Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

Part 6.2—KEY MANAGEMENT—TRANSACTION KEYS

This Australian Standard was prepared by Committee IT/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 IT/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

Review of Australian Standards. *To keep abreast of progress in industry, Australian Standards are subject to periodic review and are kept up to date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.*

Full details of all Australian Standards and related publications will be found in the Standards Australia Catalogue of Publications; this information is supplemented each month by the magazine 'The Australian Standard', which subscribing members receive, and which gives details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Australian Standards, addressed to the head office of Standards Australia, are welcomed. Notification of any inaccuracy or ambiguity found in an Australian Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

This Standard was issued in draft form for comment as DR 87055.

Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

Part 6.2—KEY MANAGEMENT—TRANSACTION KEYS

First published as AS 2805.6.2—1988.

PUBLISHED BY STANDARDS AUSTRALIA
(STANDARDS ASSOCIATION OF AUSTRALIA)
1 THE CRESCENT, HOMEBUSH, NSW 2140
ISBN 0 7262 4834 7

PREFACE

This Standard was prepared by the Association's Committee on Electronic Funds Transfer as Part 6.2 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*
Part 6.2: Key Management—Transaction Keys* (this Standard)
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 6.2) 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.

This Standard is based on the concept of transaction keys that was first described by H J Beker, J M K Friend and P W Halliden in a paper 'Simplifying Key Management in Electronic Fund Transfer Point of Sale Systems' published in Electronics Letters, 9th June 1983, Vol.19, No.12. This concept was developed and enhanced through several years of effort and deliberation by the Association's Subcommittee on EFT Authentication and Security. Acknowledgement is made of the valuable contribution made by the authors in initiating this concept and of the assistance given to the Subcommittee during the preparation of this Standard.

The key management scheme described in this Standard provides several security safeguards (see Foreword for details), in particular, protection against back tracking. In addition, the scheme also offers protection against forward tracking provided that some of the information encoded on the magnetic stripe of the card known as Other Card Data (OCD) is not transmitted. However, the non-transmission of OCD may not be practicable or convenient for every card-originated message, and hence, has not been made a mandatory requirement of the Standard. Instead, the non-transmission of OCD has been specified as an option.

This Standard provides for the construction of a privacy key but does not specify how it is used. (The use of the privacy key will be dealt with in a later edition.)

Appendices A and B are included for the guidance of users and do 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 is to define the principles to be observed for key management when developing specifications. Part 6.2 (this Standard) 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.

The key management system described in this Standard is based on a terminal key whose value at any time is dependent on the Message Authentication Code (MAC) residues of previous transactions. For each transaction a new set of transaction keys, including a MAC key and a PIN encryption key, is cryptographically generated using the terminal key and data read from the plastics card.

The advantages of this system are as follows:

(a) The keys (and hence the MAC from the terminal) change for each transaction in a manner known only to the card acceptor and acquirer.

(b) There is no need for fixed keys in the terminal.

(c) The response proves that the acquirer received the original message and generated the reply.

(d) Multiple acquirers are allowed access to terminals and each is responsible for its own security; less security on the part of one acquirer does not jeopardize the security of others.

(e) The audit trail, if retained, connects all transactions between a terminal/retail system and an issuer's or acquirer's processing centre.

(f) It supports the concept of a card key and hence a migration to intelligent card technology.

(g) It establishes that the card issuer's processor approved the transaction for the requested value.

(h) It may provide end-to-end PIN protection.

STANDARDS ASSOCIATION OF AUSTRALIA

Australian Standard

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

Part 6.2: KEY MANAGEMENT—TRANSACTION KEYS

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

NOTE: Principles concerning key management are given in AS 2805.6.1.

2 APPLICATION. This Standard may be adopted in situations where a secure terminal-acquirer dialogue is desired and a physically secure device as specified in AS 2805.6.1, is unavailable.

This Standard can be used in conjunction with the node to node system described in AS 2805.6.3.

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

AS 2805 Electronic Funds Transfer—Requirements for Interfaces

- AS 2805.2 Message Structure, Format and Content
- AS 2805.3 PIN Management and Security
- AS 2805.4 Message Authentication
- AS 2805.5 Data Encryption Algorithm
- AS 2805.6.1 Key Management—Principles
- AS 2805.6.3 Key Management—Session Keys—Node to Node
- AS 2805.8 Financial Institution Message Content

AS 3524 Identification Cards—Financial Transaction Cards

AS 3525 Bank cards—Magnetic Stripe Data Content for Track 3

4 DEFINITIONS. For the purpose of this Standard, the definitions below 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.

4.2 Acquirer network—a network of one or more processing centres which may represent one or more acquirers or card issuers or both.

4.3 Amount, Transaction (AT)—funds requested by the cardholder in the local currency of the acquirer or source location of the transaction, exclusive of any transaction amount fees.

NOTES:

1. This field is described in AS 2805.2, and occupies Bit Map Position P-4.
2. 'Amount, transaction' is referred to in this Standard as 'transaction amount'.

4.4 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.

4.5 Authentication Parameter (AP)—a value constructed by the card issuer, or its agent, which confirms the approval of a transaction, and specifically, of the amount of that transaction.

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

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

4.8 Card Acceptor Terminal Identification (CATID)—unique code identifying a terminal at the card acceptor location.

NOTE: This field is described in AS 2805.2, and occupies Bit Map Position P-41.

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

NOTE: Hereinafter referred to as 'issuer'.

4.10 Card key—a key constructed from data recorded on the plastics card.

NOTE: 'Card key' is sometimes referred to as 'personal key'.

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

4.12 Cipher text—clear text that has been encrypted.

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

4.14 Completion message—a message generated to confirm that a transaction has been completed.

4.15 Confirmation message—a message generated to confirm that a transaction has been completed.

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

NOTE: A DEA is specified in AS 2805.5.

4.17 Decoupling key—a key constructed from the card key and data recorded on the plastics card and used in the construction of the authentication parameter.