AS 2805.6.1—2002
(Incorporating Amendment Nos 1, 2 and 3)

AS 2805.6.1—2002

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.1: Key management—Principles

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 14 January 2002.
This Standard was published on 19 March 2002.

The following are represented on Committee IT-005:

- 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

This Standard was issued in draft form for comment as DR 00352.

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Standards may also be withdrawn.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.

AS 2805.6.1—2002
(Incorporating Amendment Nos 1, 2 and 3)

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.1: Key management—Principles

Originated as AS 2805.6.1—1988.
Second edition 2002.
Reissued incorporating Amendment No. 1 (November 2003).
Reissued incorporating Amendment No. 2 (February 2006).
Reissued incorporating Amendment No. 3 (January 2007).

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

ISBN 0 7337 4348 X

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems to supersede AS 2805.6.1—1988.

This Standard incorporates Amendment 1 (November 2003), Amendment 2 (February 2006) and Amendment 3 (January 2007). The changes arising from the Amendments are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure, or part thereof affected.

The objective of this Standard is to describe procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment.

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 (this Standard)
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 the AS 2805 series of Standards:

HB 127 Electronic funds transfer—Implementing message content Standards—Conversion Handbook (changing from AS 2805.2 to the 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

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

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the appendix to which they apply. A ‘normative’ appendix is an integral part of a Standard, whereas an ‘informative’ appendix is only for information and guidance.

CONTENTS

Page

FOREWORD

This document describes procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. It is noted that management of keys used in an Integrated Circuit Card (ICC) environment is not covered by this Standard but will be addressed in another Standard.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this Standard addresses the key management requirements that are applicable in the accessible domain of retail banking services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and transactions and automated teller machine (ATM) transactions.

Key management is the process whereby cryptographic keys are provided for use between authorized communicating parties and those keys continue to be subject to secure procedures until they have been destroyed. The security of the enciphered data is dependent upon the prevention of disclosure and unauthorized modification, substitution, insertion, or termination of keys. Thus, key management is concerned with the generation, storage, distribution, use, and destruction procedures for keys. Also, by the formalization of such procedures, provision is made for audit trails to be established.

This part of the AS 2805.6 series does not provide a means to distinguish between parties who share common keys. The final details of the key management procedures need to be agreed upon between the communicating parties concerned and will thus remain the responsibility of the communicating parties. One aspect of the details to be agreed upon will be the identity and duties of particular individuals. The AS 2805.6 series does not concern itself with allocation of individual responsibilities; this needs to be considered for each key management implementation.

This document is applicable to the management of the keys introduced by Parts 3, 4, 9 and 10 of this Standard, and to the keys introduced by the rest of Part 6. Additionally, the key management procedures may themselves require the introduction of further keys, e.g. key encipherment keys. The key management procedures are equally applicable to those keys.

Appendix A presents an example of the different parties involved in the retail banking environment and Appendix B presents examples of threats to keys and other secret data in such an environment.

STANDARDS 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, encipherment and decipherment of electronic messages relating to financial transactions within the retail banking environment.

2 APPLICATION

This Standard applies both to the keys of symmetric cipher systems, where both originator and recipient use the same secret key(s), and to the private and public keys of asymmetric cipher systems.

The use of ciphers often involves control information other than keys, e.g., initialization vectors and key identifiers. This other information is collectively called 'keying material'. Although this Standard specifically addresses the management of keys, the principles, services, and techniques applicable to keys may also be applied to keying material.

This Standard is appropriate for use by financial institutions and other organizations engaged in the area of retail financial services, where the interchange of information requires confidentiality, integrity, or authentication. Retail financial services include but are not limited to such processes as POS debit and credit authorizations, automated dispensing machine and ATM transactions, etc.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS

2805		Electronic funds transfer — Requirements for interfaces
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
2805.5.2	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
2805.13.3	Part 13.3:	Secure hash functions—SHA-1
2805.14.1	Part 14.1:	Secure cryptographic devices (retail) — Concepts, requirements and evaluation methods

ISO

7498		Information processing systems—Open Systems Interconnection—Basic Reference Model
7498-2	Part 2:	Security Architecture

