
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

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 General requirements..... 2

4.1 Asymmetric key pair generation 2

4.2 Authenticity prior to use 2

4.3 Public key certification..... 2

4.4 Asymmetric key pair transfer 2

4.5 Key storage 3

4.6 Key retrieval 4

4.7 Public key distribution 4

4.8 Public key certificate verification..... 5

4.9 Key use 5

4.10 Public key registration 5

4.11 Public key revocation..... 5

4.12 Key replacement..... 5

4.13 Private key destruction 6

4.14 Private key deletion 6

4.15 Private key termination 6

4.16 Public key archive 6

4.17 Key pair recovery..... 6

5 Implementation requirements 6

5.1 Asymmetric key pair generation 6

5.2 Authenticity prior to use	7
5.3 Public key certification	7
5.4 Asymmetric key pair transfer	7
5.5 Key storage	8
5.6 Key retrieval	10
5.7 Public key distribution	10
5.8 Public key verification.....	10
5.9 Key use.....	10
5.10 Public key registration	11
5.11 Public key revocation.....	11
5.12 Key replacement.....	11
5.13 Private key destruction	11
5.14 Private key deletion.....	11
5.15 Private key termination	11
5.16 Public key archive	11
5.17 Key pair recovery.....	12

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.

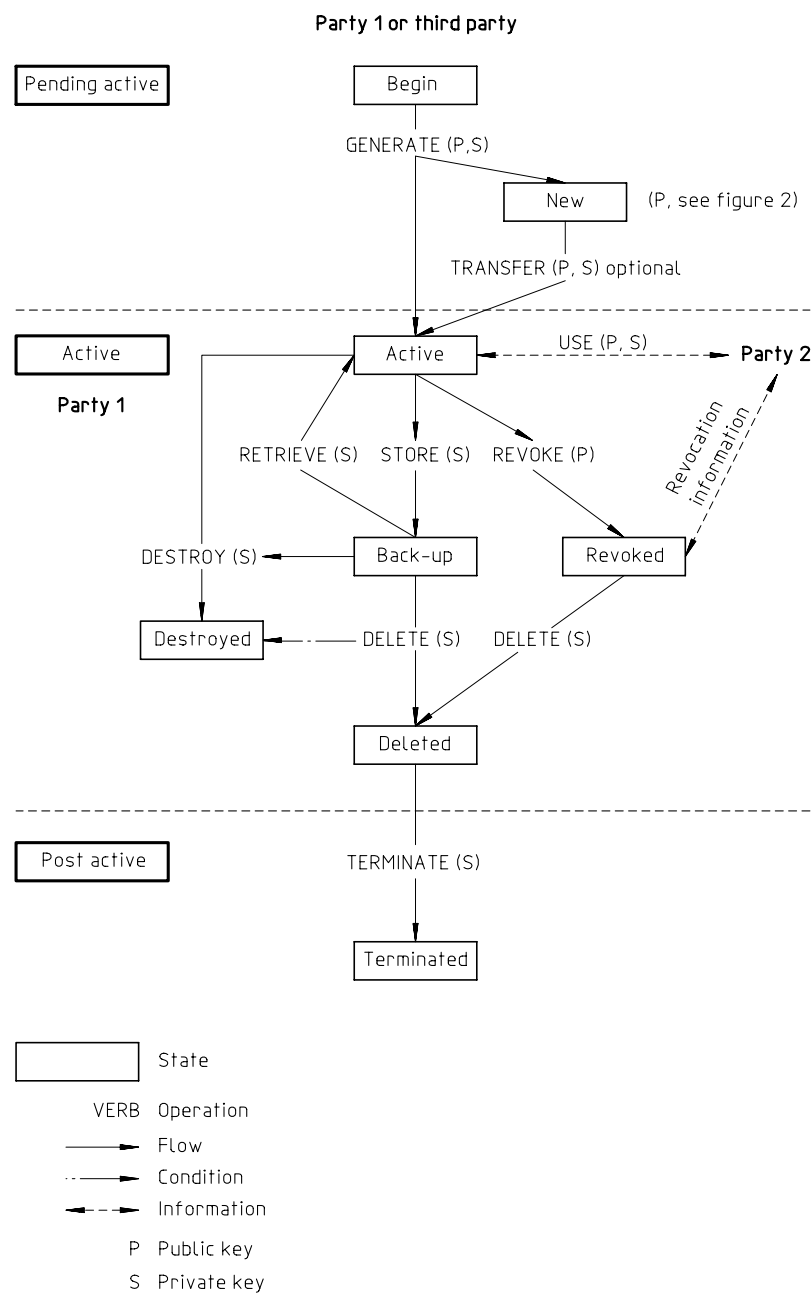


Figure 1 — Private key life cycle

