**3GPP TSG-SA3 Meeting #117 *S3-24XXXX***

**Maastricht, Netherlands 19 - 23 Aug 2024**

**Title: (Draft) Reply LS on** **User Identities and Authentication Architecture**

**Response to: S3-242724/S2-2407236**

**Release: Rel-19**

**Work Item: FS\_UIA\_Sec**

**Source: SA3**

**To: SA2**

**Cc: SA3-LI, SA1**

**Contact person: Lihui Xiong**

 **xionglihui@oppo.com**

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

**Attachments:** none

# Overall description

SA3 would like to thank SA2 for the LS on User Identities and Authentication Architecture and provide the following answers.

|  |
| --- |
| ***Question1a:****During the discussion related to Key Issue #1 and Key Issue #2 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 NSSAA 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.* |

**Answer1a:**

SA3 prefers the majority views for the Authentication and Authorization of User Identities. The user identifier could be linked/unlinked with one or multiple SUPI, and the linking/unlinking information could be stored in UDM/UDR as subscription data. The user authentication can be trigged by the secure user identifier transmission, and performed with the user credentials. In addition, SA3 has been working at the Authentication and Authorization of Human User ID and would keep SA2 informed of progress.

|  |
| --- |
| ***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 to understand the user consent requirements for the following new information:**- the verification result indicating whether the User Identifier authentication is successful.* |

**Answer 1b:**

The user consent framework as specified in Annex V of TS33.501, the purpose is for providing technical means to manage subscriber permissions at the operator domain such that Network Functions of the 3GPP system can request or can be provisioned/configured with subscriber-related data in accordance with local laws and regulations. Hence the user consent mechanism is not suitable for such case.

SA3 understands the main use case in this release is for Single Sign-on which requires to expose authentication results only. Whether to expose the authentication result (i.e., the verification result indicating whether the User Identifier authentication is successful) can be based on the SLA, the authorized AF relies on the Core Network to perform he user authentication and determine whether to provide service to the user according to the authentication result.

|  |
| --- |
| ***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.* |

**Answer 2:**

SA3 has been working on the KI of User privacy in TR 33.700-32, and would discuss whether there is a privacy issue exists in such scenario and how to resolve this issue. SA3 would keep SA2 informed of progress.

# Actions

**To SA2:**

**ACTION:** SA3 kindly asks SA2 to take the above information into account

# 3 Dates of next TSG SA2 meetings

3GPP TSG SA3#118 2024‑10‑14 to 2024‑10‑18 Hyderabad, IN

3GPP TSG SA2#119 2024‑11‑11 to 2024‑11‑15 Orlando, US