Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.1.4: Key management—Asymmetric cryptosystems—Key management and life cycle

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 08013.

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Standards may also be withdrawn.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 6.1.4: Key management—Asymmetric cryptosystems—Key management and life cycle

First published as AS 2805.6.1.4—2009.

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

ISBN 0 7337 9013 5

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems.

The objective of this Standard is to align Australian usage with world best practice and facilitate financial services interoperability.

This Standard is identical with, and has been reproduced from ISO 11568-4:2007, *Banking—Key management (retail)—Part* 4: *Asymmetric cryptosystems—Key management and life cycle*.

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 11568' 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 or Australian/New Zealand Standard*	
ISO		AS ISO/IEC	
10118 (all parts)	Information technology—Security techniques—Hash functions	10118 (all parts)	Information technology—Security techniques—Hash functions
		AS	
11568	Banking—Key management (retail)	2805	Electronic funds transfer—Requirements for interfaces
11568-1	Part 1: Principles	2805.6.1.1	Part 6.1.1: Key management—Principles
11568.2	Part 2: Symmetric ciphers, their key management and life cycle	2805.6.1.2	Part 6.1.2: Key management—Symmetric ciphers, their key management and life cycle
13491	Banking—Secure cryptographic devices (retail)	2805	Electronic funds transfer—Requirements for interfaces
13491-1	Part 1: Concepts, requirements and evaluation methods	2805.14.1	Part 14.1: Secure cryptographic devices (retail)— Concepts, requirements and evaluation methods
13491-2	Part 2: Security compliance checklists for devices used in magnetic stripe card systems	2805.14.2	Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems
ISO/IEC		AS/NZS ISO/IEC	
18033	Information technology—Security techniques—Encryption algorithms	18033	Information technology—Security techniques
18033-2	Part 2: Asymmetric ciphers	18033.2	Part 2: Asymmetric cryptosystems

Only international references or Australia/New Zealand Standards have been listed.

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

ISO 11568 is one of a series of International Standards describing procedures for the secure management of cryptographic keys used to protect messages in a retail financial services environment; e.g. messages between an acquirer and a card acceptor, or an acquirer and a card issuer.

This part of ISO 11568 addresses the key management requirements that are applicable in the domain of retail financial services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machines (ATM) transactions.

ISO 11568-2 and ISO 11568-4 describe key management techniques which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

a) key separation;

b) key substitution prevention;

c) key identification;

d) key synchronization;

e) key integrity;

f) key confidentiality;

g) key compromise detection.

This part of ISO 11568 also describes the key life cycle in the context of secure management of cryptographic keys for asymmetric cryptosystems. It states both requirements and implementation methods for each step in the life of such a key, utilizing the key management principles, services and techniques described herein and in ISO 11568-1. This part of ISO 11568 does not cover the management or key life cycle for keys used in symmetric ciphers, which are covered in ISO 11568-2.

This part of ISO 11568 is one of a series that describes requirements for security in the financial services environment, as follows:

ISO 9564-1; ISO 9564-2; ISO 9564-3; ISO/TR 9564-4; ISO 11568; ISO 13491; ISO/TR 19038.

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 6.1.4:
Key management—Asymmetric cryptosystems—Key management and life cycle

1 Scope

This part of ISO 11568 specifies techniques for the protection of symmetric and asymmetric cryptographic keys in a retail financial services environment using asymmetric cryptosystems and the life cycle management of the associated asymmetric keys. The techniques described in this part of ISO 11568 enable compliance with the principles described in ISO 11568-1. For the purposes of this document, the retail financial services environment is restricted to the interface between:

— a card-accepting device and an acquirer;

— an acquirer and a card issuer;

— an ICC and a card-accepting device.

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, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

ISO/IEC 9796-2:2002, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash functions*

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

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

ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

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

ISO 13491-2, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*