Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 10.2: Secure file transfer (retail) (ISO 15668:1999, MOD)

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 3 February 2003 and published on 18 March 2003.

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

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 Standards may also be withdrawn.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 01320.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 10.2: Secure file transfer (retail) (ISO 15668:1999, MOD)

First published as AS 2805.10.2—2003.

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

ISBN 0 7337 5056 7

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems. This Standard is an adoption with national modifications to reflect local conditions and has been reproduced from, ISO 15668:1999, *Banking—Secure file transfer (retail)*. For the purpose of this standard ISO 15668:1999, *Banking—Secure file transfer (retail)* shall be modified as set out in Annex ZA. A vertical line in the margin indicates where the base publication has been modified by Annex ZA.

The objective of this Standard is to specify the different kinds of file transfer used in the retail banking environment.

This Standard is Part 10.2 of AS 2805, *Electronic funds transfer—Requirements for interfaces*, which is published in parts 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
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:	Electronic funds transfer—Requirements for interfaces—File transfer integrity validation
2805.10.2	Part 10.2:	Secure file transfer (retail) (this Standard)
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

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

The terms 'normative' and 'informative' are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

None of the normative references in the source document have been adopted as Australian or Australian/New Zealand Standards.

As this Standard is reproduced from an International Standard, the following applies:

(a) Its number does not appear on each page of text and its identity is shown only on the cover and title page.

(b) In the source text 'this International Standard' should read 'this Australian Standard'.

(c) A full point should be substituted for a comma when referring to a decimal marker.

CONTENTS

Page

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 10.2: Secure file transfer (retail) (ISO 15668:1999, MOD)

1 Scope

In contrast to file transfers in a wholesale banking environment characterised by exchanges of large volume, between mainframes, in a relatively high-security environment ("bulk file transfers"); those in a retail banking environment are characterised by low volumes and a lower degree of reliability of environment in which downloaded devices are operated. Such devices may be, but not limited to, an electronic point of sale terminal (EPOS), an automated vending machine (AVM), an automated teller machine (ATM), or a merchant server in communication with payment gateways.

It is assumed that a pre-established relationship exists between the entities involved in the secure file transfer, especially to cover the legal and commercial aspects related to the file transfer liabilities.

This International Standard applies to the different kinds of file transfer used in retail banking environment, but does not cover transaction messages identified in ISO 8583.

The transfer may require timeliness, and requires at least one of the following security services:

— message origin authentication;

— receiver authentication;

— integrity;

— confidentiality;

— non repudiation of origin;

— non repudiation of delivery;

— auditability.

It is assumed that all data forwarded by the originator shall have been confirmed as legitimate and correct prior to the transfer.

The different types of files to be transferred could contain:

— software;

— the retail transactions which have been performed and registered, (uploading);

— technical data related to an acquirer (access parameters...), (downloading);

— application data related to an acquirer (BIN list, hot list, ...), (downloading).