3GPP TS 55.236 V16.0.0(2020-07)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Specification of A8\_V MILENAGE algorithm:

An example algorithm for the key generation function A8\_V

(Release 16)

 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.   
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.   
This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

GSM, Algorithm, Security

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [4](#__RefHeading___Toc169680393)

1 Scope [5](#__RefHeading___Toc169680394)

2 References [5](#__RefHeading___Toc169680395)

3 Definitions, symbols and abbreviations [5](#__RefHeading___Toc169680396)

3.1 Definitions [5](#__RefHeading___Toc169680397)

3.2 Symbols [5](#__RefHeading___Toc169680398)

3.3 Abbreviations [6](#__RefHeading___Toc169680399)

4 Introductory information [6](#__RefHeading___Toc169680400)

4.1 Introduction [6](#__RefHeading___Toc169680401)

4.2 Notation [6](#__RefHeading___Toc169680402)

4.2.1 Bit/byte ordering [6](#__RefHeading___Toc169680403)

4.2.2 List of symbols [6](#__RefHeading___Toc169680404)

4.3 List of variables [6](#__RefHeading___Toc169680405)

4.4 Algorithm inputs and outputs [6](#__RefHeading___Toc169680406)

5 The A8\_V MILENAGE algorithm [7](#__RefHeading___Toc169680407)

6 Test data for A8\_V MILENAGE [7](#__RefHeading___Toc169680408)

6.1 Introduction [7](#__RefHeading___Toc169680409)

6.2 Format [7](#__RefHeading___Toc169680410)

6.3 Test Sets [8](#__RefHeading___Toc169680411)

Annex A (informative): Change history [12](#__RefHeading___Toc169680412)

# 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.

# 1 Scope

The present document contains an example algorithm which may be used as the VSTK key generation function A8\_V as described in TS 43.020 [4]. (It is not mandatory that the particular algorithm specified in this document is used - the A8\_V function is operator-specifiable rather than being fully standardised.)

Clause 4 introduces the algorithm and describes the input and output parameters. Clause 5 defines the algorithm. Clause 6 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: "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: "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: "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 43.020: " Security related network functions".

[5] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [5], TS 35.206 [1] and TS 43.020 [4], and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [5], TS 35.206 [1] or TS 43.020 [4].

## 3.2 Symbols

= The assignment operator.

|| The concatenation of the two operands.

X[i] The ith bit of the variable **X**. (**X = X[0] || X[1] || X[2] || …..** ).

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [5], TS 35.206 [1] and TS 43.020 [4], and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [5], TS 35.206 [1] or TS 43.020 [4].

VBS Voice Broadcast Service

VGCS Voice Group Call Service

# 4 Introductory information

## 4.1 Introduction

For VGCS and VBS ciphering in the GSM system the security function A8\_V has been specified. The operation of this function falls completely within the domain of an individual operator, and the function is therefore to be specified by each operator rather than being fully standardized. The algorithm specified in this document is an example that may be used by an operator which does not wish to design its own.

The inputs and outputs of the function A8\_V is defined in clause 4.4.

## 4.2 Notation

### 4.2.1 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.

### 4.2.2 List of symbols

See clause 3.2

## 4.3 List of variables

For V\_Ki, VSTK\_RAND and VSTK see TS 43.020 [4]

For all f3-function related variables see TS 35.206 [1]

## 4.4 Algorithm inputs and outputs

The inputs to the algorithm are given in table 1, the output in table 2 below.

Table 1: Inputs to A8\_V

|  |  |  |
| --- | --- | --- |
| Parameter | Size (bits) | Comment |
| V\_Ki | 128 | Group key V\_Ki[0]…V\_Ki[127] |
| VSTK\_RAND | 36 | Random challenge VSTK\_RAND[0]…VSTK\_RAND[35] |

Table 2: Outputs from A8\_V

|  |  |  |
| --- | --- | --- |
| Parameter | Size (bits) | Comment |
| VSTK | 128 | Cipher key VSTK[0]…VSTK[127] |

# 5 The A8\_V MILENAGE algorithm

An example algorithm set for UMTS, called MILENAGE (see Note 1), is specified in TS 35.206 [1]. A8\_V MILENAGE makes use of MILENAGE.

Specifically, the function f3 from the UMTS MILENAGE is making use of (all input and output names are prefixed by "MIL3G-" to distinguish them clearly from the inputs and outputs of A8\_V MILENAGE):

|  |  |  |
| --- | --- | --- |
| **Function** | **Inputs** | **Output** |
| **f3** | MIL3G-K[0]…MIL3G-K[127]  MIL3G-RAND[0]…MIL3G-RAND[127] | MIL3G-CK[0]…MIL3G-CK[127] |

The A8\_V MILENAGE functions are defined as follows:

- Let (MIL3G-K[0]…MIL3G-K[127]) = (V\_Ki[0]…V\_Ki[127])

- Let (MIL3G-RAND[0]…MIL3G-RAND[127]) = (**EXP\_RAND**[0]…**EXP\_RAND**[127])

Whereby

**EXP\_RAND**[bits 0,1, . . .126,127] = **EXPAND**[bits 0,1, . . .39] || **EXPAND**[bits 0,1, . . .39] || **EXPAND**[bits 0,1, . . .39] || ‘11111111’

**EXPAND** [bits 0,1, . . .39]  **= ‘**1111**’** **|| VSTK\_RAND**[bits 0,1, . . .35]

- Compute MIL3G-CK from MIL3G-K and MIL3G-RAND, using the MILENAGE function ***f*3**

- Set (VSTK[0]…VSTK[127]) = (MIL3G-CK[0]…MIL3G-CK[127])

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.

# 6 Test data for A8\_V MILENAGE

## 6.1 Introduction

The test data sets presented here have been derived from the MILENAGE test sets in [3].

## 6.2 Format

The format of each test data set is as follows:

|  |  |
| --- | --- |
| Test Set *n* | |
| V\_Ki | secret group key |
| VSTK\_RAND | 36-bit random challenge |
| MIL3G-RAND | 128-bit expansion of VSTK\_RAND according to clause 4 |
| OP | operator-specific MILENAGE constant |
| OPc | derived from OP and V\_Ki — see [1] |
| MIL3G-CK (VSTK) | MILENAGE ***f*3** output, that equals the Short Term Key for use in VGCS and VBS ciphering |

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 | |
| V\_Ki | 01000110 01011011 01011100 11101000 10110001 10011001 10110100 10011111 10101010 01011111 00001010 00101110 11100010 00111000 10100110 10111100 |
| VSTK\_RAND | 00100011 01010101 00111100 10111110 1001 |
| MIL3G-RAND | 11110010 00110101 01010011 11001011 11101001 11110010 00110101 01010011 11001011 11101001 11110010 00110101 01010011 11001011 11101001 11111111 |
| 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-CK (VSTK) | 11010111 01110011 11000111 11111111 11000110 01000000 11001101 00100100 10000001 11110101 00010010 11011100 10111101 01011100 11000000 11110110 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 1 | | | | |
| V\_Ki | 465b5ce8 | b199b49f | aa5f0a2e | e238a6bc |
| VSTK\_RAND | 23553cbe | 9 |  |  |
| MIL3G-RAND | f23553cb | e9f23553 | cbe9f235 | 53cbe9ff |
| OP | cdc202d5 | 123e20f6 | 2b6d676a | c72cb318 |
| OPc | cd63cb71 | 954a9f4e | 48a5994e | 37a02baf |
| MIL3G-CK (VSTK) | d773c7ff | c640cd24 | 81f512dc | bd5cc0f6 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 2 | | | | |
| V\_Ki | fec86ba6 | eb707ed0 | 8905757b | 1bb44b8f |
| VSTK\_RAND | 9f7c8d02 | 1 |  |  |
| MIL3G-RAND | f9f7c8d0 | 21f9f7c8 | d021f9f7 | c8d021ff |
| OP | dbc59adc | b6f9a0ef | 735477b7 | fadf8374 |
| OPc | 1006020f | 0a478bf6 | b699f15c | 062e42b3 |
| MIL3G-CK (VSTK) | a0b28afe | ca802828 | c324eb86 | a7b06903 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 3 | | | | |
| V\_Ki | 9e5944ae | a94b8116 | 5c82fbf9 | f32db751 |
| VSTK\_RAND | ce83dbc5 | 4 |  |  |
| MIL3G-RAND | fce83dbc | 54fce83d | bc54fce8 | 3dbc54ff |
| OP | 223014c5 | 806694c0 | 07ca1eee | f57f004f |
| OPc | a64a507a | e1a2a98b | b88eb421 | 0135dc87 |
| MIL3G-CK (VSTK) | f2abba4c | 9d52cf6b | 99b43d2a | 799e9470 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 4 | | | | |
| V\_Ki | 4ab1deb0 | 5ca6ceb0 | 51fc98e7 | 7d026a84 |
| VSTK\_RAND | 74b0cd60 | 3 |  |  |
| MIL3G-RAND | f74b0cd6 | 03f74b0c | d603f74b | 0cd603ff |
| OP | 2d16c5cd | 1fdf6b22 | 383584e3 | bef2a8d8 |
| OPc | dcf07cbd | 51855290 | b92a07a9 | 891e523e |
| MIL3G-CK (VSTK) | d4500866 | a11b5b7d | 3d89d485 | d25e14da |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 5 | | | | |
| V\_Ki | 6c38a116 | ac280c45 | 4f59332e | e35c8c4f |
| VSTK\_RAND | ee6466bc | 9 |  |  |
| MIL3G-RAND | fee6466b | c9fee646 | 6bc9fee6 | 466bc9ff |
| OP | 1ba00a1a | 7c6700ac | 8c3ff3e9 | 6ad08725 |
| OPc | 3803ef53 | 63b947c6 | aaa225e5 | 8fae3934 |
| MIL3G-CK (VSTK) | bafd96fb | 7c417cce | 58597e0f | 118b6a02 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 6 | | | | |
| V\_Ki | 2d609d4d | b0ac5bf0 | d2c0de26 | 7014de0d |
| VSTK\_RAND | 194aa756 | 0 |  |  |
| MIL3G-RAND | f194aa75 | 60f194aa | 7560f194 | aa7560ff |
| OP | 460a4838 | 5427aa39 | 264aac8e | fc9e73e8 |
| OPc | c35a0ab0 | bcbfc925 | 2caff15f | 24efbde0 |
| MIL3G-CK (VSTK) | b4d5f9b7 | 94d269c5 | 706ee6e3 | 1453a426 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 7 | | | | |
| V\_Ki | a530a7fe | 428fad10 | 82c45edd | fce13884 |
| VSTK\_RAND | 3a4c2b32 | 4 |  |  |
| MIL3G-RAND | f3a4c2b3 | 24f3a4c2 | b324f3a4 | c2b324ff |
| OP | 511c6c4e | 83e38c89 | b1c5d8dd | e62426fa |
| OPc | 27953e49 | bc8af6dc | c6e730eb | 80286be3 |
| MIL3G-CK (VSTK) | b8b143ae | 303bbdd6 | 8539ee34 | a69c530e |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 8 | | | | |
| V\_Ki | d9151cf0 | 4896e258 | 30bf2e08 | 267b8360 |
| VSTK\_RAND | f761e5e9 | 3 |  |  |
| MIL3G-RAND | ff761e5e | 93ff761e | 5e93ff76 | 1e5e93ff |
| OP | 75fc2233 | a44294ee | 8e6de25c | 4353d26b |
| OPc | c4c93eff | e8a08138 | c203d4c2 | 7ce4e3d9 |
| MIL3G-CK (VSTK) | 6e6aa729 | 1a54c264 | 6188e2e0 | 2002fda5 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 9 | | | | |
| V\_Ki | a0e2971b | 6822e8d3 | 54a18cc2 | 35624ecb |
| VSTK\_RAND | 08eff828 | b |  |  |
| MIL3G-RAND | f08eff82 | 8bf08eff | 828bf08e | ff828bff |
| OP | 323792fa | ca21fb4d | 5d6f13c1 | 45a9d2c1 |
| OPc | 82a26f22 | bba9e948 | 8f949a10 | d98e9cc4 |
| MIL3G-CK (VSTK) | e360f5fe | 8a5b1602 | 5fb8acbf | f3b9cbb2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 10 | | | | |
| V\_Ki | 0da6f7ba | 86d5eac8 | a19cf563 | ac58642d |
| VSTK\_RAND | 679ac4db | a |  |  |
| MIL3G-RAND | f679ac4d | baf679ac | 4dbaf679 | ac4dbaff |
| OP | 4b9a26fa | 459e3acb | ff36f401 | 5de3bdc1 |
| OPc | 0db1071f | 8767562c | a43a0a64 | c41e8d08 |
| MIL3G-CK (VSTK) | 805879c0 | 53864ea5 | a8c41c18 | 95976d41 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 11 | | | | |
| V\_Ki | 77b45843 | c88e58c1 | 0d202684 | 515ed430 |
| VSTK\_RAND | 4c47eb30 | 7 |  |  |
| MIL3G-RAND | f4c47eb3 | 07f4c47e | b307f4c4 | 7eb307ff |
| OP | bf3286c7 | a51409ce | 95724d50 | 3bfe6e70 |
| OPc | d483afae | 562409a3 | 26b5bb0b | 20c4d762 |
| MIL3G-CK (VSTK) | 74909b16 | e577b2d4 | cf1ff01a | 213cfc54 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 12 | | | | |
| V\_Ki | 729b1772 | 9270dd87 | ccdf1bfe | 29b4e9bb |
| VSTK\_RAND | 311c4c92 | 9 |  |  |
| MIL3G-RAND | f311c4c9 | 29f311c4 | c929f311 | c4c929ff |
| OP | d04c9c35 | bd2262fa | 810d2924 | d036fd13 |
| OPc | 228c2f2f | 06ac3268 | a9e616ee | 16db4ba1 |
| MIL3G-CK (VSTK) | b102a313 | d2692e01 | 1b7301c2 | ad188adc |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 13 | | | | |
| V\_Ki | d32dd23e | 89dc6623 | 54ca12eb | 79dd32fa |
| VSTK\_RAND | cf7d0ab1 | d |  |  |
| MIL3G-RAND | fcf7d0ab | 1dfcf7d0 | ab1dfcf7 | d0ab1dff |
| OP | fe75905b | 9da47d35 | 6236d031 | 4e09c32e |
| OPc | d22a4b41 | 80a53257 | 08a5ff70 | d9f67ec7 |
| MIL3G-CK (VSTK) | 995729ba | d5e7c84d | 46d0980a | 4729351f |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 14 | | | | |
| V\_Ki | af7c65e1 | 927221de | 591187a2 | c5987a53 |
| VSTK\_RAND | 1f0f8578 | 4 |  |  |
| MIL3G-RAND | f1f0f857 | 84f1f0f8 | 5784f1f0 | f85784ff |
| OP | 0c7acb8d | 95b7d4a3 | 1c5aca6d | 26345a88 |
| OPc | a4cf5c81 | 55c08a7e | ff418e54 | 43b98e55 |
| MIL3G-CK (VSTK) | 485e7bfd | 24492467 | 420b93ad | 3fce8ac2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 15 | | | | |
| V\_Ki | 5bd7ecd3 | d3127a41 | d12539be | d4e7cf71 |
| VSTK\_RAND | 59b75f14 | 2 |  |  |
| MIL3G-RAND | f59b75f1 | 42f59b75 | f142f59b | 75f142ff |
| OP | f967f760 | 38b920a9 | cd25e10c | 08b49924 |
| OPc | 76089d3c | 0ff3efdc | 6e36721d | 4fceb747 |
| MIL3G-CK (VSTK) | 1b32d440 | 99fb51f5 | 0505149d | a25e7760 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 16 | | | | |
| V\_Ki | 6cd1c6ce | b1e01e14 | f1b82316 | a90b7f3d |
| VSTK\_RAND | f69b78f3 | 0 |  |  |
| MIL3G-RAND | ff69b78f | 30ff69b7 | 8f30ff69 | b78f30ff |
| OP | 078bfca9 | 564659ec | d8851e84 | e6c59b48 |
| OPc | a219dc37 | f1dc7d66 | 738b5843 | c799f206 |
| MIL3G-CK (VSTK) | c7ada658 | f4bf89dc | 184b1d31 | 9df554d9 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 17 | | | | |
| V\_Ki | b73a90cb | cf3afb62 | 2dba83c5 | 8a8415df |
| VSTK\_RAND | b120f1c1 | a |  |  |
| MIL3G-RAND | fb120f1c | 1afb120f | 1c1afb12 | 0f1c1aff |
| OP | b672047e | 003bb952 | dca6cb8a | f0e5b779 |
| OPc | df0c6786 | 8fa25f74 | 8b7044c6 | e7c245b8 |
| MIL3G-CK (VSTK) | ca8cf524 | d78c8c55 | aa5aba14 | 22737909 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 18 | | | | |
| V\_Ki | 51222502 | 14c33e72 | 3a5dd523 | fc145fc0 |
| VSTK\_RAND | 81e92b6c | 0 |  |  |
| MIL3G-RAND | f81e92b6 | c0f81e92 | b6c0f81e | 92b6c0ff |
| OP | c9e87632 | 86b5b9ff | bdf56e12 | 97d0887b |
| OPc | 981d464c | 7c52eb6e | 50362349 | 84ad0bcf |
| MIL3G-CK (VSTK) | a8d5cdb6 | 47335bf5 | 8e2c884d | a5efcdd5 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Set 19 | | | | |
| V\_Ki | 90dca4ed | a45b53cf | 0f12d7c9 | c3bc6a89 |
| VSTK\_RAND | 9fddc720 | 9 |  |  |
| MIL3G-RAND | f9fddc72 | 09f9fddc | 7209f9fd | dc7209ff |
| OP | 3ffcfe5b | 7b111158 | 9920d352 | 8e84e655 |
| OPc | cb9cccc4 | b9258e6d | ca476037 | 9fb82581 |
| MIL3G-CK (VSTK) | c699833a | 2c22bf44 | b6473390 | 8a7142c3 |

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | | |
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **Old** | **New** |
| 2005-11 | SA3#41 | - | - | - | - | Draft version presented at SA3#41 |  | 0.1.0 |
| 2006-02 | SA3#42 | - | - | - | - | Inclusion of Test Sets generated by ETSI SAGE | 0.1.0 | 1.0.0 |
| 2006-02 |  |  |  |  |  | Editorial clean up by MCC to conform to 21.801. | 1.0.0 | 1.0.1 |
| 2006-02 |  |  |  |  |  | Raised to 1.0.2 to accept changes for presentation to SA #31 | 1.0.1 | 1.0.2 |
| 2006-03 | - | - | - | - | - | Editorial update to stylesheet and removal of comment | 1.0.2 | 1.0.3 |
| 2006-03 | SP-31 | SP-060059 | - | - | - | Approved at SA #31 | 1.0.3 | 6.0.0 |
| 2006-06 | SP-32 | SP-060378 | 0001 | - | F | Missing bit in MIL3G RAND test set 1 example and correcting used functions | 6.0.0 | 6.1.0 |
| 2007-06 | SP-36 | - | - | - | - | Update to Rel-7 version (MCC) | 6.1.0 | 7.0.0 |
| 2008-12 | SP-42 | - | - | - | - | Update to Rel-8 version (MCC) | 7.1.0 | 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** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-06 | - | - | - | - | - | Update to Rel-15 version (MCC) | **15.0.0** |
| 2020-07 | - | - | - | - | - | Update to Rel-16 version (MCC) | **16.0.0** |