**3GPP TSG-SA3 Meeting #124 S3-253229-r1**

**Wuhan, China, 13 – 17 October 2025 merger of S3-253229, S3-253153, S3-253308, S3-253619**

**Source: Apple, KDDI, Samsung, Interdigital**

**Title: New Security Area on Cryptographic algorithm**

**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 security area for TR 33.801-01.

\* \* \* 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:

1. Cryptographic algorithm deals with any potential vulnerability or enhancement related with algorithms for 6G System.

## 4.2 Potential high level security requirements

Editor's Note: This clause will document high-level requirements that guide the study.

6G system should support the protocol enhancement to indicate any new algorithms when necessary.

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

# 5 Key issues and solutions

## 5.x Security area #x: Cryptographic algorithms

### 5.x.1 Introduction

Editor's Note: Detailed description of the security area

Cryptographic algorithms are used from authentication, key agreement, key derivation, ciphering to integrity protection. Security mechanisms and protocols for many use cases rely on the secure cryptographic algorithms, therefore, the security of cryptographic algorithms is an important for 6G System. Another important factor of cryptographic algorithms is the efficiency so that the service requirements of 6G System can be met.

SA3 is working on the FS\_PQC(Study on transitioning to Post Quantum Cryptography (PQC) in 3GPP) and FS\_AEAD(New Study on supporting AEAD algorithms), which could lead to protocol change to the 6G system. For example, in case the AEAD1 algorithm is agreed in FS\_AEAD, 6G system shall make corresponding changes in the AS SMC and NAS SMC, as well as the PDCP functionalities which is now separately handling encryption and integrity protection.

NOTE 1: 5G PDCP protocol is defined in TS 38.323, the corresponding changes (if necessary) in 6G will be made in RAN2 group.

This security area also covers the Post-Quantum Readiness (PQR), which addresses the need to future-proof 6G mobile networks against quantum computing threats that could compromise widely deployed public-key algorithms such as RSA, ECC, and DH. As a horizontal domain, PQR spans and supports vertical areas including RAN security, authentication and key agreement, authorization, security context and key management, and overall security architecture. Its objectives include identifying vulnerabilities to quantum attacks, analyzing threats such as “harvest now, decrypt later” scenarios and downgrade exploits, and defining requirements for quantum-resistant algorithms, cryptographic agility, and migration mechanisms that enable coexistence with classical cryptography during transition phases.To meet these objectives, the PQR considers solutions such as hybrid key exchange mechanisms in AKA, post-quantum digital signatures, PQC-based identity protection, and quantum-safe key management frameworks. It also studies integration challenges across diverse environments, including IoT, edge, and NTN deployments, as well as performance considerations in latency-sensitive services. With 6G expected to operate at a massive scale, support AI-native and autonomous networks, and serve devices with extended lifespans, PQR aims to ensure long-term confidentiality, integrity, and resilience by embedding cryptographic agility and quantum-resistant mechanisms into the design of the 6G security framework.

NOTE 2: This clause may incorporate the conclusion in the AEAD study in TR 33.771 [yy].

NOTE 3: This clause may incorporate the conclusion in the PQC study in TR 33.703 [zz].

### 5.x.2 Security assumptions

Security mechanisms and protocols rely on the use of secure and efficient cryptographic algorithms.

It is assumed that currently deployed public-key cryptographic algorithms, such as RSA, ECC, and DH will be vulnerable to quantum computing attacks within the service lifetime of 6G systems.

It is assumed that long-term confidentiality of sensitive information (e.g., subscriber identities, authentication credentials, and session keys) must be preserved against “harvest now, decrypt later” attacks.

It is assumed that 6G security architecture shall incorporate quantum-resilient protections as a horizontal capability supporting vertical areas, including RAN security, authentication and key agreement, authorization, and key management.

It is assumed that hybrid or transitional cryptographic schemes combining classical and post-quantum algorithms will be required to support migration and backward compatibility with legacy systems.

It is assumed that cryptographic agility will be an essential property, enabling seamless introduction, coexistence, and replacement of algorithms in response to evolving standards and threat landscapes.

It is assumed that PQC adoption must accommodate the performance and integration constraints of resource-limited environments such as IoT devices, edge platforms, and NTN systems.

It is assumed that post-quantum mechanisms will need to support long device lifespans (10–15 years or more) to ensure forward secrecy and durability of protections throughout the lifecycle.

\* \* \* Next 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".

[yy] 3GPP TR 33.771: "Study on supporting AEAD algorithms".

[zz] 3GPP TR 33.703: "Study on transitioning to Post Quantum Cryptography (PQC) in 3GPP".

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