|  |
| --- |
| 3GPP TR 33.703 V0.1.0 (2025-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP (Release 20) |
|   |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttps://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Overview 8

4.1 Background Information 8

4.1.1 Transition Timeline 8

4.2 General Assumptions 9

5 Principles and attributes of PQC to use in 3GPP procedures 9

5.1 PQC security level 9

5.2 Hybrid and standalone schemes 9

6 Protocols expected to be updated for PQC by other SDOs 9

6.1 General 9

6.X Protocol #X 9

7 Protocols expected to be updated for PQC by 3GPP 10

7.1 Threats 10

7.1.1 Protocol #1: SUCI calculations 10

7.1.2 Protocol #2: MIKEY-SAKKE key exchange 10

7.2 Solutions 10

7.2.X Solutions to Protocol #X: <Title> 10

7.2.X.Y Solution #Y to Protocol #X: <Title> 11

7.2.X.Y.1 Introduction 11

7.2.X.Y.2 Solution details 11

7.2.X.Y.3 Evaluation 11

8 Conclusions 11

Annex A (informative): Change history 12

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the complexities involved with the introduction of standalone and/or hybrid Post Quantum Cryptography (PQC) algorithms in existing security protocols used by 5G specifications. These security protocols and their associated algorithms have been listed in TR 33.938 [2] “3GPP Cryptographic Inventory”. Specifically,

* Studies principles and attributes of PQC relevant to use in 3GPP procedures.

- Studies the impact of using hybrid and standalone PQC algorithms in 3GPP procedures

- Impact to 3GPP procedures due to larger length of PQC key, signature, and message compared to the length of those in traditional cryptography.

- Determines security levels (I-V) required to align with existing 3GPP procedures level of assurance.

- Studies the suitability of classes of post-quantum signature algorithms (e.g., lattice-based, hash-based) to 3GPP procedures.

* Identifies the protocols with asymmetric cryptography listed in TR 33.938 [2] that are not expected to be updated by other Standards Development Organizations (SDOs) in a near future to use PQC, e.g., MIKEY-SAKKE and SUCI calculation
* Studies security threats and alternative solutions for the 3GPP procedures if they are not updated to use PQC.
* Documents the expected timeline for when security protocols defined by other SDOs will include PQC algorithms and be available for inclusion into 3GPP procedures. The timeline includes the availability of stable protocols.
* Studies solutions to update 3GPP defined security protocols (for example SUCI calculation) to use the appropriate PQC algorithm, if those protocols are not expected to be updated by other SDOs to use PQC algorithms.

The present document is Generation agnostic.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.938: "3GPP Cryptographic Inventory".

[3] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] IETF Internet-Draft: “Post-Quantum Cryptography for Engineers”.

[6] IETF RFC 6509: ''MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)''.

[7] IETF RFC 9794: “Terminology for Post-Quantum Traditional Hybrid Schemes”.

[8] NIST IR 8547: “Transition to Post-Quantum Cryptography Standards”.

[9] SECG SEC 1: “Recommended Elliptic Curve Cryptography”, Version 2.0, 2009. Available at <http://www.secg.org/sec1-v2.pdf>.

[10] SECG SEC 2: “Recommended Elliptic Curve Domain Parameters”, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>.

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ECIES Elliptic Curve Integrated Encryption Scheme

MIKEY-SAKKE Multimedia Internet KEYing – Sakai-Kasahara Key Encryption

PQC Post Quantum Cryptography

SDO Standards Development Organizations

SECG Security Engineering & Consulting Group

SUCI Subscription Concealed Identifier

# 4 Overview

## 4.1 Background Information

### 4.1.1 Transition Timeline

Editor’s Note: Timeline information from other organizations.

## 4.2 General Assumptions

Editor's Note: This clause contains overall assumption and/or security assumptions for this study.

# 5 Principles and attributes of PQC to use in 3GPP procedures

Editor’s Note: This clause contains impact of using hybrid and standalone PQC algorithms in 3GPP procedures, impact to 3GPP procedures due to larger length of PQC key, signature, and message compared to the length of those in traditional cryptography, security levels (I-V) required to align with existing 3GPP procedures level of assurance, suitability of classes of post-quantum signature algorithms (e.g., lattice-based, hash-based) to 3GPP procedures.

### 5.1 PQC security level

Both IETF and NIST use the concept of security levels/security strength categories to group algorithms, keys, and protocols related to PQC. The security is defined as a function of resources required to break AES and SHA2/SHA3 algorithms, i.e., exhaustive key recovery for AES and optimal collision search for SHA2/SHA3. The security strength is broadly grouped into the following 5 levels [5], [8]:

Level 1: At least as hard as breaking AES-128 (exhaustive key recovery)

Level 2: At least as hard as breaking SHA-256/SHA3-256 (collision search)

Level 3: At least as hard as breaking AES-192 (exhaustive key recovery)

Level 4: At least as hard as breaking SHA-384/SHA3-384 (collision search)

Level 5: At least as hard as breaking AES-256 (exhaustive key recovery)

### 5.2 Hybrid and standalone schemes

Post-Quantum Traditional (PQT) hybrid scheme as defined in RFC 9794 [7] is a multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm. Both the PQT hybrid scheme and the standalone PQC scheme are considered in the present document.

# 6 Protocols expected to be updated for PQC by other SDOs

Editor’s Note: This clause contains the expected timeline for when security protocols defined by other SDOs will include PQC algorithms and be available for inclusion into 3GPP procedures. The timeline includes the availability of stable protocols.

### 6.1 General

Editor’s Note: This subclause states e.g. that protocols in TR 33.938 that are to be updated in other SDO and their profiles to be used in 3GPP are described here.

## 6.X Protocol #X

Editor’s Note: Protocol profile description.

# 7 Protocols expected to be updated for PQC by 3GPP

Editor’s Note: This clause contains identification of the protocols with asymmetric cryptography listed in TR 33.938 that are not expected to be updated by other SDOs in a near future to use PQC, e.g., MIKEY-SAKKE and SUCI calculation, security threats and alternative solutions for the 3GPP procedures if they are not updated to use PQC.

### 7.1 Threats

Most of security protocols used in 3GPP systems are specified in other standards development organizations (SDOs). In case that these protocols are not updated to use PQC in other SDOs, the 3GPP system may be vulnerable to attacks based on quantum computation. The clause 7.2 contains all of these protocols identified and potential solutions to address the issues.

### 7.1.1 Protocol #1: SUCI calculations

Editor’s Note: If only SUCI calculation is considered, this subclause may be removed. If other protocol, e.g. MIKEY-SAKKE is studied, this subclause is used for each of such protocol identified.

As per TS 33.501 [4] and Table 4.3.2-1 of 3GPP Cryptographic inventory 3GPP TR 33.938 [2], the SUCI calculation is done based on ECIES scheme. The ECIES is specified in the SECG version 2 [9] and [10].

Since ECIES will not be updated by SECG with PQC algorithms, 3GPP should study alternative solutions for SUCI calculation due to post-quantum threats to existing ECIES scheme.

### 7.1.2 Protocol #2: MIKEY-SAKKE key exchange

MIKEY-SAKKE is a key exchange method specified in the IETF RFC 6509 [6]. As described in TR 33.938 [2], it is used in the 3GPP system to securely transport cryptographic keys for Mission Critical Services [3]. It employs asymmetric cryptography for key distribution. It may be vulnerable to quantum computing if not updated using Post Quantum Cryptography (PQC).

Editor’s Note: It is ffs whether the IETF will update it to use PQC in the near future, and if not, how the potential risk can be addressed.

### 7.2 Solutions

Editor’s Note: This clause contains solutions to update 3GPP defined security protocols (for example SUCI calculation) to use the appropriate PQC algorithm, if those protocols are not expected to be updated by other SDOs to use PQC algorithms.

### 7.2.X Solutions to Protocol #X: <Title>

Editor’s Note: If only SUCI calculation is considered, this subclause may be removed. If other protocol, e.g. MIKEY-SAKKE is studied, this subclause is used for each of such protocol identified.

#### 7.2.X.Y Solution #Y to Protocol #X: <Title>

##### 7.2.X.Y.1 Introduction

##### 7.2.X.Y.2 Solution details

##### 7.2.X.Y.3 Evaluation

# 8 Conclusions

Editor’s Note: This clause contains agreed conclusions and any normative work is recommended.

Annex A (informative):
Change history

|  |
| --- |
| Change history |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2025-08 | SA3#123 | S3-252632 |  |  |  | TR 33.703 skeleton | 0.0.0 |
| 2025-08 | SA3#123 | S3-252975 |  |  |  | Incorporate pCRs from S3-252976, S3-252977, S3-252978, S3-252983, S3-252984, S3-253037 | 0.1.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |