3GPP TS 55.253 V16.0.0(2020-07)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

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

Design conformance test data

(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

GEA5,GIA5,test,data,algorithm,GPRS,security,conformance

***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___Toc476044848)

Introduction [4](#__RefHeading___Toc476044849)

1 Scope [5](#__RefHeading___Toc476044850)

2 References [5](#__RefHeading___Toc476044851)

3 Definitions and abbreviations [5](#__RefHeading___Toc476044852)

3.1 Definitions [5](#__RefHeading___Toc476044853)

3.2 Abbreviations [5](#__RefHeading___Toc476044854)

4 Introductory information [5](#__RefHeading___Toc476044855)

4.1 Introduction [5](#__RefHeading___Toc476044856)

4.2 Notation [6](#__RefHeading___Toc476044857)

4.2.1 Radix [6](#__RefHeading___Toc476044858)

4.2.2 Conventions [6](#__RefHeading___Toc476044859)

4.2.3 Bit/Byte ordering [6](#__RefHeading___Toc476044860)

4.3 List of Variables [6](#__RefHeading___Toc476044861)

5 Design conformance test data [7](#__RefHeading___Toc476044862)

Annex A (informative): Change history [7](#__RefHeading___Toc476044863)

# 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

The present document has been prepared by the 3GPP Task Force, and gives a detailed specification of the 3GPP encryption algorithm GEA5 and integrity algorithm GIA5.

The present document is the second of three, which between them form the entire specification of the 3GPP encryption algorithm GEA5 and integrity algorithm GIA5:

- 3GPP TS 55.251: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the GEA5 encryption and GIA5 integrity algorithms for GPRS; GEA5 and GIA5 specification".

- 3GPP TS 55.252: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the GEA5 encryption and GIA5 integrity algorithms for GPRS; Implementers' test data".

**- 3GPP TS 55.253: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the GEA5 encryption and GIA5 integrity algorithms for GPRS; Design conformance test data".**

# 1 Scope

The present document defines the design conformance test data of the 3GPP encryption algorithm GEA5 and 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 55.251: "Specification of the GEA5 and GIA5 encryption algorithms for GPRS; GEA5 and GIA5 specification".

# 3 Definitions 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].

## 3.2 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].

# 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" is used to indicate hexadecimal numbers.

### 4.2.2 Conventions

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

<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 the present document 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 for a message:

0x0123456789ABCDEFFEDCBA987654321086545381AB594FC28786404C50A37…

is:

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

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 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' (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 Design conformance test data

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):   
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-03 | SA#75 | SP-170091 |  |  |  | Presented for approval | 2.0.0 |
| 2017-03 | SA#75 |  |  |  |  | Upgrade to change control version | 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** |