**3GPP TSG-SA3 Meeting #124 draft\_S3-253787-r4**

**Wuhan, China, 13 – 17 October 2025 Merger of S3-253388, S3-253591, S3-253262, S3-253197, S3-253386, S3-253196, S3-253263**

**Source: Huawei, HiSilicon, Ericsson**

**Title: New key issue about the AEAD algorithm interface**

**Document for: Approval**

**Agenda item: 5.3.2**

**Spec: 3GPP TR 33.771**

**Version: 0.0.1**

**Work Item: FS\_AEAD**

**Comments**

It is proposed to add a new key issue about studying the interface of AEAD algorithm inputs.

\* \* \* First 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".

[y1] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[y2] 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".

[y3] 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".

[y4] 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".

[X1] RFC 5116, “Authenticated Encryption with Associated Data”

\* \* \* Second Change \* \* \* \*

## 5.X Key issue #X: AEAD algorithm interface

5.X.1 Key issue One of the advantages of using a combined AEAD mode is that some important security decisions have already been made in the construction of the mode, such as in which order encryption and integrity protection is applied. From SA3 perspective, this means that we don't need to discuss in which order operations are to be applied in PDCP and NAS.

Many different AEAD constructs are available and by using a generic interface, it is possible to treat the AEAD as a black box where the underlying construction is transparent to the user of the interface. One such interface is specified in RFC 5116 [X1].

Existing interfaces for encryption and integrity algorithms in Annex D.2 and Annex D.3 of TS 33.501 [y1] cannot be used for the new AEAD algorithms directly. This is because the new algorithms combine both operations and also require additional input parameters as described in TS 35.240 [y2], TS 35.243 [y3], TS 35.246 [y4]. For example, in addition to the key and IV, an AAD parameter (as described in TS 35.240 [y2], TS 35.243 [y3], TS 35.246 [y4]) is required to enable flexible partial encryption, the output parameters include both the ciphertext and the MAC.

Consequently, how to set the input parameters for NAS and PDCP needs to be further studied because the existing requirements in clause 6.4.3, 6.4.4, 6.5.1, 6.5.2, 6.6.3, 6.6.4 of TS 33.501 [y1] cannot be directly applied.

Existing construction of IV for encryption and integrity algorithms in Annex D.2 and Annex D.3 of TS 33.501 contains a 32-bit COUNT, a 5-bit BEARER, a 1-bit DIRECTION. ETSI SAGE anticipates that in the future, the entropy for the IV might need to increase from the 38 bits defined by 3GPP. Hence, an extra entropy field called EXTRA\_IV of 6 bytes is introduced as described in TS 35.240 [y2], TS 35.243 [y3], TS 35.246 [y4].

### 5.X.2 Security threats

There is a threat to system evolution. For example, if the interface is not designed well from day one, it will not be stable for future enhancements and there can be problems to add new functionality. This will not only increase complexity of the system but will also make it more difficult to analyze from a security perspective, and hence the risk for missing threats increases.

5.X.3 Potential security requirements

TBD.

\* \* \* End of Change \* \* \* \*