Australian Standard™

Electronic funds transfer—Requirements for interfaces

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

Standards Australia

This Australian Standard was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 30 July 2001 and published on 4 October 2001.

The following interests are represented on Committee IT-005:

Australian Association of Permanent Building Societies

Australian Bankers Association

Australian Electrical and Electronic Manufacturers Association

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 Standards may also be withdrawn.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 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, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 00372.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

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

First published as AS 2805.4.2—2001.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 4102 9

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems to provide a specification for a MAC algorithm based on the use of secure hash functions.

This Standard is based on 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 which, when published, will be 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
2805.4.1	Part 4.1:	Message authentication—Mechanism using a block cipher
2805.4.2	Part 4.2:	Message authentication—Mechanisms using a hash function (this Standard)
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
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
2805.15	Part 15:	ICC based stored value /inter-sector electronic purse—Principles

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

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

Page

FOREWORD

Financial transaction messages need to be protected from both accidental and deliberate alteration and from the introduction of fraudulent messages. A uniform process is required which facilitates —

(a) validation of the authority of the sender (customer or correspondent);

(b) verification that selected contents of the message have not been altered in transit;

(c) use by both large and small organizations; and

(d) implementation in automated systems.

This Standard defines a process for authentication of messages from sender to receiver. This process is independent of the communications media and payment systems.

The Authentication process includes the computation, transmission, and validation of a Message Authentication Code (MAC).

The MAC is based on the complete message text. It is added to the message by the sender and is transmitted to the receiver. The message is accepted as authentic by the receiver, if the same algorithm and secret key produce a MAC identical to the received MAC. Bogus or altered messages will fail such tests.

Since the algorithms are in the public domain, the security of the authentication process is directly dependent on the security afforded to the secret key. To provide this security, the user of this Standard must establish criteria for the secure generation, secure storage, and secure retrieval of the secret key.

It is the responsibility of the user to put an overall transfer process in place with the necessary controls to ensure that the process is implemented under secure procedures. Further, the controls should include application of appropriate audit and sensitivity tests in order to ensure compliance.

This Standard provides a technique for use as part of that overall process. It applies to the message from the point of MAC computation to the MAC check. Validity of the MAC computation input values and the use of the MAC computation to check output results must be a responsibility of the overall process provided by the user.

The use of this technique in no way ensures that the overall process or even the application of the technique as part of the process will, in itself, ensure secure results. The user must ensure that the overall process is secure.

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 MAC algorithms that use a secret key and a hash-function with an *n*-bit result to calculate an *m*-bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorized manner. They can 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, *File transfer integrity validation.*

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 Standards are referred to in this Standard:

AS

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
2805.6.1	Part 6.1: Key management—Principles
2805.10	Part 10: File transfer integrity validation
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

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 hash-function