**3GPP TSG-SA3 Meeting #115 S3-240875**

**Athens, February 26 – March 01, 2024 (revision of S3-240286)**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Updates on WID on Addition of 256-bit security Algorithms**

**Document for: Approval**

**Agenda Item: 4.5**

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:

### WID on Addition of 256-bit security Algorithms

Acronym:

256\_Algo

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 |
|  | 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) |
| 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 |
|  |  | {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, 256-bit algorithms should be developed now in preparation for a possible adoption. The corresponding algorithms have been developed and evaluated by the ETSI SAGE at 3GPP’s request.

# 4 Objective

The objectives to the WID are:

* Define the new 256-bit Integrity, Encryption, and Authenticated Encryption Algorithms for 5G NAS and AS layers based on AES, SNOW and ZUC.
* For all 3 algorithms, define algorithm specification, implementation test data and conformance test data.

NOTE 1: 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 WG and 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 | 35.240 | Specification of the 256-NEA4 encryption, 256-NIA4 integrity and 256-NCA4 authenticated encryption algorithm for 5G; 256-NEA4, 256-NIA4 and 256-NCA4 specification | SA#103  (Mar-24) | SA#104  (Jun-24) | Orkopoulos, Stawros, stawros.orkopoulos@nokia.com |
| TS | 35.241 | Specification of the 256-NEA4 encryption, 256-NIA4 integrity and 256-NCA4 authenticated encryption algorithm for 5G; 256-NEA4, 256-NIA4 and 256-NCA4 Implementers Test Data | SA#103  (Mar-24) | SA#104  (Jun-24) |
| TS | 35.242 | Specification of the 256-NEA4 encryption, 256-NIA4 integrity and 256-NCA4 authenticated encryption algorithm for 5G; 256-NEA4, 256-NIA4 and 256-NCA4 Conformance Test Data | SA#103  (Mar-24) | SA#104  (Jun-24) |
| TS | 35.243 | Specification of the 256-NEA5 encryption, 256-NIA5 integrity and 256-MCA5 authenticated encryption algorithm for 5G; 256-NEA5, 256-NIA5 and 256-NCA5 specification | SA#103  (Mar-24) | SA#104  (Jun-24) |
| TS | 35.244 | Specification of the 256-NEA5 encryption, 256-NIA5 integrity and 256-NCA5 authenticated encryption algorithm for 5G; 256-NEA5, 256-NIA5 and 256-NCA5 Implementers Test Data | SA#103  (Mar-24) | SA#104  (Jun-24) |
| TS | 35.245 | Specification of the 256-NEA5 encryption, 256-NIA5 integrity and 256-NCA5 authenticated encryption algorithm for 5G; 256-NEA5, 256-NIA5 and 256-NCA5 Conformance Test Data | SA#103  (Mar-24) | SA#104  (Jun-24) |
| TS | 35.246 | Specification of the 256-NEA6 encryption, 256-NIA6 integrity and 256-NCA6 authenticated encryption algorithm for 5G; 256-NEA6, 256-NIA6 and 256-NCA6 specification | SA#103  (Mar-24) | SA#104  (Jun-24) |
| TS | 35.247 | Specification of the 256-NEA6 encryption, 256-NIA6 integrity and 256-NCA6 authenticated encryption algorithm for 5G; 256-NEA6, 256-NIA6 and 256-NCA6 Implementers Test Data | SA#103  (Mar-24) | SA#104  (Jun-24) |
| TS | 35.248 | Specification of the 256-NEA6 encryption, 256-NIA6 integrity and 256-NCA6 authenticated encryption algorithm for 5G; 256-NEA6, 256-NIA6 and 256-NCA6 Conformance Test Data | SA#103  (Mar-24) | SA#104  (Jun-24) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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

Orkopoulos, Stawros, stawros.orkopoulos@nokia.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Nokia |
| Nokia Shanghai Bell |
| Vodafone |
| Thales |
| NIST |
| US NSA |
| Ericsson |
| MITRE |
| Qualcomm Incorporated |
| Orange |
| Deutsche Telekom |