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)

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

Published in Switzerland

Contents

Page

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 decipherment [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.