INTERNATIONAL STANDARD

ISO 11568-1

Second edition
2005-06-15

Banking — Key management (retail) —

Part 1: Principles

Banque — Gestion de clés (services aux particuliers) —

Partie 1: Principes

Reference number
ISO 11568-1:2005(E)

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 11568-1 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 11568-1:1994), which has been technically revised.

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— *Part 3: Key life cycle for symmetric ciphers* [To be withdrawn and incorporated into Part 2]

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— *Part 5: Key life cycle for public key cryptosystems* [To be withdrawn and incorporated into Part 4]

Part 6 entitled *Key management schemes* has been withdrawn.

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.

Banking — Key management (retail) —

Part 1: Principles

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*