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

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.

3.5
computationally infeasible
the property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it with the current or predicted power of computers

3.6
credentials
key identification data for an entity, incorporating at a minimum the entity's distinguished name and public key

NOTE Additional data may be included.

3.7
digital signature
a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protects the sender against forgery by third parties or the recipient

3.8
digital signature system
a public key cryptosystem which provides for the creation and subsequent verification of digital signatures

3.9
hash function
a one-way function which maps a set of arbitrary strings onto a set of fixed-length strings of bits

NOTE A collision-resistant hash function is one with the property that it is computationally infeasible to construct distinct inputs which map to the same output.

3.10
key agreement
the establishment of a common secret key without reference to another common secret key

3.11
key pair owner
the party to which the key pair belongs

3.12
non-repudiation of origin
the property that the originator of a message and associated cryptographic check value (digital signature) is not able to subsequently deny, with an accepted level of credibility, having originated the message

3.13
public key cryptosystem
a 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

3.14
public key distribution system
a public key cryptosystem which allows a secret key to be jointly created by two communicating entities

3.15
public key user
the party which uses the public key of another party for a cryptographic service

NOTE The Certification Authority is not a public key user.

4 Uses of public key cryptosystems in retail banking systems

In retail banking systems, public key cryptosystems are used primarily for key management; firstly for the management of the keys of symmetric ciphers, and secondly for the management of the keys of the public key cryptosystems themselves. This clause describes these applications of public key cryptosystems; the techniques employed in support of these applications are described in clause 5.

4.1 Distribution of symmetric keys

Distribution of one or more keys of a symmetric cipher may be by key transport or by key agreement.

NOTE Mechanisms for the distribution of symmetric keys are described in ISO/IEC 11770-3, where key distribution is referred to as key establishment.

4.1.1 Key transport

When key transport is used, the symmetric keys shall be enciphered using an asymmetric cipher and the resulting enciphered key block shall be transmitted to the intended recipient. Key encipherment ensures the confidentiality of the symmetric keys during distribution; the authenticity and integrity of the key block or of the complete transmitted message may be ensured by signing the block or message using a digital signature system.

Key encipherment is described in clause 5.

NOTE ISO 11166-1 describes protocols for the transport of symmetric keys. The protocols use both key encipherment and digital signatures.

4.1.2 Key agreement

When key agreement is used, the keys for the symmetric cipher shall be established by the use of a public key distribution system (see annex D). The mechanism used shall ensure the authenticity of the communicating entities.

4.2 Storage and distribution of asymmetric public keys

The public key of an asymmetric key pair needs to be distributed to, and stored by, one or more users for subsequent use as an encipherment key and/or signature verification key, or for use in a key agreement mechanism. Although this key need not be protected from disclosure, the distribution and storage procedures shall ensure that key authenticity and integrity is maintained.

NOTE Some applications are designed such that the required security is dependent on the non-disclosure of the public key.

One of the following methods may be used to ensure the authenticity and integrity of a public key during storage or distribution:

— sign the public key and associated data using a digital signature system, thereby creating a key certificate. Key certificates, and the management of the keys used to create and verify the certificates, are described in 5.3 and clause 6;

— create a MAC for the public key and associated data, using the algorithm defined by ISO 9807 and a key used only for this purpose;

— encipher the public key and associated data, using a symmetric or asymmetric cipher.

Key encipherment is described in 5.2.

The following additional method may be used to ensure the authenticity and integrity of a public key during distribution only:

— distribute the public key over an unprotected channel, and distribute a key verification value of the public key and associated data using an authenticated channel with dual controls. Key verification is described in 5.5.

4.3 Storage and transfer of asymmetric private keys

Since the private key of an asymmetric key pair does not need to be provided to any site other than that of the user, in some cases it can be kept within the secure cryptographic device that generated it. If it must be output from the device that generated it (e.g. for transport to another secure cryptographic device where it is to be used, or for backup purposes) it shall be protected from compromise by at least one of the following three techniques:

— encipherment with another cryptographic key (see 5.2);

— dividing into two or more components, such that each bit in the protected key depends on all components;

— outputting into another secure cryptographic device, which is the secure cryptographic device where it is to be used, or a secure transport device intended for this use. (If the communications path is not fully secured, then the transfer shall only be permitted inside a secure environment.)

5 Techniques for the provision of key management services

This clause describes the techniques which may be used individually or in combination, to provide the key management services introduced in ISO 11568-1. Some techniques provide multiple key management services.

It is often necessary (or desirable) to use a public key pair for multiple purposes, e.g. digital signatures and encipherment. In these cases, key separation techniques shall be employed which ensure that the system is not open to attack by transformations using the key pair.

The selected techniques shall be implemented in a secure cryptographic device. The functionality of the cryptographic device shall ensure that the implementation of a technique is such that the intended purpose of the technique is achieved.

The characteristics and management requirements for a secure cryptographic device are defined in ISO 13491-1.

5.1 Generation of an asymmetric key pair

The two keys of an asymmetric key pair are mathematically related as defined by the design of the particular public key cryptosystem. The relationship is such that it is computationally infeasible to determine the private key from the public key.

Most public key cryptosystems are based on modular arithmetic. The size of the modulus not only determines the sizes of the data and key blocks, but also the difficulty in breaking the system. Where the strength of the system is directly related to the size of the modulus, the modulus shall be chosen to be sufficiently large so as to render attacks computationally infeasible.

While ensuring that the required relationship between the two keys exists, key generation shall utilize a random or pseudo-random process such that it is not possible to predict any key or determine that certain keys within the key space are significantly more probable than others.

NOTE In some cryptosystems it is possible to use a known constant value for a part of the public key. This does not conflict with the requirement identified above.

5.2 Key encipherment

Key encipherment is a technique whereby one key is enciphered using another key. The resulting enciphered key may then be managed securely (with confidentiality and/or authenticity ensured) outside of a secure cryptographic device. A key used to perform such encipherment is called a key encipherment key (KEK).

Three differing cases of key encipherment involving asymmetric keys and ciphers are described here, namely:

a) Encipherment of a symmetric key using an asymmetric cipher.

b) Encipherment of an asymmetric key using an asymmetric cipher.

c) Encipherment of an asymmetric key using a symmetric cipher.

NOTE Key encipherment using a symmetric cipher to encipher a symmetric key is addressed in ISO 11568-2.

Although key encipherment ensures key confidentiality is maintained, other techniques may need to be employed in association with the key encipherment in order to ensure adequate key separation, e.g. key tagging (see 5.4).

5.2.1 Encipherment of a symmetric key using an asymmetric cipher

Encipherment of a symmetric key using the public key of an asymmetric cipher is typically used for the distribution of that key using a non-secure channel. The enciphered key may be a working key, or may itself be a KEK. Thus, mixed key hierarchies may be created which incorporate the keys of both symmetric and asymmetric ciphers.

NOTE Key hierarchies are described in ISO 11568-2.

The symmetric key must be formatted into a data block appropriate to the encipherment operation. As the block size of asymmetric ciphers tend to be larger than the key size of symmetric ciphers, it is usually possible to include more than one key in the data block for encipherment. Additionally, formatting information, random padding and redundancy characters may be incorporated in the data block.

5.2.2 Encipherment of an asymmetric key using an asymmetric cipher

Either the public key or the private key of an asymmetric cipher may itself be enciphered using an asymmetric cipher.

5.2.3 Encipherment of an asymmetric key using a symmetric cipher

Either the public key or the private key of an asymmetric cipher may be required to be enciphered using a symmetric cipher.

As the keys of asymmetric ciphers tend to be larger than the block size of symmetric ciphers, the asymmetric key must be formatted into multiple data blocks for encipherment. Therefore, the cipher block chaining mode of operation should be used for the encipherment operation.

NOTE 1 Modes of operation for an *n*-bit block cipher algorithm are standardized in ISO/IEC 10116.

Double-length keys shall be used in the encipherment of asymmetric private keys.

NOTE 2 Encipherment using a double-length key is described in ISO 11568-2.

5.3 Key certification

During distribution to authorized recipients, or during storage in a key database, the authenticity of a user's public key must be ensured.

Key certification is a technique which ensures the authenticity of a public key by creating a digital signature for the key and associated validation data. Prior to using the public key, a recipient checks its authenticity by verifying the digital signature.