

INTERNATIONAL STANDARD

ISO
11568-3

First edition
1994-12-01

Banking — Key management (retail) — **Part 3:** Key life cycle for symmetric ciphers

Banque — Gestion de clés (services aux particuliers) —

*Partie 3: Cycle de vie des clés pour les algorithmes cryptographiques
symétriques*



Reference number
ISO 11568-3:1994(E)
AVA Documents
Document Sharing Hub

Contents

	Page
1 Scope	1
2 Normative references	1
3 Definitions	1
4 Requirements	2
4.1 Key generation	2
4.2 Key storage	2
4.3 Key retrieval from back up	3
4.4 Key distribution and loading	3
4.5 Key use	3
4.6 Key replacement	3
4.7 Key destruction	4
4.8 Key deletion	4
4.9 Key archive	4
4.10 Key termination	5
5 Methods	5
5.1 Key generation	5
5.2 Key storage	5
5.3 Key retrieval from back up	5
5.4 Key distribution and loading	5
5.5 Key use	7
5.6 Key replacement	7
5.7 Key destruction	7
5.8 Key deletion	7
5.9 Key archive	7
5.10 Key termination	8

Foreword

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

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

International Standard ISO 11568-3 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Subcommittee SC 6, *Financial transaction cards, related media and operations*.

ISO 11568 consists of the following parts, under the general title *Banking — Key management (retail)* :

- *Part 1 : Introduction to key management*
- *Part 2 : Key management techniques for symmetric ciphers*
- *Part 3 : Key life cycle for symmetric ciphers*
- *Part 4 : Key management techniques for asymmetric ciphers*
- *Part 5 : Key life cycle for asymmetric ciphers*
- *Part 6 : Key management schemes*

Introduction

ISO 11568 is one of a series of standards describing procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. Key management of keys used in an integrated circuit card (ICC) environment is not covered by ISO 11568.

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

This part of this ISO 11568 describes the key life cycle in the secure management of cryptographic keys for symmetric ciphers. It states both requirements and implementation methods for each step in the life of such a key, utilizing the key management principles, services and techniques described in ISO 11568-1 and ISO 11568-2.

The key life cycle consists of three phases :

- a) Pre-use : during which the key is generated.
- b) Use : during which the key is distributed amongst communicating parties for operational use.

In a process where both communicating parties contribute to the generation of a new key, key generation and distribution are closely integrated.

Some key management schemes are designed for transforming keys automatically during operational use.

- c) Post-use : during which a key is archived or terminated.

Figure 0.1 gives a schematic overview of the key life cycle. It shows how a given operation on a key changes its state.

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

- destruction of a single key instance ;
- deletion of a key from a given location, which implies destruction of all instances of this key at that location.
- termination of a key; which implies deletion of the key from all locations.

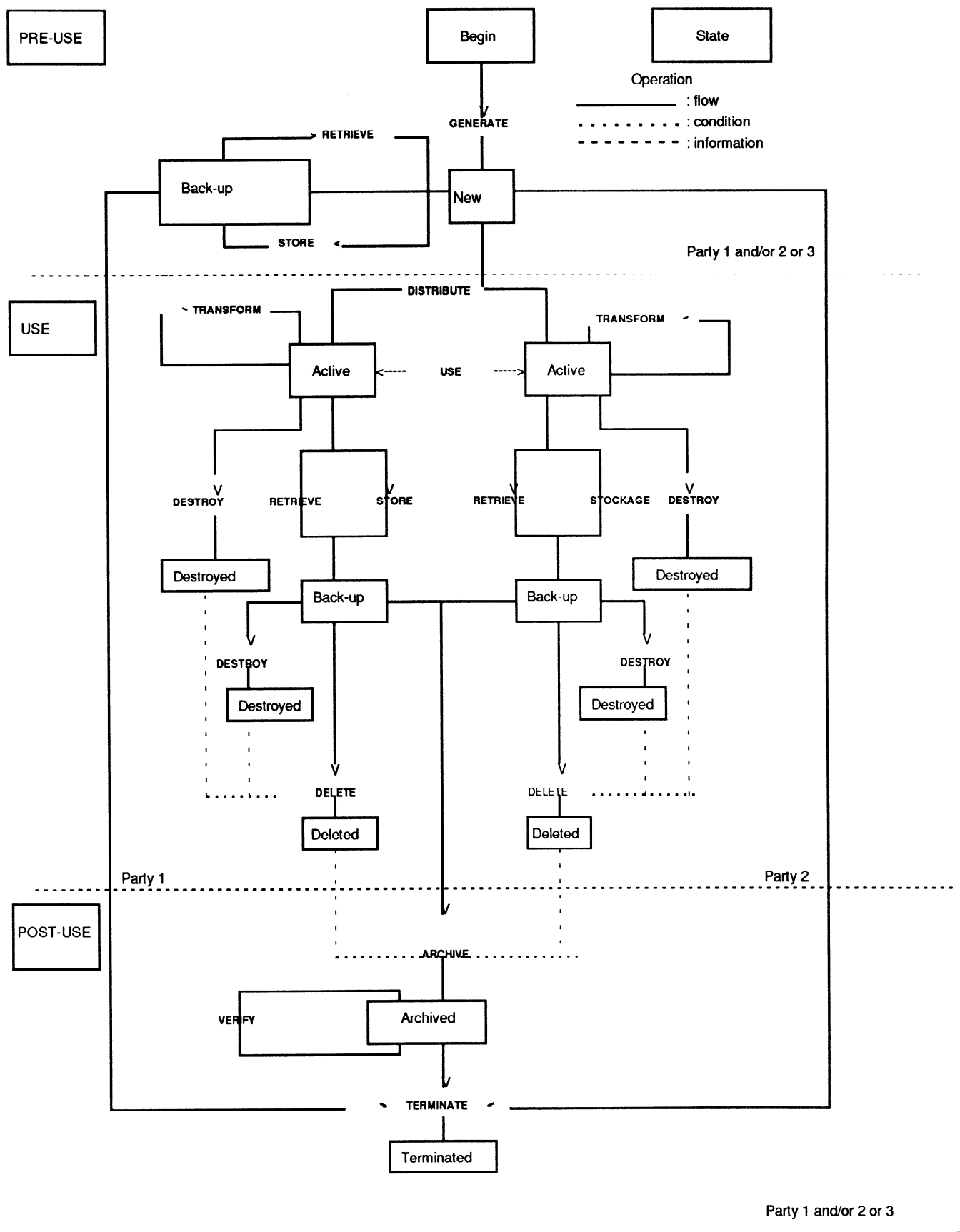


Figure 0.1 — Key life cycle