**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222626-r1***

e-meeting, 10 - 14 October 2022

**Title: LS on the data and analytics exchange between two NWDAFs in different PLMNs**

**Response to: LS S2-2207142 on LS OUT to GSMA on the data and analytics exchange between two NWDAFs in different PLMNs from 3GPP SA WG2**

**Release: 18**

**Work Item: FS\_eNA\_Ph3**

**Source: SA3 Meeting #108e-AdHoc**

**To: 3GPP SA WG2**

**Cc: GSMA**

**Contact person: German Peinado**

 **german.peinado@nokia.com**

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

**Attachments:**

# 1 Overall description

SA3 would like to thank SA2 for their LS S2-2207142 on data and analytics exchange between two NWDAFs in different PLMNs in the context of the Rel-18 study TR 23.7000-81.

S3 study TR 33.738 addresses this issue in KI#1. The study has not been concluded yet, so the provided feedback is preliminary and based on the identified security requirements so far.

**Question 1:** Does SA3 have feedback to the security aspects outlined in the key issue description? For example, are there any privacy and security protection for data and/or analytics exchange between PLMNs (VPLMN and HPLMN) already defined in SA3 or are there any privacy and security issues foreseen when exchange data and/or analytics between PLMNs?

**SA3 response:** KI#1 of TR 33.738 describes the identified threats and potential security requirements with respect to the key issue description of SA2. The security requirements require in general the 5GS to support confidentiality, integrity, and replay protection for data and analytics exchange between PLMNs, and also to be able to control the amount of exposed data and to abstract or hide internal network aspects based on operator policy, regulatory constraints and/or roaming agreements. There are security mechanisms available in the SA3 specifications (TS 33.501, appendix X) to enforce the authorization of the services (i.e., OAuth 2.0), and filter the data to be exposed as per TS 23.288, which may be extended for inter PLMN data and/or analytics exchange. Further mechanisms (e.g., anonymization) are still under study phase. SA3 will inform SA2 when the conclusions of KI#1 are agreed on.

**Question 2:** Whether it is necessary to verify user consent for UE-specific data and/or analytics by the VPLMN? If so, what scenario required user consent verification? How to verify user consent in roaming scenario in VPLMN?

**SA3 response:** If UE-specific data/analytics is needed from VPLMN by HPLMN, the user consent check maybe needed in case the VPLMN is in the same regulation region with HPLMN.The view in SA3 is that user consent for UE-specific data and/or analytics should be verified by the VPLMN via interactions with the HPLMN, and the detailed procedure will be determined based on relevant procedures through coordination between SA2 and SA3. For example, if analytics provided by the VPLMN requires UE-specific data and/or analytics user consent verification is required, NDWAF in VPLMN needs to check the user consent flag in HPLMN UDM. Similarly, if HPLMN NWDAF collects data from VPLMN the check on user consent can be done in HPLMN UDM.

Please note that SA3 has initiated a UC phase 2 study (TR 33.896) where the user consent in roaming scenarios is studied, including eNA (Key Issue #1 "User consent for roaming case in eNA"). Verification of user consent in the roaming scenario will largely reuse the procedures for user consent defined in TS 33.501. SA3 will provide feedback to SA2 once the study has concluded.

More specifically, for data that requires user consent, SA3 needs to have the following questions answered:

1. Is there any legitimate interest for the data or analytics? Some examples of these are:
2. service or feature provisioning, performance improvements including network optimization,
3. performance of subscriber contract (to which the data subject is a party),
4. general network maintenance and optimization,
5. emergency scenarios,
6. etc.
7. Does the data or analytics contain any Personal Identifiable Information? If yes, would it be possible to de-identify the data and/or analytics?
8. Will the data be disclosed to third parties?
9. For the purpose of anomaly and fault detection an impact assessment should be carried out to understand the consequences of consent being withheld or withdrawn.

# 2 Actions

**To SA2**

**ACTION:** Take the above information in consideration. More detailed information will be provided once the corresponding studies in S3 (TR 33.738, TR 33.896) are concluded.

# 3 Dates of next TSG SA WG 3 meetings

SA3#109 14 - 18 November 2022 Toulouse (France)

SA3#110e 16 - 20 January 2023 Online (electronic meeting)