Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

[ISO title: Banking—Secure cryptographic devices (retail), Part 1: Concepts, requirements and evaluation methods]

Standards Australia

This Australian Standard was prepared by Committee IT/5, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 18 November 1999 and published on 15 February 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 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 Standards may also be withdrawn.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 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.

This Standard was issued in draft form for comment as DR 99312.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

First published as AS 2805.14.1—2000.

Published by Standards Australia International Ltd
PO Box 1055, Strathfield, NSW 2135, Australia

ISBN 0 7337 3193 7

PREFACE

This Standard was prepared by the Standards Australia Committee IT/5, Financial Transaction Systems. This Standard is identical with and has been reproduced from Dual Number and Year:

ISO 13491-1:1998, *Banking—Secure cryptographic devices (retail*), Part 1: *Concepts, requirements and evaluation methods*.

The objective of this Standard is to provide designers of electronic funds transfer systems with requirements for secure cryptographic devices which incorporate cryptographic processes, and with a methodology for verifying compliance with those requirements.

This Standard is Part 14.1 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:	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 (this Standard)

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

Parts of the AS 2805 series that are in the course of preparation are 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 annex to which it applies. An ‘informative’ annex is only for information and guidance.

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 part of ISO 13491’ should read ‘this Australian Standard’.

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

References to International Standards should be replaced by references to equivalent Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian or Australian/New Zealand Standard*	
ISO		AS	
7498	Information processing systems—Open Systems Interconnection—Basic Reference Model	2777	Information processing systems—Open Systems Interconnection—Basic reference model
7498-2	Part 2: Security architecture	2777.2	Part 2: Security architecture
8908	Banking and related financial services—Vocabulary and data elements	—	
9564	Banking—Personal Identification Number management and security	—	
9564-1	Part 1: PIN protection principles and techniques	—	
9807	Banking and related financial services—Requirements for message authentication (retail)	—	
10202	Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards	—	
11568	Banking key management (retail)	—	
13491	Banking—Secure cryptographic devices (retail)	—	
13491-2	Part 2: Security compliance checklists for devices using magnetic stripe cards	—	

CONTENTS

Page

Page

Pag

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 14.1:
Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

1 Scope

This part of ISO 13491 specifies the requirements for Secure Cryptographic Devices which incorporate the cryptographic processes defined in ISO 9564, ISO 9807 and ISO 11568.

This part of ISO 13491 has two primary purposes:

1. to state the requirements concerning both the operational characteristics of SCD's and the management of such devices throughout all stages of their life cycle,

2. to standardize the methodology for verifying compliance with those requirements.

Appropriate device characteristics are necessary to ensure that the device has the proper operational capabilities and provides adequate protection for the data it contains. Appropriate device management is necessary to ensure that the device is legitimate, that it has not been modified in an unauthorized manner, e.g., by "bugging", and that any sensitive data placed within the device (e.g., cryptographic keys) has not been subject to disclosure or change.

Absolute security is not practically achievable. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of cryptographic device security. These aim for a high probability of detection of any illicit access to sensitive or confidential data should device characteristics fail to prevent or detect the security compromise.

Annex A provides an informative illustration of the concepts of security levels described in this part of ISO 13491 as being applicable to secure cryptographic devices.

This part of ISO 13491 does not address issues arising from the denial of service of a SCD.

Specific requirements for the characteristics and management of specific types of SCD functionality used in the retail banking environment are contained in another part of ISO 13491.

2 Normative references

The following standards contain provisions which, through references in this text, constitute provisions of this part of ISO 13491. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreements based upon this part of ISO 13491 should apply the most recent edition of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security architecture.*

ISO 8908:1993, *Banking and related financial services — Vocabulary and data elements.*

ISO 9564-1:—[1)], *Banking — Personal Identification Number management and security — Part 1: PIN protection priniciples and techniques.*

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail).*

ISO 10202 (all parts), *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards.*

ISO 11568 (all parts), *Banking key management (retail).*

ISO 13491-2:—[2)], *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices using magnetic stripe cards.*