**3GPP TSG-SA3 Meeting #103-e *S3-211715r2***

**e-meeting, 17 – 28 May 2021**

**Source: Apple**

**Title: Revising key issue#2 for user consent in TR 33.867**

**Document for: Approval**

**Agenda Item: 5.14**

# 1 Decision/action requested

***It is proposed to revise the key issue#2 for user consent in TR 33.867.***

# 2 References

[1] 3GPP TR 33.867, v0.3.0

# 3 Rationale

The current key issue#3 includes a bunch of requirments on user consent for data collection, however, the revocation of the user consent is not clearly stated, especially on the network behavior when the user consent is revoked.

This pCR proposes to add a new requirement in key issue#2 in TR 33.867.

# 4 Detailed proposal

\*\*\*\*\*\* START OF CHANGE \*\*\*\*\*\*\*\*\*

6.2 Key Issue #2 User consent for UE data collection

6.2.1 Key issue details

5GS NFs will collect data about the UE being served. The NFs keep privacy related sensitive data such as profiling information, location information, etc. UE related data may also need to be transferred to another NF to fulfil a service request or, e.g., for analytics purposes. For example, the NWDAF shares the analytics results to the consumer NF which may be an internal NF or a 3rd party and exposes the UE Identifier, UE location in order to support tracking or checking the valid location of the UE.

In order to meet related private information requirements stated above, user consent is needed.

6.2.2 Security threats

If the 5G NFs are not aware of the current status of user consent for a specific service, they may share information with other NF’s that are not essential for 5G communication that could lead to a compromise in the users privacy.  For example, sharing location, timings and device ID with a third party service or with a NF from an operator that is neither the home or visited network.

6.2.3 Potential security requirements

The 3GPP system shall provide a means for an NF to authenticate a request for information that may compromise a user’s privacy.

The 5GS shall provide a means for an NF to verify the status of user consent for a request for information that may compromise a user’s privacy.

The 5GS shall specify where an NF can find the status of user consent for service that it delivers.

The 5GS shall specify a means that allows a user to change or add consent for a service/for any UE sensitive information collection (e.g. UE location information).

~~5GS shall support mechanism to halt gathering and sharing of user information as soon as the user revokes consent.~~

5G NFs shall provide protect potential privacy related information both in transit and in storage.

Editor's Note: the key issue needs to cover also user consent not based on privacy regulation.

\*\*\*\*\*\*\*\*\*END OF CHANGE\*\*\*\*\*\*\*\*\*