

Second edition  
2011-03-01

---

---

## Information technology — Security techniques — Message Authentication Codes (MACs) —

### Part 1: Mechanisms using a block cipher

*Technologies de l'information — Techniques de sécurité — Codes d'authentification de message (MAC) —*

*Partie 1: Mécanismes utilisant un chiffrement par blocs*

---

---

Reference number  
ISO/IEC 9797-1:2011(E)



This is a preview of "ISO/IEC 9797-1:2011". [Click here to purchase the full version from the ANSI store.](#)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO/IEC 9797-1:2011". Click here to purchase the full version from the ANSI store.

## Contents

Page

Foreword .....	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions .....	1
4 Symbols and notation .....	3
5 Requirements.....	4
6 Model for MAC algorithms.....	5
6.1 General .....	5
6.2 Step 1 (key derivation) .....	6
6.2.1 General .....	6
6.2.2 Key Derivation Method 1.....	6
6.2.3 Key Derivation Method 2.....	7
6.3 Step 2 (padding) .....	7
6.3.1 General .....	7
6.3.2 Padding Method 1.....	7
6.3.3 Padding Method 2.....	7
6.3.4 Padding Method 3.....	7
6.3.5 Padding Method 4.....	8
6.4 Step 3 (splitting) .....	8
6.5 Step 4 (iteration) .....	8
6.6 Step 5 (final iteration).....	8
6.6.1 General .....	8
6.6.2 Final iteration 1 .....	8
6.6.3 Final iteration 2 .....	8
6.6.4 Final iteration 3 .....	9
6.7 Step 6 (output transformation).....	9
6.7.1 General .....	9
6.7.2 Output Transformation 1 .....	9
6.7.3 Output Transformation 2 .....	9
6.7.4 Output Transformation 3 .....	9
6.8 Step 7 (truncation).....	9
7 MAC algorithms .....	9
7.1 General .....	9
7.2 MAC Algorithm 1 .....	10
7.3 MAC Algorithm 2 .....	10
7.4 MAC Algorithm 3 .....	11
7.5 MAC Algorithm 4 .....	12
7.6 MAC Algorithm 5 .....	13
7.7 MAC Algorithm 6 .....	14
Annex A (normative) Object identifiers .....	16
Annex B (informative) Examples .....	19
B.1 General .....	19
B.2 MAC Algorithm 1 .....	20
B.3 MAC Algorithm 2 .....	22
B.4 MAC Algorithm 3 .....	23
B.5 MAC Algorithm 4 .....	24

This is a preview of "ISO/IEC 9797-1:2011". [Click here to purchase the full version from the ANSI store.](#)

<b>B.6</b>	<b>MAC Algorithm 5</b> .....	<b>26</b>
<b>B.6.1</b>	<b>Examples of MAC generation process</b> .....	<b>26</b>
<b>B.6.2</b>	<b>AES using a 128-bit key</b> .....	<b>27</b>
<b>B.6.3</b>	<b>AES using a 192-bit key</b> .....	<b>27</b>
<b>B.6.4</b>	<b>AES using a 256-bit key</b> .....	<b>27</b>
<b>B.6.5</b>	<b>Three-key triple DEA</b> .....	<b>28</b>
<b>B.6.6</b>	<b>Two-key triple DEA</b> .....	<b>28</b>
<b>B.7</b>	<b>MAC Algorithm 6</b> .....	<b>29</b>
<b>B.7.1</b>	<b>Examples of MAC generation process</b> .....	<b>29</b>
<b>B.7.2</b>	<b>AES using a 128-bit key</b> .....	<b>29</b>
<b>B.7.3</b>	<b>AES using a 192-bit key</b> .....	<b>29</b>
<b>B.7.4</b>	<b>AES using a 256-bit key</b> .....	<b>30</b>
<b>Annex C</b>	<b>(informative) A security analysis of the MAC algorithms</b> .....	<b>31</b>
<b>C.1</b>	<b>General</b> .....	<b>31</b>
<b>C.2</b>	<b>Rationale</b> .....	<b>33</b>
<b>Annex D</b>	<b>(informative) A comparison with previous MAC algorithm standards</b> .....	<b>38</b>
<b>Bibliography</b>	.....	<b>39</b>

This is a preview of "ISO/IEC 9797-1:2011". [Click here to purchase the full version from the ANSI store.](#)

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 9797-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9797-1:1999), which has been technically revised. MAC Algorithms 5 and 6 of ISO/IEC 9797-1:1999, which consisted of two single CBC-MAC computations, have been replaced by two other MAC algorithms, which perform single CBC-MAC computations and which offer improved efficiency. Annex A on object identifiers has been added. The security analysis in Annex C has been updated and Annex D on the relationship to previous standards has been added.

ISO/IEC 9797 consists of the following parts, under the general title *Information technology — Security techniques — Message Authentication Codes (MACs)*:

- *Part 1: Mechanisms using a block cipher*
- *Part 2: Mechanisms using a dedicated hash-function*
- *Part 3: Mechanisms using a universal hash-function*

Further parts may follow.

## Introduction

In an IT environment, it is often required that one can verify that electronic data has not been altered in an unauthorized manner and that one can provide assurance that a message has been originated by an entity in possession of the secret key. A MAC (Message Authentication Code) algorithm is a commonly used data integrity mechanism that can satisfy these requirements.

This part of ISO/IEC 9797 specifies six MAC algorithms that are based on an  $n$ -bit block cipher. They compute a short string as a function of a secret key and a message of variable length.

The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits)  $k^*$  and secrecy of the key, on the block length (in bits)  $n$  and strength of the block cipher, on the length (in bits)  $m$  of the MAC, and on the specific mechanism.

The first mechanism specified in this part of ISO/IEC 9797 is commonly known as CBC-MAC (CBC is an abbreviation of Cipher Block Chaining).

The other five mechanisms are variants of CBC-MAC. MAC Algorithms 2, 3, 5 and 6 apply a special transformation at the end of the processing. MAC Algorithm 6 is an optimized variant of MAC Algorithm 2. MAC Algorithm 5 uses the minimum number of encryptions. MAC Algorithm 5 requires only a single block cipher key setup but it needs a longer internal key. MAC Algorithm 4 applies a special transformation at both the beginning and the end of the processing; this algorithm is recommended for use in applications which require that the key length of the MAC algorithm be twice that of the block cipher.