

INTERNATIONAL STANDARD

ISO/IEC 11770-2

First edition
1996-04-15

Information technology — Security techniques — Key management —

Part 2:

Mechanisms using symmetric techniques

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

Partie 2: Mécanismes utilisant des techniques symétriques



Reference number
ISO/IEC 11770-2:1996(E)

AVA Documents
Document Sharing Hub

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. 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.

International Standard ISO/IEC 11770-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-committee 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: Key management framework*
- *Part 2: Mechanisms using symmetric techniques*
- *Part 3: Mechanisms using asymmetric techniques*

Further parts may follow.

Annexes A, B and C of this part of ISO/IEC 11770 are for information only.

© ISO/IEC 1996

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 the publisher.

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Information technology — Security techniques — Key management —

Part 2:

Mechanisms using symmetric techniques

1 Scope

The purpose of key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic algorithms according to the security policy in force. This part of ISO/IEC 11770 defines key establishment mechanisms using symmetric cryptographic techniques.

Key establishment mechanisms using symmetric cryptographic techniques can be derived from entity authentication mechanisms of ISO/IEC 9798-2 and ISO/IEC 9798-4 by specifying the use of text fields available in those mechanisms. Other key establishment mechanisms exist for specific environments; see for example ISO 8732. Besides key establishment, goals of such a mechanism may include unilateral or mutual authentication of the communicating entities. Further goals may be the verification of the integrity of the established key, or key confirmation.

This part of ISO/IEC 11770 addresses three environments for the establishment of keys: Point-to-Point, Key Distribution Centre (KDC) and Key Translation Centre (KTC). This part of ISO/IEC 11770 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. The document does not indicate other information which may be contained in the messages or specify other messages such as error messages. The explicit format of messages is not within the scope of this part of ISO/IEC 11770.

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 management mechanisms; there may be different products that comply with this part of ISO/IEC 11770 and yet are not compatible.

¹ To be published.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 11770. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 11770 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2: 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*.

ISO/IEC 9798-2: 1994, *Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms*.

ISO/IEC 9798-4: 1995, *Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function*.

ISO/IEC 11770-1: - ¹, *Information technology - Security techniques - Key management - Part 1: Key management framework*.

3 Definitions and Notation

3.1 Definitions

For the purposes of this part of ISO/IEC 11770 the definitions given in ISO/IEC 11770-1 apply. In addition, this part of ISO/IEC 11770 makes use of the following terms:

3.1.1 distinguishing identifier: Information which unambiguously distinguishes an entity.

- 3.1.2 entity authentication:** The corroboration that an entity is the one claimed.
- 3.1.3 key confirmation:** The assurance for one entity that another identified entity is in possession of the correct key.
- 3.1.4 key control:** The ability to choose the key, or the parameters used in the key computation.
- 3.1.5 key generating function:** A function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application. The function shall have the property that it shall be computationally infeasible to deduce the output without prior knowledge of the secret input.
- 3.1.6 point-to-point key establishment:** The direct establishment of keys between entities, without involving a third party.
- 3.1.7 random number:** A time variant parameter whose value is unpredictable.
- 3.1.8 redundancy:** Any information that is known and can be checked.
- 3.1.9 sequence number:** A time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period.
- 3.1.10 time variant parameter:** A data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp.

3.2 Notation

Throughout this part of ISO/IEC 11770 the following notation is used:

X	is the distinguishing identifier of entity X.
KDC	denotes a Key Distribution Centre.
KTC	denotes a Key Translation Centre.
T	is the distinguishing identifier of the Key Distribution Centre or the Key Translation Centre.
F	denotes keying material.
K _{XY}	is a secret key associated with the entities X and Y.
R	is a random number.
R _X	is a random number issued by entity X.
T/N	is a time stamp or a sequence number.
T _X /N _X	is a time stamp or a sequence number issued by entity X.
TVP	is a time variant parameter.

TVP _X	is a time variant parameter issued by entity X.
eK(Z)	is the result of the encipherment of data Z with a symmetric algorithm using the key K.
dK(Z)	is the result of the decipherment of data Z with a symmetric algorithm using the key K.
vK(Z)	is the result of a cryptographic check function computed on data Z using the key K. vK(Z) is also called message authentication code (MAC) and may be denoted as macK(Z).
f	denotes a key generating function.
X Y	is the result of the concatenation of data items X and Y in that order.

The fields *Text1*, *Text2*, ... specified in the mechanisms may contain optional data for use in applications outside the scope of this part of ISO/IEC 11770 (they may be empty). Their relationship and contents depend upon the specific application. One such possible application is message authentication (see annex B for an example).

Likewise, optional plaintext text fields may be prepended or appended to any of the messages. They have no security implications and are not explicitly included in the mechanisms specified in this part of ISO/IEC 11770.

Data items that are optional in the mechanisms are shown in *italics*.

4 Requirements

The key establishment mechanisms specified in this part of ISO/IEC 11770 make use of symmetric cryptographic techniques, more specifically symmetric encipherment algorithms and/or key generating functions. The cryptographic algorithms and the key life-time shall be chosen such that it is computationally infeasible for a key to be deduced during its life-time. If the following additional requirements are not met, the key establishment process may be compromised or it cannot be implemented.

For those mechanisms making use of a symmetric encipherment algorithm, either assumption a) or assumption b) is required.

- The encipherment algorithm, its mode of operation and the redundancy in the plaintext shall provide the recipient with the means to detect forged or manipulated data.
- The integrity of the enciphered data shall be ensured by a data integrity mechanism. If a hash-function is used for this purpose the hash-code shall either be appended to the data before encipherment or be placed in a plaintext text field.

NOTES

- 1 - Modes of operation for block cipher algorithms are standardized in ISO/IEC 10116.
- 2 - A data integrity mechanism is standardized in ISO/IEC 9797. Hash-functions are standardized in ISO/IEC 10118.
- 3 - When a KDC or KTC is involved, assumptions a) and b) are not always equivalent in terms of the ability to detect unambiguously on which link an active attack is being performed. See Annex B for examples.

In each exchange specified in the mechanisms of clauses 5, 6 and 7, the recipient of a message shall know the claimed identity of the originator. If this is not the case from the context in which the mechanism is being used then this could, e.g., be achieved by the inclusion of identifiers in additional plaintext text fields of certain of the messages.

Keying material may be established using either secure or insecure communication channels. When using only symmetric cryptographic techniques, at least the first key shall be exchanged between two entities using a secure channel in order to allow secure communications.

The key establishment mechanisms in this part of ISO/IEC 11770 require the use of time variant parameters such as time stamps, sequence numbers, or random numbers. In this context the use of the term random number also includes unpredictable pseudo-random numbers. The properties of these parameters, in particular that they are non-repeating, are important for the security of these mechanisms. For additional information on time variant parameters see Annex B of ISO/IEC 9798-2.

5 Point-to-Point Key Establishment

The basic mechanism of every key establishment scheme is point-to-point key establishment which requires that the entities already share a key so that further keys may be established directly between the entities.

For the implementation of the mechanisms specified in this clause it is assumed that

- A key K_{AB} is shared by the entities A and B.
- At least one of A or B is able to generate, acquire or contribute to a secret key K as described in the individual mechanism.
- Security requirements are concerned with the confidentiality of K , and modification and replay detection.

5.1 Key Establishment Mechanism 1

In key establishment mechanism 1 the key K is derived from a time variant parameter TVP, e.g., a random number R , a time stamp T , or a sequence number N , using a key generating function. Key establishment mechanism 1 provides no authentication of the key K established by the mechanism. The mechanism requires that A is able to generate a TVP.

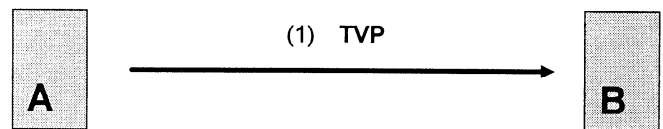


Figure 1 - Mechanism 1

Steps:

- (1) A generates a random number R , a time stamp T , or a sequence number N and transfers it to B.
- (1a) Both A and B then derive the key K by using a key generating function f with inputs the shared secret key K_{AB} and the time variant parameter TVP:

$$K = f(K_{AB}, \text{TVP}).$$

See Annex B for examples of possible key generating functions.

NOTE - To also provide authentication, key establishment mechanism 1 may be combined with an authentication mechanism as specified in 9798-2 or 9798-4. See annex B for an example.

5.2 Key Establishment Mechanism 2

In key establishment mechanism 2 the key K is supplied by entity A. The mechanism provides no authentication of the key K established by the mechanism nor does it provide entity authentication.

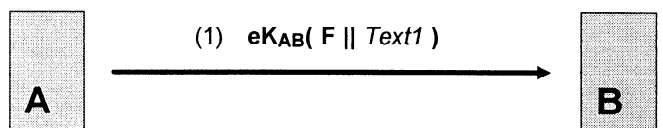


Figure 2 - Mechanism 2

Steps:

- (1) A sends B the keying material F (key K and optional data) enciphered with K_{AB} .
- (1a) On receipt of the message, B deciphers the enciphered part and thus obtains the key K.

5.3 Key Establishment Mechanism 3

Key establishment mechanism 3 is derived from the one pass entity authentication mechanism of ISO/IEC 9798-2, clause 5.1.1. In this mechanism the key K is supplied by entity A. Key establishment mechanism 3 provides unilateral authentication, i.e., entity A is authenticated by the mechanism. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that both A and B are able to maintain mechanisms for generating or verifying the validity of time stamps T or sequence numbers N.

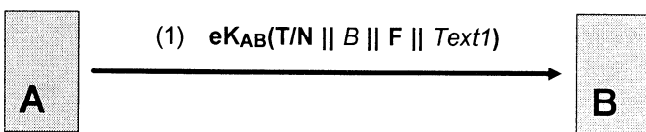


Figure 3 - Mechanism 3

Steps:

- (1) A sends B a time stamp or sequence number T/N, the distinguishing identifier B, and the keying material F (key K and optional data). The inclusion of the distinguishing identifier B is optional. The data fields are enciphered with K_{AB} .
- (1a) On receipt of the message, B deciphers the enciphered part, checks the correctness of its distinguishing identifier, if present, checks the time stamp or sequence number, and obtains the key K.

NOTE - Distinguishing identifier B is included in step (1) to prevent a substitution attack, i.e., the re-use of this message by an adversary masquerading as B (see Annex A). In environments where such attacks cannot occur, the identifier may be omitted.

5.4 Key Establishment Mechanism 4

Key establishment mechanism 4 is derived from the two pass unilateral entity authentication mechanism of ISO/IEC 9798-2, clause 5.1.2. In this mechanism the key K is supplied by entity A. Key establishment mechanism 4

provides unilateral authentication, i.e., entity A is authenticated by the mechanism. Uniqueness/timeliness is controlled by a random number R_B . The mechanism requires that B is able to generate random numbers.

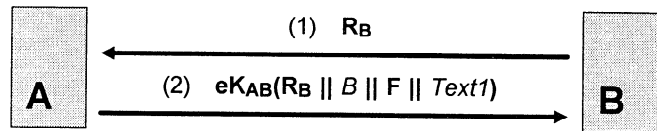


Figure 4 - Mechanism 4

Steps:

- (1) B sends A a random number R_B .
- (2) A sends B the received number R_B , the distinguishing identifier B, and the keying material F (key K and optional data). The inclusion of the distinguishing identifier B is optional. The data fields are enciphered with K_{AB} .
- (2a) On receipt of message (2), B deciphers the enciphered part, checks the correctness of its distinguishing identifier, if present, checks that the random number R_B , sent to A in step (1), was used in constructing message (2), and obtains the key K.

NOTE - Distinguishing identifier B is included in step (2) to prevent a substitution attack, i.e., the re-use of this message by an adversary masquerading as B (see Annex A). In environments where such attacks cannot occur, the identifier may be omitted.

5.5 Key Establishment Mechanism 5

Key establishment mechanism 5 is derived from the two pass mutual authentication mechanism of ISO/IEC 9798-2, clause 5.2.1. This mechanism enables both A and B to contribute part of the established key K. Key establishment mechanism 5 provides mutual authentication, i.e., both communicating entities are authenticated by the mechanism. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that both A and B are able to maintain mechanisms for generating and verifying the validity of time stamps T or sequence numbers N.

Steps:

- (1) A sends B a time stamp or sequence number T_A/N_A , the distinguishing identifier B, and the keying material F_A . The inclusion of the