**3GPP TSG-SA3 Meeting #117 *S3-24xxxx***

**Maastricht, The Netherlands, 19th - 23rd August 2024**

**Source: KDDI**

**Title: New WID on supporting 256-bit ciphering and integrity protection algorithms**

**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: New WID on supporting 256-bit ciphering and integrity protection algorithms

Acronym: TBD

Unique identifier: TBD

Potential target Release: Rel-19

# 1 Impacts

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Study  |
|  | Normative – Stage 1 |
| X | 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 |
|  |  |  |

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

None

# 3 Justification

In order to adopt 256-bit algorithms, the official algorithm indicators must be specified.

# 4 Objective

The objectives of this work item are the normative work according to the conclusions from TR 33.700-41:

* Assign algorithm identifier values for 256-bit ciphering and integrity protection algorithms; and
* Specify optional support for them in the 5G System.

# 5 Expected Output and Time scale

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| TS 33.501 | Security architecture and procedures for 5G system | SA#105 |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

CT1 for algorithm identifiers used in NAS and AS.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| KDDI |
|  |
|  |
|  |
|  |
|  |