**SA WG2 Meeting #163 S2-2407059**

**Jeju, Korea, May 27 – May 31, 2024**

**Title: [Draft] LS on User Identities and Authentication Architecture**

**Response to: -**

**Release: Rel-19**

**Work Item: FS\_UIA\_ARC**

**Source: OPPO [to be: SA2]**

**To: SA3, SA3-LI**

**Cc: SA1**

**Contact person : Peng Tan**

 **v-tanpeng@oppo.com**

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

**Attachments:**

# Overall description

SA2 is studying on User Identities and Authentication Architecture (FS\_UIA\_ARC). During SA2#163, SA2 has identified several security aspects that may require feedback from SA3 and SA3-LI. SA2 kindly asks SA3 and SA3-LI to provide feedback on the following aspects for KI#1 and KI#3 of TR 23.700-32, which is related to Human User.

**Question1a:**

During the discussion related to Key Issue #1 most companies believe that it is appropriate to send the user identifier in NAS (e.g. to trigger authentication by the network and to activate the user with a subscription). Different from the majority view, some companies objected to this conclusion and raised the issue of trust of the user identifier and credentials for the MNO (HPLMN), and questioning whether the HPLMN will be able to trust the user identifier and credentials.

While considering that the views from majority of companies being,

* the user identity and credentials that will be used to identify the user in HPLMN might not be stored in UICC. For example, a User Interface could be used to retrieve user identifier and credentials directly from the human user; or the User Interface could identify the human (e.g. based on biometric authentication) and related human user identifier and credentials could be retrieved by the operating system (e.g. from the UICC or other local storage).
* procedures and methods similar to NSSAAF will be used to authenticate the user.

SA2 requests SA3 to provide feedback if their views are inline to the majority view as described above.

**Question1b:**

Regarding the Key Issue #3 of TR 23.700-32, can any existing information of the UE subscription with whom the user identifier is active, or new information related to the user to be allowed to be exposed to an authorized AF, and if so, is user consent required for the exposure of this information? Specifically we would like understand the user consent requirements for the following new information:

* The verification result indicating whether the User Identifier authentication is successful

**Question2:**

Regarding Key Issue #1 of TR 23.700-32, SA2 kindly requests SA3 to provide their opinion whether there is a privacy issue if the network keeps providing SMS and IMS services to a UE when a user identifier is active with the UE subscription.

**Question3:**

Regarding Key Issue #1 of TR 23.700-32, in SA2 also certain companies question whether the user identity that is using the UE also needs to be known for LI purposes e.g. to comply to regulatory requirements.

# Actions

**To SA3:**

**ACTION:** SA2 kindly asks SA WG3 to provide answers 1a, 1b, and 2.

**To SA3-LI:**

**ACTION:** SA2 kindly asks SA3-LI to provide answers to question 3.

# 3 Dates of next TSG SA2 meetings

3GPP TSG SA2#164 19th August- 23th August, 2024 Maastricht, NL

3GPP TSG SA2#165 14th October- 18th October,2024 India, IN