| China Mobile |
| China Unicomn |
| CAICT |
| Samsung |
| FutureWei |
| Xiaomi |
| OPPO |
| Ericsson |
| CABLABS |