

INTERNATIONAL
STANDARD

ISO
11568-3

First edition
1994-12-01

Banking — Key management (retail) —

Part 3:

Key life cycle for symmetric ciphers

iTeh STANDARD PREVIEW

(standards.iteh.ai)

Banque — Gestion de clés (services aux particuliers) —

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

<https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994>



Reference number
ISO 11568-3:1994(E)

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

ITeH STANDARD PREVIEW
(standards.iteh.ai)

ISO 11568-3:1994
<https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994>

© ISO 1994

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

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)* :

- iTeh STANDARD PREVIEW**
(standards.iteh.ai)
- 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
- <https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100646220011/iso-11568-3-1994>

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.

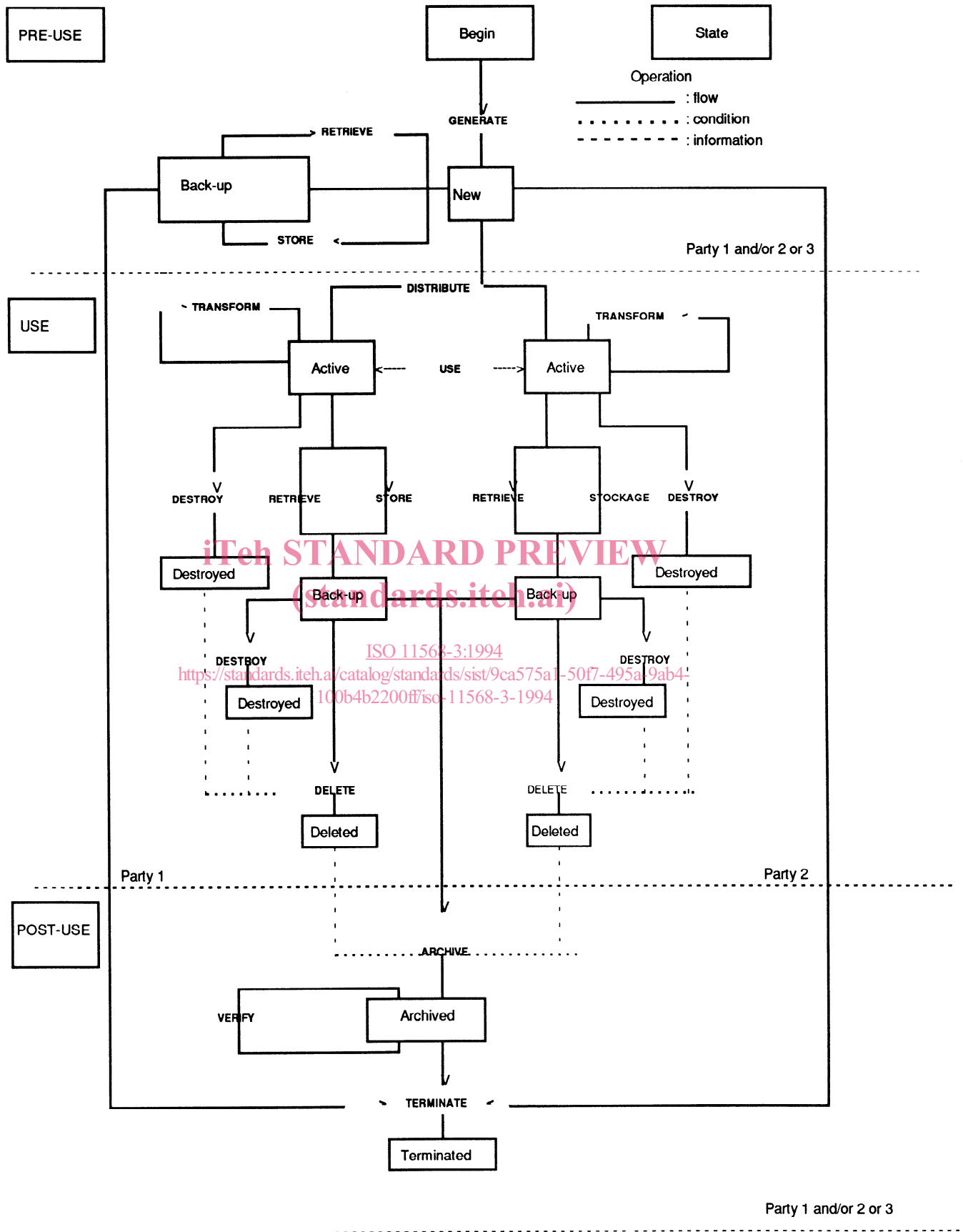


Figure 0.1 — Key life cycle

iTeh STANDARD PREVIEW

This page intentionally left blank
(standards.iteh.ai)

ISO 11568-3:1994

<https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994>

Banking — Key management (retail) —

Part 3 : Key life cycle for symmetric ciphers

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.

The key life cycle applies to keys at all levels of a key hierarchy.

It is applicable to any organisation that is responsible for the protection of keys used in a symmetric cipher.

This part of ISO 11568 is applicable to institutions responsible for implementing techniques for the management of keys used to protect data in bank card originated transactions.

2 Normative references

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 9564-1:1991, *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*.

3 Definitions

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

3.1 dual control : A process of utilising two or more separate entities (usually persons), operating in concert to protect sensitive functions or information whereby no single entity is able to access or utilise the materials, e.g. cryptographic key.

3.2 key component : One of at least two parameters having the characteristics (e.g. format, randomness) of a cryptographic key that is combined with one or more like parameters to form a cryptographic key.

3.3 key mailer : Envelope that has been designed to convey a key component to an authorised person.

3.4 split knowledge : A condition under which two or more parties separately and confidentially have custody of the constituent part of a single cryptographic key that, individually, convey no knowledge of the resultant cryptographic key.

3.5 secure cryptographic device : A device that provides secure storage for secret information such as keys and provides security services based on this secret information.

ISO 11568-3:1994
<https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-493a-9ab4-100b4b2200ff/iso-11568-3-1994>

4 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.

4.1 Key generation

Each key and each key component shall be generated by a random or pseudo-random process, such that it is not feasible to predict any key nor to determine that certain keys are more probable than other keys from the set of all possible keys.

Except for the variants of a key, the non reversible transformations of a key, and keys enciphered under a key or derived from a key, compromise of one secret key shall not provide any feasibly useful information about any other secret key.

4.2 Key storage

The objective of secure key storage is to protect keys against unauthorized disclosure and substitution and to provide key separation.

4.2.1 Permissible forms

A key shall exist only in the following forms as defined in this subclause :

- plaintext key ;
- key components ;
- enciphered key.

4.2.1.1 Plaintext key

Plaintext secret key(s) whose compromise would affect multiple parties shall exist only within a secure cryptographic device.

Plaintext secret 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.

4.2.1.2 Key components

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

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

When the same key must be created on more than one occasion, different sets of key components

should be used. In this case, 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 key 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 unauthorised access has a high probability of being detected.

If key components are stored in enciphered form all requirements for enciphered keys shall apply.

4.2.1.3 Enciphered key

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

4.2.2 Protection against substitution

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

- a) Physically and procedurally preventing unauthorized access to the key-storage area ;
- b) Storing a key enciphered as a function of its intended use ;
- c) Ensuring that it is not possible to know both a plaintext value and its corresponding ciphertext enciphered under a key encipherment key.

4.2.3 Provisions for key separation

In order to ensure that a stored key is useable only for its intended purpose, key separation for stored keys shall be provided by one or more of the following :

- a) Physically segregating stored keys as a function of their intended purpose ;
- b) Storing a key enciphered under a KEK dedicated to encipherment of a specific type of key ;
- c) Modifying or appending information to a key as a function of its intended purpose, prior to encipherment of the key for storage.

4.3 Key retrieval from back up

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

The requirements for key retrieval from back up are the same as for key distribution and loading described in 4.4.

4.4 Key distribution and loading

A secure cryptographic device should remain in a physically secure environment until loaded with one or more keys.

4.4.1 Plaintext keys

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

- a) The key distribution process shall not disclose any portion of a plaintext key ;
- b) A plaintext key shall be loaded into a 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 ;
- c) A plaintext 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 the transferred key ;
- d) A secure cryptographic device shall transfer a plaintext key only when at least two authorised persons are identified by the device, for example by means of passwords;
- e) When a device is used to transfer keys between the cryptographic device which generated the key and the cryptographic device which will use the key, it 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.

4.4.2 Key components

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

- a) The key component distribution process shall not disclose any portion of a key component to an unauthorised person ;
- b) Key components shall be loaded into a cryptographic device only when it can be assured that the device has not been subject to prior tampering that might lead to the disclosure of keys or sensitive data ;
- c) Key components shall be transferred into a cryptographic device only when it can be ensured

that there is no tap at the interface that might disclose the transferred components ;

- d) The key distribution and loading process shall be performed according to the principles of dual control and split knowledge.

4.4.3 Enciphered keys

Enciphered keys may be distributed and loaded electronically via a communications channel.

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

4.5 Key use

Unauthorized key use shall be prevented. Therefore,

- A key shall be used for only one function. However a variant of a key may be used for a different function from that of the original key ;
- A key shall only be used for its intended function in its intended locations ;
- Any key shall exist in the minimum number of locations consistent with effective system operation. Any key that exists in a transaction-originating device shall not exist in any other such device ;
- A key shall cease to be used when its compromise is known or suspected.

4.6 Key replacement

A key and its variants shall be replaced when compromise of the key is known or suspected. If the key under suspicion is a key encipherment key or a key from which other keys are derived, then all keys which are hierarchically under it shall also be replaced.

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 key by exhaustive 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 key substitution has occurred, both the key and the associated key encipherment key shall be replaced.

Replacement of a key shall take place in all operational locations where the key exists.

Replaced keys shall not be returned to active use.

There are two ways to replace keys :

- by distributing a new key
- by non reversibly transforming the current key.