AS 2805.4.2—2006

Australian Standard®

# Electronic funds transfer—Requirements for interfaces

## Part 4.2: Message authentication—Mechanisms using a hash-function



This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 31 March 2006. This Standard was published on 7 July 2006.

---

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
- Credit Card Industry
- Credit Union Services Corporation (Australia)
- Department of Defence (Australia)
- Independent EFT Services
- Reserve Bank of Australia

---

This Standard was issued in draft form for comment as DR 05490.

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 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Standards may also be withdrawn.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 transfer—Requirements for interfaces

# Part 4.2: Message authentication—Mechanisms using a hash-function

Originally as AS 2805.4.2—2001.
Second edition 2006.



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

ISBN 0 7337 7599 3

# PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems to supersede AS 2805.4.2—2001.

The objective of this Standard presents a choice of hash functions algorithms for use within the Australian Electronic Funds Transfer (EFT) environment.

This revision is to update the Standard in a number of areas, notably anomalies with MAC sizes and printing errors.

This Standard is based on the International Standard ISO/IEC 9797-2 but presents a different choice of algorithms and presentation layout. For compatibility with the ISO Standard users should choose the SHA-1 function as the hash algorithm.

This Standard forms part of the AS 2805 series of Standards on electronic funds transfer (EFT) requirements for interfaces, as follows:

| AS | | |
|---|---|---|
| 2805 | Electronic funds transfer—Requirements for interfaces | |
| 2805.1 | Part 1: | Communications |
| 2805.2 | Part 2: | Message structure, format and content |
| 2805.3.1 | Part 3.1: | PIN management and security—General |
| 2805.3.2 | Part 3.2: | PIN management and security—Offline |
| 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 |
| 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 |
| 2805.14.2 | Part 14.2: | Security, compliance checklists for devises used in magnetic stripe and card systems |

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)

128 Electronic funds transfer—Implementing message content Standards—Terminal Handbook

129 Electronic funds transfer—Implementing message content Standards—Interchange Handbook

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 4.2: Message authentication—Mechanisms using a hash-function

## 1 SCOPE

This Standard specifies two Message Authentication Code (MAC) algorithms that use a secret key and a hash-function with an $n$-bit result to calculate an $m$-bit MAC. These mechanisms are data integrity mechanisms to verify that data has not been altered in an unauthorized manner. They may also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits) $k$ and secrecy of the key, on the length (in bits) $n$ of the hash-function and its strength, on the length (in bits) $m$ of the MAC, and on the specific mechanism.

This Standard provides a method for protection against accidental or deliberate alteration of messages between sending and receiving parties.

A hash-function based file integrity mechanism is described in AS 2805.10.1.

This Standard does not provide for—

(a) the use of encryption for the protection of messages against unauthorized disclosure; or

(b) protection against message loss or duplication.

## 2 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS

1776 Information Processing—7-bit coded character set for information interchange

2805 Electronic Funds Transfer—Requirements for interfaces
2805.2 Part 2: Message structure, format and content
2805.4.1 Part 4.1: Message authentication—Mechanism using a block cipher
2805.6 Part 6: Key management—Principles
2805.10.1 Part 10.1: File transfer integrity validation
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

ISO/IEC

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

9797 Information technology—Security techniques—Message Authentication Codes (MACs)
9797-2 Part 2: Mechanisms using a dedicated hash-function



 