3GPP TS 55.251 V16.0.0(2020-07)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Specification of the GEA5 and GIA5 encryption algorithms for General Packet Radio Service (GPRS);

GEA5 and GIA5 algorithm specification

(Release 16)

 

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.

Keywords

security, algorithm

***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.

© 2020, 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 [5](#__RefHeading___Toc467767840)

Introduction [5](#__RefHeading___Toc467767841)

1 Scope [6](#__RefHeading___Toc467767842)

2 References [6](#__RefHeading___Toc467767843)

3 Definitions, symbols and abbreviations [6](#__RefHeading___Toc467767844)

3.1 Definitions [6](#__RefHeading___Toc467767845)

3.2 Symbols [6](#__RefHeading___Toc467767846)

3.3 Abbreviations [7](#__RefHeading___Toc467767847)

4 Introductory information [7](#__RefHeading___Toc467767848)

4.1 Introduction [7](#__RefHeading___Toc467767849)

4.2 Notation [7](#__RefHeading___Toc467767850)

4.2.1 Radix [7](#__RefHeading___Toc467767851)

4.2.2 Conventions [7](#__RefHeading___Toc467767852)

4.2.3 Bit/byte ordering [7](#__RefHeading___Toc467767853)

4.3 List of variables [8](#__RefHeading___Toc467767854)

5 Confidentiality algorithm GEA5 [9](#__RefHeading___Toc467767855)

5.1 Introduction [9](#__RefHeading___Toc467767856)

5.2 Inputs and outputs [9](#__RefHeading___Toc467767857)

5.3 Components and architecture [9](#__RefHeading___Toc467767858)

5.4 Initialisation [9](#__RefHeading___Toc467767859)

5.5 Keystream generation [9](#__RefHeading___Toc467767860)

5.6 Output octets [9](#__RefHeading___Toc467767861)

6 Integrity algorithm GIA5 [10](#__RefHeading___Toc467767862)

6.1 Introduction [10](#__RefHeading___Toc467767863)

6.2 Inputs and outputs [10](#__RefHeading___Toc467767864)

6.3 Components and architecture [10](#__RefHeading___Toc467767865)

6.3.1 SNOW 3G [10](#__RefHeading___Toc467767866)

6.3.2 MULx [10](#__RefHeading___Toc467767867)

6.3.3 MULxPOW [10](#__RefHeading___Toc467767868)

6.3.4 MUL [10](#__RefHeading___Toc467767869)

6.4 Initialization [11](#__RefHeading___Toc467767870)

6.5 Calculation [11](#__RefHeading___Toc467767871)

Annex A (informative): Mathematical background of some operations of the GIA5 Algorithm [12](#__RefHeading___Toc467767872)

A.1 The function EVAL\_S [12](#__RefHeading___Toc467767873)

A.2 The function MUL(V, P, c) [12](#__RefHeading___Toc467767874)

Annex B (informative): Implementation options for some operations of the GIA5 algorithm [13](#__RefHeading___Toc467767875)

B.1 Overview [13](#__RefHeading___Toc467767876)

B.2. Procedure Pre\_Mul\_P [13](#__RefHeading___Toc467767877)

B.3 Function Mul\_P [13](#__RefHeading___Toc467767878)

Annex C (informative): Figures of the GEA5 and GIA5 algorithms [14](#__RefHeading___Toc467767879)

Annex D (informative): Simulation program listing [15](#__RefHeading___Toc467767880)

D.1 GEA5 [15](#__RefHeading___Toc467767881)

D.2 GIA5 [15](#__RefHeading___Toc467767882)

Annex E (informative): Change history [16](#__RefHeading___Toc467767883)

# 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.

# Introduction

This specification has been prepared by the 3GPP Task Force, and gives a detailed specification of the 3GPP confidentiality algorithm GEA5 and the 3GPP integrity algorithm GIA5.

This document is the first of three, which between them form the entire specification of the 3GPP confidentiality algorithm GEA5 and the 3GPP integrity algorithm GIA5:

- **3GPP TS 55.251: "Specification of the GEA5 and GIA5 encryption algorithms for GPRS; GEA5 and GIA4 algorithm specification".**

- 3GPP TS 55.252: "Specification of the GEA5 and GIA5 encryption algorithms for GPRS; Implementers' test data".

- 3GPP TS 55.253: "Specification of the GEA5 and GIA5 encryption algorithms for GPRS; Design conformance test data".

# 1 Scope

The present document defines the technical details of the 3GPP confidential algorithm GEA5 and the 3GPP integrity algorithm GIA5.

# 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 33.216: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions 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].

(none)

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

= The assignment operator.

 The bitwise exclusive-OR operation.

|| The concatenation of the two operands.

KASUMI[x]k The output of theKASUMIalgorithm applied to input value **x**using the key k.

X[i] The ith bit of the variable X. (X = X[0] || X[1] || X[2] || ….. ).

Yi The ith block of the variable Y. (Y = Y0 || Y1  || Y2 || …. ).

ceiling(x) The smallest integer greater than or equal to the real number x.

&n The bitwise AND operation in an n-bit register.

<<n t t-bit left shift in an n-bit register.

>>n t t-bit right shift in an n-bit register.

## 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].

CBC-MAC Cipher Block Chaining Message Authentication Code

MAC Message Authentication Code

# 4 Introductory information

## 4.1 Introduction

The confidentiality algorithm GEA5 is a stream cipher that is used to encrypt/decrypt blocks of data under a confidentiality key KC128. The block of data may be between 1 and 65536 octets long. The algorithm uses SNOW 3G [2] as a keystream generator.

The integrity algorithm GIA5 computes a 32-bit MAC (Message Authentication Code) of a given input message using an integrity key KI128. The approach adopted uses SNOW 3G.

## 4.2 Notation

### 4.2.1 Radix

The prefix "0x" indicates hexadecimal numbers.

### 4.2.2 Conventions

The assignment operator "=", as used in several programming languages.

<variable> = <expression>

means that <*variable*> assumes the value that <*expression*> had before the assignment took place. For instance,

*x* = *x* + *y* + 3

means

(new value of *x*) becomes (old value of *x*) + (old value of *y*) + 3.

### 4.2.3 Bit/byte ordering

All data variables in this specification are presented with the most significant bit (or byte) on the left hand side and the least significant bit (or byte) on the right hand side. Where a variable is broken down into a number of sub-strings, the left most (most significant) sub-string is numbered 0, the next most significant is numbered 1 and so on through to the least significant.

For example an n-bit MESSAGE is subdivided into 64-bit substrings MB0, MB1 … MBi so if the message is:

0x0123456789ABCDEFFEDCBA987654321086545381AB594FC28786404C50A37…

then:

MB0 = 0x0123456789ABCDEF  
MB1 **=** 0xFEDCBA9876543210  
MB2 = 0x86545381AB594FC2  
MB3 = 0x8786404C50A37…

In binary this is:

000000010010001101000101011001111000100110101011110011011110111111111110…

with MB0 = 0000000100100011010001010110011110001001101010111100110111101111  
MB1 **=** 1111111011011100101110101001100001110110010101000011001000010000  
MB2 = 1000011001010100010100111000000110101011010110010100111111000010  
MB3 = 1000011110000110010000000100110001010000101000110111…

## 4.3 List of variables

CONSTANT-F a 32-bit parameter which is constant for any given FRAMETYPE input.

DIRECTION the 1-bit input to both the GEA5 and GIA5 functions indicating the direction of transmission (uplink or downlink).

FRAMETYPE an 8-bit input to the GEA5 and GIA5 functions indicating the type of frame to be protected.

INPUT the 32-bit time variant input to the GEA5 function

INPUT-I the 32-bit time variant input to the GIA5 function

KC128 the 128-bit confidentiality key.

KI128 the 128-bit integrity key.

KS[i] the ith bit of keystream produced by the keystream generator.

L the number of 32-bit words of SNOW 3G keystream that are generated by GEA5 (equal to ceiling(M/4) ).

LENGTH a 64 bit parameter defined within GIA5 which specifies the number of bits of message to be MAC’d (equal to 8 times M).

M the input to the GEA5 function which specifies the number of octets of output required (1-65536); also the input to the GIA5 function which specifies the number of octets of message to be MAC’d (1-65536).

MAC the 32-bit message authentication code (MAC) produced by the integrity function GIA5.

MESSAGE the input bitstream of LENGTH bits that is to be processed by the GIA5 function.

OUTPUT the output octets from the GEA5 function.

S1, S2, … a sequence of 64-bit words derived from MESSAGE and LENGTH which is used within GIA5 to construct the MAC

z1, z2, … the 32-bit words forming the keystream sequence of SNOW 3G. The word produced first is z1, the next word z2 and so on.

# 5 Confidentiality algorithm GEA5

## 5.1 Introduction

The confidentiality algorithm GEA5 is a stream cipher that encrypts/decrypts blocks of data between 1 and 65536 octets in length.

## 5.2 Inputs and outputs

The inputs to the algorithm are given in Table 5.2.1, the output in Table 5.2.2:

Table 5.2.1: GEA5 inputs

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Size (bits)** | **Comment** |
| INPUT | 32 | Frame dependent input INPUT[0]…INPUT[31] |
| DIRECTION | 1 | Direction of transmission DIRECTION[0] |
| FRAMETYPE | 8 | Input value signifying the type of frame to be protected |
| KC128 | 128 | Confidentiality key KC128[0]….KC128[127] |
| M |  | The number of octets of output required in the range 1 to 65536 inclusive |

Table 5.2.2: GEA5 output

|  |  |  |
| --- | --- | --- |
| Parameter | Size (bits) | Comment |
| OUTPUT | 8M | Keystream octets OUTPUT{0}….OUTPUT{M-1} |

## 5.3 Components and architecture

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

## 5.4 Initialisation

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

## 5.5 Keystream generation

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

## 5.6 Output octets

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

# 6 Integrity algorithm GIA5

## 6.1 Introduction

The integrity algorithm GIA5 computes a Message Authentication Code (MAC) on an input message under an integrity key KI128. The message may be between 1 and 65536 octets long.

For ease of implementation the algorithm is based on the same stream cipher (SNOW 3G) [2] as is used by the confidentiality algorithm GEA5.

## 6.2 Inputs and outputs

The inputs to the algorithm are given in table 6.2.1, the output in table 6.2.2:

Table 6.2.1: GIA5 inputs

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Size (bits)** | **Comment** |
| INPUT-I | 32 | Frame dependent input INPUT-I[0]…INPUT-I[31] |
| M |  | The length of MESSAGE in octets (1-65536) |
| MESSAGE | 8M | Input octet stream MESSAGE{0}….MESSAGE{M-1} |
| DIRECTION | 1 | Direction of transmission DIRECTION[0] |
| FRAMETYPE | 8 | Input value signifying the type of frame to be protected |
| KI128 | 128 | Integrity key KI128[0]…KI128[127] |

Table 6.2.2: GIA5 output

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Size (bits)** | **Comment** |
| MAC | 32 | Message authentication code MAC[0]…MAC[31] |

## 6.3 Components and architecture

### 6.3.1 SNOW 3G

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

### 6.3.2 MULx

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

### 6.3.3 MULxPOW

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

### 6.3.4 MUL

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

## 6.4 Initialization

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

## 6.5 Calculation

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

Annex A (informative):  
Mathematical background of some operations of the GIA5 Algorithm

# A.1 The function EVAL\_S

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

# A.2 The function MUL(V, P, c)

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

Annex B (informative):  
Implementation options for some operations of the GIA5 algorithm

# B.1 Overview

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

# B.2. Procedure Pre\_Mul\_P

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

# B.3 Function Mul\_P

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

Annex C (informative):  
Figures of the GEA5 and GIA5 algorithms

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

Annex D (informative):  
Simulation program listing

# D.1 GEA5

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

# D.2 GIA5

This clause only available under licence.   
See <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>.

Annex E (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2016-04 | SA3#83 |  | - | - | - | First Draft | 0.1.0 |
| 2016-04 | SA3#83 |  | - | - | - | Removed algorithm details until permission to publish is received from French Government. | 0.0.2 |
| 2016-04 | SA3#83 |  | - | - | - | Updated version sent to French Government for permission to publish | 0.2.0 |
| 2016-05 | SA3#83 |  | - | - | - | Updated titles after comments in SA3 #83 | 0.2.1 |
| 2016-05 | SA3#83 |  | - | - | - | Removed algorithm details until permission to publish is received from French Government. | 0.2.2 |
| 2016-11 | SA3#85 |  | - | - | - | Full Specification with Example Code | 0.3.0 |
| 2016-06 | SA#72 | SP-160380 |  |  |  | EditHelp editorial fix and presented for information | 1.0.0 |
| 2016-11 | SA3#85 |  |  |  |  | Updated version only | 1.1.0 |
| 2016-11 | SA3#85 |  |  |  |  | Updated the editors note to reflect the need for a licence to see the content | 1.1.1 |
| 2016-11 | SA#74 | SP-160792 |  |  |  | MCC clean up, redacted version for TSG SA approval | 2.0.0 |
| 2016-12 | SA#74 |  |  |  |  | Approved by TSG SA | 13.0.0 |
| 2017-03 | SA#75 | - | - | - |  | Promotion to Release 14 without technical change | **14.0.0** |
| 2018-06 | - | - | - | - | - | Update to Rel-15 version (MCC) | **15.0.0** |
| 2020-07 | - | - | - | - | - | Update to Rel-16 version (MCC) | **16.0.0** |