|  |
| --- |
| 3GPP TR 33.700-41 V0.0.2 (2024-03) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on enabling a cryptographic algorithm transition to 256-bits(Release 19) |
|   |
|  | 3GPP-logo_web |
|  |
| 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 16Internethttp://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.© 2022, 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

Introduction 5

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 7

5 Key issues 7

6 Solutions 7

6.1 Mapping of solutions to key issues 7

6.Y Solution #Y: <Title> 7

6.Y.1 Introduction 7

6.Y.2 Solution details 7

6.Y.3 Evaluation 7

7 Conclusions 7

Annex A: Change history 8

# 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.

## Introduction

# 1 Scope

This study aims to address key requirements for introducing support for 256-bit symmetric algorithms into the 5G System as well as the coexistence of 128-bit and 256-bit cryptographic algorithms. Considering findings and conclusions from preceding work, the following points should be addressed as part of the present document:

Studying key issues and candidate solutions concerning the negotiation (selection) of key sizes between UE and network, including:

- Potential risks and impacts to the current system when supporting both 128-bit and 256-bit algorithms in parallel and the adoption of 256-bit algorithms in existing deployments where 128 bits is already supported, e.g. handover scenarios within 5G system

- How to prioritise the use of 256-bit algorithms and mitigate bidding-down attacks when negotiating key sizes;

- How to ensure 256-bit security is achieved concerning varying levels of support for 256-bit algorithms by different UEs and within the network; potential dependencies in key-length selection of AS and NAS layers

- Study the implications and requirements for the key hierarchies to support 256-bit cryptographic algorithms

- Study the implications and requirements to AKA procedures.

# 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 23.501: "System Architecture for the 5G System".

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

[4] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP 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 3GPP 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 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Assumptions

The 5G System supports already procedures for the selection and activation of the AS and NAS security based on the UE security capabilities and network configuration.

The UE security capabilities IE is defined in TS 24.501 [4] clause 9.1.3.54. The IE includes already space for the introduction of new 5G algorithms, 4 for each type of algorithm (ciphering or integrity protection).

The NAS and AS SMC procedures described in TS 33.501 [3] in clauses 6.7.2 and 6.7.4 respectively enable the network and the UE to securely select and activate NAS and AS security based on the UE security capabilities and network configuration.

The UE security capabilities are sent to the network in an initial NAS message that can be unprotected. This is the reason why the 5G System supports a mechanism to protect against bidding down attacks by a man-in-the-middle tampering with the initial NAS message as pointed out in NOTE 1 of clause 6.7.2 of TS 33.501 [3]. This is the reason the UE security capabilities are replayed in the NAS SMC message.

Editor's Note: Further assumptions are ffs.

# 5 Key issues

Editor's Note: This clause contains all the key issues identified during the study.

### 5.X Key issue #X: <Title>

#### 5.X.1 Key issue details

#### 5.X.2 Threats

#### 5.X.3 Potential security requirements

# 6 Solutions

Editor's Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.1 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#X | KI#Y | KI#Z |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6.Y Solution #Y: <Title>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

Editor's Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | SA3#115 | S3-240330 |  |  |  | Document Skeleton | 0.0.2 |
| 2024-02 | SA3#115 | S3-241008 |  |  |  | scope | 0.0.2 |
| 2024-02 | SA3#115 | S3-241009 |  |  |  | assumption | 0.0.2 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |