

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

## Part 2: Mechanisms using a dedicated hash-function

ICS 35.040

# National foreword

This British Standard reproduces verbatim ISO/IEC 9797-2:2002 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

### Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

**Compliance with a British Standard does not of itself confer immunity from legal obligations.**

### Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii to v, a blank page, pages 1 to 14, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Policy and Strategy Committee on 2 July 2002

© BSI 2 July 2002

### Amendments issued since publication

| Amd. No. | Date | Comments |
|----------|------|----------|
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |

ISBN 0 580 39940 0

---

---

**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*



## Contents

|          |                                                                     |          |
|----------|---------------------------------------------------------------------|----------|
| <b>1</b> | <b>Scope</b>                                                        | <b>1</b> |
| <b>2</b> | <b>Normative references</b>                                         | <b>1</b> |
| <b>3</b> | <b>Terms and denitions</b>                                          | <b>1</b> |
| <b>4</b> | <b>Symbols and notation</b>                                         | <b>2</b> |
| <b>5</b> | <b>Requirements</b>                                                 | <b>3</b> |
| <b>6</b> | <b>MAC Algorithm 1</b>                                              | <b>3</b> |
| 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        |
| <b>7</b> | <b>MAC Algorithm 2</b>                                              | <b>5</b> |
| 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        |
| <b>8</b> | <b>MAC Algorithm 3</b>                                              | <b>6</b> |
| 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        |

## 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.

