A1 (Incorporating Amendment No. 1)

AS 2805.6.1.1—2009

Australian Standard®

Electronic funds transfer—Requirements for interfaces

A1

Part 6.1.1: Key management—Principles (ISO 11568-1:2005, MOD)

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 08011.

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Standards may also be withdrawn.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 6.1.1: Key management—Principles (ISO 11568-1:2005, MOD)

A1

Originally as AS 2805.6.1—1988.
Previous edition AS 2805.6.1—2002.
Revised and redesignated AS 2805.6.1.1—2009.
Reissued incorporating Amendment No. 1 (June 2011).

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

ISBN 0 7337 9011 9

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.6.1—2002, *Electronic funds transfer—Requirements for interfaces*—Part 6.1: *Key management—Principles*.

This Standard incorporates Amendment No. 1 (June 2011). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

The objective of this Standard is to align Australian key management usage with international principles and facilitate financial service interoperability.

A1 This Standard is an adoption with national modifications and has been reproduced from ISO 11568-1:2005, *Banking—Key management (retail)—Part 1: Principles*. Variations to ISO 11568-1:2005 for application of this Standard in Australia are set out in Appendix ZZ following the source text.

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 Standard*	
ISO		AS	
11568	Banking—Key management (retail)	2805	Electronic funds transfer—Requirements for interfaces
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
11568-4	Part 4: Asymmetric cryptosystems—Key management and life cycle	2805.6.1.4	Part 6.1.4: Key management—Asymmetric cryptosystems—Key management and life cycle

The terms 'normative' and 'informative' are used 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.

CONTENTS

Page

INTRODUCTION

The ISO 11568 series of International Standards describes procedures for the secure management of the cryptographic keys used to protect the confidentiality, integrity and authenticity of data in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this part of ISO 11568 addresses the key management requirements that are applicable in the accessible domain of retail banking services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machine (ATM) transactions.

Key management is the process whereby cryptographic keys are provided for use between authorized communicating parties and those keys continue to be subject to secure procedures until they have been destroyed. The security of the data is dependent upon the prevention of disclosure and unauthorized modification, substitution, insertion, or termination of keys. Thus, key management is concerned with the generation, storage, distribution, use, and destruction procedures for keys. Also, by the formalization of such procedures, provision is made for audit trails to be established.

This part of ISO 11568 does not provide a means to distinguish between parties who share common keys. The final details of the key management procedures need to be agreed upon between the communicating parties concerned and will thus remain the responsibility of the communicating parties. One aspect of the details to be agreed upon will be the identity and duties of particular individuals. ISO 11568 does not concern itself with allocation of individual responsibilities; this needs to be considered for each key management implementation.

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 6.1.1:
Key management—Principles (ISO 11568-1:2005, MOD)

1 Scope

This part of ISO 11568 specifies the principles for the management of keys used in cryptosystems implemented within the retail banking environment. The retail banking environment includes the interface between

— a card accepting device and an acquirer,

— an acquirer and a card issuer,

— an ICC and a card-accepting device.

An example of this environment is described in Annex B, and threats associated with the implementation of this part of ISO 11568 in the retail banking environment are elaborated in Annex C.

This part of ISO 11568 is applicable both to the keys of symmetric cipher systems, where both originator and recipient use the same secret key(s), and to the private and public keys of asymmetric cryptosystems, unless otherwise stated. The procedure for the approval of cryptographic algorithms used for key management is specified in Annex A.

The use of ciphers often involves control information other than keys, e.g. initialization vectors and key identifiers. This other information is collectively called "keying material". Although this part of ISO 11568 specifically addresses the management of keys, the principles, services, and techniques applicable to keys may also be applicable to keying material.

This part of ISO 11568 is appropriate for use by financial institutions and other organizations engaged in the area of retail financial services, where the interchange of information requires confidentiality, integrity, or authentication. Retail financial services include but are not limited to such processes as POS debit and credit authorizations, automated dispensing machine and ATM transactions, etc.

ISO 9564 and ISO 16609 specify the use of cryptographic operations within retail financial transactions for personal identification number (PIN) encipherment and message authentication, respectively. The ISO 11568 series of standards is applicable to the management of the keys introduced by those standards. Additionally, the key management procedures may themselves require the introduction of further keys, e.g. key encipherment keys. The key management procedures are equally applicable to those keys.

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 11568-2:1994, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO 11568-4:1998, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*