Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

Part 6.1—KEY MANAGEMENT—PRINCIPLES

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 17 December 1987 and published on 5 February 1988.

The following interests are represented on Committee IS/5:

Australian Association of Permanent Building Societies

Australian Bankers Association

Australian Computer Equipment Manufacturers Association

Australian Electrical and Electronics Manufacturers Association

Australian Federation of Credit Unions Ltd

Australian Information Industry Association Ltd

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 87054.

Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

Part 6.1—KEY MANAGEMENT—PRINCIPLES

First published as AS 2805.6.1—1988.

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

ISBN 0 7262 4831 2

PREFACE

This Standard was prepared by the Association's Committee on Electronic Funds Transfer as Part 6.1 of the AS 2805 series of Standards on electronic funds transfer (EFT) requirements for interfaces. The parts of AS 2805 are as follows:

Part 1: Communications Interface and Data Representation

Part 2: Message Structure, Format and Content

Part 3: PIN Management and Security

Part 4: Message Authentication

Part 5: Data Encryption Algorithm

Part 6.1: Key Management—Principles* (this Standard)

Part 6.2: Key Management—Transaction Keys*

Part 6.3: Key Management—Session Keys—Node to Node*

Part 6.4: Key Management—Session Keys—Terminal to Acquirer*

Part 7: POS Message Content

Part 8: Financial Institution Message Content

Parts 1 to 5 were first published on 17 May 1985 and Parts 7 and 8 were first published on 3 November 1986.

This Standard (Part 6.1) was developed from the experience gained by existing providers of EFT/POS systems in Australia, and by subsequent international developments in the area. It is not intended to invalidate existing EFT/POS systems, but to constitute a formal specification which will standardize future development of EFT/POS systems in Australia.

Appendix A defines the notation used in this Standard for describing cryptographic operations.

Appendix B describes key management within terminal cryptographic units and does not form part of the requirements of this Standard.

---

* Published simultaneously.

CONTENTS

FOREWORD

Keys must be protected. Maintaining the secrecy of keys is of the utmost importance because the compromise of any key allows the compromise of all data ever encrypted under it. The generation, distribution, and protection of keys is called ‘key management’.

Key management is a critical part of application specifications. In the AS 2805 series, the intent of Part 6.1 (this Standard) is to define the principles to be observed for key management when developing specifications. Part 6.2 deals with transaction keys and Parts 6.3 and 6.4 with session keys. Choice of an appropriate implementation will be governed by the nature of the interface application and the constraints of maintaining the security principles within it.

STANDARDS ASSOCIATION OF AUSTRALIA

Australian Standard
ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

PART 6.1: KEY MANAGEMENT—PRINCIPLES

1 SCOPE. This Standard specifies key management principles for keys used in the authentication, encryption and decryption of electronic messages relating to financial transactions.

2 REFERENCED DOCUMENTS. The following Standards are referred to in this Standard:

AS 2805 Electronic Funds Transfer—Requirements for Interfaces
AS 2805.4 Message Authentication
AS 2805.5 Data Encryption Algorithm

3 DEFINITIONS. For the purpose of this Standard, the definitions below apply.

3.1 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.

3.2 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.

3.3 Back tracking—the ability to use current key values together with information previously transmitted or received, to determine previous key values.

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

NOTE: Hereinafter referred to as 'issuer'.

3.5 Cipher text—clear text that has been encrypted.

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

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

NOTE: A DEA is specified in AS 2805.5.

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

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

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

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

3.10 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.

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

3.12 Key encrypting key (KEK)—a key which is used to encrypt other keys and which may be used to exchange session keys between two systems.

3.13 Key storage—the secure area used to store keys.

3.14 Key verification code (KVC)—a 24-bit code which is cryptographically derived from a given key and which is used to prove that the key was correctly loaded.

3.15 Message Authentication Code (MAC)—a code appended to or included with a message for the purpose of verifying the origin of the message and for verifying that the message content has not been changed.

NOTE: The procedure for generating a MAC is specified in AS 2805.4.

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

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

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

3.18 Point of Service (POS)—location where a transaction originated.

3.19 POS terminal—a terminal located at a point of service.

3.20 Reference PIN—the official version of a cardholder's PIN used for comparison against the PIN as entered in the PIN entry device.

3.21 Split knowledge—a condition under which two or more parties, separately and confidentially, have custody of components of a single key that, individually, convey no knowledge of the resultant key.

3.22 Statistically unique—an acceptably low statistical probability of an item or code being duplicated by either chance or intent.

3.23 Terminal—the equipment which is capable of originating a transaction for input to a transaction interchange network.

3.24 Terminal Cryptographic Unit (TCU)—that part of a terminal which performs secure cryptographic functions.