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

AS ISO/IEC 9797.2:2019

Australian STANDARD®

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

Part 2: Mechanisms using a dedicated hash-function

STANDARDS Australia

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

Australian STANDARD®

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.

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.

Contents