**3GPP TSG-SA3 Meeting #124 S3-253304**

**Wuhan, China, 13 – 17 October 2025**

**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\* \* \* \*

\* \* \* Second Change\* \* \* \*

## 4.2 Potential high level security requirements

It shall be possible to authenticate the UE using its subscription credentials and device capabilities in an optimized manner to authorize the UE for network access and services preserving subscription privacy.

Based on deployment scenarios and network configuration it shall be possible to perform additional authentication or secondary authentication of the UE to authorize the UE for different network access types and services.

It shall be possible for the network to re-authenticate the UE whenever required in an optimal manner.

It shall be possible to offer authentication as a service to external enterprises.

\* \* \* End of Second Change \* \* \* \*

\* \* \* 3rd 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.

The network may also re-authenticate the UE at any time by triggering re-authentication.

The network may also offer authentication as a service to other enterprises.

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

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