INTERNATIONAL STANDARD

ISO 11568-5

First edition
1998-07-15

Banking — Key management (retail) —

Part 5:
Key life cycle for public key cryptosystems

Banque — Gestion de clés (services aux particuliers) —

Partie 5: Cycle de vie des clés pour les systèmes cryptographiques à clé publique

Reference number
ISO 11568-5:1998(E)

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

Introduction

ISO 11568 describes procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. Management of keys used in an Integrated Circuit Card (ICC) environment is not covered by ISO 11568.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this standard addresses the key management requirements that are applicable in the accessible domain of retail banking services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machines (ATM) transactions.

ISO 11568 is a multi-part standard. The different parts are listed in ISO 11568-1.

This part of ISO 11568 describes the key life cycle in the secure management of cryptographic keys for public key cryptosystems.

A public key cryptosystem uses a public key and a private key. These keys are collectively known as a key pair in this part of ISO 11568.

Clause 4 states the general security requirements for each step in the life of such a key pair, utilizing the key management principles, services and techniques described in ISO 11568-1 and ISO 11568-4.

Clause 5 states the requirements for the implementation methods related to these general security requirements.

The key life cycle consists of three phases:

1. Pending active: during which the key pair is generated and may be transferred.

2. Active: during which the public key is distributed to at least one or more parties for operational use.

3. Post active: during which the public key of a key pair is archived and the private key of a key pair is terminated.

A schematic overview of the private key (S) life cycle and the public key (P) life cycle are given respectively in Figures 1 and 2 . The figures show how a given operation on a key changes its state.

A key is considered to be a single object of which multiple instances may exist at different locations and in different forms. A clear distinction is made between the following operations:

- distribution of the public key to a communicating party;

- transfer of a key pair to its owner in an implementation where the party does not have the capacity to generate key pairs.

and:

- destruction of a single private key instance;

- deletion of a private key from a given location, which implies destruction of all instances of this key at that location;

- termination of a private key, which implies deletion of the key from all locations.

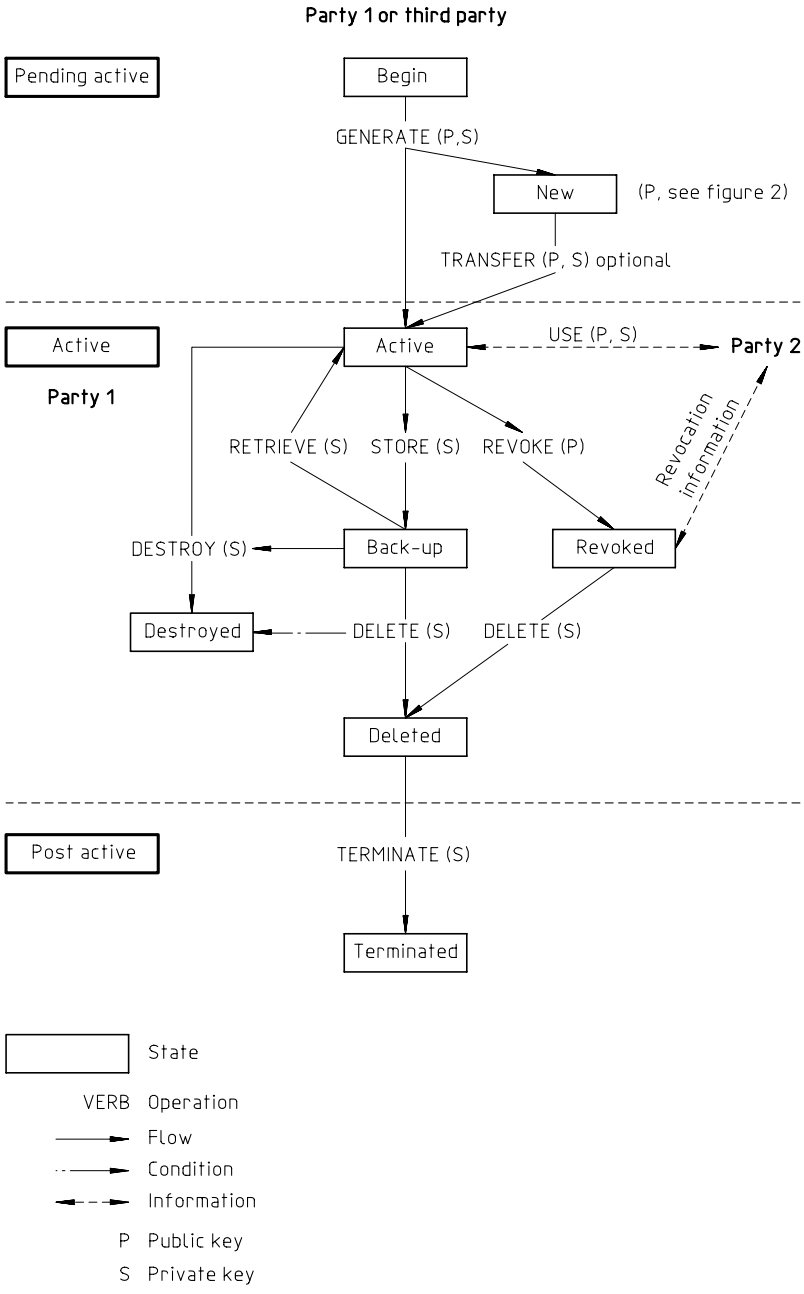

Figure 1 — Private key life cycle

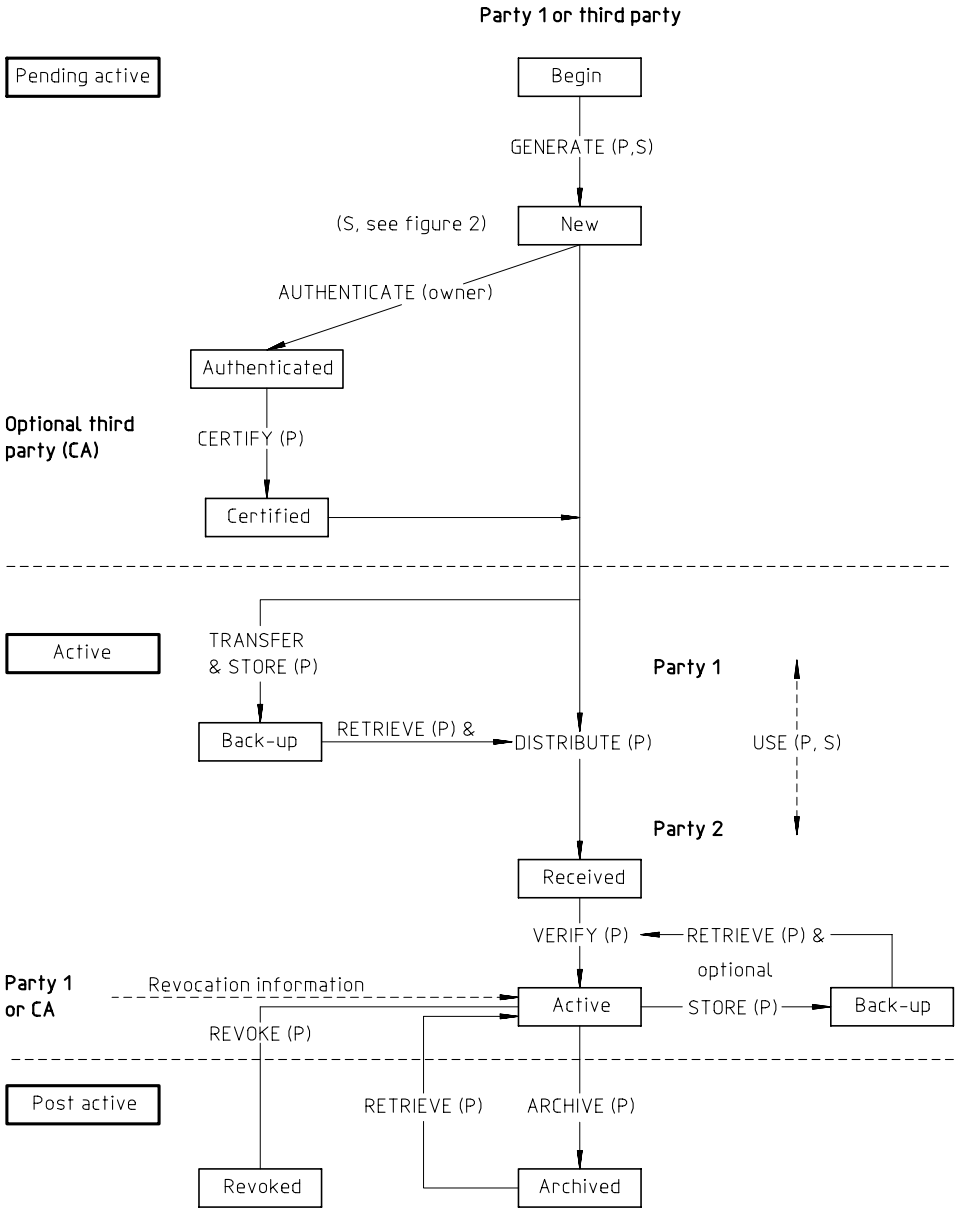

Figure 2 — Public key life cycle

Banking — Key management (retail) — Part 5: Key life cycle for public key cryptosystems

1 Scope

This part of ISO 11568 specifies for the retail banking environment the security requirements and the implementation methods for each step in the key life cycle for both the private key and the public key of an asymmetric key pair.

It is applicable to any organization which is responsible for implementing techniques based on public key cryptosystems for the management of keys used to protect data.

2 Normative reference(s)

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 11568. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 11568 are encouraged to investigate the possibility of applying the most recent edition of the standards 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.*

ISO 9564-1:— [1], *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques.*

ISO 11568-1:1994, *Banking — Key management (retail) — Part 1: Introduction to key management.*

ISO 11568-2:1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers.*

ISO 11568-3:1994, *Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers.*

ISO 11568-4:— [2], *Banking — Key management (retail) — Part 4: Key management techniques using public key cryptosystems.*

ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework.*

ISO/IEC 11770-3:— [2], *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques.*

ISO 13491:— [2], *Banking — Secure cryptographic devices (retail)* [all parts].

3 Terms and definitions

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

3.1 asymmetric key pair generator: A secure cryptographic device used for the generation of asymmetric cryptographic keys.

3.2 communicating party: The party that receives the public key for the communication with the party that owns the public key.

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

---

[1] To be published. (Revision of ISO 9564-1:1991)

[2] To be published.

4 General requirements

Every operation performed on a key changes its state. This clause specifies the requirements for obtaining a given state or performing a given operation.

Requirements applying to specific life cycle stages are specified in the following subclauses.

Note that the requirements hereafter may depend upon the implementation of key pair generation. In particular, the requirements are different if the key pair is generated by a third party asymmetric key pair generator or if the owner generates and stores its key pair.

4.1 Asymmetric key pair generation

The asymmetric key pair generation is the process by which a new pair of keys composed of a private key and the related public key are generated for use in a specific asymmetric cryptosystem. Possibly, other asymmetric keying information can be produced during this process. Inputs to this process may require predetermined values.

The key pair generation process is achieved by or on behalf of a single party. This party becomes the owner of the key pair.

Each private key and each private key component shall be generated in such a way that it is not feasible to predict any private key nor to determine that certain private keys are significantly more provable than others from the set of possible private keys. Where appropriate, the process shall incorporate random or pseudo-random values, depending upon the asymmetric cipher.

An asymmetric key pair shall be generated in such a way that the secrecy of the private key and the integrity of the public key is assured. For the generation of an asymmetric key pair for non-repudiation service, the integrity of the public key and the secrecy of the private key shall be provable to a third party.

The private key shall not be available in human-comprehensible form to any person at any time during the generation process.

If the key pair is generated by a system that will not use it:

- the key pair and all related secret seed elements shall be deleted immediately after the transfer has been ensured,
- in addition, the integrity of the private key shall be ensured.

Asymmetric key pairs, when generated, should have an expiry date to establish their life cycle.

The generation process shall conform to the requirements described in ISO 11658-4.

NOTE Added information should be joined to the public key, such as identification of the owner, key type and expiry date, to avoid repudiation by means of public key substitution.

4.2 Authenticity prior to use

The authenticity of the public key shall be assured prior to its use and throughout its life. Certification should be used to provide this assurance.

4.3 Public key certification

Public key certification is the process by which a trusted third party, referred to as the Certification Authority, establishes a proof which links a public key and other relevant information to its owner.

Key certification and the Certification Authority are described in ISO 11568-4.

The public key of the Certification Authority which is used to verify the public key in a certificate should be transferred to the key pair owner in an authenticated way.

4.4 Asymmetric key pair transfer

The asymmetric key pair transfer is the process by which the key pair and the certificate of the public key are conveyed to the owner of the key pair. This process occurs when the owner does not have the capacity to generate its key pair.

The identity of the owner shall be authenticated prior to being given its key pair.

4.4.1 Private key transfer

A private key shall only be transferred in one of the following forms as defined in this subclause:

- plaintext key
- key components
- enciphered key.

4.4.1.1 Plaintext private key

The general requirements for the transfer and loading of plaintext private keys are:

1. The key transfer process shall not disclose any portion of the plaintext key.

2. The key transfer and loading processes shall be performed according to the principles of dual control and split knowledge.

3. A secure cryptographic device shall transfer a plaintext private key only when at least two authorized persons are authenticated by the device, for example, by means of passwords.

4. A plaintext private key shall be loaded into a secure cryptographic device only when it can be assured that the device has not been subject to prior tampering which might lead to the disclosure of keys or sensitive data.

5. A plaintext private key shall be transferred between secure cryptographic devices only when it can be ensured that there is no tap at the interface that might disclose any element of the transferred key.

6. When a device is used to transfer private keys between the cryptographic device which generates the key and the cryptographic device which will use the key, this device shall be a secure cryptographic device. After loading of the key into the target device, the key transfer device shall not retain any information which might disclose that key.

4.4.1.2 Private key components

The general requirements for the transfer and loading of private key components are:

1. The key component transfer process shall not disclose any portion of a key component to an unauthorized person.

2. Key components shall be loaded into a secure cryptographic device only when it can be assured that the device has not been subject to prior tampering which might lead to the disclosure of keys or sensitive data.

3. Key components shall be transferred into a secure cryptographic device only when it can be ensured that there is no tap at the interface that might disclose the transferred components.

4. The key transfer and loading process shall be performed according to the principles of dual control and split knowledge.

4.4.1.3 Enciphered private key

Enciphered keys may be transferred and loaded electronically via a communication channel. Encipherment of a key using a key encipherment key shall take place within a secure cryptographic device.

In this case, the requirements described in ISO 11568-2 and ISO 11568-4 shall apply.

The process of transferring enciphered private keys shall protect against key substitution and modification.

4.4.2 Public key transfer

The public key transfer techniques shall ensure the authenticity of the key. They should be the same as those used for private key transfer.

4.5 Key storage

During storage, keys shall be protected against unauthorized disclosure and substitution, and key separation shall be provided.

Storage of the private key requires that secrecy and integrity are ensured. Storage of the public key requires that authenticity and integrity are ensured.

4.5.1 Permissible forms for private keys

A private key shall only be stored in the forms defined in 4.4.1.

4.5.1.1 Plaintext private key

A plaintext private key shall exist only within a secure cryptographic device.

4.5.1.2 Key components

A private key existing in the form of at least two separate key components shall be protected by the principles of split knowledge and dual control.

Each bit of the resulting key shall be a function of all key components.

When the same key value must be created on more than one occasion, different sets of key components should be used. If new components are created, the values of any of these key components shall not be the same except by chance.

A key component shall be accessible only to that person or group of persons to whom it has been entrusted for the minimum duration required.

If a key component is in human comprehensible form (e.g. printed in plaintext inside a mailer), it shall be known to only one authorized person at only one point in time, and only for as long as required for the component to be entered into a secure cryptographic device.

No person with access to one component of the key shall have access to any other component of that key.

Key components shall be stored in such a way that unauthorized access has a high probability of being detected. If key components are stored in enciphered form, all requirements for enciphered keys shall apply.

4.5.1.3 Enciphered private key

Encipherment of a key using a key encipherment key shall take place within a secure cryptographic device.

In this case, the requirements described in ISO 11568-2 and ISO 11568-4 of shall apply.

4.5.2 Permissible forms for public keys

In an asymmetric cipher there is no secrecy requirement for the storage of the public key, but authenticity and integrity of this key are essential.

It shall not be possible to substitute or alter any public key or associated information without detection.

Considering these requirements, a public key should be stored only in the following forms:

- plaintext key within a certificate
- enciphered key.

The use of key components is of no consequential value since the public key need not be kept secret.

4.5.2.1 Plaintext public key

If a public key is not certified, it shall be stored with sufficient protection to ensure that the value of the key and its identity cannot be modified without detection.

It is highly desirable that public keys are certified when stored electronically.

4.5.2.2 Enciphered public key

Although a public key does not need secrecy, a means to ensure its authenticity and integrity is to store it in an enciphered form. In this case, the requirements defined in ISO 11568-2 and ISO 11568-4 shall apply.

4.5.3 Protection against substitution during storage

When plaintext public keys are stored and are not in the form of a certificate, or when their certificate has been checked and they will be used without re-checking the certificate, integrity and authenticity shall be ensured by means described in 5.5.3 and by techniques described in ISO 11568-4.

4.5.4 Provisions for key separation

To ensure that a given key is only used for its intended purpose, key separation shall be achieved by means described in 5.5.4 and by techniques described in ISO 11568-4 (e.g. key tagging).

4.5.5 Key back-up

Key back-up is the storage of a copy for the purpose of reinstating a key that is accidentally destroyed but the compromise of which is not suspected.

Back-up copies shall be held in one of the permissible forms of the key. All back-up copies of keys shall be subject to the same or greater level of security control as keys in current use.

If back-up copies of private keys are held in a secure cryptographic device, access to the stored values shall be controlled by positive user identification (e.g. access identifier and password or other methods) to prevent unauthorized use of the key.

4.6 Key retrieval

The requirements for public key retrieval from back-up are the same as for public key distribution described in 4.7.

The requirements for private key retrieval from back-up are the same as for key transfer of private keys.

4.7 Public key distribution

Key distribution is the process by which a public key is conveyed to the communicating party intended to use it.

Public keys may be distributed manually or automatically via a communication channel.

The process by which a public key is distributed shall ensure the integrity and authenticity of the public key.

The substitution of a public key during distribution shall be prevented, preferably by key certification.

NOTE Key certification is explained in ISO 11568-4.

4.8 Public key certificate verification

Public key certificate verification is the process by which a communicating party verifies that the received public key belongs to the intended owner and optionally is intended for the indicated usage.

Key verification is described in 5.8.

4.9 Key use

The use of asymmetric private and public keys is described in ISO 11568-4.

In an asymmetric cryptosystem, each key of a key pair is used for separate functions. The following requirements address both keys of a key pair except where otherwise mentioned.

Unauthorized key use shall be prevented; therefore,

1. A key shall be used for only one function.

2. A key shall be used only for its intended function in its intended locations.

3. Any private key shall exist in the minimum number of locations consistent with effective system operation.

4. A key pair shall cease to be used at the end of the cryptoperiod or when the compromise of the private key is known or suspected.

5. A public key should be used only when its authenticity and integrity have been verified and are correct.

4.10 Public key registration

Public key registration is the process whereby the key pair owner registers appropriate credentials and the corresponding public key with an authorized agency for the purpose of authenticity.

Note that the authorized agency may be a Certification Authority where the proof of authenticity is a Public Key Certificate.

Key pair owners shall provide authenticity of their public key(s) to public key users.

Key pair owners should register their public keys(s) with an authorized agency, such as a Certificate Authority.

4.11 Public key revocation

Public key revocation is the process whereby the use of a public key is terminated for one of the following reasons:

- public key expiry date
- private key compromise
- business reasons.

Public keys, when generated and issued for use, typically have an expiry date which determines the key pair life cycle. Public keys shall not be used beyond their valid expiry date and should be automatically revoked.

When a private key compromise is known, the corresponding public key shall be revoked.

For business reasons, authorized entities may rescind the use of an asymmetric key pair. In this case, the public key shall be revoked.

Public key users shall be notified[3)] that a public key has been revoked and upon receipt of such notification shall cease using that public key.

A public key that has been revoked may need to be used to verify information that has been previously signed, or may be needed for legal purposes and will be recovered from the archive.

4.12 Key replacement

Key replacement shall occur:

1. at the end of the cryptoperiod (when the expiry date is reached) or

2. when compromise of the private key is known or suspected.

In the case of key replacement, both the public and the private key of a key pair shall be replaced. If the key pair under suspicion is used as a key encipherment key, then all keys which are hierarchically under it shall also be replaced.

---

3) Notification can be active, such as broadcasting to all public key users that a public key has been revoked, or passive, such as posting the revocation on a generally accessible data base.

In case of key replacement, the revocation of the corresponding certificate shall occur as described in ISO 11568-4.

A key shall be replaced within the time deemed feasible to perform a dictionary attack upon the data enciphered under this key, or within the time deemed feasible to determine the private key by crypto-analytic attack. This will depend upon the specific implementation and the technology available at the time of the attack.

If it is believed or known that a private key used for decipherment purposes is compromised, the communicating parties should be informed that the key pair shall no longer be used.

Replacement of a key pair shall take place in all operational locations where the keys exist.

Replaced keys shall not be returned to active use.

A key pair shall be replaced only by distributing a new public key. Key replacement requires that the old private key shall be destroyed.

4.13 Private key destruction

An instance of a private key shall be destroyed when it is no longer required for active use. Electronic instances of a private key may be destroyed by erasure. However, information may still reside at the operational location so that the key may subsequently be restored for active use.

The corresponding public key shall not be distributed again to corresponding parties. If public keys are stored at corresponding parties' locations, they shall be informed of the destruction of the corresponding private key.

When a secure cryptographic device is accessible, and known to be permanently removed from service, all private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose shall be destroyed.

4.14 Private key deletion

When a private key is no longer required at a given operational location, it shall be deleted.

Key deletion occurs when all instances of the private key have been destroyed at a given location.

4.15 Private key termination

Private key termination occurs when the private key has been deleted from all locations where it has ever occurred. Subsequent to private key termination, no information shall exist from which the private key can feasibly be reconstructed.

4.16 Public key archive

Public key archive is the process by which a public key is stored for the purpose of verifying signatures that occurred prior to revocation. After such verification, the instance of the key necessary to perform the verification should be destroyed.

An archived public key shall be securely stored in order to ensure its integrity as long as data verifiable by this key still exists.

Public key archive shall be ensure with the same level of security as for public key storage (see 4.5).

4.17 Key pair recovery

Key pair recovery is the process whereby a new key pair replaces a revoked key pair.

If the key pair has expired or is revoked due to business reasons, replacement of the key pair may not be necessary or appropriate.

If the private key is compromised, the public key shall be immediately revoked and may be replaced with a newly generated key pair.

During key pair recovery, the key pair owner shall adhere to all of the requirements for key pair generation.

During key pair recovery, the key pair owner shall adhere to all of the requirements for public key registration.

5 Implementation requirements

Throughout the key life cycle, equipment and procedures used to store and manage keys shall be subject to controls and audits so as to prevent or detect key compromise.

5.1 Asymmetric key pair generation

Key pairs and key components shall be generated according to the requirements described in ISO 11568-4.

Asymmetric key pair generation shall be performed by using an appropriate asymmetric key pair generator.

In order to ensure the generation of non-repeatable key pairs, a random or pseudo-random process shall be used.

Generation of an asymmetric key pair is accomplished by either the Certification Authority (CA), the key pair owner, or an authorized third party.

The following three subclauses describe the roles and responsibilities of the Certification Authority, the key pair owner, or the third party.

5.1.1 Certification Authority

The CA shall generate the asymmetric key pair in a secure cryptographic device and shall transport the private key to the key pair owner in accordance to the requirements in 4.4.

The CA shall transport the public key to the key pair owner in a certificate.

The CA shall neither record nor retain any information that could possibly compromise the private key or allow it to be recreated.

5.1.2 Key pair owner

The key pair owner shall generate the asymmetric key pair in a secure cryptographic device and shall either:

- generate the key pair in the same cryptographic device in which it will be used, or
- inject the private key directly from the device where it was generated into the device in which it will be used.

The key pair owner shall retain as few copies of the private key as is operationally feasible[4)].

5.1.3 Third party

The third party shall generate the asymmetric key pair in a secure cryptographic device and shall transport the private key to the key pair owner in accordance with the requirements in 5.4.1.

The third party shall transport the public key to the key pair owner in accordance with the requirements in 5.4.2.

The third party shall neither record nor retain any information that could possibly compromise the private key or allow it to be recreated.

5.2 Authenticity prior to use

If certificates are to be used, the procedure described in ISO 11568-4 shall be used to ensure authenticity and integrity of the key and its owner.

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

5.3 Public key certification

The implementation of public key certification is described in ISO 11568-4.

5.4 Asymmetric key pair transfer

The transfer of an asymmetric key pair shall use one of the following techniques.

The key pair should be stored in secure cryptographic devices, such as the key transfer devices described in ISO 13491-1.

The permissible methods for transfer of an asymmetric key pair are described in Table 1.

5.4.1 Private key transfer

5.4.1.1 Plaintext private key

When a plaintext private key is directly and electronically transferred between two secure cryptographic devices, it shall be ensured that the devices are directly connected to each other (without an intervening tap) and operated under continuous dual control.

The private key shall be protected against disclosure and substitution. The public key should not be distributed until the private key has been successfully installed.

4) The fewer the instances of the private key, the stronger the claim of non-repudiation as there is a lower probability of compromise.

Table 1 — Permissible methods for transfer of an asymmetric key pair (P: public key, S: private key)

Techniques / Key forms	Manual	Electronic		
		Direct	Device	Network
Plaintext key	P	P,S	P,S	P
Key components	P,S	P	P	P
Enciphered keys	P,S	P,S	P,S	P,S
Certificate	P	P	P	P

When a key transfer device is used, the key (and its identifier, if explicit key identification is used) shall be transferred from the cryptographic device which generated the key into the key transfer device. This portable device shall be physically transported to the cryptographic device which will actually use the key. Appropriate custody shall be maintained over the key transfer device to ensure that the private key can only be transferred to the intended key-using device. The key (and its identifier) shall be then transferred from the key transfer device into the key-using device. If the key-using device is a transaction-originating device, then the key shall be immediately erased from the key transfer device. The transfer of plaintext keys shall take place as specified above for direct electronic key loading.

5.4.1.2 Private key components

When key components are used, the components that will form the key shall be entered into the device manually or using a key transfer device. When key components are distributed in human-comprehensible form, each such component shall be distributed in a document which does not disclose the value of the component until opened.

Prior to entering the key component, the document shall be checked for signs of tampering. If tampering of any of the components is detected, the set of components shall not be used and shall be destroyed following the procedures outlined in ISO 9564-1.

The key components shall be entered individually by each holder of a key component. The key verification methods described in ISO 11568-3 should be used to verify correct key entry. When the last component has been entered, the cryptographic device shall perform the action required to construct the key. If provided, a key verification code generated by one of the methods described in ISO 11568-3 should be used to verify correct key entry.

If available, the key verification code for each of the key components and for the resulting key should be verified.

5.4.1.3 Enciphered private key

Key identifier and related data shall be transferred together with the private key. The private key shall be enciphered as described in ISO 11568-4.

5.4.2 Public key transfer

Public key transfer techniques shall ensure the authenticity of the key; they should be the same as those used for private key transfer.

When the key pair is not generated by the key owner then, prior to the distribution of the public key, the correct transfer of the public key should be verified by the key pair owner using the private key.

5.5 Key storage

This clause describes the implementation of secure key storage for each of the permissible forms.

Private keys are protected against unauthorized disclosure by the implementation of one of the secure key storage forms described in 5.5.1.

Private and public keys are protected against substitution by one of the secure key storage forms described in 5.5.2.

Replacement of a key for which substitution is known, suspected or anticipated requires the execution of the procedures described in 5.10.

5.5.1 Permissible forms for private key

One of the following techniques should be used to store private keys:

1. Plaintext key: In a secure cryptographic device.

2. Key component: In at least two components, designed so that knowledge of all but one component does not facilitate an attack on the key. The components shall be stored separately and controlled by different entities.

3. Enciphered keys: Enciphered under a key encipherment key.

5.5.1.1 Plaintext private key

A secure cryptographic device shall comply with the requirements as stated in ISO 13491-1.

5.5.1.2 Key components

A key component shall be conveyed to authorized persons by means of a key mailer or key transfer device.

A key mailer shall be printed in such a way that the key component cannot be observed until the envelope is opened. The envelope shall display the minimum data necessary to deliver the key mailer to the authorized person. A key mailer shall be constructed such that it is highly likely that accidental or fraudulent opening will be obvious to a recipient, in which case the key component shall not be used.

After the key component has been entered into a secure cryptographic device, the key mailer shall be destroyed.

Key components when stored in a key transfer device shall be protected by adequate access controls, such as passwords.

5.5.1.3 Enciphered private key

The encipherment of a private key shall be implemented as specified in ISO 11568-2 and ISO 11568-4.

When a symmetric cipher is used to encipher the private key of a key pair, the corresponding key encipherment key shall be a double-length key. Furthermore, as the private key is generally longer than the block size, a cipher block chaining mode shall be used.

5.5.2 Permissible forms for public keys

5.5.2.1 Plaintext public key

When the public key is stored in plaintext as a certificate, the techniques described in ISO 11568-4 shall apply for the production of this certificate.

When the public key does not appear as a certificate, it should be stored in plain text in a secure cryptographic device designed to detect unauthorized key replacement.

5.5.2.2 Enciphered public key

In some implementations the public key may be stored enciphered in order to ensure its integrity. In this case, the techniques described in ISO 11568-2 and ISO 11568-4 shall apply.

5.5.3 Protection against substitution during storage

Protection against substitution of the public key during storage is essential. For example, the substitution of a public key used for encipherment may result in a threat to data secrecy.

One means of protecting a public key against substitution is to implement the same techniques as for a private key. Another means is to store the public key in a certificate, allowing verification of the key's integrity and authenticity before use.

The unauthorized substitution of stored public keys shall be prevented by one or more of the following means:

1. Physically and procedurally preventing unauthorized access to the key storage area.

2. Storing a key enciphered as a function of its intended use and ensuring that it is not possible to know both a chosen plaintext value and its corresponding ciphertext enciphered under the key encipherment key.

3. Storing a certificate containing a public key and verifying the key prior to its use.

The techniques used to achieve protection against substitution are described in more detail in ISO 11568-4.

If unauthorized key substitution is known or suspected, distribution of the public key shall be repeated.

5.5.4 Provisions for key separation

In order to ensure that each key of an asymmetric key pair is only usable for its intended purpose, key separation for stored keys shall be provided by one or more of the following means:

1. Physically segregating stored keys as a function of their intended purpose.

2. Storing a key enciphered under a key encipherment key dedicated to encipherment of a specific type of key.

3. Modifying or appending information to a key as a function of its intended purpose, prior to encipherment of the key for storage.

4. For public keys, providing a certificate including the usage of the key.

5.5.5 Key back-up

Key back-up is ensured using the same principles and techniques as for key storage.

5.6 Key retrieval

Retrieval of a public key from back-up shall be implemented by one of the methods described for public key distribution and loading in 5.7.

Retrieval of a private key from back-up shall be implemented by one of the methods described for private key storage in 5.5.

5.7 Public key distribution

The techniques used for public key distribution are described in ISO 11568-4.

The techniques used for protection against substitution during distribution are described in ISO 11568-4. These are:

1. The use of a certificate.

2. Appending a message authentication code (MAC) to the public key or using a digital signature technique.

3. Encipherment of the public key.

4. Confirmation of the value of the key and associated information through an independent channel.

5.8 Public key verification

The verification of the authenticity of a public key should be achieved by any of the following means:

1. A secure channel through a symmetric cipher relationship.

2. The distribution of the public key within a certificate.

3. By confirmation of the value of the key and associated information through an independent channel.

Techniques for the implementation of public key certificate verification are described in ISO 11568-4.

5.9 Key use

Private keys are used to decipher a key or to create a digital signature; public keys are used to encipher a key or verify a signature.

The secrecy of a private key shall be protected. Therefore, it shall not be used outside a secure cryptographic device.

A fixed device such as a host security module could be used to operate the private key. If the key is stored so that on-line access is possible, a secure method to prevent unauthorized use of the key shall be implemented.

Physical and logical controls shall be implemented to prevent unauthorized key use.

The recipient of a public key shall verify its integrity and authenticity before use.

ISO 11568-4 contains a list of techniques which should be used to obtain proper key separation and to verify integrity and authenticity of a public key.

Subsequent use of a key suspected of compromise shall be prevented by either:

1. Deleting the key from all operational locations.

2. Blocking the means used to obtain the key (e.g. a revocation list).

Protection against misuse of keys during their operational use requires the application of one of the techniques described in ISO 11568-4.

5.10 Public key registration

Public key cryposystems should use a Certification Authority (CA) and optionally a Local Registration Authority (LRA) for registration.

The following three subclauses describe the roles and responsibilities of the Certification Authority, the key pair owner, and the public key user.

5.10.1 Certification Authority

The CA shall verify the key pair owner's credentials and shall provide a mechanism that binds the key pair owner's identity to the corresponding public key. Refer to ISO 11568-4 for public key certificate management.

5.10.2 Key pair owner

The key pair owner shall register appropriate credentials and the corresponding public key with the CA.

5.10.3 Public key user

The public key user should use only those public keys issued by the CA.

The public key user shall verify the integrity and authenticity of the public key prior to each use or shall maintain the public keys in such a manner that the integrity and authenticity are ensured during operational use.

5.11 Public key revocation

Public key cryposystems should use a Certification Authority (CA) for revocation.

The following three subclauses describe the roles and responsibilities of the Certification Authority, the key pair owner, and the public key user:

5.11.1 Certification Authorities

The CA shall implement and manage a list of all revoked certificates known as a Certificate Revocation List (CRL).

The CA shall authorize the revocation of any certificate and shall authenticate revocation requests from any entity.

The CA shall update the CRL immediately whenever a certificate has been revoked.

The CA shall maintain the integrity and provide authenticity of the CRL by resigning each revoked certificate.

The CA shall make the CRL available to all public key users.

5.11.2 Key pair owner

In the event of a private key compromise, the key pair owner shall immediately notify the CA that the corresponding public key must be revoked.

5.11.3 Public key user

The public key user shall periodically check the CRL as is operationally feasible and in accordance with the policies of the CA.

5.12 Key replacement

Key replacement shall be implemented by repeating the appropriate key generation, transfer, distribution and loading procedures.

5.13 Private key destruction

Private key destruction shall be implemented either by completely overwriting the key with a new key value or a value that may be non-secret such that no information about the erased key is retained, or by destroying the key storage media following the procedures outlined in ISO 9564-1.

5.14 Private key deletion

Private key deletion shall be implemented by completely erasing all forms of the key at an operational location, whether the key is physically secured, enciphered or in the form of components.

When a key component available in human comprehensible form is to be deleted, the media on which the key component is recorded shall be destroyed by burning or an equivalently effective process.

5.15 Private key termination

Private key termination shall be effected by destroying all instances of the key at all locations according to the requirements and methods described in this part of ISO 11568.

If key certificates are used and the key is terminated before the expiration date in the certificate, the corresponding public key shall be revoked.

5.16 Public key archive

A public key shall be archived by one of the permissible storage forms described in 5.5.2.

5.16.1 Plaintext keys

The separation of archived keys from active keys or protection against substitution of active keys by archived keys shall be achieved by using one of the appropriate techniques as described in ISO 11568-2 and ISO 11568-4.

5.16.2 Enciphered keys

The key encipherment key used for the archival process shall not intentionally be the same as any of the key encipherment keys used to encipher active keys.

Archived keying material should be stored separately from operational keying material.

5.17 Key pair recovery

The recovery of an asymmetric key pair may be necessary for a key pair owner or the key pair of the Certification Authority (CA) itself.

The following two subclauses describe the roles and responsibilities of the Certification Authority and the key pair owner.

5.17.1 Certification Authority

In the event where the CA private key is compromised, the CA shall:

- revoke all current certificates, as any certificate signed with the compromised private key is suspect[5].
- generate a new asymmetric key pair and distribute the corresponding public key to all key pair owners and public key users
- replace the revoked certificates with new certificates using the new private key

The CA should initially generate more than one asymmetric key pair and consequently distribute all CA public keys.

The CA should issue certificates with multiple signatures using different private keys. In the event of a compromise, the existing certificates would remain secure.

5.17.2 Key pair owner

In the event that the key pair owner's private key is compromised, the key pair owner:

- shall immediately notify the CA to revoke the certificate
- may generate a new key pair and register the new public key with the CA.

---

[5] Note that the CA can not sign the revoked certificates with the compromised private key.

ICS 35.240.40

Descriptors: banking, banking documents, messages, identification cards, credit cards, data processing, information interchange, protection of information, cryptography, key management, life cycle.

Price based on 12 pages