AS 2805.6.1.2—2009

Australian Standard®

# Electronic funds transfer—Requirements for interfaces

# Part 6.1.2: Key management—Symmetric ciphers, their key management and life cycle



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 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 08012.

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Standards may also be withdrawn.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 6.1.2: Key management—Symmetric ciphers, their key management and life cycle

First published as AS 2805.6.1.2—2009.



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

ISBN 0 7337 9012 7

# PREFACE

This Standard was prepared by 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 service interoperability.

This Standard is identical with, and has been reproduced from ISO 11568-2:2005, *Banking—Key management (retail)—Part 2: Symmetric ciphers, their 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 'the 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 | |
| 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 |
| 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 |
| 18033-1 | Part 1: General | 18033.1 | Part 1: Encryption algorithms—General |

Only international references that have been adopted as Australian/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 11568-2 is one of a series of standards describing procedures for the secure management of cryptographic keys used to protect messages in a retail financial services environment, for instance, 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 machine (ATM) transactions.

This part of ISO 11568 describes key management techniques which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

— key separation;

— key substitution prevention;

— key identification;

— key synchronization;

— key integrity;

— key confidentiality;

— key compromise detection.

The key management services and the corresponding key management techniques are cross-referenced in Clause 7.

This part of ISO 11568 also describes the key life cycle in the context of secure management of cryptographic keys for symmetric ciphers. 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 asymmetric ciphers, which are covered in ISO 11568-4.

In the development of the ISO 11568 series due consideration was given to ISO/IEC 11770; the mechanisms adopted and described in this part of ISO 11568 are those required to satisfy the needs of the financial services industry.

AUSTRALIAN STANDARD

# Electronic funds transfer—Requirements for interfaces

## Part 6.1.2:
## Key management—Symmetric ciphers, their 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 banking environment using symmetric ciphers and the life-cycle management of the associated symmetric keys. The techniques described enable compliance with the principles described in ISO 11568-1.

The techniques described are applicable to any symmetric key management operation. The notation used in this part of ISO 11568 is given in Annex A.

Algorithms approved for use with the techniques described in this part of ISO 11568 are given in Annex B.

## 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/IEC 10116, *Information Technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO 11568-1:2005, *Banking — Key management (retail) — Part 1: Principles*

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

ISO 13491-2:2000, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in magnetic stripe card systems*

ISO 16609:2004, *Banking — Requirements for message authentication using symmetric techniques*

ISO/IEC 18033-1, *Information technology — Security techniques — Encryption algorithms — Part 1: General*

ISO/TR 19038 [1)], *Banking and related financial services — Triple DEA — Modes of operation — Implementation guidelines*

ANSI X9.24 Part 1-2004, *Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques*

ANSI X9.65, *Triple Data Encryption Algorithm (TDEA), Implementation Standard*

1) To be published