



JAPANESE
INDUSTRIAL
STANDARD

Translated and Published by
Japanese Standards Association

JIS X 5055-2 : 2003

(ISO/IEC 9797-2 : 2002)

**Information technology—
Security techniques—Message
Authentication Codes (MACs)—
Part 2 : Mechanisms using
a dedicated hash-function**

ICS 35.040

Reference number : JIS X 5055-2 : 2003 (E)

PROTECTED BY COPYRIGHT

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 9797-2 : 2002** *Information technology—Security techniques—Message Authentication Codes (MACs)—Part 2 : Mechanisms using a dedicated hash-function* 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 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 5055-2:2003, 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 MAC Algorithm 1	2
7 MAC Algorithm 2	2
8 MAC Algorithm 3	2
Annex A (informative) Examples	2
Annex B (informative) A security analysis of the MAC algorithms	2
Bibliography	2
Annex 1 (informative) ISO/IEC 9797-2 : 2002	3

**Information technology—
Security techniques—
Message Authentication Codes (MACs)—
Part 2 : Mechanisms using a dedicated
hash-function**

Introduction This Japanese Industrial Standard has been prepared by summarizing the first edition of *ISO/IEC 9797-2 Information technology—Security techniques—Message Authentication Codes (MACs)—Part 2 : Mechanisms using a dedicated hash-function* published in 2002 without any modification in technical contents. For clause 1, the same clause of the original International Standard is entirely adopted, and for clause 2 and subsequent clauses, the contents of the same clause of the original International Standard are referred to them, respectively.

1 Scope This Standard specifies three MAC algorithms that use a secret key and a hash-function (or its round-function) with an n -bit result 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 length (in bits) n of a hash-code produced by the hash-function, on the strength of the hash-function, on the length (in bits) m of the MAC, and on the specific mechanism.

The three mechanisms specified in this Standard are based on the dedicated hash-functions specified in **JIS X 5057-3**. The first mechanism is commonly known as MDx-MAC. It calls the complete hash-function once, but it makes a small modification to the round-function by adding a key to the additive constants in the round-function. The second mechanism is commonly known as HMAC. It calls the complete hash-function twice. The third mechanism is a variant of MDx-MAC that takes as input only short strings (at most 256 bits). It offers a higher performance for applications that work with short input strings only.

This Standard can be applied to the security services of any security architecture, process, or application.

Note : The corresponding International Standard to this Standard is as follows:

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

ISO/IEC 9797-2 : 2002 *Information technology—Security techniques—Message Authentication Codes (MACs)—Part 2 : Mechanisms using a dedicated hash-function* (IDT)

2 Normative references The normative references shall be in accordance with Clause 2 Normative references of **ISO/IEC 9797-2 : 2002**.

3 Definitions The definitions shall be in accordance with Clause 3 Terms and definitions of **ISO/IEC 9797-2 : 2002**.

4 Symbols and notation The symbols and notation shall be in accordance with Clause 4 Symbols and notation of **ISO/IEC 9797-2 : 2002**.

5 Requirements The requirements shall be in accordance with Clause 5 Requirements of **ISO/IEC 9797-2 : 2002**.

6 MAC Algorithm 1 The MAC Algorithm 1 shall be in accordance with Clause 6 MAC Algorithm 1 of **ISO/IEC 9797-2 : 2002**.

7 MAC Algorithm 2 The MAC Algorithm 2 shall be in accordance with Clause 7 MAC Algorithm 2 of **ISO/IEC 9797-2 : 2002**.

8 MAC Algorithm 3 The MAC Algorithm 3 shall be in accordance with Clause 8 MAC Algorithm 3 of **ISO/IEC 9797-2 : 2002**.

Annex A (informative) Examples The examples shall be in accordance with Annex A (informative) Examples of **ISO/IEC 9797-2 : 2002**.

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 9797-2 : 2002**.

Bibliography The bibliography shall be in accordance with Bibliography of **ISO/IEC 9797-2 : 2002**.

Annex 1 (informative)
ISO/IEC 9797-2 : 2002

Information technology—Security techniques—Message Authentication Codes
(MACs)—Part 2 : Mechanisms using a dedicated hash-function.

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

INTERNATIONAL STANDARD

ISO/IEC 9797-2

First edition
2002-06-01

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

Part 2: Mechanisms using a dedicated hash-function

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

Partie 2: Mécanismes utilisant une fonction de hachage

Reference number
ISO/IEC 9797-2:2002(E)



© ISO/IEC 2002

PROTECTED BY COPYRIGHT

AVA Documents
Document Sharing Hub

ISO/IEC 9797-2:2002(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 2002

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.ch
Web www.iso.ch

Printed in Switzerland

Contents

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and notation	2
5	Requirements	3
6	MAC Algorithm 1	3
6.1	Description of MAC Algorithm 1	4
6.1.1	Step 1 (key expansion)	4
6.1.2	Step 2 (modification of the constants and the <i>IV</i>)	4
6.1.3	Step 3 (hashing operation)	4
6.1.4	Step 4 (output transformation)	4
6.1.5	Step 5 (truncation)	4
6.2	Efficiency	4
6.3	Computation of the constants	4
6.3.1	Dedicated Hash-Function 1	5
6.3.2	Dedicated Hash-Function 2	5
6.3.3	Dedicated Hash-Function 3	5
7	MAC Algorithm 2	5
7.1	Description of MAC Algorithm 2	6
7.1.1	Step 1 (key expansion)	6
7.1.2	Step 2 (hashing operation)	6
7.1.3	Step 3 (output transformation)	6
7.1.4	Step 4 (truncation)	6
7.2	Efficiency	6
8	MAC Algorithm 3	6
8.1	Description of MAC Algorithm 3	6
8.1.1	Step 1 (key expansion)	6
8.1.2	Step 2 (modification of the constants and the <i>IV</i>)	7
8.1.3	Step 3 (padding)	7
8.1.4	Step 4 (application of the round-function)	7
8.1.5	Step 5 (truncation)	7
8.2	Efficiency	7