



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

## **Part 1: Mechanisms using a block cipher**



## 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](http://www.standards.org.au)

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



# **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.

# Contents

<b>Preface</b> .....	<b>ii</b>
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and notation</b> .....	<b>3</b>
<b>5 Requirements</b> .....	<b>4</b>
<b>6 Model for MAC algorithms</b> .....	<b>5</b>
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
<b>7 MAC algorithms</b> .....	<b>9</b>
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
<b>Annex A</b> (normative) <b>Object identifiers</b> .....	<b>16</b>
<b>Annex B</b> (informative) <b>Examples</b> .....	<b>18</b>
<b>Annex C</b> (informative) <b>A security analysis of the MAC algorithms</b> .....	<b>29</b>
<b>Annex D</b> (informative) <b>A comparison with previous MAC algorithm standards</b> .....	<b>36</b>
<b>Bibliography</b> .....	<b>37</b>

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- 
- Looking for additional Standards? Visit Intertek Inform Infostore
  - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-