ETSI TS 155 205 V15.0.0 (2018-11)

Digital cellular telecommunications system (Phase 2+) (GSM); Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8
(3GPP TS 55.205 version 15.0.0 Release 15)

Reference
RTS/TSGS-0355205vf00

Keywords
GSM,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This document has been prepared by the 3GPP Task Force, and contains an example set of algorithms which may be used as the GSM authentication and key generation functions A3 and A8. (It is not mandatory that the particular algorithms specified in this document are used - the A3 and A8 functions are operator-specifiable rather than being fully standardised).

1 Scope

The present document contains an example set of algorithms which may be used as the GSM authentication and key generation functions A3 and A8. (It is not mandatory that the particular algorithms specified in this document are used - the A3 and A8 functions are operator-specifiable rather than being fully standardised).

Section 3 (normative) introduces the algorithms and describes their input and output parameters. Section 4 (normative) defines the algorithms. Section 5 (informative) describes an alternative algorithm that some operators may prefer. Section 6 (informative) provides test data.

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 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".

[2] 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".

[3] 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".

[4] 3GPP TS 33.102 version 3.10.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 1999)".

[5] 3GPP TS 03.20 version 8.1.0: "3rd Generation Partnership Project; Digital cellular telecommunications system (Phase 2+); Security related network functions (Release 1999)".

3 Introductory information (normative)

3.1 Introduction

Within the security architecture of the GSM system there are security functions A3 and A8. The operation of these functions falls completely within the domain of an individual operator, and the functions are therefore to be specified by each operator rather than being fully standardised. 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 the two functions are defined in section 3.2.

3.2 Algorithm Inputs and Outputs

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

Table 1: Inputs to A3 and A8

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

Table 2: A3 output

Parameter	Size (bits)	Comment
SRES	32	Signed response SRES[0]…SRES[31]

Table 3: A8 output

Parameter	Size (bits)	Comment
K_C	64	Cipher key $K_C[0]…K_C[63]$

3.3 Notation

3.3.1 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. When a variable, with bit length L, is shown in hexadecimal format, bit 0 is the most significant bit of the leftmost hexadecimal digit, and bit L-1 is the least significant bit of the rightmost hexadecimal digit.

3.3.2 List of Symbols

=	The assignment operator.
||	The concatenation of the two operands.
⊕	The bitwise exclusive-OR operation.
X[i]	The i^{th} bit of the variable **X**. (**X = X[0] || X[1] || X[2] || …..**).

4 The GSM-MILENAGE algorithms (normative)

An example algorithm set for UMTS, called MILENAGE (note 1), is specified in [1]. GSM-MILENAGE makes use of MILENAGE.

Specifically, the functions from the UMTS MILENAGE which we make use of are the following (we prefix all input and output names by "MIL3G-" to distinguish them clearly from the inputs and outputs of A3 and A8):

Function	Inputs	Output
f2	MIL3G-K[0]…MIL3G-K[127]	MIL3G-RES[0]…MIL3G-RES[63]
f3	MIL3G-RAND[0]…MIL3G-RAND[127]	MIL3G-CK[0]…MIL3G-CK[127]
f4		MIL3G-IK[0]…MIL3G-IK[127]

The GSM-MILENAGE functions are defined as follows:

- Let (MIL3G-K[0]…MIL3G-K[127]) = ($K_i[0]…K_i[127]$)
- Let (MIL3G-RAND[0]…MIL3G-RAND[127]) = (RAND[0]…RAND[127])

- Compute MIL3G-RES, MIL3G-CK and MIL3G-IK from MIL3G-K and MIL3G-RAND, using the MILENAGE functions ***f2, f3,*** and ***f4*** respectively

- Set (K_C[0]…K_C[63]) = (MIL3G-CK[0]…MIL3G-CK[63]) ⊕
  (MIL3G-CK[64]…MIL3G-CK[127]) ⊕
  (MIL3G-IK[0]…MIL3G-IK[63]) ⊕
  (MIL3G-IK[64]…MIL3G-IK[127])

- Derive SRES from MIL3G-RES using an operator-selected **SRES Derivation Function**. This function must be precisely specified for the GSM-MILENAGE A3 algorithm to be fully defined. The two main recommended options are as follows (note 2):

  - Recommended SRES Derivation Function #1:
    (SRES[0]…SRES[31]) = (MIL3G-RES[0]…MIL3G-RES[31]) ⊕ (MIL3G-RES[32]…MIL3G-RES[63]).

  - Recommended SRES Derivation Function #2:
    (SRES[0]…SRES[31]) = (MIL3G-RES[0]…MIL3G-RES[31]).

Alternative SRES Derivation Functions may be specified.

NOTE 1: MILENAGE uses a 128-bit operator-specific constant **OP**; a value has to be assigned to this constant for MILENAGE to be fully specified.

NOTE 2: The 3GPP standard conversion function to derive a GSM SRES of 32 bits from a UMTS XRES of up to 128 bits is as follows [4]:
SRES = XRES*1 xor XRES*2 xor XRES*3 xor XRES*4, where XRES* is 16 octets long and XRES* = XRES if XRES is 16 octets long and XRES* = XRES || 0...0 if XRES is shorter than 16 octets, XRES*i are all 4 octets long and XRES* = XRES*1 || XRES*2 || XRES*3 || XRES*4

Recommended SRES Derivation Function #1 is the result of applying this standard conversion function to a 64-bit XRES equal to MIL3G-RES[0]…MIL3G-RES[63] from MILENAGE. Recommended SRES Derivation Function #2 is the result of applying this standard conversion function to a 32-bit XRES equal to MIL3G-RES[0]…MIL3G-RES[31] from MILENAGE.

5 An alternative algorithm (informative)

The GSM-MILENAGE algorithms defined in section 3 are obtained by applying standard 3G-to-2G conversion functions defined in [4] to the outputs of the UMTS MILENAGE algorithms.

If there is no desire to retain this compatibility with UMTS MILENAGE used in its 2G mode, a much simpler and more efficient algorithm would be to set TEMP = E_{K_i} (RAND), where E is the 128-bit block cipher used as a basic building block in MILENAGE, i.e. TEMP = the result of encrypting RAND using the key K_i; then choose non-overlapping substrings of TEMP to be SRES and K_C, e.g. SRES = TEMP[0]...TEMP[31] and K_C = TEMP[64]…TEMP[127].

This alternative does *not* form any part of the GSM-MILENAGE algorithms; it is included just for information.

6 Test data for GSM-MILENAGE (informative)

6.1 Introduction

The test data sets presented here are derived directly from the MILENAGE test sets in [3].

6.2 Format

The format of each test data set is as follows:

Test Set *n*	
Ki	subscriber secret key
RAND	random challenge
OP	operator-specific MILENAGE constant
OPc	derived from OP and Ki — see [1]
MIL3G-RES	MILENAGE ***f2*** output, included for information only
SRES#1	A3 output SRES, if Recommended SRES Derivation Function #1 is used — see section 4, page 7
SRES#2	A3 output SRES, if Recommended SRES Derivation Function #2 is used — see section 4, page 7
MIL3G-CK	MILENAGE ***f3*** output, included for information only
MIL3G-IK	MILENAGE ***f4*** output, included for information only
Kc	A8 output (cipher key)

All test data in this tabular format is shown in hexadecimal representation. The first test set is also shown in binary, to show explicitly the relationship between the binary data and the hexadecimal representation.

6.3 Test Sets

Test Set 1 in binary format	
Ki	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
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
MIL3G-RES	10100101 01000010 00010001 11010101 11100011 10111010 01010000 10111111
SRES#1	01000110 11111000 01000001 01101010
SRES#2	10100101 01000010 00010001 11010101
MIL3G-CK	10110100 00001011 10101001 10100011 11000101 10001011 00101010 00000101 10111011 11110000 11011001 10000111 10110010 00011011 11111000 11001011
MIL3G-IK	11110111 01101001 10111100 11010111 01010001 00000100 01000110 00000100 00010010 01110110 01110010 01110001 00011100 01101101 00110100 01000001
Kc	11101010 11100100 10111110 10000010 00111010 11111001 10100000 10001011

Test Set 1				
Ki	465b5ce8	b199b49f	aa5f0a2e	e238a6bc
RAND	23553cbe	9637a89d	218ae64d	ae47bf35
OP	cdc202d5	123e20f6	2b6d676a	c72cb318
OPc	cd63cb71	954a9f4e	48a5994e	37a02baf
MIL3G-RES	a54211d5	e3ba50bf		
SRES#1	46f8416a			
SRES#2	a54211d5			
MIL3G-CK	b40ba9a3	c58b2a05	bbf0d987	b21bf8cb
MIL3G-IK	f769bcd7	51044604	12767271	1c6d3441
Kc	eae4be82	3af9a08b		

Test Set 2				
Ki	fec86ba6	eb707ed0	8905757b	1bb44b8f
RAND	9f7c8d02	1accf4db	213ccff0	c7f71a6a
OP	dbc59adc	b6f9a0ef	735477b7	fadf8374
OPc	1006020f	0a478bf6	b699f15c	062e42b3
MIL3G-RES	8011c48c	0c214ed2		
SRES#1	8c308a5e			
SRES#2	8011c48c			
MIL3G-CK	5dbdbb29	54e8f3cd	e665b046	179a5098
MIL3G-IK	59a92d3b	476a0443	487055cf	88b2307b
Kc	aa01739b	8caa976d		

Test Set 3				
Ki	9e5944ae	a94b8116	5c82fbf9	f32db751
RAND	ce83dbc5	4ac0274a	157c17f8	0d017bd6
OP	223014c5	806694c0	07ca1eee	f57f004f
OPc	a64a507a	e1a2a98b	b88eb421	0135dc87
MIL3G-RES	f365cd68	3cd92e96		
SRES#1	cfbce3fe			
SRES#2	f365cd68			
MIL3G-CK	e203edb3	971574f5	a94b0d61	b816345d
MIL3G-IK	0c4524ad	eac041c4	dd830d20	854fc46b
Kc	9a8ec95f	408cc507		

Test Set 4				
Ki	4ab1deb0	5ca6ceb0	51fc98e7	7d026a84
RAND	74b0cd60	31a1c833	9b2b6ce2	b8c4a186
OP	2d16c5cd	1fdf6b22	383584e3	bef2a8d8
OPc	dcf07cbd	51855290	b92a07a9	891e523e
MIL3G-RES	5860fc1b	ce351e7e		
SRES#1	9655e265			
SRES#2	5860fc1b			
MIL3G-CK	7657766b	373d1c21	38f307e3	de9242f9
MIL3G-IK	1c42e960	d89b8fa9	9f2744e0	708ccb53
Kc	cdc1dc08	41b81a22		

Test Set 5				
Ki	6c38a116	ac280c45	4f59332e	e35c8c4f
RAND	ee6466bc	96202c5a	557abbef	f8babf63
OP	1ba00a1a	7c6700ac	8c3ff3e9	6ad08725
OPc	3803ef53	63b947c6	aaa225e5	8fae3934
MIL3G-RES	16c8233f	05a0ac28		
SRES#1	13688f17			
SRES#2	16c8233f			
MIL3G-CK	3f8c7587	fe8e4b23	3af676ae	de30ba3b
MIL3G-IK	a7466cc1	e6b2a133	7d49d3b6	6e95d7b4
Kc	df75bc5e	a899879f		

Test Set 6				
Ki	2d609d4d	b0ac5bf0	d2c0de26	7014de0d
RAND	194aa756	013896b7	4b4a2a3b	0af4539e
OP	460a4838	5427aa39	264aac8e	fc9e73e8
OPc	c35a0ab0	bcbfc925	2caff15f	24efbde0
MIL3G-RES	8c25a16c	d918a1df		
SRES#1	553d00b3			
SRES#2	8c25a16c			
MIL3G-CK	4cd08460	20f8fa07	31dd47cb	dc6be411
MIL3G-IK	88ab80a4	15f15c73	711254a1	d388f696
Kc	84b417ae	3aeab4f3		

Test Set 7				
Ki	a530a7fe	428fad10	82c45edd	fce13884
RAND	3a4c2b32	45c50eb5	c71d0863	9395764d
OP	511c6c4e	83e38c89	b1c5d8dd	e62426fa
OPc	27953e49	bc8af6dc	c6e730eb	80286be3
MIL3G-RES	a63241e1	ffc3e5ab		
SRES#1	59f1a44a			
SRES#2	a63241e1			
MIL3G-CK	10f05bab	75a99a5f	bb98a9c2	87679c3b
MIL3G-IK	f9ec0865	eb32f223	69cade40	c59c3a44
Kc	3b4e244c	dc60ce03		

Test Set 8				
Ki	d9151cf0	4896e258	30bf2e08	267b8360
RAND	f761e5e9	3d603feb	730e2755	6cb8a2ca
OP	75fc2233	a44294ee	8e6de25c	4353d26b
OPc	c4c93eff	e8a08138	c203d4c2	7ce4e3d9
MIL3G-RES	4a90b217	1ac83a76		
SRES#1	50588861			
SRES#2	4a90b217			
MIL3G-CK	71236b71	29f9b22a	b77ea7a5	4c96da22
MIL3G-IK	90527eba	a5588968	db417273	25a04d9e
Kc	8d4ec01d	e597acfe		

Test Set 9				
Ki	a0e2971b	6822e8d3	54a18cc2	35624ecb
RAND	08eff828	b13fdb56	2722c65c	7f30a9b2
OP	323792fa	ca21fb4d	5d6f13c1	45a9d2c1
OPc	82a26f22	bba9e948	8f949a10	d98e9cc4
MIL3G-RES	4bc2212d	8624910a		
SRES#1	cde6b027			
SRES#2	4bc2212d			
MIL3G-CK	08cef6d0	04ec6147	1a3c3cda	048137fa
MIL3G-IK	ed0318ca	5deb9206	272f6e8f	a64ba411
Kc	d8debc4f	fbcd60aa		

Test Set 10				
Ki	0da6f7ba	86d5eac8	a19cf563	ac58642d
RAND	679ac4db	acd7d233	ff9d6806	f4149ce3
OP	4b9a26fa	459e3acb	ff36f401	5de3bdc1
OPc	0db1071f	8767562c	a43a0a64	c41e8d08
MIL3G-RES	6fc30fee	6d123523		
SRES#1	02d13acd			
SRES#2	6fc30fee			
MIL3G-CK	69b1cae7	c7429d97	5e245cac	b05a517c
MIL3G-IK	74f24e8c	26df58e1	b38d7dcd	4f1b7fbd
Kc	f0eaa50a	1edcebb7		

Test Set 11				
Ki	77b45843	c88e58c1	0d202684	515ed430
RAND	4c47eb30	76dc55fe	5106cb20	34b8cd78
OP	bf3286c7	a51409ce	95724d50	3bfe6e70
OPc	d483afae	562409a3	26b5bb0b	20c4d762
MIL3G-RES	aefa357b	eac2a87a		
SRES#1	44389d01			
SRES#2	aefa357b			
MIL3G-CK	908c43f0	569cb8f7	4bc971e7	06c36c5f
MIL3G-IK	c251df0d	888dd932	9bcf4665	5b226e40
Kc	82dbab7f	83f063da		

Test Set 12				
Ki	729b1772	9270dd87	ccdf1bfe	29b4e9bb
RAND	311c4c92	9744d675	b720f3b7	e9b1cbd0
OP	d04c9c35	bd2262fa	810d2924	d036fd13
OPc	228c2f2f	06ac3268	a9e616ee	16db4ba1
MIL3G-RES	98dbbd09	9b3b408d		
SRES#1	03e0fd84			
SRES#2	98dbbd09			
MIL3G-CK	44c0f23c	5493cfd2	41e48f19	7e1d1012
MIL3G-IK	0c9fb816	13884c25	35dd0eab	f3b440d8
Kc	3c66cb98	cab2d33d		

Test Set 13				
Ki	d32dd23e	89dc6623	54ca12eb	79dd32fa
RAND	cf7d0ab1	d9430695	0bf12018	fbd46887
OP	fe75905b	9da47d35	6236d031	4e09c32e
OPc	d22a4b41	80a53257	08a5ff70	d9f67ec7
MIL3G-RES	af4a411e	1139f2c2		
SRES#1	be73b3dc			
SRES#2	af4a411e			
MIL3G-CK	5af86b80	edb70df5	292cc112	1cbad50c
MIL3G-IK	7f4d6ae7	440e1878	9a8b75ad	3f42f03a
Kc	9612b5d8	8a4130bb		

Test Set 14				
Ki	af7c65e1	927221de	591187a2	c5987a53
RAND	1f0f8578	464fd59b	64bed2d0	9436b57a
OP	0c7acb8d	95b7d4a3	1c5aca6d	26345a88
OPc	a4cf5c81	55c08a7e	ff418e54	43b98e55
MIL3G-RES	7bffa5c2	f41fbc05		
SRES#1	8fe019c7			
SRES#2	7bffa5c2			
MIL3G-CK	3f8c3f3c	cf7625bf	77fc94bc	fd22fd26
MIL3G-IK	abcbae8f	d46115e9	961a55d0	da5f2078
Kc	75a150df	3c6aed08		

Test Set 15				
Ki	5bd7ecd3	d3127a41	d12539be	d4e7cf71
RAND	59b75f14	251c7503	1d0bcbac	1c2c04c7
OP	f967f760	38b920a9	cd25e10c	08b49924
OPc	76089d3c	0ff3efdc	6e36721d	4fceb747
MIL3G-RES	7e3f44c7	591f6f45		
SRES#1	27202b82			
SRES#2	7e3f44c7			
MIL3G-CK	d42b2d61	5e49a03a	c275a5ae	f97af892
MIL3G-IK	0b3f8d02	4fe6bfaf	aa982b8f	82e319c2
Kc	b7f92e42	6a36fec5		

Test Set 16				
Ki	6cd1c6ce	b1e01e14	f1b82316	a90b7f3d
RAND	f69b78f3	00a0568b	ce9f0cb9	3c4be4c9
OP	078bfca9	564659ec	d8851e84	e6c59b48
OPc	a219dc37	f1dc7d66	738b5843	c799f206
MIL3G-RES	70f6bdb9	ad21525f		
SRES#1	ddd7efe6			
SRES#2	70f6bdb9			
MIL3G-CK	6edaf99e	5bd9f85d	5f36d91c	1272fb4b
MIL3G-IK	d61c853c	280dd9c4	6f297bae	c386de17
Kc	88d9de10	a22004c5		

Test Set 17				
Ki	b73a90cb	cf3afb62	2dba83c5	8a8415df
RAND	b120f1c1	a0102a2f	507dd543	de68281f
OP	b672047e	003bb952	dca6cb8a	f0e5b779
OPc	df0c6786	8fa25f74	8b7044c6	e7c245b8
MIL3G-RES	479dd25c	20792d63		
SRES#1	67e4ff3f			
SRES#2	479dd25c			
MIL3G-CK	66195dbe	d0313274	c5ca7766	615fa25e
MIL3G-IK	66bec707	eb2afc47	6d7408a8	f2927b36
Kc	a819e577	a8d6175b		

Test Set 18				
Ki	51222502	14c33e72	3a5dd523	fc145fc0
RAND	81e92b6c	0ee0e12e	bceba8d9	2a99dfa5
OP	c9e87632	86b5b9ff	bdf56e12	97d0887b
OPc	981d464c	7c52eb6e	50362349	84ad0bcf
MIL3G-RES	28d7b0f2	a2ec3de5		
SRES#1	8a3b8d17			
SRES#2	28d7b0f2			
MIL3G-CK	5349fbe0	98649f94	8f5d2e97	3a81c00f
MIL3G-IK	9744871a	d32bf9bb	d1dd5ce5	4e3e2e5a
Kc	9a8d0e88	3ff0887a		

Test Set 19				
Ki	90dca4ed	a45b53cf	0f12d7c9	c3bc6a89
RAND	9fddc720	92c6ad03	6b6e4647	89315b78
OP	3ffcfe5b	7b111158	9920d352	8e84e655
OPc	cb9cccc4	b9258e6d	ca476037	9fb82581
MIL3G-RES	a95100e2	760952cd		
SRES#1	df58522f			
SRES#2	a95100e2			
MIL3G-CK	b5f2da03	883b69f9	6bf52e02	9ed9ac45
MIL3G-IK	b4721368	bc16ea67	875c5598	688bb0ef
Kc	ed29b2f1	c27f9f34		

Annex A (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2002-05	-	-	-	-	-	ETSI SAGE version 1.0 produced and forwarded to SA WG3 for approval.		SAGE 1.0
2002-12	SP-18	SP-020724	-	-	-	Approved by SA WG3 meeting #26 (S3-020675). Editorial update to change MILENAGE-2G to GSM-MILENAGE and correction to references. Updated to 3GPP TS format (Technically equivalent to ETSI SAGE version 1.0). Presentation to TSG SA#18 for approval (Release 6).	SAGE 1.0	1.0.0
2002-12	SP-18	-	-	-	-	Approved at TSG SA#18. Updated to Version 6.0.0 for publication (Rel-6)	1.0.0	6.0.0
2003-12	SP-22	SP-030606	0001	-	D	Correction of reference	6.0.0	6.1.0
2006-03	SP-31	SP-060057	0002	-	F	Clarifying the Bit/Byte ordering and symbols for GSM-MILENAGE example algorithm	6.1.0	6.2.0
2007-06	SP-36	-	-	-	-	Update to Rel-7 version (MCC)	6.2.0	7.0.0
2008-12	SP-42	-	-	-	-	Update to Rel-8 version (MCC)	7.0.0	8.0.0
2009-12	-	-	-	-	-	Update to Rel-9 version (MCC)	8.0.0	9.0.0
2011-03	-	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
2012-09	-	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	**11.0.0**
2014-09	-	-	-	-	-	Update to Rel-12 version (MCC)	11.0.0	**12.0.0**
2016-01	-	-	-	-	-	Update to Rel-13 version (MCC)	12.0.0	**13.0.0**
2017-03	SA#75	-	-	-	-	Promotion to Release 14 without technical change	13.0.0	**14.0.0**
2018-10	-	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	**15.0.0**

History

Document history		
V15.0.0	November 2018	Publication