INTERNATIONAL STANDARD

ISO 11568-2

Third edition
2012-02-01

Financial services — Key management (retail) —

Part 2: Symmetric ciphers, their key management and life cycle

Services financiers — Gestion de clés (services aux particuliers) —

Partie 2: Algorithmes cryptographiques symétriques, leur gestion de clés et leur cycle de vie

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

Reference number
ISO 11568-2:2012(E)

© ISO 2012

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

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 2.

The main task of technical committees is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 11568-2 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

This third edition cancels and replaces the second edition (ISO 11568-2:2005), which has been technically revised.

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

— *Part 1: Principles*

— *Part 2: Symmetric ciphers, their key management and life cycle*

— *Part 4: Asymmetric cryptosystems — Key management and life cycle*

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

Introduction

ISO 11568 is one of a series of standards describing procedures for the secure management of cryptographic keys used to protect messages in a retail financial services environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer.

This part of ISO 11568 addresses the key management requirements that are applicable in the domain of retail financial 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 ISO 11568 describes key management techniques which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

- key separation;
- key substitution prevention;
- key identification;
- key synchronization;
- key integrity;
- key confidentiality;
- key compromise detection.

The key management services and corresponding key management techniques are cross-referenced in Clause 7.

This part of ISO 11568 also describes the key life cycle in the context of 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 herein and in ISO 11568-1. This part of ISO 11568 does not cover the management or key life cycle for keys used in asymmetric ciphers, which are covered in ISO 11568-4.

In the development of ISO 11568, due consideration was given to ISO/IEC 11770; the mechanisms adopted and described in this part of ISO 11568 are those required to satisfy the needs of the financial services industry.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

Financial services — Key management (retail) —

Part 2:
Symmetric ciphers, their key management and life cycle

1 Scope

This part of ISO 11568 specifies techniques for the protection of symmetric and asymmetric cryptographic keys in a retail banking environment using symmetric ciphers and the life-cycle management of the associated symmetric keys. The techniques described enable compliance with the principles described in ISO 11568-1.

The techniques described are applicable to any symmetric key management operation.

The notation used in this part of ISO 11568 is given in Annex A.

Algorithms approved for use with the techniques described in this part of ISO 11568 are given in Annex B.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO 11568-1:2005, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-4, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*

ISO 13491-1, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 13491-2:2005, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

ISO 16609, *Financial services — Requirements for message authentication using symmetric techniques*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Abbreviations used in this part of ISO 11568 are given in Annex C.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

3.1
cipher
pair of operations that effect transformations between plaintext and ciphertext under the control of a parameter called a key

NOTE The encipherment operation transforms data (plaintext) into an unintelligible form (ciphertext). The decipherment operation restores the plaintext.

3.2
counter
incrementing count used between two parties, e.g. to control successive key distributions under a particular key encipherment key

3.3
cryptographic key
mathematical value that is used in an algorithm to transform plain text into cipher text, or vice versa

3.4
data integrity
property that data has not been altered or destroyed in an unauthorized manner

3.5
data key
cryptographic key used for the encipherment, decipherment or authentication of data

3.6
dual control
process of utilizing 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 utilize the materials

NOTE Materials might be, for example, the cryptographic key.

3.7
hexadecimal digit
single character in the range 0 to 9, A to F (upper case), representing a four-bit string

3.8
key component
one of at least two randomly or pseudo-randomly generated parameters having the characteristics (e.g. format, randomness) of a cryptographic key that is combined with one or more like parameters (e.g. by means of modulo-2 addition) to form a cryptographic key

3.9
key mailer
tamper-evident envelope that has been designed to convey a key component to an authorized person

3.10
key offset
offset
result of adding a counter to a cryptographic key using modulo-2 addition

3.11
key space
set of all possible keys used within a cipher

3.12
key transfer device
secure cryptographic device that provides key import, storage and export functionalities

NOTE See ISO 13491-2:2005, Annex F.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

3.13
key transformation
derivation of a new key from an existing key using a non-reversible process

3.14
MAC
message authentication code
code in a message between an originator and a recipient, used to validate the source and part or all of the text of a message

NOTE The code is the result of an agreed calculation.

3.15
modulo-2 addition
XOR
exclusive-or
binary addition with no carry, giving the following values:

$0 + 0 = 0$

$0 + 1 = 1$

$1 + 0 = 1$

$1 + 1 = 0$

3.16
n-bit block cipher
block cipher algorithm with the property that plaintext blocks and ciphertext blocks are n-bits in length

3.17
notarization
method of modifying a key encipherment key in order to authenticate the identities of the originator and the ultimate recipient

3.18
originator
party that is responsible for originating a cryptographic message

3.19
pseudo-random
statistically random and essentially unpredictable although generated by an algorithmic process

NOTE Pseudo-random number generators commonly found in commercial software packages do not provide sufficient randomness for use in cryptographic operations.

3.20
recipient
party that is responsible for receiving a cryptographic message

3.21
secure cryptographic device
SCD
device that provides secure storage for secret information, such as keys, and provides security services based on this secret information

NOTE See ISO 13491-2.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

3.22
split knowledge
condition under which two or more parties separately and confidentially have custody of the constituent part of a single cryptographic key which, individually, conveys no knowledge of the resultant cryptographic key

4 General environment for key management techniques

4.1 General

The techniques that may be used to provide the key management services are described in Clause 5 and the key life cycle in Clause 6. This clause describes the environment within which those techniques operate and introduces some fundamental concepts and operations, which are common to several techniques.

4.2 Functionality of a secure cryptographic device

4.2.1 General

The most fundamental cryptographic operations for a symmetric block cipher are to encipher and decipher a block of data using a supplied secret key. For multiple blocks of data, these operations might use a mode of operation of the cipher as described in ISO/IEC 10116. At this level, no meaning is given to the data, and no particular significance is given to the keys. Typically, in order to provide the required protection for keys and other sensitive information, a secure cryptographic device provides a higher level functional interface, whereby each operation includes several of the fundamental cryptographic operations using some combination of keys and data obtained from the interface or from an intermediate result. These complex cryptographic operations are known as functions, and each one operates only on data and keys of the appropriate type.

4.2.2 Data types

Application level cryptography assigns meaning to data, and data with differing meanings are manipulated and protected in different ways by the secure cryptographic device. Data with a specific meaning constitutes a data type.

The secure cryptographic device ensures that it is not possible to manipulate a data type in an inappropriate manner. For example, a PIN is a data type which is required to remain secret, whereas other transaction data may constitute a data type which requires authentication but not secrecy.

A cryptographic key may be regarded as a special data type. A secure cryptographic device ensures that a key can exist only in the permitted forms given in 4.7.2.

4.2.3 Key types

A key is categorized according to the type of data on which it operates and the manner in which it operates. The secure cryptographic device ensures that key separation is maintained, so that a key cannot be used with an inappropriate data type or in an inappropriate manner. For example, a PIN encipherment key is a key type that is used only to encipher PINs, whereas a key encipherment key (KEK) is a key type that is used only to encipher other keys. Additionally, a KEK may require categorization such that it operates only on one type of key, e.g. one type of KEK may encipher a PIN encipherment key, while another may encipher a message authentication code (MAC) key.

4.2.4 Cryptographic functions

The set of functions supported by the secure cryptographic device directly reflects the cryptographic requirements of the application. It might include such functions as:

— enciphering a PIN;

— verifying an enciphered PIN;

— generating a MAC;

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

— generating an enciphered random key.

The design of the secure cryptographic device is such that no individual function can be used to obtain unauthorized sensitive information. Additionally, no combination of functions exists which might result in such data being obtained. Such a design is referred to as being logically secure. A secure cryptographic device may be required to manage keys of several types. Cryptographic keys used in such a system may be held securely outside of the cryptographic device by being stored in an enciphered form using KEKs, which either exist only within the cryptographic device, or are enciphered under a higher level KEK. One technique of providing key separation is to use a different KEK type for the encipherment of each type of key. When this technique is used, and an enciphered key is passed to the secure cryptographic device, the key is deciphered using the KEK type appropriate for the expected key type. If this key is an incorrect type, and thus is enciphered under some other KEK type associated with some other key type, the decipherment produces a meaningless key value.

4.3 Key generation

4.3.1 General

The key management principles given in ISO 11568-1 require that keys be generated using a process that ensures that it is not possible to predict any key or determine that certain keys within the key space are more probable than others.

In order to conform with this principle, keys and key components shall be generated using a random or pseudo-random process. The pseudo-random key generation process may be either non-repeatable or repeatable.

The random or pseudo-random process used shall be such that it is not feasible to predict any key or to determine that certain keys are more probable than other keys from the set of all possible keys.

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

4.3.2 Non-repeatable key generation

This process may involve a non-deterministic value such as the output of a random number generator, or it may be a pseudo-random process.

An example of a pseudo-random process for generating a key, Kx, is as follows:

$$\mathrm{Kx} = \mathrm{eK}[\mathrm{eK}\,(DT) \oplus V]$$

where

K is a secret cryptographic key reserved for key generation,
V is a secret seed value, and
DT is a date-time vector updated on each key generation.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

A new seed value, V, is generated as follows:

$$V = \mathrm{eK}[\mathrm{Kx} \oplus \mathrm{eK}\,(DT)]$$

NOTE This method, among others, can be found in ISO/IEC 18031.

4.3.3 Repeatable key generation

It is sometimes convenient to generate one or more keys, perhaps thousands, from a single key using a repeatable process. Such a process allows for any of the resultant keys to be regenerated, as required, in any location that possesses the seed key and appropriate generation data, and facilitates significant reductions in the number of keys which require manual management, storage or distribution.

The generation process shall be such that if the initial key is unpredictable within the key space (as required by the key management principles), then so is each resultant key.

The procedure may be used iteratively, as a key generated from one initial key may subsequently be used as an initial key to generate others.

The generation process shall be non-reversible, such that disclosure of a generated key discloses neither the initial key nor any other generated key. An example of such a process is the encipherment of a non-secret value using the initial key.

4.4 Key calculation (variants)

It is possible to obtain a number of keys from a single key using a reversible process. An example of such a process is the modulo-2 addition of the key and a non-secret value.

Key calculation has the qualities of speed and simplicity, but disclosure of one key calculated in this manner discloses the original key and all other keys calculated from it.

4.5 Key hierarchies

A key hierarchy is a conceptual structure in which the confidentiality of certain keys is dependent upon the confidentiality of other keys. By definition, disclosure of a key at one level of the key hierarchy shall not disclose any key at a higher level.

Key encipherment introduces a key hierarchy whereby a KEK is considered to be at a higher level than the key that it enciphers. The simplest is a two-level hierarchy, whereby the working keys are enciphered by KEKs which are themselves stored in a cryptographic device. In a three-level hierarchy, these KEKs are also managed in an enciphered form using a higher-level KEK. The concept may be extended to four or more layers.

Similarly, when an initial key or key generating key (KGK) participates in the generation of other keys using a deterministic process, a hierarchy may result whereby the KGK is considered to be at a higher level than the generated keys.

Keys at the higher levels of the key hierarchy shall be of equal or greater strength than the keys they are protecting.

Due consideration shall be paid to known attacks when assessing the equivalent strength of various cryptographic algorithms. Generally, an algorithm can be said to provide s bits of strength where the best-known attack would take, on average, $2^{s-1}T$ to attack, where T is the amount of time that is required to perform one encryption of a plaintext value and to compare the result against the corresponding ciphertext value. Recommended equivalent key sizes at the time of publication are given in Table 1. In assessing these numbers, consideration shall be paid to any further developments in cryptanalysis, factoring and computing generally. See ISO/TR 14742 for additional information.

Table 1 — Encryption algorithms: equivalent strengths

Effective Strength	Symmetric	RSA	Elliptic curve
80	112-bit TDEA (with 2^{40} known pairs)	1 024	160
112	112-bit TDEA (with no known pairs)	2 048	224
	168-bit TDEA		
128	128-bit AES	3 072	256
192	192-bit AES	7 680	384
256	256-bit AES	15 360	521

NOTE At the time of publication, in the retail banking environment, where TDEA keys are used for protecting other keys and are changed such that the collection of quantities of plaintext/ciphertext pairs sufficient to significantly weaken the underlying cipher is improbable, 112-bit TDEA can be considered to offer sufficient security for the protection of 168-bit TDEA and 2 048-bit RSA keys.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

4.6 Key life cycle

The phases that make up a key's lifetime are collectively referred to as the key's life cycle. Keys shall be protected at all stages throughout their life cycle. An operation that changes a key's state is referred to as a life cycle operation. This subclause specifies the requirements for attaining a given state or performing a given operation.

The key life cycle consists of three phases as follows.

a) Pre-use, during which the key is generated and optionally stored prior to its use.

b) Use, during which the key is distributed among 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.

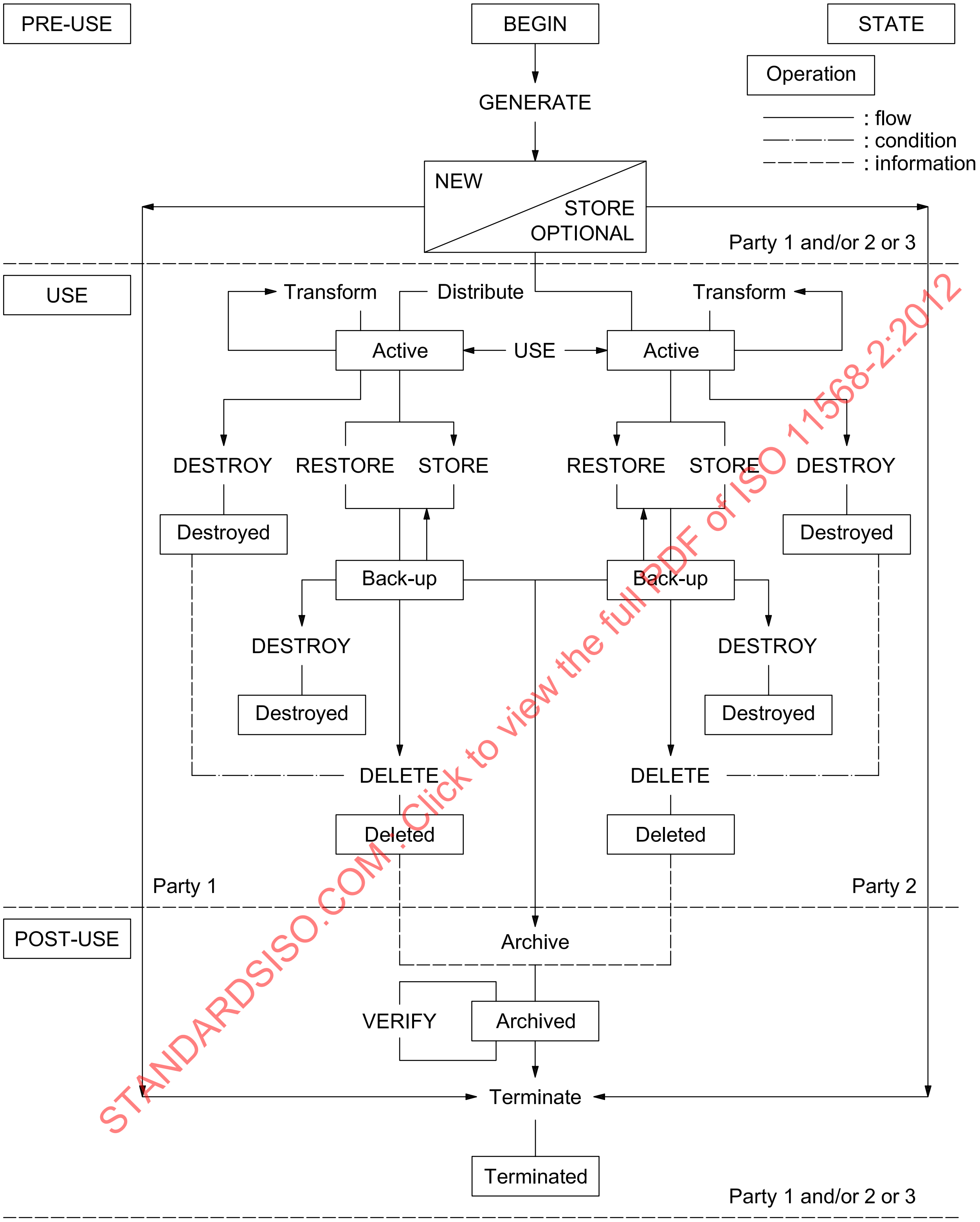
Figure 1 gives a schematic overview of the key life cycle. It shows how a given operation on a key changes its state.

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

Figure 1 — Key life cycle schematic

© ISO 2012 – All rights reserved

4.7 Key storage

4.7.1 General

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

4.7.2 Permissible forms

4.7.2.1 General

A key shall exist only in the following forms:

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

4.7.2.2 Plaintext key

Plaintext secret keys, the compromise of which would affect multiple parties, shall exist only within a secure cryptographic device.

Plaintext secret keys, the compromise of which 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.

4.7.2.3 Key components

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

Key components shall be created such that knowledge of any bit of a component does not provide knowledge of any bit of the corresponding key. For example, each component of a “double length” key is the full length of the final “double length” key.

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 visible 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.

When in component form, it is recommended that a key encrypting key that protects a large number of keys, such as an acquirer or issuer top-level key, comprises at least three components.

4.7.2.4 Enciphered key

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

4.7.3 Key integrity

The integrity of a key shall be protected using techniques such as:

a) MACs (see ISO 16609);

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

b) key block binding methods;

c) digital signatures (see ISO 11568-4).

4.7.4 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 KEK.

4.7.5 Provisions for key separation

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

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.

4.8 Key restoration 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 restoration from back-up are the same as for key distribution and loading described in 4.9.

4.9 Key distribution and loading

4.9.1 General

A secure cryptographic device should remain in an environment as defined in ISO 13491-2:2005, H.3 until loaded with one or more keys.

Keys shall be protected during their distribution and loading by one or more of the following forms:

a) plaintext within an SCD or during transfer between SCDs (see 4.9.2);

b) in component form (see 4.9.3);

c) enciphered (see 4.9.4).

4.9.2 Plaintext keys

The minimum requirements for the distribution and loading of plaintext keys are as follows.

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 ensured 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.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

d) A secure cryptographic device shall transfer a plaintext key only when at least two authorized persons are authenticated by the device, e.g. by means of passwords.

e) A key transfer device is a portable device used to transfer keys between the SCD that generated the key and the SCD that will use the key. A key transfer 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 that might disclose that key.

f) A key injection device is a device used within a key injection facility to transfer keys to the SCD that will use the keys. A key injection device shall be an SCD and shall remain at all times within a key injection facility while in service.

4.9.3 Key components

The minimum requirements for the distribution and loading of a key component are as follows.

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

b) A key component shall be loaded into a cryptographic device only when it can be ensured that the device has not been subject to prior tampering that might lead to the disclosure of keys or sensitive data.

c) A key component shall be transferred to a cryptographic device only when it can be ensured that there is no tap at the interface that might disclose the transferred component.

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

4.9.4 Enciphered keys

An enciphered key may be distributed and loaded electronically via a communications channel.

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

NOTE Methods for achieving the above requirements can be found in ISO/IEC 11770-2.

4.10 Key use

Unauthorized key use shall be prevented. A key shall be used for its intended function and only in its intended location. However, a variant of a key may be used for a different function from that of the original key.

A key shall be used for a single function only.

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

4.11 Key cryptoperiod

Key cryptoperiods serve to:

a) limit the information (related to a specific key) available for cryptanalysis;

b) limit exposure in the case of compromise of a single key;

c) limit the use of a particular technology to its estimated effective lifetime; and

d) limit the time available for computationally intensive cryptanalytic attacks (in applications where long-term key protection is not required).

The cryptoperiod of a key shall be no longer than the least time deemed feasible to perform a dictionary or key exhaustion attack (see ISO/TR 14742 for guidance on usable key life). This time will depend upon the specific implementation and the technology available at the time of the attack.

Keys may be classified based on temporal considerations as follows.

1) Long-term keys, e.g. key-encrypting keys, keys used to validate PINs.

2) Short-term keys, e.g. session keys used for PIN encryption, MACs.

In well-designed crypto systems, key hierarchies are employed to lessen the effects of key compromise. By layering keys into a key hierarchy, each individual key is used less often than would be the case if only single fixed keys were used. Additionally, the higher level (long-term) key encrypting keys are usually used in a manner that prevents access to plaintext/ciphertext pairs for cryptanalysis. In order for such systems to be effective, the lower level (short-term) keys should be replaced on a sufficiently frequent basis to a) limit exposure in case of key compromise, and b) reduce the total plaintext/ciphertext pairs potentially available for cryptanalysis.

At the conclusion of a key's cryptoperiod, it shall be replaced (see 4.12).

4.12 Key replacement

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

— by distributing a new key;

— by non-reversibly transforming the current key.

When the compromise of a key is known or suspected, the key shall be replaced by distribution of a new key and not by the non-reversible transformation of the original key.

Key replacement requires destruction of the old key.

Transformation of a key prevents backtracking, i.e. compromise of the current key does not compromise previously used keys.

4.13 Key destruction

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

When a secure cryptographic device is to be permanently removed from service, all keys stored within the device shall be destroyed.

4.14 Key deletion

When a key is no longer required at an operational location it shall be deleted.

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

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

4.15 Key archive

An archived key shall only be used to verify the legitimacy of transactions that occurred prior to archiving. After such verification, the instance of the key necessary to perform the verification shall be destroyed.

An archived key shall not be returned to operational use.

Archived keys shall be securely stored for the life of all data or keys enciphered under such keys.

A key shall be archived in such a way that the risk of exposure of keys that are still in operational use is not increased.

An archived key shall be retained for no longer than is necessary to meet regulatory, legal and/or business obligations.

4.16 Key termination

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

5 Techniques for the provision of key management services

5.1 General

This clause describes the techniques that shall be used, individually or in combination, to provide the key management services introduced in ISO 11568-1. Some techniques provide multiple key management services. A cross-reference between the key management services and the techniques is given in Clause 7.

The selected techniques shall be implemented in a secure cryptographic device (see ISO 13491-1 and ISO 13491-2) that ensures the intended purpose of the technique and its security objectives are achieved.

5.2 Key encipherment

Key encipherment is a technique whereby one key is enciphered using another key. The resulting enciphered key may then be managed securely outside the protected environment of a secure cryptographic device. A KEK is used to perform such encipherment. Although key encipherment ensures that key confidentiality is maintained, other techniques might need to be employed in association with the key encipherment in order to ensure adequate key separation, to prevent key substitution and to ensure key integrity.

Where the length of the enciphered key exceeds the block size of the key encrypting cipher, the individual blocks of the enciphered key shall:

a) have integrity, whereby no block in the key has been altered in an unauthorized manner since the time it was generated, transmitted or stored by an authorized source;

b) be used in the appropriate order, as specified by the particular mode;

c) be considered a fixed quantity in which an individual block cannot be manipulated while leaving the other block(s) unchanged;

d) be such that they cannot be unbundled for any unauthorized purpose.

5.3 Key variants

Key variants allow a set of keys to be obtained from a single key, with each resulting key having a different key type.

This technique provides key separation while eliminating the need to manage a separate, unrelated key of each required type. Each variant key is calculated from the original key and one constant from a set of non-secret constants using a repeatable process, f, as illustrated in Figure 2. The process of repeatable key calculation is described in 4.3.3.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

A constant having a unique value in the set of constants shall be allocated to each key type to be calculated from the original key using the key variants technique.

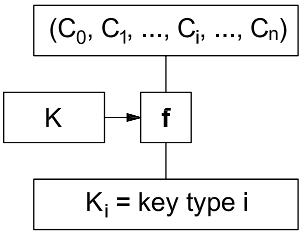


Figure 2 — Variant key calculation

A variant key calculated using a reversible process shall exist only in the cryptographic device which contains the original key.

The key variants technique is applicable at all levels of a key hierarchy. A single key may be used to calculate a set of KEKs of different types, i.e. each KEK is to be used to encipher a different key type. Alternatively, a single key may generate a set of working keys of different types.

5.4 Key derivation

Key derivation is a technique by which a (potentially large) number of keys is generated ("derived") from a single initial key and non-secret variable data, with each resulting key being the initial key for a different secure cryptographic device, typically the PIN pad of a POS terminal. The initial key is called a "derivation key" and each key generated from it is called a "derived key". Key derivation provides key separation by generating a (statistically) unique key for each cryptographic device without the need to manage a large number of separate, unrelated keys. This eliminates the need to store the ciphertext of each initial key at the acquirer or receiving node. Similarly, when a key is needed for subsequent use it is derived again from the derivation key and appropriate derivation data.

The derived key generation procedure utilizes a non-reversible process, as illustrated in Figure 3, using the derivation key and data that uniquely identify the target cryptographic device.

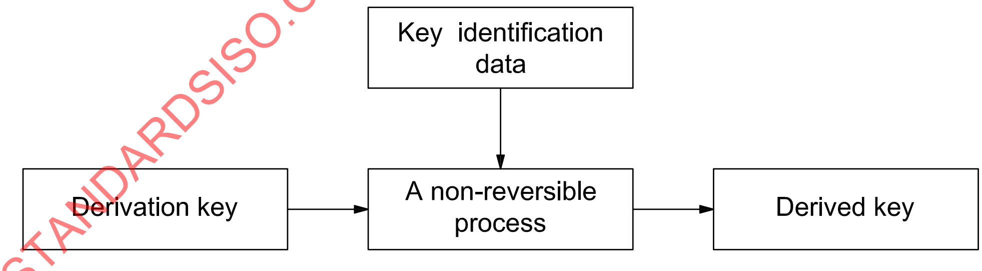


Figure 3 — Generation of a derived key

The use of a non-reversible process ensures that the compromise of a derived key does not disclose the derivation key or any other derived keys. However, compromise of a derivation key discloses all keys derived from it.

Key calculation (see 4.4), through its use of a reversible process, is not suitable for use as a key derivation method.

5.5 Key transformation

Key transformation is a technique whereby a secure cryptographic device (typically the PIN pad of a POS terminal) effects key replacement by generating one or more future keys from its current key and then erasing all trace of the current key.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

Key transformation lessens the impact of key compromise by enabling the cryptographic device to replace its key or keys at frequent intervals (e.g. after every transaction) without the need for a key distribution process.

Key transformation is accomplished by using the current key as the initial key for a non-reversible key generation process, as illustrated in Figure 4. The process also involves other data relevant to the implementation that may be device- or transaction-related data, or may be a key replacement counter.

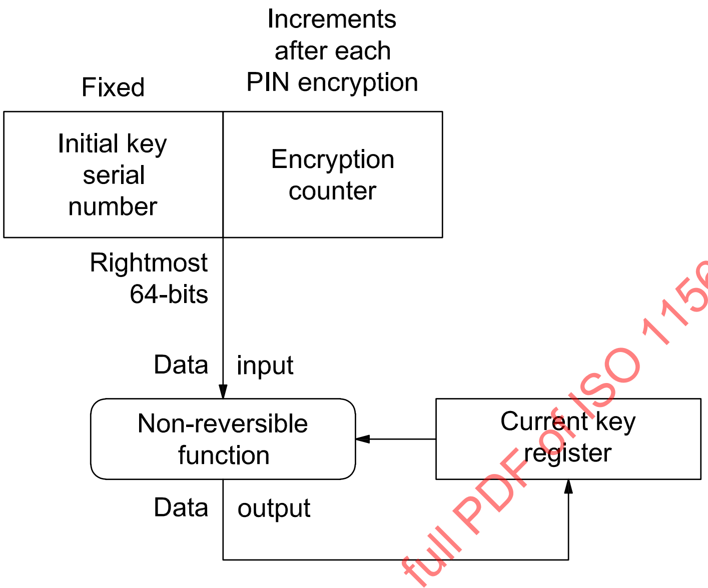


Figure 4 — Generation of future keys

The use of a non-reversible function ensures that the compromise of a cryptographic device using transformed keys does not disclose any key previously used by the device, even given the knowledge of all relevant data, which has ever existed outside of the device other than within another cryptographic device.

Equipment in cryptographic communication with a device which utilizes key transformation determines the key in use by the device at any time by one of the following means.

a) Replicating the key transformation process in synchronization with the device, and storing the resultant key or keys for subsequent use.

b) Receiving the current value of the key replacement counter, which is included in the transaction data transmitted from the device, and generating the current key from the counter and the initial key. This procedure involves performing all those key transformations which lead directly from the initial key to the current key. Typically, the number of transformations required is small, e.g. 10, even though the key replacement counter increments to a large value, e.g. 1 million (see ANSI X9.24-1:2009, Annex A).

5.6 Key offsetting

Key offsetting is a technique for calculating a new KEK from an initial key each time a new enciphered key is to be transmitted to a receiving node.

The technique prevents the substitution of a previous (but replaced) key for the current key exchanged between communicating parties.

A counter, which is incremented each time a replacement key is required, is combined with the initial KEK using a repeatable process (e.g. modulo-2 addition). The resulting key is the KEK with which the replacement key is enciphered, as illustrated in Figure 5.

Typically, the current value of the counter is transmitted to the receiving node along with the enciphered key.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

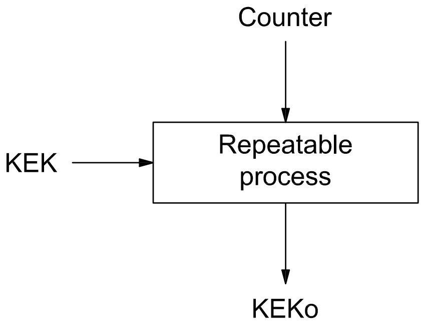


Figure 5 — Calculation of a KEK offset (KEKo)

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

5.7 Key notarization

5.7.1 Description

Key notarization is a technique whereby the identities of the communicating parties are incorporated in the KEK, or KEKs, before key encipherment occurs.

Key notarization prevents key substitution. Should an enciphered key intended for use between other parties be substituted for the correct enciphered key, the decipherment of the substituted key would produce a garbled result.

Key notarization is a method for sealing keys with the identities of the communication pair. It is achieved by creating a notary seal (NS). Once notarized, using the method described below, keys can only be recovered with knowledge of the key used to perform the notarization (KP) and the identities of the communication pair. KEKs or data enciphering keys (KD) may be notarized by encipherment using a notarizing key (KN) formed by taking the modulo-2 sum of the KP with the NS.

5.7.2 Method

A unique identifier shall be used to identify each party to the notarization process. If necessary, an identifier may be replicated to form the requisite key length. Suppose that Party A wishes to send a key to Party B. Let FM1 be the first eight bytes of Party A's identifier and let FM2 be the second eight bytes. Similarly let TO1 and TO2 represent the first and second halves of Party B's identifier. Each party has prior knowledge of the shared secret key (KP) used to perform the notarization.

An intermediate key (KI) is formed by the modulo-2 addition of KP and the concatenation of TO1 and FM1.

KI = KP XOR (TO1 || FM1)

Then the NS is formed from the concatenation of the results of encrypting TO2 and FM2 with the KI.

NS = eKI(TO2) || eKI(FM2)

The KN is formed by the modulo-2 addition of KP with NS.

KN = KP XOR NS

KN is then used to notarize (by encipherment) either a KD or KEK.

5.8 Key tagging

Key tagging is a technique whereby a key existing outside of a cryptographic device has an associated tag that identifies the key type. A key and its tag are bound together in a manner that prevents undetectable modification of the key tag.

© ISO 2012 – All rights reserved

Key tagging provides key separation. It is used in combination with key encipherment and allows multiple key types to be enciphered using a single KEK.

A key tag consists of a distinct but otherwise arbitrary constant. A different key tag shall be allocated to each key type to be tagged. When a key is generated in the secure cryptographic device, it is bound together with the tag appropriate to the key type as part of the key encipherment process, as illustrated in Figure 6. The tagged key may then be stored or distributed outside a cryptographic device.

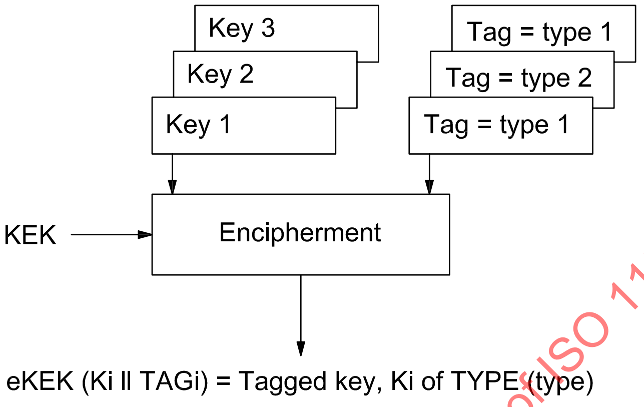


Figure 6 — Tagged key generation

When a tagged key is passed into a secure cryptographic device for use in a specific function, it is first deciphered, then the key tag is recovered and checked within the device, as illustrated in Figure 7. If the key tag reveals that the type is not appropriate to the requested function, the function shall be aborted.

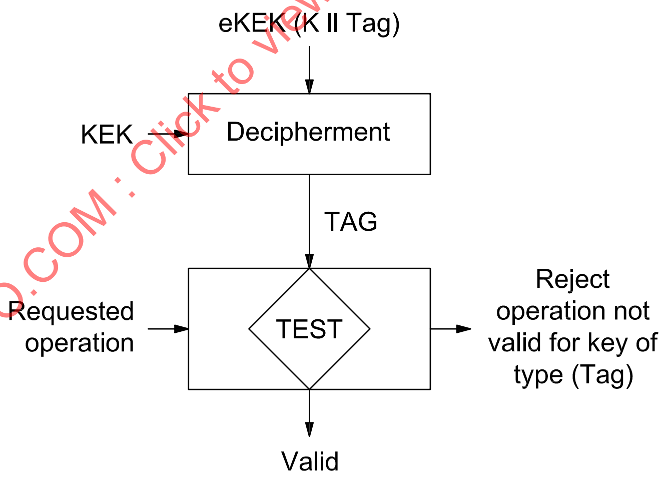


Figure 7 — Tagged key use

The manner in which the key and its tag are bound is dependent on whether or not their combined length exceeds the block length of the cipher used for key encipherment. If the block length is not exceeded, the key bits and tag bits may be concatenated or interleaved and the resultant block enciphered. If the block length is exceeded, the key and tag occupy separate blocks for encipherment. In this case, a chaining mode of encipherment (see ISO/IEC 10116), together with integrity protection techniques, shall be used in order to bind the key and its tag together.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

5.9 Key verification

A key verification code (KVC) is a value cryptographically related to the key and some additional non-secret information. When used in conjunction with appropriate integrity-assurance mechanisms, the KVC provides assurance that one or more of the following conditions has been met:

a) a key has been correctly entered into a cryptographic device;

b) a key has been correctly received over a communications channel;

c) a key has not been altered;

d) an instance of a key transformation or derivation remains in synchronization.

A common use of KVCs is to find where keys have been altered or corrupted in a network. Any key failing the KVC test shall be suspected of having been corrupted or compromised.

An example of a KVC implementation is to encipher a fixed, commonly known, non-secret constant (e.g. a 16-digit hexadecimal value) under the key in question (see Figure 8), then truncate the resulting ciphertext (e.g. six digits).

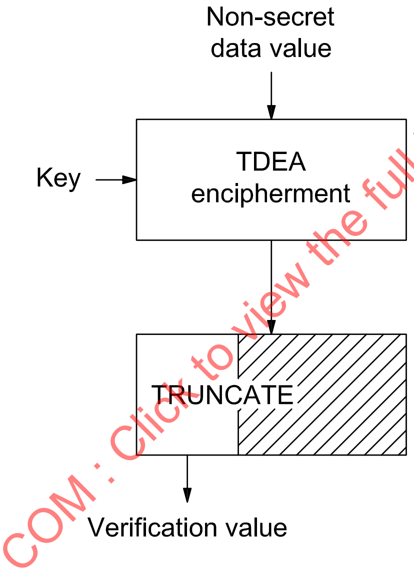


Figure 8 — Example of KVC function

The KVC is transported via an integrity assured channel (either electronically or by other means) to the location where verification will take place, then entered into the cryptographic processor. The key that it is verifying may be sent to this location by the same or by a different route. The same cryptographic function is then performed on the received key and the output of this is compared to the key verification code.

The known, non-secret value should be supplied by the cryptographic device that generates the KVC, and the KVC should be substantially truncated (e.g. to six digits). Otherwise, the KVC-produced capability could be misused to encipher known plaintext.

The KVC shall only be calculated over the entire key.

5.10 Key identification

Key identification enables the transaction recipient to determine the appropriate key or keys associated with the transaction. Two methods are available: explicit and implicit.

Explicit key identification is the inclusion in a transaction message of information that identifies the key or keys used to encipher or authenticate data in that message. The technique is especially useful when many

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

cryptographic devices, all with unique keys, communicate with a single facility. This is because it enables this facility to determine the key or keys to be used with any given message it receives.

With implicit key identification, the key used with a message is determined from other message-related information, such as the terminal identifier or the communications line over which the message is received.

5.11 Controls and audit

It is not always possible or feasible to prevent security compromises. However, the effects of a compromise can often be averted if the compromise is detected. It is especially important:

a) to detect the disclosure of a key, and

b) to detect the substitution of a disclosed key for a legitimate key.

Key disclosure can be detected by:

— audits and controls imposed on those individuals who manage keys and/or cryptographic devices, in order to detect possible collusion between such people which might have resulted in key disclosure;

— periodic inspection of, and control over, interfaces through which unenciphered keys or key components are transferred, in order to detect “bugs” or “taps” that might have resulted in the disclosure of transferred keying material;

— control and auditing of cryptographic devices that contain keys, in order to detect any lost or stolen devices.

If it is known or suspected that a cryptographic device has been lost or stolen, the keys contained in the device are considered to have been disclosed.

Key substitution (of a disclosed key) can be detected by the following means.

1) When explicit key identification is used, verifying that a just-received key identifier has the expected value.

2) Maintaining a “negative file” of keys whose disclosure is known or suspected and, when appropriate, performing audits of presumed valid keys to ensure that none is listed on the negative file. When explicit key identification is used, the key identifier of the disclosed key can be used to identify the key in the “negative file” entry, otherwise the enciphered version of the key itself can be used to identify the disclosed key in the “negative file” entry.

3) Performing periodic audits of presumed-valid keys to ensure that no key is associated with more than one cryptographic device (the audit can use enciphered keys, or key identifiers). This detects the replication of a disclosed key.

Unauthorized key modification, deletion and insertion, as well as some instances of key substitution, which have occurred in association with a cryptographic device (e.g. a device that enciphers) are detected when the corresponding cryptographic device that performs the inverse operation (e.g. decipherment) produces a garbled or otherwise invalid result.

The above audits and controls also serve to deter, and thus prevent, some security compromises. Furthermore, an audit of a cryptographic device’s functionality can prevent key misuse by ensuring that the device is capable of performing only authorized functions.

5.12 Key integrity

Techniques shall be used that cryptographically link all bits of the key in order to address the key integrity requirements listed in 5.2.

Examples of methods for ensuring the integrity of enciphered keys include those given in ISO/TR 19038.

Other methods are permissible, provided the requirements of 5.2 are met.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

6 Symmetric key life cycle

6.1 General

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 and to ensure integrity.

Requirements applying to specific life cycle stages are specified in 6.2 to 6.8.

6.2 Key generation

Keys and key components shall be generated by one of the following methods, as described in 4.3.

a) Non-repeatable key generation using

   1) a random process, or

   2) a pseudo-random process.

b) Repeatable key generation using

   1) key transformation, or

   2) key derivation.

6.3 Key storage

6.3.1 General

Keys are protected against unauthorized disclosure and substitution by implementation of one of the secure key storage forms described in 4.7.2.

Replacement of a key for which substitution is known, suspected or anticipated requires execution of the procedures described in 6.3.3.

6.3.2 Permissible forms

6.3.2.1 General

This subclause describes the methods of secure key storage for each of the permissible forms.

6.3.2.2 Plaintext key

A plaintext key shall only be stored in a secure cryptographic device that complies with the requirements given in ISO 13491-1 and ISO 13491-2.

6.3.2.3 Key components

A key component shall be conveyed to authorized persons by means of a uniquely identifiable (e.g. serialized) key mailer or a 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 in such a way that it is highly likely that accidental or fraudulent opening will be obvious to the 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 or sealed in a new tamper-evident key mailer for possible future use.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved

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

6.3.2.4 Enciphered key

Key encipherment shall be as specified in 5.2.

6.3.3 Key substitution — Remediation

If unauthorized key substitution is known, suspected or anticipated, based on information that an adversary has already obtained, the following procedure to replace the key shall be followed.

a) Erase the enciphered version of any stored key for which substitution is known and verify that all currently stored enciphered keys are legitimate; if any are not legitimate, they shall be deleted.

b) Translate the legitimate stored enciphered keys to encipherment under a new KEK.

c) Delete the old KEK at all operational locations.

6.4 Key restoration from back-up

Restoration of keys from back-up shall be implemented by one of the methods described for loading and distribution.

6.5 Key distribution and loading

6.5.1 General

This subclause describes the implementation of key distribution and loading techniques for each of the permissible key forms satisfying the requirements given in 4.9.

The distribution and loading of keys into a secure cryptographic device shall be performed using one of following techniques:

a) manual, e.g. key component entry via a key pad;

b) electronic direct loading, e.g. direct key injection via a cable from the originating device or a key transfer device;

c) network distribution and loading, e.g. remote key transport via a network.

The permissible techniques to load keys into a secure cryptographic device as a function of the different key forms are indicated by a check mark in Table 2.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

Table 2 — Permissible key distribution and loading techniques

	Techniques		
		Electronic	
Key forms	**Manual**	**Direct**	**Network**
Plaintext keys		√	
Key components	√	√	
Enciphered	√	√	√

6.5.2 Plaintext keys

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

When explicit key identification is used, the (non-secret) key identifier should be transferred at the same time that the (secret) key is transferred.

When a key transfer device is used, the key (and its identifier, if explicit key identification is used) is transferred from the source secure cryptographic device into the key transfer device. This portable device is then physically transported to the secure cryptographic device that will actually use the key. The key (and its identifier) is 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 for direct electronic key loading.

A key transfer device may be given a number of unique keys (each with its identifier, if appropriate), and thus may be used to provide initial keys to a number of remote cryptographic devices.

An alternative version of a key transfer device uses a key generation mechanism to establish unique cryptographic relationships between a number of remote cryptographic devices communicating with a single central cryptographic device. During the initialization process, the key transfer device is attached to the central cryptographic device to receive an initial key. The key transfer device shall then use non-reversible derivations of this key to generate unique keys for the remote cryptographic devices, to which it is physically transported. The key generation device shall not retain any information that could disclose any key after generation and loading.

If available, the key verification code should be verified after key loading.

6.5.3 Key components

When this technique is used the components that form the key are manually entered into the device. When key components are distributed in human-comprehensible form, each such component shall be distributed in a key mailer that does not disclose the value of the component until opened.

Prior to entering the key component, the key mailer shall be checked for signs of tampering. If tampering of one 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 5.9 shall be used to verify correct key component 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 over the resultant key by one of the methods described in 5.9 shall be used to verify correct key construction.

6.5.4 Enciphered keys

The distribution of enciphered keys over a network may require the transmission of special cryptographic service messages, by which the party initiating the key change so informs the other party. Care shall be taken to avoid cryptographic synchronization problems.

A KEK shall be at least of equal or greater strength than the key that it is protecting.

NOTE As noted in 4.5, at the time of publication, in the retail banking environment, where TDEA keys are used for protecting other keys, and are changed such that the collection of quantities of plaintext/ciphertext pairs sufficient to significantly weaken the underlying cipher is improbable, 112-bit TDEA can be considered to offer sufficient security for the protection of 168-bit TDEA and 2048-bit RSA keys. See Table 1.

Protection against misuse of keys during their operational use requires the application of one of the techniques described in this part of ISO 11568 in order to protect against substitution and modification.

Keys used for encipherment of other keys shall be known to both the originator and the recipient of the enciphered keys.

STANDARDSISO.COM : Click to view the full PDF of ISO 11568-2:2012

© ISO 2012 – All rights reserved