**3GPP TSG-SA3 Meeting #124 S3-253785r2**

**Wuhan, China, 13 – 17 October 2025 merger of S3-253188, S3-253193, S3-253194, 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.

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.

Depending on the security policy or scenario, AEAD can provide following protections:

1. Encryption,
2. Integrity protection or
3. Encryption and integrity protection.

When negotiating the AEAD algorithm, it can also be necessary to decide which protections are required.

The key issue is to study following:

 - whether AEAD only is sufficient or AEAD and standalone algorithms are required, and

 - how to enhance algorithm selection for AEAD algorithms and their protections.

### 5.X.2 Security threat

TBD

### 5.X.3 Potential requirements

Algorithm selection may need an enhancement to support AEAD algorithms.

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