Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 5.4: Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques

Standards Australia

This Australian Standard was prepared by Committee IT/5, Financial Transactions Systems. It was approved on behalf of the Council of Standards Australia on 31 January 2000 and published on 3 April 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 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 Standards may also be withdrawn.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 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 99239.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 5.4: Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques

First published as AS 2805.5.4—2000.

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

ISBN 0 7337 3286 0

PREFACE

This Standard was prepared by the Standards Australia Committee IT/5, Financial Transactions Systems, to provide specification of the DEA 3 ciphering algorithm and related techniques.

This Standard forms part of the AS 2805 series of Standards on electronic funds transfer (EFT) requirements for interfaces, which is published 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 (this Standard)
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 communication
2805.10	Part 10:	File transfer integrity validation
2805.11	Part 11:	Card parameter tables
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 cyptographic devices (retail)—Concepts, requirements and evaluation methods

The following Handbooks relate to 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

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, the definitions of words and phrases used are specific to the Part in which they appear.

CONTENTS

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 5.4: Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques

1 SCOPE

This Standard specifies the DEA 3 ciphering algorithm, which combines three instances of the DEA 1 algorithm defined in AS 2805.5.1 in order to achieve greater security against attack. Some related cryptographic processes of similarly higher security are also specified.

2 APPLICATION

DEA 3, as defined in this Standard, is for application in all situations where DEA 1 is now used. DEA 3 can be implemented by existing DEA 1 hardware and software and supersedes DEA 1.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS		
2805	Electronic funds transfer—Requirements for interfaces	
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
2805.6.1	Part 6.1:	Key management—Principles

4 DEFINITIONS

For the purpose of this Standard the definitions below apply.

4.1 Algorithm

A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

4.2 Authentication

The act of determining that a message comes from a source authorized to originate messages of that type and that the message is authorized.

4.3 Cipher block chaining

A mode of operation of an n-bit block cipher, as defined in AS 2805.5.2.

4.4 Cipher text

Enciphered information.

4.5 Data encipherment algorithm (DEA)

An algorithm designed to encipher and decipher blocks of data.

4.6 Decipherment

The transformation of cipher text into plain text.

NOTE: Decipherment is sometimes referred to as ‘decryption’.