INTERNATIONAL STANDARD

ISO/IEC 11770-5

First edition
2011-12-15

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

Reference number
ISO/IEC 11770-5:2011(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 11770-5 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.

3.3
ancestor nodes of node *v*
set of nodes in a tree that can be reached by repeatedly going to the parent node from *v*

3.4
backward secrecy with interval *T*
security condition in which an entity joining at time $t = t_0$ cannot obtain any former shared secret keys at time $t < t_0 - T$

3.5
batch rekeying
rekeying method in which the shared secret key, and optionally, key encryption keys are updated at every rekeying interval *T*

3.6
child keys of key *k*
set of keys in a logical key hierarchy where the keys are assigned to the child nodes of the node to which *k* is assigned

NOTE One of the keys in a set of child keys shall be a key encryption key or individual key.

3.7
child nodes of node *w*
set of nodes in a tree which hang on *w*

3.8
***d*-ary tree**
tree where each node has *d* children except the leaf nodes in the tree

3.9
forward secrecy with interval *T*
security condition in which an entity leaving at time $t = t_0$ cannot obtain any subsequent shared secret keys at time $t > t_0 + T$

3.10
inactive
state of an entity in which the entity cannot obtain the shared secret key

3.11
individual key
key shared between the key distribution centre and each entity

3.12
individual rekeying
rekeying method in which the shared secret key, and optionally, key encryption keys are updated when an entity joins or leaves

3.13
key
sequence of symbols that controls the operations of a cryptographic transformation

3.14
key chain
set of cryptographic keys which are not necessarily independent

3.15
key distribution centre
KDC
entity trusted to generate or acquire, and distribute keys to entities

3.16
key encryption key
cryptographic key that is used for the encryption or decryption of other keys

[ISO/IEC 19790:2006]

3.17
leaf node
node in a tree which is not a parent of any other node, i.e. has no child nodes

3.18
logical key hierarchy
tree used for managing the shared secret key and key encryption keys

3.19
logical key structure
logical structure to manage keys

NOTE This structure has no correlation with the network topology.

3.20
one-way function
function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input which maps to this output

[ISO/IEC 11770-3:2008]

3.21
one-way function with trapdoor
function that is known to be easy to compute but hard to invert unless some secret information (trapdoor) is known

3.22
parent node of node *c*
node on which node *c* hangs

3.23
perfect backward secrecy
security condition in which a joining entity cannot obtain any former shared secret keys

3.24
perfect forward secrecy
security condition in which a leaving entity cannot obtain any subsequent shared secret keys

3.25
random number
time variant parameter whose value is unpredictable

[ISO/IEC 11770-1:2010]

3.26
rekeying
process of updating and redistributing the shared secret key, and optionally, key encryption keys

NOTE This process is executed by the key distribution centre.

3.27
root node
node in a tree which is not a child of any other node

3.28
shared secret key
key which is shared with all the active entities via a key establishment mechanism for multiple entities

3.29
symmetric key based key establishment mechanism for multiple entities
process of establishing a shared secret key between all active entities, using symmetric cryptographic techniques

3.30
tree
connected, acyclic graph with an identified special vertex, the root node

4 Symbols and abbreviations

AK	Ancestor key
BWK_i	Backward key for the time instance *i*
CK	Child key
COM(*X,Y*)	Function, which generates from the data items *X* and *Y* a key designed to be applied as key of the used encryption algorithm
CUT(*k*,*S*)	Function which outputs a substring of length *k* of the least significant bits of a string *S* of bits
d	Number of children of a parent node (see term *d*-ary tree)
e(*K,Z*)	Result of encrypting data *Z* with a symmetric encryption algorithm using the secret key *K*
f	One-way function with trap door
f^{-1}	Inverted function of *f,* which requires the trapdoor of *f*
FWK_i	Forward key for the time instance *i*
g_1	One-way function
g_2	One-way function
h	Number of ancestor nodes of a leaf node excluding the root node
IK	Individual key
IK x	Individual key shared between entity *x* and the key distribution centre
KDC	Key distribution centre
KEK	Key encryption key
LKH	Logical key hierarchy
m	Number of entities connected to the hub in a star structure
MAC(*K,Z*)	MAC function as defined in ISO/IEC 9797 using key *K* and data *Z*
$r_{BWKinit}$	Random number to initialize the backward key chain

$r_{FWKinit}$	Random number to initialize the forward key chain
RSA	Digital signature mechanism as defined in ISO/IEC 14888-2
s	Private key
SHA-1	Dedicated hash function as defined in ISO/IEC 10118-3
SSK	Shared secret key
v	Public key
$X\|\|Y$	Result of concatenating data items X and Y in that order

5 Requirements

The key establishment mechanisms specified in this part of ISO/IEC 11770 realize point-to-multipoint key communication by using logical key structures. The point-to-multipoint communication requires a key updating process when a new entity joins or an entity leaves the communication in order to maintain the secrecy of the communication.

a) There are two types of security requirements, perfect backward secrecy and forward secrecy and backward secrecy and forward secrecy with intervals. One of these security requirements shall be chosen depending on the security requirements of the particular application. Key establishment mechanisms for multiple entities require two different rekeying methods according to the security requirements: individual rekeying and batched rekeying. Individual re-keying provides perfect backward secrecy and forward secrecy, and batched rekeying provides backward secrecy and forward secrecy with interval *T*. The rekeying method and parameter setting have a strong influence on the security requirements; thus, they shall be determined according to the security policy of the application.

b) The encryption algorithm shall be chosen in accordance with the following:

1) A symmetric encryption algorithm shall be chosen from among those standardised in ISO/IEC 18033-3 and ISO/IEC 18033-4.

2) If a block cipher encryption algorithm is used, then the Mode of Operation employed shall be one of those standardised in ISO/IEC 10116, ISO/IEC 18033-3, ISO/IEC 18033-4 and ISO/IEC 19772. An encryption algorithm used for key encryption shall provide integrity, and input length shall be more than 128 bits. One of the mechanisms in ISO/IEC 19772 shall be used for integrity protection.

c) The shared secret key is established using either a secure or insecure communication channel. At least the individual key shall be exchanged between the key distribution centre and each entity using a secure channel in order to allow secure communication. A secure communication channel is one where an attacker cannot eavesdrop or tamper with messages in the channel.

d) The key establishment mechanisms in this part of ISO/IEC 11770 require the use of random numbers to generate the shared secret key, and optionally, key encryption keys. For means of generating random numbers, see ISO/IEC 18031.

6 Tree based key establishment mechanisms for multiple entities

6.1 General model

Key establishment for multiple entities enables the transmission of a message to all the entities, such that any active entities can decrypt the message correctly and any coalition of inactive entities cannot decrypt it. All the active entities share the shared secret key that is used to encrypt the message. An active entity may dynamically change to being inactive, and vice versa. The key distribution centre updates the shared secret key to prevent the joining entity from obtaining the former messages and the leaving entity from obtaining the subsequent messages.

Figure 1 shows the general model of key establishment for multiple entities, in which the key distribution centre can communicate with all the entities. The communication between the key distribution centre and entities does not need to be secure. The key distribution centre and each entity shall share a distinct individual key. The key distribution centre is responsible for distributing the shared secret key to all the active entities. The join/leave request is represented by (1) and the distribution of keys to the entities by (2), (3), ..., (n+1). From ii onward, the order in which the updates take place is not important.

NOTE if one of the entities that knows the shared secret key cannot be contacted for a period of time, that entity may miss a key update message, and cannot compute the updated shared secret key.

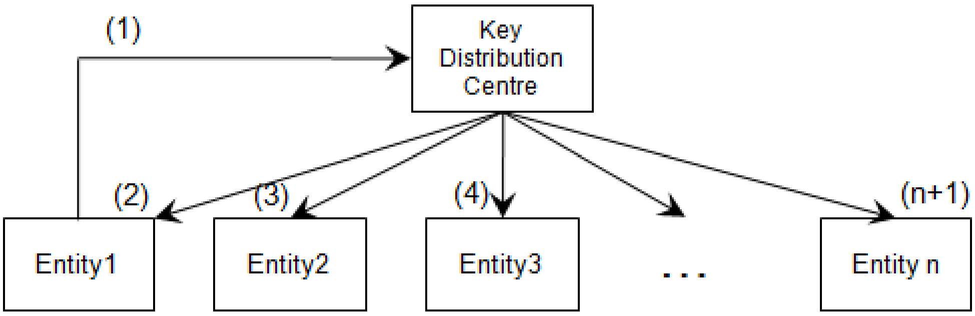

Figure 1 — General model of key establishment for multiple entities

6.2 Joining process

An entity sends a joining request to the key distribution centre in order to start obtaining the shared secret key. The key distribution centre executes the rekeying process after the requesting entity was accepted to join in the case where individual rekeying is adopted. On the other hand, the key distribution centre does not execute the rekeying process in the joining process in the case where batched rekeying is adopted.

6.3 Leaving process

An entity sends a leave request to the key distribution centre in order to stop obtaining the shared secret key. The key distribution centre executes rekeying after the leaving entity has left in the case where individual rekeying is adopted. On the other hand, there is no explicit leaving process in the case where batched rekeying is adopted. However, the key distribution centre shall record the leaving entities for the next rekeying process.

NOTE When the batched rekeying is used, the entity leaving the group can still decrypt communications in the group until the next batch rekeying takes place.

6.4 Rekeying process

The key distribution centre updates the shared secret key, and optionally, key encryption keys in order to satisfy security requirements. This process is executed in both the joining and leaving processes in the case where individual rekeying is adopted, and executed at regular time intervals in the case where batched rekeying is adopted.