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— *Part 3: Key life cycle for symmetric ciphers* [To be withdrawn and incorporated into Part 2]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— *Part 5: Key life cycle for public key cryptosystems* [To be withdrawn and incorporated into Part 4]

Part 6 entitled *Key management schemes* has been withdrawn.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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 11568-2, ISO 11568-4 and the following apply.

3.1
asymmetric key pair
public key and related private key created by and used with a public key cryptosystem

3.2
cipher
pair of operations that effect transformations between plaintext and ciphertext under the control of a parameter called a key

NOTE The encipherment operation transforms data (plaintext) into an unintelligible form (ciphertext). The decipherment operation restores the original data.

3.3
cryptographic algorithm
SET OF RULES FOR THE TRANSFORMING OF DATA USING A CRYPTOGRAPHIC KEY SUCH AS:

a) the transformation from plaintext to ciphertext and vice versa (i.e. a cipher);

b) generation of keying material;

c) digital signature computation or validation

3.4
cryptographic key
parameter that determines the operation of a cryptographic algorithm

3.5
cryptosystem
set of cryptographic primitives used to provide information security services

3.6
data integrity
property that data has not been altered or destroyed in an unauthorized manner

3.7
dictionary attack
attack in which an adversary builds a dictionary of plaintext and corresponding ciphertext

NOTE When a match is able to be made between intercepted ciphertext and dictionary-stored ciphertext, the corresponding plaintext is immediately available from the dictionary.

3.8
digital signature
result of an asymmetric cryptographic transformation of data that allows a recipient of the data to validate the origin and integrity of the data and protects the sender against forgery by third parties or the recipient

3.9
message authentication code
MAC
code in a message between an originator and recipient used to validate the source and part or all of the text of a message

NOTE The code is the result of an agreed calculation.

3.10
private key
portion of an asymmetric key pair, the value of which is secret

3.11
public key
portion of an asymmetric key pair, the value of which can be made public

3.12
secret key
cryptographic key used in a symmetric cipher system

4 Aspects of key management

4.1 Purpose of security

Messages and transactions in a retail banking system contain both cardholder sensitive data and related financial information. The use of cryptography to protect this data reduces the risk of financial loss by fraud, maintains the integrity and confidentiality of the systems, and instils user confidence in business provider/retailer relationships. To this end, system security shall be incorporated into the total system design. The maintenance of security and system procedures over the keys in such systems is called key management.

4.2 Level of security

The level of security to be achieved needs to be related to a number of factors, including the sensitivity of the data concerned and the likelihood that it will be intercepted; the practicality of any envisaged encipherment process; and the cost of providing (and breaking) a particular means of security. It is therefore necessary for communicating parties to agree on the key management procedures and extent and detail of security as specified in ISO 13491 (all parts).

4.3 Key management objectives

The primary objectives of key management are to provide those keys needed to perform the required cryptographic operations and to control the use of those keys. Key management also ensures that those keys are protected adequately during their life cycle. The security objectives of key management are to minimize the opportunity for a breach of security, to minimize the consequences or damages of a security breach, and to maximize the probability of detection of any illicit access or change to keys that may occur, despite preventive measures. This applies to all stages of the generation, distribution, storage, use and archiving of keys, including those processes that occur in cryptographic equipment and those related to communication of cryptographic keys between communicating parties.

NOTE This part of ISO 11568 covers the above issues. Total system security also includes such issues as protecting communications, data processing systems, equipment and facilities.

5 Principles of key management

Compliance with the following principles is required in order to protect keys from threats to subvert a retail banking system.

a) Keys shall exist only in those forms permitted by ISO 11568.

b) No one person shall have the capability to access or ascertain any plaintext secret/private key.

c) Systems shall prevent the disclosure of any secret/private key that has been or will be used to protect any data.

d) Secret/private keys shall be generated using a process such that it is not possible to predict any resultant value or to determine that certain values are more probable than others from the total set of all the possible values.

e) Systems should detect the attempted disclosure of any secret/private key and the attempted use of a secret/private key for other than its intended purpose.

f) Systems shall prevent or detect the use of a secret/private key, or portion of that key, for other than its intended purpose, and the accidental or unauthorized modification, use, substitution, deletion or insertion of any key.

g) A key shall be replaced with a new key within the time deemed feasible to determine the old key.

h) A key shall be replaced with a new key within the time deemed feasible to perform a successful dictionary attack on the data enciphered under the old key.

i) A key shall cease to be used when its compromise is known or suspected.

j) The compromise of a key shared among one group of parties shall not compromise keys shared among any other group of parties.

k) A compromised key shall not provide any information to enable the determination of its replacement.

l) A key shall only be loaded into a device when it may be reasonably assured that the device is secure and has not been subjected to unauthorized modification or substitution.

6 Cryptosystems

6.1 Overview

A cryptosystem is a general term referring to a set of cryptographic primitives used to provide information security services. Most often the term is used in conjunction with primitives providing confidentiality, i.e. encryption. Such systems are referred to as cipher systems. The key management practices described in this part of ISO 11568 may utilize these cryptosystems or may be applied to the keys of these cryptosystems.

6.2 Cipher systems

A cipher system comprises an encipherment operation and the inverse decipherment operation. Additionally it may include other aspects such as padding rules and key management requirements. Encipherment transforms plaintext to ciphertext using an encipherment key; decipherment transforms the ciphertext back to plaintext using a decipherment key. Retail banking applications employ cipher systems to protect sensitive cardholder and financial transaction data. The data to be protected is enciphered by the originator and subsequently deciphered by the receiver. There are two types of cipher systems:

a) symmetric;

b) asymmetric.

Whilst this clause illustrates cipher systems for protecting data, the applicability of ISO 11568 includes the protection and management of keys used in other cryptographic techniques such as key derivation, message authentication, digital signatures and related functions.

6.3 Symmetric cipher systems

A symmetric cipher system is one in which the encipherment key and decipherment key are equal. The keys are kept secret at both the originator and recipient locations. Possession of the secret key(s) permits secure communications between the originator and recipient. An example of a symmetric cipher system is shown in Figure 1.

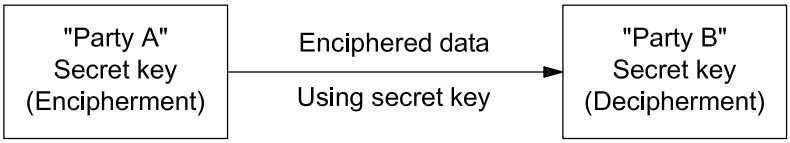

Figure 1 — Example of a symmetric cipher system

If a symmetric cipher system is implemented with appropriate key management techniques coupled with secure cryptographic devices, it may distinguish each end and support uni-directional key services. If the same set of keys provides protection of data transmitted in both directions, it is known as bi-directional keying. When a different set of keys is used to provide protection of data transmitted in each direction, it is known as uni-directional keying.

The key management principles shall be properly applied to ensure the confidentiality, integrity and authenticity of the secret keys.

6.4 Asymmetric cipher systems

An asymmetric cipher system is one in which the encipherment key and decipherment key are different, and it is computationally infeasible to deduce the decipherment key from the encipherment key. The encipherment key of an asymmetric cipher may be made public while the corresponding decipherment key is kept secret. The keys are then referred to as the public key and the private key.

Figure 2 — Example of an asymmetric cipher system

The characteristics of asymmetric cipher systems require that the recipient hold a private key with which the data may be deciphered. A public key is used by the originator to encipher the data. Thus, asymmetric cipher systems are uni-directional in nature, i.e. a pair of public and private keys provides protection for data transmitted in one direction only. Public knowledge of the public key does not compromise the cipher system. When protection for data transmitted is required in both directions, two sets of public and private key pairs are required. One common use for asymmetric ciphers is the secure distribution of initial keys for symmetric cipher systems.

The key management principles shall be properly applied to ensure the confidentiality of the private key and the integrity and authenticity of both the public and private keys.

6.5 Other cryptosystems

The key management practices described in this part of ISO 11568 may equally be applied to keys used in other cryptosystems, e.g. message authentication systems, digital signature systems or key establishment systems. As an example of a cryptosystem, Figure 3 illustrates an asymmetric cryptosystem used for data authentication through the use of digital signatures.