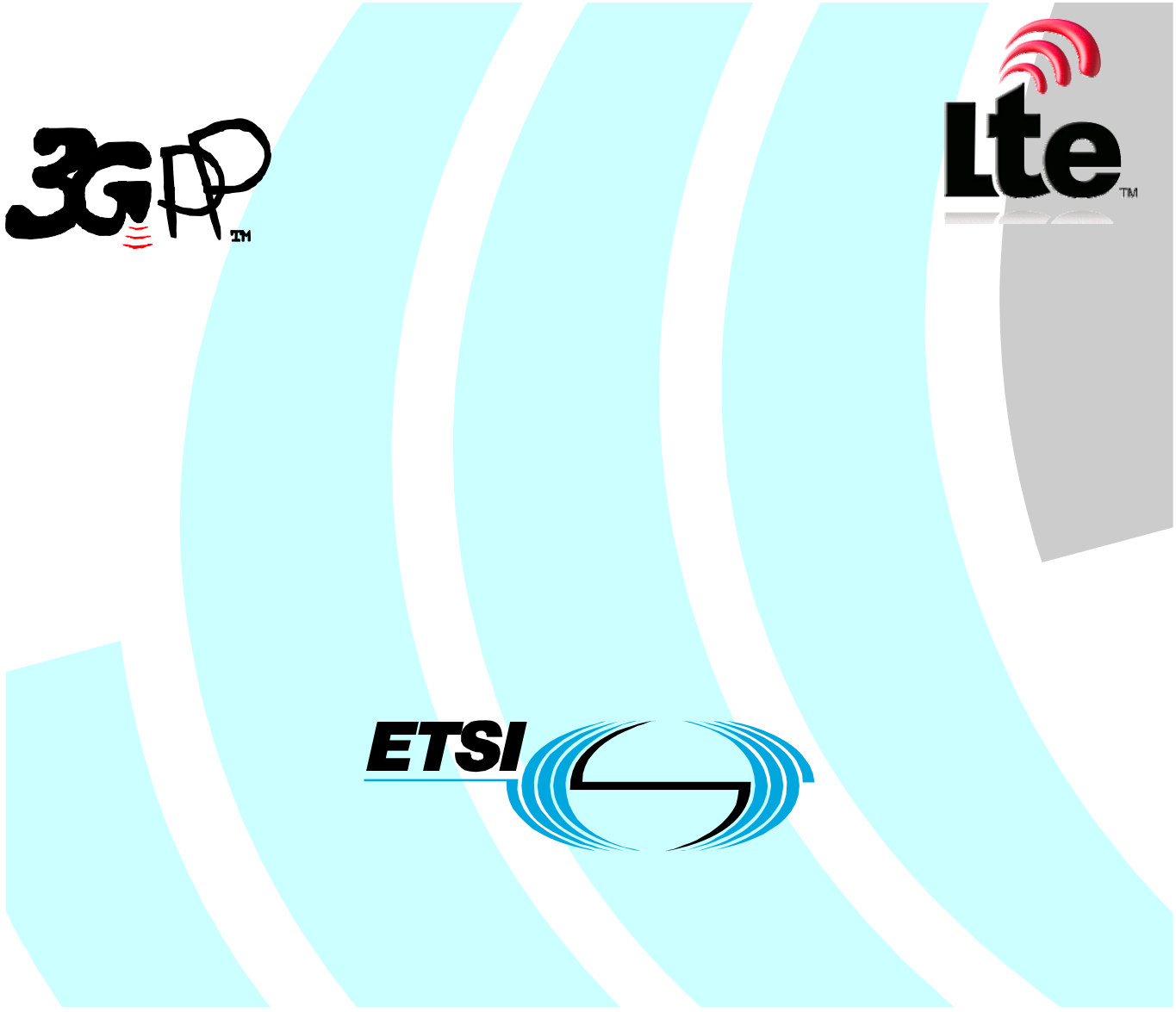
ETSI TS 135 207 V9.0.0 (2010-02)

Technical Specification

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 f1, f1*, f2, f3, f4, f5 and f5*;
Document 3: Implementors' test data
(3GPP TS 35.207 version 9.0.0 Release 9)



Reference
RTS/TSGS-0335207v900

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

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 (http://webapp.etsi.org/IPR/home.asp).

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.

Contents

Foreword

This Technical Specification (TS) 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 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 implementors' test data

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

Section 3 provides test data for the Rijndael kernel function.

Section 4 provides test data for the authentication algorithms *f1* and *f1**.

Section 5 provides test data for the algorithms *f2*, *f5* and *f3*.

Section 6 provides test data for the algorithms *f4* 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" (this document).

[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".

[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.

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_C	a 128-bit value derived from **OP** and **K** 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_{MS}.)

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 *f1* and *f1**

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 ***f1**** this input is more precisely called SQN_{MS}.)
AMF	16	Authentication management field AMF[0]…AMF[15]

Table 2. inputs to *f2*, *f3*, *f4*, *f5* and *f5**

Parameter	Size (bits)	Comment
K	128	Subscriber key K[0]…K[127]
RAND	128	***Random challenge RAND[0]…RAND[127]***

Table 3. *f1* output

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

Table 4. *f1 output**

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

Table 5. *f2* output

Parameter	Size (bits)	Comment
RES	64	Response RES[0]…RES[63]

Table 6. *f3* output

Parameter	Size (bits)	Comment
CK	128	Confidentiality key CK[0]…CK[127]

Table 7. *f4* output

Parameter	Size (bits)	Comment
IK	128	Integrity key IK[0]…IK[127]

Table 8. *f5* output

Parameter	Size (bits)	Comment
AK	48	Anonymity key AK[0]…AK[47]

Table 9. *f5 output**

Parameter	Size (bits)	Comment
AK	48	Resynch anonymity key AK[0]…AK[47]

NOTE: Both f5 and f5* 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

The test data sets for the kernel function Rijndael have been chosen in a way that, provided all data sets are tested:

- Every S-Box entry is being used.
- Each input bit has been in both the '0' and '1' state.

The test data sets for all seven functions are based on the test data sets above. The values for OP, K and RAND have been chosen such that the input values of the first encryption are the test data sets of Rijndael. This way, the following coverage is being reached, provided all test data sets are tested:

- The conditions for Rijndael seen above.
- Each input bit for the functions has been in both the '0' and '1' state.

3 Rijndael test data

3.1 Overview

The test data sets presented here are for the cryptographic kernel function Rijndael with 128-bit key and data as it is specified in [3].

3.2 Format

Rijndael is composed of 10 rounds that transform the input into the output. An intermediate result is called the State. The State can be pictured as a 4x4 rectangular array of bytes (128 bits in total). The cipher key is similarly pictured as a 4x4 rectangular array. In each of the data intermediate values of the round key array and of the State are given. For the first set the value of the State after each step of the algorithm is given. In the remaining data sets only the value of the State as it is at the end of each round is given.

The internal states will be written as hexadecimal strings, column by column and from top to bottom within each column (the same way as plaintext bytes are fed into the matrix).

Example: The State

C2	37	2E	21
3C	69	51	9E
62	EC	9D	23
CC	29	D8	F7

is represented by the string c23c62cc 3769ec29 2e519dd8 219e23f7.

3.3 Test Set 1

```
Key: 465b5ce8 b199b49f aa5f0a2e e238a6bc
Plaintext: ee36f7cf 037d37d3 692f7f03 99e7949a
Round key  0: 465b5ce8 b199b49f aa5f0a2e e238a6bc
Round key  1: 407f3970 f1e68def 5bb987c1 b981217d
Round key  2: 4e82c626 bf644bc9 e4ddcc08 5d5ced75
Round key  3: 00d75b6a bfb310a3 5b6edcab 063231de
Round key  4: 2b104605 94a356a6 cfcd8a0d c9ffbbd3
Round key  5: 2dfa20d8 b959767e 7694fc73 bf6b47a0
Round key  6: 725ac0d0 cb03b6ae bd974add 02fc0d7d
Round key  7: 828d3fa7 498e8909 f419c3d4 f6e5cea9
Round key  8: db06ece5 928865ec 6691a638 90746891
Round key  9: 52436d85 c0cb0869 a65aae51 362ec6c0
Round key 10: 55f7d780 953cdfe9 336671b8 0548b778
add keys(0):     a86dab27 b2e4834c c370752d 7bdf3226
Substitution(1): c23c62cc 3769ec29 2e519dd8 219e23f7
Row shift(1):    c2699df7 375123cc 2e9e6229 213cecd8
mix column(1):   4e5b885c 723c6fa8 ae860fdc 32aead18
add keys(1):     0e24b12c 83dae247 f53f881d 8b2f8c65
Substitution(2): ab36c871 ec5798a0 e675c4a4 3d15644d
Row shift(2):    ab57c44d ec756471 e615c8a0 3d3698a4
mix column(2):   3d1fb8ef 49dbc2dc 802f83b7 1c46d7ba
add keys(2):     739d7ec9 f6bf8915 64f24fbf 411a3acf
Substitution(3): 8f5ef3dd 4208a759 43898408 83a2808a
Row shift(3):    8f08848a 428980dd 43a2f359 835ea708
mix column(3):   13821109 590dac6e d14bf726 50c59077
add keys(3):     13554a63 e6bebccd 8a252b8d 56f7a1a9
Substitution(4): 7dfcd6fb 8eae65bd 7e3ff15d b16832d3
Row shift(4):    7daef1d3 8e3f32fb 7e68d6bd b1fc655d
mix column(4):   31e14465 8f5dc369 2f727d5d 5ea060eb
add keys(4):     1af10260 1bfe95cf e0bff750 975fdb38
Substitution(5): a2a177d0 afbb2a8a e1086853 88cfb907
Row shift(5):    a2bb6807 af08b9d0 e1cf778a 88a12a53
mix column(5):   e670c020 34bfa5e0 6e77458f 8afc88ae
add keys(5):     cb8ae0f8 8de6d39e 18e3b9fc 3597cf0e
Substitution(6): 1f7ee141 5d8e660b ad1156b0 96888aab
Row shift(6):    1f8e56ab 5d118a41 ad88e10b 967e66b0
mix column(6):   4a49dbb4 42bb80fe 2895e193 6370efc2
add keys(6):     38131b64 89b83650 9502ab4e 618ce2bf
Substitution(7): 077daf43 a76c0553 2a77622f ef649808
Row shift(7):    076c6208 a7779843 2a64af53 ef7d052f
mix column(7):   d071b717 17b93e9b 045bfe13 6835e90c
add keys(7):     52fc88b0 5e37b792 f0423dc7 9ed027a5
Substitution(8): 00b0c4e7 589aa94f 8c2c27c6 0b70cc06
Row shift(8):    009a2706 582ccce7 8c70c44f 0bb0a9c6
mix column(8):   9440deb1 efa8c5dd 1874bea5 b256a393
add keys(8):     4f463254 7d20a031 7ee5189d 2222cb02
Substitution(9): 845a2320 ffb7e0c7 f3d9ad5e 93931f77
Row shift(9):    84b7ad77 ffd91f20 f39323c7 935ae05e
mix column(9):   0b6aeb63 aa57789c b76c742b 6d42f0a8
add keys(9):     592986e6 6a9c70f5 1136da7a 5b6c3668
Substitution(10):cba5448e 02de51e6 820557da 39500545
Row shift(10):   cbde5745 0205058e 825044e6 39a551da
add keys(10):    9e2980c5 9739da67 b136355e 3cede6a2
Ciphertext:   9e2980c5 9739da67 b136355e 3cede6a2
```

3.4. Test Set 2

```
Key: 0396eb31 7b6d1c36 f19c1c84 cd6ffd16
Plaintext: 93cc3640 c5d6a521 d81235bd 0882bf0a
Round key  0: 0396eb31 7b6d1c36 f19c1c84 cd6ffd16
Round key  1: aac2ac8c d1afb0ba 2033ac3e ed5c5128
Round key  2: e21398d9 33bc2863 138f845d fed3d575
Round key  3: 80100562 b3ac2d01 a023a95c 5ef07c29
Round key  4: 0400a03a b7ac8d3b 178f2467 497f584e
Round key  5: c66a8f01 71c6023a 6649265d 2f367e13
Round key  6: e399f214 925ff02e f416d673 db20a860
Round key  7: 145b22ad 8604d283 721204f0 a932ac90
Round key  8: b7ca427e 31ce90fd 43dc940d eaee389d
Round key  9: 84cd1cf9 b5038c04 f6df1809 1c312094
Round key 10: 757a3e65 c079b261 36a6aa68 2a978afc
End of Round 0:  905add71 bebbb917 298e2939 c5ed421c
End of round 1:  7605c840 32e4a13b bf94cea5 2775d315
End of round 2:  fb262fc1 7c78fe50 b567e7ef f4991c6f
End of round 3:  7d736610 e36a13d8 7e5d4d65 5db3231a
End of round 4:  a6677d9e ad85d9ed 0f927ff5 6bfcb6f2
End of round 5:  779f0321 d4145989 eb0bfa22 96e1dff5
End of round 6:  cc129610 1c05a8a2 f23ec385 cec8c0e6
End of round 7:  9f3ad732 18f8d6bb f2c1107c b1fad328
End of round 8:  27e20beb bd1aec49 d9f70961 1c2cb788
End of round 9:  3f992786 b9a0f782 1f4e477a ad2089b8
Ciphertext:   009a9e09 96561525 f611667b bf79e226
```

3.5. Test Set 3

```
Key: fec86ba6 eb707ed0 8905757b 1bb44b8f
Plaintext: 8f7a8f0d 108b7f2d 97a53eac c1d958d9
Round key  0: fec86ba6 eb707ed0 8905757b 1bb44b8f
Round key  1: 727b1809 990b66d9 100e13a2 0bba582d
Round key  2: 8411c022 1d1aa6fb 0d14b559 06aeed74
Round key  3: 6444524d 795ef4b6 744a41ef 72e4ac9b
Round key  4: 05d5460d 7c8bb2bb 08c1f354 7a255fcf
Round key  5: 2a1accd7 56917e6c 5e508d38 2475d2f7
Round key  6: 97afa4e1 c13eda8d 9f6e57b5 bb1b8542
Round key  7: 7838880b b9065286 26680533 9d738071
Round key  8: 77f52b55 cef379d3 e89b7ce0 75e8fc91
Round key  9: f745aac8 39b6d31b d12daffb a4c5536a
Round key 10: 67a8a881 5e1e7b9a 8f33d461 2bf6870b
End of Round 0:  71b2e4ab fbfb01fd 1ea04bd7 da6d1356
End of round 1:  3cb90132 a33ad591 8deb73c9 8e09d283
End of round 2:  b18781c8 bf3e51ff 494e89da 10c3d8ab
End of round 3:  e763dbdf 9143322b 6a2f76ac 423f31b6
End of round 4:  6e736a14 03ec0ad6 db08e567 8610665a
End of round 5:  21cced1d 3925460d 8696fbd7 c41843c2
End of round 6:  1d181787 f09d9b62 79437634 0a71746b
End of round 7:  8e178364 1104c2af f5220eee b3714a51
End of round 8:  3224e59e ea6e1a8d 5476716c a93953a3
End of round 9:  a2b75585 8266b04a 2304d3ea b1d71930
Ciphertext:   5d9bce85 4decaf0d a93d28b7 e35f608c
```

3.6 Test Set 4

```
Key: 9e5944ae a94b8116 5c82fbf9 f32db751
Plaintext: 68c98bbf ab628ec1 adf2a3d9 0c34a751
Round key  0: 9e5944ae a94b8116 5c82fbf9 f32db751
Round key  1: 47f095a3 eebb14b5 b239ef4c 4114581d
Round key  2: bf9a3120 51212595 e318cad9 a20c92c4
Round key  3: 45d52d1a 14f4088f f7ecc256 55e05092
Round key  4: ac8662e6 b8726a69 4f9ea83f 1a7ef8ad
Round key  5: 4fc7f744 f7b59d2d b82b3512 a255cdbf
Round key  6: 937aff7e 64cf6253 dce45741 7eb19afe
Round key  7: 1bc2448d 7f0d26de a3e9719f dd58eb61
Round key  8: f12bab4c 8e268d92 2dcffc0d f097176c
Round key  9: 62dbfbc0 ecfd7652 c1328a5f 31a59d33
Round key 10: 52853807 be784e55 7f4ac40a 4eef5939
End of Round 0:  f690cf11 02290fd7 f1705820 ff191000
End of round 1:  3e3e036c bba920a8 08a087f6 0cef0044
End of round 2:  a2b7531f 96e51993 40c28eb2 7d0d6d5c
End of round 3:  12272200 bcaa9ea6 b6a0a2d4 b306ec9b
End of round 4:  e4564f18 e4e6cd2e d584d859 ccc5974d
End of round 5:  96e9eccd e14c4c00 fad9d057 8a7010e3
End of round 6:  b23995ae a7a5fcde d841096f d2d345fd
End of round 7:  2aae8b7b d31a1204 fc27054a 82aad44c
End of round 8:  9f0541e3 643ad4fe 768997a8 fec108c3
End of round 9:  f2b6d9e2 b9aac122 01df0181 6bd28059
Ciphertext:  db2944cc e8e683cd 03fff199 31a12135
```

3.7 Test Set 5

```
Key: 4ab1deb0 5ca6ceb0 51fc98e7 7d026a84
Plaintext: a840b1dd 60249aa3 22016b4b 31daf3b8
Round key  0: 4ab1deb0 5ca6ceb0 51fc98e7 7d026a84
Round key  1: 3cb3814f 60154fff 31e9d718 4cebbd9c
Round key  2: d7c95f66 b7dc1099 8635c781 cade7a1d
Round key  3: ce13fb12 79cfeb8b fffa2c0a 35245617
Round key  4: f0a20b84 896de00f 7697cc05 43b39a12
Round key  5: 8d1ac29e 04772291 72e0ee94 31537486
Round key  6: 40888659 44ffa4c8 361f4a5c 074c3eda
Round key  7: 293ad19c 6dc57554 5bda3f08 5c9601d2
Round key  8: 394664d6 54831182 0f592e8a 53cf2f58
Round key  9: a8530e3b fcd01fb9 f3893133 a0461e6b
Round key 10: c42171db 38f16e62 cb785f51 6b3e413a
End of Round 0:  e2f16f6d 3c825413 73fdf3ac 4cd8993c
End of round 1:  c4f1362f 8343731b 423af5a1 576add5f
End of round 2:  e81fc43b 3b66dadd 72bd09b7 3964d3ba
End of round 3:  43195665 ac918275 67d94f0c b4fdcaff
End of round 4:  ce20b983 d6477b7c b7efd855 c846fcbe
End of round 5:  b4c7c29e d5035f3c 93178158 e55176d0
End of round 6:  b097f842 7a443a13 33fe2b1a 5a221a77
End of round 7:  d516d0b5 9aa33f60 549a6a7e 9a1ad15c
End of round 8:  691db74f 07c70966 12662783 77953444
End of round 9:  c7699f17 a4df4ed5 9ec7ce96 4b0f6209
Ciphertext:  02bffada 7137c492 c00e8452 d8c76eaa
```

3.8 Test Set 6

```
Key: 6c38a116 ac280c45 4f59332e e35c8c4f
Plaintext: d66789ef f5996b9c ffd89e0a 77148657
Round key  0: 6c38a116 ac280c45 4f59332e e35c8c4f
Round key  1: 275c2507 8b742942 c42d1a6c 27719623
Round key  2: 86cc03cb 0db82a89 c99530e5 eee4a6c6
Round key  3: ebe8b7e3 e6509d6a 2fc5ad8f c1210b49
Round key  4: 1ec38c9b f89311f1 d756bc7e 1677b737
Round key  5: fb6a16dc 03f9072d d4afbb53 c2d80c64
Round key  6: ba9455f9 b96d52d4 6dc2e987 af1ae5e3
Round key  7: 584d4480 e1201654 8ce2ffd3 23f81a30
Round key  8: 99ef40a6 78cf56f2 f42da921 d7d5b311
Round key  9: 8182c2a8 f94d945a 0d603d7b dab58e6a
Round key 10: 629bc0ff 9bd654a5 96b669de 4c03e7b4
End of Round 0:  ba5f28f9 59b167d9 b081ad24 94480a18
End of round 1:  af2ac41c ec979046 e6079852 9a743063
End of round 2:  4a8f6863 46779622 255afa56 d12d3b90
End of round 3:  15d86e9a 92abb035 f40d6e6e 09e3b591
End of round 4:  14650a94 69b5eb49 88e7961d cf19b897
End of round 5:  68028187 03a5d481 7c4a28c1 574cf516
End of round 6:  49c6b78a df871147 3698dc8a b00fd1c1
End of round 7:  e9b1f7ac 4c0e3069 154b3e58 cd8fd4c8
End of round 8:  1999a956 3dd2f44b 42d34338 9b8570d5
End of round 9:  ef0a9266 fde4bf7d 97a4f536 63bb1809
Ciphertext:  bdf226fe cf9ff996 1e5c2621 b764efb1
```

4 Authentication algorithms *f1* AND *f1**

4.1 Overview

The test data sets presented here are for the authentication algorithms *f1, f1**. No detailed data of the internal states of Rijndael are presented here as these are covered in chapter 3.

4.2 Format

Each test starts by showing the various inputs (K, RAND, SQN, AMF) to the functions. This will be followed by the configuration field OP. Thereafter a table is shown with various intermediate values described in the left column. The value OP_C in the second row should not be computed on but off the USIM. In the example code OP_C is computed inside the functions, so it was included in the table.

4.3 Test Set 1

```
K:    465b5ce8 b199b49f aa5f0a2e e238a6bc
RAND: 23553cbe 9637a89d 218ae64d ae47bf35
SQN:  ff9bb4d0 b607
AMF:  b9b9
OP:   cdc202d5 123e20f6 2b6d676a c72cb318
```

SQN,AMF expanded to 128 bits	***ff9bb4d0 b607b9b9 ff9bb4d0 b607b9b9***
OP_C	cd63cb71 954a9f4e 48a5994e 37a02baf
Value after 1st encryption	9e2980c5 9739da67 b136355e 3cede6a2
(SQN,AMF) XOR OP_C, rotated	b73e2d9e 81a79216 32f87fa1 234d26f7
Input to 2nd encryption	2917ad5b 169e4871 83ce4aff 1fa0c055
Output of 2nd encryption	87fc31b2 c19530fd 496a36d0 f3485a46
Value of *f1*	4a9ffac3 54dfafb3
Value of *f1**	01cfaf9e c4e871e9

4.4 Test Set 2

```
K:    0396eb31 7b6d1c36 f19c1c84 cd6ffd16
RAND: c00d6031 03dcee52 c4478119 494202e8
SQN:  fd8eef40 df7d
AMF:  af17
OP:   ff53bade 17df5d4e 793073ce 9d7579fa
```

SQN,AMF expanded to 128 bits	***fd8eef40 df7daf17 fd8eef40 df7daf17***
OP_C	53c15671 c60a4b73 1c55b4a4 41c0bde2
Value after 1st encryption	009a9e09 96561525 f611667b bf79e226
(SQN,AMF) XOR OP_C, rotated	e1db5be4 9ebd12f5 ae4fb931 1977e464
Input to 2nd encryption	e141c5ed 08eb07d0 585edf4a a60e0642
Output of 2nd encryption	0e34e569 c1e813c3 b495a241 5f341ea1
Value of *f1*	5df5b318 07e258b0
Value of *f1**	a8c016e5 1ef4a343

4.5 Test Set 3

```
K:    fec86ba6 eb707ed0 8905757b 1bb44b8f
RAND: 9f7c8d02 1accf4db 213ccff0 c7f71a6a
SQN:  9d027759 5ffc
AMF:  725c
OP:   dbc59adc b6f9a0ef 735477b7 fadf8374
```

SQN,AMF expanded to 128 bits	***9d027759 5ffc725c 9d027759 5ffc725c***
OP_C	1006020f 0a478bf6 b699f15c 062e42b3
Value after 1st encryption	5d9bce85 4decaf0d a93d28b7 e35f608c
(SQN,AMF) XOR OP_C, rotated	2b9b8605 59d230ef 8d047556 55bbf9aa
Input to 2nd encryption	76004880 143e9fe2 24395de1 b6e49926
Output of 2nd encryption	8cadc1e6 91e8f977 2318bafe b52a0197
Value of *f1*	9cabc3e9 9baf7281
Value of *f1**	95814ba2 b3044324

4.6 Test Set 4

```
K:    9e5944ae a94b8116 5c82fbf9 f32db751
RAND: ce83dbc5 4ac0274a 157c17f8 0d017bd6
SQN:  0b604a81 eca8
AMF:  9e09
OP:   223014c5 806694c0 07ca1eee f57f004f
```

SQN,AMF expanded to 128 bits	***0b604a81 eca89e09 0b604a81 eca89e09***
OP_C	a64a507a e1a2a98b b88eb421 0135dc87
Value after 1st encryption	db2944cc e8e683cd 03fff199 31a12135
(SQN,AMF) XOR OP_C, rotated	b3eefea0 ed9d428e ad2a1afb 0d0a3782
Input to 2nd encryption	68c7ba6c 057bc143 aed5eb62 3cab16b7
Output of 2nd encryption	d2efd25a 2a0ae5c2 14a2736b 97b2c4b0
Value of *f1*	74a58220 cba84c49
Value of *f1**	ac2cc74a 96871837

4.7 Test Set 5

```
K:    4ab1deb0 5ca6ceb0 51fc98e7 7d026a84
RAND: 74b0cd60 31a1c833 9b2b6ce2 b8c4a186
SQN:  e880a1b5 80b6
AMF:  9f07
OP:   2d16c5cd 1fdf6b22 383584e3 bef2a8d8
```

SQN,AMF expanded to 128 bits	***e880a1b5 80b69f07 e880a1b5 80b69f07***
OP_C	dcf07cbd 51855290 b92a07a9 891e523e
Value after 1st encryption	02bffada 7137c492 c00e8452 d8c76eaa
(SQN,AMF) XOR OP_C, rotated	51aaa61c 09a8cd39 3470dd08 d133cd97
Input to 2nd encryption	53155cc6 789f09ab f47e595a 09f4a33d
Output of 2nd encryption	9517f960 43e73c62 27af7eaa bfa56d9c
Value of *f1*	49e785dd 12626ef2
Value of *f1**	9e857903 36bb3fa2

4.8 Test Set 6

```
K:    6c38a116 ac280c45 4f59332e e35c8c4f
RAND: ee6466bc 96202c5a 557abbef f8babf63
SQN:  414b9822 2181
AMF:  4464
OP:   1ba00a1a 7c6700ac 8c3ff3e9 6ad08725
```

SQN,AMF expanded to 128 bits	***414b9822 21814464 414b9822 21814464***
OP_C	3803ef53 63b947c6 aaa225e5 8fae3934
Value after 1st encryption	bdf226fe cf9ff996 1e5c2621 b764efb1
(SQN,AMF) XOR OP_C, rotated	ebe9bdc7 ae2f7d50 79487771 423803a2
Input to 2nd encryption	561b9b39 61b084c6 67145150 f55cec13
Output of 2nd encryption	3f8930e7 eb9d5d91 2a864e68 8e2885c5
Value of *f1*	078adfb4 88241a57
Value of *f1**	80246b8d 0186bcf1

5 Algorithms *f2, f5* and *f3*

5.1 Overview

The test data sets presented here are for the algorithms *f2, f5* and *f3*. No detailed data of the internal states of Rijndael are presented here as these are covered in chapter 3.

5.2 Format

Each Test starts by showing the inputs K and RAND to the algorithms, followed by the configuration field OP.

Thereafter five rows of data are shown:

Row 1, denoted a, shows the value of OP_C.
Row 2, denoted b, shows the output of the first encryption after XORing the value OP_C.
Row 3, denoted c, shows the input of the second encryption.
Row 4, denoted d, shows the output of the second encryption.
Row 5, denoted e, shows the values of *f2, f5* and *f3*.

The value OP_C in the first row should not be computed on but off the USIM. In the example code OP_C is computed inside the functions, so it was included in the table.

5.3 Test Set 1

K: 465b5ce8 b199b49f aa5f0a2e e238a6bc
RAND: 23553cbe 9637a89d 218ae64d ae47bf35
OP: cdc202d5 123e20f6 2b6d676a c72cb318

	f2 and f5		*f3*
a	cd63cb71 954a9f4e	48a5994e 37a02baf	
b	534a4bb4 02734529	f993ac10 0b4dcd0d	
c	534a4bb4 02734529 f993ac10 0b4dcd0c		02734529 f993ac10 0b4dcd0d 534a4bb6
d	670b5715 163a3350 ede7889b d41a7b10		796862d2 50c1b54b f35540c9 85bbd364
e	a54211d5 e3ba50bf	aa689c64 8370	b40ba9a3 c58b2a05 bbf0d987 b21bf8cb

5.4 Test Set 2

K: 0396eb31 7b6d1c36 f19c1c84 cd6ffd16
RAND: c00d6031 03dcee52 c4478119 494202e8
OP: ff53bade 17df5d4e 793073ce 9d7579fa

	f2 and f5		*f3*
a	53c15671 c60a4b73	1c55b4a4 41c0bde2	
b	535bc878 505c5e56	ea44d2df feb95fc4	
c	535bc878 505c5e56 ea44d2df feb95fc5		505c5e56 ea44d2df feb95fc4 535bc87a
d	97b6d5e8 9978a10d cff39c49 d9469d12		0b05658e bc7ac9df c87196ab 6aa778b4
e	d3a628ed 988620f0	c4778399 5f72	58c433ff 7a7082ac d424220f 2b67c556

5.5 Test Set 3

K: fec86ba6 eb707ed0 8905757b 1bb44b8f
RAND: 9f7c8d02 1accf4db 213ccff0 c7f71a6a
OP: dbc59adc b6f9a0ef 735477b7 fadf8374

	f2 and f5		*f3*
a	1006020f 0a478bf6	b699f15c 062e42b3	
b	4d9dcc8a 47ab24fb	1fa4d9eb e571223f	
c	4d9dcc8a 47ab24fb 1fa4d9eb e571223e		47ab24fb 1fa4d9eb e571223f 4d9dcc88
d	234e4fcd 192cdf7e 368835d0 0a0f0c61		4dbbb926 5eaf783b 50fc411a 11b4122b
e	8011c48c 0c214ed2	33484dc2 136b	5dbdbb29 54e8f3cd e665b046 179a5098

5.6 Test Set 4

K: 9e5944ae a94b8116 5c82fbf9 f32db751
RAND: ce83dbc5 4ac0274a 157c17f8 0d017bd6
OP: 223014c5 806694c0 07ca1eee f57f004f

	f2 and f5		*f3*
a	a64a507a e1a2a98b	b88eb421 0135dc87	
b	7d6314b6 09442a46	bb7145b8 3094fdb2	
c	7d6314b6 09442a46 bb7145b8 3094fdb3		09442a46 bb7145b8 3094fdb2 7d6314b4
d	56f390f0 318c0249 4beb7949 3decf211		4449bdc9 76b7dd7e 11c5b940 b923e8da
e	f365cd68 3cd92e96	f0b9c08a d02e	e203edb3 971574f5 a94b0d61 b816345d

5.7 Test Set 5

K: 4ab1deb0 5ca6ceb0 51fc98e7 7d026a84
RAND: 74b0cd60 31a1c833 9b2b6ce2 b8c4a186
OP: 2d16c5cd 1fdf6b22 383584e3 bef2a8d8

	f2 and f5	*f3*
a	dcf07cbd 51855290	b92a07a9 891e523e
b	de4f8667 20b29602	792483fb 51d93c94
c	de4f8667 20b29602 792483fb 51d93c95	20b29602 792483fb 51d93c94 de4f8665
d	ed1166dd c09d1433 e14afbb2 472b4c40	aaa70ad6 66b84eb1 81d9004a 578c10c7
e	5860fc1b ce351e7e 31e11a60 9118	7657766b 373d1c21 38f307e3 de9242f9

5.8 Test Set 6

```
K:    6c38a116 ac280c45 4f59332e e35c8c4f
RAND: ee6466bc 96202c5a 557abbef f8babf63
OP:   1ba00a1a 7c6700ac 8c3ff3e9 6ad08725
```

	f2 and f5	*f3*
a	3803ef53 63b947c6	aaa225e5 8fae3934
b	85f1c9ad ac26be50	b4fe03c4 38cad685
c	85f1c9ad ac26be50 b4fe03c4 38cad684	ac26be50 b4fe03c4 38cad685 85f1c9af
d	7db319c9 d3d51ccb bc6a06da 8a0e951c	078f9ad4 9d370ce5 9054534b 519e830f
e	16c8233f 05a0ac28 45b0f69a b06c	3f8c7587 fe8e4b23 3af676ae de30ba3b

6 Algorithms *f4* and *f5**

6.1 Overview

The test data sets presented here are for the algorithms *f4* and *f5**. No detailed data of the internal states of Rijndael are presented here as these are covered in chapter 3.

6.2 Format

Each Test starts by showing the inputs K and RAND to the algorithms, followed by the configuration field OP.

Thereafter five rows of data are shown:

Row 1, denoted a, shows the value of OP_C.
Row 2, denoted b, shows the output of the first encryption after XORing the value OP_C.
Row 3, denoted c, shows the input of the second encryption.
Row 4, denoted d, shows the output of the second encryption.
Row 5, denoted e, shows the values of *f4* and *f5**.

The value OP_C in the first row should not be computed on but off the USIM. In the example code OP_C is computed inside the functions, so it was included in the table.

6.3 Test Set 1

```
K:    465b5ce8 b199b49f aa5f0a2e e238a6bc
RAND: 23553cbe 9637a89d 218ae64d ae47bf35
OP:   cdc202d5 123e20f6 2b6d676a c72cb318
```

	f4	*f5**
a	cd63cb71 954a9f4e	48a5994e 37a02baf
b	534a4bb4 02734529	f993ac10 0b4dcd0d
c	f993ac10 0b4dcd0d 534a4bb4 0273452d	0b4dcd0d 534a4bb4 02734529 f993ac18
d	3a0a77a6 c44ed94a 5ad3eb3f 2bcd1fee	887d409d 3171e7ae b1e55195 635d0a6e
e	f769bcd7 51044604 12767271 1c6d3441	451e8bec a43b

6.4 Test Set 2

```
K:    0396eb31 7b6d1c36 f19c1c84 cd6ffd16
RAND: c00d6031 03dcee52 c4478119 494202e8
OP:   ff53bade 17df5d4e 793073ce 9d7579fa
```

	f4	*f5**
a	53c15671 c60a4b73	1c55b4a4 41c0bde2
b	535bc878 505c5e56	ea44d2df feb95fc4
c	ea44d2df feb95fc4 535bc878 505c5e52	feb95fc4 535bc878 505c5e56 ea44d2d7
d	72699788 ef7a61a8 2226302c f8357838	63304f01 a7cb2601 408d9704 046ac887
e	21a8c1f9 29702adb 3e738488 b9f5c5da	30f11970 61c1

6.5 Test Set 3

```
K:    fec86ba6 eb707ed0 8905757b 1bb44b8f
RAND: 9f7c8d02 1accf4db 213ccff0 c7f71a6a
OP:   dbc59adc b6f9a0ef 735477b7 fadf8374
```

	f4	*f5**
a	1006020f 0a478bf6	b699f15c 062e42b3
b	4d9dcc8a 47ab24fb	1fa4d9eb e571223f
c	1fa4d9eb e571223f 4d9dcc8a 47ab24ff	e571223f 4d9dcc8a 47ab24fb 1fa4d9e3
d	49af2f34 4d2d8fb5 fee9a493 8e9c72c8	ceaadf8b 86811f35 71465e88 8475bd38
e	59a92d3b 476a0443 487055cf 88b2307b	deacdd84 8cc6

6.6 Test Set 4

```
K:    9e5944ae a94b8116 5c82fbf9 f32db751
RAND: ce83dbc5 4ac0274a 157c17f8 0d017bd6
OP:   223014c5 806694c0 07ca1eee f57f004f
```

	f4	*f5**
a	a64a507a e1a2a98b	b88eb421 0135dc87
b	7d6314b6 09442a46	bb7145b8 3094fdb2
c	bb7145b8 3094fdb2 7d6314b6 09442a42	3094fdb2 7d6314b6 09442a46 bb7145b0
d	aa0f74d7 0b62e84f 650db901 847a18ec	c6cff816 8ec16553 38d688d7 a64aae30
e	0c4524ad eac041c4 dd830d20 854fc46b	6085a86c 6f63

6.7 Test Set 5

```
K:    4ab1deb0 5ca6ceb0 51fc98e7 7d026a84
RAND: 74b0cd60 31a1c833 9b2b6ce2 b8c4a186
OP:   2d16c5cd 1fdf6b22 383584e3 bef2a8d8
```

	f4	*f5**
a	dcf07cbd 51855290	b92a07a9 891e523e
b	de4f8667 20b29602	792483fb 51d93c94
c	792483fb 51d93c94 de4f8667 20b29606	51d93c94 de4f8667 20b29602 792483f3
d	c0b295dd 891edd39 260d4349 f992996d	22d52958 1b2c5255 c399f91e 11dff7d5
e	1c42e960 d89b8fa9 9f2744e0 708ccb53	fe2555e5 4aa9

6.8 Test Set 6

```
K:    6c38a116 ac280c45 4f59332e e35c8c4f
RAND: ee6466bc 96202c5a 557abbef f8babf63
OP:   1ba00a1a 7c6700ac 8c3ff3e9 6ad08725
```

	f4	*f5**
a	3803ef53 63b947c6 aaa225e5 8fae3934	
b	85f1c9ad ac26be50 b4fe03c4 38cad685	
c	b4fe03c4 38cad685 85f1c9ad ac26be54	38cad685 85f1c9ad ac26be50 b4fe03cc
d	9f458392 850be6f5 d7ebf653 e13bee80	27502278 72aa1db7 919ff0c7 b0c849cf
e	a7466cc1 e6b2a133 7d49d3b6 6e95d7b4	1f53cd2b 1113

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	Updated to Release 4
SP-16	4.0.0	-	-	5.0.0	Updated to Release 5
SP-26	5.0.0	-	-	6.0.0	Updated to Release 6
SP-36	6.0.0	-	-	7.0.0	Updated to Release 7
SP-42	7.0.0	-	-	8.0.0	Updated to Release 8
SP-46	8.0.0	-	-	9.0.0	Updated to Release 9

History

Document history		
V9.0.0	February 2010	Publication