**3GPP TSG-SA3 Meeting #124 draft\_S3-253399-r1**

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

**Source: Huawei, HiSilicon, China Mobile, ZTE**

**Title: Adding 6G security area on security visibility and configurability**

**Document for: Approval**

**Agenda item: 5.3.1**

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

**Version: 0.1.0**

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

**Comments:**

According to the SA3 6G SID’s objectives, the study aims to cover all the possible areas as stated in the following note:

*‘NOTE3: In the above WTs, the study will cover possible security enhancements of the procedures from previous generations and new security aspects that arise from work in other working groups (including the developments regarding different particular verticals and deployments).’*

Security visibility and configurability are important aspects that have been considered in all previous releases (e.g. 3G, LTE, 5G), The goal is to keep the device users informed about whether certain security feature is in operation or not, and whether the use/provision of services should depend on the security feature. Typically ciphering has been one of such features which is shown on the device display whenever activated. Other features such as generation selection configuration or even false base station detection are widely available but mainly based on proprietary solutions.

Currently, visibility (not only security visibility) has proved is a success feature that is benefit to the industry, for example, Non-Standalone (NSA) network deployment shows 5G logo to let the user know 5G is using, even without 5G core. This brought questions whether visibility on security will bring more to the user.

Does a user know the operator provides security to the user? The answer is only few people knows security is provided nowadays. But the answer will be changed to “Yes, it double checked with me” if the question is about whether a bank application provides security link when you transfer the money. Let people awaring the security is provided may make users more rely on the operator. However, this purpose may only be achieved by showing the security features which is currently invisible to the user.

The goal of this area is to collect key issues and solutions related to visibility and configurability. It is worth noticing that user awareness about security has been constantly increasing in our societies, and the next generation network is supposed to be functional that with more comprehensive than the previous generations. In this regard, developing a new generation always presents a new opportunity to revisit the existing features and study whether there is need and how to enhance existing standard mechanisms in a way that benefits the 6G system and its new use cases.

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

4 Security areas and high-level security requirements

4.1 Security areas

Editor's Note: This clause further clarifies the scope of the study by listing the security areas that SA3 is working on.

This document includes the following security areas:

X) The security area of security visibility and configurability deals with how to keep users informed about the status of certain security features and also how to enable them to configure such features.

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

# 5 Key issues and solutions

## 5.X Security areas #X: Security visibility and configurability

### 5.X.1 Introduction

The user using a UE may need to be aware of a more comprehensive security status to benefit the user’s decision on the used service, e.g. to not perform operation requiring high security level under weak security protection. On the other hand, configurability of security features offers a flexible security capability exposure to user, allowing user to manage security of its service.

This security area aims to investigate and evaluate how the security can be configured by the user or an application in the 6G system and how to provide visibility of the currently used/unused security to the user and the applications.

 \* \* \* End of Changes \* \* \* \*