AS 2805.14.2—2009
ISO 13491-2:2005

AS 2805.14.2—2009

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in financial transactions

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems.
It was approved on behalf of the Council of Standards Australia on 13 January 2009.
This Standard was published on 11 February 2009.

The following are represented on Committee IT-005:

- Australian Association of Permanent Building Societies
- Australian Bankers Association
- Australian Electrical and Electronic Manufacturers Association
- Australian Information Industry Association
- Australian Payments Clearing Association
- Australian Retailers Association
- Reserve Bank of Australia

This Standard was issued in draft form for comment as DR 08014.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that 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Standards may also be withdrawn.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 that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in financial transactions

Originated as AS 2805.14.2—2003.
Second edition 2009.

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

ISBN 0 7337 9014 3

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.14.2—2003, *Electronic funds transfer — Requirements for interfaces Part 14.2: Secure cryptographic devices (retail) — Security compliance checklists for devices used in magnetic stripe card systems.*

The objective of this Standard is align Australian usage with world's best practice and help promote financial transaction device interoperability.

This Standard is identical with, and has been reproduced from ISO 13491-2:2005, *Banking—Secure cryptographic devices (retail)—Part 2: Security compliance checklists for devices used in financial transactions*.

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

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this part of ISO 13491' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

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

Reference to International Standard		*Australian Standard*	
ISO		AS	
11568	Banking—Key management (retail)	2805	Electronic funds transfer—Requirements for interfaces
		2805.6.1.1	Part 6.1.1: Key management—Principals
13491	Banking—Secure cryptographic devices (retail)	2805.14.1	Part 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods
13491-1	Part 1: Concepts, requirements and evaluation methods		

The term 'normative' is used to define the application of the annex to which it applies. A normative annex is an integral part of a standard.

CONTENTS

Page

INTRODUCTION

This part of ISO 13491 specifies both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys and other sensitive information used in a retail financial services environment.

The security of retail financial services is largely dependent upon the security of these cryptographic devices.

Security requirements are based upon the premise that computer files can be accessed and manipulated, communication lines can be “tapped” and authorized data or control inputs in a system device can be replaced with unauthorized inputs. While certain cryptographic devices (e.g. host security modules) reside in relatively high-security processing centres, a large proportion of cryptographic devices used in retail financial services (e.g., PIN entry devices etc.) now reside in non-secure environments. Therefore when PINs, MACs, cryptographic keys and other sensitive data are processed in these devices, there is a risk that the devices may be tampered with or otherwise compromised to disclose or modify such data.

It must be ensured that the risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper physical and logical security characteristics and are properly managed. To ensure that SCDs have the proper physical and logical security, they require evaluation.

This part of ISO 13491 provides the security compliance checklists for evaluating SCDs used in financial services systems in accordance with ISO 13491-1. Other evaluation frameworks exist and may be appropriate for formal security evaluations e.g. parts 1 to 3 of ISO/IEC 15408 and ISO/IEC 19790, and are outside the scope of this part of ISO 13491.

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) have 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 device management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of cryptographic device security. These measures aim for a high probability of detection of any illicit access to sensitive or confidential data in the event that device characteristics fail to prevent or detect the security compromise.

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 14.2:
Secure cryptographic devices (retail)—Security compliance checklists for devices used in financial transactions

1 Scope

This part of ISO 13491 specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes, as specified in parts 1 and 2 of ISO 9564, ISO 16609 and parts 1 to 6 of ISO 11568, in the financial services environment. IC payment cards are subject to the requirements identified in this part of ISO 13491 up until the time of issue, after which they are to be regarded as a "personal" device and outside of the scope of this document.

This part of ISO 13491 does not address issues arising from the denial of service of an 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 viable, 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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

ISO 9564-2, *Banking — Personal Identification Number management and security — Part 2: Approved algorithms for PIN encipherment*

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

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

ISO 16609, *Banking — Requirements for message authentication using symmetric techniques*

ISO 18031, *Information technology — Random number generation*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13491-1 and the following apply.

3.1
auditor
one who has the appropriate skills to check, assess, review and evaluate compliance with an informal evaluation on behalf of the sponsor or audit review body