Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 10.1: File transfer integrity validation

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 6 February 2004 and published on 13 May 2004.

The following are represented on Committee IT-005:

Australian Association of Permanent Building Societies

Australian Bankers Association

Australian Electrical and Electronic Manufacturers Petroleum

Australian Retailers Association

Credit Card Industry

Reserve Bank of Australia

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 Standards may also be withdrawn.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

This Standard was issued in draft form for comment as DR 03387.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 10.1: File transfer integrity validation

Originated as AS 2805.10—1997.
Revised and redesignated as AS 2805.10.1—2004.

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

ISBN 0 7337 5923 8

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, on the subject of electronic funds transfer (EFT) as one of a series on EFT requirements for interfaces. It supersedes AS 2805.10—1997.

The AS 2805 series of Standards comprises the following:

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—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
2805.9	Part 9:	Privacy of communications
2805.10.1	Part 10.1:	File transfer integrity validation (this Standard)
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:	Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems

Parts 7 and 8 in this series have been superseded by Appendices H and J, respectively, in AS 2805.12.

The objective of this Standard is to provide users with methods to ensure the integrity of a file during transfer between communicating entities by means of an integrity check value directly calculated from the file or calculated from a hash result derived from the file.

In an EFT environment, it is sometimes necessary to transfer data files between communicating entities. For example, configuration data may need to be loaded into a secure cryptographic device (SCD) during initialization, or new parameter files may be required to be loaded into the SCD.

This Standard provides techniques to ensure that files can be transmitted across a network in an EFT environment, and that the contents of the files can be verified to be the same as those sent.

CONTENTS

STANDARDS AUSTRALIA

Australian Standard
Electronic funds transfer—Requirements for interfaces

Part 10.1: File transfer integrity validation

1 SCOPE

This Standard specifies methods for ensuring the integrity of a file during transfer between communicating entities.

Two methods are specified as follows:

(a) An integrity check value is derived cryptographically from the whole file using a secret or private key for authentication.

(b) A hash code is derived from the whole file and is authenticated by encipherment by a secret or private key.

The integrity check value is referred to as a file validation value (FVV). See Clause 4.5.

This Standard does not include any requirements about the mechanism of the file transfer process, only the way to verify the data.

This Standard does not cover techniques for ensuring the privacy of files, or techniques for the conveyance of files.

2 APPLICATION

This Standard may be adopted in all situations where there is a requirement to include an integrity check above that provided by external controls.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS		
2805		Electronic Funds Transfer—Requirements for interfaces
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
2805.5.3	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
2805.13.1	Part 13.1:	Secure hash functions—General
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	Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems

4 DEFINITIONS

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

4.1 Cryptographic key

Parameter used, in conjunction with an algorithm, for the purpose of validation, authentication, encipherment, or decipherment.