**3GPP TSG-SA3 Meeting #124 S3-253782r1**

**Wuhan, China, 13 – 17 October 2025 (revision of S3-253190)**

**Source: KDDI**

**Title: Scope for TR 33.771**

**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 \* \* \* \*

# 1 Scope

The present document identifies potential challenges and requirements for supporting AEAD algorithms specified in TS 35.240[x1] TS 35.243[x2] and TS 35.246[x3] for NAS and AS security (including control and user plane security) in the 6G System, including the following:

- Impact to AS and NAS security

- Key hierarchy and management to support AEAD algorithms

NOTE 1: Key hierarchy includes long term key (i.e. full key hierarchy) for usage of AEAD. Procedure aspects (e.g. AKA framework) are not covered in the present document.

- Negotiation of encryption and/or integrity protection when using AEAD algorithms

- Creation and handling of AEAD algorithm inputs, such as Nonce and Associated Data

Co-existence of AEAD-compatible systems and legacy deployments and algorithms (i.e., only AEAD algorithms or both AEAD and standalone algorithms) is taken into account.

\* \* \* 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: specification of the 256-NEA4 encryption, the 256-NIA4 integrity, and the 256-NCA4 authenticated encryption algorithm for 5G; Document 1: algorithm specification

[x2] 3GPP TS 35.243 Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G; Document 1: algorithm specification

[x3] 3GPP TS 35.246 Specification of the ZUC based 256-bits algorithm set: Specification of the 256-NEA6 encryption, the 256-NIA6 integrity, and the 256-NCA6 authenticated encryption algorithm for 5G; Document 1: algorithm specification

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