**3GPP TSG-SA3 Meeting #124 draft\_S3-253661-r1**

**Wuhan, China, 13 – 17 October 2025 merge of S3-253418, S3-253613**

**Source: Huawei, HiSilicon, Samsung**

**Title: New Security Area on Security Architecture**

**Document for: Approval**

**Agenda item: 5.3.1**

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

**Version: 0.1.0**

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

**Comments**

This contribution proposes a new area on security architecture in TR 33.801-01.

The motivation is that the security architecture will lay the foundation for all the procedures and the mechanisms necessary to protect the communication between the devices and the network as well as within the network. During the course of a generation lasting over several releases, the security architecture barely changes. Enhancements and modifications after the introduction of a new generation would be extremely challenging. Therefore, future-proofness is one of the most crucial properties that a new design must fulfil.

Security architecture has been evolving throughout the development of different generations of mobile network systems. In fact, 5G was marked by the introduction of independent standalone security functions such as SEAF, AUSF, ARPF and SEPP [1]. This enables proper separation of security functionality as well as clear enforcement of principles such as key isolation, forward and backward security. This also provides flexibility and better control in deployments. In fact, product implementing such functions could be subject to more stringent security requirements. This is by comparison to other products for example implementing only SMF, UPF functionalities or any non-security related functionality.

The 5G design proved to be sufficiently future-proof. In fact, new features such as AKMA [2], SoR and UPU requiring all new services could be introduced smoothly without any backward compatibility issues. This is thanks to the SBA framework and the introduction of the AUSF which could serve as a security anchor function in the HPLMN though not initially intended to.

However, if one knew in advance, then the design of the security architecture would have included a designated security anchor function in the HPLMN. Furthermore, reflecting on how the SoR and UPU procedures were designed, it would have been simpler with a separate stratum (similar to NAS and AS) and a designated security termination point in the HPLMN for the secure delivery of information between the HPMNL and the device. There were also other complications. For example, the decision to collocate SEAF with AMF proved to be a limitation for the AMF relocation procedure. These are not security issues but rather consequences of certain design choices that maybe we could have done differently.

Now is the opportunity to reflect on such past design decisions, in light of the new challenges and use cases, in order to design the security architecture for 6G.

**References:**

[1] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

[2] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)"

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[xx] 3GPP TR 23.801-1: "Study on Architecture for 6G System".

\* \* \* Next 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:

1. Security architecture deals with aspects such as identifying the different security domains and their characteristics, defining the different security functions, developing the key hierarchy, designing the different security strata and their respective termination points, etc.

\* \* \* Next Change \* \* \* \*

# 5 Key issues and solutions

## 5.x Security area #x: Security architecture

### 5.x.1 Introduction

This security area addresses the security principles, features, and requirements inherent to the security architecture of 6G systems. This will lay the foundation for all the procedures and the mechanisms necessary to protect the communication between the devices and the network as well as within the network. The security architecture defined herein provides the foundation for all other security work and is integral to the overall 6G system architecture. The baseline for the work here is to be aligned with the architectural framework described in 3GPP TR 23.801-01 [xx].

Solutions in this area are expected to build upon the strong foundations of 5G while addressing the new challenges and use cases in 6G. The goal is to design a future proof security architecture that follows the same principles for key isolation, backward security, forward security, etc. and guarantees at least the same security "level" for all communication as in 5G. This amounts, but not limited, to the following.

- Identifying the different security domains and their characteristics.

- Defining the security functions, e.g., for authentication, security anchor, credential storage.

- Developing the key hierarchy.

- Designing the different security strata and their respective termination points.

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