Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 9: Privacy of communications

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 18 May 2000. This Standard was published on 19 June 2000.

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 99398.

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 the 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Standards may also be withdrawn.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 9: Privacy of communications

Originally as AS 2805.9—1991.
Second edition 2000.
Reissued incorporating Amendment No. 1 (June 2011).

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 3471 5

PREFACE

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

This Standard incorporates Amendment No. 1 (June 2011). 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 AS 2805 series of Standards is 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	Part 4:	Message authentication
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
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 (this Standard)
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

Part of the AS 2805 series that is in the course of preparation is as follows:

Message authentication using DEA 3.

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

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

STANDARDS AUSTRALIA

Australian Standard
Electronic funds transfer—Requirements for interfaces

Part 9: Privacy of communications

1 SCOPE

This Standard specifies methods of protecting from disclosure the information contained in electronic messages formatted in accordance with AS 2805. This Standard is not intended to address the issue within operational facilities, which are assumed to have controlled access and effective physical security.

2 APPLICATION

This Standard may be adopted in all situations where protection against unauthorized disclosure is required.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS	
2805	Electronic funds transfer—Requirements for interfaces
2805.2	Part 2: Message structure, format and content
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
2805.5.4	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
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

4 DEFINITIONS

For the purpose of this Standard, the following definitions apply:

4.1 Acquirer

The institution, or its agent, which acquires, from the card acceptor, the data relating to the card transaction, and which initiates that data into an interchange system.

4.2 Card issuer

The institution, or its agent, which issues the identification card to the cardholder.

4.3 Cipher text

Enciphered information.

4.4 Data encipherment algorithm (DEA)

An algorithm designed to encipher and decipher blocks of data.

NOTE: A DEA is specified in AS 2805.5.4.

