ETSI TS 155 243 V13.0.0 (2017-04)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+) (GSM); Specification of the GIA4 integrity algorithm for General Packet Radio Service (GPRS); Design conformance test data (3GPP TS 55.243 version 13.0.0 Release 13)

Reference
RTS/TSGS-0355243vd00

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

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

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

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 integrity algorithm GIA4.

The present document is the third of three, which between them form the entire specification of the 3GPP Integrity Algorithm GIA4:

- 3GPP TS 55.241: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the GIA4 integrity algorithms for GPRS; GIA4 specification".
- 3GPP TS 55.242: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the GIA4 integrity algorithms for GPRS; Implementers' test data".
- **3GPP TS 55.243: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the GIA4 integrity algorithms for GPRS; Design conformance test data".**

1 Scope

The present document defines the Design conformance test data for 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 55.241: "Specification of the GIA4 encryption algorithms for GPRS; GIA4 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 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" is used to indicate hexadecimal numbers.

4.2.2 Conventions

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

<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 MB_0,MB_1…MB_i so for the following message:

0x0123456789ABCDEFFEDCBA987654321086545381AB594FC28786404C50A37…

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 = 10000111100001100100000000100110001010000101000110111…

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 Conformance 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-170089				Presented for approval	2.0.0
2017-03	SA#75					Upgrade to change control version	13.0.0

History

Document history		
V13.0.0	April 2017	Publication