Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 4.1: Message authentication—Mechanism using a block cipher

This Australian Standard was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 5 December 2000.
This Standard was published on 25 January 2001.

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
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 Standards may also be withdrawn.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 Web Shop 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 Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

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.org.au, or write to the Chief Executive, Standards Australia, GPO Box 476, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 00086.

AS 2805.4.1—2001
(Incorporating Amendment No. 1)

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 4.1: Message authentication—Mechanism using a block cipher

Originated as AS 2805.4.1—1985.
Revised and redesignated in part as AS 2805.4.1—2001.
Reissued incorporating Amendment No. 1 (February 2006).

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

ISBN 0 7337 3669 6

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems.

This Standard incorporates Amendment No. 1 (February 2006). 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 define a process for authentication of messages from sender to receiver.

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	Part 4:	Message authentication
2805.4.1	Part.4.1:	Message authentication—Mechanism using a block cipher (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.

CONTENTS

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). AS 2805.5.4 specifies a Data Encryption Algorithm (DEA) which is not designed for hand computation and which requires a secret key. It is used in this Standard to generate a 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 or message elements are 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 DEA algorithm is 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.

To support the varying operational demands of different users and their customers, the authentication algorithm can be implemented either through special equipment or computer programs. The authentication process can be performed using independent devices or as part of a computerized system.

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 a part of the process will, in itself, ensure secure results. The user must ensure that the overall process is secure.

STANDARDS AUSTRALIA

Australian
Electronic funds transfer—Requirements for interfaces

Part 4.1: Message authentication—Mechanism using a block cipher

1 SCOPE

This Standard specifies a method for authenticating card-originated electronic messages relating to financial transactions.

NOTE: The identity of the sending party is implicitly validated by proper use of this Standard. Further, this Standard provides a method for protection against accidental or deliberate alteration of messages between sending and receiving parties.

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	Message structure, format and content
A1	2805.5.1	Ciphers—Data encipherment algorithm 1 (DEA 1)
	2805.5.2	Ciphers—Modes of operation for an n-bit block cipher algorithm
	2805.5.4	Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques
	2805.12.1	Message content—Structure and format
	ISO/IEC	
A1	9797	Information technology—Security techniques—Message Authentication Codes (MACs)
	9797-1	Part 1: Mechanisms using a block cipher

3 DEFINITIONS

For the purpose of this Standard, the following definitions apply:

3.1 Algorithm

A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

3.2 Authentication

The act of determining that a message comes from a source authorized to originate messages of that type and that the message is as authorized.

