**3GPP TSG-SA3 Meeting #111 *S3-23xxxx***

**Berlin, Germany, 22 - 26 May 2023** **(revision of S3-230695)**

**Source: Vodafone**

**Title: New WID on Addition of 256 bit UP security 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 Addition of 256 bit UP security Algorithms

Acronym:

### 256-UP-Algos

Unique identifier:

-

Potential target Release: Rel-19

# 1 Impacts

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Study  |
|  | Normative – Stage 1 |
|  | 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) |
| FS\_256-Algorithms | 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 |
|  |  | {optional free text}  |

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

none

# 3 Justification

*As detailed in TR 33.841,* Quantum computing poses a long-term threat to information security not only for data collected once the ability to compromise existing security is discovered but also for any historic data that may have legal, financial, commercial or governmental importance that has been collected for future decoding.

TR33.841 identified that whilst symmetric key algorithms are not as susceptible as public key related algorithms to the enhancements in quantum computing, 256bit algorithms should be developed now in preparation.

# 4 Objective

This Work Item delivers 3 new 256bit User Plane Integrity and Encryption Algorithms for 5G based on AES, SNOW and ZUC and detailed in TR 33.841. These algorithms have been developed by ETSI SAGE at 3GPP SA3's request.

For each Algorithm there are 3 TS documents: a specification, implementors test data and conformance test data.

Finally, this work item delivers CR(s) to TS 33.501 to incorporate the use of these algorithms into 5G.

**NOTE: Due to Laws governing the publication of secure algorithms, the unredacted versions of these specifications will require special handling. Permission to publish these specifications will need to be sought from the relevant governments.**

# 5 Expected Output and Time scale

**NOTE: These dates are for redacted versions of the specifications at TSG SA (unredacted versions shall be seen at the WGand to TSG members by arrangement to comply with French Law on sensitive security algorithms)**

|  |
| --- |
| 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 | 55.XXX | Specification of the NEA4 encryption algorithm for 5G; NEA4 specification | SA#101(Sept-23) | SA#103(Mar-23) | Evans, Tim, Vodafone, tim.evans1@vodafone.com |
| TS | 55.XXX | Specification of the NEA4 encryption algorithm for 5G; NEA4 Implementers Test Data | SA#102(Dec-23) | SA#103(Mar-23) |
| TS | 55.XXX | Specification of the NEA4 encryption algorithm for 5G; NEA4 Conformance Test Data | SA#102(Dec-23) | SA#103(Mar-23) |
| TS | 55.XXX | Specification of the NEA5 encryption algorithm for 5G; NEA5 specification | SA#101(Sept-23) | SA#103(Mar-23) |
| TS | 55.XXX | Specification of the NEA5 encryption algorithm for 5G; NEA5 Implementers Test Data | SA#102(Dec-23) | SA#103(Mar-24) |
| TS | 55.XXX | Specification of the NEA5 encryption algorithm for 5G; NEA5 Conformance Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NEA6 encryption algorithm for 5G; NEA6 specification | SA#101*(Sept-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NEA6 encryption algorithm for 5G; NEA6 Implementers Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NEA6 encryption algorithm for 5G; NEA6 Conformance Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA4 integrity algorithm for 5G; NIA4 specification | SA#101*(Sept-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA4 integrity algorithm for 5G; NIA4 Implementers Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA4 integrity algorithm for 5G; NIA4 Conformance Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA5 integrity algorithm for 5G; NIA5 specification | SA#101*(Sept-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA5 integrity algorithm for 5G; NIA5 Implementers Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA5 integrity algorithm for 5G; NIA5 Conformance Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA6 integrity algorithm for 5G; NIA6 specification | SA#101*(Sept-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA6 integrity algorithm for 5G; NIA6 Implementers Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |
| TS | 55.XXX | Specification of the NIA6 integrity algorithm for 5G; NIA6 Conformance Test Data | SA#102*(Dec-23)* | SA#103*(Mar-24)* |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| 33.501 | Addition of new 256bit algorithms to Sections 5.2.2, 5.2.3, 5.3.2, 5.3.3, 5.5.1, 5.5.2, 5.11.1.1, 5.11.1.2, 6.5.1, 6.5.2, 6.6.3, 6.6.4, 8.4.2, 10.2.2.1 and Annex D. | SA#104(June-24) | Evans, Tim, Vodafone, tim.evans1@vodafone.com |

# 6 Work item Rapporteur(s)

Evans, Tim, Vodafone, tim.evans1@vodafone.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

To be identified

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Vodafone |
| NIST |
|  |
|  |
|  |
|  |