**3GPP TSG-SA3 Meeting #124 S3-253193**

**Wuhan, China, 13 – 17 October 2025 merger of S3-253188, S3-253193, S3-253265, S3-253342, S3-253477 and S3-253478**

**Source: KDDI, ZTE Corporation?, vivo?, Beijing Xiaomi Mobile Software?, LG Electronics?**

**Title: New KI of algorithm selection**

**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 \* \* \* \*

## 5.X Key issue #X: Algorithm selection

### 5.X.1 Key issue details

The current 5G System uses dedicated algorithms for encryption (NEA0, 128-NEA1, 128-NEA2, 128-NEA3) and integrity protection (NIA0, 128-NIA1, 128-NIA2, 128-NIA3) which are selected independently. This means a given session may use the same or different algorithms for encryption and integrity protection (including NULL), on both AS and NAS layer. Even when using AEAD algorithms that combine encryption and integrity protection, the option to select the NULL algorithm may still be required to signal the use of encryption only or integrity protection only.

In scenarios when both encryption and integrity protection are required, one aspect that needs to be specified is whether algorithms are to be selected independently (e.g., 256-NEA4 and 256-NIA4), or whether the system should implicitly choose the AEAD algorithm in such cases (e.g., 256-NCA4). When either encryption or integrity protection is required, it also needs to be specified whether dedicated algorithm (e.g., 256-NEA4 if encryption is required or 256-NIA4 if integrity protection is required) is to be selected or AEAD algorithm is to be selected (e.g., use 256-NCA4 for encryption only or integrity protection only).

Another aspect is whether selecting different algorithms to be supported for encryption and integrity protection (e.g., 256-NEA4 and 256-NIA5). Since the existing 256-bit integrity protection algorithms all use the same Mac5G framework based on GMAC, the MAC computation of three 256-NIAs is fundamentally the same. Therefore, the only difference between the combination of 256-NEA4 and 256-NIA4 and the combination of 256-NEA4 and 256-NIA5 is the input parameters.

Having to support both dedicated encryption and integrity protection algorithms and combined algorithms may complicate implementations without a tangible security benefit. Additionally, providing encryption and integrity protection with a single AEAD algorithm may be preferable in terms of performance to running the dedicated algorithms twice.

NOTE: The common design of the 256-bit integrity protection algorithms and thus, the lack in algorithm diversity may be considered a security risk, especially considering recent cryptanalysis targeting polynomial-based MAC constructions.

### 5.X.2 Security threat

TBD

### 5.X.3 Potential requirements

6G System shall support the negotiation of AEAD algorithms for AS and NAS security.

It is required to define whether to use dedicated algorithms or AEAD algorithms or both.

\* \* \* 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".

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