



JAPANESE  
INDUSTRIAL  
STANDARD

Translated and Published by  
Japanese Standards Association

---

---

**JIS X 5055-1** : 2003

(ISO/IEC 9797-1 : 1999)

**Information technology—  
Security techniques—Message  
Authentication Codes (MACs)—  
Part 1 : Mechanisms using  
a block cipher**

---

ICS 35.040

Reference number : JIS X 5055-1 : 2003 (E)

PROTECTED BY COPYRIGHT



**Documents**

Document \$5.8  
Sharing Hub

## Foreword

This translation has been made based on the original Japanese Industrial Standard established by the Minister of Economy, Trade and Industry through deliberations at the Japanese Industrial Standards Committee based on the Industrial Standardization Law.

This establishment is made based on **ISO/IEC 9797-1 : 1999** *Information technology—Security techniques—Message Authentication Codes (MACs)—Part 1 : Mechanisms using a block cipher* in order to facilitate the comparison between Japanese Industrial Standard and International Standard, the development of Japanese Industrial Standard identical with International Standard and the proposal of the draft of International Standard based on Japanese Industrial Standard.

Attention shall be drawn to the possibility that some parts of this Standard may conflict with a patent right, application for a patent after opening to the public, utility model right or application for registration of utility model after opening to the public which have technical properties. The Minister of Economy, Trade and Industry and the Japanese Industrial Standards Committee are not responsible for identifying the patent right, application for a patent after opening to the public, utility model right or application for registration of utility model after opening to the public which have the said technical properties.

**JIS X 5055** consists of the following 2 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.*

Date of Establishment: 2003-09-20

Date of Public Notice in Official Gazette: 2003-09-22

Investigated by: Japanese Industrial Standards Committee  
Standards Board  
Technical Committee on Information  
Technology

---

JIS X 5055-1 : 2003, First English edition published in 2004-02

Translated and published by: Japanese Standards Association  
4-1-24, Akasaka, Minato-ku, Tokyo, 107-8440 JAPAN

---

In the event of any doubts arising as to the contents,  
the original JIS is to be the final authority.

© JSA 2004

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 the publisher.

Printed in Japan

## Contents

|                                                                       | Page |
|-----------------------------------------------------------------------|------|
| Introduction .....                                                    | 1    |
| 1 Scope .....                                                         | 1    |
| 2 Normative references .....                                          | 2    |
| 3 Definitions .....                                                   | 2    |
| 4 Symbols and notation .....                                          | 2    |
| 5 Requirements .....                                                  | 2    |
| 6 Model for MAC algorithms .....                                      | 2    |
| 7 MAC algorithms .....                                                | 2    |
| Annex A (informative) Examples .....                                  | 2    |
| Annex B (informative) A security analysis of the MAC algorithms ..... | 2    |
| Bibliography .....                                                    | 2    |
| Annex 1 (informative) ISO/IEC 9797-1 : 1999 .....                     | 3    |

# Information technology— Security techniques— Message Authentication Codes (MACs)— Part 1 : Mechanisms using a block cipher

**Introduction** This part of **JIS X 5055** has been prepared by summarizing the first edition of **ISO/IEC 9797-1** *Information technology—Security techniques—Message Authentication Codes (MACs)—Part 1 : Mechanisms using a block cipher* published in 1999 without any modification in technical contents. For the clause 1, the same clause of the original International Standard is entirely adopted, and for the clause 2 and subsequent clauses, the contents of the same clause of the original International Standard are referred to them, respectively.

**1 Scope** This part of **JIS X 5055** specifies six MAC algorithms that use a secret key and an  $n$ -bit block cipher to calculate an  $m$ -bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorised manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. 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 three mechanisms specified in this part of **JIS X 5055** are commonly known as CBC-MAC (CBC is the abbreviation of Cipher Block Chaining). The calculation of a MAC as described in **ISO 8731-1** and **ANSI X9.9** is a specific case of this part of **JIS X 5055** when  $n = 64$ ,  $m = 32$ , MAC Algorithm 1 and Padding Method 1 are used, and the block cipher is DEA (**ANSI X3.92** : 1981). The calculation of a MAC as described in **ANSI X9.19** and **ISO 9807** is a specific case of this part of **JIS X 5055** when  $n = 64$ ,  $m = 32$ , either MAC Algorithm 1 or MAC Algorithm 3 is used (both with Padding Method 1), and the block cipher is DEA (**ANSI X3.92** : 1981).

The fourth mechanism is a variant of CBC-MAC with a special initial transformation. It is recommended for applications which require that the key length of the MAC algorithm is twice that of the block cipher.

- Notes
- 1 For example, in the case of DEA (**ANSI X3.92** : 1981), the block cipher key length is 56 bits, while the MAC algorithm key length is 112 bits.
  - 2 When used with DEA (which is also known as DES), this algorithm is called MacDES.

The fifth and sixth mechanism use two parallel instances of the first and fourth mechanism respectively, and combine the two results with a bitwise exclusive-or operation. They are recommended for applications which require an increased security level against forgery attacks (see Annex B). The fifth mechanism uses a single length MAC algorithm key, while the sixth mechanism doubles the MAC algorithm key length.

This part of **JIS X 5055** can be applied to the security services of any security architecture, process, or application.

Note : The International Standard corresponding to this part of **JIS X 5055** is as follows:

In addition, symbols which denote the degree of correspondence in the contents between the relevant International Standard and **JIS** are IDT (identical), MOD (modified), and NEQ (not equivalent) according to **ISO/IEC Guide 21**.

ISO/IEC 9797-1 : 1999 *Information technology—Security techniques—Message Authentication Codes (MACs)—Part 1 : Mechanisms using a block cipher* (IDT)

**2 Normative references** The normative references shall be in accordance with Clause 2 Normative references of **ISO/IEC 9797-1 : 1999**.

**3 Definitions** The definitions shall be in accordance with Clause 3 Definitions of **ISO/IEC 9797-1 : 1999**.

**4 Symbols and notation** The symbols and notation shall be in accordance with Clause 4 Symbols and notation of **ISO/IEC 9797-1 : 1999**.

**5 Requirements** The requirements shall be in accordance with Clause 5 Requirements of **ISO/IEC 9797-1 : 1999**.

**6 Model for MAC algorithms** The model for MAC algorithms shall be in accordance with Clause 6 Model for MAC algorithms of **ISO/IEC 9797-1 : 1999**.

**7 MAC algorithms** The MAC algorithms shall be in accordance with Clause 7 MAC algorithms of **ISO/IEC 9797-1 : 1999**.

**Annex A (informative) Examples** The examples shall be in accordance with Annex A (informative) Examples of **ISO/IEC 9797-1 : 1999**.

**Annex B (informative) A security analysis of the MAC algorithms** The security analysis of the MAC algorithms shall be in accordance with Annex B (informative) A security analysis of the MAC algorithms of **ISO/IEC 9797-1 : 1999**.

**Bibliography** The bibliography shall be in accordance with Bibliography of **ISO/IEC 9797-1 : 1999**.

**Annex 1 (informative)**  
**ISO/IEC 9797-1 : 1999**

Information technology—Security techniques—Message Authentication Codes  
(MACs)—Part 1 : Mechanisms using a block cipher.

This Annex (informative) does not constitute provisions of this Standard.

# INTERNATIONAL STANDARD

# ISO/IEC 9797-1

First edition  
1999-12-15

---

## 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 (MACs) —*

*Partie 1: Mécanismes utilisant un cryptogramme bloc*

---

Reference number  
ISO/IEC 9797-1:1999(E)



© ISO/IEC 1999

PROTECTED BY COPYRIGHT

**ISO/IEC 9797-1:1999(E)****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.

© ISO/IEC 1999

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 22 734 10 79  
E-mail [copyright@iso.ch](mailto:copyright@iso.ch)  
Web [www.iso.ch](http://www.iso.ch)

Printed in Switzerland

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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 part of ISO/IEC 9797 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

This first edition of ISO/IEC 9797-1, together with the subsequent parts of ISO/IEC 9797, cancels and replaces ISO/IEC 9797:1994, which has been revised and extended to a multi-part standard. Note, however, that implementations which comply with ISO/IEC 9797:1994 will be compliant with this edition of ISO/IEC 9797-1.

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 hash-function*

Further parts may follow.

Annexes A and B of this part of ISO/IEC 9797 are for information only.