|  |
| --- |
| 3GPP TR 33.938 V0.1.0 (2025-02) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on 3GPP Cryptographic Inventory(Release 19) |
|   |
|  |  |
|  |
| 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 Inventory of security protocols 6

Annex A (informative): Change history 7

# 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 lists the security protocols that use cryptography in 3GPP specifications for the 5G System in the Standalone mode. They

* 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 (e.g., integrity, confidentiality, and/or authentication)

NOTE: the present document does not include resolution to PQC migration, and does not contain solutions that lead to any specification/normative work.

# 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 TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[3] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[4] 3GPP TS 33.501: “Security architecture and procedures for 5G system”.

# 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 3GPP Cryptographic Inventory – 5G System

## 4.1 General

This clause provides inventory of security protocols that use cryptography in 3GPP specifications for 5G systems (limited to the standalone mode). The clause 4.2 and 4.3 present inventory in table formats whereas the detailed protocol list is described in 4.4.

## 4.2 3GPP Symmetric Cryptographic Algorithms

Editor’s Note: The current table is for example and placeholder purposes. It would be revised/refined onces the detailed protocol list description has been agreed.

Table 4.2-1: 3GPP Symmetric Cryptographic Algorithms (5G System)

|  |  |  |  |
| --- | --- | --- | --- |
| Protocol | 3GPP Cryptographic Profile | Cryptographic Algorithm(s) | Feature(s) |
| e.g., PDCP (TS 38.323[]) | TS 33.501 [4] | 128-NxA1 | Confidentiality and Integrity Protection |
|  |  | 128-NxA2 | Confidentiality and Integrity Protection |
|  |  |  |  |

## 4.3 3GPP Asymmetric Cryptographic Algorithms

Editor’s Note: The current table is for example and placeholder purposes. It would be revised/refined onces the detailed protocol list description has been agreed.

Table 4.3-1: 3GPP Asymmetric Cryptographic Algorithms (5G System)

|  |  |  |  |
| --- | --- | --- | --- |
| Protocol | 3GPP Cryptographic Profile | Cryptographic Algorithm(s) | Feature(s) |
| e.g., TLS (IETF RFC 8446) | TS 33.210 [2] | ECDHE (IETF RFC 8996) | Key Agreement |
|  |  | RSA (IETF RFC 8017) | Digital Signature and Authentication |
|  |  |  |  |

## 4.4 Detailed Protocol List

Editor’s Note: This detailed protocol list is expected to finalize first.

### 4.4.1 DTLS

DTLS is used in 5G system in standalone mode to protect the following:

N2 interface (see clause 9.2 of TS 33.501 [4]).

Xn interface (see clause 9.4 of TS 33.501 [4]).

DIAMETER or GTP-based interfaces (see clause 9.5 of TS 33.501 [4]).

gNB internal interfaces (see clause 9.8 of TS 33.501 [4]).

Security profiles for DTLS implementation and usage in 3GPP are given in clause 6.2 of TS 33.210 [2] and the certificate profile is given in clause 6.1.3a of TS 33.310 [3].

DTLS employs symmetric cryptography for confidentiality and integrity protection.

DTLS employs asymmetric cryptography for digital signature and key agreement.

### 4.4.2 TLS

TLS is used in 5G system in standalone mode to protect the following:

NIDD interfaces (see clause 6.16.3 of TS 33.501 [4]).

DIAMETER or GTP-based interfaces (see clause 9.5 of TS 33.501 [4]).

NEF – AF interface (see clauses 12.2 and 12.3 of TS 33.501 [4]).

Interfaces between network functions (see clauses 13.1, 13.2, 13.5 of TS 33.501 [4]).

N32 interface (see clause 13.2 of TS 33.501 [4]).

Network slice management interfaces (see clauses 15.2 and 15.3 of TS 33.501 [4]).

Message Service interfaces for MIoT over the 5G System (see clauses Y.2 – Y.4 of TS 33.501 [4]).

Security profiles for TLS implementation and usage in 3GPP are given in clause 6.2 of TS 33.210 [2] and the certificate profile is given in clause 6.1.3a of TS 33.310 [3].

TLS employs symmetric cryptography for confidentiality and integrity protection.

TLS employs asymmetric cryptography for digital signature and key agreement.

# Annex A (informative):Change history

|  |
| --- |
| Change history |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2025-02 | SA3#120 | S3-250401 |  |  |  | TR 33.938 skeleton | 0.0.0 |
| 2025-02 | SA3#120 | S3-250977 |  |  |  | Incorporate pCRs from S3‑250402, S3-251072, S3-251073, S3-251074 | 0.1.0 |