Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 13.1: Secure hash functions—General

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 29 October 1999.
This Standard was published on 20 January 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
- National card issuers
- National network operators
- Reserve Bank of Australia
- Software and Services Industry Federation of Australia
- Telstra Corporation

This Standard was issued in draft form for comment as DR 98623.

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Standards may also be withdrawn.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.

AS 2805.13.1—2000
(Incorporating Amendment No. 1)

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 13.1: Secure hash functions—General

First published as AS 2805.13.1—2000.
Reissued incorporating Amendment No. 1 (April 2008).

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 3088 4

PREFACE

This Standard was prepared by the Standards Australia Committee, IT-005, Financial Transaction Systems. This Standard is based on ISO/IEC 10118-1:1994, Information technology—Security techniques—Hash–functions, Part 1: General.

This Standard incorporates Amendment No. 1 (April 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 objective of this Standard is to provide specifications of secure hash functions for the providers of authentication, integrity and non-repudiation services.

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 (this Standard)
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.

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

CONTENTS

FOREWORD

Hash functions map arbitrary strings of bits to a given range. They can be used for—

(a) reducing a message to a short imprint for input to a digital signature mechanism;

(b) committing the user to a given string of bits without revealing this string; and

(c) proving the correct input of keying data which has been entered in parts or transmitted in enciphered form (key verification).

Although the purpose of this Standard is to provide a variety of hash functions that are suitable for security techniques, hash functions may be used for other purposes outside the scope of this Standard, such as simulating a random number generator.

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 13.1: Secure hash functions—General

1 SCOPE

This Standard specifies secure hash functions and is applicable to the provision of authentication, integrity and non-repudiation services.

NOTE: In contrast to the calculation of a message authentication code (MAC), the goal of which is to ensure authentication of a message using a secret key, the generation of a hash code does not involve a secret key. A method of calculation of the MAC is given in AS 2805.4.

2 APPLICATION

This Standard is for application wherever a secure hash function is required. This Standard neither mandates the use of a hash function nor warrants that the hash function selected is fit for the purpose.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS	
2805	Electronic funds transfer—Requirements for interfaces
2805.4	Part 4: Message authentication
2805.13.2	Part 13.2: Secure hash functions—MD5
AS ISO/IEC	
A1 10118	Information technology—Security techniques—Hash-functions
10118-3	Part 3: Dedicated hash-functions

4 DEFINITIONS

For the purpose of this Standard, the definitions below apply.

4.1 Authentication

A process used between a sender and a receiver, to ensure data integrity and to provide proof of data origin.

4.2 Collision resistant

Describes a property of a function in which it is computationally infeasible to find any two distinct inputs which map to the same output.

NOTE: Computational feasibility depends on the user's specific security requirements and environment.

4.3 Compression function

A function that takes a fixed-length input and returns a shorter fixed-length output. (See Clause 4.6.)

4.4 Data string (data)

The string of bits that is the input to a hash function.