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— *Part 3: Key life cycle for symmetric ciphers* [To be withdrawn and incorporated into Part 2]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— *Part 5: Key life cycle for public key cryptosystems* [To be withdrawn and incorporated into Part 4]

Part 6 entitled *Key management schemes* has been withdrawn.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

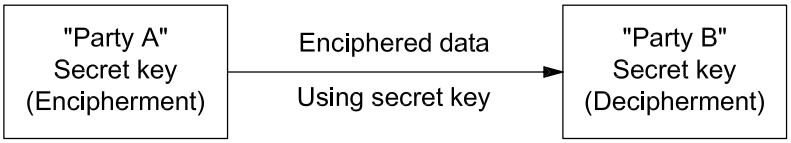

Figure 1 — Example of a symmetric cipher system

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.

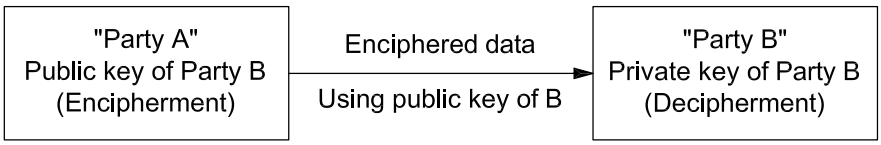

Figure 2 — Example of an asymmetric cipher system

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.

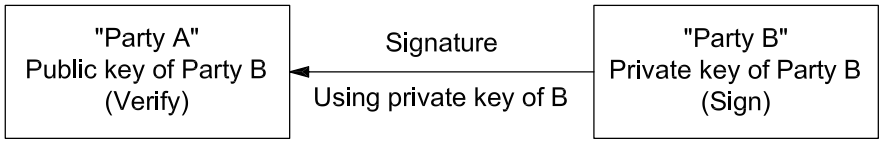

Figure 3 — Example of an asymmetric cryptosystem used for data authentication

The characteristics of asymmetric digital signature systems require that the recipient hold an authenticated public key with which the signature may be verified. A private key is used by the originator to generate the signature of the data.

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.

7 Physical security for cryptographic environments

7.1 Physical security considerations

For both symmetric and asymmetric cipher systems, the confidentiality of the secret/private keys and the integrity and authenticity of public and secret/private 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 confidential data (as described in 7.2); and

b) the security of the environment in which the cryptographic processing and storage of the keys and other confidential data occurs (as described in 7.3).

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/private keys or other confidential data should these preventive measures fail.

7.2 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 are addressed in ISO 13491 (all parts).

7.3 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 confidential 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 plaintext keys and useful residues have been destroyed.

8 Security considerations

8.1 Cryptographic environments for secret/private keys

Plaintext secret/private keys shall exist only within a secure cryptographic device or within a physically secure environment as described below.

Plaintext secret/private key(s) whose compromise would affect more than one party shall exist only within a secure cryptographic device. Plaintext secret/private 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. A multiple party example would be an acquirer ATM environment and a single party example would be an in-house private card personalization system.

8.2 Cryptographic environments 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.

8.3 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.

9 Key management services for cryptosystems

9.1 General

Key management services are employed with symmetric and asymmetric cryptosystems 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 and ISO 11568-4.

9.2 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 secret/private 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.

9.3 Substitution prevention

Key substitution prevention prohibits the unauthorized replacement of keys.

While Clause 5 f) dictates that the selection of the appropriate key in any system shall be such that no inappropriate use of the key occurs, e.g. in another cryptographic domain, there is no specific key management service that accomplishes this requirement. Attention should be given to this requirement during the design of any cryptosystem.

9.4 Identification

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

9.5 Synchronization (availability)

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

9.6 Integrity

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

9.7 Confidentiality

Key confidentiality ensures that secret/private keys are never disclosed.

9.8 Compromise detection

Where security has been compromised, adverse results may be avoided or limited if the compromise is detected. Security compromises are detected by means of controls and audit.

10 Key life cycles

10.1 General

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.

10.2 Common requirements for key life cycles

The following requirements apply to both symmetric and asymmetric key life cycles unless specifically stated. Detailed information on key life cycles can be found in ISO 11568-2 and ISO 11568-4.

10.2.1 Generation

Key generation involves the creation of a new key, or key pair in the case of asymmetric ciphers, for subsequent use.

10.2.2 Storage

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

10.2.3 Backup

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

10.2.4 Distribution and loading

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

Public key distribution and loading is the process by which a key is manually or electronically transferred to the intended users.

10.2.5 Use

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

10.2.6 Replacement

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

10.2.7 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.

10.2.8 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.

10.2.9 Archive

Key archiving is the process of securely storing keys that are no longer in operational use.

10.2.10 Termination

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

10.2.11 Erasure summary

	Location	Information affected	
		Instance of a key	Information for reconstruction
Destruction	Single	Single instance erased	
Deletion	Single	All instances erased	Erased
Termination	All	All instances erased	Erased

10.3 Additional requirements for asymmetric cryptosystems

The following life cycle requirements are specific for asymmetric cryptosystems, details of which can be found in ISO 11568-4.

10.3.1 Authenticity prior to use

The authenticity of the public key needs to be assured prior to its use and throughout its life.

10.3.2 Public key revocation

The process whereby the public key is terminated as a result of known, suspected, or likely compromise of the corresponding private key, i.e. emergency revocation.

10.3.3 Public key expiration

The process whereby the public key is withdrawn from service on reaching the end of its planned life cycle.

Annex A
(normative)

Procedure for approval of additional cryptographic algorithms

A.1 Approved algorithms

ISO 11568-2 and ISO 11568-4 detail algorithms already approved for use in a retail banking environment. Only algorithms approved by ISO/IEC JTC1/SC27 and subsequently confirmed by ISO TC68/SC2 are candidates for inclusion in this part of ISO 11568. To obtain approval for additional cryptographic algorithms, a submission has to be made to ISO TC68/SC2 provided approval is already held from ISO/JTC1/SC27.

A.2 Approval process

The following procedure for approval of an algorithm for use with this part of ISO 11568 shall be used by ISO TC68.

A.2.1 Justification of proposal

ISO/TC 68 shall require the originator to justify a proposal by describing:

a) the purpose the proposal is to serve;

b) how this purpose is better achieved by the proposal than algorithms already in the ISO 11568 series of standards;

c) additional merits not described elsewhere;

d) experience in use with the new algorithm.

A.2.2 Documentation

The proposed algorithm shall be completely documented when submitted for consideration. The documentation shall include:

e) a full description of the algorithm proposed;

f) a clear acknowledgement that the algorithm satisfies, or is compatible with, all the requirements of this part of ISO 11568;

g) a definition and explanation of any new terms, factors, or variables introduced;

h) a step-by-step example illustrating the operation of the algorithm;

i) detailed information on any prior testing to which the proposed algorithm has been subjected, particularly concerning its security, reliability and stability. Such information should include an outline of the testing procedures used, the results of the tests, and the identity of the agency or group performing the tests and certifying the results (that is, sufficient information should be provided to enable an independent agency to conduct the same tests and to compare the results achieved).

A.2.3 Public disclosure

Any algorithm submitted for consideration shall be free of security classification. If copyright or patent application has been made on the algorithm, the originator shall submit the appropriate letter stating that the originator is willing to grant a license under these copyrights and patents on reasonable and non-discriminatory terms and conditions to anyone wishing to obtain such a license to allow free and unconditional use by testers, users and suppliers of supporting equipment or material. All documentation and information submitted with the request for consideration of the algorithm shall be considered public information available to any individual, organization or agency for review, testing and usage.

A.2.4 Examination of proposals

ISO/TC 68 shall examine and prepare a report on each new proposal submitted. The report shall normally be sent to the ISO/TC 68 Secretariat within 180 days of receipt of the proposal (see A.2.5). The report shall state if the proposal is adequately documented, if it has been properly tested and certified already, and if the proposed algorithm satisfies the conditions and requirements of this part of ISO 11568. The examination may also include submission of the proposal for public review (see A.2.5)

The ISO/TC 68 Secretariat shall determine in each case whether such report and recommendations are best prepared by correspondence between the members or by a meeting. If a meeting is to be held, at least 60 days notice of the date shall be given. The papers to be dealt with at the meeting shall be provided 60 days prior to that meeting.

Where a majority of members of ISO/TC 68 recommends the rejection of the proposal, the Secretariat shall notify the originator, in writing, advising of the rejection and the reasons for it.

A.2.5 Public review

ISO/TC 68 shall forward proposals that it considers should be accepted (and which have not already been subjected to extensive testing or experience) to selected agencies or institutions with an international reputation in this field. These agencies and institutions will be requested to examine and report on the proposals within 90 days of receipt.

This period of public review may extend the 180 days allowed for ISO/TC 68 to prepare its overall report on the proposal (see A.2.4).

A.2.6 Appeal procedure

Originators whose proposals are rejected by ISO/TC 68 (see A.2.4) may ask the Secretariat of ISO/TC 68 to have the proposals subjected to public review (see A.2.5) if this has not already been done. If, following submission of the public review reports, ISO/TC 68 still recommends rejection, the originator may request the ISO/TC 68 Secretariat to circulate the proposal, together with copies of all relevant reports on it, for ballot by P-members of the subcommittee whose ruling in the matter shall be final.

A.2.7 Incorporation of new algorithms

New algorithms recommended for acceptance by ISO/TC 68, together with relevant reports on them, shall be circulated for letter ballot by the Secretariat of ISO/TC 68 to all P-members of the subcommittee. Proposals approved as a result of this process shall be forwarded to the secretariat of ISO/TC 68 for action. Once approval is given, the new encipherment algorithm shall be added to the ISO 11568 series of standards.

A.2.8 Maintenance

An algorithm approved by the method described in this part of ISO 11568 shall be reviewed at intervals of no more than five years.

Annex B
(informative)

Example of a retail banking environment

B.1 General

This annex presents an example of the different parties involved in the retail banking environment. Transaction processing systems are composed of subsystems operated by one or more of these parties.

This example is included to provide additional insight into the key management principles and requirements discussed within this part of ISO 11568. This example has been simplified and may not apply to all national or international retail banking environments. This example is illustrative of a retail banking environment supporting a magnetic stripe card environment and may not fully apply to integrated circuit card systems.

B.2 Cardholder and card issuer

The cardholder has a contractual relationship with the card issuer. The card issuer guarantees payment for transactions or services whenever the cardholders identify themselves. The card serves to identify the cardholder and the card issuer. In addition, the card may carry other information such as period of validity (e.g. expiration date) and security-related information (e.g. PIN offset). The cardholder and card issuer may agree on the method of issuing the unique, secret PIN (see ISO 9564-1) to be used during transactions. The transaction processing system has an obligation to maintain the PIN secrecy while transporting the transaction of the cardholder between the card acceptor and the card issuer. The card issuer maintains the confidentiality of sensitive cardholder data (e.g. PINs). The card issuer may delegate responsibility for verification of the PIN to an agent.

B.3 Card acceptor

The card acceptor is the party that accepts cards as a means of payment for goods or services. In POS systems, this may be a retailer, services company, financial institution, etc. In ATM systems the card acceptor may be the same party as the acquirer. Rather than accepting the card as direct proof of payment, the card acceptor may forward transaction information to an acquirer. The card acceptor takes a transaction authorization from the acquirer as guarantee for payment. The security of the transaction information exchanged with the acquirer is important. Security features may include message authentication (see ISO 16609) and/or encipherment of the PIN.

B.4 Acquirer

The transaction acquirer provides transaction processing to card acceptors and card issuers. The acquirer takes responsibility for all or for part of the transaction content according to business arrangements with card issuers or their agents. Thus, for some transactions the acquirer may authorize a transaction acting as agent of a card issuer. In other cases (e.g. the transaction value exceeds a certain threshold), the transaction information is sent to a card issuer or its agent for authorization.

For the acquisition function, the acquirer needs facilities that provide secure processing for translation of enciphered PINs in node-to-node systems, message authentication for transaction exchanges, etc. For combined acquisition and authorization functions, the acquirer needs security facilities to satisfy the requirements of the card issuer that they represent.

B.5 Third party processor

The third party processor delivers retail transactions sent from card acceptors to acquirers and card issuers. In some cases, these services are limited to data transmission, whereas in other cases more complex conversion facilities are needed. For example, a switch in an interchange environment may offer the latter type of services. Such a switch needs security facilities that complement and satisfy the requirements of all business parties involved in the electronic delivery of the transaction. These facilities may provide secure PIN translation, PIN verification, and message authentication.

Annex C
(informative)

Examples of threats in the retail banking environment

C.1 General

This annex presents examples of threats to keys and other confidential data in the retail banking environment. These examples are included to provide insight into the need to implement key management schemes to provide data security. The information presented in this annex is drawn from ISO 7498-2:1989, Annex A.

C.2 Threats

Threats to retail banking systems include the following:

a) destruction of information and/or other resources;

b) corruption, modification or insertion of information;

c) theft, removal or loss of information and/or other resources;

d) disclosure of information; and

e) interruption of services.

Threats may be classified as accidental or intentional and may be active or passive.

C.2.1 Accidental threats

Accidental threats are those that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs.

C.2.2 Intentional threats

Intentional threats may range from casual examination using easily available monitoring tools to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered an “attack”.

C.2.3 Passive threats

Passive threats are those that, if realized, would not result in any modification to any information contained in the system(s) and where neither the operation nor the state of the system is changed.

Examples of passive threats that may be realized are the use of passive wiretapping to observe data being transmitted over a communications line, the unauthorized modification (or “bugging) of a device to disclose secret/private keys or other confidential data in the clear, or the substitution of a counterfeit device for a legitimate device, where the counterfeit has the capability to disclose secret/private keys or other confidential data.

C.2.4 Active threats

Active threats to a system involve the alteration of information in the system or changes to the state of operation of the system. Examples of active attacks are a malicious change to the routing tables of a system by an unauthorized user or the fraudulent modification of a “transaction declined” code to a “transaction approved” code.

C.2.4.1 Masquerade

A masquerade is where one party pretends to be a different party. A masquerade is usually used with some form of an active attack such as replay and modification of messages or data. For instance, authentication sequences may be captured and replayed after a valid authentication sequence has taken place. An authorized party with few privileges may use a masquerade to obtain extra privileges by impersonating a party that has those privileges.

C.2.4.2 Replay

A replay occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example, a valid message containing authentication information may be replayed by another party in order to authenticate itself (as something that it is not).

C.2.4.3 Modification of messages

Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect. For example, a message "Allow John Smith to read confidential file named accounts" is changed to "Allow Fred Brown to read confidential file named accounts".

C.2.4.4 Denial of service

Denial of service occurs when a party fails to perform its proper function or acts in a way that prevents other parties from performing their proper functions. The attack may be general, as when a party suppresses all messages directed to a particular destination, such as a security audit service or when a party generates extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay parties that make routing decisions based upon status reports received from other relay parties.

C.2.4.5 Insider attacks

Insider attacks occur when legitimate users of a system behave in unintended or unauthorized ways. Most known computer crime has involved insider attacks that compromised the security of the system.

C.2.4.6 Outsider attacks

Outsider attacks may use techniques such as

a) wire tapping (active or passive);

b) intercepting emissions;

c) masquerading as authorized users of the system or the components of the system;

d) bypassing authentication or access control mechanisms; and

e) penetrating a cryptographic device to determine the keys stored within it.

C.2.4.7 Trapdoor

A trapdoor is a hidden unauthorized software or hardware mechanism that may be triggered to allow the system security features to be bypassed. The trigger may be an external command (e.g. a special key sequence) or an internal predetermined event (e.g. a counter or date/time value). For example, a password validation program could be modified so that when a specific key sequence is entered, the attacker's password is validated.

C.2.4.8 Trojan horse

When a software program that performs a legitimate function contains a hidden unauthorized function that exploits the legitimate function, the unauthorized function is called a Trojan horse. For example, a program that legitimately copies secret/private keys or other confidential data to a protected file could be modified to also copy the data to a file accessible by the attacker.

Bibliography

[1] ISO 9564-1:2002, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

[2] ISO 9564-2:2005, *Banking — Personal Identification Number management and security — Part 2: Approved algorithms for PIN encipherment*

[3] ISO 9564-3:2003, *Banking — Personal Identification Number management and security — Part 3: Requirements for offline PIN handling in ATM and POS systems*

[4] ISO/TR 9564-4:2004, *Banking — Personal Identification Number (PIN) management and security — Part 4: Guidelines for PIN handling in open networks*

[5] ISO 13491-1:1998, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

[6] ISO 13491-2:2005, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

[7] ISO 16609:2004, *Banking — Requirements for message authentication using symmetric techniques*

ICS 35.240.40

Price based on 16 pages