



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



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.

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 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

Preface	ii
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols, abbreviated terms and notation	3
4.1 Symbols and abbreviated terms	3
4.2 Notation	4
5 Requirements	4
6 Electronic Codebook (ECB) mode	5
6.1 Preliminaries	5
6.2 Encryption	5
6.3 Decryption	5
7 Cipher Block Chaining (CBC) mode	6
7.1 Preliminaries	6
7.2 Encryption	6
7.3 Decryption	6
7.4 Avoiding ciphertext expansion	7
7.4.1 General	7
7.4.2 Three ciphertext stealing variants of CBC	7
8 Cipher Feedback (CFB) mode	8
8.1 Preliminaries	8
8.2 Encryption	9
8.3 Decryption	10
8.4 Avoiding ciphertext expansion	10
9 Output Feedback (OFB) mode	11
9.1 Preliminaries	11
9.2 Encryption	11
9.3 Decryption	12
9.4 Avoiding ciphertext expansion	12
10 Counter (CTR) mode	13
10.1 Preliminaries	13
10.2 Encryption	13
10.3 Decryption	14
10.4 Avoiding ciphertext expansion	14
Annex A (normative) Object identifiers	15
Annex B (informative) Properties of the modes of operation and important security guidance	17
Annex C (informative) Figures describing the modes of operation	22
Annex D (informative) Numerical examples for the modes of operation	27
Bibliography	38

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](#)
-