**3GPP TSG-SA3 Meeting #119 S3-242xxx**

Orlando, US 11 - 15 November 2024

**Source: KDDI Corp.**

**Title: Use of AEAD in Next-Generation 3GPP System**

**Document for: Discussion**

**Agenda Item: tbd**

# 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 algorihms for AS and NAS security. Although such a change is not in scope of 5G, 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 33.501

[2] 3GPP TS 32.240

[3] 3GPP TS 32.243

[4] 3GPP TS 32.246

[5] RFC 8452, “AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption”

[6] [Power Consumption of Common Symmetric Encryption Algorithms on Low-Cost Microchips](https://dl.gi.de/server/api/core/bitstreams/51fa9d0a-fefa-4b29-b927-99faa0b474bc/content); Marc Ohm, Lars Taufenbach, Karsten Weber, Timo Pohl

[7] 3GPP TS 38.323

[8] 3GPP TS 38.331

# 3 Rationale

## Motivation for AEAD

ETSI SAGE and 3GPP SA3 have recently completed specifications for 256-bit cryptographic algorithms. For the very first time in 3GPP, these specifications also include authenticated encryption with associated data (AEAD) algorithms [2][3][4]. With the industry’s increasing focus on higher throughput and data-intensive applications, SA3 should also consider adoption of these AEAD algorithms to be used for AS/NAS security in a next-generation 3GPP System.

Cryptographic algorithms operating in AEAD mode combine both encryption and integrity protection to a single operation. Generally speaking, this approach has two main benefits:

* **Enhanced throughput and power consumption**
	+ Single-pass operation: Ideally, they provide data encryption and authentication in a single pass (in contrast to the two-pass “Encrypt, then MAC” scheme used today). This can also lead to reduced power consumption.
	+ Reduced power consumption: There is data that suggests that, for smaller payloads, AEAD algorithms can exhibit reduced power consumption compared to other symmetric key schemes that generate the MAC / authentication tag separately [6]
* **Simplified system design and key management**
	+ Fewer keys to manage: With AEAD, only one key is needed for both encryption and integrity protection, simplifying key management.
	+ Less Error-Prone: Using separate algorithms can introduce complexity and potential errors in their combination. AEAD reduces the risk of such errors by providing a single, well-defined process.

## Procedures impacted from AEAD

Considering the motivations outlined above, it is crucial to consider deployment for an AEAD mode compatible security architecture. To ensure a next-generation 3GPP System is able to utilize AEAD algorithms, the following key issues would need to be agreed.

### Algorithm negotiation

The current 5G system uses dedicated algorithms for encryption (128-NEAs) and integrity protection (128-NIAs). These algorithms are negotiated independently from each other. This means a given session may use the same or different algorithms for encryption and integrity protection, on both AS and NAS layer. When using AEAD algorithms, both operations are combined in one. Therefore, a next-generation system may also simplify the selection procedure and allow UE and network to negotiate a combined cipher suite. A potential solution may be as trivial as omitting one algorithm indicator in the existing AS/NAS SMC procedure.

### Key hierarchy

The current system uses two separate key pairs for encryption and integrity protection. A next-generation system utilizing AEAD algorithms would only require one key pair for both operations, allowing for a simplified key hierarchy. Similar to algorithm negotiation, a possible solution may be as trivial as omitting one part of the key derivations that is performed today in the AMF (KNAS 🡪 KNASenc / KNASint) and in the gNB (KgNB 🡪 KRRCenc / KRRCint, KgNB 🡪 KUPenc / KUPint).

### AEAD algorithm inputs

#### Nonce

AEAD algorithms commonly require a nonce that is not to be reused as it ensures the uniqueness and integrity of the ciphertext. When a nonce is misused, in other words, a nonce is repeated for a given key, an attacker may be able to exploit the repetition to recover the encryption key or manipulate the ciphertext [5].Without a mechanism in the 3GPP System to prevent such threat by providing a unique nonce, the algorithm may not be able to provide effective security.

Note: It is expected that this key issue may require involvement of ETSI SAGE.

#### Associated Data

Authentication Encryption Algorithms also can have Associated Data the use of which is yet to be determined in the specifications. A next-generation system may require further study into how to utilize the Associated Data input for various possible use cases.

### Backwards compatibility with separate encryption and integrity protection algorithms

#### Mobility

Assuming that a next-generation 3GPP System would solely support AEAD algorithms to fully leverage the benefits mentioned earlier in this document, the intra-RAT mobility case would be trivial. In this scenario, all security termination points unanymously support AEAD. Other scenarios, such as inter-RAT handovers would fall under the “Interworking” section.

#### Interworking

It is fair to assume that existing generations of the 3GPP System (e.g., 4G/LTE, 5G) will not feature support for AEAD. In these scenarios, the question arises how to realize interworking between next-generation (AEAD-compatible) networks and legacy (AEAD-incompatible) networks. Specifically, one needs to consider differences in the security context maintained by the UE and the network as well as associated procedures, such as key derivation.

#### Multi-RAT Dual connectivity

Similar to mobility and interworking scenarios, the conditions remain the same with AEAD-compatible updated next generation networks, and previous networks without support. In these situations, there is a risk of inconsistent key sizes being used to protect different communication paths associated to a single subscriber session when using dual connectivity. Specifically, one can envisage a scenario in which the UE is connected to both a Master Node (MN) or Primary RAN and Secondary Node (SN) or Secondary RAN. Assuming a mixed deployment in which the MN already supports AEAD mode, but the SN only supports legacy algorithms (or vice versa), this can lead to a situation where the RRC and UP between the UE and the MN or SN is protected with algorithms using different modes resulting in inconsistent performance output.

### Order of Encryption and Integrity protection for NAS and AS security

In the current 5G system, it is observed for the AS security to be MAC-then-Encrypt (MtE) order [7] while the NAS security is the opposite order, being formulated to have the NAS message to first be ciphered, then the NAS sequence number to be integrity protected by calculating the MAC, hence, Encrypt-then-MAC (EtM) [8]. The order of NAS security is more suitable for the adoption of AEAD, encryption and integrity protection can be achieved with single operation of AEAD. While the current order of AS security requires two operations of AEAD, the MAC tag is generated in the first operaton and ciphertext is generated in the second. For the next-generation system, it should be studied whether the current Encrypt-then-MAC order of AS security is suitable for the AEAD algorithms.

# 4 Detailed proposal

It is proposed to thoroughly analyze requirements of a next-generation 3GPP System for supporting AEAD algorithms for AS/NAS security, identify potential challenges, including but not limited to the forementioned challenges outlined in this paper, and utilize these findings during the development of the next-generation 3GPP System.