**3GPP TSG-SA3 Meeting #124 S3-253776-r4**

**Wuhan, China, 13 – 17 October 2025** (merger of S3-253614,S3-253395,S3-253225,S3-253419,S3-253641,S3-253641,S3-253304,S3-253493,S3-253549,S3-253295)

**Source: Samsung, Xiaomi, Apple, Huawei, Vivo, Ericsson, ZTE, Interdigital, Nokia.**

**Title: Pseudo-CR on Security area Authentication and Authorization**

**Document for: Approval**

**Agenda item: 5.3.1**

**Spec: 3GPP TR 33.801-01**

**Version: V0.1.0**

**Work Item: FS\_6G\_SEC**

**Comments**

This contribution proposes a new security area, Authentication and Authorization in the 6G Security TR 33.801-01.

\* \* \* First Change\* \* \* \*

# 4 Security areas and high level security requirements

## 4.1 Security areas

X) Authentication and Authorization: This security area will study the key issues relating to the different aspects the authentication and authorization and related privacy aspects (e.g. subscriber privacy) for UEs accessing 6G network

\* \* \* End of First Change\* \* \* \*

\* \*

\* \* \* 2nd Change\* \* \* \*

# 5 Key issues and solutions

## 5.x Security area #x: Subscriber Authentication and Authorization

### 5.x.1 Introduction

This security area includes the following security aspects related to authentication and authorization between the UE and the 6GS:

* Primary authentication including key agreement and authorization between the UE and the 6GS.

Editor’s note: Other types of authentication is ffs (eg secondary authentication, slice specific authentication, etc)

* Re-authentication between the UE and the 6GS in different conditions of mobility.
* Privacy aspects such as subscriber privacy.
* Long term credentials storage and processing

\* \* \* End of 3rd Change\* \* \* \*