**3GPP TSG-SA3 Meeting #123 draft-S3-253050-r1**

**Goteborg, Sweden, 25 – 29 August 2025** **(revision of S3‑252554)**

**Source: KDDI**

**Title: New SID on supporting AEAD algorithms**

**Document for: Approval**

**Agenda Item: 6.3 New 6G SIDs/WIDs**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on supporting AEAD algorithms

Acronym: FS\_AEAD

Unique identifier: tbd

Potential target Release: Rel-20

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes | X | X | X | X |  |
| No |  |  |  |  |  |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Study  |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| N/A |  | {optional free text}  |

**Dependency on non-3GPP (draft) specification:**

{This section is to be typically used to identify the IETF dependencies. Delete the header "Dependency on non-3GPP (draft) specification:" if no such dependency}

# 3 Justification

ETSI SAGE and 3GPP SA3 have recently completed specifications for 256-bit cryptographic algorithms. For the very first time in 3GPP, these specifications also include Authenticated Encryption with Associated Data (AEAD) algorithms [1][2][3]. With the industry’s increasing focus on higher throughput and data-intensive applications, SA3 should consider adoption of these AEAD algorithms to be used for NAS and AS security (including control and user plane security) in a 3GPP System.

Cryptographic algorithms operating in AEAD mode, for example algorithms based on the construction in [5], combine both encryption and integrity protection to a single operation. Generally speaking, this approach has two main benefits:

* **Enhanced throughput and power consumption**
	+ Single-pass operation: Ideally, they provide data encryption and authentication in a single pass (in contrast to the separate ciphering and integrity protection algorithms used today).
	+ Reduced power consumption: There is data that suggests that, for smaller payloads, AEAD algorithms, at least on software implementation, can exhibit reduced power consumption compared to other symmetric key schemes that generate the MAC / authentication tag separately [4].
	+ Enhanced throughput: When conducting both encryption and integrity, it is observed, at least on software implementation, AEAD mode produces better efficiency compared to legacy mode encryption and integrity protection combined. [4]
* **Simplified system design and key management**
	+ Fewer algorithms to implement: As encryption and integrity protection can be achieved by a single algorithm, the number of algorithms to be implemented can be reduced.
	+ Fewer keys to manage: With AEAD, only one key is needed for both encryption and integrity protection, simplifying key management.
	+ Less Error-Prone: Using separate algorithms can introduce complexity (e.g. security policy complexity) and potential errors in their combination. AEAD reduces the risk of such errors by providing a single, well-defined process.

Reference:

[1] 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

[2] 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

[3] 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

[4] S3-250369, “Use of AEAD in Next-Generation 3GPP System”

[5] IETF Internet draft, Galois Counter Mode with Secure Short Tags (GCM-SST)

# 4 Objective

This study aims to identify potential challenges and requirements for supporting AEAD algorithms [1, 2, 3] 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).

* 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) should be taken into account.

NOTE 2: The conclusion of the study will be used to guide AEAD adoption for 6G with WID agreement.

**TU estimates and dependencies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe)  | Inter Work Tasks Dependency  |
|  | 4 TUs |  | Maybe |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| Internal TR | 33. XYZ | Study on supporting AEAD algorithms | SA#113 | SA#113 | tbd |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| N/A |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

For a Stage 2 WID requiring Stage 3 to be done by another group: on a best-effort basis, indicate which potential WG is expected to specify the Stage 3: {possible values: "Not applicable", " unknown", "CT WGs", etc}

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Apple |
| CableLabs |
| Charter Communications |
| China Mobile |
| Ericsson |
| Huawei |
| KDDI |
| Lenovo |
| LG Electronics |
| NEC |
| Nokia |
| Philips International B.V. |
| Samsung |
| Vivo |
| Xiaomi |
| ZTE |