

# ETSI TS 135 208 V17.0.0 (2022-04)



**Universal Mobile Telecommunications System (UMTS);  
LTE;  
3G Security;  
Specification of the MILENAGE algorithm set: An example  
algorithm set for the 3GPP authentication and key generation  
functions  $f_1$ ,  $f_1^*$ ,  $f_2$ ,  $f_3$ ,  $f_4$ ,  $f_5$  and  $f_5^*$ ;  
Document 4: Design conformance test data  
(3GPP TS 35.208 version 17.0.0 Release 17)**



---

**Reference**

RTS/TSGS-0335208vh00

---

**Keywords**

LTE,SECURITY,UMTS

**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 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**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](http://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/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our  
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**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 2022.  
All rights reserved.

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

**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 a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# 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 Outline of the design conformance test data ..... | 5         |
| 1.1 References .....                                | 5         |
| 2 Introductory information .....                    | 5         |
| 2.1 Introduction .....                              | 5         |
| 2.2 Radix .....                                     | 6         |
| 2.3 Bit/Byte ordering.....                          | 6         |
| 2.4 List of Variables .....                         | 6         |
| 2.5 Algorithm Inputs and Outputs .....              | 7         |
| 2.6 Coverage.....                                   | 8         |
| 3 Conformance test data for Rijndael.....           | 8         |
| 3.1 Overview .....                                  | 8         |
| 3.2 Format .....                                    | 8         |
| 3.3 Test Sets .....                                 | 8         |
| 3.3.1 Set 1 Binary Format.....                      | 8         |
| 3.3.2 Hexadecimal Format.....                       | 9         |
| 4 Conformance test data for MILENAGE.....           | 9         |
| 4.1 Overview .....                                  | 9         |
| 4.2 Format .....                                    | 9         |
| 4.3 Test Sets .....                                 | 10        |
| 4.3.1 Set 1 .....                                   | 10        |
| 4.3.2 Test Set 2 .....                              | 10        |
| 4.3.3 Test Set 3 .....                              | 11        |
| 4.3.4 Test Set 4 .....                              | 11        |
| 4.3.5 Test Set 5 .....                              | 11        |
| 4.3.6 Test Set 6 .....                              | 12        |
| 4.3.7 Test Set 7 .....                              | 12        |
| 4.3.8 Test Set 8 .....                              | 12        |
| 4.3.9 Test Set 9 .....                              | 13        |
| 4.3.10 Test Set 10 .....                            | 13        |
| 4.3.11 Test Set 11 .....                            | 13        |
| 4.3.12 Test Set 12 .....                            | 14        |
| 4.3.13 Test Set 13 .....                            | 14        |
| 4.3.14 Test Set 14 .....                            | 14        |
| 4.3.15 Test Set 15 .....                            | 15        |
| 4.3.16 Test Set 16 .....                            | 15        |
| 4.3.17 Test Set 17 .....                            | 15        |
| 4.3.18 Test Set 18 .....                            | 16        |
| 4.3.19 Test Set 19 .....                            | 16        |
| 4.3.20 Test Set 20 .....                            | 16        |
| <b>Annex A (informative): Change history .....</b>  | <b>17</b> |
| History .....                                       | 18        |

---

## Foreword

This Technical Specification (TS) has been produced by the 3<sup>rd</sup> 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 document has been prepared by the 3GPP Task Force, and contains an example set of algorithms which may be used as the authentication and key generation functions *f1*, *f1\**, *f2*, *f3*, *f4*, *f5* and *f5\**. (It is not mandatory that the particular algorithms specified in this document are used — all seven functions are operator-specifiable rather than being fully standardised). This document is one five, which between them form the entire specification of the example algorithms, entitled:

- 3GPP TS 35.205: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1\**, *f2*, *f3*, *f4*, *f5* and *f5\**; Document 1: General".
- 3GPP TS 35.206: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1\**, *f2*, *f3*, *f4*, *f5* and *f5\**; Document 2: Algorithm Specification".
- 3GPP TS 35.207: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1\**, *f2*, *f3*, *f4*, *f5* and *f5\**; Document 3: Implementors' Test Data".
- 3GPP TS 35.208: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1\**, *f2*, *f3*, *f4*, *f5* and *f5\**; **Document 4: Design Conformance Test Data**".
- 3GPP TR 35.909: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1\**, *f2*, *f3*, *f4*, *f5* and *f5\**; Document 5: Summary and results of design and evaluation".

---

# 1 Outline of the design conformance test data

Section 2 introduces the algorithms and describes the notation used in the subsequent sections.

Section 3 provides test data for the cryptographic kernel function Rijndael.

Section 4 provides test data for the MILENAGE authentication and key generation algorithms  $f1$ ,  $f1^*$ ,  $f2$ ,  $f3$ ,  $f4$ ,  $f5$  and  $f5^*$ .

## 1.1 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 TS 33.102 v3.5.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [2] 3GPP TS 33.105 v3.4.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements".
- [3] 3GPP TS 35.206: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions  $f1$ ,  $f1^*$ ,  $f2$ ,  $f3$ ,  $f4$ ,  $f5$  and  $f5^*$ ; Document 2: Algorithm Specification".
- [4] 3GPP TS 35.207: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions  $f1$ ,  $f1^*$ ,  $f2$ ,  $f3$ ,  $f4$ ,  $f5$  and  $f5^*$ ; Document 3: Implementors' Test Data".
- [5] 3GPP TS 35.208: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions  $f1$ ,  $f1^*$ ,  $f2$ ,  $f3$ ,  $f4$ ,  $f5$  and  $f5^*$ ; Document 4: Design Conformance Test Data" (this document).
- [6] Joan Daemen and Vincent Rijmen: "AES Proposal: Rijndael", available at <http://csrc.nist.gov/encryption/aes/round2/AESAlgs/Rijndael/Rijndael.pdf> or <http://www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip>
- [7] <http://csrc.nist.gov/encryption/aes/>

---

## 2 Introductory information

### 2.1 Introduction

Within the security architecture of the 3GPP system there are seven security functions  $f1$ ,  $f1^*$ ,  $f2$ ,  $f3$ ,  $f4$ ,  $f5$  and  $f5^*$ . The operation of these functions falls within the domain of one operator, and the functions are therefore to be specified

by each operator rather than being fully standardized. The algorithms specified in this document are examples that may be used by an operator who does not wish to design his own.

The inputs and outputs of all seven algorithms are defined in section 2.5.

This document provides sets of input/output test data for 'black box' testing of physical realizations of all algorithms.

## 2.2 Radix

Unless stated otherwise, all test data values presented in this document are in hexadecimal.

## 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 substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

## 2.4 List of Variables

|                 |   |
|-----------------|---|
| AK              | a 48-bit anonymity key that is the output of either of the functions $f5$ and $f5^*$ .  |
| AMF             | a 16-bit authentication management field that is an input to the functions $f1$ and $f1^*$ .  |
| c1,c2,c3,c4,c5  | 128-bit constants, which are XORed onto intermediate variables.   |
| CK              | a 128-bit confidentiality key that is the output of the function $f3$ .   |
| IK              | a 128-bit integrity key that is the output of the function $f4$ .   |
| K               | a 128-bit subscriber key that is an input to the functions $f1$ , $f1^*$ , $f2$ , $f3$ , $f4$ , $f5$ and $f5^*$ .   |
| MAC-A           | a 64-bit network authentication code that is the output of the function $f1$ .  |
| MAC-S           | a 64-bit resynchronisation authentication code that is the output of the function $f1^*$ .  |
| OP              | a 128-bit Operator Variant Algorithm Configuration Field that is a component of the functions $f1$ , $f1^*$ , $f2$ , $f3$ , $f4$ , $f5$ and $f5^*$ .        |
| OP <sub>c</sub> | a 128-bit value derived from <b>OP</b> and <b>K</b> and used within the computation of the functions.   |
| r1,r2,r3,r4,r5  | integers in the range 0–127 inclusive, which define amounts by which intermediate variables are cyclically rotated.   |
| RAND            | a 128-bit random challenge that is an input to the functions $f1$ , $f1^*$ , $f2$ , $f3$ , $f4$ , $f5$ and $f5^*$ .   |
| RES             | a 64-bit signed response that is the output of the function $f2$ .  |
| SQN             | a 48-bit sequence number that is an input to either of the functions $f1$ and $f1^*$ . (For $f1^*$ this input is more precisely called SQN <sub>MS</sub> .) |

## 2.5 Algorithm Inputs and Outputs

The inputs to the algorithms are given in tables 1 and 2, the outputs in tables 3–9 below.

**Table 1. inputs to  $f_1$  and  $f_1^*$**

| Parameter | Size (bits) | Comment   |
|-----------|-------------|---|
| K         | 128         | Subscriber key K[0]...K[127]  |
| RAND      | 128         | Random challenge RAND[0]...RAND[127]  |
| SQN       | 48          | Sequence number SQN[0]...SQN[47]. (For $f_1^*$ this input is more precisely called SQN <sub>MS</sub> .) |
| AMF       | 16          | Authentication management field AMF[0]...AMF[15]  |

**Table 2. inputs to  $f_2$ ,  $f_3$ ,  $f_4$ ,  $f_5$  and  $f_5^*$**

| Parameter | Size (bits) | Comment                              |
|-----------|-------------|--------------------------------------|
| K         | 128         | Subscriber key K[0]...K[127]         |
| RAND      | 128         | Random challenge RAND[0]...RAND[127] |

**Table 3.  $f_1$  output**

| Parameter | Size (bits) | Comment  |
|-----------|-------------|--|
| MAC-A     | 64          | Network authentication code MAC-A[0]...MAC-A[63] |

**Table 4.  $f_1^*$  output**

| Parameter | Size (bits) | Comment  |
|-----------|-------------|--|
| MAC-S     | 64          | Resynch authentication code MAC-S[0]...MAC-S[63] |

**Table 5.  $f_2$  output**

| Parameter | Size (bits) | Comment                   |
|-----------|-------------|---------------------------|
| RES       | 64          | Response RES[0]...RES[63] |

**Table 6.  $f_3$  output**

| Parameter | Size (bits) | Comment                             |
|-----------|-------------|-------------------------------------|
| CK        | 128         | Confidentiality key CK[0]...CK[127] |

**Table 7.  $f_4$  output**

| Parameter | Size (bits) | Comment                       |
|-----------|-------------|-------------------------------|
| IK        | 128         | Integrity key IK[0]...IK[127] |

**Table 8.  $f_5$  output**

| Parameter | Size (bits) | Comment                      |
|-----------|-------------|------------------------------|
| AK        | 48          | Anonymity key AK[0]...AK[47] |

**Table 9.  $f_5^*$  output**

| Parameter | Size (bits) | Comment                              |
|-----------|-------------|--------------------------------------|
| AK        | 48          | Resynch anonymity key AK[0]...AK[47] |

Note: Both  $f_5$  and  $f_5^*$  outputs are called AK according to reference [2]. In practice only one of them will be calculated in each instance of the authentication and key agreement procedure.



## 2.6 Coverage

For each of the algorithms the test data sets have been selected such that, provided the entire set of tests is run:

- Each input bit of the Rijndael kernel function will have been in both the '0' and '1' states.
- Each input bit of the modes (RAND, K, SQN, AMF) will have been in both the '0' and '1' states.
- Every S-Box entry of the Rijndael kernel function will have been used.

---

## 3 Conformance test data for Rijndael

### 3.1 Overview

The test data sets presented here are for the cryptographic kernel function Rijndael. The first 6 test sets are the same as in document 3: implementors' test data.

### 3.2 Format

The first test set is shown twice, once in binary format, once in hexadecimal format. This is to explicitly show the relationship between the binary data and the hexadecimal representation. The remainder of the test sets are presented in hexadecimal format only. A hexadecimal number will be broken up in two rows of two 32-bit words. For example, the number `ee36f7cf037d37d3692f7f0399e7949a` will be written as

```
ee36f7cf 037d37d3
692f7f03 99e7949a.
```

### 3.3 Test Sets

#### 3.3.1 Set 1 Binary Format

```
Plaintext: 11101110 00110110 11110111 11001111 00000011 01111101 00110111 11010011 01101001
00101111 01111111 00000011 10011001 11100111 10010100 10011010
Ciphertext: 10011110 00101001 10000000 11000101 10010111 00111001 11011010 01100111 10110001
00110110 00110101 01011110 00111100 11101101 11100110 10100010
Key: 01000110 01011011 01011100 11101000 10110001 10011001 10110100 10011111 10101010
01011111 00001010 00101110 11100010 00111000 10100110 10111100
```

### 3.3.2 Hexadecimal Format

| Set | Plaintext                              | Ciphertext                              | Key                                    |
|-----|--|---|--|
| 1   | ee36f7cf 037d37d3<br>692f7f03 99e7949a | 9e2980c5 9739da67<br>b136355e 3cede6a2  | 465b5ce8 b199b49f<br>aa5f0a2e e238a6bc |
| 2   | 93cc3640 c5d6a521<br>d81235bd 0882bf0a | 009a9e09 96561525<br>f611667b bf79e226  | 0396eb31 7b6d1c36<br>f19c1c84 cd6ffd16 |
| 3   | 8f7a8f0d 108b7f2d<br>97a53eac c1d958d9 | 5d9bce85 4decaf0d<br>a93d28b7 e35f608c  | fec86ba6 eb707ed0<br>8905757b 1bb44b8f |
| 4   | 68c98bbf ab628ec1<br>adf2a3d9 0c34a751 | db2944cc e8e683cd<br>03fff199 31a12135  | 9e5944ae a94b8116<br>5c82fbf9 f32db751 |
| 5   | a840b1dd 60249aa3<br>22016b4b 31daf3b8 | 02bffdada 7137c492<br>c00e8452 d8c76eaa | 4ab1deb0 5ca6ceb0<br>51fc98e7 7d026a84 |
| 6   | d66789ef f5996b9c<br>ffd89e0a 77148657 | bdf226fe cf9ff996<br>1e5c2621 b764efb1  | 6c38a116 ac280c45<br>4f59332e e35c8c4f |
| 7   | 8cbdb88c 620ffe88<br>f8ce0042 a5052568 | fe8d6888 b5a5c146<br>efea6660 f7b4e699  | 523ace48 994925ca<br>0495efd5 0c7c71e2 |
| 8   | 83a4dbcc f3ff12e2<br>154dbf45 512b5a32 | 1c3aff64 cd717a6e<br>959c95c8 b9cd7d3f  | e4aee4fa eeb2f93d<br>43604f5f 2e65ff25 |
| 9   | d117610c 04f5d3d6<br>1d8cb6bc 910a918b | 21bc0073 cc9aa7a3<br>81257774 43f8663f  | b2c211ec 004d0323<br>022e49cc d363c8ff |
| 10  | 9d7cf334 be57ea4d<br>37f28c8f 8f0a7259 | 1591d87d 8fa69176<br>eae9fae9 02cd61a4  | 443c5a67 59e04dc2<br>c9c6e465 823dd5b6 |
| 11  | 0f3c382c 488efe2d<br>8ce7eaa7 7093a486 | c59e0669 76d92f8e<br>567b806f 94fb09d2  | 23e5c9b1 8034df64<br>21f22972 c3bd2d93 |
| 12  | 51c0d9dc cb03b860<br>43d378ea 5f0dd0f8 | ff00e5a1 a02f7594<br>3b4a5a1e 39bf5dc3  | d6856512 fd11bf4f<br>91781e3b 1ea9d8de |
| 13  | 886f7d2c 6f1dc0cc<br>851fdd41 82e09d99 | 3f65bc17 b47b645b<br>0fbfbfe8 da4269bf  | e5e436d4 593ef7cb<br>a221cd07 lccadfdf |
| 14  | dfb0cd05 5b43bd5b<br>7a31c294 0174b44f | 32976e2e d7fb97b2<br>bcaaba00 80faf1e5  | d9c9453e 1b858f22<br>dab53e20 44e849de |
| 15  | 7ced704d b8df58f4<br>4972cecc 0531bc04 | 53772447 4cf17c9b<br>105673b5 f37581c8  | 38fe9997 cbac8d9a<br>c4fc78cc 1fcb1e22 |
| 16  | 878d0fee ad58387e<br>1b4aaacf b6805e9f | e555cfb7 9663f0ea<br>fdcc9665 55d6498d  | 8d493a28 f17cfb7d<br>e5be8354 333a66f4 |
| 17  | 29f852ce 631605e3<br>1722fd87 3bc74208 | d78106ad 6fdae41c<br>95dd2f7b 5b479a79  | 5d733139 16bde011<br>c7c26700 0bfe2a9c |
| 18  | 8995e0d7 0281690a<br>666070db bd6f0f27 | 70b059ad f647d183<br>a18512a3 72ae683c  | 32448511 c137459f<br>f1d12c17 2cdf7262 |
| 19  | d1ce62ef b1010adb<br>2f6eabb2 63e16ee4 | ec7fc8b1 10246889<br>cff7293f e30c8465  | 93833efa 7bb1316e<br>ebb3dbe3 20a5448d |
| 20  | 260a7f00 98fe903e<br>9bb255f6 56840627 | 91747de6 7effaff8<br>578381ef 27e497ec  | 09fa653a cbf5acc8<br>3e307caa 6e18aa67 |

## 4 Conformance test data for MILENAGE

### 4.1 Overview

The test data sets presented here are for the seven functions  $f1$ ,  $f1^*$ ,  $f2$ ,  $f3$ ,  $f4$ ,  $f5$  and  $f5^*$ . The first 6 test sets are the same as in document 2: implementors' test data.

### 4.2 Format

Each Test shows the various inputs to the algorithm. This is followed by the configuration field OP, the value  $OP_C = OP \oplus E[OP]_K$  and finally by the function outputs.

The first test set is shown twice, once in binary format, once in hexadecimal format. This is to explicitly show the relationship between the binary data and the hexadecimal representation. The remainder of the test sets are presented in hexadecimal format only.

## 4.3 Test Sets

### 4.3.1 Set 1

#### Binary Format

```

K:      01000110 01011011 01011100 11101000 10110001 10011001 10110100 10011111 10101010 01011111
        00001010 00101110 11100010 00111000 10100110 10111100
RAND:  00100011 01010101 00111100 10111110 10010110 00110111 10101000 10011101 00100001 10001010
        11100110 01001101 10101110 01000111 10111111 00110101
SQN:   11111111 10011011 10110100 11010000 10110110 00000111
AMF:   10111001 10111001
OP:    11001101 11000010 00000010 11010101 00010010 00111110 00100000 11110110 00101011 01101101
        01100111 01101010 11000111 00101100 10110011 00011000
OPc:   11001101 01100011 11001011 01110001 10010101 01001010 10011111 01001110 01001000 10100101
        10011001 01001110 00110111 10100000 00101011 10101111
f1:    01001010 10011111 11111010 11000011 01010100 11011111 10101111 10110011
f1*:   00000001 11001111 10101111 10011110 11000110 11000100 01110001 11101001
f2:    10100101 01000010 00010001 11010101 11100011 10111010 01010000 10111111
f5:    10101010 01101000 10011100 01100100 10000011 01110000
f3:    10110100 00001011 10101001 10100011 11000101 10001011 00101010 00000101 10111011 11110000
        11011001 10000111 10110010 00011011 11111000 11001011
f4:    11110111 01101001 10111100 11010111 01010001 00000100 01000110 00000100 00010010 01110110
        01110010 01110001 00011100 01101101 00110100 01000001
f5*:   01000101 00011110 10001011 11101100 10100100 00111011

```

#### Hexadecimal Format

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 465b5ce8 b199b49f aa5f0a2e e238a6bc |
| RAND     | 23553cbe 9637a89d 218ae64d ae47bf35 |
| SQN      | ff9bb4d0 b607                       |
| AMF      | b9b9                                |
| OP       | cdc202d5 123e20f6 2b6d676a c72cb318 |
| OPc      | cd63cb71 954a9f4e 48a5994e 37a02baf |
| f1       | 4a9ffac3 54dfafb3                   |
| f1*      | 01cfaf9e c4e871e9                   |
| f2       | a54211d5 e3ba50bf                   |
| f5       | aa689c64 8370                       |
| f3       | b40ba9a3 c58b2a05 bbf0d987 b21bf8cb |
| f4       | f769bcd7 51044604 12767271 1c6d3441 |
| f5*      | 451e8bec a43b                       |

### 4.3.2 Test Set 2

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 465b5ce8 b199b49f aa5f0a2e e238a6bc |
| RAND     | 23553cbe 9637a89d 218ae64d ae47bf35 |
| SQN      | ff9bb4d0 b607                       |
| AMF      | b9b9                                |
| OP       | cdc202d5 123e20f6 2b6d676a c72cb318 |
| OPc      | cd63cb71 954a9f4e 48a5994e 37a02baf |
| f1       | 4a9ffac3 54dfafb3                   |
| f1*      | 01cfaf9e c4e871e9                   |
| f2       | a54211d5 e3ba50bf                   |
| f5       | aa689c64 8370                       |
| f3       | b40ba9a3 c58b2a05 bbf0d987 b21bf8cb |
| f4       | f769bcd7 51044604 12767271 1c6d3441 |
| f5*      | 451e8bec a43b                       |

### 4.3.3 Test Set 3

| Variable | Value                               |
|----------|-------------------------------------|
| K        | fec86ba6 eb707ed0 8905757b 1bb44b8f |
| RAND     | 9f7c8d02 1accf4db 213ccff0 c7f71a6a |
| SQN      | 9d027759 5ffc                       |
| AMF      | 725c                                |
| OP       | dbc59adc b6f9a0ef 735477b7 fadf8374 |
| OPc      | 1006020f 0a478bf6 b699f15c 062e42b3 |
| f1       | 9cab3e9 9baf7281                    |
| f1*      | 95814ba2 b3044324                   |
| f2       | 8011c48c 0c214ed2                   |
| f5       | 33484dc2 136b                       |
| f3       | 5dbdbb29 54e8f3cd e665b046 179a5098 |
| f4       | 59a92d3b 476a0443 487055cf 88b2307b |
| f5*      | deacdd84 8cc6                       |

### 4.3.4 Test Set 4

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 9e5944ae a94b8116 5c82fbf9 f32db751 |
| RAND     | ce83dbc5 4ac0274a 157c17f8 0d017bd6 |
| SQN      | 0b604a81 eca8                       |
| AMF      | 9e09                                |
| OP       | 223014c5 806694c0 07ca1eee f57f004f |
| OPc      | a64a507a e1a2a98b b88eb421 0135dc87 |
| f1       | 74a58220 cba84c49                   |
| f1*      | ac2cc74a 96871837                   |
| f2       | f365cd68 3cd92e96                   |
| f5       | f0b9c08a d02e                       |
| f3       | e203edb3 971574f5 a94b0d61 b816345d |
| f4       | 0c4524ad eac041c4 dd830d20 854fc46b |
| f5*      | 6085a86c 6f63                       |

### 4.3.5 Test Set 5

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 4ab1deb0 5ca6ceb0 51fc98e7 7d026a84 |
| RAND     | 74b0cd60 31a1c833 9b2b6ce2 b8c4a186 |
| SQN      | e880a1b5 80b6                       |
| AMF      | 9f07                                |
| OP       | 2d16c5cd 1fdf6b22 383584e3 bef2a8d8 |
| OPc      | dcf07cbd 51855290 b92a07a9 891e523e |
| f1       | 49e785dd 12626ef2                   |
| f1*      | 9e857903 36bb3fa2                   |
| f2       | 5860fc1b ce351e7e                   |
| f5       | 31e11a60 9118                       |
| f3       | 7657766b 373d1c21 38f307e3 de9242f9 |
| f4       | 1c42e960 d89b8fa9 9f2744e0 708ccb53 |
| f5*      | fe2555e5 4aa9                       |

### 4.3.6 Test Set 6

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 6c38a116 ac280c45 4f59332e e35c8c4f |
| RAND     | ee6466bc 96202c5a 557abbef f8babf63 |
| SQN      | 414b9822 2181                       |
| AMF      | 4464                                |
| OP       | 1ba00a1a 7c6700ac 8c3ff3e9 6ad08725 |
| OPc      | 3803ef53 63b947c6 aaa225e5 8fae3934 |
| f1       | 078adf84 88241a57                   |
| f1*      | 80246b8d 0186bcf1                   |
| f2       | 16c8233f 05a0ac28                   |
| f5       | 45b0f69a b06c                       |
| f3       | 3f8c7587 fe8e4b23 3af676ae de30ba3b |
| f4       | a7466cc1 e6b2a133 7d49d3b6 6e95d7b4 |
| f5*      | 1f53cd2b 1113                       |

### 4.3.7 Test Set 7

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 2d609d4d b0ac5bf0 d2c0de26 7014de0d |
| RAND     | 194aa756 013896b7 4b4a2a3b 0af4539e |
| SQN      | 6bf69438 c2e4                       |
| AMF      | 5f67                                |
| OP       | 460a4838 5427aa39 264aac8e fc9e73e8 |
| OPc      | c35a0ab0 bcbfc925 2caff15f 24efbde0 |
| f1       | bd07d300 3b9e5cc3                   |
| f1*      | bcb6c2fc ad152250                   |
| f2       | 8c25a16c d918a1df                   |
| f5       | 7e6455f3 4cf3                       |
| f3       | 4cd08460 20f8fa07 31dd47cb dc6be411 |
| f4       | 88ab80a4 15f15c73 711254a1 d388f696 |
| f5*      | dc6dd01e 8f15                       |

### 4.3.8 Test Set 8

| Variable | Value                               |
|----------|-------------------------------------|
| K        | a530a7fe 428fad10 82c45edd fce13884 |
| RAND     | 3a4c2b32 45c50eb5 c71d0863 9395764d |
| SQN      | f63f5d76 8784                       |
| AMF      | b90e                                |
| OP       | 511c6c4e 83e38c89 b1c5d8dd e62426fa |
| OPc      | 27953e49 bc8af6dc c6e730eb 80286be3 |
| f1       | 53761fbd 679b0bad                   |
| f1*      | 21adfd33 4a10e7ce                   |
| f2       | a63241e1 ffc3e5ab                   |
| f5       | 88196c47 986f                       |
| f3       | 10f05bab 75a99a5f bb98a9c2 87679c3b |
| f4       | f9ec0865 eb32f223 69cade40 c59c3a44 |
| f5*      | c987a3d2 3115                       |

### 4.3.9 Test Set 9

| Variable | Value                               |
|----------|-------------------------------------|
| K        | d9151cf0 4896e258 30bf2e08 267b8360 |
| RAND     | f761e5e9 3d603feb 730e2755 6cb8a2ca |
| SQN      | 47ee0199 820a                       |
| AMF      | 9113                                |
| OP       | 75fc2233 a44294ee 8e6de25c 4353d26b |
| OPc      | c4c93eff e8a08138 c203d4c2 7ce4e3d9 |
| f1       | 66cc4be4 4862af1f                   |
| f1*      | 7a4b8d7a 8753f246                   |
| f2       | 4a90b217 1ac83a76                   |
| f5       | 82a0f528 7a71                       |
| f3       | 71236b71 29f9b22a b77ea7a5 4c96da22 |
| f4       | 90527eba a5588968 db417273 25a04d9e |
| f5*      | 527dbf41 f35f                       |

### 4.3.10 Test Set 10

| Variable | Value                               |
|----------|-------------------------------------|
| K        | a0e2971b 6822e8d3 54a18cc2 35624ecb |
| RAND     | 08eff828 b13fdb56 2722c65c 7f30a9b2 |
| SQN      | db5c0664 81e0                       |
| AMF      | 716b                                |
| OP       | 323792fa ca21fb4d 5d6f13c1 45a9d2c1 |
| OPc      | 82a26f22 bba9e948 8f949a10 d98e9cc4 |
| f1       | 9485fe24 621cb9f6                   |
| f1*      | bce325ce 03e2e9b9                   |
| f2       | 4bc2212d 8624910a                   |
| f5       | a2f858aa 9e5d                       |
| f3       | 08cef6d0 04ec6147 1a3c3cda 048137fa |
| f4       | ed0318ca 5deb9206 272f6e8f a64ba411 |
| f5*      | 74e76fbb ec38                       |

### 4.3.11 Test Set 11

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 0da6f7ba 86d5eac8 a19cf563 ac58642d |
| RAND     | 679ac4db acd7d233 ff9d6806 f4149ce3 |
| SQN      | 6e2331d6 92ad                       |
| AMF      | 224a                                |
| OP       | 4b9a26fa 459e3acb ff36f401 5de3bdc1 |
| OPc      | 0db1071f 8767562c a43a0a64 c41e8d08 |
| f1       | 2831d7ae 9088e492                   |
| f1*      | 9b2e1695 1135d523                   |
| f2       | 6fc30fee 6d123523                   |
| f5       | 4c539a26 e1fa                       |
| f3       | 69b1cae7 c7429d97 5e245cac b05a517c |
| f4       | 74f24e8c 26df58e1 b38d7dcd 4f1b7fbd |
| f5*      | 07861e12 6928                       |

### 4.3.12 Test Set 12

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 77b45843 c88e58c1 0d202684 515ed430 |
| RAND     | 4c47eb30 76dc55fe 5106cb20 34b8cd78 |
| SQN      | fe1a8731 005d                       |
| AMF      | ad25                                |
| OP       | bf3286c7 a51409ce 95724d50 3bfe6e70 |
| OPc      | d483afae 562409a3 26b5bb0b 20c4d762 |
| f1       | 08332d7e 9f484570                   |
| f1*      | ed41b734 489d5207                   |
| f2       | aefa357b eac2a87a                   |
| f5       | 30ff25cd adf6                       |
| f3       | 908c43f0 569cb8f7 4bc971e7 06c36c5f |
| f4       | c251df0d 888dd932 9bcf4665 5b226e40 |
| f5*      | e84ed0d4 677e                       |

### 4.3.13 Test Set 13

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 729b1772 9270dd87 ccdflbfe 29b4e9bb |
| RAND     | 311c4c92 9744d675 b720f3b7 e9b1cbd0 |
| SQN      | c85c4cf6 5916                       |
| AMF      | 5bb2                                |
| OP       | d04c9c35 bd2262fa 810d2924 d036fd13 |
| OPc      | 228c2f2f 06ac3268 a9e616ee 16db4ba1 |
| f1       | ff794fe2 f827ebf8                   |
| f1*      | 24fe4dc6 1e874b52                   |
| f2       | 98dbbd09 9b3b408d                   |
| f5       | 5380d158 cfe3                       |
| f3       | 44c0f23c 5493cfd2 41e48f19 7e1d1012 |
| f4       | 0c9fb816 13884c25 35dd0eab f3b440d8 |
| f5*      | 87ac3b55 9fb6                       |

### 4.3.14 Test Set 14

| Variable | Value                               |
|----------|-------------------------------------|
| K        | d32dd23e 89dc6623 54ca12eb 79dd32fa |
| RAND     | cf7d0ab1 d9430695 0bf12018 fbd46887 |
| SQN      | 484107e5 6a43                       |
| AMF      | b5e6                                |
| OP       | fe75905b 9da47d35 6236d031 4e09c32e |
| OPc      | d22a4b41 80a53257 08a5ff70 d9f67ec7 |
| f1       | cf19d62b 6a809866                   |
| f1*      | 5d269537 e45e2ce6                   |
| f2       | af4a411e 1139f2c2                   |
| f5       | 217af492 72ad                       |
| f3       | 5af86b80 edb70df5 292cc112 1cbad50c |
| f4       | 7f4d6ae7 440e1878 9a8b75ad 3f42f03a |
| f5*      | 900e101c 677e                       |

### 4.3.15 Test Set 15

| Variable | Value                               |
|----------|-------------------------------------|
| K        | af7c65e1 927221de 591187a2 c5987a53 |
| RAND     | 1f0f8578 464fd59b 64bed2d0 9436b57a |
| SQN      | 3d627b01 418d                       |
| AMF      | 84f6                                |
| OP       | 0c7acb8d 95b7d4a3 1c5aca6d 26345a88 |
| OPc      | a4cf5c81 55c08a7e ff418e54 43b98e55 |
| f1       | c37cae78 05642032                   |
| f1*      | 68cd09a4 52d8db7c                   |
| f2       | 7bffa5c2 f41fbc05                   |
| f5       | 837fd7b7 4419                       |
| f3       | 3f8c3f3c cf7625bf 77fc94bc fd22fd26 |
| f4       | abcbae8f d46115e9 961a55d0 da5f2078 |
| f5*      | 56e97a60 90b1                       |

### 4.3.16 Test Set 16

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 5bd7ecd3 d3127a41 d12539be d4e7cf71 |
| RAND     | 59b75f14 251c7503 1d0bcbac 1c2c04c7 |
| SQN      | a298ae89 29dc                       |
| AMF      | d056                                |
| OP       | f967f760 38b920a9 cd25e10c 08b49924 |
| OPc      | 76089d3c 0ff3efdc 6e36721d 4fceb747 |
| f1       | c3f25cd9 4309107e                   |
| f1*      | b0c8ba34 3665afcc                   |
| f2       | 7e3f44c7 591f6f45                   |
| f5       | 5be11495 525d                       |
| f3       | d42b2d61 5e49a03a c275a5ae f97af892 |
| f4       | 0b3f8d02 4fe6bfaf aa982b8f 82e319c2 |
| f5*      | 4d6a34a1 e4eb                       |

### 4.3.17 Test Set 17

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 6cd1c6ce ble01e14 f1b82316 a90b7f3d |
| RAND     | f69b78f3 00a0568b ce9f0cb9 3c4be4c9 |
| SQN      | b4fce5fe b059                       |
| AMF      | e4bb                                |
| OP       | 078bfca9 564659ec d8851e84 e6c59b48 |
| OPc      | a219dc37 f1dc7d66 738b5843 c799f206 |
| f1       | 69a90869 c268cb7b                   |
| f1*      | 2e0fdcf9 fd1cfa6a                   |
| f2       | 70f6bdb9 ad21525f                   |
| f5       | 1c408a85 8b3e                       |
| f3       | 6edaf99e 5bd9f85d 5f36d91c 1272fb4b |
| f4       | d61c853c 280dd9c4 6f297bae c386de17 |
| f5*      | aa4ae52d aa30                       |



### 4.3.18 Test Set 18

| Variable | Value                               |
|----------|-------------------------------------|
| K        | b73a90cb cf3afb62 2dba83c5 8a8415df |
| RAND     | b120f1c1 a0102a2f 507dd543 de68281f |
| SQN      | f1e8a523 a36d                       |
| AMF      | 471b                                |
| OP       | b672047e 003bb952 dca6cb8a f0e5b779 |
| OPc      | df0c6786 8fa25f74 8b7044c6 e7c245b8 |
| f1       | ebd70341 bcd415b0                   |
| f1*      | 12359f5d 82220c14                   |
| f2       | 479dd25c 20792d63                   |
| f5       | aefdaa5d dd99                       |
| f3       | 66195dbe d0313274 c5ca7766 615fa25e |
| f4       | 66bec707 eb2afc47 6d7408a8 f2927b36 |
| f5*      | 12ec2b87 fbb1                       |

### 4.3.19 Test Set 19

| Variable | Value                               |
|----------|-------------------------------------|
| K        | 51222502 14c33e72 3a5dd523 fc145fc0 |
| RAND     | 81e92b6c 0ee0e12e bceba8d9 2a99dfa5 |
| SQN      | 16f3b3f7 0fc2                       |
| AMF      | c3ab                                |
| OP       | c9e87632 86b5b9ff bdf56e12 97d0887b |
| OPc      | 981d464c 7c52eb6e 50362349 84ad0bcf |
| f1       | 2a5c23d1 5ee351d5                   |
| f1*      | 62dae385 3f3af9d2                   |
| f2       | 28d7b0f2 a2ec3de5                   |
| f5       | ada15aeb 7bb8                       |
| f3       | 5349fbe0 98649f94 8f5d2e97 3a81c00f |
| f4       | 9744871a d32bf9bb d1dd5ce5 4e3e2e5a |
| f5*      | d461bc15 475d                       |

### 4.3.20 Test Set 20

| Variable | Value                                |
|----------|--------------------------------------|
| K        | 90dca4ed a45b53cf 0f12d7c9 c3bc6a89  |
| RAND     | 9fddc720 92c6ad03 6b6e4647 89315b78  |
| SQN      | 20f813bd 4141                        |
| AMF      | 61df                                 |
| OP       | 3ffcf5e5b 7b111158 9920d352 8e84e655 |
| OPc      | cb9cccc4 b9258e6d ca476037 9fb82581  |
| f1       | 09db94ea b4f8149e                    |
| f1*      | a29468aa 9775b527                    |
| f2       | a95100e2 760952cd                    |
| f5       | 83cfd54d b913                        |
| f3       | b5f2da03 883b69f9 6bf52e02 9ed9ac45  |
| f4       | b4721368 bc16ea67 875c5598 688bb0ef  |
| f5*      | 4f203939 2ddc                        |

## Annex A (informative): Change history

| Change history |            |    |           |               |                                      |
|----------------|------------|----|-----------|---------------|--------------------------------------|
| TSG SA #       | Version    | CR | Tdoc SA   | New Version   | Subject/Comment                      |
| SP-10          | SAGE v 1.0 | -  | SP-010630 | 3.0.0         | Approved as Release 1999             |
| SP-11          | 3.0.0      | -  | -         | 4.0.0         | <a href="#">Updated to Release 4</a> |
| SP-16          | 4.0.0      | -  | -         | 5.0.0         | <a href="#">Updated to Release 5</a> |
| SP-26          | 5.0.0      | -  | -         | 6.0.0         | <a href="#">Updated to Release 6</a> |
| SP-36          | 6.0.0      | -  | -         | 7.0.0         | <a href="#">Updated to Release 7</a> |
| SP-42          | 7.0.0      | -  | -         | 8.0.0         | <a href="#">Updated to Release 8</a> |
| SP-46          | 8.0.0      | -  | -         | 9.0.0         | <a href="#">Updated to Release 9</a> |
| SP-51          | 9.0.0      | -  | -         | 10.0.0        | Updated to Release 10                |
| 2012-09        | -          | -  | -         | 11.0.0        | Update to Rel-11 version (MCC)       |
| 2014-09        | -          | -  | -         | 12.0.0        | Update to Rel-12 version (MCC)       |
| 2016-01        | 12.0.0     | -  | -         | <b>13.0.0</b> | Update to Rel-13 version (MCC)       |

| Change history |         |      |    |     |     |  |               |
|----------------|---------|------|----|-----|-----|--|---------------|
| Date           | Meeting | TDoc | CR | Rev | Cat | Subject/Comment                                  | New version   |
| 2017-03        | SA#75   |      |    |     |     | Promotion to Release 14 without technical change | 14.0.0        |
| 2018-10        | -       | -    | -  | -   | -   | Update to Rel-15 version (MCC)                   | <b>15.0.0</b> |
| 2020-07        | -       | -    | -  | -   | -   | Update to Rel-16 version (MCC)                   | <b>16.0.0</b> |
| 2022-03        | -       | -    | -  | -   | -   | Update to Rel-17 version (MCC)                   | <b>17.0.0</b> |

---

# History

| <b>Document history</b> |            |             |
|-------------------------|------------|-------------|
| V17.0.0                 | April 2022 | Publication |
|                         |            |             |
|                         |            |             |
|                         |            |             |
|                         |            |             |