INTERNATIONAL STANDARD

ISO/IEC 11770-2

Second edition
2008-06-15

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 11770-2:2008(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 11770-2 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 11770-2:1996), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 11770-2:1996/Cor.1:2005.

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*

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 the 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, the goals of such a mechanism might include unilateral or mutual authentication of the communicating entities. Further goals might 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. It does not indicate other information which can 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 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 a secret key with at least one other entity (e.g. a TTP). 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 management mechanisms; products complying with this part of ISO/IEC 11770 might not be compatible.

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 11770-1, *Information technology — Security techniques — Key management — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 11770-1 and the following apply.

3.1
distinguishing identifier
information which unambiguously distinguishes an entity

3.2
entity authentication
corroboration that an entity is the one claimed

[ISO/IEC 9798-1]

3.3
explicit key authentication from entity *A* to entity *B*
assurance for entity *B* that entity *A* is the only other entity that is in possession of the correct key

[ISO/IEC 11770-3]

NOTE Implicit key authentication from *A* to *B* and key confirmation from *A* to *B* together imply explicit key authentication from *A* to *B*.

3.4
implicit key authentication from entity *A* to entity *B*
assurance for entity *B* that entity *A* is the only other entity that can possibly be in possession of the correct key

[ISO/IEC 11770-3]

3.5
key confirmation from entity *A* to entity *B*
assurance for entity *B* that entity *A* is in possession of the correct key

[ISO/IEC 11770-3]

3.6
key control
ability to choose the key, or the parameters used in the key computation

3.7
key generating function
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, and which has the property that it is computationally infeasible to deduce the output without prior knowledge of the secret input

3.8
point-to-point key establishment
direct establishment of keys between entities, without involving a third party

3.9
random number
time variant parameter whose value is unpredictable

3.10
redundancy
information that is known and can be checked

3.11
sequence number
time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

3.12
time variant parameter
data item used to verify that a message is not a replay, such as a random number, sequence number, or a time stamp

4 Symbols and abbreviated terms

$d_K(Z)$	result of decrypting data Z with a symmetric encryption algorithm using the secret key K
$e_K(Z)$	result of encrypting data Z with a symmetric encryption algorithm using the secret key K
f	key generating function
F	keying material
F_X	keying material originated by entity X
I_X	the distinguishing identifier of entity X
KDC	Key Distribution Centre
KTC	Key Translation Centre
K_{XY}	secret key associated with entities X and Y
MAC	Message Authentication Code
$MAC_K(Z)$	result of applying a MAC function to data Z using the secret key K
P	Key Distribution Centre or Key Translation Centre
R	random number
R_X	random number issued by entity X
T/N	time stamp or sequence number
TVP	Time Variant Parameter
TVP_X	Time Variant Parameter issued by entity X
T_X/N_X	time stamp or sequence number issued by entity X
$X\|\|Y$	result of concatenating data items X and Y in that order

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

Likewise, optional plaintext text fields can be included as a prefix, 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 square brackets, [thus].

5 Requirements

The key establishment mechanisms specified in this part of ISO/IEC 11770 make use of symmetric cryptographic techniques, more specifically, symmetric encryption algorithms, MACs, 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 lifetime. If the following additional requirements are not met, the key establishment process may be compromised.

a) For those mechanisms making use of a symmetric encryption algorithm, either assumption 1) or assumption 2) is required.

   1) The encryption algorithm, its mode of operation, and the redundancy in the plaintext shall provide the recipient with the means to detect forged or manipulated data.

   2) The integrity of the encrypted data shall be ensured by a MAC.

   Choices for encryption and integrity algorithms should be in accordance with the following.

   i) Assumption 1) above can be guaranteed if an authenticated encryption technique is used; use of one of the techniques standardized in ISO/IEC 19772 is recommended.

   ii) The choice for a symmetric encryption algorithm should be chosen from amongst those standardized in ISO/IEC 18033-3 and ISO/IEC 18033-4.

   iii) If a block cipher encryption algorithm is used, then the mode of operation employed should be one of those standardized in ISO/IEC 10116.

   iv) If a MAC is used, then the techniques shall be chosen from amongst those standardized in ISO/IEC 9797.

   NOTE 1 When a KDC or KTC is involved, assumptions 1) and 2) are not always equivalent in terms of the ability to unambiguously detect on which link an active attack is being performed. See Annex C for examples.

b) In each exchange specified in the mechanisms of clauses 6, 7 and 8, the recipient of a message shall know the claimed identity of the originator. If this is not the case, i.e. if the context of use of the mechanism does not establish the claimed identity, then this could, for example, be achieved by the inclusion of identifiers in additional plaintext text fields of one or more of the messages.

   NOTE 2 The specifications of many of the mechanisms in this part of ISO/IEC 11770 require the correctness of an identifier included in a message to be checked. This shall be done by comparing the received identifier with the expected identifier (as specified in the mechanism concerned). If the identifier in question is that of the originator of the message, then the recipient shall know the value of the expected identifier because of requirement b) above.

c) 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.

d) 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 9798-1. For means of generating random numbers, see ISO/IEC 18031.

6 Point-to-point key establishment

Underlying every key management scheme is a point-to-point key establishment procedure, the use of which requires that the entities already share a key so that further keys may be established directly between the two entities. In this clause, six point-to-point key establishment mechanisms are specified.

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

a) a key K_{AB} is shared by entities *A* and *B*,

b) at least one of *A* and *B* is able to generate, acquire or contribute to a secret key *K*, as described in the individual mechanism,

c) security requirements are concerned with the confidentiality of *K*, and the detection of modification or replay of keys and messages.

6.1 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 does not provide authentication of the key *K* established by the mechanism. The mechanism requires that *A* is able to generate a TVP.

Figure 1 — Mechanism 1

The mechanism involves the following steps (see Figure 1):

1) *A* generates a time variant parameter TVP_A, which can be a random number R_A, a time stamp T_A, or a sequence number N_A, and transfers it to *B*.

   i) Both *A* and *B* then derive the key *K* by using a key generating function *f* which takes as inputs the shared secret key K_{AB} and the time variant parameter TVP_A:

      $K = f(K_{AB}, TVP_A)$.

      See Annex C for examples of possible key generating functions.

NOTE In order to also provide entity authentication, key establishment mechanism 1 may be combined with an authentication mechanism as specified in ISO/IEC 9798-2 or ISO/IEC 9798-4. See Annex C for an example.

6.2 Key Establishment Mechanism 2

In key establishment mechanism 2 the key *K* is supplied by entity *A*. The mechanism does not provide authentication of the key *K* established by the mechanism, nor does it provide entity authentication.

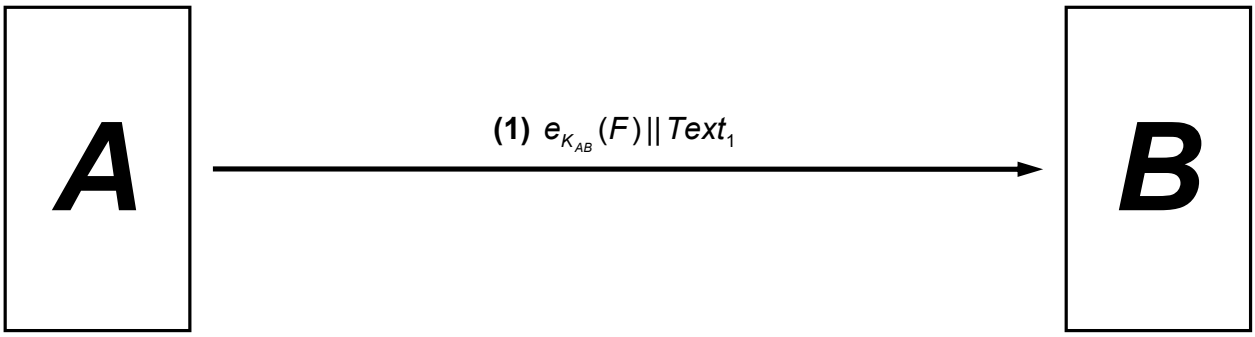

Figure 2 — Mechanism 2

The mechanism involves the following steps (see Figure 2):

1) *A* sends *B* the keying material *F* (made up of a key *K*, together with optional data), encrypted using the key K_{AB}.

   i) On receipt of the message, *B* deciphers the encrypted part, and thus obtains the key *K*.

6.3 Key Establishment Mechanism 3

Key establishment mechanism 3 is derived from the one-pass unilateral authentication mechanism specified in ISO/IEC 9798-2. In this mechanism, the key *K* is supplied by entity *A*. Key establishment mechanism 3 provides unilateral authentication, i.e. the mechanism enables entity *B* to authenticate entity *A*. 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_A or sequence numbers N_A, respectively.

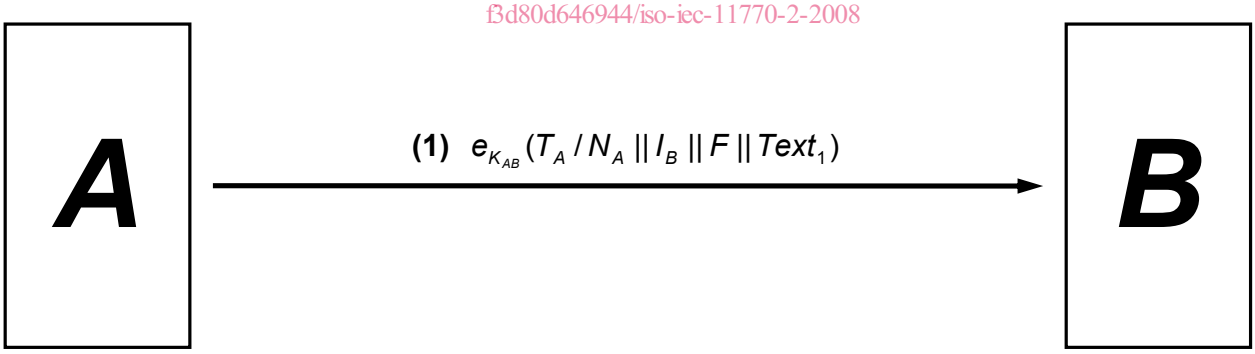

Figure 3 — Mechanism 3

The mechanism involves the following steps (see Figure 3):

1) *A* sends *B* a time stamp T_A or sequence number N_A, the distinguishing identifier I_B, and the keying material *F* (made up of a key *K* together with optional data). The inclusion of the distinguishing identifier I_B is optional. he data fields are encrypted using the key K_{AB}.

   i) On receipt of the message, *B* deciphers the encrypted 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 I_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* to *A* (see Annex B). In environments where such attacks cannot occur, the identifier may be omitted.

6.4 Key Establishment Mechanism 4

Key establishment mechanism 4 is derived from the two-pass unilateral authentication mechanism specified in ISO/IEC 9798-2. In this mechanism, the key K is supplied by entity A. Key establishment mechanism 4 provides unilateral authentication, i.e. the mechanism enables entity B to authenticate entity A. Uniqueness/timeliness is controlled by a random number R_B. The mechanism requires that B is able to generate random numbers.

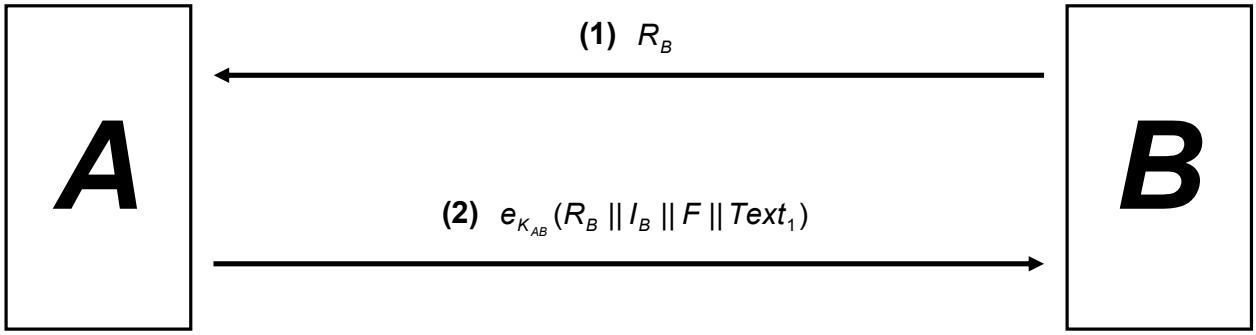

Figure 4 — Mechanism 4

The mechanism involves the following steps (see Figure 4):

1) B sends A a random number R_B.

2) A sends B the received number R_B, the distinguishing identifier I_B, and the keying material F (made up of a key K together with optional data). The inclusion of the distinguishing identifier I_B is optional. The data fields are encrypted using the key K_{AB}.

   i) On receipt of message 2, B deciphers the encrypted 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 I_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 to A (see Annex B). In environments where such attacks cannot occur, the identifier may be omitted.

6.5 Key Establishment Mechanism 5

Key establishment mechanism 5 is derived from the two-pass mutual authentication mechanism specified in ISO/IEC 9798-2. This mechanism enables both A and B to contribute part of the established key K. Key establishment mechanism 5 provides mutual authentication between A and B. 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.

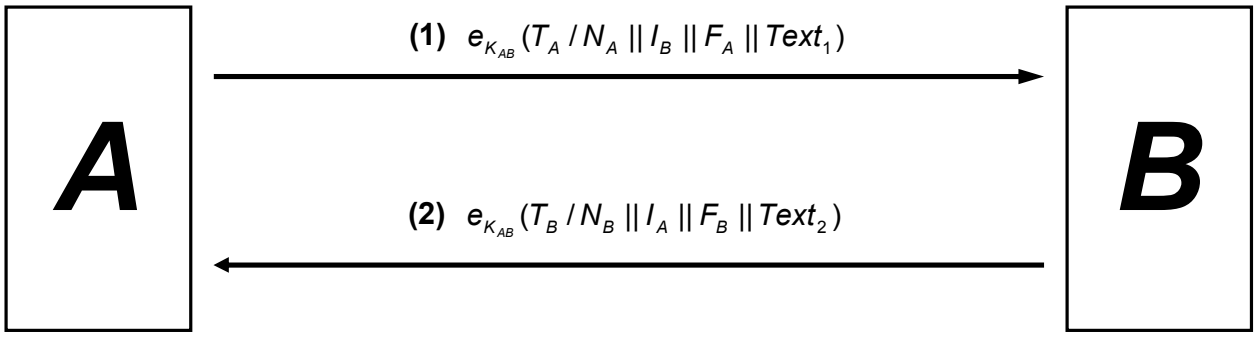

Figure 5 — Mechanism 5

The mechanism involves the following steps (see Figure 5):

1) *A* sends *B* a time stamp T_A or sequence number N_A, the distinguishing identifier I_B, and the keying material F_A. The inclusion of the distinguishing identifier I_B is optional. The data fields are encrypted using the key K_{AB}.

   i) On receipt of message 1, *B* deciphers the encrypted part, checks the correctness of its distinguishing identifier, if present, and checks the time stamp or sequence number.

2) *B* sends *A* a time stamp T_B or sequence number N_B, the distinguishing identifier I_A, and the keying material F_B. The inclusion of the distinguishing identifier I_A is optional. The data fields are encrypted using the key K_{AB}.

   i) On receipt of message 2, *A* deciphers the encrypted part, checks the correctness of its distinguishing identifier, if present, and checks the time stamp or sequence number.

   ii) Both *A* and *B* derive the key *K* using a key generating function *f*, taking as input the secret keying material fields F_A and F_B:

   $$K = f(F_A, F_B).$$

   See Annex C for examples of possible key generating functions.

In key establishment mechanism 5, either of the two keying material fields F_A and F_B may be empty, but not both. If either of these keying material fields is empty, the key shall be computed using the key generating function *f*, as described above, but with the relevant one of the two inputs equal to either the empty string or a fixed string (depending on the nature of the function *f*).

NOTE Distinguishing identifier I_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* to *A* (see Annex B). For similar reasons, distinguishing identifier I_A is present in step 2. In environments where such attacks cannot occur, one or both of the identifiers may be omitted.

6.6 Key Establishment Mechanism 6

Key establishment mechanism 6 is derived from the three-pass mutual authentication mechanism specified in ISO/IEC 9798-2. This mechanism enables both *A* and *B* to contribute part of the established key *K*. Key establishment mechanism 6 provides mutual authentication between *A* and *B*. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that both *A* and *B* are able to generate random numbers.

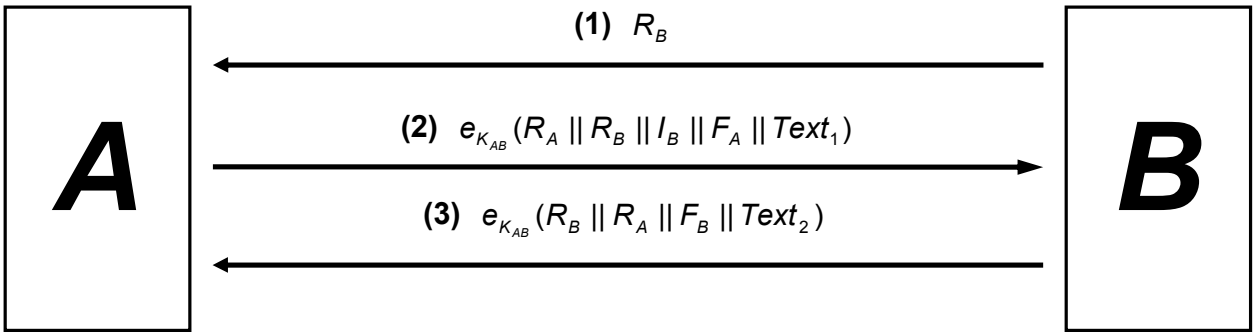

Figure 6 — Mechanism 6