AS ISO/IEC 10116:2019
ISO/IEC 10116:2017

AS ISO/IEC 10116:2019

Information technology — Security techniques – Modes of operation for an *n*-bit block cipher

AS ISO/IEC 10116:2019

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 28 August 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
Westpac Banking Corporation
Woolworths Group

This Standard was issued in draft form for comment as DR AS ISO/IEC 10116:2019.

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 559 4

AS ISO/IEC 10116:2019
ISO/IEC 10116:2017

Australian STANDARD

Information technology — Security techniques – Modes of operation for an *n*-bit block cipher

Originated as part of AS 2805.5—1985.
Revised and redesignated as AS 2805.5.2—1992.
Previous edition 2009.
Revised and redesignated as AS ISO/IEC 10116:2019.

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS ISO 2805.5.2—2009, *Electronic funds transfer — Requirements for interfaces, Part 5.2: Ciphers — Modes of operation for an n-bit block cipher.*

The objective of this Standard is to establish five modes of operation for applications of an *n*-bit block cipher (e.g. protection of data during transmission or in storage). The defined modes only provide protection of data confidentiality. Protection of data integrity is not within the scope of this document. Also, most modes do not protect the confidentiality of message length information.

This document specifies the modes of operation and gives recommendations for choosing values of parameters (as appropriate).

This Standard is identical with, and has been reproduced from, ISO/IEC 10116:2017, *Information technology — Security techniques — Modes of operation for an n-bit block cipher.*

As this document has been reproduced from an International Standard, 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