AS 2805.6.2—2002
(Incorporating Amendment Nos 1 and 2)

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.2: Key management—Transaction keys

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 25 March 2002. This Standard was published on 15 May 2002.

The following are represented on Committee IT-005:

- ANZ Banking Group
- Cashcard Australia
- Coles Myer
- Commonwealth Bank of Australia
- CSC Australia
- Eracom
- First Data Resources Australia
- Fujitsu ICL Retail Systems
- Intellect Australia
- Keycorp
- Mag-Tek
- National Australia Bank
- NCR Australia
- Pacific Research
- Racal Australia
- Security Consulting Services
- Telstra Corporation
- Westpac Banking Corporation

This Standard was issued in draft form for comment as DR 01025.

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 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Standards may also be withdrawn.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 6.2: Key management—Transaction keys

Originally as AS 2805.6.2—1988.
Second edition 2002.
Reissued incorporating Amendment No. 1 (February 2006).
Reissued incorporating Amendment No. 2 (February 2007).

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

ISBN 0 7337 4495 8

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems to supersede AS 2805.6.2—1988. It is one of the series of Standards on electronic funds transfer (EFT) requirements for interfaces.

This Standard incorporates Amendments No. 1 (February 2006) and No. 2 (February 2007). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

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 forms part of the AS 2805 series of Standards on electronic funds transfer (EFT) requirements for interfaces which will be 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
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 (this Standard)
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 2805.2 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

This Standard (Part 6.2) was developed from the experience gained by existing providers of EFTPOS systems in Australia, and by subsequent international developments in the area. It is not intended to invalidate existing EFTPOS systems, but to constitute a formal specification which will standardize future development of EFTPOS systems in Australia.

This Standard is based on the concept of transaction keys which 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 Sales Systems' published in *Electronics Letters*, June 1983, vol. 19, no. 12. This concept was developed and enhanced through several years of effort and deliberation by the subcommittee on EFT Authentication and Security. Acknowledgment 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 the original (1988) Standard.

This Standard provides for the construction of a privacy key but does not specify how it is used. (The use of the privacy key is specified in AS 2805.9.)

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

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 enciphered 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, Part 6.1 defines 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) residue of previous transactions. For each transaction a new set of transaction keys, including a MAC key and a PIN encipherment key, is cryptographically generated using the terminal key and data read from the plastic 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) The audit trail, if retained, connects all transactions between a terminal/retail system and an issuer’s or acquirer’s processing centre.

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

(f) It may establish that the card issuer’s processor approved the transaction for the requested value.

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

STANDARDS 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, encipherment and decipherment 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 in conjunction with minimally tamper resistant devices with tamper evidence characteristics as specified in AS 2805.14.1. 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	
2805.2	Part 2:	Message structure, format and content
2805.3	Part 3:	PIN management and security
2805.4.1	Part 4.1:	Message authentication—Mechanisms using a block cipher
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
2805.6.3	Part 6.3:	Key Management—Session Keys—Node to node
2805.12.1	Part 12.1:	Message content—Structure and format
2805.14.1	Part 14.1:	Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods
3523	Identification cards—Identification of issuers	
3523.1	Part 1:	Numbering system

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.