3GPP TS 55.241 V16.0.0(2020-07)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Specification of the GIA4 integrity algorithm for   
General Packet Radio Service (GPRS);

GIA4 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 [4](#__RefHeading___Toc467768450)

Introduction [4](#__RefHeading___Toc467768451)

1 Scope [5](#__RefHeading___Toc467768452)

2 References [5](#__RefHeading___Toc467768453)

3 Definitions, symbols and abbreviations [5](#__RefHeading___Toc467768454)

3.1 Definitions [5](#__RefHeading___Toc467768455)

3.2 Symbols [5](#__RefHeading___Toc467768456)

3.3 Abbreviations [6](#__RefHeading___Toc467768457)

4 Introductory information [6](#__RefHeading___Toc467768458)

4.1 Introduction [6](#__RefHeading___Toc467768459)

4.2 Notation [6](#__RefHeading___Toc467768460)

4.2.1 Radix [6](#__RefHeading___Toc467768461)

4.2.2 Conventions [6](#__RefHeading___Toc467768462)

4.2.3 Bit/byte ordering [6](#__RefHeading___Toc467768463)

4.3 List of variables [7](#__RefHeading___Toc467768464)

5 Integrity algorithm GIA4 [7](#__RefHeading___Toc467768465)

5.1 Introduction [7](#__RefHeading___Toc467768466)

5.2 Inputs and outputs [7](#__RefHeading___Toc467768467)

5.3 Components and architecture [8](#__RefHeading___Toc467768468)

5.4 Initialisation [8](#__RefHeading___Toc467768469)

5.5 Calculation [8](#__RefHeading___Toc467768470)

Annex A (informative): Components and architecture of the GIA4 algorithm [9](#__RefHeading___Toc467768471)

Annex B (informative): Simulation program listing [10](#__RefHeading___Toc467768472)

Annex C (informative): Change history [11](#__RefHeading___Toc467768473)

# 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 integrity algorithm GIA4.

This document is the first of three, which between them form the entire specification of the 3GPP Integrity Algorithm GIA4:

- **3GPP TS 55.241: "Specification of the GIA4 encryption algorithms for GPRS; GIA4 specification".**

- 3GPP TS 55.242: "Specification of the GIA4 encryption algorithms for GPRS; Implementers' test data".

- 3GPP TS 55.243: "Specification of the GIA4 encryption algorithms for GPRS; Design conformance test data".

# 1 Scope

The present document defines the technical details of the 3GPP integrity algorithm GIA4.

# 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 35.202: "3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI 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 [2] 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 || …. ).

## 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 integrity algorithm GIA4computes a 32-bit MAC (Message Authentication Code) of a given input message using integrity key KI128. The approach adopted uses KASUMI [2] in a form of CBC-MAC mode.

## 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 would be:

000000010010001101000101011001111000100110101011110011011110111111111110…

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

## 4.3 List of variables

A, B are 64-bit registers that are used within the function to hold intermediate values.

BLOCKS an integer variable indicating the number of successive applications of KASUMI that need to be performed.

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

DIRECTION a 1-bit input indicating the direction of transmission (uplink or downlink).

FRAMETYPE an 8-bit input to the function indicating the type of frame to be protected.

INPUT-I a 32-bit time variant input to the function.

KI128 the 128-bit integrity key.

KM a 128-bit constant that is used to modify a key.

M an input to the 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 function.

MESSAGE the input octet stream of length M octets that is to be processed by the function.

PS is the input padded string processed by the function.

# 5 Integrity algorithm GIA4

## 5.1 Introduction

The integrity algorithm GIA4 computes a Message Authentication Code (MAC) on an input message under an integrity key IK128. The input message may be between 1 and 65536 octets long.

For ease of implementation the algorithm is based on the same block cipher (KASUMI) as is used by the confidentiality algorithm GEA4.

## 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: GIA4 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 5.2.2: GIA4 output

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

## 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 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):  
Components and architecture of the GIA4 algorithm

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):  
Simulation program listing

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):  
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 |  | - | - | - | Updated and Shared with French Government | 0.2.0 |
| 2016-05 | SA3#83 |  | - | - | - | Algorithm redacted | 0.2.2 |
| 2016-04 | SA3#85 |  | - | - | - | Full Specification with Example Code | 0.3.0 |
| 2016-06 | SA#72 | SP-160377 |  |  |  | EditHelp editorial fix and presented for information | 1.0.0 |
| 2016-11 | SA3#85 |  |  |  |  | Sent for Approval with only version changes | 1.1.0 |
| 2016-11 | SA3#85 |  |  |  |  | Changed editors note to reflect availability of the content | 1.1.1 |
| 2016-11 | SA#74 | SP-160791 |  |  |  | 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** |
| 2018-06 |  |  |  |  |  | Change to GSM logo | **15.0.1** |
| 2020-07 | - | - | - | - | - | Update to Rel-16 version (MCC) | **16.0.0** |