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

**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 for various types of UEs/terminal devices accessing 6G network in all scenarios.

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

\* \*

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

# 5 Key issues and solutions

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

### 5.x.1 Introduction

A successful Authentication Key Agreement and Authorization between the UE and network is the primary procedure before the UE can get any service from the network.

In addition to the primary authentication procedure, in some cases, secondary authentication is also involved. While primary authentication is always between the UE and the UDM in the HPLMN, secondary authentication involves an external enterprise AAA server in the case of external DNN access or a network slice specific AAA server in the case of network slices.

Re-authentication between the UE and the network is required in different conditions of mobility, UE state, UE context lifetime and change of security domains etc to authenticate the validity of the UE and network. Since the conditions to trigger the re-authentication of the UE are varied and many, network need a flexible and optimal method to trigger re-authentication of the UE at any time.

Making use of the mobile authentication infrastructure, operators are able to offer authentication as a service to other enterprises too. 4G and 5G already offer services such as NSWO and AKMA etc, these are expected to continue in an efficient manner in 6G.

Issues related to all such procedures are studied under this security area.

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