Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 3: PIN management and security

Standards Australia

This Australian Standard was prepared by Committee IT/5, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 15 March 2000 and published on 13 April 2000.

The following interests are represented on Committee IT/5:

Australian Association of Permanent Building Societies

Australian Bankers Association

Australian Electrical and Electronic Manufacturers Association

Australian Institute of Petroleum

Australian Retailers Association

Consumers Federation of Australia

Credit Card Industry

Credit Union Services Corporation (Australia)

Reserve Bank of Australia

Telstra Corporation

Keeping Standards up-to-date

Standards are living documents which 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 Standards may also be withdrawn.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 which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, PO Box 1055, Strathfield, NSW 2135.

This Standard was issued in draft form for comment as DR 99415.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 3: PIN management and security

Originated AS 2803.3—1985.
Second edition 2000.

Published by Standards Australia International Ltd
PO Box 1055, Strathfield, NSW 2135, Australia

ISBN 0 7337 3357 3

PREFACE

This Standard was prepared by the Standards Australia Committee IT/5, Financial Transaction Systems to supersede AS 2805.3 —1985.

The AS 2805 series of Standards is as follows:

AS		
2805	Electronic funds transfer—Requirements for interfaces	
2805.1	Part 1:	Communications
2805.2	Part 2:	Message structure, format and content
2805.3	Part 3:	PIN management and security (this Standard)
2805.4	Part 4:	Message authentication
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
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
2805.9	Part 9:	Privacy of communications
2805.10	Part 10:	File transfer integrity validation
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 13.3:	Secure hash functions—SHA-1
2805.14.1	Part 14.1:	Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

The following Handbooks relate to AS 2805 series of Standards:

HB 127 Electronic funds transfer—Implementing message content Standards—Conversion Handbook (changing from AS 2805 Part 2 to 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

Part of the AS 2805 series that is in the course of preparation is as follows:

Message authentication using DEA 3

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

The term ‘informative’ has been used in this Standard to define the application of the appendix to which it applies. An ‘informative’ appendix is for information and guidance only.

This Standard is based on ISO 9564, Banking — Personal Identification Number management and security, Parts 1 and 2.

CONTENTS

FOREWORD

The Personal Identification Number (PIN) is a means of verifying the identity of a customer within an electronic funds transfer (EFT) network.

The objective of PIN management is to protect the PIN against unauthorized disclosure, compromise, and misuse throughout its life cycle and in so doing to minimize the risk of fraud occurring within EFT systems. The secrecy of the PIN needs to be assured at all times during its life cycle, which consists of its selection, issuance, activation, storage, entry, transmission, validation, deactivation, and any other use made of it.

PIN security also depends upon sound key management. Maintaining the secrecy of cryptographic keys is of the utmost importance because the compromise of any key allows the compromise of any PIN ever enciphered under it.

Wherever possible, this Standard specifies requirements in absolute terms. In some instances a level of subjectivity cannot be practically avoided especially when discussing the degree of level of security desired or to be achieved.

The level of security to be achieved is related to a number of factors, including the sensitivity of the data concerned and the likelihood that it will be intercepted, the practicality of any envisaged encipherment process, and the cost of providing, and breaking, a particular means of providing security. It is, therefore, necessary for each card acceptor, acquirer and issuer to agree on the extent and level of security and PIN management procedures. Absolute security is not practically achievable. Therefore, PIN management procedures should implement preventive measures to reduce the opportunity for a breach in security and aim for a ‘high’ probability of detection of any illicit access or change to PIN material should these preventive measures fail. This applies at all stages of the generation, exchange and use of a PIN, including those processes that occur in cryptographic equipment and those related to communication of PINs.

This Standard is designed so that issuers can uniformly make certain, to whatever degree is practicable, that a PIN, while under the control of other institutions, is properly managed. Techniques are given for protecting the PIN-based customer authentication process by safeguarding the PIN against unauthorized disclosure during the PIN’s life cycle.

STANDARDS AUSTRALIA

Australian Standard
Electronic funds transfer — Requirements for interfaces

Part 3: PIN management and security

1 SCOPE

This Standard specifies the minimum security measures required for effective PIN management. Standard means of interchanging PIN data are provided. This Standard does not cover the following:

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

(b) Privacy of non-PIN transaction data (see AS 2805.9).

(c) Protection of transaction messages against alteration or substitution, e.g. an authorization response to a PIN verification (see AS 2805.4).

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

(e) Specific key management techniques (see AS 2805.6 series).

(f) PIN management and security for transactions conducted using integrated circuit cards (ICC).

(g) The use of asymmetric encipherment algorithms for PIN management.

NOTE: For a detailed discussion on the need for personal identification number (PIN) protection, see Appendix A.

(h) Physical and logical security (see AS 2805.14.1).

NOTE: Further information on PIN management for security is given in Appendices A and C.

2 APPLICATION

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

This Standard applies in all situations where a customer-entered PIN is part of a transaction with a financial institution. It applies when any part of the PIN entry, verification, and response process involves a financial 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.

3 REFERENCED DOCUMENTS

The following Standards are referred to in this Standard:

AS		
2805	Electronic funds transfer — Requirements for interfaces	
2805.4	Part 4:	Message authentication
2805.5.2	Part 5.2:	Ciphers — Modes of operation for an n-bit block cipher algorithm
2805.5.4	Part 5.4:	Ciphers — Data encipherment algorithm 3 (DEA 3) and related techniques
2805.9	Part 9:	Privacy of communications
2805.14.1	Part 14.1:	Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods.
3523	Identification cards — Numbering system and registration procedure for issuer identifiers	