INTERNATIONAL STANDARD

ISO/IEC 11770-1

First edition
1996-12-15

Information technology — Security techniques — Key management —

Part 1: Framework

Technologies de l'information — Techniques de sécurité —

Partie 1: Cadre général

Reference number
ISO/IEC 11770-1:1996(E)

Contents

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Annexes

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 11770-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques.*

ISO/IEC 11770 consists of the following parts, under the general title *Information technology — Security techniques — Key management:*

- *Part 1: Framework*
- *Part 2: Mechanisms using symmetric techniques*
- *Part 3: Mechanisms using asymmetric techniques*

Further parts may follow.

Annexes A to E of this part of ISO/IEC 11770 are for information only.

Introduction

In Information Technology there is an ever increasing need to use cryptographic mechanisms for the protection of data against unauthorised disclosure or manipulation, for entity authentication, and for non-repudiation functions. The security and reliability of such mechanisms are directly dependent on the management and protection afforded to a security parameter, the key. The secure management of these keys is critical to the integration of cryptographic functions into a system, since even the most elaborate security concept will be ineffective if the key management is weak. The purpose of key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms.

The fundamental problem is to establish keying material whose origin, integrity, timeliness and (in the case of secret keys) confidentiality can be guaranteed to both direct and indirect users. Key management includes functions such as the generation, storage, distribution, deletion and archiving of keying material in accordance with a security policy (ISO 7498-2).

This part of 11770 has a special relationship to the frameworks for Open System Security (ISO/IEC 10181). All the frameworks, including this one, identify the basic concepts and characteristics of mechanisms covering different aspects of security. This part of ISO/IEC 11770 introduces general models for key management that are fundamental for symmetric and asymmetric cryptographic mechanisms.

This page intentionally left blank

INTERNATIONAL STANDARD © ISO/IEC **ISO/IEC 11770-1 : 1996 (E**

Information technology — Security techniques — Key management —

Part 1: Framework

1 Scope

This part of ISO/IEC 11770:

1. identifies the objective of key management;
2. describes a general model on which key management mechanisms are based;
3. defines the basic concepts of key management common to all the parts of this multi-part standard;
4. defines key management services;
5. identifies the characteristics of key management mechanisms;
6. specifies requirements for the management of keying material during its life cycle; and
7. describes a framework for the management of keying material during its life cycle.

This framework defines a general model of key management that is independent of the use of any particular cryptographic algorithm. However, certain key distribution mechanisms may depend on particular algorithm properties, for example, properties of asymmetric algorithms.

Specific key management mechanisms are addressed by other parts of ISO/IEC 11770. Symmetric mechanisms are addressed in part 2 (ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*). Asymmetric mechanisms are addressed in part 3 (ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*). This part of ISO/IEC 11770 contains the material required for a basic understanding of parts 2 and 3. Examples of the use of key management mechanisms are included in ISO 8732 and ISO 11166. If non-repudiation is required for key management, ISO/IEC 13888 should be used.

This part of ISO/IEC 11770 addresses both the automated and manual aspects of key management, including outlines of data elements and sequences of operations that are used to obtain key management services. However it does not specify details of protocol exchanges that may be needed.

As with other security services, key management can only be provided within the context of a defined security policy. The definition of security policies is outside the scope of this multi-part standard.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 11770. 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/IEC 11770 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 7498-2: 1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.*

ISO/IEC 9798-1: 1991, *Information technology — Security techniques — Entity authentication mechanisms — Part 1: General model.*

ISO/IEC 10181-1: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview.*

3 Definitions

The following terms are used as defined in ISO 7498-2:

data integrity

data origin authentication

digital signature

The following term is used as defined in ISO/IEC 9798-1:

entity authentication

The following terms are used as defined in ISO/IEC 10181-1:

security authority

security domain

trusted third party (TTP)

For the purposes of ISO/IEC 11770, the following definitions apply.

3.1 asymmetric cryptographic technique: A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

3.2 certification authority (CA): A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities.

3.3 decipherment: The reversal of a corresponding encipherment.

3.4 encipherment: The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data.

3.5 key: A sequence of symbols that controls the operation of a cryptographic transformation (e.g., encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

3.6 key agreement: The process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key.

3.7 key confirmation: The assurance for one entity that another identified entity is in possession of the correct key.

3.8 key control: The ability to choose the key, or the parameters used in the key computation.

3.9 key distribution centre (KDC): An entity trusted to generate or acquire, and distribute keys to entities that each share a key with the KDC.

3.10 keying material: The data (e.g., keys, initialisation values) necessary to establish and maintain cryptographic keying relationships.

3.11 key management: the administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

3.12 key translation centre (KTC): An entity trusted to translate keys between entities that each share a key with the KTC.

3.13 private key: That key of an entity's asymmetric key pair which should only be used by that entity.

NOTE: A private key shall not normally be disclosed.

3.14 public key: That key of an entity's asymmetric key pair which can be made public.

3.15 public key certificate: The public key information of an entity signed by the certification authority and thereby rendered unforgeable.

3.16 public key information: information specific to a single entity which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, and the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms.

3.17 random number: A time variant parameter whose value is unpredictable.

3.18 secret key: A key used with symmetric cryptographic techniques and usable only by a set of specified entities.

3.19 sequence number: A time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period.

3.20 symmetric cryptographic technique: A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

3.21 time stamp: A time variant parameter which denotes a point in time with respect to a common time reference.

3.22 time variant parameter: A data item used by an entity to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp.

4 General Discussion of Key Management

Key management is the administration and use of the services of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material.

The objective of key management is the secure administration and use of these key management services and therefore the protection of keys is extremely important.

Key management procedures depend on the underlying cryptographic mechanisms, the intended use of the key and the security policy in use. Key management also includes those functions that are executed in cryptographic equipment.

4.1 Protection of Keys

Keys are a critical part of any security system that relies on cryptographic techniques. The appropriate protection of keys depends on a number of factors, such as the type of application for which the keys are used, the threats they face, the different states the keys may assume, etc. Primarily, depending upon the cryptographic technique, they have to be protected against disclosure, modification, destruction and replay. Examples of possible threats to keys are given in Annex A. The validity of a key shall be limited in time and amount of use. These constraints are governed by the time and amount of data required to conduct a key-recovery attack and the strategic value of the secured information over time. Keys that are used to generate keys need more protection than the generated keys. Another important aspect of the protection of keys is avoidance of their misuse, e.g., use of a key encipherment key to encipher data.

4.1.1 Protection by Cryptographic Techniques

Some threats to keying material can be countered using cryptographic techniques. For example: encipherment counters key disclosure and unauthorised use; data integrity mechanisms counter modification; data origin authentication mechanisms, digital signatures, and entity authentication mechanisms counter masquerade.

Cryptographic separation mechanisms counter misuse. Such separation of functional use may be accomplished by binding information to the key. For example: binding control information to the key assures that specific keys are used for specific tasks (e.g. key encipherment, data integrity); key control is required for non-repudiation using symmetric techniques.

4.1.2 Protection by non-Cryptographic Techniques

Time stamps may be used to restrict the use of keys to certain valid time periods. Together with sequence numbers, they also protect against the replay of recorded key agreement information.

4.1.3 Protection by Physical Means

Each cryptographic device within a secure system usually needs to protect the keying material it uses against the threats of modification, deletion and, except for public keys, disclosure. The device typically provides a secure area for key storage, key use and cryptographic algorithm implementation. It may provide the means

- to load keying material from a separate secure key storage device,
- to interact with cryptographic algorithms implemented in separate *smart* security facilities (for example, smart cards, memory cards), or
- to store keying material off-line (for example, on diskette).

Secure areas typically are protected by physical security mechanisms.

4.1.4 Protection by Organisational Means

One means of protecting keys is to organise them into key hierarchies. Except at the lowest level of the hierarchy, keys in one level of a hierarchy are used solely to protect keys in the next level down. Only keys in the lowest level of the hierarchy are used directly to provide data security services. This hierarchical approach allows the use of each key to be limited, thus limiting exposure and making attacks difficult. For example, the compromise of a single session key is limited to compromising only the information protected by that key.

The use of secure areas addresses the threats of key disclosure, modification and deletion by unauthorised entities. However, the threat remains that system administrators, authorised to perform certain management functions on components of the key management service, may misuse the special access privileges they possess. In particular, they might try to obtain a master key (a top level key in a key hierarchy). Disclosure of a master key will potentially enable the possessor to discover or manipulate all other keys protected by it (i.e. all other keys in that particular key hierarchy). It is therefore desirable to minimise access to this key, perhaps by arranging that no single user has access to its value. Such a requirement can be met by dividing the key (dual control or even n-times control) or using dedicated cryptographic schemes *(Secret Sharing Schemes).*

4.2 Generic Key Life Cycle Model

A cryptographic key will progress through a series of states that define its life cycle. The three principal states are:

Pending Active: In the Pending Active state, a key has been generated, but has not been activated for use.

Active: In the Active state, the key is used to process information cryptographically.

Post Active: In this state, the key shall only be used for decipherment or verification.

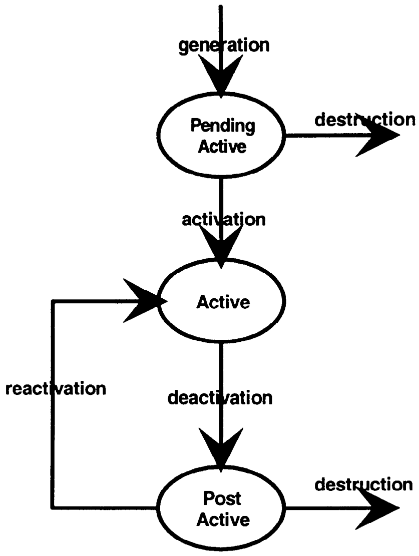

Figure 1 — Key Life Cycle

NOTE: The user of a Post Active key shall be assured that the data had been cryptographically processed before the key became Post Active. This assurance is commonly provided by a trusted time variant parameter.

A key that is known to be compromised shall become Post Active immediately and may require special handling. A key is said to be compromised when its unauthorised use is known or suspected.

Figure 1 shows these states and the corresponding transitions.

Figure 1 represents a generic life cycle model. Other life cycle models may have additional details that may be substates of the three states presented. The majority of life cycles require an archival activity. This activity may be associated with any of the states, depending on the particular details of the life cycle.

4.2.1 Transitions between Key States

When a key progresses from one state to another it undergoes one of the following transitions as also depicted in figure 1:

Generation is the process of generating a key. Key Generation should be performed according to prescribed key generation rules; the process may involve a test procedure to verify whether these rules have been followed..

Activation makes a key valid for cryptographic operations.

Deactivation limits a key's use. This might occur because the key has expired or has been revoked.

Reactivation allows a Post Active key to be used again for cryptographic operations.

Destruction ends a key's life cycle. It covers logical destruction of the key and may also involve its physical destruction.

Transitions may be triggered by events such as the need for new keys, the compromise of a key, the expiration of a key, and the completion of the key life cycle. All these transitions include a number of services for key management. The relationships between the transitions and the services are shown in Table 1. These services are explained in Clause 5.

Any particular cryptographic approach will only require a subset of the services offered in Table 1.

4.2.2 Transitions, Services and Keys

Keys for particular cryptographic techniques will use different combinations of services during their life cycles. Two examples are given below.

For symmetric cryptographic techniques, following the generation of a key, the transition from Pending Active to Active includes key installation and may also include key registration and distribution. In some cases, installation may involve the derivation of a specific key. The lifetime of a key should be limited to a fixed period. Deactivation ends the Active state, usually upon expiration. If compromise of a key in the Active state is suspected or known, revocation also causes it to enter the Post Active state. A Post Active key may be archived. If an archived key is needed again, it will be reactivated and may need to be installed or distributed again before it is fully active. Otherwise, following deactivation, the key may be deregistered and destroyed.

For asymmetric cryptographic techniques, a pair of keys (public and private) is generated and both keys enter the Pending Active state. Note that the life cycles of the two keys are related but not identical. Before it enters the Active state, a private key may optionally be registered, may optionally be distributed to its user and is always installed. The transitions between the Active and the Post Active states for a private key, including deactivation, reactivation, and destruction, are similar to those described above for symmetric keys. When a public key is certified, commonly a certificate containing the public key is created by the CA, to assure the validity and ownership of the public key. This public key certificate may be placed in a directory or other similar service for distribution, or may be passed back to the owner for distribution. When the owner sends out information signed with his private key he may add his certificate. The key pair becomes active when the public key is certified. When a key

Table 1 — Transitions and Services

Transition	Service	Notes
Generation	generate-key	mandatory
	register-key	optional either here or activation
	create-key-certificate	optional
	distribute-key	optional
	store-key	optional
Activation	create-key-certificate	optional
	distribute-key	optional
	derive-key	optional
	install-key	mandatory
	store-key	optional
	register-key	optional either here or generation
Deactivation	store-key	optional
	archive-key	optional either here or destruction
	revoke-key	optional
Reactivation	create-key-certificate	optional
	distribute-key	optional
	derive-key	optional
	install-key	mandatory
	store-key	optional
Destruction	deregister-key	mandatory, if registered
	destroy-key	mandatory
	archive-key	optional either here or deactivation

pair is used for digital signature purposes the public key may remain in the Active or Post Active state for an indefinite time after its related private key has been deactivated or destroyed. Access to the public key may be necessary to verify digital signatures made before the original expiration date of the associated private key. When asymmetric techniques are used for encipherment and the key used for encipherment has been deactivated or destroyed, the corresponding key of the pair may remain in the Active or Post Active state for later decipherment.

The use or application of a key may determine the services for that key. For example, a system may decide not to register session keys, since the registration process may last longer than their lifetime. By contrast, it is necessary to register a secret key when symmetric techniques are used for digital signature.

5 Concepts of Key Management

5.1 Key Management Services

This Clause describes a general structure for key management to aid understanding of the key management services, how they fit together and how they are supported.

Key management relies on the basic services of generation, registration, certification, distribution, installation, storage, derivation, archiving, revocation, deregistration and destruction. These services may be part of a key management system or be provided by other service providers. Depending on the kind of service, the service provider must fulfil certain minimum security requirements (e.g., secure exchange) to be trusted by all entities involved. For example, the service provider may be a trusted third party. Figure 2 shows that the key management