|  |
| --- |
| 3GPP TR 33.703 V0.0.0 (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 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Assumptions 6

5 Principles and attributes of PQC to use in 3GPP procedures 7

6 Protocols expected to be updated for PQC by other SDOs 7

6.1 General 7

6.X Protocol #X 7

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

7.1 Threats 7

7.1.X Protocol #X: <Title> 7

7.2 Solutions 7

7.2.X Solutions to Protocol #X: <Title> 7

7.2.X.Y Solution #Y to Protocol #X: <Title> 8

7.2.X.Y.1 Introduction 8

7.2.X.Y.2 Solution details 8

7.2.X.Y.3 Evaluation 8

8 Conclusions 8

Annex A (informative): Change history 9

# 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

# 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".

# 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].

<ABBREVIATION> <Expansion>

# 4 Assumptions

Editor's Note: This clause contains overall assumptions for this study.

# 5 Impacts of use of PQC in 3GPP procedures

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

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

Editor’s Note: This clause identifies protocols used in 3GPP procedures that are expected to be updated for PQC by other SDOs and the expected timeline for when security these protocols will include PQC algorithms for incorporation into 3GPP procedures. The timeline is for the availability of stable protocols. These clause is expected to be consistent with TR 33.938.

## 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, and describes security threats and alternative solutions for the 3GPP procedures assuming these protocols are not updated to use PQC.

### 7.1 Threats

Editor’s Note: This clause contains security threats for 3GPP procedures if these protocols are not updated to use PQC.

### 7.1.X Protocol #X: <Title>

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

### 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. These protocols are not expected to be updated by other SDOs to use PQC algorithms.

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

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

#### 7.2.X.Y Solution #Y for 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 that 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 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |