INTERNATIONAL STANDARD

ISO/IEC 11770-1

Second edition
2010-12-01

Information technology — Security techniques — Key management —

Part 1: Framework

Technologies de l'information — Techniques de sécurité — Gestion de clés —

Partie 1: Cadre général

Reference number
ISO/IEC 11770-1:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

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) 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

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

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

This second edition cancels and replaces the first edition (ISO/IEC 11770-1:1996), which has been technically revised.

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*

— *Part 4: Mechanisms based on weak secrets*

The following part is under preparation:

— *Part 5: Group key management*

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.

This part of ISO/IEC 11770 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.

This part of ISO/IEC 11770 contains the material required for a basic understanding of subsequent parts.

Examples of the use of key management mechanisms are included in ISO 11568. If non-repudiation is required for key management, ISO/IEC 13888 is applicable.

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 might 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 ISO/IEC 11770.

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 ISO/IEC 11770 has a special relationship to the security frameworks for open systems (ISO/IEC 10181). All the frameworks, including this one, identify the basic concepts and characteristics of mechanisms covering different aspects of security.

Information technology — Security techniques — Key management —

Part 1:
Framework

1 Scope

This part of ISO/IEC 11770

a) establishes the general model on which key management mechanisms are based,

b) defines the basic concepts of key management which are common to all the parts of ISO/IEC 11770,

c) specifies the characteristics of key management services,

d) establishes general principles on the management of keying material during its life cycle, and

e) establishes the conceptual model of key distribution.

2 Terms and definitions

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

2.1
asymmetric cryptographic technique
cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key)

NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

2.2
asymmetric key pair
pair of related keys where the private key defines the private transformation and the public key defines the public transformation

[ISO/IEC 11770-3:2008]

2.3
certification authority
entity trusted to create and assign public key certificates

2.4
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2:1989]

2.5
data origin authentication
corroboration that the source of data received is as claimed

[ISO 7498-2:1989]

2.6
decryption
reversal of a corresponding encryption

NOTE Decryption [ISO/IEC 18033-1] and decipherment [ISO/IEC 9798-1] are equivalent terms.

2.7
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[ISO/IEC 9798-1:1997]

2.8
directory maintenance authority
entity responsible for making the public key certificates available online for ready use by the user entities

2.9
distinguishing identifier
information which unambiguously distinguishes an entity

2.10
encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data

NOTE Encryption [ISO/IEC 18033-1] and encipherment [ISO/IEC 9798-1] are equivalent terms.

2.11
entity authentication
corroboration that an entity is the one claimed

[ISO/IEC 9798-1:1997]

2.12
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g., encryption, decryption, cryptographic check function computation, signature generation, or signature verification)

2.13
key agreement
process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key

2.14
key archiving
service which provides a secure, long-term storage of keys after normal use

2.15
key certification
service which assures the association of a public key with an entity

2.16
key confirmation
assurance for one entity that another identified entity is in possession of the correct key

2.17
key control
ability to choose the key, or the parameters used in the key computation

2.18
key deregistration
procedure provided by a key registration authority that removes the association of a key with an entity

2.19
key derivation
service which forms a potentially large number of keys using a secret original key called the derivation key, non-secret variable data and a secure transformation process

2.20
key destruction
service for the secure destruction of keys that are no longer needed

2.21
key distribution
service which securely provides key management information objects to authorized entities

2.22
key distribution centre
entity that is trusted to generate or acquire keys and to distribute the keys to communicating parties and that shares a unique symmetric key with each of the parties

2.23
key establishment
process of making available a shared key to one or more entities, where the process includes key agreement or key transport

[ISO/IEC 11770-3:2008]

2.24
key generation
process of generating a key

2.25
key generator
entity responsible for generation of an asymmetric key pair

2.26
key installation
service which securely establishes a key within a key management facility in a manner that protects it from compromise

2.27
keying material
data necessary to establish and maintain cryptographic keying relationships

EXAMPLES Keys, initialization values.

2.28
key management
administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

2.29
key registration
service which associates a key with an entity

2.30
key revocation
service which assures the secure deactivation of a key

2.31
key storage
service which provides secure storage of keys intended for current or near-term use or for backup

2.32
key translation centre
entity trusted to decrypt a key that was generated and encrypted by one party and re-encrypt it for another party

2.33
key transport
process of transferring a key from one entity to another entity, suitably protected

[ISO/IEC 11770-3:2008]

2.34
personal identification number
secret number sequence used for entity authentication, which is a memorized weak secret

2.35
private key
key of an entity's asymmetric key pair that is kept private

NOTE The security of an asymmetric system depends on the privacy of this key.

2.36
public key
key of an entity’s asymmetric key pair which can usually be made public without compromising security

2.37
public key certificate
public key information of an entity signed by the certification authority

2.38
public key information
information containing at least the entity’s distinguishing identifier and public key, but which can include other static information regarding the certification authority, the entity, restrictions on key usage, the validity period, or the involved algorithms

[ISO/IEC 11770-3:2008]

2.39
random number
random bit
time variant parameter whose value is unpredictable

2.40
registration authority
entity responsible for providing assured user identities to the certification authority

2.41
secret key
key used with symmetric cryptographic techniques and usable only by a set of specified entities

2.42
security authority
entity that is responsible for the definition, implementation or enforcement of security policy

[ISO/IEC 10181-1:1996]

2.43
security domain
set of elements, security policy, security authority and set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain

[ISO/IEC 10181-1:1996]

2.44
sequence number
time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

2.45
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation

NOTE Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

2.46
time stamp
data item which denotes a point in time with respect to a common time reference

[ISO/IEC 11770-3:2008]

2.47
time variant parameter
data item such as a random number, a sequence number, or a time stamp

[ISO/IEC 11770-3: 2008]

2.48
trusted third party
security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy)

[ISO/IEC 10181-1:1996]

3 Symbols and abbreviated terms

3.1 Symbols

A, B	distinguishing identifiers of entities
CA	Certification Authority
DIR	Directory Maintenance Authority
KDC	Key Distribution Centre
KG	Key Generator
KTC	Key Translation Centre
RA	Registration Authority
S_A	Signature key of entity A
V_A	Verification key of entity A
X	distinguishing identifier of authority

3.2 Abbreviated terms

CA	Certification Authority
MAC	Message Authentication Code
PIN	Personal Identification Number
RA	Registration Authority
TTP	Trusted Third Party
TVP	Time Variant Parameter

4 General model of key management

4.1 General

The objective of key management is the secure administration and use of 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 devices.

4.2 Protection of keys

4.2.1 General aspects of key management

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. More than one of the following protection techniques may be required to protect against these threats. 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 for key encryption to encrypt data.

4.2.2 Protection by cryptographic techniques

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

For encryption algorithm standards, refer to ISO/IEC 18033. For data integrity mechanisms, refer to ISO/IEC 9796, ISO/IEC 9797, ISO/IEC 10118 and ISO/IEC 14888. For digital signatures, refer to ISO/IEC 9796 and ISO/IEC 14888. For entity authentication mechanisms, refer to ISO/IEC 9798.

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 encryption, data integrity); key control is required for non-repudiation using symmetric techniques. For non-repudiation using symmetric techniques, refer to ISO/IEC 13888-2.

4.2.3 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. For time stamps, refer to ISO/IEC 18014.

4.2.4 Protection by physical means

A cryptographic device within a secure system will typically need 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,
- interact with cryptographic algorithms implemented in separate security facilities (for example, smart cards), or
- store keying material off-line (for example, on memory cards).

Secure areas are typically protected by physical security mechanisms. Physical security mechanisms may include passive mechanisms preventing direct access to the secure area as well as active tamper detection mechanisms that destroy key material in the event of possible intrusion to the secure area. The physical security mechanisms employed will depend on the strategic value of the secured keys over time. Security protection for cryptographic devices is standardized in ISO/IEC 19790.

4.2.5 Protection by organisational means

One means of protecting keys is to organise them into a key hierarchy. 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 effect of the compromise of a single session key is limited to compromising only the information protected by that key.

Allowing people to have access to keys can cause significant problems in terms of being able to prevent disclosure and (particularly for non-repudiation) to prove that the key can not have been misused. Keys should only be available in plaintext when inside secure devices. If they shall be exported, then special measures should be used such as dividing the key into components and not allowing one person to access all components.

Use of a key shall also be controlled, to prevent its use in a manner that might divulge the key or the data it protects.

4.3 Generic key life cycle model

4.3.1 Key life cycle definitions

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 data cryptographically, or to decrypt or verify processed data.

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

A key that is known to be compromised shall become Post Active immediately and shall not be trusted for any other purpose than decrypting or verifying data that was processed prior to the compromise. In particular, a compromised key shall not be reactivated.

A key is said to be compromised when it has been determined to have been subjected to unauthorized access or control.

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 sub-states 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.

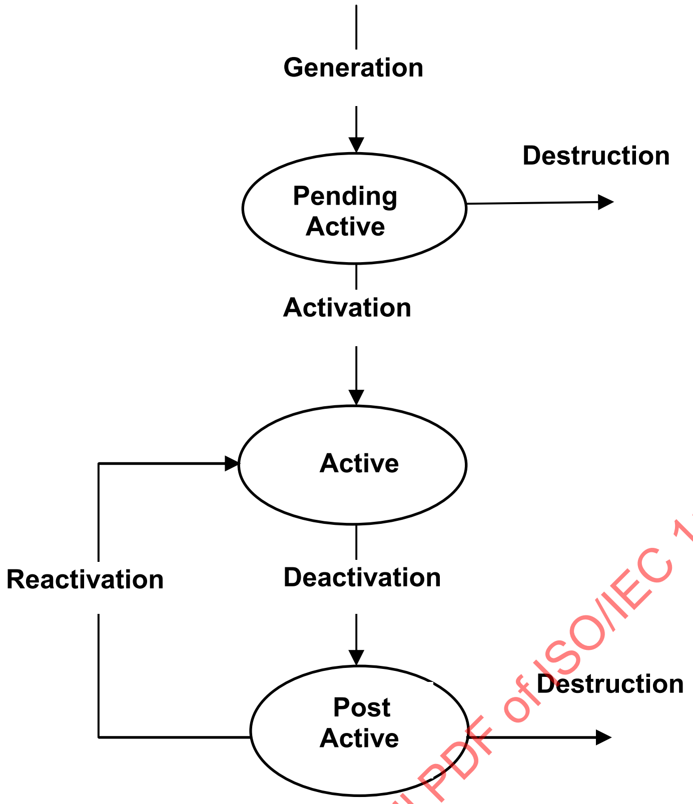

Figure 1 — Key life cycle

4.3.2 Transitions between key states

When a key progresses from one state to another, it undergoes one of the following transitions, as 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. It should be noted that during key generation a source of unpredictable random numbers is of the utmost importance, otherwise even the strongest algorithms cannot provide adequate protection. For guidance on random number generation, refer to ISO/IEC 18031.

- **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 expiry of a key, and the completion of the key life cycle. All these transitions include a number of services for key management.

4.3.3 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 expiry. 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 data signed with his private key he may add his certificate. The key pair becomes active when the public key is certified. When a key 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 expiry date of the associated private key. When asymmetric techniques are used to implement confidentiality services and the key used for encryption has been deactivated or destroyed, the corresponding key of the pair may remain in the Active or Post Active state for later decryption.

Therefore, for signature keys the public part of the key will remain in the Active or Post Active state and for encryption keys the private part of the key will remain in the Active or Post Active state.

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 Basic concepts of key management

5.1 Key management services

5.1.1 Summary of key management services

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.

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 shall fulfill 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 (TTP). Figure 2 shows that the key management 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.

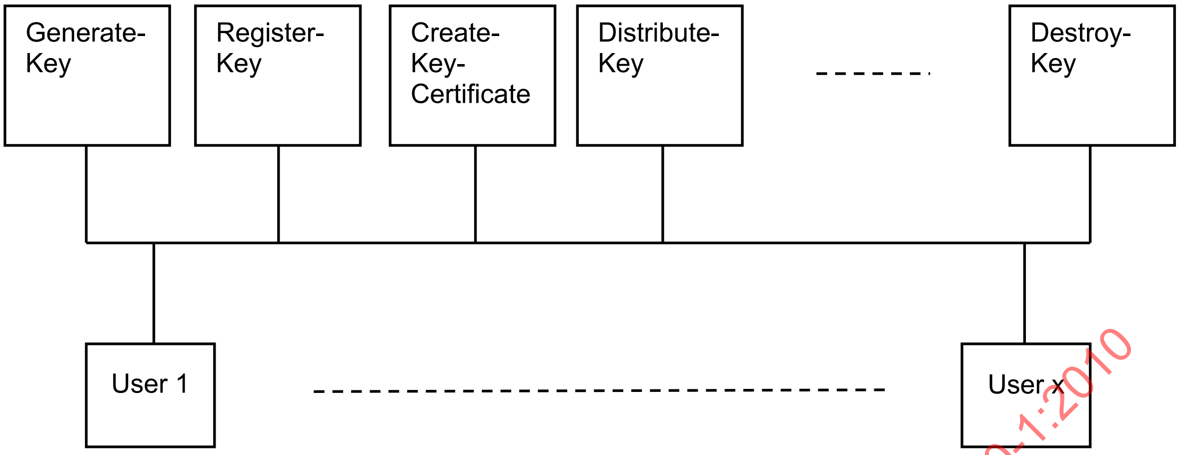

Figure 2 — Key management services

The relationships between the transitions and the services are shown in Table 1. These services are explained below. Any particular cryptographic approach will only require a subset of the services offered in Table 1.

Table 1 — Transitions and services

Transitions (Refer to Figure 1)	**Services**	**Notes**
Generation	Generate-Key	Mandatory
	Derive-Key	Optional
	Register-Key	Optional either in here or in 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 in here or in Generation
Deactivation	Store-Key	Optional
	Archive-Key	Optional either in here or in 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 in here or in Deactivation

5.1.2 Generate-Key (key generation)

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.

Key generation always involves random number generators. It is essential that random number generators not only generate random numbers that are unpredictable, but also that they generate random numbers that will span the entire key space of the algorithm in a uniform way. For instance, if a random number generator input into key generation routines effectively only generates 32 bits of entropy while it generates keys for a 128-bit symmetrical algorithm, the key generation process is flawed. For guidance on random number generation, refer to ISO/IEC 18031.

5.1.3 Register-Key (key registration)

The service Register-Key associates a key with an entity. It is provided by a registration authority, and is usually applied when asymmetric 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.

5.1.4 Create-Key-Certificate (key certification)

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.

5.1.5 Distribute-Key (key distribution)

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 6.3). 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.

5.1.6 Install-Key (key installation)

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. In the minimum case, the only function of Install-Key is to mark the key as 'in use'.

5.1.7 Store-key (key storage)

The service Store-Key provides secure storage of keys intended for current or near-term use or for backup. 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 a memory card),
- encryption 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. Generally it is difficult to detect attempted key compromise when protection is purely based on a password / PIN stored in software. In such a case the protected keys can be copied and password / PIN cracking can take place offline which is virtually impossible to detect. For such cases other procedural security measures shall be considered, depending on the application.

5.1.8 Derive-Key (key derivation)

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.

5.1.9 Archive-Key (key archiving)

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 has been discontinued.

5.1.10 Revoke-Key (key revocation)

When the compromise of a key is suspected or known, the service Revoke-Key assures the secure deactivation of the key. This service is also necessary for keys having reached their expiry date. Revocation of keys may also take place when a key owner’s circumstances change. After a key is revoked it shall only be used for decryption and verification. In the case of a key being revoked because of compromise, only data processed prior to the compromise may be decrypted or verified.

NOTE Some applications use the term Delete-Key for this service.

5.1.11 Deregister-Key (key deregistration)

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 5.1.12 Destroy-Key).

5.1.12 Destroy-Key (key destruction)

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 shall be carried out to ensure that no archived material protected by these keys will ever be needed again.

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

5.2 Support services

5.2.1 Key management facility services

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

- **Access control**

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

- **Audit**

  This service is for tracking of security-relevant actions that appear in a key management system. Audit trails can help identify security risks and security leaks.

- **Authentication**

  This service is to establish an entity as an authorised member of a security domain.

- **Cryptographic services**

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

- **Time service**

  This service is for generating time variant parameters (TVPs) such as validity durations.

5.2.2 User-oriented services

There are 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 for two entities

6.1 Introduction to 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.

6.2 Key distribution between two 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.

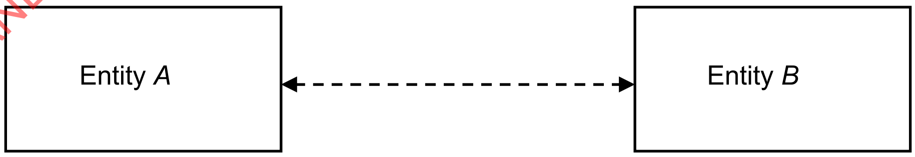

Figure 3 — Communications link between two entities

Cases where direct communicating entities are involved are key agreement, key control and key confirmation.

6.3 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.

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:

a) By one entity generating the key and sending it to a Key Translation Centre (*KTC*);

b) By one entity asking a Key Distribution Centre (*KDC*) 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 encrypted key from entity *A* (1), decrypts it and re-encrypts it using the key shared between itself and entity *B*. Then it may

— either forward the encrypted key to entity *B* (2), or

— send it back to entity *A* (3), who forwards it to entity *B* (4).

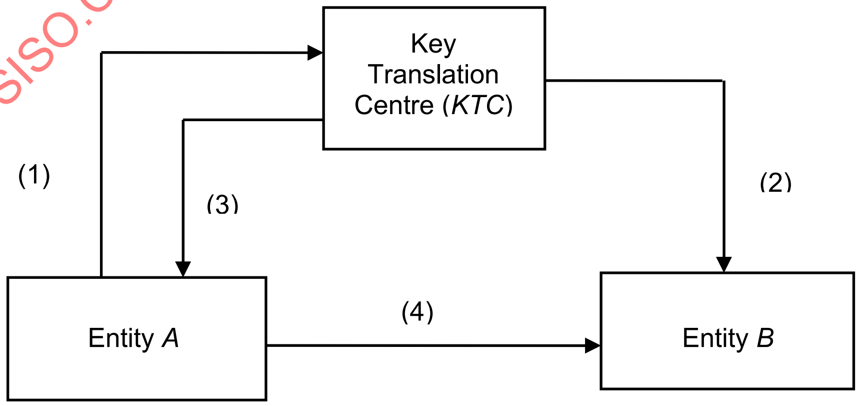

Figure 4 — Key Translation Centre

If key generation is carried out by a trusted third party (TTP), 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 (*KDC*) — 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 (1) and the distribution of the key to the communicating partners (2a) and (2b).

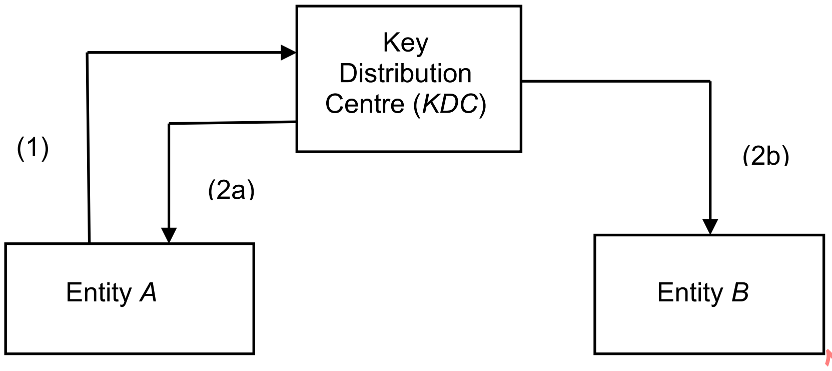

Figure 5 — Conceptual model of a Key Distribution Centre

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 (1) and the distribution to entity *A* (2).The forwarding of this key from *A* to *B* is represented (3).

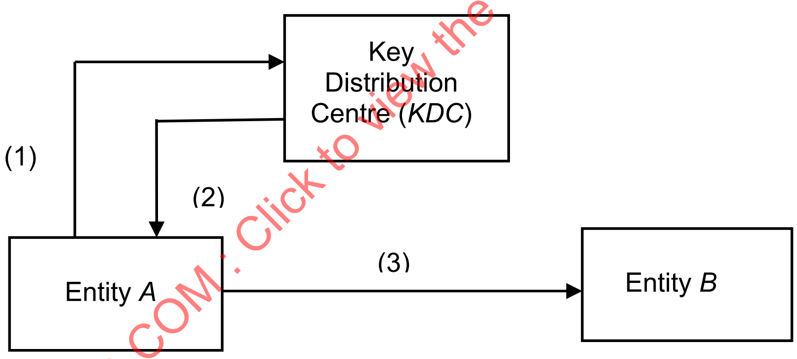

Figure 6 — Key distribution by forwarding a key from entity *A* to entity *B*

6.4 Key distribution between two 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). See Figure 7 for asymmetric case and Figure 8 for symmetric case. 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 6.2 or 6.3.

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, each needs access to the other's certificate (See Figure 7). When entity *A*'s authority issues a certificate for *A* (2) according to *A*'s request (1), that certificate is generally posted to a directory, either by *A* (3) or its authority (3'). The directory may be open, in which case *B* may obtain the *A*'s certificate directly from *A*'s directory (7). If both authorities of *A* and *B* have a cross-posting agreement (8), *B* may find *A*'s certificate in its own directory (10). Failing that, *A* will send its own certificate to *B* along with the exchange, or as part of a key establishment protocol (11).

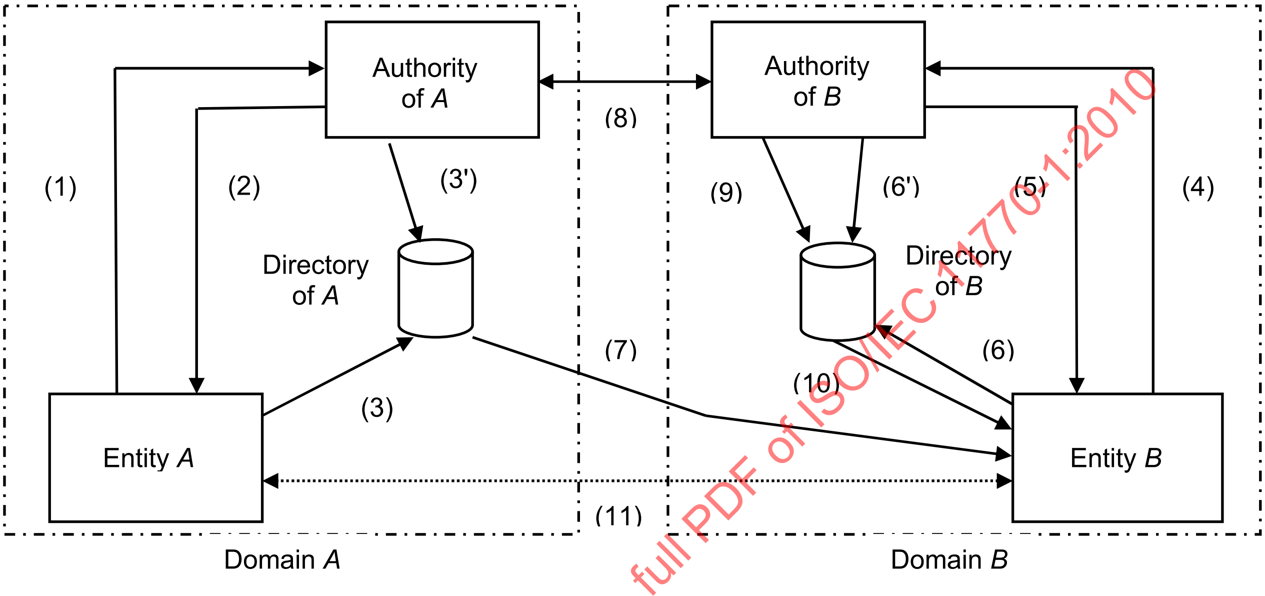

Figure 7 — Key distribution between two domains using asymmetric techniques

When the entities communicate using a symmetric technique each entity also has to contact its respective authority securely (1) (see Figure 8) 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.

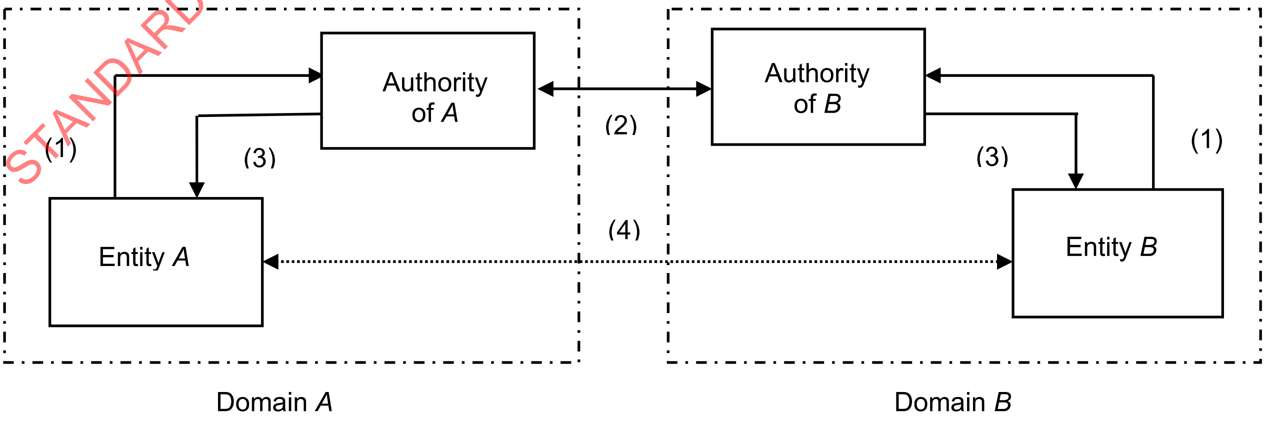

Figure 8 — Key distribution between two domains using symmetric techniques

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 9 [see (2a) and (2b)]. Authority *X* may generate a key and distribute it to the authorities of *A* and *B* in Figure 9 [see (3a) and (3b) in Figure 9]. 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 9] who may then exchange information securely (5). It may be necessary to seek successive authorities until a chain of trust is established.

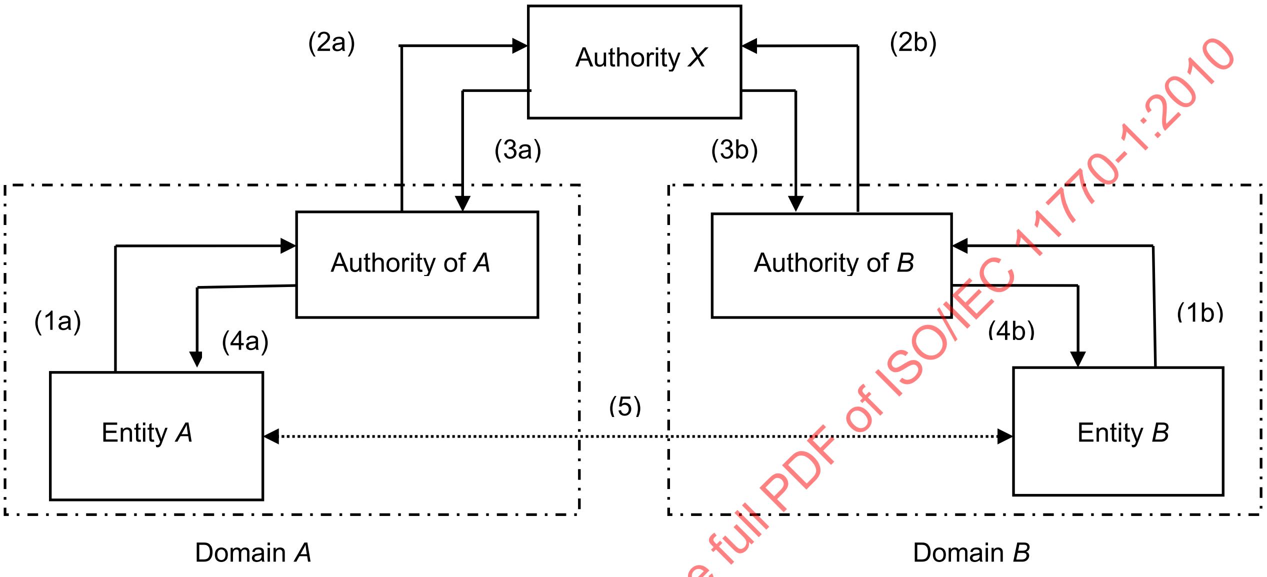

Figure 9 — Chain of trust between authorities

7 Specific service providers

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

- a Key Registration Authority or a Key Certification Authority
- a Key Distribution Centre
- a Key Translation Centre

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 encrypted and can be decrypted.

- **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 encrypting key for data encryption.
  - The use of a key management facility for a purpose for which it is not authorised, e.g., the unauthorised encryption or decryption 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 key pair is controlled by the agreed use of the other, one for encryption and the other for decryption.).

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., encryption, decryption);
- the authorised 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 optimisation 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 public 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.

Annex C
(informative)

Classes of cryptographic applications

C.1 Common classification of cryptographic systems

The common classification of cryptographic systems is defined by the two principal cryptographic techniques used, i.e. symmetric and asymmetric. Because key management should 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 services: integrity and authenticity services and confidentiality services. Confidentiality services are used to cryptographically protect information; i.e., they provide data confidentiality. Integrity and authenticity 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.

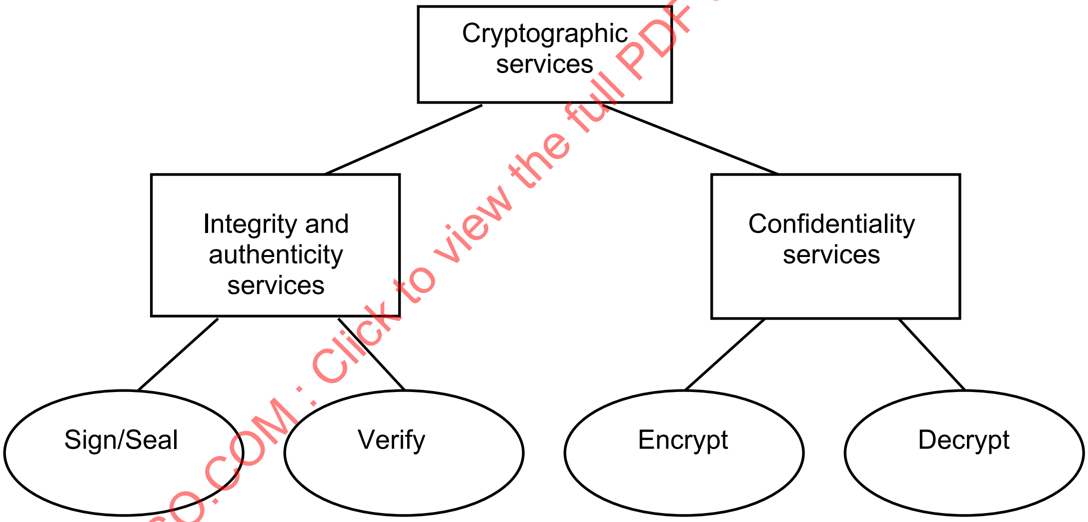

Figure C.1 — Cryptographic services and corresponding mechanisms

C.2 Integrity and authenticity services and keys

Integrity and authenticity 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. These services 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. For message authentication codes (MACs), refer to ISO/IEC 9797.

- **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 integrity and authenticity services 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 integrity and authenticity services use 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, integrity and authenticity services use 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 key* and a *private key*.

C.3 Confidentiality services and keys

Confidentiality services primarily provide confidentiality of information. They make use of two basic mechanisms:

encrypt which produces ciphertext from the data it is given;

decrypt which produces plaintext from the corresponding ciphertext.

Confidentiality services may be characterised by the cryptographic technique used, i.e. symmetric or asymmetric. When using symmetric techniques the operations of encryption and decryption are handled by the same key (shared *secret key*). When using asymmetric techniques, the operations of encryption and decryption are handled by two distinct but related keys, i.e., the *public key* and the *private key*.

C.4 Combined services

Some encryption schemes may also provide confidentiality, data integrity and/or origin authentication. In particular, the authenticated encryption schemes described in ISO/IEC 19772 and the MULTI-SO1 mode of operation of a stream cipher described in ISO/IEC 18033-4 provide confidentiality, data integrity and origin authentication using symmetric cryptographic techniques. The signcryption schemes described in ISO/IEC 29150 provide confidentiality, data integrity and origin authentication using asymmetric cryptographic techniques. Depending on the technique used, security functions such as authentication and non-repudiation might be included.

Annex D
(informative)

Certificate lifecycle management

D.1 General

Where a Certification Authority is used, applications of the following requirements and procedures as they apply to the management of the public key certificate lifecycle are recommended.

D.2 Certification Authority (CA)

D.2.1 CA's responsibilities

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 should be confirmed by an independent audit function (internal, external or both) which should make the audit results available to subscribers.

The CA should be responsible for:

a) Identifying the entities whose public key information is presented for certification.

b) Securing the certification process and the private key used to sign the public key information.

c) 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.

d) Assigning and checking of validity periods.

e) Advising the entity identified in the public key information that a public key certificate has been issued. The means used to convey this advice should be independent of the method used to convey the public key information to the CA.

f) Ensuring that two different entities are not assigned the same identity so that they can be properly distinguished.

g) Maintaining and issuing of revocation lists.

h) 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 should be obtained and authenticated by some means other than with public key certificates.

D.2.2 CA’s asymmetric key pair

The CA should have access to a secure management facility that is able to generate the asymmetric key pair for use by that CA. The generation process should ensure the unpredictability of the keying material. No opponent should 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 should be given a high level of protection. Thus, the CA’s private key should be well protected when used inside the key management facility. The key should be strongly protected if it appears outside the key management facility.

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 should be taken to ensure its authenticated distribution. At the user sites provision should 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 should ensure that the verification key is currently valid.

D.3 Certification process

D.3.1 Model for public key certification

D.3.1.1 Basic model

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

- **Certification Authority (*CA*):**

  The entity responsible for certifying the public key information of a user entity.

- **Directory Maintenance Authority (*DIR*):**

  The entity responsible for making the public key certificates available online for ready use by the user entities.

- **Key Generator (*KG*):**

  The entity responsible for generation of an asymmetric key pair.

- **Registration Authority (*RA*):**

  The entity responsible for providing assured user identities to the *CA*.

- **User entity (*A*):**

  The relations between the logical entities of the model and the corresponding security requirements on these relations are discussed. The logical entities may be combined. For example, *A* and the *KG* may be combined when the user entity generates the asymmetric key pair itself, or the *CA* and the *KG* may be combined if the *CA* generates the key pairs on behalf of the user entities.

Care should be taken that a certificate generated by a combined *RA* and *CA* is the same as one produced by an *RA* and *CA* that are separate and distinct.