INTERNATIONAL STANDARD

ISO 11568-2

Second edition
2005-10-01

Banking — Key management (retail) —

Part 2: **Symmetric ciphers, their key management and life cycle**

Banque — Gestion de clés (services aux particuliers) —

Partie 2: Algorithmes cryptographiques symétriques, leur gestion de clés et leur cycle de vie

Reference number
ISO 11568-2:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 11568-2 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 11568-2:1994), which has been technically revised. It also cancels and replaces ISO 11568-3:1994, the content of which has been incorporated into this part of ISO 11568.

ISO 11568 consists of the following parts, under the general title *Banking — Key management (retail)*:

— *Part 1: Principles*

— *Part 2: Symmetric ciphers, their key management and life cycle*

— *Part 4: Asymmetric cryptosystems — Key management and life cycle*

— *Part 5: Key life cycle for public key cryptosystems [To be withdrawn and incorporated into Part 4]*

— *Part 6: Key management schemes [since withdrawn]*

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.

Banking — Key management (retail) —

Part 2: **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