ETSI TS 155 241 V16.0.0 (2020-08)

TECHNICAL SPECIFICATION

**Digital cellular telecommunications system (Phase 2+) (GSM);
Specification of the GIA4 integrity algorithm
for General Packet Radio Service (GPRS);
GIA4 specification
(3GPP TS 55.241 version 16.0.0 Release 16)**

A GLOBAL INITIATIVE

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference
RTS/TSGS-0355241vg00

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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

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.
$\oplus$	The bitwise exclusive-OR operation.
$\|\|$	The concatenation of the two operands.
$\text{KASUMI}[x]_k$	The output of the KASUMI algorithm [2] applied to input value **x** using the key k.
X[i]	The i^{th} bit of the variable X. (X = X[0] $\|\|$ X[1] $\|\|$ X[2] $\|\|$ …..).
Y_i	The i^{th} block of the variable Y. ($Y = Y_0 \|\| Y_1 \|\| Y_2 \|\|$ ….).

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 GIA4 computes 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 MB_0, MB_1… MB_i so if the message is:

0x0123456789ABCDEFFEDCBA987654321086545381AB594FC28786404C50A37…

then:

MB_0 = 0x0123456789ABCDEF
MB_1 = 0xFEDCBA9876543210
MB_2 = 0x86545381AB594FC2
MB_3 = 0x8786404C50A37…

In binary this would be:

0000000100100011010001010110011110001001101010111100110111101111111111110…

with MB_0 = 0000000100100011010001010110011110001001101010111100110111101111
MB_1 = 1111111011011100101110101001100001110110010101000011001000010000
MB_2 = 1000011001010100010100111000000110101011010110010100111111000010
MB_3 = 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**

History

Document history		
V16.0.0	August 2020	Publication