**TSG SA Meeting #102 SP-231743**

**December 11 – 15, 2023, Edinburgh, Scotland**

**Source: SA WG3**

**Title: New WID on Milenage-256 algorithm**

**Document for: Approval**

**Agenda Item: 6.2.3**

**3GPP TSG-SA3 Meeting #113 *S3-235072***

**Chicago, US, 6 - 10 november 2023** **(revision of S3-234681)**

**Source: Thales, Idemia, NIST, ORANGE, Nokia, Telecom Italia**

**Title: New WID on Milenage-256 algorithm**

**Document for: Approval**

**Agenda Item: 6.2**

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: Addition of Milenage-256 algorithm

Acronym: Milenage\_256

Unique identifier: 1020036

-

Potential target Release: Rel-19

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  |  |  |
| No | X | X | X | X |  |
| 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 |
| 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) |
| 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:**

None

# 3 Justification

The 256-bit algorithms including two different versions of MILENAGE-256 have been developed and evaluated by the ETSI SAGE at 3GPP’s request on development of 256-bit algorithms which is one of the results of the study captured in TR 33.841.

# 4 Objective

The objectives to the WID are the following work tasks (WT):

* WT1: Selection of the version of Milenage-256 algorithm to specify.
* WT2: Specification of the Milenage-256 algorithm, implementors’ test data and design conformance test data, summary and results of design and evaluation.

## TU estimates and dependencies

|  |  |  |
| --- | --- | --- |
| Work Task ID | TU Estimate  (Normative) | Other 3GPP Group Dependency  (Yes/No/Maybe) |
| WT1 | 1 | No |
| WT2 | 1 | No |

**Total TU estimates: 2 TUs**

# 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 |
| TS | 35.234 | Specification of the MILENAGE-256 algorithm set:  An example set of 256-bit 3GPP Authentication and Key Generation functions f1, f1\*, f2, f3, f4, f5, f5\* and f5\*\*; Document 1: General | SA#105  (Sept-24) | SA#106  (Dec-24) | mireille.pauliac@thalesgroup.com |
| TS | 35.235 | Specification of the MILENAGE-256 algorithm set:  An example set of 256-bit 3GPP Authentication and  Key Generation functions  f1, f1\*, f2, f3, f4, f5, f5\* and f5\*\*;  Document 2: Algorithm Specification | SA#105  (Sept-24) | SA#106  (Dec-24) | mireille.pauliac@thalesgroup.com |
| TS | 35.236 | Specification of the MILENAGE-256 algorithm set:  An example set of 256-bit 3GPP Authentication and  Key Generation functions  f1, f1\*, f2, f3, f4, f5, f5\* and f5\*\*;  Document 3: Implementors’ Test Data and Design  Conformance Test Data | SA#105  (Sept-24) | SA#106  (Dec-24) | mireille.pauliac@thalesgroup.com |
| TS | 35.237 | Specification of the MILENAGE-256 algorithm set:  An example set of 256-bit 3GPP Authentication and  Key Generation functions  f1, f1\*, f2, f3, f4, f5, f5\* and f5\*\*;  Document 4: Summary and Results of Design and  Evaluation | SA#105  (Sept-24) | SA#106  (Dec-24) | mireille.pauliac@thalesgroup.com |

|  |  |  |  |
| --- | --- | --- | --- |
| 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)

Mireille Pauliac mireille.pauliac@thalesgroup.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

None

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Thales |
| Idemia |
| NIST |
| ORANGE |
| Nokia |
| Telecom Italia |
| Ericsson |
| CableLabs |
| Huawei |