Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 13.2: Secure hash functions—MD5

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 Institute of Petroleum

Australian Retailers Association

National card issuers

National network operators

Reserve Bank of Australia

Software and Services Industry Federation 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 Standards may also be withdrawn.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 98624.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 13.2: Secure hash functions— MD5

First published as AS 2805.13.2—2000.

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

ISBN 0 7337 3085 X

PREFACE

This Standard was prepared by the Standards Australia Committee IT/5, Financial Transaction Systems. Much of the content of this Standard is based on *The MD5 Message Digest Algorithm,** and acknowledgement is hereby made of the considerable assistance provided by that document.

The objective of this Standard is to specify the algorithm for the secure hash function MD5.

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
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
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 (this Standard)
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

---

* Rivest, R.L., *The MD5 Message Digest Algorithm*, RFC1321, Internet Activities Board, April 1992.

Part 4.1, Message authentication using DEA 3, of the AS 2805 series is in the course of 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 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 13.2: Secure hash functions—MD5

1 SCOPE

This Standard specifies the algorithm for the secure hash function MD5.

NOTES:

1 MD5 was developed by Rivest in 1991 and is an improved version of MD4, also developed by Rivest. It is one of a family of similar hash functions whose members include MD4, SHA, RIPEMD and HAVAL.

2 Examples of MD5 hash codes are given in Appendix A.

3 Comment on the use of this Standard are given in Appendix B.

4 A reference implementation may be found in Ref. 1 (See Appendix C).

2 APPLICATION

This Standard is for use where a secure hash function is required and where a 128–bit hash code is considered adequate.

This Standard may be used in conjunction with the key management systems specified in AS 2805.6 (all Parts) for key verification.

NOTE: Comment on the use of this Standard is given in Appendix B.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS	
2805	Electronic funds transfer – Requirements for interfaces
2805.6	Part 6: Key management (all Parts)
2805.13.1	Part 13.1: Hash functions—General

4 DEFINITIONS

For the purpose of this Standard, the definitions in AS 2805.13.1 apply.

