AS 2805.3.2—2008

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 3.2: PIN management and security—Offline

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 19 February 2007.
This Standard was published on 7 April 2008.

The following are represented on Committee IT-005:

- Australian Association of Permanent Building Societies
- Australian Bankers Association
- Australian Electrical and Electronic Manufacturers Association
- Australian Institute of Petroleum
- Australian Retailers Association
- Credit Card Industry
- Reserve Bank of Australia

This Standard was issued in draft form for comment as DR 05484.

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Standards may also be withdrawn.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 3.2: PIN management and security—Offline

Originated as part of AS 2805.3—1985.
Previous edition part of AS 2085.3—2000.
Revised in part and redesignated AS 2805.3.2—2008.

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

ISBN 0 7337 8545 X

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems to supersede part of AS 2805.3—2000, *Electronic funds transfer—Requirements for interfaces*, Part 3: *PIN management and security*.

This Standard is Part 3.2 of the following series:

AS		
2805	Electronic funds transfer—Requirements for interfaces	
2805.1	Part 1:	Communications
2805.2	Part 2:	Message structure, format and content
2805.3.1	Part 3.1:	PIN management and security—General
2805.3.2	Part 3.2:	PIN management and security —Offline
2805.4.1	Part 4.1:	Message authentication —Mechanisms using a block cipher
2805.4.2	Part 4.2:	Message authentication—Mechanisms using a hash function
2805.5.1	Part 5.1:	Ciphers—Data encipherment algorithm 1 (DEA 1)
2805.5.2	Part 5.2:	Ciphers—Modes of operation for an n-bit block cipher algorithm
2805.5.3	Part 5.3:	Ciphers—Data encipherment algorithm 2 (DEA 2)
2805.5.4	Part 5.4:	Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques
2805.6.1	Part 6.1:	Key management—Principles
2805.6.2	Part 6.2:	Key management—Transaction keys
2805.6.3	Part 6.3:	Key management—Session keys—Node to node (this Standard)
2805.6.4	Part 6.4:	Key management—Session keys—Terminal to acquirer
2805.6.5.1	Part 6.5.1:	Key management—TCU initialization—Principles
2805.6.5.2	Part 6.5.2:	Key management—TCU initialization—Symmetric
2805.6.5.3	Part 6.5.3:	Key management—TCU initialization—Asymmetric
2805.6.6	Part 6.6:	Key management—Session keys—Node to node with KEK replacement
2805.9	Part 9:	Privacy of communications
2805.10.1	Part 10.1:	File transfer integrity validation
2805.10.2	Part 10.2:	Secure file transfer (retail)
2805.11	Part 11:	Card parameter table
2805.12.1	Part 12.1:	Message content—Structure and format
2805.12.2	Part 12.2:	Message content—Codes
2805.12.3	Part 12.3:	Message content—Maintenance of codes
2805.13.1	Part 13.1:	Secure hash functions—General
2805.13.2	Part 13.2:	Secure hash functions—MD5
2805.13.3	Part 13.2	Secure hash functions SHA-1
2805.14.1	Part 14.1:	Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods
2805.14.2	Part 14.2:	Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems

The following Handbooks relate to the AS 2805 series of Standards:

HB 127	Electronic funds transfer—Implementing message content Standards—Conversion Handbook (changing from AS 2805.2 to the AS 2805.12 series)
HB 128	Electronic funds transfer—Implementing message content Standards—Terminal Handbook
HB 129	Electronic funds transfer—Implementing message content Standards—Interchange Handbook

In the AS 2805 series of Standards, definitions are specific to the Part in which they appear.

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the appendix to which they apply. A ‘normative’ appendix is an integral part of a Standard whereas an ‘informative’ appendix is for information and guidance only.

This Standard is based on ISO 9564-3, *Banking—Personal Identification Number management and security*, Part 3: *Requirements for offline PIN handling in ATM and POS systems.*

CONTENTS

Page

FOREWORD

The introduction of financial transaction cards with embedded Integrated Circuits (IC) brings the technical feasibility of performing PIN verification offline using the IC card. Issuers may now choose whether to have PIN verification performed online or offline. This part of AS 2805 provides specific requirements for addressing offline PIN management using IC Cards.

Offline PIN verification does not require that a cardholder's PIN be sent to the issuer host for verification and so many security requirements relating to PIN protection over networks are not applicable. However, many general PIN protection principles and techniques are still applicable even though a PIN may be verified offline. This standard restricts itself to requirements relating specifically to the offline nature of PIN management and, unless explicitly excluded, the basic principles of PIN management described in AS 2805.3.1 are applicable.

ISO 10202 (all parts), *Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards*, and in particular Part 6 of that standard, defines security requirements for cardholder verification using IC cards. It should be noted that ISO 10202 defines requirements on the IC card itself, rather than on the acquirer IC card acceptance systems, and so can be considered as a complementary set of documents to AS 2805.3.

STANDARDS AUSTRALIA

Australian Standard
Electronic funds transfer—Requirements for interfaces

Part 3.2: PIN management and security—Offline

1 SCOPE

This Standard specifies the minimum security measures required for PIN management in an off-line environment.

It is applicable to financial transaction card originated transactions requiring offline PIN verification by an IC card and to those institutions responsible for implementing techniques for the management and protection of the PIN at Automated Teller Machines (ATM) and Point-of-Sale (POS) terminals.

The provisions of this part of AS 2805.3 are not intended to cover:

(a) PIN management and security in the online PIN environment, which is covered in AS 2805.3.1.

(b) The protection of the PIN against loss or intentional misuse by the customer or authorized employees of the issuer or their agents.

(c) Privacy of non-PIN transaction data.

(d) Protection of transaction messages against alteration or substitution, e.g. an online authorisation response.

(e) Protection against replay of the PIN or transaction.

(f) Specific key management techniques.

(g) The decision as to whether the IC card is to receive the PIN enciphered.

(h) Contactless IC cards.

Requirements associated with multi-application IC cards are considered to be the responsibility of the issuer and are not included in this Standard. This Standard is described in terms applicable to IC card technology, however this language is not meant to restrict the applicability of this part to IC card technology.

2 APPLICATION

This Standard is applicable to institutions responsible for implementing techniques for the management and protection of the PIN for card originated transactions in the off-line environment.

This Standard applies in all situations where a customer-entered PIN is part of an off-line transaction with a financial institution either directly or indirectly. It applies when any part of the PIN entry, verification, and response process involves a financial institution including an ICC card supplied by that institution. It also applies to all elements of the entire verification process, including interchange, network, switch, individuals, financial institutions, and any other designated end-user organizations.

