**3GPP TSG-SA3 Meeting #113** ***S3-23XXYY***

**Chicago, USA, 6 - 10 November 2023** **(revision of xx-yyxxxx)**

**Source:** **KDDI Corporation**

**Title: New SID on study on enabling a cryptographic algorithm transition to 256-bits**

**Document for: Approval**

**Agenda Item: 6**

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 enabling a cryptographic algorithm transition to 256-bits

Acronym: FS\_CAT256

Unique identifier: tbd

Potential target Release: Rel-19

# 1 Impacts

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

# 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) |
| FS\_256\_Algo | SA3 |  | Study on supporting 256-bit algorithms for 5G |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
|  |  |  |

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

# 3 Justification

SA3 previously studied the support of 256-bit algorithms for 5G, resulting in TR 33.841 [1]. Said TR leaves a number of important questions unanswered and does not cover some of the practical challenges associated with the transition to 256-bit algorithms. Some of the unanswered questions have already been discussed in LSs exchanged with ETSI SAGE referenced below [2] [3] [4] [5]. Followings are the details of the open questions and challenges, which needs to be resolved in this study item:

* Negotiation of key lengths between the UE and the network. While the existing negotiation of security algorithms may be reused in principle, a few details would need to be clarified, such as:
* How to prevent bid-down attacks?
* Which key length should be selected if the bit length of the long-term secret is only 128-bit?
* Security risks related to selection of algorithms with different key sizes between the UE and the different security end points in the network. Specifically, is there a need to ensure the same level of protection (i.e., cryptographic key length) for AS and NAS security?
  + What happens in handover scenarios where source and target may not unanimously support 256-bit cryptographic algorithms (applicable to both AS and NAS security)?
  + Similarly, what happens in 5G NSA deployments and interworking scenarios?
* TR 33.841 already indicates the need for longer MACs, at least for certain use cases. Among others, such a change raises the following questions:
  + Negotiation of MAC lengths between the UE and the network.
  + Will the MAC length be bound to the negotiated algorithm, as is the case today?
  + Is there a need to ensure the same MAC length for AS and NAS security?

ETSI SAGE has since finalized their evaluation of current candidate algorithms[6][7], adding further justification to studying the essential prerequisites for the transition to 256-bit cryptographic algorithms now.

As the above challenges and open questions show, adding support for 256-bit cryptographic algorithms to the 5G system requires clarifying the interplay of the new algorithms with the legacy procedures to prevent security vulnerabilities. Even if solutions to some of these issues may be evident, it seems prudent to study these problems, list solutions and document SA3’s conclusions and the expected behaviour of the 5G System.

References:

[1] TR 33.841 Study on the support of 256-bit algorithms for 5G

[2] S3-211510 LS on Security risk evaluation of using long term key for another key derivation than AKA

[3] SAGE (20)01 LS on Resynchronizations

[4] SAGE (20)05 Observations and questions on 256-bit security goals

[5] SAGE (19)28 LS reply on expectations and requirements for 256-bit algorithms

[6] SAGE (22)01 Specification of the 256-bit air interface algorithms

[7] SAGE(23)01 Specification of Milenage-256 finalized

# 4 Objective

This study aims to address key requirements for introducing support for 256-bit symmetric algorithms into the 5G System as well as the coexistence of 128-bits and 256-bits cryptographic algorithms. Considering findings and conclusions from preceding work, the following points should be addressed as part of this study:

- Studying key issues and candidate solutions concerning the negotiation (selection) of key sizes between UE and network, including:

- Potential risks of supporting 128-bit and 256-bit algorithms in parallel and the adoption of 256-bit algorithms in existing deployments where 128 bits is already supported

- How to prioritise the use of 256-bit algorithms and prevent bidding-down attacks when negotiating key sizes;

- How to ensure 256-bit security concerning varying levels of support for 256-bit algorithms by different UEs and within the network; potential dependencies in key-length selection of AS and NAS layer

- How to ensure the effective key length equals the key bit length of the long-term keys used for the AKA procedure

- Studying key issues and candidate solutions concerning the negotiation of MAC lengths between UE and network, incl.:

- What MAC length(s) other than 32-bit should be supported by the 5G system?

- Define the minimum MAC length for each 128-bit and 256-bit ciphering algorithms

- How to secure the negotiation of MAC lengths between UE and network?

- Security architecture impacts associated with use of MAC tags longer than 32-bits:

- What are the Network functions required to be involved in the negotiation?

- What are implications to the MAC due to the negotiation of key sizes?

- What is the overhead impact of longer MAC lengths in practice (to NAS and AS layer)?

NOTE: coordinate with other working groups maybe needed during the study.

# 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 | tbd | Study on cryptographic algorithm transition to 256 bits | TSG SA#104 | TSG SA#105 | Cho, Minkyoung, KDDI, Minkyoung.cho@tohmatsu.co.jp |
|  |  |  |  |  |  |

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

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

None identified yet

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| KDDI |
| BSI |
| Deutsche Telekom |
| Motorola Solutions |
| NEC |
| Nokia |
| US NSA |
| Lenovo |
| NCSC |
| MITRE |