**3GPP TSG-SA3 Meeting #115S3-240630**

**Athens, Greece, 26th February - 1st March 2024**

**Source: Ericsson**

**Title: New WID on f5\*\* algorithm**

**Document for: Agreement**

**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 specification of f5\*\* algorithm

Acronym: f5\*\*

Unique identifier:

-

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 |
| X | 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 |
|  |  | {optional free text}  |

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

None

# 3 Justification

Based on SA3's request in S3-220541, ETSI SAGE has designed a new f5\* (called f5\*\*) algorithm for MILENAGE-128 and Tuak, which provides security against the resynchronisation attacks. ETSI SAGE has shared this new algorithm with SA3 via the LS S3-240252 titled "SAGE-23-02 Resynchronisation protection f5\*\* for MILENAGE-128 and Tuak". SA3 needs to create a new specification for this new f5\* function.

# 4 Objective

The objective of the WID is to specify the f5\*\* algorithm for MILENAGE-128 and Tuak.

## TU estimates and dependencies

s

|  |  |
| --- | --- |
| TU Estimate(Normative) | Other 3GPP Group Dependency(Yes/No/Maybe) |
| 1 | No |

**Total TU estimates: 1 TU**

# 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.XXX | Specification of the f5\*\* algorithm for MILENAGE-128 and Tuak; Document 1: Algorithm specification and test data | SA#104(June-24) | SA#104(June-24) | TBD |
| TR | 35.9XX | Specification of the f5\*\* algorithm for MILENAGE-128 and Tuak; Document 2: Security Analysis | SA#104(June-24) | SA#104(June-24) | TBD |

|  |
| --- |
| 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

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Ericsson |
| Thales |
| Idemia |
| Qualcomm |
|  |
|  |