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

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.

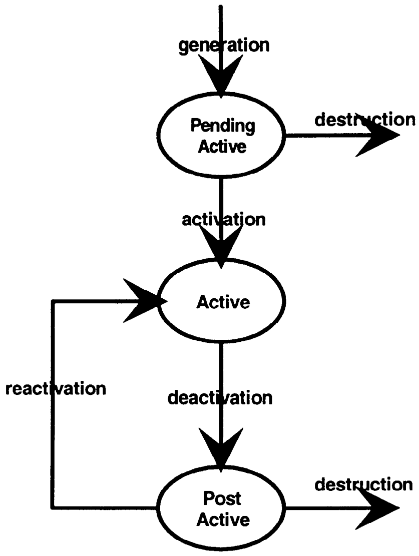

Figure 1 — Key Life Cycle

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 ceıtificate 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

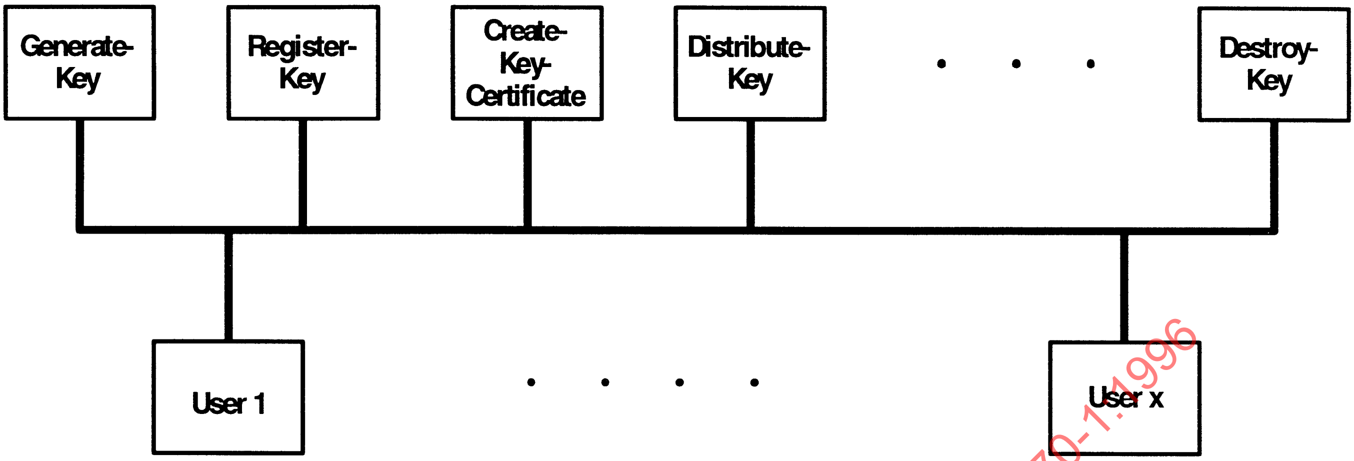

Figure 2 — Key Management Services

services are positioned at the same level and may be used by a variety of different users (persons or processes). These users may utilise different key management facilities within different applications, making use of services specific to their needs. The key management services are listed in Table 1.

5.1.1 Generate-Key

Generate-Key is a service that is invoked to generate keys in a secure way for a particular cryptographic algorithm. This implies that the key generation cannot be manipulated and, that the keys are generated in an unpredictable way and according to a prescribed distribution. This distribution is imposed by the cryptographic algorithm for which it will be used and the required level of cryptographic protection. The generation of some keys, e.g., master keys, demands special care because knowledge of these keys offers access to all related or derived keys.

5.1.2 Register-Key

The service Register-Key associates a key with an entity. It is provided by a registration authority, and is usually applied when symmetric cryptographic techniques are used. When an entity wishes to register a key it has to contact the registration authority. Key registration involves a request for registration and a confirmation of that registration.

A registration authority maintains a register of keys and related information in a suitably secure manner. Annex B offers details of key management information.

Operations provided by a key registration authority are registration and deregistration.

5.1.3 Create-Key-Certificate

The service Create-Key-Certificate assures the association of a public key with an entity and is provided by a certification authority. When a request for key certification is accepted, the certification authority creates a key certificate. Public key certificates are discussed in more detail in ISO/IEC 11770-3.

5.1.4 Distribute-Key

Key distribution is a set of procedures to provide key management information objects (see example in Annex B) securely to authorised entities. A specific case of key distribution is key translation where keying material is established between entities using a key translation centre (see Subclause 6.2). ISO/IEC 11770-2 offers different mechanisms to establish keys between entities. ISO/IEC 11770-3 includes mechanisms for key agreement of secret keys and transport mechanisms for secret and public keys.

5.1.5 Install-Key

The service Install-Key is always needed before the use of a key. The installation of the key means the establishment of the key within a key management facility in a manner that protects it from compromise.

5.1.6 Store-Key

The service Store-Key provides secure storage of keys intended for current or near-term use or for back-up. It is usually advantageous to provide physically separate key storage. For example, it ensures confidentiality and integrity for keying material or integrity for public keys. Storage may occur in all key states (i.e. Pending Active, Active and Post Active) of a key's life cycle. Depending on the importance of the keys, they can be protected using one of the following mechanisms:

- physical security (e.g., by storing them within a tamper-resistant device or by external means such as diskette or memory card),
- encipherment with keys that are themselves protected by physical security, or
- protecting the access to them by password or PIN.

For all keying material, any attempted compromise should be detectable.

5.1.7 Derive-Key

The service Derive-Key forms a potentially large number of keys using a secret original key called the derivation key, non-secret variable data and a transformation process (which also need not be secret). The result of this process is the derived key. The derivation key needs special protection. The derivation process should be non-reversible and non-predictable to ensure that the compromise of a derived key does not disclose the derivation key or any other derived key.

5.1.8 Archive-Key

Key archiving provides a process for the secure, long-term storage of keys after normal use. It may use the service of key storage but allows for a different implementation such as off-line storage. Archived keys may need to be retrieved at a much later date to prove or disprove certain claims after normal use is discontinued.

5.1.9 Revoke-Key

When the compromise of a key is suspected or known the service Revoke-Key assures the secure deactivation of the key. This service is necessary for keys having reached their expiration date. Revocation of keys will also take place when a key owner's circumstances change. After a key is revoked it may only be used for decipherment and verification. The service Revoke-Key is not appropriate to certificate based schemes, where key life is controlled by expiry of the certificate.

NOTE: Some applications use the term delete-key for this service

5.1.10 Deregister-Key

The service Deregister-Key is a procedure provided by a key registration authority that removes the association of a key with an entity. It is part of the destruction process (see 5.1.11 Destroy-Key). When an entity wishes to deregister a key, the registration authority is contacted.

5.1.11 Destroy-Key

The service Destroy-Key provides a process for the secure destruction of keys that are no longer needed. Destroying a key means eliminating all records of this key management information object, such that no information remaining after the destruction provides any means of recovering the destroyed key. This is taken to include the destruction of all archived copies. However, before archived keys are destroyed a check must be carried out to ensure that no archived material protected by these keys will ever be needed again.

NOTE: Some keys may be stored outside an electronic device or system. Destruction of those keys requires additional administrative measures.

5.2 Support Services.

Other services may be needed to support key management.

5.2.1 Key Management Facility Services

Key management services may make use of other services that are security related. These services include:

access control This service may be used to ensure that the resources of a key management system can be accessed only by authorised entities in an authorised manner.

audit The tracking of security-relevant actions that appear in a key management system. Audit trails may help identify security risks and security leaks.

authentication This service should be used to establish an entity as an authorised member of a security domain.

cryptographic services These services should be used by key management services to provide integrity, confidentiality, authentication and non-repudiation.

time service This service is necessary for generating time variant parameters such as validity durations.

5.2.2 User-oriented Services

Cryptographic systems and devices may require other services that are necessary for adequate functionality, e.g., user registration services. These services are implementation specific and beyond the scope of this part of ISO/IEC 11770.

6 Conceptual Models for Key Distribution

The distribution of keys between entities can be complex. It is influenced by the nature of the communications links, the trust relationships involved and the cryptographic techniques used. The entities may either communicate directly or indirectly, may belong to the same or different security domains, and may or may not use the services of a trusted authority. The following conceptual models illustrate how these different cases influence the distribution of keys and information.

6.1 Key Distribution between Communicating Entities

Communication between entities is influenced by the link between these entities, the trust between these entities and the cryptographic techniques used.

There exists a connection between entities A and B, who wish to exchange information using cryptographic techniques. This communication connection is illustrated in Figure 3. Generally, key distribution must take place over a secure channel that is logically different from the traffic channel.

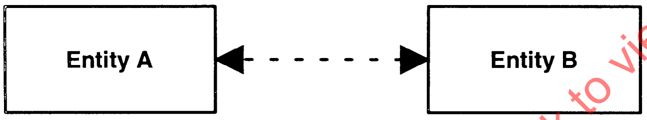

Figure 3 — Communications Link between Two Entities

Cases where direct communicating entities are involved are key agreement, key control and key confirmation. Further details of these cases are within Part 2 (ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*) and Part 3 (ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*) of ISO/IEC 11770.

6.2 Key Distribution within One Domain

The following model is based on the concept of a security domain with a security authority according to ISO/IEC 10181-1. This authority may offer key management services such as the translation of keys. When the entities use an asymmetric technique for the secure exchange of information, the following cases can be distinguished:

- For data integrity or data origin authentication, the recipient requires the sender's corresponding public key certificate.
- For confidentiality the sender requires a valid public key certificate of the recipient.
- For authentication, confidentiality, and integrity, each partner requires the public key certificate of the other. This provides the means for mutual non-repudiation.

Each entity may need to contact its authority to get an appropriate public key certificate. If the communicating partners trust each other and can mutually authenticate their public key certificates, then no authority is needed.

NOTE: There exist cryptographic applications where no authority is involved. In that situation the communicating partners may only securely exchange specific public information instead of their public key certificates.

When symmetric cryptography is in use between two such partners, key generation is initiated in one of two ways:

1. By one entity generating the key and sending it to a Key Translation Centre (KTC);
2. By one entity asking a Key Distribution Centre to generate a key for subsequent distribution.

If key generation is carried out by one of the entities, secure distribution of the key can be handled by a Key Translation Centre, as illustrated in Figure 4. The numbers represent the steps of the exchange. The KTC receives the enciphered key from entity A (1), deciphers it and re-enciphers it using the key shared between itself and entity B. Then it may

- either forward the enciphered key to entity B (2), or
- send it back to entity A (3), who forwards it to entity B (4).

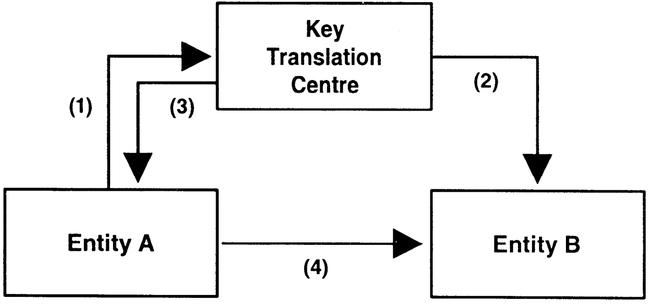

Figure 4 — Key Translation Centre

If key generation is carried out by a trusted third party, there are two options for subsequent distribution of the key to the communicating partners; these cases are illustrated in Figure 5 — Conceptual Model of a Key Distribution Centre — and Figure 6 — Key Distribution by Forwarding a Key from Entity A to Entity B.

Figure 5 illustrates the case in which the Key Distribution Centre is able to communicate securely with both entities. In this case, once a key has been generated at the request of one of the entities, the Key Distribution Centre is responsible for securely distributing the key to both entities. The request of the shared key is represented by (1) and the distribution of the key to the communicating partners by (2a) and (2b).

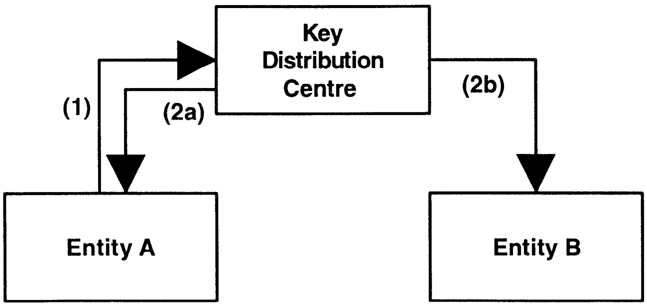

Figure 5 — Conceptual model of a Key Distribution Centre.

When only entity A asks for a secret key to be shared between entities A and B, the authority may act in two different ways. If it can securely communicate to both entities it may distribute the secret key to both of them as described above. If the authority can only communicate with entity A, entity A is responsible for distributing the key to entity B. Figure 6 illustrates this kind of key distribution. The request for a shared key is represented by (1) and the distribution to entity A by (2).The forwarding of this key from A to B is represented by (3).

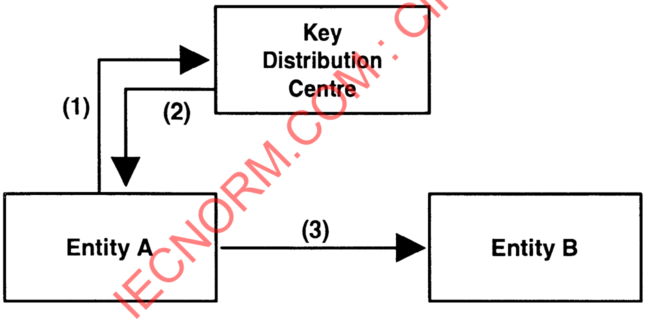

Figure 6 — Key Distribution by Forwarding a Key from an Entity A to Entity B

6.3 Key Distribution between Domains

The model here involves two entities named A and B belonging to two different security domains which share at least one cryptographic technique (i.e. symmetric or asymmetric). Each security domain has its own security authority: one trusted by A and one trusted by B. If A and B either trust each other or each trusts the authority of the other's domain, then keys are distributed according to Subclause 6.1 or 6.2.

Two cases can be distinguished for key establishment between A and B:

- the obtaining of the public key certificate of B (when applicable), and
- the establishment of a shared secret key between A and B.

Different key relationships are possible between these components. These key relationships reflect the nature of the trust between the components.

When the entities use an asymmetric technique for the exchange of information and do not have access to a common directory service that offers the public key certificates, each shall contact its respective authority to get its partner's public key certificate (see Figure 7 (1)). The authorities of A and B exchange the public key certificates of entities A and B (2) and forward them to A and B (3). Then A and B are able to communicate securely and directly (4).

A different approach for the exchange of public key certificates is cross-certification (see also Annex D).

When the entities communicate using a symmetric technique each entity also has to contact its respective authority securely (1) to receive a secret key that allows them to communicate. The authorities agree on a common secret key (2) to be used by the entities. One authority distributes the secret key to both entities using the other authority as a distribution centre. The latter authority may also provide key translation ((2) and (3)).

When only the entity A asks for a secret key for communication with entity B, the authority may act in two ways. If it can communicate to both entities it may distribute the secret key to both of them as described above. If the authority can only communicate with one entity, the entity receiving the key is responsible for forwarding the key to the other entity.

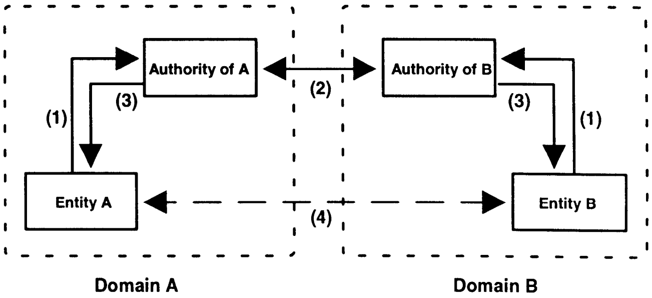

Figure 7 — Key Distribution between two Domains

Sometimes the authorities of A and B will have neither a mutual trust relationship nor a direct communications path. Then they shall involve an authority, X, whom they both trust as illustrated in Figure 8 (see arrows (2a) and (2b)). Authority X may generate a key and distribute it to the authorities of A and B (see arrows (3a) and (3b) in Figure 8). Alternatively, Authority X may forward a received secret key or public key certificate (for example (2a)) from the authority of A to the authority of B (3b). The authorities then have to forward the received key to their respective entities (see (4a) and (4b) in Figure 8) who may then exchange information securely (5). It may be necessary to seek successive authorities until a chain of trust is established.

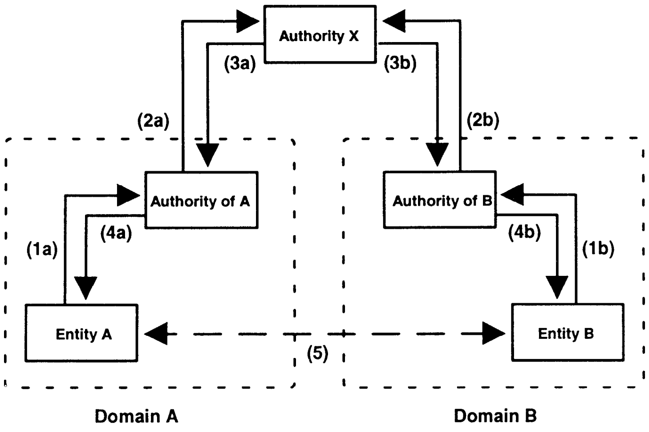

Figure 8 — Chain of Trust between Authorities

7 Specific Service Providers

Some of the services that a key management system requires may be provided by external service providers. Possible entities for services are:

- a Key Registration or Certification Authority,
- a Key Distribution Centre as defined in ISO/IEC 8732,
- a Key Translation Centre as defined in ISO/IEC 8732.

Annex A
(informative)

Threats to Key Management

Key management is susceptible to a number of threats. These include the following.

Disclosure of the keying material: Either the keying material is in plaintext, is not protected and can be accessed, or is enciphered and can be deciphered.

Modification of keying material: Changing the keying material so that it does not operate as intended.

Unauthorised deletion of keying material: Removal of the key or key related data.

Incomplete destruction of keying material: This may lead to the compromise of current or future keys.

Unauthorised revocation: The direct or indirect removal of a valid key or keying material.

Masquerade: The impersonation of an authorised user or entity.

Delay in executing key management functions: This may result in a failure to generate, distribute, revoke or register a key, a failure to update the key repository in a timely manner, in a failure to maintain a user's authorisation levels, and so on. The delay threat may result from any of the previously mentioned threats or from physical failure of the key related equipment.

Misuse of keys

- The use of a key for a purpose for which it is not authorised, e.g., the use of a key enciphering key for data encipherment.
- The use of a key management facility for a purpose for which it is not authorised, e.g., the unauthorised encipherment or decipherment of data.
- The use of a key after it has expired.
- Excessive use of a key.
- Provision of keys to an unauthorised recipient.

Annex B
(informative)

Key Management Information Objects

A key management information object consists of a key or keys, together with, optionally, other information that controls how the key(s) may be used. The control information may, rather than being explicit, be implied by conventions controlling the use of the key management information object. (For example, the use of one key of an asymmetric cipher pair is controlled by the agreed use of the other, one for encipherment and the other for decipherment.).

The control information may control the following:

- the type of object the key may protect (e.g., data or key management information object);
- valid operations (e.g., encipherment, decipherment);
- the allowed user;
- the environment in which the key may be used;
- other aspects particular to the specific control technique or application that uses the key management information object.

For the purposes of optimization the key management information object may be partially or wholly created within the key generation process.

A particular example of a key management information object is a key certificate. It contains at least the following signed by a certification authority:

- the keying material;
- the identity of the user who is able to use the corresponding key management information object;
- the operations which the corresponding key management information object performs (may be implicit);
- the period of validity;
- the identity of the certification authority.

The following ASN.1-definition is an example of a key management information object, although key management information objects may contain other, implementation specific parameters:

```
Key           ::=    PROTECTED   {KeyContents, protectionType};
KeyContents   ::=    SEQUENCE            {
                     keyID               [0]    Key_Identity,
                     keyValue            [1]    Key_Value,
                     checkValue          [2]    Check_Value,
                     cryptoMethod        [3]    Cryptographic_Method,
                     timeStamp           [4]    Time_Stamp,
                     generAuthority      [5]    Generating_Authority,
                     certiAuthority      [6]    Certification_Authority,
                     issuer              [7]    Issuer,
                     validity            [8]    Validity_of_Key};
```

It consists of the parameters Key_Identity (unambiguous identity), Key_Value (the value of the key) and Check_Value (a check sum to ensure integrity of the key) where only the Key_Value is mandatory. The parameters Cryptographic_Method, Issuer and Validity_of_Key control the use of the key in restricting it to specific algorithms for a limited time and a specific user. These parameters are important for the control of a key's use, but are optional. The parameters Generating_Authority, Certification_Authority and Time_Stamp are important for the proof of a key's origin and its age, but are also optional. For a key certificate the parameter Issuer is mandatory.

Annex C
(informative)
Classes of Cryptographic Applications

The common classification of cryptographic systems is defined by the two principal cryptographic techniques used, i.e. symmetric and asymmetric. Because key management must cater for both techniques another approach is needed. Therefore the following section classifies cryptographic systems according to the functionality provided by the technique.

In general, a cryptographic system offers two different types of cryptographic service: authentication services and encipherment services. Encipherment services are used to cryptographically protect information; i.e., they provide data confidentiality. Authentication services are primarily used for entity authentication, data origin authentication, data integrity and non-repudiation. The types of cryptographic systems and the corresponding operations are demonstrated in Figure C-1.

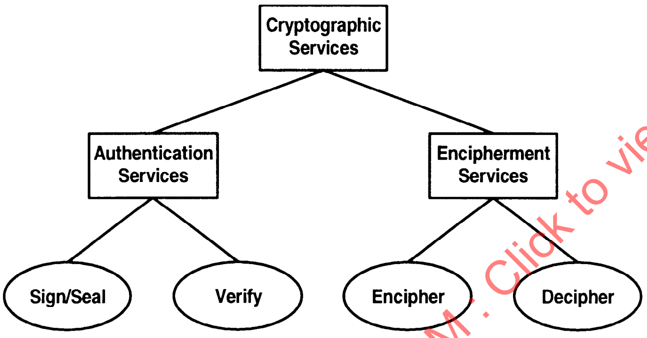

Figure C-1 — Cryptographic Services and Corresponding Mechanisms

C.1 Authentication Services and Keys

Authentication services provide for the authentication of communicating entities (entity authentication), for the authentication of the source of data (data origin authentication), for non-repudiation, and for data integrity. This service may make use of the following mechanisms:

seal a data unit which involves the production of a cryptographic check value of the data for data integrity, e.g., generate a message authentication code (MAC) with a symmetric algorithm.

sign a data unit which involves the generation of a digital signature for data origin authentication, data integrity and/or non-repudiation.

verify a sealed data unit which involves calculating a cryptographic check value of the data and comparing it with the referenced check value (proof of data integrity).

verify a signed data unit which involves the verification of a digital signature to determine whether it was produced by the claimed originator and/or the proof of data integrity.

Within the authentication service the signing and the sealing processes use information which is either private (i.e. unique and confidential) to the originator or secret and only known by the originator and the recipient; the verifying process uses either procedures and information that are publicly available but from which the originator's private information cannot be deduced or the shared secret of the originator and the recipient. The essential characteristic of signing is that the signature can only be produced using the originator's private information, his *private key.* Thus when the signature is verified by using the originator's *public key*, it can subsequently be proven to a third party (e.g., a notarisation authority) that only the unique holder of the private information could have produced the signature.

An authentication service uses two out of three types of keys:

sealing key a shared, *secret* key.

signature key a unique, *private* key that is associated with the originator.

verification key either a *public key* or a *secret key.*

For symmetric techniques an authentication service uses a sealing key and a verification key which are represented by the same secret key, for asymmetric techniques it uses the signature key and the verification key which are represented by a key pair consisting of a public and a private key.

C.2 Encipherment Services and Keys

Encipherment services primarily provide confidentiality of information but also data integrity. Depending on the technique used security services such as authentication and non-repudiation might be included. It makes use of two basic mechanisms:

encipher	which produces ciphertext from the data it is given;
decipher	which produces plaintext from the corresponding ciphertext.

An encipherment service may be characterised by the cryptographic technique used, i.e., symmetric or asymmetric. When using symmetric techniques the operations encipher and decipher are handled by the same key (shared secret key). When using asymmetric techniques the operations encipher and decipher are handled by two distinct but related keys, i.e., the public and the private key.

Annex D
(informative)
Certificate Lifecycle Management

This informative Annex describes the requirements and procedures as they apply to the management of the public key certificate lifecycle.

D.1 The Certification Authority

The CA is "trusted" by its subscribers. Such trust is based on the use of adequate cryptographic mechanisms and equipment, and on professional management and control practices. This trust shall be confirmed by an independent audit function (internal, external or both) which shall make the audit results available to subscribers.

The CA shall be responsible for:

1. Identifying the entities whose public key information is presented for certification.
2. Ensuring the quality of the asymmetric key pair used to produce public key certificates.
3. Securing the certification process and the private key used to sign the public key information.
4. Managing the system-specific data that are to be included into the public key information, such as public key certificate serial number, certification authority identification, etc.
5. Assigning and checking of validity periods.
6. Advising the entity identified in the public key information that a public key certificate has been issued. The means used to convey this advice shall be independent of the method used to convey the public key information to the CA.
7. Ensuring that two different entities are not assigned the same identity, so that they can be properly distinguished.
8. Maintaining and issuing of revocation lists.
9. Logging all steps involved in the public key certificate generation process.

One CA can certify another CA's public key information to provide a public key certificate. Hence, authentication may involve a chain of public key certificates. The first public key certificate in such a chain shall be obtained and authenticated by some means other than with public key certificates.

D.1.1 The CA's Asymmetric Key Pair

The CA shall have a secure key management facility that is able to generate the asymmetric key pair for use by that CA. The generation process shall ensure the unpredictability of the keying material. No opponent shall gain any advantage by knowledge of the generation process.

The CA's private key is used to sign the entity's public key information. Since its possession would enable an opponent to masquerade as the CA and generate forged public key certificates, it shall be given a high level of protection. Thus, the CA's private key shall be well protected when used inside the key management facility. It shall enter or leave the key management facility in a protected way and under the control of the CA itself.

The integrity of the CA's public verification key is essential to the security of the public key certificate system. If the CA's public key is not contained in a public key certificate, then special precautions shall be taken to ensure its authenticated distribution. At the user sites provision shall be taken to ensure the authenticity of the stored copy of the CA's public key.

The CA's public verification key is used to validate the public key certificates of other users. Before each use of the CA's public key, the user shall assure that the verification key is currently valid.

D.2 The Certification Process

This Clause describes requirements and procedures as they apply to the certification process.

D.2.1 Model for Public Key Certification

This Clause specifies a basic model for the certification of public keys. The model separates the main functions into logical entities (see Figure D-1):

1. Certification authority (CA): the entity responsible for certifying the public key information of a user entity.
2. Directory (DIR): the entity responsible for making the public key certificates available online for ready use by the user entities.
3. Key Generator (KG): the entity responsible for the generation of an asymmetric key pair.