
**Information technology — Security
techniques — Key management —**

**Part 5:
Group key management**

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

Partie 5: Gestion de clés de groupe



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviations	4
5 Requirements	5
6 Tree based key establishment mechanisms for multiple entities	5
6.1 General model.....	5
6.2 Joining process	6
6.3 Leaving process	6
6.4 Rekeying process.....	6
6.5 Logical key structure	7
6.6 Symmetric key based key establishment mechanisms	8
7 Key chain based group key management	12
8 Key chain based group key management with unlimited forward key chain	13
8.1 Calculations by the key distribution centre.....	13
8.2 Calculations by the client entity	15
9 Key chain based group key management with limited forward key chain	18
9.1 Calculations by the key distribution centre.....	18
9.2 Calculations by the client entity	19
Annex A (normative) Object identifiers	20
Annex B (informative) Load balancing mechanism for general tree based structure	21
Bibliography	22

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 11770-5 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*
- *Part 4: Mechanisms based on weak secrets*
- *Part 5: Group key management*

Introduction

This part of ISO/IEC 11770 does not specify the means to be used to establish initial secret keys; that is, all the mechanisms specified in this part of ISO/IEC 11770 require an entity to share the secret key with another entity, the key distribution centre (KDC). For general guidance on the key lifecycle see ISO/IEC 11770-1. This part of ISO/IEC 11770 does not explicitly address the issue of interdomain key management. This part of ISO/IEC 11770 also does not define the implementation of key establishment mechanisms; products complying with this part of ISO/IEC 11770 might be compatible.

This part of ISO/IEC 11770 does not specify the information which has no relation with key establishment mechanisms, nor does it specify other messages such as error messages. The explicit format of messages is not within the scope of this part of ISO/IEC 11770.

The mechanisms specified in this part of ISO/IEC 11770 have been assigned object identifiers in accordance with ISO/IEC 9834. The list of assigned object identifiers is given in the normative Annex A. Any change to the specification of the mechanisms resulting in a change of functional behavior will result in a change of the object identifier assigned to the mechanisms.

Information technology — Security techniques — Key management —

Part 5: Group key management

1 Scope

This part of ISO/IEC 11770 specifies key establishment mechanisms for multiple entities to provide procedures for handling cryptographic keying material used in symmetric or asymmetric cryptographic algorithms according to the security policy in force.

It defines symmetric key based key establishment mechanisms for multiple entities with a key distribution centre (KDC), and defines symmetric key establishment mechanisms based on a general tree based structure with both individual rekeying and batched rekeying. It also defines key establishment mechanisms based on a key chain with both unlimited forward key chain and limited forward key chain. The two types of key establishment mechanisms can be combined by applications.

This part of ISO/IEC 11770 also describes the required content of messages which carry keying material or are necessary to set up the conditions under which the keying material can be established.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

3 Terms and definitions

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

3.1

active

state of an entity in which the entity can obtain the shared secret key

3.2

ancestor keys of key k

set of keys in a logical key hierarchy that are assigned to the ancestor nodes of the node to which k is assigned

NOTE One of the keys in a set of ancestor keys is either the shared secret key or a key encryption key.