AS ISO/IEC 9797.1:2019
ISO/IEC 9797-1:2011

AS ISO/IEC 9797.1:2019

Australian STANDARD®

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

Part 1: Mechanisms using a block cipher

STANDARDS Australia

AS ISO/IEC 9797.1:2019

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

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 9797.1:2019.

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 572 3

AS ISO/IEC 9797.1:2019
ISO/IEC 9797-1:2011

Australian STANDARD®

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

Part 1: Mechanisms using a block cipher

Originated as AS 2805.4.1—1985.
Previous edition 2001.
Revised and redesignated as AS ISO/IEC 9797.1:2019.

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 2805.4.1—2001, *Electronic funds transfer—Requirements for interfaces, Part 4.1: Message authentication—Mechanism using a block cipher*.

The objective of this Standard is to specify six MAC algorithms that use a secret key and an n-bit block cipher to calculate an *m*-bit MAC.

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

Key management mechanisms are outside the scope of this Standard.

This Standard is to specify object identifiers that can be used to identify each mechanism in accordance with ISO/IEC 8825-1. Numerical examples and a security analysis of each of the six specified algorithms are provided, and the relationship of this Standard to previous standards is explained.

This Standard is identical with, and has been reproduced from, ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*.

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 4
6 Model for MAC algorithms 5
6.1 General 5
6.2 Step 1 (key derivation) 6
6.2.1 General 6
6.2.2 Key Derivation Method 1 6
6.2.3 Key Derivation Method 2 7
6.3 Step 2 (padding) 7
6.3.1 General 7
6.3.2 Padding Method 1 7
6.3.3 Padding Method 2 7
6.3.4 Padding Method 3 7
6.3.5 Padding Method 4 8
6.4 Step 3 (splitting) 8
6.5 Step 4 (iteration) 8
6.6 Step 5 (final iteration) 8
6.6.1 General 8
6.6.2 Final iteration 1 8
6.6.3 Final iteration 2 8
6.6.4 Final iteration 3 9
6.7 Step 6 (output transformation) 9
6.7.1 General 9
6.7.2 Output Transformation 1 9
6.7.3 Output Transformation 2 9
6.7.4 Output Transformation 3 9
6.8 Step 7 (truncation) 9
7 MAC algorithms 9
7.1 General 9
7.2 MAC Algorithm 1 10
7.3 MAC Algorithm 2 10
7.4 MAC Algorithm 3 11
7.5 MAC Algorithm 4 12
7.6 MAC Algorithm 5 13
7.7 MAC Algorithm 6 14
Annex A (normative) **Object identifiers** 16
Annex B (informative) **Examples** 18
Annex C (informative) **A security analysis of the MAC algorithms** 29
Annex D (informative) **A comparison with previous MAC algorithm standards** 36
Bibliography 37

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.

Attention is drawn to the possibility that some of the elements of this document 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 9797-1 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 9797-1:1999), which has been technically revised. MAC Algorithms 5 and 6 of ISO/IEC 9797-1:1999, which consisted of two single CBC-MAC computations, have been replaced by two other MAC algorithms, which perform single CBC-MAC computations and which offer improved efficiency. Annex A on object identifiers has been added. The security analysis in Annex C has been updated and Annex D on the relationship to previous standards has been added.

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.

© Standards Australia Limited 2019

Introduction

In an IT environment, it is often required that one can verify that electronic data has not been altered in an unauthorized manner and that one can provide assurance that a message has been originated by an entity in possession of the secret key. A MAC (Message Authentication Code) algorithm is a commonly used data integrity mechanism that can satisfy these requirements.

This part of ISO/IEC 9797 specifies six MAC algorithms that are based on an n-bit block cipher. They compute a short string as a function of a secret key and a message of variable length.

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 mechanism specified in this part of ISO/IEC 9797 is commonly known as CBC-MAC (CBC is an abbreviation of Cipher Block Chaining).

The other five mechanisms are variants of CBC-MAC. MAC Algorithms 2, 3, 5 and 6 apply a special transformation at the end of the processing. MAC Algorithm 6 is an optimized variant of MAC Algorithm 2. MAC Algorithm 5 uses the minimum number of encryptions. MAC Algorithm 5 requires only a single block cipher key setup but it needs a longer internal key. MAC Algorithm 4 applies a special transformation at both the beginning and the end of the processing; this algorithm is recommended for use in applications which require that the key length of the MAC algorithm be twice that of the block cipher.

© Standards Australia Limited 2019

Australian Standard®

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

Part 1: Mechanisms using a block cipher

1 Scope

This part of ISO/IEC 9797 specifies six MAC algorithms that use a secret key and an *n*-bit block cipher to calculate an *m*-bit MAC.

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

Key management mechanisms are outside the scope of this part of ISO/IEC 9797.

This part of ISO/IEC 9797 specifies object identifiers that can be used to identify each mechanism in accordance with ISO/IEC 8825-1. Numerical examples and a security analysis of each of the six specified algorithms are provided, and the relationship of this part of ISO/IEC 9797 to previous standards is explained.

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 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

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

3.1
block
bit string of length *n*

3.2
block cipher key
key that controls the operation of a block cipher

3.3
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 9798-1:2010]

3.4
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2]

© Standards Australia Limited 2019