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— *Part 3: Key life cycle for symmetric ciphers (withdrawn; incorporated into Part 2)*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

3.8
credentials
identification data for an entity, incorporating at a minimum the entity's distinguished name and public key

NOTE Additional data can be included.

3.9
cryptoperiod
time span during which a specific key is authorized for use or in which the keys for a given system may remain in effect

3.10
digital signature system
asymmetric cryptosystem that provides for the creation and subsequent verification of digital signatures

3.11
hash function
one-way function that maps a set of strings of arbitrary length on to 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 that map to the same output.

3.12
independent communication
process that allows an entity to counter-verify the correctness of a credential and identification documents prior to producing a certificate (e.g., call-back, visual identification, etc.)

3.13
key agreement
process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key

3.14
key share
one of at least two parameters related to a cryptographic key generated in such a way that a quorum of such parameters can be combined to form the cryptographic key but such that fewer than a quorum provide no information about the key

3.15
non-repudiation of origin
property that the originator of a message and associated cryptographic check value (i.e., digital signature) is not able to subsequently deny, with an accepted level of credibility, having originated the message

4 Uses of asymmetric cryptosystems in retail financial services systems

4.1 General

Asymmetric cryptosystems include asymmetric ciphers, digital signature systems and key agreement systems.

In financial services systems, asymmetric cryptosystems are used predominantly for key management; firstly for the management of the keys of symmetric ciphers, and secondly for the management of the keys of the asymmetric cryptosystems themselves. This clause describes these applications of asymmetric cryptosystems. Clause 5 describes the techniques employed in support of these applications relating to key management services and certificate management. Clause 6 describes how these techniques and methods are used in relation to the security and implementation requirements for the key pair life cycle.

4.2 Establishment and storage of symmetric keys

Keys of a symmetric cipher may be established by key transport or by key agreement. Mechanisms for key transport and key agreement are described in ISO/IEC 11770-3. The mechanisms used shall ensure the authenticity of the communicating parties.

Symmetric keys shall be stored as described in ISO 11568-2.

4.3 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 as defined in 5.6.1.

Mechanisms for the distribution of asymmetric public keys are described in ISO/IEC 11770-3.

4.4 Storage and transfer of asymmetric private keys

The private key of an asymmetric key pair does not necessarily need to be distributed to any entity. In some cases it can be maintained only within the secure cryptographic device (SCD) that generated it.

If it must be output from the SCD that generated it (e.g., for transfer to another SCD where it is to be used, or for backup purposes) it shall be protected from compromise by at least one of the following techniques:

— encipherment with another cryptographic key as defined in 5.2;

— if non-encrypted and outside an SCD, as key shares using an acceptable key segmentation algorithm (see clause 6.3.2.3 and Bibliography [8]);

— outputting into another SCD, which either is the SCD where it is to be used, or is a secure key transfer device intended for this use; if the communications path is not fully secured, then the transfer shall only be permitted inside a secure environment.

The integrity of the private key shall be ensured using one of the techniques defined in 5.6.2.

5 Techniques for the provision of key management services

5.1 Introduction

This clause describes the techniques that 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.

Asymmetric key pairs should not be used for multiple purposes. However, if a key pair is used for multiple purposes, e.g. digital signatures and encipherment, then special 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 an SCD. 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 an SCD are defined in ISO 13491-1.

5.2 Key encipherment

5.2.1 General

Key encipherment is a technique whereby one key is enciphered using another key. The resulting enciphered key may then exist securely outside of an SCD. A key used to perform such encipherment is called a key encipherment key (KEK).

Two differing cases of key encipherment involving asymmetric keys and ciphers are described here:

a) encipherment of a symmetric key using an asymmetric cipher;

b) encipherment of an asymmetric key using a symmetric cipher.

5.2.2 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, as described in ISO 11568-2, may be created which incorporate the keys of both symmetric and asymmetric ciphers.

The symmetric key shall be formatted into a data block appropriate to the encipherment operation. As the block size of asymmetric ciphers tends 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 shall be incorporated in the data block (see ISO/IEC 18033-2).

5.2.3 Encipherment of an asymmetric key using a symmetric cipher

Asymmetric keys may be enciphered using a symmetric cipher.

As the keys of asymmetric cryptosystems tend to be larger than the block size of symmetric ciphers, the asymmetric key may be formatted into multiple data blocks for encipherment. Therefore, the cipher block chaining mode of operation (see ISO/IEC 10116) or an equivalent operation shall be used for encipherment.

Due consideration shall be paid to known attacks when assessing the equivalent strength of various cryptographic algorithms. Generally an algorithm can be said to provide s bits of strength where the best-known attack would take, on average, $2^{s-1}T$ to attack, where T is the amount of time that is required to perform one encryption of a plaintext value and comparison of the result against the corresponding ciphertext value.

For example in ISO/IEC 10116, an attack against 112-bit TDEA is presented that requires O(k) space and $2^{120-\log k}$ operations, where k is the number of known plaintext-ciphertext pairs. As discussed in reference [11], given 2^{40} known plaintext-ciphertext pairs, this reduces the strength of two-key (112-bit) TDEA to 80 bits. Recommended equivalent key sizes at the time of publication are given in Table 1. In assessing these numbers, consideration must be paid to any further developments in cryptanalysis, factoring and computing generally.

NOTE Currently, in the retail banking environment, where TDEA keys are used for protecting other keys, and are changed such that the collection of quantities of plaintext/ciphertext pairs sufficient to significantly weaken the underlying cipher is improbable, 112-bit TDEA can be considered to offer sufficient security for the protection of 168-bit TDEA and 2 048-bit RSA keys.

Table 1 — Encryption algorithms — Equivalent strengths

Effective strength	Symmetric	RSA	Elliptic curve
80	112-bit TDEA (with 2^{40} known pairs)	1 024	160
112	112-bit TDEA (with no known pairs)	2 048	224
	168-bit TDEA		

5.3 Public key certification

Key certification is a technique that, when used in accordance with ISO 15782-1, 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.

The public key and associated validity data for the owner are together known as the owner's credentials. The validity data typically incorporates owner and key identification data, and key validity data (e.g., expiry date). A key certificate is issued by a trusted third party referred to as the Certification Authority. A key certificate is created by signing the owner's credentials using a private key owned by the Certification Authority and used only for this purpose.

An independent communication shall be used to verify that the identification of the key and its owner are correct and authorized. This may require confirmation obtained via a different channel from the one whereby the information was originally obtained.

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

5.4 Key separation techniques

5.4.1 General

In order to ensure that a stored key is useable only for its intended purpose, key separation for stored keys shall be provided by one or more of the following:

a) physically segregating stored keys as a function of their intended purpose;

b) storing a key enciphered under a key encipherment key dedicated to encipherment of a specific type of key;

c) modifying or appending information to a key as a function of its intended purpose, prior to encipherment of the key for storage i.e., key tagging.

5.4.2 Key tagging

5.4.2.1 General

Key tagging is a technique for identifying the type of a key existing outside a secure cryptographic facility and the uses to which that key can be put. The key value and its privileges are bound together in a manner that prevents undetectable modifications to either.

5.4.2.2 Explicit key tagging

Explicit key tagging involves the use of a field containing information defining the limits of privilege for the associated key and key type. This field is bound together with the key value in a manner that prevents undetectable modifications to either.

5.4.2.3 Implicit key tagging

Implicit key tagging does not rely on the use of an explicit field containing information defining the limits of privilege for the associated key and key type, but rather relies on other characteristics of the system such as the position of the key in the record, or the associated functions to determine and limit the rights and privileges of the key.

5.5 Key verification

Key verification is a technique that allows the value of a key to be checked and verified, without exposing any secret values and without using public key certificates. The technique utilizes a key verification code (KVC) that is cryptographically related to the key via a collision-resistant one-way function. For example, the reference KVC may be computed as the hash of the public or private key and associated data using an algorithm defined in ISO/IEC 10118.