

Australian Standard™

**Electronic funds transfer—
Requirements for interfaces**

**Part 13.3: Secure hash functions—
SHA-1**



S t a n d a r d s A u s t r a l i a

This Australian Standard was prepared by Committee IT/5, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 5 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 Information Industry Association
Australian Institute of Petroleum
Australian Retailers Association
Credit Card Industry
Credit Union Services Corporation (Australia)
Consumers Federation of 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 Standards may also be withdrawn.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 the 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 website at www.standards.com.au and looking up the relevant Standard in the online 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.

Australian Standard™

**Electronic funds transfer—
Requirements for interfaces**

**Part 13.3: Secure hash functions—
SHA-1**

published as AS 2805.13.3—2000.

COPYRIGHT

© Standards Australia International

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 International Ltd
PO Box 1055, Strathfield, NSW 2135, Australia

ISBN 0 7337 3259 3

PREFACE

This Standard was prepared by the Standards Australia Committee IT/5, Financial Transaction Systems, to provide a specification of the algorithm for the secure hash function SHA-1.

This Standard is technically equivalent to, but does not correspond in presentation to, US Federal Information Processing Standard 180-1, and 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 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
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 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.

The term 'informative' has been used in this Standard to define the application of the appendices to which it applies. An 'informative' appendix is for information and guidance only.

CONTENTS

	<i>Page</i>
1 SCOPE	4
2 APPLICATION	4
3 REFERENCED DOCUMENTS	4
4 DEFINITIONS.....	4
5 SYMBOLS AND NOTATION	5
6 ALGORITHM DESCRIPTION	5
APPENDICES	
A EXAMPLES	8
B COMMENT ON USE.....	9
C BIBLIOGRAPHY	10

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 13.3: Secure hash functions—SHA-1

1 SCOPE

This Standard specifies the algorithm for the secure hash function SHA-1 which is one of a family of similar hash functions whose members include MD4, MD5, RIPEMD and HAVAL.

2 APPLICATION

The Secure Hash Algorithm (SHA-1) was designed for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and may be used whenever a secure hash algorithm is required. For a message of length less than 2^{64} bits, the SHA-1 produces a 160-bit condensed representation of the message called a message digest. The message digest is used during generation of a signature for the message. The SHA-1 is also used to compute a message digest for the received version of the message during the process of verifying the signature. Any change to the message in transit will usually result in a different message digest, and the signature will fail to verify.

The SHA-1 is designed so that it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest.

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

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: Secure hash functions—General

U.S. Department of Commerce/National Institute of Standards and Technology (NIST)

FIPS

- 108-1 Secure hash
- 186 Digital signature

DEFINITIONS

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