AS 2805.6.4—2001
(Incorporating Amendment No. 1)

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 6.4: Key management—Session keys—Terminal to acquirer

Standards Australia

This Australian Standard was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 21 November 2000 and published on 25 January 2001.

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

Keeping Standards up-to-date

Standards are living documents which 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 Standards may also be withdrawn.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 which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 00106.

AS 2805.6.4—2001
(Incorporating Amendment No. 1)

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 6.4: Key management—Session keys—Terminal to acquirer

Originated as AS 2805.6.4—1988.
Second edition 2001.
Reissued incorporating Amendment No. 1 (January 2003).

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 3728 5

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems.

This Standard incorporates Amendment No. 1 (January 2003). 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 objective of this Standard is to specify key management techniques for keys used in the authentication, enciphering and deciphering of electronic messages relating to financial transactions using session keys.

The AS 2805 series of Standards when published 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—Mechanism 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
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 (this Standard)
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
2805.15	Part 15:	ICC Based Stored Value/Inter-sector Electronic Purse—Principles

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 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.

This Standard (AS 2805.6.4) 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 instead to constitute a formal specification which will give one of several options for standardization of future development of EFTPOS systems in Australia.

Appendix B is included for the guidance of users.

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

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 deals with transaction keys, Part 6.3 with node-to-node session keys and Part 6.4 (this Standard) with terminal-to-acquirer session keys. Parts 6.5.1, 6.5.2 and 6.5.3 deal with provision of initial secret values to terminal cryptographic units (TCUs). 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 implementation described in this Standard uses session keys.

The terminal to acquirer mechanism provides for session keys to be generated by the acquirer and for these to be communicated to the terminal enciphered under a key enciphering key. The key enciphering keys are not like traditional master keys in that they are themselves updated by means of a one way function from information that is not transmitted. The key update is initiated by each acquirer, who controls the update frequency. This scheme is used to make back tracking of key enciphering keys as difficult as breaking the data encryption algorithm.

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 6.4: Key management—Session keys—Terminal to acquirer

1 SCOPE

This Standard specifies key management techniques for keys used in the authentication, enciphering and deciphering of electronic messages relating to financial transactions using session keys.

In particular, this Standard—

(a) defines security interface procedures between terminals and acquirers;

(b) defines methods of interchange of the various enciphering keys used for securing transactions; and

(c) ensures that messages can only be authenticated at their correct destination.

NOTE: Principles concerning key management and physical security are dealt with in AS 2805.6.1.

2 APPLICATION

This Standard may be adopted in all situations where a secure terminal-to-acquirer dialogue is desired

This Standard can be used in conjunction with the node-to-node system described in AS 2805.6.3, and the TCU initialization schemes described in the Parts of AS 2805.6.5.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS	
2805	Electronic funds transfer—Requirements for interfaces
2805.2	Message structure, format and content
2805.3	PIN management and security
2805.4.1	Message authentication—Mechanism using a block cipher
2805.5.4	Ciphers – Data Encipherment Algorithm 3 (DEA 3) and related techniques
2805.6.1	Key management—Principles
2805.6.3	Key management—Session keys—Node to node
2805.6.5.1	Key management—TCU initialization—Principles
2805.6.5.2	Key management—TCU initialization—Symmetric
2805.6.5.3	Key management—TCU initialization—Asymmetric
2805.12.1	Message content—Structure and format
3523	Identification cards—Identification of issuers
3524	Identification cards—Financial transaction cards
ISO/IEC	
10731	Information technology—Open systems interconnection—Basic reference model—Conventions for the definition of OSI services

