3GPP TSG-SA3 Meeting #117 S3-242xxx

Maastricht, Netherlands 19 - 23 August 2024

**Title: Reply LS on User Identities and Authentication Architecture**

**Response to:** LS S3-242724/ S2-2407236 LS on User Identities and Authentication Architecture

**Release: Rel-19**

**Work Item: TEIxx**

**Source: 3GPP SA3 meeting #117**

**To: SA2,**

**Cc: SA1 SA3-LI**

**Contact person: saurabh khare**

 **Saurabh.khare@nokia.com**

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

**Attachments:** NA

# 1 Overall description

SA3 would like to thank SA2 for their LS S3-242724/ S2-2407236 LS on User Identities and Authentication Architecture.

Regarding the question asked in the LS

**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.*

SA3 reply>> SA3 believes that the user can be authenticated and trusted, considering the user and subscriber (UE) made an agreement before the user started using the UE, and 5GC authenticates the user on the pre-agreed UE.

In the case of UAV security work defined in TS 33.256, UAV and UE are identified and authenticated separately. I.e., UE is authenticated by 5GC, and UAV is authenticated by UTM/AF. Once UTM/AF confirms the authentication of the UAV to 5GC, the 5GC provides the UAS service to UE. Similarly, users can also be authenticated and trusted by 5GC. SA3 is discussing multiple solutions to authenticate the user, and hopefully we will converge soon.

**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.

SA3 reply>> SA3 also believes that user consent validation is required from both the user and subscriber before exposing the user information and/or associated UE subscription information. If both consents are allowed, then user information (e.g., authentication results or already exposed information) should be exposed.

**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.

SA3 Reply >> As user and subscriber agrees to share the device and user can read the already available SMS/call history as well, there is no privacy issue.

# 2 Actions

**To SA2**

**ACTION:** SA3 kindly asks SA2 to consider the above responses.

# 3 Dates of next TSG SA WG 3 meetings

SA3#118 14 - 18 October 2024 Hyderabad (India)

SA3#119 11 - 15 November 2024 Orlando (US)