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

Reference number
ISO 11568-2:2012(E)

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

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*

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.

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.

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.

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.

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;

— 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.

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.