Australian Standard™

Electronic funds transfer—
Requirements for interfaces

Part 11: Card parameter table

This Australian Standard was prepared by Committee IT/5, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 29 October 1999 and published on 10 January 2000.

The following interests are represented on Committee IT/5:

Australian Association of Permanent Building Societies

Australian Bankers Association

Australian Electrical and Electronic Manufacturers Association

Australian Information Industry Association

Australian Institute of Petroleum

Australian Retailers Association

Credit card industry

Consumers Federation of 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 Standards may also be withdrawn.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 the 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, PO Box 1055, Strathfield, NSW 2135.

This Standard was issued in draft form for comment as DR 98488.

Australian Standard™

Electronic funds transfer – Requirements for interfaces

Part 11: Card parameter table

First published as AS 2805.11—2000.

Published by Standards Australia International Ltd
PO Box 1055, Strathfield, NSW 2135, Australia

ISBN 0 7337 3077 9

PREFACE

This Standard was prepared by the Standards Australia Committee IT/5, Financial Transaction Systems, on the subject of electronic funds transfer (EFT) as one of a series on EFT requirements for interfaces.

This Standard is Part 11 of the following series:

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
2805.10	Part 10:	File transfer integrity validation
2805.11	Part 11:	Card parameter table (this Standard)
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 4.1, Message authentication using DEA 3, of the AS 2805 series is in the course of preparation.

The objective of this Standard is to provide the requirements to control parameters governing PIN entry, PAN entry, signature verification and the selection of acquirer encipherment keys.

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

In a multiple acquirer environment, the terminal cryptographic unit (TCU) maintains an independent cryptographic relationship with each party (sponsor or acquirer) defined to the TCU. This relationship, although initiated by the sponsor, must make sure that each party is cryptographically separated from each other. If this cannot be achieved, then the secrecy of PIN information cannot be ensured. The card parameter table (CPT) forms part of this separation.

The CPT also provides information that determines the route that the transaction will take when leaving the TCU. In order to prevent the opportunity for a bogus acquirer's address to be added to the CPT, a file validation value (FVV) has been specified (in AS 2805.10) to protect the contents of the CPT.

The other part of the security of the transaction is defined in the transaction handling parameters, which identifies how the acquirer wants the card holder identified, what accounts are available and to what financial limit.

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 11: Card parameter table

1 SCOPE

This Standard specifies the minimum requirements for the content of the card parameter table (CPT) for multiple acquirer TCUs.

This Standard does not cover—

(a) techniques for the conveyance of the CPT;

(b) techniques for the secure entry of the CPT; or

(c) techniques for the maintenance of the CPT.

NOTE: Examples of CPT layout, processing, and attributes are shown in Appendices A, B, and C, respectively.

2 APPLICATION

This Standard may be adopted in all situations where there is a requirement to control parameters governing PIN entry, PAN entry, signature verification and the selection of acquirer encipherment keys.

These requirements support AS 2805.6.2 and AS 2805.6.4.

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
2805.6.1	Part 6.1: Key management—Principles
2805.6.2	Part 6.2: Key management—Transaction keys
2805.6.4	Part 6.4: Key management—Session keys—Terminal to acquirer
3524	Identification cards—Financial transaction cards

4 ABBREVIATIONS AND DEFINITIONS

4.1 Abbreviations

The following abbreviations are used in this Standard:

AIIC	Acquiring institution identification code
CKT	Cryptographic key table
CPT	Card parameter table
EFT	Electronic funds transfer
IIN	Institution identification number
PAN	Primary account number
PIN	Personal identification number
TCU	Terminal cryptographic unit

