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)
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

Intellectual Property Rights ................................................................................................................................ 2  
Legal Notice ....................................................................................................................................................... 2  
Modal verbs terminology .................................................................................................................................... 2  
Foreword ............................................................................................................................................................. 4  
Introduction ........................................................................................................................................................ 4  

1 Scope .................................................................................................................................................................. 5  

2 References ................................................................................................................................................ 5  

3 Definitions, symbols and abbreviations ................................................................................................... 5  
3.1 Definitions .................................................................................................................................................. 5  
3.2 Symbols .................................................................................................................................................... 5  
3.3 Abbreviations ............................................................................................................................................. 6  

4 Introductory information .............................................................................................................................. 6  
4.1 Introduction .............................................................................................................................................. 6  
4.2 Notation .................................................................................................................................................... 6  

4.2.1 Radix .................................................................................................................................................... 6  
4.2.2 Conventions ........................................................................................................................................... 6  
4.2.3 Bit/byte ordering ..................................................................................................................................... 6  
4.3 List of variables .......................................................................................................................................... 7  

5 Integrity algorithm GIA4 .......................................................................................................................... 7  
5.1 Introduction .............................................................................................................................................. 7  
5.2 Inputs and outputs .................................................................................................................................... 7  
5.3 Components and architecture ............................................................................................................. 8  
5.4 Initialisation ............................................................................................................................................... 8  
5.5 Calculation ................................................................................................................................................ 8  

Annex A (informative): Components and architecture of the GIA4 algorithm ............................................. 9  
Annex B (informative): Simulation program listing ....................................................................................... 10  
Annex C (informative): Change history ......................................................................................................... 11  

History .............................................................................................................................................................. 12
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".

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 the KASUMI algorithm [2] applied to input value x using the key k.
X[i] The i\textsuperscript{th} bit of the variable X. (X = X[0] || X[1] || X[2] || ...).
Y_{i} The i\textsuperscript{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].

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBC-MAC</td>
<td>Cipher Block Chaining Message Authentication Code</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
</tbody>
</table>

4 Introductory information

4.1 Introduction


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.

\[ \text{<variable>} = \text{<expression>} \]

means that \text{<variable>} assumes the value that \text{<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:

0x0123456789ABCDEFEDCBA987654321086545381AB594FC28786404C50A37…

then:

\[ \text{MB}_0 = 0x0123456789ABCDEF} \]
\[ \text{MB}_1 = 0xFEDCBA9876543210} \]
\[ \text{MB}_2 = 0x86545381AB594FC2} \]
\[ \text{MB}_3 = 0x8786404C50A37… \]
In binary this would be:

```
000000010010001101000101011001111000100110101011110011011110111111111110...
```

with

- $MB_0 = 00000010010001101000101011001111000100110101011110011011110111111111110…$
- $MB_1 = 111111110110111001101000111000011101010100001010000100001000010000$
- $MB_2 = 10000110101010001100110111000011101010101100101010011011111111000010$
- $MB_3 = 1000011100001110010000001001100100010100000100011010110111…$

### 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>
<thead>
<tr>
<th>Parameter</th>
<th>Size (bits)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>INPUT-I</td>
<td>32</td>
<td>Frame dependent input INPUT-I[0]...INPUT-I[31]</td>
</tr>
<tr>
<td>M</td>
<td></td>
<td>The length of MESSAGE in octets (1-65536)</td>
</tr>
<tr>
<td>MESSAGE</td>
<td>8M</td>
<td>Input octet stream MESSAGE[0]...MESSAGE[M-1]</td>
</tr>
<tr>
<td>DIRECTION</td>
<td>1</td>
<td>Direction of transmission DIRECTION[0]</td>
</tr>
<tr>
<td>FRAMETYPE</td>
<td>8</td>
<td>Input value signifying the type of frame to be protected</td>
</tr>
<tr>
<td>KI128</td>
<td>128</td>
<td>Integrity key KI128[0]...KI128[127]</td>
</tr>
</tbody>
</table>
Table 5.2.2: GIA4 output

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Size (bits)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>32</td>
<td>Message authentication code MAC[0]…MAC[31]</td>
</tr>
</tbody>
</table>

5.3 Components and architecture

This clause only available under licence.

5.4 Initialisation

This clause only available under licence.

5.5 Calculation

This clause only available under licence.
Annex A (informative):
Components and architecture of the GIA4 algorithm

This clause only available under licence.
Annex B (informative):
Simulation program listing

This clause only available under licence.
Annex C (informative):
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Meeting/TDoc</th>
<th>CR</th>
<th>Rev</th>
<th>Cat</th>
<th>Subject/Comment</th>
<th>New version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-04</td>
<td>SA3#83</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>First Draft</td>
<td>0.1.0</td>
</tr>
<tr>
<td>2016-04</td>
<td>SA3#83</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Updated and Shared with French Government</td>
<td>0.2.0</td>
</tr>
<tr>
<td>2016-05</td>
<td>SA3#83</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Algorithm redacted</td>
<td>0.2.2</td>
</tr>
<tr>
<td>2016-06</td>
<td>SA3#85</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Full Specification with Example Code</td>
<td>0.3.0</td>
</tr>
<tr>
<td>2016-06</td>
<td>SA72/SP-160377</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>EditHelp editorial fix and presented for information</td>
<td>1.0.0</td>
</tr>
<tr>
<td>2016-11</td>
<td>SA3#85</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Sent for Approval with only version changes</td>
<td>1.1.0</td>
</tr>
<tr>
<td>2016-11</td>
<td>SA74/SP-160791</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Changed editors note to reflect availability of the content</td>
<td>1.1.1</td>
</tr>
<tr>
<td>2016-11</td>
<td>SA74/SP-160791</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>MCC clean up, redacted version for TSG SA approval</td>
<td>2.0.0</td>
</tr>
<tr>
<td>2016-12</td>
<td>SA74</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Approved by TSG SA</td>
<td>13.0.0</td>
</tr>
<tr>
<td>2017-03</td>
<td>SA75</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Promotion to Release 14 without technical change</td>
<td>14.0.0</td>
</tr>
<tr>
<td>2018-06</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Update to Rel-15 version (MCC)</td>
<td>15.0.0</td>
</tr>
<tr>
<td>2018-06</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Change to GSM logo</td>
<td>15.0.1</td>
</tr>
<tr>
<td>2020-07</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Update to Rel-16 version (MCC)</td>
<td>16.0.0</td>
</tr>
</tbody>
</table>
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td>V16.0.0</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>