**3GPP TSG-SA3 Meeting #122 S3-25xxxx**

**Fukuoka, Japan, 19 - 23 May 2025**

**Source: KDDI**

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

**Document for: Approval**

**Agenda Item: 6 New Study/Work Item Proposals**

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: tbd

Unique identifier: tbd

Potential target Release: Rel-20

# 1 Impacts

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | 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:**

# 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 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 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 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.

Current NAS and AS security mechanisms use 32-bit Message Authentication Code (MAC) tags for the integrity protection. A 32-bit MAC is too short to provide enough security margin against forgery and longer length is recommended. Since new AEAD algorithms allow generating up to 128-bit tags, SA3 should also consider a longer MAC length.

Note that AEAD is merely a new operating mode for the 256-bit versions of the existing cryptographic algorithms, there is no reason to separate the introduction of AEAD mode from that of the 256-bit algorithms themselves. Therefore the normative phase for introducing 256-bit algorithms can be considered after this study.

Reference:

[1] TS 35.240 Specification of the Snow 5G based 256-bits algorithm set

[2] TS 35.243 Specification of the AES based 256-bits algorithm set

[3] TS 35.246 Specification of the ZUC based 256-bits algorithm set

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

# 4 Objective

This study aims to identify potential challenges and requirements for supporting AEAD algorithms for NAS and AS security (including control and user plane security) in the next-generation 3GPP System, including the following:

* Studying potential challenges and requirements concerning the AEAD1 operating mode, such as:
  + Studying whether the current order of encryption and integrity protection AS security (Mac-then-Encrypt) is suitable for AEAD1 (Encrypt-then-MAC).
  + If the Mac-then-Encrypt order is to be maintained for AS security, studying how AEAD1 can be used to support this order without any change of AEAD1 algorithm and performance degradation.
* Studying potential challenges and requirements concerning the adoption of AEAD algorithms in a 3GPP system:
  + Key hierarchy and management to support AEAD algorithms
  + Negotiation of encryption and/or integrity protection when using AEAD algorithms
  + Creation and handling of AEAD algorithm inputs, such as Nonce and Associated Data
  + Backwards compatibility between AEAD-compatible systems and legacy deployments
  + Number of supported modes, only AEAD algorithms or both AEAD and dedicated algorithms
* Studying potential challenges and requirements concerning MAC length.

# 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#112 | SA#112 | tbd |
|  |  |  |  |  |  |

|  |  |
| --- | --- |
| **TU count / planning** |  |
| SA3#123 | 1/2 TU |
| SA3#124 | 1/2 TU |
| SA3#125 | 1/2 TU |
| SA3#126 | 1/2 TU |
| SA3#127 | 1/2 TU |
| SA3#128 | 1/2 TU |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| KDDI |
|  |
|  |
|  |
|  |
|  |
|  |
|  |