AS 2805.14.2—2003
ISO 13491-2:2000

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems

[ISO title: Banking—Secure cryptographic devices (retail)—Part 2: Security compliance checklists for devices used in magnetic stripe card systems]

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 Standards may also be withdrawn.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 01316.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems

First published as AS 2805.14.2—2003.

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

ISBN 0 7337 5058 3

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems. This Standard is identical with and has been reproduced from ISO 13491-2:2000, *Banking—Secure cryptographic devices (retail)*—Part 2: *Security compliance checklists for devices used in magnetic stripe card systems*.

The objective of this Standard is to provide a security compliance checklist for evaluating secure cryptographic devices (SCDs) used in magnetic stripe systems in accordance with AS 2805.14.1:2000.

This Standard is Part 14.2 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:	File transfer integrity validation
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 (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

The terms 'normative' and 'informative' have been used in this Standard 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.

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 the following identical Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*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
13491	Banking—Secure cryptographic devices (retail)	2805	Electronic funds transfer—Requirements for interfaces
13491-1	Part 1: Concepts, requirements and evaluation	2805.14.1	Part 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

The following Australian Standards have equivalent technical content to the International Standards and may be used instead of the International Standards.

ISO		AS	
9807	Banking and related financial services—Requirements for message authentication (retail)	2805.4	Electronic funds transfer—Requirements for interfaces Part 4.1: Message authentication—Mechanism using a block cipher
11568 (all parts)	Banking—Key management (retail)	2805.6 (all parts)	Electronic funds transfer—Requirements for interfaces—Key management

AS 2805.3, *Electronic funds transfer—Requirements for interfaces,* Part 3: *PIN management and security*, contains technical information from ISO 9564-1:2002, *Banking—Personal Identification Number (PIN) management and security,* Part 1: *Basic principles and requirements for online PIN handling in ATM and POS systems* and ISO 9564-2, *Banking—Personal Identification Number management and security,* Part 2: *Approved algorithm(s) for PIN encipherment*.

CONTENTS

Page

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Use of security compliance checklists **3**
4.1 General **3**
4.2 Informal evaluation **4**
4.3 Semi-formal evaluation **4**
4.4 Formal evaluation **4**

5 Summary **4**

Annex A (normative) **Physical, logical and device management characteristics common to all secure cryptographic devices** **5**

Annex B (normative) **Devices with PIN entry functionality** **12**

Annex C (normative) **Devices with PIN management functionality** **15**

Annex D (normative) **Devices with message authentication functionality** **17**

Annex E (normative) **Devices with key generation functionality** **19**

Annex F (normative) **Devices with key transfer and loading functionality** **22**

Annex G (normative) **Devices with digital signature functionality** **26**

Annex H (informative) **Categorization of environments** **28**

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 14.2
Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card system

1 Scope

This part of ISO 13491 specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes, as specified in ISO 9564, ISO 9807 and ISO 11568, in a magnetic stripe card environment. It does not specify checklists for SCDs used in an integrated circuit card (ICC) environment.

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

In the checklists given in annexes A to H, the term “not feasible” is intended to convey the notion that although a particular attack might be technically possible it would not be economically prudent, since carrying out the attack would cost more than any benefits obtained from a successful attack. In addition to attacks for purely economic gain, malicious attacks directed toward loss of reputation need to be considered.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 13491. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 13491 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

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

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

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

ISO 9564-2, *Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment*.

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

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

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