**3GPP TSG-SA3 Meeting #116 *S3-242505-r2***

Jeju, South Korea, 20th - 24th May 2024

**Source: Philips International B.V.**

**Title: New Solution: Human User ID authentication and authorization**

**Document for: Approval**

**Agenda Item: 5.10**

# 1 Decision/action requested

***SA3 is kindly requested to approve the new solution proposed.***

# 2 References

# 3 Rationale

*This contribution proposes a solution to KI#1: Authentication and Authorization of Human User ID, in TR 33.700-32, to achieve the security goals.*

# 4 Detailed proposal

*\*\*\* START OF CHANGES \*\*\**

## 5.X New Solution: Human User ID authentication and authorization

### 5.X.1 Introduction

This solution addresses KI#1 Authentication and Authorization of Human User ID and proposes an overall procedure to achieve these security goals.

### 5.X.2 Solution details



Figure 5.X.2-1: Human User ID authentication and authorization

The procedure is described in reference to figure 5.X.1-1, as follows:

* In step 1, the User accesses the UE e.g., unlocks ME and SIM.
* In Step 2, the UE performs initial registration and primary authentication with the 5GC.
* In Step 3, based on the type of services requested/ to be provided and the UE subscription details, the 5GC (e.g., UDM) can trigger a User Identification procedure by sending a User Identity Request to the UE.
* In Step 4, Upon receiving the User Identity Request, the User may be prompted (e.g., through the user interface) to provide its User Identity and authentication information. If the User approves the request, the User Identity and authentication information (e.g., User identifier, user biometric data) is sent protected to the 5GC.

Note 1: In case a 3rd party User Identity Management Server (UIMS) is used, the User Identity may be protected based on security materials shared between the UE and the 3rd party UIMS, which are outside of the 3GPP scope.

* In Step 5, the 5GC processes the protected User Identity and authentication information received in step 4, and authenticates the User based on whether the User Identity is associated with the UE subscription, as stored at the 5GC (e.g., UDR). Alternatively, If the User Identity is managed by a 3rd party UIMS, the User identification and authentication is performed by the 3rd party UIMS and the identification and authentication result is then provided to the 5GC, which may subsequently check whether the identified and authenticated User is associated with a user subscription, as stored in the 5GC (e.g., UDR).

Editor’s Note: Details on how identification is triggered in step 3 and authentication is performed in step 5 are FFS.

* In Step 6, based on whether the User Identity authentication is successful, and the type of services requested by the user, the 5GC (e.g., PCF) determines whether the User is authorized for such services.

### 5.X.3 Evaluation

TBD.

*\*\*\* END OF CHANGES \*\*\**