**3GPP TSG-SA3 Meeting #124 S3-253783-r1**

**Wuhan, China, 13 – 17 October 2025 (revision of S3-253192)**

**Source: KDDI**

**Title: introduction to AEAD**

**Document for: Approval**

**Agenda item: 5.3.2**

**Spec: 3GPP TR 33.771**

**Version: 0.0.1**

**Work Item: FS\_AEAD**

**Comments**

<Proposals, reason for change, abstract, comments if necessary (optional)>

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

Annex A: Introduction to AEAD

## A.1 Protection provided by AEAD

Authenticated Encryption (AE) is a type of cryptographic algorithms. The key characteristic of AE is that ciphering, and integrity protection are executed in a combined operation. This way, data encryption and authentication can ideally be provided in a single pass. Authenticated Encryption with Associated Data (AEAD) additionally allows for input that is authenticated, but not encrypted. This can be leveraged in use cases where solely data integrity is required while the plain text remains visible for processing.

Additionally, AEAD algorithms allow selective ciphering and integrity protection as needed. If only ciphering is required, it may be possible depending on the AEAD algorithm to only output the ciphertext. If only integrity protection is required, all input data can be processed as associated data. Finally, it is also possible to combine both approaches and provide ciphering and integrity protection for one part of a message while another part is only integrity protected (e.g., because certain message contents need to be accessible in plain text).

The 256-bit cryptographic algorithms specified in TS 35.240 [x1], TS 35.243 [x2] and TS 35.246 [x3] are all based on AEAD1, which also allows for confidentiality protection, integrity protection, and a combined AEAD mode.

|  |  |
| --- | --- |
|  | **Cryptographic algorithm** |
| **Snow 5G** | **AES-256** | **ZUC-256** |
| **Operating mode** | **Confidentiality**  | 256-NEA4 | 256-NEA5 | 256-NEA6 |
| **Integrity** | 256-NIA4 | 256-NIA5 | 256-NIA6 |
| **Authenticated Encryption with Associated Data (AEAD)** | 256-NCA4 | 256-NCA5 | 256-NCA6 |

**Table A.1-1: 256-bit cryptographic algorithms specified in by ETSI SAGE**

## A.2 Algorithm inputs and outputs

AEAD algorithms can take a unique nonce, a single cryptographic key, plaintext and associated data as inputs. The plaintext is an optional when only integrity protection is required. The associated data is an optional if there is no data which requires only integrity protection.

## A.3 Order of operations

When using an AEAD algorithm, important security decisions are already made such that in which order encryption and integrity protection is applied.

\* \* \* 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".

[x1] 3GPP TS 35.240 Specification of the Snow 5G based 256-bits algorithm set

[x2] 3GPP TS 35.243 Specification of the AES based 256-bits algorithm set

[x3] 3GPP TS 35.246 Specification of the ZUC based 256-bits algorithm set

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