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

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.

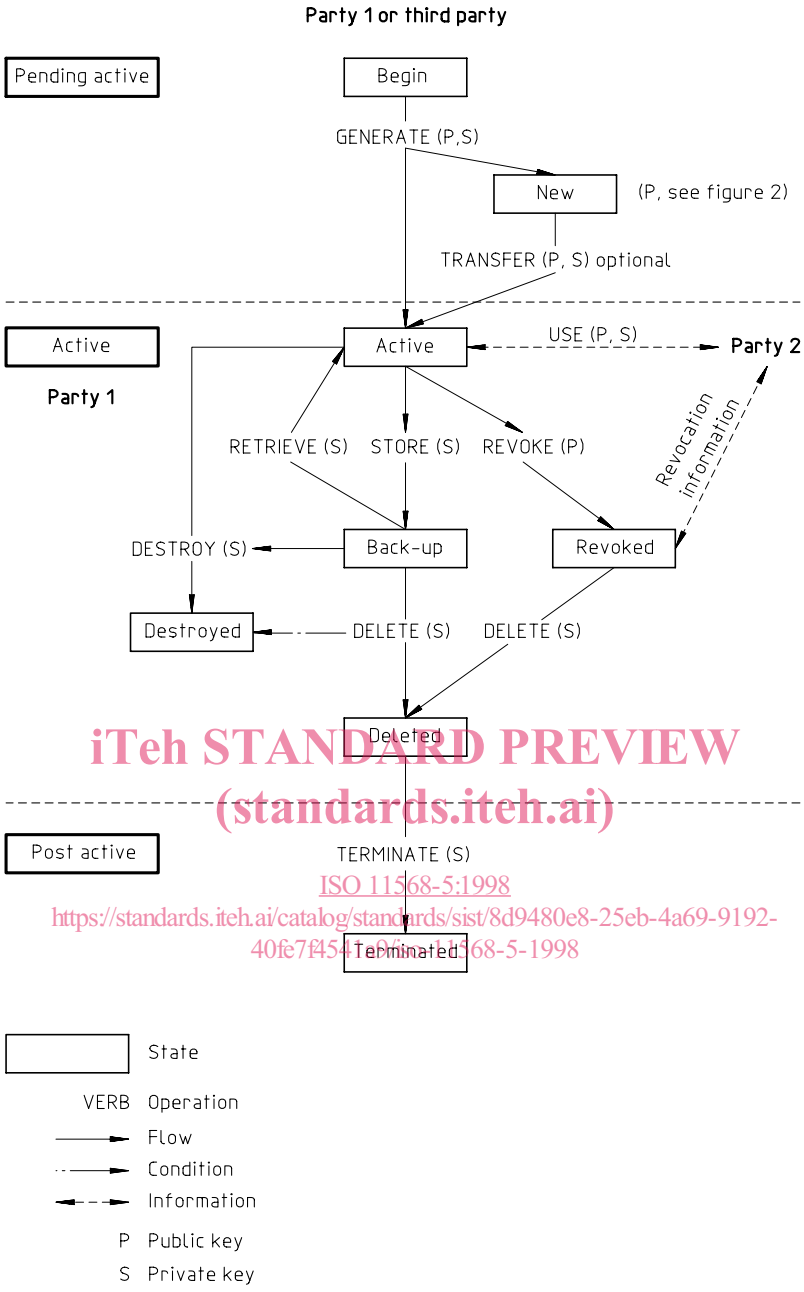

Figure 1 — Private key life cycle

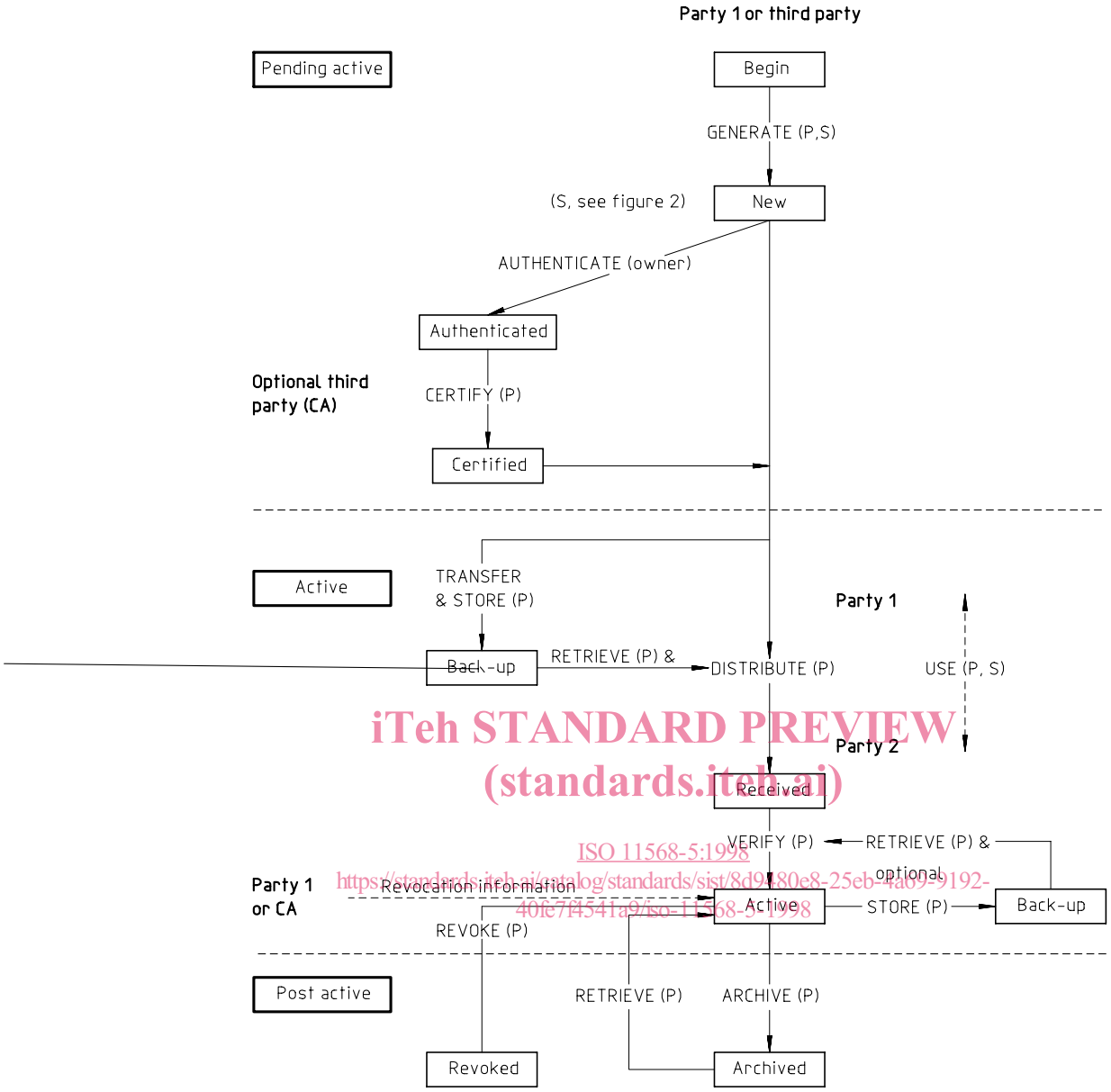

Figure 2 — Public key life cycle

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.