INTERNATIONAL STANDARD

ISO 11568-4

Second edition
2007-07-01

Banking — Key management (retail) —

Part 4: Asymmetric cryptosystems — Key management and life cycle

Banque — Gestion de clés (services aux particuliers) —

Partie 4: Cryptosystèmes asymétriques — Gestion des clés et cycle de vie

Reference number
ISO 11568-4:2007(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 11568-4 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, Security*.

This second edition cancels and replaces the first edition (ISO 11568-4:1998) which has been technically revised and incorporates revised text from the former part 5.

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— *Part 3: Key life cycle for symmetric ciphers (withdrawn; incorporated into Part 2)*

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

— *Part 5: Key life cycle for public key cryptosystems*

— *Part 6: Key management schemes (withdrawn)*

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.

Banking — Key management (retail) —

Part 4:
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*

ISO/IEC 14888-3, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

ISO 15782-1:2003, *Certificate management for financial services — Part 1: Public key certificates*

ISO/IEC 15946-3:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment*

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

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ANSI X9.42-2003, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*

3 Terms and definitions

For the purposes of this document, the definitions in ISO 11568-1, ISO 11568-2 and the following apply.

3.1
asymmetric cipher
cipher in which the encipherment key and the decipherment key are different, and in which it is computationally infeasible to deduce the (private) decipherment key from the (public) encipherment key

3.2
asymmetric cryptosystem
cryptosystem consisting of two complementary operations each utilizing one of two distinct but related keys, the public key and the private key, having the property that it is computationally infeasible to determine the private key from the public key

3.3
asymmetric key pair generator
secure cryptographic device used for the generation of asymmetric cryptographic keys

3.4
certificate
credentials of an entity, signed using the private key of the certification authority which issued it, and thereby rendered unforgeable

3.5
certification authority
CA
entity trusted by one or more entities to create, assign and revoke or hold public key certificates

NOTE Optionally the certification authority can create and assign keys to the entities.

3.6
communicating party
party that sends or receives the public key for the communication with the party that owns the public key

3.7
computationally infeasible
property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it

