**3GPP TSG-SA3 Meeting #119 S3-245142-r3**

**Orlando, US, 11 -15 November 2024 (revision of S3-244618)**

**Source: Nokia, Nokia Shanghai Bell**

**Title: New Study on 3GPP Cryptographic Inventory**

**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: Study on 3GPP Cryptographic Inventory

Acronym: FS\_CryptoInv

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-19

# 1 Impacts

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

{Tick one or more box(es). The full structure of all existing Work Items is shown in the 3GPP Work Plan in <https://ftp.3gpp.org/Information/WORK_PLAN>}

|  |  |
| --- | --- |
| X | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 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

{List here other Work Items which relate to the proposed one, such as a Work Item in an earlier Release if further enhancing the feature from the previous Release)}

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| N/A |  | {optional free text} |

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

N/A

# 3 Justification

The ETSI QSC group has developed a document for a Quantum Safe Cryptography migration strategy and recommendations to quantum safe schemes [3]. As part of a migration strategy, a protocol inventory must be created for the development of a preparation and PQC migration plan as well as the migration execution itself.

As per the LS [1], the ETSI QSC is seeking for additional information like “A detailed list of cryptographic algorithms and / or protocol implementations”. The detailed list may include a “guidance on algorithm exposure, effective key lengths, potential for hybrid deployment and potential for crypto agility”.

As per another LS [2], the GSMA has developed Guidelines for Telecom Use Cases document [4] which to some extent includes the development of a “comprehensive cryptographic inventory”.

Based on the ETSI QSC and the GSMA descriptions the 3GPP SA3 is targeting the goal to generate an overview of all cryptographic algorithms that are mandated/used in 3GPP specifications (in 3GPP defined functions and interfaces), their quantum safe status, and applicable protocols within the 5G system.

The 3GPP Cryptographic Inventory has been presented first time at the SA3#117 meeting in Maastricht for initial discussion and in this context a potential migration path towards post-quantum computing has been shown by listing the corresponding PQ algorithms and their referred specification documents.

As per the LS [5] and the LS [6], the SA3 does not have yet created a 3GPP cryptographic inventory nor has an order of priority for the migration work. There is some dependency on IETF’s work on introduction of PQC algorithms in 3GPP protocol specifications.

This study is intended to close the gap and to generate the 3GPP cryptographic inventory.

[1] ETSI TC CYBER, ETSI QSC, “Quantum Safe Cryptographic Protocol Inventory”, S3-240223

[2] GSMA, “LS regarding the publication of the Post Quantum Cryptography – Guidelines for Telecom Use Cases document in Feb 24”

[3] ETSI TR 103 619 V1.1.1 (2020-07), “Migration strategies and recommendations to Quantum Safe schemes”

[4] GSMA, “Post Quantum Cryptography – Guidelines for Telecom Use Cases”

[5] S3-243812, LS reply to 3GPP Reply-LS on PQC Migration

[6] S3-244307, Reply-LS on PQC Migration

# 4 Objective

The objective of this study item is to:

* Create an inventory of protocols that use cryptography used in 3gpp release 19 specifications in a TR 9xy-series document.
  + List the security protocols that use cryptography in 3GPP specifications
    - Include the type of cryptography used by the protocol (symmetric/Asymmetric)
    - Include the pointers to the protocol specification.
    - Include the pointers to the relevant 3GPP cryptographic profiles.
    - Include usage type (integrity, confidentiality or authentication)
* List the standardized post quantum cryptographic algorithms and their properties and restrictions,
* List the relevant updated IETF protocol specifications that are expected to include PQC algorithms.

NOTE 1: The scope of this SID does not include resolution to PQC migration, and this SID does not lead to any specification/normative work.

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |
| External TR | 33.9xy | Study on 3GPP Cryptographic Inventory | SA#106 | SA#107 | tbd |
|  |  |  |  |  |  |

|  |  |
| --- | --- |
| **TU count / planning** |  |
| SA3#119 | 1/2 TU |
| SA3#119\_bis | 1/2 TU |
| SA3#120 | 1/2 TU |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
| N/A |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

tbd

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

None.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Apple |
| Deutsche Telekom |
| Intel |
| NTT Docomo |
| Thales |
| Verizon |
| Xiaomi |
|  |