INTERNATIONAL STANDARD

ISO 11568-4

First edition
1998-07-15

Banking — Key management (retail) —

Part 4:
Key management techniques using public key cryptography

Banque — Gestion de clés (services aux particuliers) —

Partie 4: Techniques de gestion de clés utilisant la cryptographie à clé publique

Reference number
ISO 11568-4:1998(E)

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

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.

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.

International Standard ISO 11568-4 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

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

— *Part 1: Introduction to key management*

— *Part 2: Key management techniques for symmetric ciphers*

— *Part 3: Key life cycle for symmetric ciphers*

— *Part 4: Key management techniques using public key cryptography*

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

— *Part 6: Key management schemes*

Annexes A and B form an integral part of this part of ISO 11568. Annexes C, D and E are for information only.

Introduction

ISO 11568 describes procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. Management of keys used in an Integrated Circuit Card (ICC) environment is not covered by ISO 11568.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this standard 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.

ISO 11568 is a multi-part standard.

This part of ISO 11568 describes key management techniques which are appropriate for use with public key cryptosystems, and 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 synchronisation

— key integrity

— key confidentiality

— key compromise detection

Banking — Key management (retail) —

Part 4:
Key management techniques using public key cryptography

1 Scope

This part of ISO 11568 specifies techniques for the use and protection of the cryptographic keys of public key cryptosystems, when used in a retail banking environment.

It is applicable to any organization which is responsible for implementing procedures for the protection of keys during the life cycle. The techniques described in this part of ISO 11568 enable compliance with the principles described in ISO 11568-1.

NOTE Details of the protection required during each step in the key life cycle for public key cryptosystems are specified in ISO 11568-5.

Public key cryptosystems embrace asymmetric ciphers, digital signature systems and public key distribution systems. Although this part of ISO 11568 describes techniques using these systems when specifically applied to key management, some of the techniques have equal applicability for the secure management of data.

The techniques are described for generic public key cryptosystems. Any required details which are specific to a particular system are described in an annex.

Algorithms approved for use with the techniques described in this part of ISO 11568 and the procedures for their approval are given in annex A.

Annex B provides a normative overview of public key certificate management.

Annex C provides a description of attribute certificates, a technique that enhances the functionality of public key certificates.

Annex D provides an introduction to the three types of public key cryptosystems indicated above.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 11568. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 11568 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 8824:1990, *Information technology — Open Systems Interconnection — Specification of Abstract Syntax Notation One (ASN.1)*.

ISO/IEC 8825:1990, *Information technology — Open Systems Interconnection — Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.

ISO 8908:1993, *Banking and related services — Vocabulary and data elements*.

ISO/IEC 9594-8:1990, *Information technology — Open Systems Interconnection — The Directory — Part 8: Authentication framework*.

ISO/IEC 9796:1991, *Information technology — Security techniques — Digital signature scheme giving message recovery*.

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail)*.

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an* n*-bit block cipher algorithm*.

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash functions*.

ISO 11166 (all parts), *Banking — Key management by means of asymmetric algorithms*.

ISO/IEC 11770-3:—[1)], *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*.

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

ANSI X9.30.1-1995, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry — Part 1: The Digital Signature Algorithms (DSA)*.

ANSI X9.30.2-1993, *Public Key Cryptography — Part 2*.

AS2805-5.3 *Ciphers — DEA 2*.

3 Definitions

For the purposes of this part of ISO 11568, the definitions given in ISO 8908 and the following definitions apply.

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

3.2
asymmetric key pair
a public key and related private key created by, and used with, a public key cryptosystem

3.3
certificate
the credentials of an entity, signed using the private key of the certification authority which issued it, and thereby rendered unforgeable

3.4
certification authority (CA)
a centre trusted to create and assign certificates

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

1) To be published.