AS ISO/IEC 9797.2:2019
ISO/IEC 9797-2:2011

AS ISO/IEC 9797.2:2019



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

Part 2: Mechanisms using a dedicated hash-function



AS ISO/IEC 9797.2:2019

This Australian Standard® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 5 August 2019.

This Standard was published on 16 October 2019.

The following are represented on Committee IT-005:

Australian Payments Network
EFTPOS Payments Australia
New Payments Platform Australia

Additional Interests

American Express
ANZ Banking Group
Coles Group
Commonwealth Bank of Australia
Diebold Nixdorf
Eracom Technologies Australia
FIS Global
Gemalto
Mag-Tek
National Australia Bank
Pacific Research
SWIFT
Thales eSecurity
Triton Systems of Delaware LLC
UL Transaction Security
Woolworths Group

This Standard was issued in draft form for comment as DR AS ISO/IEC 9797.2:2019.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76072 560 0

AS ISO/IEC 9797.2:2019
ISO/IEC 9797-2:2011



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

Part 2: Mechanisms using a dedicated hash-function

Originated as AS 2805.4.2—2001.
Previous edition 2006.
Revised and redesignated as AS ISO/IEC 9797.2:2019.

COPYRIGHT

© ISO/IEC 2019 — All rights reserved
© Standards Australia Limited 2019

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.4.2—2006, *Electronic funds transfer — Requirements for interfaces, Part 4.2: Message authentication — Mechanisms using a hash-function.*

The objective of this Standard is to specify 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 unauthorized 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 and message authentication mechanisms is dependent on the entropy 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.

This Standard is identical with, and has been reproduced from, ISO/IEC 9797-2:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*.

As this document has been reproduced from an International Standard, the following applies:

(a) In the source text "this part of ISO/IEC 9797" should read "this Australian Standard".

(b) A full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms "normative" and "informative" are used in Standards to define the application of the appendices or annexes to which they apply. A "normative" appendix or annex is an integral part of a Standard, whereas an "informative" appendix or annex is only for information and guidance.

© Standards Australia Limited 2019

Contents

Preface ii
Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols and notation 3
5 Requirements 5
6 MAC Algorithm 1 6
6.1 Description of MAC Algorithm 1 6
6.1.1 Step 1 (key expansion) 6
6.1.2 Step 2 (modification of the constants and the IV) 7
6.1.3 Step 3 (hashing operation) 7
6.1.4 Step 4 (output transformation) 7
6.1.5 Step 5 (truncation) 7
6.2 Efficiency 7
6.3 Computation of the constants 8
6.3.1 Dedicated Hash-Function 1 (RIPEMD-160) 8
6.3.2 Dedicated Hash-Function 2 (RIPEMD-128) 9
6.3.3 Dedicated Hash-Function 3 (SHA-1) 9
6.3.4 Dedicated Hash-Function 4 (SHA-256) 10
6.3.5 Dedicated Hash-Function 5 (SHA-512) 10
6.3.6 Dedicated Hash-Function 6 (SHA-384) 11
6.3.7 Dedicated Hash-Function 8 (SHA-224) 11
7 MAC Algorithm 2 12
7.1 Description of MAC Algorithm 2 12
7.1.1 Step 1 (key expansion) 12
7.1.2 Step 2 (hashing operation) 12
7.1.3 Step 3 (output transformation) 13
7.1.4 Step 4 (truncation) 13
7.2 Efficiency 13
8 MAC Algorithm 3 13
8.1 Description of MAC Algorithm 3 13
8.1.1 Step 1 (key expansion) 13
8.1.2 Step 2 (modification of the constants and the *IV*) 14
8.1.3 Step 3 (padding) 14
8.1.4 Step 4 (application of the round-function) 14
8.1.5 Step 5 (truncation) 15
8.2 Efficiency 15
Annex A (normative) **ASN.1 Module** 16
Annex B (informative) **Examples** 17
Annex C (informative) **A security analysis of the MAC algorithms** 37
Bibliography 39

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.

ISO/IEC 9797-2 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 9797-2:2002), which has been technically revised by including MAC algorithms based on Dedicated Hash-Functions 4 — 7 of ISO/IEC 10118-3:2004 and Dedicated Hash-Function 8 of ISO/IEC 10118-3/Amd.1:2006.

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.

This corrected version of ISO/IEC 9797-2:2011 incorporates corrections to subclauses 3.14, 6.3, 6.3.5 and 6.3.6.

© Standards Australia Limited 2019

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 document 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 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 ISO and IEC. Information may be obtained from:

Entrust Technologies, Technology Licensing Dept., 1000 Innovation Drive, Ottawa, Ontario, Canada K2K 3E7.

Attention is drawn to the possibility that some of the elements of this document 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.

© Standards Australia Limited 2019

Australian Standard®

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 unauthorized 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 and message authentication mechanisms is dependent on the entropy 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 is commonly known as MDx-MAC. It calls the hash-function once, but it makes a small modification to the round-function in the hash-function by adding a key to the additive constants in the round-function. The second mechanism is commonly known as HMAC. It calls the 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 higher performance for applications that work with short input data strings only.

This part of ISO/IEC 9797 can be applied to the security services of any security architecture, process, or application.

NOTE A general framework for the provision of integrity services is specified in ISO/IEC 10181-6 [5].

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 10118-3:2004/Amd.1:2006, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions — Amendment 1: Dedicated Hash-Function 8 (SHA-224)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
block
bit-string of length L_1, i.e. the length of the first input to the round-function

[SOURCE: ISO/IEC 10118-3]

3.2
collision-resistant hash-function
hash-function satisfying the following property:

- it is computationally infeasible to find any two distinct inputs which map to the same output

© Standards Australia Limited 2019