|  |
| --- |
| 3GPP TS 35.235 V0.1.0 (2024-02) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and Security Aspects;Specification of the MILENAGE-256 algorithm set;An example set of 256-bit 3GPP Authentication and Key Generation functions f1, f1\*, f2, f3, f4, f5, f5\* and f5\*\*;Document 2: Algorithm Specification;(Release 19) |
|   |
|  |  |
|  |
| ***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.© 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 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

References 6

1 Scope 6

2 Structure of this specification 6

3 Introductory information 6

4 List of variables 6

5 Algorithm inputs and outputs 6

6 The algorithm framework and the specific example algorithm 7

7 Definition of the example algorithm 7

8 Implementation considerations 7

9 Specification of the xxx-256 based kernel function 7

Annex A (informative): Change history 8

# 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

Editor's Note: This clause contains preface information provided by ETSI SAGE.

The present document contains a 256-bit example of set of algorithms, collectively called MILENAGE-256, which may be used as the authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*. It is not mandatory to use the particular algorithms specified in this document – all eight functions are operator-specifiable rather than being fully standardised. Operators electing to employ this example set can further personalise the algorithms (as described in the text).

An additional function, f5\*\*, which is optional to implement and use, is also provided. This function, when used, replaces the use of f5\*, and then serves to protect against some new attacks that have been recently discovered.

The present document is one of four documents, which collectively comprise the entire specification of the example authentication and key generation algorithms. Namely:

- 3GPP TS 35.234 [2]: "Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*; Document 1: MILENAGE-256 General".

- **3GPP TS 35.235: "Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*; Document 2: MILENAGE-256 Algorithm Specification".**

- 3GPP TS 35.236 [3]: "Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*; Document 3: Implementors’ Test and Design Conformance Test Data".

- 3GPP TS 35.237 [4]: "Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*; Document 4: Summary and Results of Design and Evaluation".

# 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 35.234: "Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*; Document 1: MILENAGE-256 General".

[3] 3GPP TS 35.236: "Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*; Document 3: Implementors’ Test and Design Conformance Test Data".

[4] 3GPP TS 35.237: "Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f2, f3, f5, f5, f5\* and f5\*\*; Document 4: Summary and Results of Design and Evaluation".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 1 Scope

Editor's Note: This clause contains scope information from ETSI SAGE for selected option.

# 2 Structure of this specification

Editor's Note: this clause details how the present document is organized.

# 3 Introductory information

Editor's Note: this clause lists the notation that applies to the present document.

# 4 List of variables

Editor's Note: this clause provides list of variables that apply to the present document.

# 5 Algorithm inputs and outputs

Editor's Note: this clause provides algorithms inputs and outputs defined by ETSI SAGE.

# 6 The algorithm framework and the specific example algorithm

Editor's Note: this clause provides algorithm framework and the specific example algorithms from ETSI SAGE.

# 7 Definition of the example algorithm

Editor's Note: this clause provides definition of the example algorithms from ETSI SAGE

# 8 Implementation considerations

Editor's Note: this clause provides implementation considerations from ETSI SAGE.

# 9 Specification of the xxx-256 based kernel function

Editor's Note: this clause provides specification for the example kernel function that will be selected by 3GPP SA3.

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | SA3#115 | S3-24xxxx |  |  |  | TS skeleton | 0.0.0 |