Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES—

Part 3—PIN MANAGEMENT AND SECURITY

This Australian standard was prepared by Committee IS/5, Electronic Funds Transfer. It was approved on behalf of the Council of the Standards Association of Australia on 18 April 1985 and published on 17 May 1985.

The following interests are represented on Committee IS/5:

Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Computer Equipment Manufacturers Association
Australian Computer Equipment Suppliers Association
Australian Electrical and Electronics Manufacturers Association
Australian Federation of Credit Union Leagues
Australian Institute of Petroleum
Australian Retailers Association
Australian Software Houses Association
Catering Institute of Australia
Life Insurance Federation of Australia
National Card Issuers
National Network Operators
Reserve Bank of Australia
Telecom Australia

This standard was issued in draft form for comment as DR 84120.

Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES—

Part 3—PIN MANAGEMENT AND SECURITY

First published 1985

PUBLISHED BY STANDARDS AUSTRALIA
(STANDARDS ASSOCIATION OF AUSTRALIA)
1 THE CRESCENT, HOMEBUSH, NSW 2140

ISBN 0 7262 3762 0

PREFACE

This standard was prepared by the Association's Committee on Electronic Funds Transfer. It is one of a series of standards on electronic funds transfer (EFT), requirements for interfaces; the other standards in the series being as follows:

Part 1— Communications Interface and Data Representation

Part 2— Message Structure, Format and Content

Part 4— Message Authentication

Part 5— Data Encryption Algorithm

Part 6— Terminal Key Management and Security*

Part 7— Point of Service Message Content*

Part 8— Financial Institution Message Content*

It should be noted that in this series of standards, the definitions are specific to the Part in which they appear.

In this Part 3, Appendices A to E have been included for the guidance of users; they do not form part of the requirements of this standard.

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

This standard is based on ANSI X9.8 — 1982, American National Standard for Personal Identification Number (PIN) Management and Security, copyright 1982 by the American National Standards Institute. Material from ANSI X9.8 has been incorporated herein with the permission of the American National Standards Institute and acknowledgment is made of the assistance received from ANSI.

NOTE: Copies of ANSI X9.8 may be purchased from ANSI at 1430 Broadway, New York, NY 10018 or from SAA Head Office.

Attention is drawn to current work being undertaken (by ISO/TC68/SC2/WG6) towards the preparation of a new International (ISO) standard for PIN Management and Security. As soon as work on the new ISO standard reaches finality, it is proposed to revise this standard in order to align with the ISO requirements. It is expected that this work will lead to the definition of alternative PIN security techniques.

---

* In course of preparation

CONTENTS

STANDARDS ASSOCIATION OF AUSTRALIA

Australian Standard
for
ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES—
PART 3—PIN MANAGEMENT AND SECURITY

FOREWORD

Identification or authentication of an individual within a financial system can be accomplished by—

(a) some physical or personal characteristic (e.g. signature, fingerprint, voiceprint);

(b) something being carried (e.g. badge, plastics card and magnetic stripe); or

(c) something known or memorized (e.g. personal identification number).

This standard is restricted to an authentication technique using an alphanumeric code or password which a person has memorized i.e. Personal Identification Number (PIN). The decision to restrict this standard to PINs is based on the current state of the art and the existing requirement for using PINs in the financial industry's established systems. It is generally acknowledged that other authentication techniques have not advanced to the point where standards or guidelines can be developed.

PINs may be used in a transaction interchange environment where, at the time of initiating transactions, customers enter identification and authentication information at terminals connected to an acquirer network. This network then accesses the card issuer network responsible for authenticating the customer and authorizing the transaction. PINs also may be used in a private network, where identification and authentication of customers served by the network are accomplished entirely within it.

Whereas this standard contains the latest concepts available at the time of publication it remains the responsibility of the issuing financial institution to use the best techniques available at the time of implementing a PIN system. It gives procedures and guidelines for the management and security of the PIN's life cycle. The PIN is the basis for authentication of the identity of a customer. The standard is designed so that the PIN's life cycle is properly handled thus improving the probability that a customer engaging in a financial transaction is, in fact, the authentic customer.

Techniques are given for protecting the PIN-based customer authentication process by safeguarding the PIN against unauthorized disclosure during the PIN's life cycle.

SPECIFICATION

1 SCOPE. This standard specifies requirements for the management and security of personal identification numbers (PINs) used for authenticating customers who initiate card-originated electronic messages relating to financial transactions. It specifies a number of procedures for managing PINs, for using PINs to authenticate the initiator of a transaction, and for preventing unauthorized PIN disclosure by financial institutions handling PINs.

This standard does not include requirements to protect PINs against loss or intentional misuse by either the customer or others who have access to PINs.

This standard does not cover—

(a) transaction message integrity (see AS 2805, Part 4);
(b) key management (see AS 2805, Part 6); and
(c) privacy assurance.

2 APPLICATION. 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 2623 Credit Cards
- Part 1—Specifications, Numbering system and Registration Procedure
- Part 2—Magnetic Stripe Encoding for Tracks 1, 2 and 3

AS 2805 Electronic Funds Transfer—Requirements for Interfaces—
- Part 4—Message Authentication
- Part 5—Data Encryption Algorithm
- Part 6—Terminal Key Management and Security*

4 DEFINITIONS. For the purpose of this standard, the following definitions apply:

4.1 Acquirer—the institution, or its agent, which acquires, from the card acceptor, the financial data relating to the transaction, and which initiates that data into an interchange system.

NOTE: Any entity which passes messages without regard to the financial data therein is not regarded as an acquirer.

4.2 Algorithm—a clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

4.3 Authentication—the act of determining that a message comes from a source authorized to originate messages of that type and that the message is as authorized.

4.4 Block encryption—the technique by which 64 bits of clear text are encrypted to yield 64 bits of cipher text.

NOTE: This technique is described in AS 2805, Part 5.

4.5 Card acceptor—the party accepting the card and presenting transaction data to an acquirer.

4.6 Card issuer—the institution, or its agent, which issues the identification card to the cardholder.

4.7 Cardholder—the customer associated with the Primary Account Number (PAN) requesting the transaction from the card acceptor.

NOTE: In this standard, the cardholder is also referred to as the 'customer'.

4.8 Cipher text—clear text that has been encrypted.

4.9 Clear text—intelligible text or signals that have meaning and that can be read and used.

4.10 Data Encryption Algorithm (DEA)—an algorithm designed to encrypt and decrypt blocks of data.

NOTE: A DEA is specified in AS 2805 Part 5.

4.11 Decryption—the transformation of cipher text into clear text.

NOTE: 'Decryption' is sometimes referred to as 'decipherment'.

4.12 Encryption—the transformation of clear text into cipher text for the purpose of security or privacy.

NOTE: 'Encryption' is sometimes referred to as 'encipherment'.

4.13 Encryption algorithm—a set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations to the normal representation of the information through the use of variable elements controlled by the application of a key.

4.14 Financial institution—the institution responsible for the custody, loan, exchange, or issue of money; for the extension of credit; and for facilitating transmission of funds.

4.15 Identification—the process of associating a unique characteristic to an individual.

4.16 Interchange—the mutual acceptance and exchange of financial transaction messages.

4.17 Irreversible encryption—transformation of clear text to cipher text in such a way that the original clear text cannot be recovered by other than exhaustive procedures.

4.18 Key—a 64-bit quantity which is used for transformations between cipher text and clear text.

4.19 Modulo 2 Addition—a mathematical operation equivalent to binary addition without carry.

NOTE: 'Modulo 2 addition' is represented by the symbol $\oplus$ and is sometimes referred to as an 'exclusive OR' operation.

4.20 Offset—a number that mathematically relates a calculated identification code to a customer-selected PIN.

4.21 Personal Identification Number (PIN)—a numeric or alphanumeric code or password made up of between 4 and 12 characters that the cardholder possesses for the purpose of identification.

4.22 PIN assignment—the process of establishing the relationship between customer authentication and customer identification data.

4.23 PIN issuance—the act of conveying PIN information to a customer.

4.24 PIN offset—the number that mathematically relates a calculated identification code to a customer selected PIN.

---

* In course of preparation.