AS 2805.14.1—2011
ISO 13491-1:2007

AS 2805.14.1—2011

Australian Standard®

Electronic funds transfer—Requirements for interfaces

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

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 1 June 2011. This Standard was published on 17 June 2011.

The following are represented on Committee IT-005:

- Australian Association of Permanent Building Societies
- Australian Industry Group
- Australian Bankers Association
- Australian National Retailers Association
- Australian Payments Clearing Association
- EFTPOS Payments Australia
- Reserve Bank of Australia

This Standard was issued in draft form for comment as DR AS 2805.14.1.

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Standards may also be withdrawn.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 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

Originated as AS 2805.14.1—2000.
Second edition 2011.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9875 7

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.14.1—2000, *Electronic funds transfer—Requirements for interfaces*, Part 14.1: *Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods*.

The objective of this Standard is to align Australian usage with world's best practice and to provide designers of electronic funds transfer systems with requirements for secure cryptographic devices that incorporate cryptographic processes, and with a methodology for verifying compliance with those requirements.

This Standard is identical with, and has been reproduced from, ISO 13491-1:2007, *Banking—Secure cryptographic devices (retail)—Part* 1: *Concepts, requirements and evaluation methods.*

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	
		2805	Electronic funds transfer—Requirements for interfaces
9564	Banking—Personal Identification Number (PIN) management and security (series)	2805.3	Part 3: PIN management and security (series)
11568	Banking—Key management (retail)	2805.6.1	Part 6.1: Key management (series)
11568-1	Part 1: Principles	2805.6.1.1	Part 6.1.1: Principles
11568-2	Part 2: Symmetric ciphers, their key management and life cycle	2805.6.1.2	Part 6.1.2: Symmetric ciphers, their key management and life cycle
11568-4	Part 4: Asymmetric cryptosystems—Key management and life cycle	2805.6.1.4	Asymmetric cryptosystems—Key management and life cycle
13491-2	Banking—Secure cryptographic devices (retail), Part 2: Security compliance checklists for devices used in financial transactions	2805.14.2	Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in financial transactions

In the AS 2805 series of Standards, the definitions of terms 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.

CONTENTS

INTRODUCTION

ISO 13491 describes 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 electronic payment systems is largely dependent upon the security of these cryptographic devices. This security is based upon the premise that computer files can be accessed and manipulated, communications lines can be “tapped” and authorized data or control inputs into system equipment can be replaced with unauthorized inputs. When Personal Identification Numbers (PINs), message authentication codes (MACs), cryptographic keys and other sensitive data are processed, there is a risk of tampering or other compromise to disclose or modify such data. The risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper characteristics and are properly managed.

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 (SCDs) based on the cryptographic processes defined in ISO 9564, ISO 16609 and ISO 11568.

This part of ISO 13491 has two primary purposes:

— to state the requirements concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle, and

— 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 achievable in practical terms. 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 SCD security. These aim for a high probability of detection of any unauthorized 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 SCDs.

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

Specific requirements for the characteristics and management of specific types of SCD functionality used in the retail financial services environment are contained in ISO 13491-2.

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 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2:2005, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*