**3GPP TSG-SA3 Meeting #122** **S3-25xxxx**

**Fukuoka, Japan, 19 - 23 May 2025**

**Source: KDDI**

**Title: Discussion paper on supporting AEAD algorithms**

**Document for: Discussion**

**Agenda Item: 6**

# 1 Decision/action requested

***With this contribution, KDDI would like to start a discussion about changes that would allow a future 3GPP System to utilize AEAD algorithms for AS and NAS security. We believe it is necessary to consider implications of AEAD algorithms early on to ensure readiness of the next-generation system.***

# 2 References

[1] 3GPP TS 35.240 Specification of the Snow 5G based 256-bits algorithm set

[2] 3GPP TS 35.243 Specification of the AES based 256-bits algorithm set

[3] 3GPP TS 35.246 Specification of the ZUC based 256-bits algorithm set

[4] S3-250369, “Use of AEAD in Next-Generation 3GPP System”

[5] NIST Special Publication 800-38B, “Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication”

# 3 Rationale

ETSI SAGE and 3GPP SA3 have recently completed specifications for 256-bit cryptographic algorithms. For the first time in 3GPP, these specifications also include authenticated encryption with associated data (AEAD) algorithms　[1][2][3].

As demonstrated in [4], AEAD mode offer performance and efficiency advantages compared to using two dedicated algorithms for encryption and integrity protection. These advantages as well as the simplified system design that a combined encryption and integrity protection would allow for making it a strong alternative to the operating modes specified for the cryptographic algorithms currently.

Furthermore, the adoption of 256-bit algorithms provides a security advantage and offers a much larger security margin compared to 128-bit algorithms for AS and NAS security. The impact of a cryptographically relevant quantum computer on symmetric algorithms is less significant than on asymmetric algorithms. However, in the interest of ensuring an adequate security margin in the long term, it is prudent to make this change with the introduction of 6G.

Considering the above advantages, introducing a study on the adoption of AEAD mode in the 3GPP System at this point in time is essential to prepare for its adoption in 6G. Delaying this study to later Releases risks missing the opportunity of ensuring architectural system-readiness. Hhence, Rel-20 presents the most suitable timing for this study based on the current state of 5G Advanced. The findings and guardrails for potential solutions resulting out of this study can in turn be leveraged during the design of the 6G System.

It is unlikely that the adoption of AEAD impose any security threats to the 3GPP System, therefore there will be no need to consider any countermeasures. Having said that, the current 3GPP System is designed to use encryption algorithms for confidentiality and message authentication code algorithms for integrity protection for AS and NAS security, and it cannot accommodate AEAD algorithms. In order to support AEAD algorithms, modifications need to be applied to the 3GPP System. The objective of AEAD study is to identify any protocols/procedures which are impacted by adoption of AEAD and consider possible updates to 3GPP System.

When AEAD algorithms are used for encryption and integrity protection, they first encrypt the plaintext and generate the ciphertext. Then the MAC tag is generated over the ciphertext. In NAS security, the MAC tag is generated over the ciphertext and suitable for AEAD. In AS security, on the other hand, the MAC tag is generated over the plaintext and both plaintext and MAC tag are encrypted. A trivial way to achieve this with AEAD is to apply AEAD twice: first for MAC tag generation and second for encryption. However, this will impose computational overhead. Changin the design of AEAD algorithm only for AS requires security analysis and increases the number of algorithms. It is more reasonable to keep the same design and change AS security mechanism.

Once 256-bit algorithms are introduced, AEAD mode will serve three purposes: (1) encryption only and (2) integrity protection only, just like the stand-alone algorithms today, as well as (3) both encryption and integrity protection combined. Therefore, there will be no reason to introduce 256-bit encryption only algorithms and 256-bit integrity protection only algorithms.

Current AS and NAS security mechanism use 32-bit message authentication tag for integrity protection. It is recommended to use at least 64-bit long [5]. The extension of MAC length is a long-wanted security improvement for integrity protection. If protocols and procedures related to encryption and integrity protection are updated, it is reasonable to consider updating the MAC length at the same time so that overall impact to the architecture can be minimised.

The result of the study can be captured in a technical report and proposed structure is given in clause 4.

# 4 TR structure

It is proposed to use the following structure as a baseline of the TR:

1 Scope

2 References

3 Definitions of terms, symbols and abbreviations

4 Procedures and protocols impacted by AEAD and potential modifications

5 Procedures and protocols impacted by extension of MAC length and potential modifications

6 Conclusion

Annex

# 5 Detailed proposal

It is proposed to initiate a new study item to analyse potential challenges and requirements related to supporting AEAD algorithms for AS/NAS security. It is also proposed to use the proposed structure given in clause 4 of this document to capture the result of study.