3GPP TS 35.203 V16.0.0(2020-07)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

3G security;

Specification of the 3GPP confidentiality

and integrity algorithms;

Document 3: implementors' test data

(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

UMTS, algorithm, KASUMI

***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___Toc169677968)

Introduction [4](#__RefHeading___Toc169677969)

0 Scope [5](#__RefHeading___Toc169677970)

1 Outline of the implementors' test data [5](#__RefHeading___Toc169677971)

1.1 References [5](#__RefHeading___Toc169677972)

2 Introductory information [6](#__RefHeading___Toc169677973)

2.1 Introduction [6](#__RefHeading___Toc169677974)

2.2 Radix [6](#__RefHeading___Toc169677975)

2.3 Bit/Byte ordering [6](#__RefHeading___Toc169677976)

2.4 Presentation of input/output data [6](#__RefHeading___Toc169677977)

3 KASUMI [6](#__RefHeading___Toc169677978)

3.1 Overview [6](#__RefHeading___Toc169677979)

3.2 Format [6](#__RefHeading___Toc169677980)

3.3 Test Set 1 [7](#__RefHeading___Toc169677981)

3.4 Test Set 2 [9](#__RefHeading___Toc169677982)

3.5 Test Set 3 [10](#__RefHeading___Toc169677983)

3.6 Test Set 4 [12](#__RefHeading___Toc169677984)

4 Confidentiality algorithm *f8* [12](#__RefHeading___Toc169677985)

4.1 Overview [12](#__RefHeading___Toc169677986)

4.2 Format [12](#__RefHeading___Toc169677987)

4.3 Test Set 1 [13](#__RefHeading___Toc169677988)

4.4 Test Set 2 [13](#__RefHeading___Toc169677989)

4.5 Test Set 3 [14](#__RefHeading___Toc169677990)

4.6 Test Set 4 [14](#__RefHeading___Toc169677991)

4.7 Test Set 5 [15](#__RefHeading___Toc169677992)

5 Integrity algorithm *f9* [15](#__RefHeading___Toc169677993)

5.1 Overview [15](#__RefHeading___Toc169677994)

5.2 Format [15](#__RefHeading___Toc169677995)

5.3 Test Set 1 [16](#__RefHeading___Toc169677996)

5.4 Test Set 2 [16](#__RefHeading___Toc169677997)

5.5 Test Set 3 [16](#__RefHeading___Toc169677998)

5.6 Test Set 4 [17](#__RefHeading___Toc169677999)

5.7 Test Set 5 [17](#__RefHeading___Toc169678000)

Annex A (informative): Change history [18](#__RefHeading___Toc169678001)

# Foreword

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

The 3GPP Confidentiality and Integrity Algorithms f8 & f9 have been developed through the collaborative efforts of the European Telecommunications Standards Institute (ETSI), the Association of Radio Industries and Businesses (ARIB), the Telecommunications Technology Association (TTA), the T1 Committee.

The f8 & f9 Algorithms Specifications may be used only for the development and operation of 3G Mobile Communications and services. Every Beneficiary must sign a Restricted Usage Undertaking with the Custodian and demonstrate that he fulfils the approval criteria specified in the Restricted Usage Undertaking.

Furthermore, Mitsubishi Electric Corporation holds essential patents on the Algorithms. The Beneficiary must get a separate IPR License Agreement from Mitsubishi Electronic Corporation Japan.

For details of licensing procedures, contact ETSI, ARIB, TTA or T1.

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

This specification has been prepared by the 3GPP Task Force, and gives detailed test data for implementors of the algorithm set. It provides visibility of the internal state of the algorithm to aid in the realisation of the algorithms.

This document is the third of four, which between them form the entire specification of the 3GPP Confidentiality and Integrity Algorithms:

- 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: *f8* and *f9* Specification".

- 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".

**- 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 3: Implementors' Test Data".**

- 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 4: Design Conformance Test Data".

This document is purely informative. The normative part of the specification of the ***f8*** (confidentiality) and the ***f9*** (integrity) algorithms is in the main body of Document 1. The normative part of the specification of **KASUMI** is found in document 2.

# 0 Scope

This specification gives detailed test data for implementors of the algorithm set. It provides visibility of the internal state of the algorithm to aid in the realisation of the algorithms.

# 1 Outline of the implementors' test data

Clause 2 introduces the algorithms and describes the notation used in the subsequent Clauses.

Clause 3 provides test data for **KASUMI**.

Clause 4 provides test data for the Confidentiality Algorithm F8.

Clause 5 provides test data for the Integrity Algorithm F9.

## 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 version 3.2.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 33.105 version 3.1.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements".

[3] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification".

[4] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".

[5] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 3: Implementors' Test Data".

[6] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 4: Design Conformance Test Data".

[7] ISO/IEC 9797-1:1999: "Information technology – Security techniques – Message Authentication Codes (MACs)".

# 2 Introductory information

## 2.1 Introduction

Within the security architecture of the 3GPP system there are two standardised algorithms; a confidentiality algorithm ***f8***, and an integrity algorithm ***f9***. These algorithms are specified in a companion document [3]. Each of these algorithms is based on the **KASUMI** algorithm that is specified in [4].

To assist implementors with their realisation of the algorithm set this document provides test data for these algorithms along with extensive detail of the internal states of the algorithms as they process the given input data.

Final testing of the algorithms should be performed using the test data sets given in the "Design Conformance" companion document [6].

## 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 sub-strings, the left most (most significant) sub-string is numbered 1, the next most significant is numbered 2 and so on through to the least significant.

For example the 128-kit key ***K*** is subdivided into eight 16-bit substrings ***K1...K8*** so if we have a key  
 ***K*** = 0123456789ABCDEFFEDCBA9876543210

we have:

***K1*** = 0123, ***K2*** = 5678, ***K3*** = 9ABC, ….. ***K8*** = 3210.

## 2.4 Presentation of input/output data

The basic data processed by the ***f8*** and ***f9*** algorithms are bit streams. In general in this document the data is presented in hexadecimal format as bytes, thus the last byte shown as part of an input or output data stream may include between 0 and 7 bits that are ignored once the **LENGTH** parameter is taken into account. (The least significant bits of the byte are ignored).

# 3 KASUMI

## 3.1 Overview

The test data sets presented here are for the **KASUMI** block cipher algorithm.

## 3.2 Format

Each test set starts by showing the input and output data values. This is followed by a table showing the internal sub-keys that are derived from the 128-bit key.

For each round the inputs and outputs are shown for the **FL**, **FO** and **FI** functions in the form:

Round i

FLi( input, KL1i, KL2i )->output

FOi( input )->output

FIi1( input, KIi1 ) -> output

FIi2( input, KIi2 ) -> output

FIi3( input, KIi3 ) -> output

In addition, for the first two rounds, the internal states of the 7-bit and 9-bit data paths within the **FI** function are shown in the form:

seven 17-> 0C-> 47-> 72-> 6C-> 21

nine 19E->05C->04B->1BB->1BF->1CD

where the first value shown is the value derived from the 16-bit input, and the subsequent values are the changes that occur as the data passes through the function down the respective 7-bit or 9-bit data paths. i.e. The values shown following the input value are:

result of S-box lookup,  
XOR with other half,  
XOR with key,  
S-box lookup,  
XOR with other half.

## 3.3 Test Set 1

Key: 2B D6 45 9F 82 C5 B3 00 95 2C 49 10 48 81 FF 48

input: EA 02 47 14 AD 5C 4D 84

output: DF 1F 9B 25 1C 0B F4 5F

Key schedule:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| KLi1 | 57AC | 8B3E | 058B | 6601 | 2A59 | 9220 | 9102 | FE91 |
| KLi2 | 0B6E | 7EEF | 6BF0 | F388 | 3ED5 | CD58 | 2AF5 | 00F8 |
| KOi1 | B3E8 | 58B0 | 6016 | A592 | 2209 | 1029 | E91F | 7AC5 |
| KOi2 | 1049 | 8148 | 48FF | D62B | 9F45 | C582 | 00B3 | 2C95 |
| KOi3 | 2910 | 1FE9 | C57A | E8B3 | B058 | 1660 | 92A5 | 0922 |
| KIi1 | 6BF0 | F388 | 3ED5 | CD58 | 2AF5 | 00F8 | 0B6E | 7EEF |
| KIi2 | 7EEF | 6BF0 | F388 | 3ED5 | CD58 | 2AF5 | 00F8 | 0B6E |
| KIi3 | CD58 | 2AF5 | 00F8 | 0B6E | 7EEF | 6BF0 | F388 | 3ED5 |

Input: EA024714 AD5C4D84

Round 1

FL1(EA024714,57AC,0B6E)->7CFFC314

FO1(7CFFC314)->58871737

FI11(CF17,6BF0)->43CD

seven 17-> 0C-> 47-> 72-> 6C-> 21

nine 19E->05C->04B->1BB->1BF->1CD

FI12(D35D,7EEF)->D85E

seven 5D-> 61-> 3E-> 01-> 32-> 6C

nine 1A6->082->0DF->030->05F->05E

FI13(A9C9,CD58)->4FB0

seven 49-> 63-> 52-> 34-> 17-> 27

nine 153->1F8->1B1->0E9->184->1B0

Round 2

FO2(F5DB5AB3)->03E715B9

FI21(AD6B,F388)->E2FC

seven 6B-> 31-> 4F-> 36-> 0D-> 71

nine 15A->015->07E->1F6->0CA->0FC

FI22(DBFB,6BF0)->BBA8

seven 7B-> 29-> 75-> 40-> 75-> 5D

nine 1B7->127->15C->0AC->1E8->1A8

FI23(A7A6,2AF5)->165E

seven 26-> 3A-> 73-> 66-> 55-> 0B

nine 14F->06F->049->0BC->038->05E

FL2(03E715B9,8B3E,7EEF)->FC1913F5

Round 3

FL3(161B54E1,058B,6BF0)->E9F55CF7

FO3(E9F55CF7)->F9C9DB3F

FI31(89E3,3ED5)->4C63

seven 63-> 2D-> 54-> 4B-> 45-> 26

nine 113->19A->1F9->12C->028->063

FI32(1408,F388)->E95D

seven 08-> 26-> 02-> 7B-> 29-> 74

nine 028->02C->024->1AC->126->15D

FI33(D5EE,00F8)->22F6

seven 6E-> 73-> 5B-> 5B-> 67-> 11

nine 1AB->046->028->0D0->0AD->0F6

Round 4

FO4(0C12818C)->F9C83A1A

FI41(A980,CD58)->4D43

seven 00-> 36-> 4E-> 28-> 65-> 26

nine 153->1F8->1F8->0A0->16B->143

FI42(57A7,3ED5)->3507

seven 27-> 30-> 72-> 6D-> 1D-> 1A

nine 0AF->0E5->0C2->017->16A->107

FI43(247C,0B6E)->C3D2

seven 7C-> 58-> 54-> 51-> 33-> 61

nine 048->0F0->08C->1E2->183->1D2

FL4(F9C83A1A,6601,F388)->0EFDFA1A

Round 5

FL5(18E6AEFB,2A59,3ED5)->6519BE7B

FO5(6519BE7B)->D1FAD9E0

FI51(4710,2AF5)->781A

seven 10-> 37-> 1D-> 08-> 26-> 3C

nine 08E->1BA->1AA->15F->012->01A

FI52(213E,CD58)->179B

seven 3E-> 69-> 5C-> 3A-> 10-> 0B

nine 042->18B->1B5->0ED->1A1->19B

FI53(7639,7EEF)->081A

seven 39-> 01-> 73-> 4C-> 1E-> 04

nine 0EC->1CB->1F2->11D->056->01A

Round 6

FO6(DDE8586C)->DD0B619B

FI61(CDC1,00F8)->8FF4

seven 41-> 74-> 51-> 51-> 33-> 47

nine 19B->0E4->0A5->05D->1A5->1F4

FI62(9DEE,2AF5)->0A93

seven 6E-> 73-> 11-> 04-> 16-> 05

nine 13B->00C->062->097->097->093

FI63(C1F8,6BF0)->BC90

seven 78-> 2A-> 42-> 77-> 4E-> 5E

nine 183->090->0E8->118->0E7->090

FL6(DD0B619B,9220,CD58)->46BE419A

Round 7

FL7(5E58EF61,9102,2AF5)->81B3CF61

FO7(81B3CF61)->C1E3AC33

FI71(68AC,0B6E)->EBA4

seven 2C-> 68-> 1A-> 1F-> 51-> 75

nine 0D1->0DE->0F2->19C->1BB->1A4

FI72(CFD2,00F8)->E526

seven 52-> 11-> 57-> 57-> 54-> 72

nine 19F->194->1C6->13E->171->126

FI73(B660,F388)->6DD0

seven 60-> 66-> 19-> 60-> 66-> 36

nine 16C->01F->07F->1F7->1B0->1D0

Round 8

FO8(1C0BF45F)->68BFA566

FI81(66CE,7EEF)->DB25

seven 4E-> 7E-> 0D-> 32-> 48-> 6D

nine 0CD->03D->073->09C->117->125

FI82(D8CA,0B6E)->47C5

seven 4A-> 56-> 65-> 60-> 66-> 23

nine 1B1->179->133->05D->1A5->1C5

FI83(2658,3ED5)->CDD9

seven 58-> 5B-> 15-> 0A-> 3F-> 66

nine 04C->196->1CE->11B->1D3->1D9

FL8(68BFA566,FE91,00F8)->81477444

Output: DF1F9B25 1C0BF45F

## 3.4 Test Set 2

Key: 8C E3 3E 2C C3 C0 B5 FC 1F 3D E8 A6 DC 66 B1 F3

input: D3 C5 D5 92 32 7F B1 1C

output: DE 55 19 88 CE B2 F9 B7

Key schedule:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| KLi1 | 19C7 | 7C58 | 8781 | 6BF9 | 3E7A | D14D | B8CD | 63E7 |
| KLi2 | 4A6B | 7813 | E1E1 | 523E | AA32 | 83E3 | 8DC0 | 7B4B |
| KOi1 | C587 | 7818 | BF96 | E7A3 | 14DD | 8CDB | 3E76 | 9C71 |
| KOi2 | A6E8 | 66DC | F3B1 | E38C | 2C3E | C0C3 | FCB5 | 3D1F |
| KOi3 | DB8C | 763E | 719C | 87C5 | 1878 | 96BF | A3E7 | DD14 |
| KIi1 | E1E1 | 523E | AA32 | 83E3 | 8DC0 | 7B4B | 4A6B | 7813 |
| KIi2 | 7813 | E1E1 | 523E | AA32 | 83E3 | 8DC0 | 7B4B | 4A6B |
| KIi3 | 83E3 | 8DC0 | 7B4B | 4A6B | 7813 | E1E1 | 523E | AA32 |

Input: D3C5D592 327FB11C

Round 1

FL1(D3C5D592,19C7,4A6B)->2F32F618

FO1(2F32F618)->9F6FAB3F

FI11(EAB5,E1E1)->9A6B

seven 35-> 6D-> 78-> 08-> 26-> 4D

nine 1D5->0A0->095->174->063->06B

FI12(50F0,7813)->F31C

seven 70-> 40-> 14-> 28-> 65-> 79

nine 0A1->124->154->147->134->11C

FI13(B7FF,83E3)->3450

seven 7F-> 03-> 28-> 69-> 4A-> 1A

nine 16F->054->02B->1C8->039->050

Round 2

FO2(AD101A23)->5BBD1022

FI21(D508,523E)->E46B

seven 08-> 26-> 35-> 1C-> 19-> 72

nine 1AA->11B->113->12D->077->06B

FI22(7CFF,E1E1)->A5F5

seven 7F-> 03-> 62-> 12-> 27-> 52

nine 0F9->11E->161->080->1E7->1F5

FI23(8876,8DC0)->4B9F

seven 76-> 24-> 60-> 26-> 3A-> 25

nine 110->032->044->184->1B9->19F

FL2(5BBD1022,7C58,7813)->AB9AA012

Round 3

FL3(785F7580,8781,E1E1)->93987582

FO3(93987582)->109659D3

FI31(2C0E,AA32)->D87A

seven 0E-> 7B-> 51-> 04-> 16-> 6C

nine 058->0A4->0AA->098->07E->07A

FI32(8633,523E)->BD6E

seven 33-> 3D-> 0E-> 27-> 30-> 5E

nine 10C->100->133->10D->149->16E

FI33(DC64,7B4B)->4945

seven 64-> 4B-> 60-> 5D-> 61-> 24

nine 1B8->1CF->1AB->0E0->118->145

Round 4

FO4(BD8643F0)->CA56843A

FI41(5A25,83E3)->5709

seven 25-> 3C-> 44-> 05-> 22-> 2B

nine 0B4->15D->178->09B->10C->109

FI42(A07C,AA32)->DEAF

seven 7C-> 58-> 25-> 70-> 40-> 6F

nine 140->001->07D->04F->0DF->0AF

FI43(933C,4A6B)->4E6C

seven 3C-> 52-> 41-> 64-> 4B-> 27

nine 126->1AF->193->1F8->008->06C

FL4(CA56843A,6BF9,523E)->6F2A109A

Round 5

FL5(1775651A,3E7A,AA32)->C08049FA

FO5(C08049FA)->C9D692DD

FI51(D45D,8DC0)->AB91

seven 5D-> 61-> 2A-> 6C-> 44-> 55

nine 1A8->016->04B->18B->1FD->191

FI52(65C4,83E3)->2BBD

seven 44-> 59-> 6B-> 2A-> 28-> 15

nine 0CB->1F6->1B2->051->197->1BD

FI53(FA13,7813)->5B0B

seven 13-> 72-> 34-> 08-> 26-> 2D

nine 1F4->155->146->155->103->10B

Round 6

FO6(7450D12D)->F6FA9BBE

FI61(F88B,7B4B)->5654

seven 0B-> 5D-> 14-> 29-> 7F-> 2B

nine 1F1->042->049->102->07D->054

FI62(11EE,8DC0)->7183

seven 6E-> 73-> 38-> 7E-> 3B-> 38

nine 023->025->04B->18B->1FD->183

FI63(11C6,E1E1)->6D44

seven 46-> 00-> 63-> 13-> 72-> 36

nine 023->025->063->182->157->144

FL6(F6FA9BBE,D14D,83E3)->81253B2F

Round 7

FL7(96505E35,B8CD,8DC0)->69B97EB4

FO7(69B97EB4)->BAE2289A

FI71(57CF,4A6B)->47F8

seven 4F-> 57-> 7D-> 58-> 5B-> 23

nine 0AF->0E5->0AA->0C1->1A0->1F8

FI72(8201,7B4B)->83AE

seven 01-> 32-> 20-> 1D-> 6F-> 41

nine 104->013->012->159->1B3->1AE

FI73(9AAB,523E)->9278

seven 2B-> 78-> 42-> 6B-> 31-> 49

nine 135->111->13A->104->013->078

Round 8

FO8(CEB2F9B7)->B7FB007B

FI81(52C3,7813)->4A98

seven 43-> 0B-> 0F-> 33-> 3D-> 25

nine 0A5->147->104->117->0AB->098

FI82(C4A8,4A6B)->04D4

seven 28-> 65-> 6F-> 4A-> 56-> 02

nine 189->022->00A->061->09E->0D4

FI83(6E3B,AA32)->B780

seven 3B-> 07-> 0D-> 58-> 5B-> 5B

nine 0DC->031->00A->038->1D8->180

FL8(B7FB007B,63E7,7B4B)->480547BD

Output: DE551988 CEB2F9B7

## 3.5 Test Set 3

Key: 40 35 C6 68 0A F8 C6 D1 A8 FF 86 67 B1 71 40 13

input: 62 A5 40 98 1B A6 F9 B7

output: 45 92 B0 E7 86 90 F7 1B

Key schedule:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| KLi1 | 806A | 8CD1 | 15F0 | 8DA3 | 51FF | 0CCF | 62E3 | 8026 |
| KLi2 | 8353 | 0B3E | 5623 | 3CFF | C725 | 7203 | 4116 | 830F |
| KOi1 | CD18 | 5F01 | DA38 | 1FF5 | CCF0 | 2E36 | 0268 | 06A8 |
| KOi2 | 6786 | 71B1 | 1340 | 3540 | 68C6 | F80A | D1C6 | FFA8 |
| KOi3 | 362E | 6802 | A806 | 18CD | 015F | 38DA | F51F | F0CC |
| KIi1 | 5623 | 3CFF | C725 | 7203 | 4116 | 830F | 8353 | 0B3E |
| KIi2 | 0B3E | 5623 | 3CFF | C725 | 7203 | 4116 | 830F | 8353 |
| KIi3 | 7203 | 4116 | 830F | 8353 | 0B3E | 5623 | 3CFF | C725 |

Input: 62A54098 1BA6F9B7

Round 1

FL1(62A54098,806A,8353)->E51240D8

FO1(E51240D8)->B2CC3045

FI11(280A,5623)->CED6

seven 0A-> 3F-> 40-> 6B-> 31-> 67

nine 050->1F5->1FF->1DC->0BD->0D6

FI12(275E,0B3E)->3CC2

seven 5E-> 1C-> 62-> 67-> 5C-> 1E

nine 04E->120->17E->040->0A5->0C2

FI13(B820,7203)->8289

seven 20-> 35-> 0B-> 32-> 48-> 41

nine 170->19E->1BE->1BD->0BB->089

Round 2

FO2(A96AC9F2)->A4AC83B6

FI21(F66B,3CFF)->0F18

seven 6B-> 31-> 7F-> 61-> 1F-> 07

nine 1EC->125->14E->1B1->179->118

FI22(B843,5623)->6246

seven 43-> 0B-> 56-> 7D-> 77-> 31

nine 170->19E->1DD->1FE->03B->046

FI23(AEE8,4116)->271A

seven 68-> 25-> 01-> 21-> 09-> 13

nine 15D->14C->124->032->13B->11A

FL2(A4AC83B6,8CD1,0B3E)->B3D38AB7

Round 3

FL3(D176CA2F,15F0,5623)->2CA9E8CF

FO3(2CA9E8CF)->C1983ADB

FI31(F691,C725)->4756

seven 11-> 71-> 23-> 40-> 75-> 23

nine 1ED->143->152->077->116->156

FI32(FB8F,3CFF)->6E01

seven 0F-> 21-> 1E-> 00-> 36-> 37

nine 1F7->1B0->1BF->140->001->001

FI33(079F,830F)->FB43

seven 1F-> 51-> 43-> 02-> 3E-> 7D

nine 00F->18D->192->09D->141->143

Round 4

FO4(68F2F329)->3279F0E1

FI41(7707,7203)->54CC

seven 07-> 60-> 59-> 60-> 66-> 2A

nine 0EE->03E->039->03A->0AC->0CC

FI42(C669,C725)->959C

seven 69-> 4A-> 29-> 4A-> 56-> 4A

nine 18C->08A->0E3->1C6->1D6->19C

FI43(BF28,8353)->C298

seven 28-> 65-> 63-> 22-> 79-> 61

nine 17E->12E->106->055->0BA->098

FL4(3279F0E1,8DA3,3CFF)->CB86F0A3

Round 5

FL5(1AF03A8C,51FF,C725)->A42B1B6C

FO5(A42B1B6C)->A62197C6

FI51(68DB,4116)->06CF

seven 5B-> 67-> 62-> 42-> 4C-> 03

nine 0D1->0DE->085->193->08D->0CF

FI52(73AA,7203)->BB82

seven 2A-> 28-> 6D-> 54-> 5F-> 5D

nine 0E7->1EF->1C5->1C6->1D6->182

FI53(1CFC,0B3E)->31E7

seven 7C-> 58-> 2C-> 29-> 7F-> 18

nine 039->108->174->04A->1CE->1E7

Round 6

FO6(CED364EF)->D6DA665D

FI61(E0E5,830F)->A727

seven 65-> 04-> 00-> 41-> 74-> 53

nine 1C1->161->104->00B->166->127

FI62(9CE5,4116)->1512

seven 65-> 04-> 53-> 73-> 18-> 0A

nine 139->0B2->0D7->1C1->161->112

FI63(FB12,5623)->B087

seven 12-> 27-> 7F-> 54-> 5F-> 58

nine 1F6->0CA->0D8->0FB->0D3->087

FL6(D6DA665D,0CCF,7203)->294C6FC9

Round 7

FL7(33BC5545,62E3,4116)->91921005

FO7(91921005)->484393F4

FI71(93FA,8353)->82E2

seven 7A-> 0F-> 1B-> 5A-> 23-> 41

nine 127->0EE->094->1C7->0B8->0E2

FI72(C1C3,830F)->DAA4

seven 43-> 0B-> 58-> 19-> 49-> 6D

nine 183->090->0D3->1DC->0BD->0A4

FI73(67F8,3CFF)->DBB7

seven 78-> 2A-> 48-> 56-> 5A-> 6D

nine 0CF->11A->162->19D->1E1->1B7

Round 8

FO8(8690F71B)->B971E5E3

FI81(8038,0B3E)->79B9

seven 38-> 4D-> 56-> 53-> 05-> 3C

nine 100->023->01B->125->1EA->1B9

FI82(08B3,8353)->37D3

seven 33-> 3D-> 73-> 32-> 48-> 1B

nine 011->0FD->0CE->19D->1E1->1D3

FI83(7E6E,C725)->5C92

seven 6E-> 73-> 46-> 25-> 3C-> 2E

nine 0FC->15B->135->010->0B7->092

FL8(B971E5E3,8026,830F)->762EE5A2

Output: 4592B0E7 8690F71B

## 3.6 Test Set 4

This test ensures that all entries in the two S-boxes are correct. It does this by ensuring that every S-box entry is used at least once during the running of the test set.

For a fixed key an initial input value, the algorithm is executed 50 times. The first encryption operates on the given input data. Each subsequent encryption takes the output of the previous encryption as its input data. After 50 operations the output should be as shown below.

Iterated test for full S-box coverage

Key = 3A 3B 39 B5 C3 F2 37 6D 69 F7 D5 46 E5 F8 5D 43

Input = CA 49 C1 C7 57 71 AB 0B

After 50 repeated encryptions

Output = 73 8B AD 4C 4A 69 08 02

# 4 Confidentiality algorithm *f8*

## 4.1 Overview

The test data sets presented here are for the ***f8*** confidentiality algorithm. No detailed data is presented for the internal states of **KASUMI** as that is covered in Clause 3.

## 4.2 Format

Each test set starts by showing the various inputs to the algorithm including the data stream to be encrypted/decrypted. (The length field is in decimal). This is followed by:

the initial value of the variable **A**.

the modified key used in the calculation **KASUMI[ A ]CK  MK**

the result of the above operation.

Thereafter four columns of data are shown.

**Column 1** shows the value of the block counter **BLKCNT**.

**KASUMI Input** shows the input to the **KASUMI** block cipher. i.e. it is the bit-wise exclusive-or of the data in column 1 with the previous block of keystream and with the modified value of **A**.

**Keystream** shows the 64-bit output from **KASUMI.**

**Enc/dec data** shows the modified input data, i.e. it is the bit-wise exclusive-or of the corresponding keystream and the input data to the algorithm. As this is a stream cipher it is purely a matter of context whether the operation is regarded as "encryption" or "decryption".

## 4.3 Test Set 1

Key = 2BD6459F82C5B300952C49104881FF48

Count = 72A4F20F

Bearer = 0C

Direction = 1

Length = 798 bits

Plaintext:

7EC61272743BF161 4726446A6C38CED1 66F6CA76EB543004 4286346CEF130F92

922B03450D3A9975 E5BD2EA0EB55AD8E 1B199E3EC4316020 E9A1B285E7627953

59B7BDFD39BEF4B2 484583D5AFE082AE E638BF5FD5A60619 3901A08F4AB41AAB

9B134880

Initial A = 72A4F20F64000000

Key used = 7E8310CAD790E655C0791C451DD4AA1D

Modified A = 34222BC8F7C39416

Key now = 2BD6459F82C5B300952C49104881FF48

BLKCNT Kasumi input Keystream enc/dec data

0 34222BC8F7C39416 AF24CC029AC39D08 D1E2DE70EEF86C69

1 9B06E7CA6D00091F 23DD1041AEECAE7B 64FB542BC2D460AA

2 17FF3B89592F3A6F D95CDAD24BC7162F BFAA10A4A093262B

3 ED7EF11ABC04823A 3F9FAA1C80D1DB1B 7D199E706FC2D489

4 0BBD81D477124F09 87782A2C1DC93006 1553296910F3A973

5 B35A01E4EA0AA415 E49BAC44F71B868C 012682E41C4E2B02

6 D0B9878C00D8129C A5398989E10ADFB3 BE2017B7253BBF93

7 911BA24116C94BA2 E07FEA9C2C20914A 09DE5819CB42E819

8 D45DC154DBE30554 0F437466F0C8A81D 56F4C99BC9765CAF

9 3B615FAE070B3C02 1BF4536E2D9900C4 53B1D0BB8279826A

10 2FD678A6DA5A94D8 3D84EA7D3CB3C739 DBBC5522E915C120

11 09A6C1B5CB705324 9F190528BF5C8DA3 A618A5A7F5E89708

12 AB3B2EE0489F19B9 082A2D8F25915EE3 9339650F

## 4.4 Test Set 2

Key = EFA8B2229E720C2A7C36EA55E9605695

Count = E28BCF7B

Bearer = 18

Direction = 0

Length = 510 bits

Plaintext:

10111231E060253A 43FD3F57E37607AB 2827B599B6B1BBDA 37A8ABCC5A8C550D

1BFB2F494624FB50 367FA36CE3BC68F1 1CF93B1510376B02 130F812A9FA169D8

Initial A = E28BCF7BC0000000

Key used = BAFDE777CB27597F2963BF00BC3503C0

Modified A = 1C05EA5F90964036

Key now = EFA8B2229E720C2A7C36EA55E9605695

BLKCNT Kasumi input Keystream enc/dec data

0 1C05EA5F90964036 2DFBDE4DF5E23990 3DEACC7C15821CAA

1 31FE3412657479A7 CA13F589782DD4CA 89EECADE9B5BD361

2 D6161FD6E8BB94FE 63F77DD82BC0B85F 4BD0C8419D710385

3 7FF29787BB56F86A EA16F385B597F957 DDBE5849EF1BAC5A

4 F61319DA2501B965 F34A65124C43BA02 E8B14A5B0A674152

5 EF4F8F4DDCD5FA31 28CB43675A509B18 1EB4E00BB9ECF3E9

6 34CEA938CAC6DB28 EB3582DFF77639D5 F7CCB9CAE74152D7

7 F730688067E079E4 E7ED211E294B6934 F4E2A034B6EA00EC

## 4.5 Test Set 3

Key = 5ACB1D644C0D51204EA5F1451010D852

Count = FA556B26

Bearer = 03

Direction = 1

Length = 120 bits

Plaintext:

AD9C441F890B38C4 57A49D421407E8

Initial A = FA556B261C000000

Key used = 0F9E4831195804751BF0A41045458D07

Modified A = 3E5A6D0A3D1C82A5

Key now = 5ACB1D644C0D51204EA5F1451010D852

BLKCNT Kasumi input Keystream enc/dec data

0 3E5A6D0A3D1C82A5 365568B78ACD43EC 9BC92CA803C67B28

1 080F05BDB7D1C148 F6BED6AC4E0BCD5F A11A4BEE5A0C25

## 4.6 Test Set 4

Key = D3C5D592327FB11C4035C6680AF8C6D1

Count = 398A59B4

Bearer = 05

Direction = 1

Length = 253 bits

Plaintext:

981BA6824C1BFB1A B485472029B71D80 8CE33E2CC3C0B5FC 1F3DE8A6DC66B1F0

Initial A = 398A59B42C000000

Key used = 869080C7672AE4491560933D5FAD9384

Modified A = F04B50A2A852469C

Key now = D3C5D592327FB11C4035C6680AF8C6D1

BLKCNT Kasumi input Keystream enc/dec data

0 F04B50A2A852469C C3A2E599FDF270CB 5BB9431BB1E98BD1

1 33E9B53B55A03656 AF169C5C14F20EE5 1B93DB7C3D451365

2 5F5DCCFEBCA0487B D558B88E566A95B2 59BB86A295AA204E

3 2513E82CFE38D32D D4D61E517976A4E2 CBEBF6F7A5101512

## 4.7 Test Set 5

Key = 6090EAE04C83706EECBF652BE8E36566

Count = 72A4F20F

Bearer = 09

Direction = 0

Length = 837 bits

Plaintext:

40981BA6824C1BFB 4286B299783DAF44 2C099F7AB0F58D5C 8E46B104F08F01B4

1AB485472029B71D 36BD1A3D90DC3A41 B46D51672AC4C966 3A2BE063DA4BC8D2

808CE33E2CCCBFC6 34E1B259060876A0 FBB5A437EBCC8D31 C19E4454318745E3

987645987A986F2C B0

Initial A = 72A4F20F48000000

Key used = 35C5BFB519D6253BB9EA307EBDB63033

Modified A = 1EDF994571692FEA

Key now = 6090EAE04C83706EECBF652BE8E36566

BLKCNT Kasumi input Keystream enc/dec data

0 1EDF994571692FEA 9D2B7F7BA8E2D9B6 DDB364DD2AAEC24D

1 83F4E63ED98BF65D BDAFABCECFB60242 FF291957B78BAD06

2 A370328BBEDF2DAA 16CCE6B720B437E2 3AC579CD9041BABE

3 08137FF251DD180B 07BBA858F5F7CA2B 89FD195C0578CB9F

4 1964311D849EE5C5 C4F692114151651F DE4217566178D202

5 DA290B5430384AF0 769D773A5F7A23AD 40206D07CFA619EC

6 6842EE7F2E130C41 B1F232366E9D3576 059F63514459FC10

7 AF2DAB731FF41A9B EE0629F0941D2312 D42DC9934E56EBC0

8 F0D9B0B5E5740CF0 4B4AEE73013DCBB1 CBC60D4D2DF17477

9 559577367054E452 785C7F04A2AB2691 4CBDCD5DA4A35031

10 6683E641D3C20971 81CAB6D67F58FCC9 7A7F12E1949471F8

11 9F152F930E31D328 630BB626D7088592 A295F272E68FC071

12 7DD42F63A661AA74 C1C6381657BE8B75 59B07D8E2D26E459

13 DF19A15326D7A492 2E1EA0BF8D97DA88 9E

# 5 Integrity algorithm *f9*

## 5.1 Overview

The test data sets presented here are for the ***f9*** integrity algorithm. No detailed data is presented for the internal states of **KASUMI** as that is covered in Clause 3.

## 5.2 Format

The test data set shows the input values to the algorithm.

Following this it shows four columns of data; input, **KASUMI** input, **KASUMI** output and the cumulative exclusive-OR where:

**Input** is the plain text input block that is being hashed. It commences with the value **COUNT || FRESH** and is followed by the **MESSAGE**. The final input block includes the **DIRECTION** bit and the padding.

**KASUMI Input** is the input value to the block cipher. In the first line this is **COUNT || FRESH**, subsequently it is the XOR of the plain text block and the previous output from **KASUMI**.

**KASUMI Output** is the output of the block cipher

**Accumulated XOR** is the XOR of all the output of all the **KASUMI** operations performed up to that point.

Finally the modified key is shown along with the input and output data from the last application of **KASUMI**.

## 5.3 Test Set 1

Key = 2BD6459F82C5B300952C49104881FF48

Count = 38A6F056

Fresh = 05D2EC49

Direction = 0

Length = 189 bits

Message:

6B227737296F393C 8079353EDC87E2E8 05D2EC49A4F2D8E0

Input Kasumi input Kasumi Output Accumulated XOR

38A6F05605D2EC49 38A6F05605D2EC49 89E0A6D036C17090 89E0A6D036C17090

6B227737296F393C E2C2D1E71FAE49AC 45C16C0142460205 CC21CAD174877295

8079353EDC87E2E8 C5B8593F9EC1E0ED E24CFA7D8471E4DD 2E6D30ACF0F69648

05D2EC49A4F2D8E2 E79E163420833C3F DFD3DCB9499275BA F1BEEC15B964E3F2

New Key: 817CEF35286F19AA3F86E3BAE22B55E2

final step: F1BEEC15B964E3F2 F63BD72C702EBC7A

MAC-I: F63BD72C

## 5.4 Test Set 2

Key = D42F682428201CAFCD9F97945E6DE7B7

Count = 3EDC87E2

Fresh = A4F2D8E2

Direction = 1

Length = 254 bits

Message::

B5924384328A4AE0 0B737109F8B6C8DD 2B4DB63DD533981C EB19AAD52A5B2BC0

Input Kasumi input Kasumi Output Accumulated XOR

3EDC87E2A4F2D8E2 3EDC87E2A4F2D8E2 3541B47339DD4168 3541B47339DD4168

B5924384328A4AE0 80D3F7F70B570B88 52EC81194ECEDDA0 67AD356A77139CC8

0B737109F8B6C8DD 599FF010B678157D 792BFE1F07A1A8B0 1E86CB7570B23478

2B4DB63DD533981C 52664822D29230AC C92F7E2C38D22B6D D7A9B55948601F15

EB19AAD52A5B2BC3 2236D4F9128900AE 4C2BEF9C82233403 9B825AC5CA432B16

New Key: 7E85C28E828AB60567353D3EF4C74D1D

final step: 9B825AC5CA432B16 A9DAF1FF12F71DE7

MAC-I: A9DAF1FF

## 5.5 Test Set 3

Key = FDB9CFDF28936CC483A31869D81B8FAB

Count = 36AF6144

Fresh = 9838F03A

Direction = 1

Length = 319 bits

Message::

5932BC0ACE2B0ABA 33D8AC188AC54F34 6FAD10BF9DEE2920 B43BD0C53A915CB7

DF6CAA72053ABFF2

Input Kasumi input Kasumi Output Accumulated XOR

36AF61449838F03A 36AF61449838F03A DDA7EAA292B010EC DDA7EAA292B010EC

5932BC0ACE2B0ABA 849556A85C9B1A56 3D65F1EB61544622 E0C21B49F3E456CE

33D8AC188AC54F34 0EBD5DF3EB910916 1D62D61E5ED97431 FDA0CD57AD3D22FF

6FAD10BF9DEE2920 72CFC6A1C3375D11 14C968BAC4F8A2A5 E969A5ED69C5805A

B43BD0C53A915CB7 A0F2B87FFE69FE12 6D0132521C61A552 846897BF75A42508

DF6CAA72053ABFF3 B26D9820195B1AA1 BF04729B5C03EA98 3B6CE52429A7CF90

8000000000000000 3F04729B5C03EA98 8B0C8BE27C74D17F B0606EC655D31EEF

New Key: 571365758239C66E2909B2C372B12501

final step: B0606EC655D31EEF 1537D316633A8831

MAC-I: 1537D316

## 5.6 Test Set 4

Key = C736C6AAB22BFFF91E2698D2E22AD57E

Count = 14793E41

Fresh = 0397E8FD

Direction = 1

Length = 384 bits

Message::

D0A7D463DF9FB2B2 78833FA02E235AA1 72BD970C1473E129 07FB648B6599AAA0

B24A038665422B20 A499276A50427009

Input Kasumi input Kasumi Output Accumulated XOR

14793E410397E8FD 14793E410397E8FD FB6A5FB59EA91B57 FB6A5FB59EA91B57

D0A7D463DF9FB2B2 2BCD8BD64136A9E5 DDF60F296850AE54 269C509CF6F9B503

78833FA02E235AA1 A57530894673F4F5 FAB7664A7F2447E7 DC2B36D689DDF2E4

72BD970C1473E129 880AF1466B57A6CE E6443647E1289007 3A6F009168F562E3

07FB648B6599AAA0 E1BF52CC84B13AA7 DA29900832EA4C7C E04690995A1F2E9F

B24A038665422B20 6863938E57A8675C 74C2F5B8172E361D 948465214D311882

A499276A50427009 D05BD2D2476C4614 79AA12C36369E686 ED2E77E22E58FE04

C000000000000000 B9AA12C36369E686 A464F43DEE74E0C7 494A83DFC02C1EC3

New Key: 6D9C6C0018815553B48C327848807FD4

final step: 494A83DFC02C1EC3 DD7DFADDD68D1EC1

MAC-I: DD7DFADD

## 5.7 Test Set 5

Key = F4EBEC69E73EAF2EB2CF6AF4B3120FFD

Count = 296F393C

Fresh = 6B227737

Direction = 1

Length = 1000 bits

Message::

10BFFF839E0C7165 8DBB2D1707E14572 4F41C16F48BF403C 3B18E38FD5D1663B

6F6D900193E3CEA8 BB4F1B4F5BE82203 2232A78D7D75238D 5E6DAECD3B4322CF

59BC7EA84AB18811 B5BFB7BC553F4FE4 4478CE287A148799 90D18D12CA79D2C8

55149021CD5CE8CA 0371CA04FCCE143E 3D7CFEE94585B588 5CAC46068B

Input Kasumi input Kasumi Output Accumulated XOR

296F393C6B227737 296F393C6B227737 47F6AA9B15F7A617 47F6AA9B15F7A617

10BFFF839E0C7165 574955188BFBD772 6C7C71FDE9AA2B8D 2B8ADB66FC5D8D9A

8DBB2D1707E14572 E1C75CEAEE4B6EFF 690286906D3EBABE 42885DF691633724

4F41C16F48BF403C 264347FF2581FA82 942B65C8198AB936 D6A3383E88E98E12

3B18E38FD5D1663B AF338647CC5BDF0D 5052A81A1A059BB0 86F1902492EC15A2

6F6D900193E3CEA8 3F3F381B89E65518 E40F45A22B41B05F 62FED586B9ADA5FD

BB4F1B4F5BE82203 5F405EED70A9925C 91C00F497A1A8199 F33EDACFC3B72464

2232A78D7D75238D B3F2A8C4076FA214 DEF053FB4EB23FEA 2DCE89348D051B8E

5E6DAECD3B4322CF 809DFD3675F11D25 BEC94AAFFE3723CC 9307C39B73323842

59BC7EA84AB18811 E7753407B486ABDD 9BD4CB606985127E 08D308FB1AB72A3C

B5BFB7BC553F4FE4 2E6B7CDC3CBA5D9A D5D5A8EECD518F4E DD06A015D7E6A572

4478CE287A148799 91AD66C6B74508D7 17B9203FC35C9882 CABF802A14BA3DF0

90D18D12CA79D2C8 8768AD2D09254A4A 206A3693096F30E7 EAD5B6B91DD50D17

55149021CD5CE8CA 757EA6B2C433D82D CF23D21C256066E9 25F664A538B56BFE

0371CA04FCCE143E CC521818D9AE72D7 C2D40AFABC92E2FE E7226E5F84278900

3D7CFEE94585B588 FFA8F413F9175776 699D61BDD036A7E5 8EBF0FE254112EE5

5CAC46068BC00000 353127BB5BF6A7E5 E3D8AE061C3A3C87 6D67A1E4482B1262

New Key: 5E4146C34D9405841865C05E19B8A557

final step: 6D67A1E4482B1262 C383839D93FFC6D1

MAC-I: C383839D

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 12-1999 | - | - | - | - | ETSI SAGE Publication (restricted) | - | SAGE v1.0 |
| 09-2000 | SA\_07 |  |  |  | Approved by TSG SA and placed under change control | SAGE v1.0 | 3.1.0 |
| 07-2001 | - | - | - | - | Word version received: Re-formatted into 3GPP TS format (MCC) No technical change from version 3.1.0. | 3.1.0 | 3.1.1 |
| 08-2001 | - |  |  |  | Addition of Mitsubishi IPR information in Foreword and correction of reference titles. No technical change from version 3.1.0. | 3.1.1 | 3.1.2 |
| 08-2001 | - | - | - | - | Release 4 version created. | 3.1.2 | 4.0.0 |
| 06-2002 | - | - | - | - | Release 5 version created. | 4.0.0 | 5.0.0 |
| 12-2004 | SP-26 | - | - | - | Release 6 version created. | 5.0.0 | 6.0.0 |
| 06-2007 | SP-36 | - | - | - | Release 7 version created. | 6.0.0 | 7.0.0 |
| 12-2008 | SP-42 | - | - | - | Release 8 version created | 7.0.0 | 8.0.0 |
| 2009-12 | - | - | - | - | Release 9 version created | 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** |
| 2018-06 | - | - | - | - | Update to Rel-15 version (MCC) | 14.0.0 | **15.0.0** |
| 2020-07 | - | - | - | - | Update to Rel-16 version (MCC) | 15.0.0 | **16.0.0** |