AS 2805.5.2—2009
ISO/IEC 10116:2006

AS 2805.5.2—2009

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 5.2: Ciphers—Modes of operation for an *n*-bit block cipher

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems.
It was approved on behalf of the Council of Standards Australia on 13 January 2009.
This Standard was published on 11 February 2009.

The following are represented on Committee IT-005:

- Australian Association of Permanent Building Societies
- Australian Bankers Association
- Australian Electrical and Electronic Manufacturers Association
- Australian Information Industry Association
- Australian Payments Clearing Association
- Australian Retailers Association
- Reserve Bank of Australia

This Standard was issued in draft form for comment as DR 08015.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 5.2: Ciphers—Modes of operation for an *n*-bit block cipher

Originated as part of AS 2805.5—1985.
Previous edition AS 2805.5.2—1992.
Second edition 2009.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 9010 0

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.5.2—1992, *Electronic funds transfer—Requirements for interfaces,* Part 5.2: *Ciphers—Modes of operation for an n-bit block cipher algorithm.*

The objective of this Standard is to align Australian block cipher usage with world's best practice and facilitate financial service interoperability.

This Standard is identical with, and has been reproduced from ISO/IEC 10116:2006, *Information technology—Security techniques—Modes of operation for an n-bit block cipher*.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this International Standard' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian or Australian/New Zealand Standard*	
ISO/IEC		AS/NZS ISO/IEC	
18033	Information technology—Security techniques—Encryption algorithms	18033	Information technology—Security techniques—Encryption algorithms
18033-3	Part 3: Block ciphers	18033.3	Part 3: Block ciphers

The terms 'normative' and 'informative' are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

CONTENTS

Page

Figures

INTRODUCTION

ISO/IEC 10116 specifies modes of operation for an n-bit block cipher. These modes provide methods for encrypting and decrypting data where the bit length of the data may exceed the size n of the block cipher.

This third edition of ISO/IEC 10116 specifies five modes of operation:

a) Electronic Codebook (ECB);

b) Cipher Block Chaining (CBC);

c) Cipher Feedback (CFB);

d) Output Feedback (OFB); and

e) Counter (CTR).

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 5.2:
Ciphers—Modes of operation for an *n*-bit block cipher

1 Scope

This International Standard establishes five modes of operation for applications of an n-bit block cipher (e.g. protection of data transmission, data storage). The defined modes only provide protection of data confidentiality. Protection of data integrity and requirements for padding the data are not within the scope of this International Standard. Also most modes do not protect the confidentiality of message length information.

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

The modes of operation specified in this International Standard have been assigned object identifiers in accordance with ISO/IEC 9834. The list of assigned object identifiers is given in Annex A. In applications in which object identifiers are used, the object identifiers specified in Annex A are to be used in preference to any other object identifiers that may exist for the mode concerned.

NOTE Annex B (informative) contains comments on the properties of each mode. Block ciphers are specified in ISO/IEC 18033-3.

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.*