

Australian Standard[®]

**Electronic funds transfers—
Requirements for interfaces**

**Part 2: Message structures, format and
content**



This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 8 August 2006. This Standard was published on 25 January 2007.

The following are represented on Committee IT-005:

- Australian Association of Permanent Building Societies
 - Australian Bankers Association
 - Australian Electrical and Electronic Manufacturers Association
 - Australian Retailers Association
 - Credit Card Industry
 - Reserve Bank of Australia
-

This Standard was issued in draft form for comment as DR 06125.

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Standards may also be withdrawn.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 transfers—
Requirements for interfaces**

**Part 2: Message structures, format and
content**

Originated as AS 2805.2—1985.
Previous edition 2000.
Fifth edition 2007.
Reissued incorporating Amendment No. 1 (July 2008).
Reissued incorporating Amendment No. 2 (August 2008).

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia
ISBN 0 7337 7998 0

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.2—2000, *Electronic funds transfer—Requirements for interfaces, Part 2: Message structure, format and content*. During the preparation of this Standard cognizance was taken of ISO 8583, *Financial transaction card originated messages—Interchange message specifications*.

This Standard incorporates Amendment No. 1 (July 2008) and Amendment No. 2 (August 2008). 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 comprises the following:

AS

	2805	Electronic funds transfer—Requirements for interfaces
	2805.1	Part 1: Communications
	2805.2	Part 2: Message structure, format and content (this Standard)
A1	2805.3.1	Part 3.1: PIN management and security—General (in preparation)
	2805.3.2	Part 3.2: PIN management and security—Off-line with ICC verification (in preparation)
	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
	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
	2805.6.6	Part 6.6: Key management—Session keys—Node to node with KEK replacement
	2805.9	Part 9: Privacy of communications
	2805.10.1	Part 10.1: File transfer integrity validation
	2805.10.2	Part 10.2: Secure file transfer (retail)
	2805.11	Part 11: Card parameter table
	2805.12.1	Part 12.1: Message content—Structure and format
A1	2805.12.2	Part 12.2: Message content—Application and registration procedures for Institution Identification Codes (IIC)
	2805.12.3	Part 12.3: Message content—Maintenance procedures for messages, data elements and code values
	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
	2805.14.2	Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems
A1	2805.16	Part 16: Merchant Category Codes (in preparation)

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

	<i>Page</i>
FOREWORD.....	5
SECTION 1 SCOPE AND GENERAL	
1.1 SCOPE	6
1.2 REFERENCED DOCUMENTS	6
1.3 DEFINITIONS	7
1.4 MESSAGE STRUCTURE.....	9
1.5 MESSAGE FLOW	9
1.6 DATE FIELDS	9
SECTION 2 MESSAGE-TYPE IDENTIFIERS	
2.1 SCOPE	10
2.2 STRUCTURE AND ATTRIBUTE	10
2.3 MESSAGE REPEATS.....	11
2.4 IDENTIFIERS	11
2.5 TYPE AND PURPOSE	12
SECTION 3 BITMAPS	
3.1 GENERAL	13
3.2 SIGNIFICANCE OF BITS	13
3.3 PRESENCE OF SECONDARY BITMAP	13
3.4 PRIMARY BITMAP	13
3.5 SECONDARY BITMAP	13
3.6 DATA ELEMENT CHARACTERISTICS	13
3.7 FORMAT	14
3.8 ATTRIBUTE.....	14
3.9 CONDITIONS.....	15
SECTION 4 DATA ELEMENTS	
4.1 GENERAL	25
4.2 MESSAGE CONSTRUCTION.....	25
4.3 DIRECTORY OF DATA ELEMENTS	25
4.4 REQUIREMENTS FOR DATA ELEMENTS	25
APPENDICES	
A THE USE OF ADDITIONAL MESSAGES AND DATA ELEMENTS	49
B AVAILABLE MESSAGES—TYPE AND PURPOSE	50
C MESSAGE FLOWS	58
D DATA ELEMENT DIRECTORY.....	66
E IMPLEMENTATION INFORMATION.....	74
F CARD ACCEPTOR REGISTRY.....	77
G MINIMAL MESSAGE SET FOR A SESSION BETWEEN A TERMINAL AND AN ACQUIRER.....	79
H MINIMAL MESSAGE SET FOR A SESSION BETWEEN INTERCHANGES.....	87
I DATA REPRESENTATION.....	95

FOREWORD

Services of the financial industry include the exchange of electronic messages relating to financial transactions. Agreements on application specifications are generally at a private level. This Standard is designed as an interface specification enabling messages to be exchanged between systems adopting a variety of application specifications. The application specification can remain at a private level. As long as messages conform to the interface format, as prescribed in this Standard, in order for interchange to take place, all other features of applications can be altered as required.

This Standard uses a concept whereby each data element is assigned a position indicator in a control field which is known as a 'bitmap'. The presence of a data element in a specific message is indicated by a one (1) in the assigned position; the absence of a data element is indicated by a zero (0) in the assigned position.

A1

Message formats used in individual systems are subject to the commercial relationships between the parties contracting to each system. The data formats specified in this Standard are designed to ensure compatibility between systems.

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfers—Requirements for interfaces

Part 2: Message structures, format and content

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

This Standard specifies the message structure, format, content, data elements and values for data elements required for an interface by which card-originated electronic messages relating to financial transactions may be interchanged.

This Standard allows for the automated reconciliation of messages previously exchanged but makes no provision for the final exchange of funds (between two or more institutions) known as ‘settlement’.

A1

1.2 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS

2632 Codes for the representation of names of countries and their subdivisions (series)

2805 Electronic funds transfer—Requirements for interfaces

2805.12 Part 12: Message content (series)

A2 | 2805.16 Part 16: Merchant category codes

3523 Identification cards—Identification of issuers

3523.1 Part 1: Numbering system

3523.2 Part 2: Application and registration procedures

3523.3 Part 3: Australian national numbering system and registration procedures

3524 Identification cards—Financial transaction cards

3525 Bank cards—Magnetic stripe data content for Track 3

HB 99 Addressing the comparison of dates for the year 2000 and beyond

ISO

4217 Codes for the representation of currencies and funds

A1

7816 Identification cards—Integrated Circuit Cards

7816-6 Part 6: Interindustry data elements for interchange

8583 Financial transaction card originated messages—Interchange message specifications (series)

ISO/IEC

646 Information technology—ISO 7-bit coded character set for information interchange