INTERNATIONAL STANDARD

ISO 11568-1

First edition
1994-12-01

Banking — Key management (retail) —

Part 1: Introduction to key management

Banque — Gestion de clés (services aux particuliers) —

Partie 1: Introduction à la gestion de clés

Reference number
ISO 11568-1:1994(E)

Contents

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Annexes

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 approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 11568-1 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services,* Subcommittee SC 6, *Financial transaction cards, related media and operations.*

ISO 11568 consists of the following parts, under the general 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 for asymmetric ciphers*

— *Part 5 : Key life cycle for asymmetric ciphers*

— *Part 6 : Key management schemes*

Annex A forms an integral part of this part of ISO 11568. Annexes B, C and D 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. Key management of keys used in an Integrated Circuit Card (ICC) environment is not covered by ISO 11568 but will be addressed in another ISO standard.

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.

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 enciphered 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.

ISO 9564 and ISO 9807 specify the use of cryptographic operations within retail financial transactions for personal identification number (PIN) encipherment and message authentication, respectively. ISO 11568 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.

This page intentionally left blank

Banking — Key management (retail) —

Part 1:
Introduction to key management

1 Scope

This part of ISO 11568 specifies the principles for the management of keys used in cipher systems implemented within the retail banking environment. The retail banking environment involves the interface between a card accepting device and an acquirer and between an acquirer and a card issuer. An example of this environment is described in annex B, and threats associated with the implementation of this standard in the retail banking environment are elaborated in annex C.

This part of ISO 11568 applies both to the keys of symmetric cipher systems, where both originator and recipient use the same secret key(s), and to the secret and public keys of asymmetric cipher systems, 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 applied 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.

2 Normative reference

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

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

3 Definitions

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

3.1 cryptographic algorithm : A set of rules specifying the procedures required to perform encipherment and decipherment of data. The algorithm is designed so that it is not possible to determine the control parameters (e.g. keys) except by exhaustive search.

3.2 cryptographic key; key : The control parameter of a cryptographic algorithm that cannot be deduced from the input and output data except by exhaustive search.

3.3 dictionary attack : Attack in which an adversary builds a dictionary of plaintext and corresponding ciphertext. When a match is able to be made between intercepted ciphertext and dictionary-stored ciphertext, the corresponding plaintext is immediately available from the dictionary.

4 Introduction to 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 instills 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 extent and detail of security and key management procedures.

4.3 Key management objectives

The primary objective of key management is to provide the users with those keys that they need 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 1 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 key ;

c) systems shall prevent the disclosure of any secret key that has been used to encipher any still-secret data ;

d) systems shall detect the disclosure of any secret key ;

e) systems shall prevent or detect the use of a secret key for other than its intended purpose, and the accidental or unauthorized modification, substitution, deletion or insertion of any key ;

f) secret keys shall be generated using a process such that it is not possible to predict any secret value or to determine that certain values are more probable than others from the total set of all the possible values ;

g) systems should detect the attempted disclosure of any secret key, the attempted use of a secret key for other than its intended purpose, and the unauthorized modification, substitution, deletion or insertion of any key ;

h) a key shall be replaced with a new key within the time deemed feasible to determine the old key ;

i) 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 ;

j) a key shall cease to be used when its compromise is known or suspected ;

k) a compromise of a key shared among one group of parties shall not compromise keys shared among any other group of parties ;

l) a compromised key shall not provide any information to enable the determination of its replacement ;

m) 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 Cipher systems

A cipher system comprises an encipherment operation and the inverse decipherment operation. 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: symmetric and asymmetric.

6.1 Symmetric ciphers

A symmetric cipher is one in which the encipherment key and decipherment key are equal or may be easily deduced from one another. 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.

NOTE — Encipherment key A = Decipherment key B.

Figure 1 — Example of a symmetric cipher system

A symmetric cipher system itself does not distinguish either end in the system. However, if a symmetric cipher system is implemented with appropriate key management techniques coupled with secure cryptographic devices, it may distinguish each end and support unidirectional key services. If the same set of keys provides protection (e.g. encipherment, authentication, etc.) of secret data transmitted in both directions, it is known as bidirectional keying. When a different set of keys is used for protection of secret data transmitted in each direction, it is known as unidirectional keying.

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

6.2 Asymmetric ciphers

An asymmetric cipher 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 secret key. An example of an asymmetric cipher system is shown in figure 2.

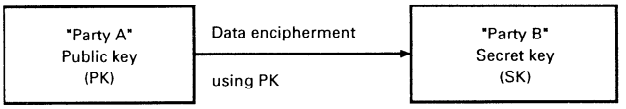

Figure 2 — Example of an asymmetric cipher system

The characteristics of asymmetric cipher systems require that the recipient hold a secret key with which the secret data may be deciphered. A different, non-secret (public) key is used by the originator to encipher the secret data. Thus, asymmetric cipher systems are unidirectional in nature, i.e. a pair of public and secret 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 secret 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 secret key and the integrity and authenticity of both the public and secret keys.

7 Cryptographic environments

For both symmetric and asymmetric cipher systems, the confidentiality of the secret keys and the integrity of both public and secret keys during storage and use depends upon a combination of the following two factors :

a) the security of the hardware device performing the cryptographic processing and storage of the keys and other secret data (as described in 7.1) ; and

b) the security of the environment in which the cryptographic processing and storage of the keys and other secret data occurs (as described in 7.2).

Absolute security is not practically achievable; therefore, key management procedures should implement preventive measures to reduce the opportunity for a breach in security and aim for a "high" probability of detection of any illicit access to secret or confidential data should these preventive measures fail.

7.1 Secure cryptographic device

A secure cryptographic device is a device that provides secure storage for secret information such as keys and provides security services based on this secret information. The characteristics and management of such devices will be addressed in another ISO standard.

7.2 Physically secure environment

A physically secure environment is one that is equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment.

Examples of a physically secure environment are a safe or a purpose-built room with continuous access control, physical security protection, and monitoring.

A physically secure environment shall remain such until all keys or other secret data and useful residue from such secret data have been removed from the environment or destroyed.

7.3 Security considerations for secret keys

Plaintext secret keys shall exist only within a secure cryptographic device or within a physically secure environment.

Plaintext secret key(s) whose compromise would affect multiple parties shall exist only within a secure cryptographic device. Plaintext secret key(s) whose compromise would affect only one party shall exist only within a secure cryptographic device or a physically secure environment operated by, or on behalf of, that party.

7.4 Security considerations for public keys

In principle, there is no need to provide protection to prevent disclosure of public keys. However, physical or logical protection shall be provided to prevent the unauthorized substitution of a public key. In addition to protecting against public key substitution, protection shall be provided to prevent the unauthorized disclosure of any secret data to be enciphered under a public key.

7.5 Protection against counterfeit devices

Protection shall be provided to prevent or detect the legitimate device from being replaced with a counterfeit having, in addition to its legitimate capabilities, unauthorized abilities that might result in the disclosure of secret data prior to encipherment.

8 Key management services for symmetric ciphers

Key management services are employed with symmetric cipher systems to ensure compliance with the key management principles listed in clause 5. These services are briefly described below. (Techniques used to provide these services are addressed in ISO 11568-2).

8.1 Separation

Key separation ensures that cryptographic processing may operate only with the specific functional key types, e.g. message authentication code (MAC) key, for which it was designed. Since keys are input to cryptographic functions in enciphered form, or recalled in clear form from secure storage within the cryptographic device, key separation may be achieved by varying the process under which they are enciphered or stored.

8.2 Substitution prevention

Key substitution prevention prohibits keys that are appropriate for use in a specific function from being used by parties, or at times, other than those for which they are intended, e.g. keys may not be used by an unauthorized party or after the keys have expired.

8.3 Identification

Key identification enables the transaction recipient to determine the appropriate key(s) associated with the transaction.

8.4 Synchronization (availability)

Cryptographic synchronization enables an originator and a recipient to ensure that the appropriate key is used when a key change occurs.

8.5 Integrity

Key integrity is ensured by verifying that the key has not been altered.

8.6 Confidentiality

Key confidentiality ensures that secret keys are never disclosed.

8.7 Compromise detection

In some situations it is not possible or feasible to prevent a security compromise, but adverse results from the compromise may be avoided or limited if the compromise is detected. Security compromises are detected by means of controls and audits.

9 Key life cycle for symmetric ciphers

Key management involves the generation of suitable keys, their distribution to and use by authorized recipients, and their termination once they are no longer required. To protect keys during their lifetime in a manner necessary to comply with the key management principles listed in clause 5, keys are processed through a series of stages, which are briefly described below. This entire procedure is called the key life cycle. (More detailed information on the key life cycle for symmetric ciphers is provided in ISO 11568-3).

9.1 Generation

Key generation involves the creation of a new key for subsequent use.

9.2 Storage

Key storage involves the holding of a key in one of the permissible forms.

9.3 Backup

Key backup occurs when a protected copy of a key is kept in storage during its operational use.

9.4 Distribution and loading

Key distribution and loading is the process by which a key is manually or electronically transferred into a secure cryptographic device.

9.5 Use

Key use occurs when a key is employed for the cryptographic purpose for which it was intended.

9.6 Replacement

Key replacement occurs when one key is substituted for another when the original key is known or suspected to be compromised or the end of its operational life is reached.

9.7 Destruction

Key destruction ensures that an instance of a key in one of the permissible key forms no longer exists at a specific location. Information may still exist at the location from which the key may be feasibly reconstructed for subsequent use.

9.8 Deletion

Key deletion is the process by which an unwanted key, and information from which the key may be reconstructed, is destroyed at its operational storage/use location. A key may be deleted from one location and continue to exist at another, e.g. for archival purposes.

9.9 Archive

Key archive is the process by which a key that is no longer in operational use at any location is stored.

9.10 Termination

Key termination occurs when a key is no longer required for any purpose and all copies of the key and information required to regenerate or reconstruct the key have been deleted from all locations where they ever existed.