

ETSI TS 155 252 V15.0.0 (2018-07)



**Digital cellular telecommunications system (Phase 2+) (GSM);
Specification of the GEA5 encryption and GIA5 integrity
algorithms for General Packet Radio Service (GPRS);
Implementers' test data
(3GPP TS 55.252 version 15.0.0 Release 15)**



Reference

RTS/TSGS-0355252vf00

Keywords

GSM,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
3 Definitions and abbreviations.....	5
3.1 Definitions	5
3.2 Abbreviations	5
4 Introductory information	5
4.1 Introduction	5
4.2 Notation.....	5
4.2.1 Radix.....	5
4.2.2 Conventions	6
4.2.3 Bit/Byte ordering	6
4.3 List of variables.....	6
5 Test data	7
Annex A (informative): Change history	8
History	9

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.

This 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 implementers test data of the 3 GPP 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. for instance:

$$\langle \text{variable} \rangle = \langle \text{expression} \rangle$$

means that $\langle \text{variable} \rangle$ assumes the value that $\langle \text{expression} \rangle$ 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 $MB_0, MB_1 \dots MB_i$ so a message:

0x0123456789ABCDEFEDCBA987654321086545381AB594FC28786404C50A37...

is:

$MB_0 = 0x0123456789ABCDEF$
 $MB_1 = 0xFEDCBA9876543210$
 $MB_2 = 0x86545381AB594FC2$
 $MB_3 = 0x8786404C50A37\dots$

In binary this would be:

0000000100100011010001010110011110001001101010111100110111101111111110...

with

$MB_0 = 0000000100100011010001010110011110001001101010111100110111101111$
 $MB_1 = 1111111011011100101110101001100001110110010101000011001000010000$
 $MB_2 = 1000011001010100010100111000000110101011010110010100111111000010$
 $MB_3 = 1000011110000110010000000100110001010000101000110111\dots$

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 i th 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 $\lceil M / 4 \rceil$).

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 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-170090				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

History

Document history		
V15.0.0	July 2018	Publication