
**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)



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 *IV*) 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 *IV*) 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

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 3.

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 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.

ISO/IEC 9797-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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*

Further parts may follow.

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

Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 9797 may involve the use of a patent concerning MAC Algorithm 1 (MDx-MAC) given in Clause 6.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he is willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with the ISO and IEC. Information may be obtained from

Entrust Technologies, Technology Licensing Dept., 750 Heron Road, Ottawa, Ontario, Canada K1V 1A7.

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 other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

1 Scope

This part of ISO/IEC 9797 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 part of ISO/IEC 9797 are based on the dedicated hash-functions specified in ISO/IEC 10118-3. The first mechanism specified in this part of ISO/IEC 9797 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 specified in this part of ISO/IEC 9797 is commonly known as HMAC. It calls the complete hash-function twice. The third mechanism specified in this part of ISO/IEC 9797 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 part of ISO/IEC 9797 can be applied to the security services of any security architecture, process, or application.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9797. For dated refer-

ences, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 9797 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 646:1991, *Information technology — ISO 7-bit coded character set for information interchange*.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*.

ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General*.

ISO/IEC 10118-3:1998, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*.

3 Terms and definitions

3.1 For the purposes of this part of ISO/IEC 9797, the following definitions from ISO/IEC 9797-1 apply.

3.1.1 MAC algorithm key: a key that controls the operation of a MAC algorithm.

3.1.2 Message Authentication Code (MAC): the string of bits which is the output of a MAC algorithm.

NOTE — A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2).

3.1.3 Message Authentication Code (MAC) algorithm: an algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: