|  |  |
| --- | --- |
| 3GPP TS 35.243 V18.0.0 (2024-03) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Specification of the AES based 256-bits algorithm set:  Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G;  Document 1: algorithm specification  (Release 18) | |
|  | |
|  |  |
|  | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://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.  © 2024, 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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® 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 Technical provisions 7

Annex A (informative): Change history 7

# Foreword

This Technical Specification 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

The present document is one of three, which between them form the entire specification set of the encryption and integrity protection algorithms, entitled:

- 3GPP TS 35.243: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G;  
**Document 1: Algorithm Specification ".**

- 3GPP TS 35.244: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G;  
Document 2: Implementation Test Data".

- 3GPP TS 35.245: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G;  
Document 3: Design Conformance Test Data".

# 1 Scope

The present document contains the algorithm specification which could be used as the encryption and integrity protection function 256-NEA5, 256-NIA5 and the combined authenticated encryption 256-NCA5 protection function for 3GPP systems.

# 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] The non-redacted specification is available via <http://www.etsi.org/WebSite/OurServices/Algorithms/3gppalgorithms.aspx> and is subject to licensing conditions described at this site.

Editor’s Note: The given reference [x] leads to the valid portal, but the desired specifications are not stored there because they are still under construction.

# 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], in the non-redacted version of the specification [2] and the following apply. A term defined in the present document and its corresponding non-redacted version [2] takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

## 3.2 Symbols

void

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], in the non-redacted version of the specification [2] and the following apply. An abbreviation defined in the present document and its corresponding non-redacted version [2] takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

# 4 Technical provisions

The technical provisions of the AES based 256-bits algorithm specification are contained in the non-redacted version of the present document [2].

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2023-11 | SA3#113 | S3-234427 |  |  |  | First time submitted for discussion and approval. | 0.1.0 |
| 2024-02 | SA3#115 | S3-240271 |  |  |  | Skeleton only submitted for approval. | 0.2.0 |
| 2024-02 | SA3#115 | S3-240280 |  |  |  | Technical provision content edited. | 0.3.0 |
| 2024-03 | SA#103 | SP-240225 |  |  |  | Presented for information and approval | 1.0.0 |
| 2024-03 | SA#103 |  |  |  |  | Upgrade to change control version | 18.0.0 |