

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)



This is a preview of "ISO/IEC 11770-1:2010". [Click here to purchase the full version from the ANSI store.](#)

**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/IEC 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO/IEC 11770-1:2010". Click here to purchase the full version from the ANSI store.

## Contents

Page

Foreword .....	iv
Introduction.....	v
1 Scope.....	1
2 Terms and definitions .....	1
3 Symbols and abbreviated terms .....	6
3.1 Symbols.....	6
3.2 Abbreviated terms .....	6
4 General model of key management.....	6
4.1 General .....	6
4.2 Protection of keys .....	7
4.2.1 General aspects of key management .....	7
4.2.2 Protection by cryptographic techniques .....	7
4.2.3 Protection by non-cryptographic techniques.....	7
4.2.4 Protection by physical means.....	7
4.2.5 Protection by organisational means .....	8
4.3 Generic key life cycle model .....	8
4.3.1 Key life cycle definitions.....	8
4.3.2 Transitions between key states .....	9
4.3.3 Transitions, services and keys .....	10
5 Basic concepts of key management .....	10
5.1 Key management services .....	10
5.1.1 Summary of key management services .....	10
5.1.2 Generate-Key (key generation) .....	12
5.1.3 Register-Key (key registration) .....	12
5.1.4 Create-Key-Certificate (key certification).....	12
5.1.5 Distribute-Key (key distribution).....	12
5.1.6 Install-Key (key installation).....	12
5.1.7 Store-key (key storage).....	12
5.1.8 Derive-Key (key derivation) .....	13
5.1.9 Archive-Key (key archiving) .....	13
5.1.10 Revoke-Key (key revocation) .....	13
5.1.11 Deregister-Key (key deregistration) .....	13
5.1.12 Destroy-Key (key destruction) .....	13
5.2 Support services .....	13
5.2.1 Key management facility services.....	13
5.2.2 User-oriented services.....	14
6 Conceptual models for key distribution for two entities.....	14
6.1 Introduction to key distribution .....	14
6.2 Key distribution between two communicating entities .....	14
6.3 Key distribution within one domain .....	15
6.4 Key distribution between two domains.....	16
7 Specific service providers.....	18
Annex A (informative) Threats to key management .....	19
Annex B (informative) Key management information objects .....	20
Annex C (informative) Classes of cryptographic applications.....	21
Annex D (informative) Certificate lifecycle management.....	23
Bibliography.....	30

## 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*

This is a preview of "ISO/IEC 11770-1:2010". [Click here to purchase the full version from the ANSI store.](#)

## 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.