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/IEC 2008

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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 2008

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2008 – All rights reserved

Contents

Page

Foreword ... iv

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 2

4 Symbols and abbreviated terms ... 3

5 Requirements ... 4

6 Point-to-point key establishment ... 5
6.1 Key Establishment Mechanism 1 ... 5
6.2 Key Establishment Mechanism 2 ... 5
6.3 Key Establishment Mechanism 3 ... 6
6.4 Key Establishment Mechanism 4 ... 7
6.5 Key Establishment Mechanism 5 ... 7
6.6 Key Establishment Mechanism 6 ... 8

7 Mechanisms using a Key Distribution Centre ... 9
7.1 Key Establishment Mechanism 7 ... 10
7.2 Key Establishment Mechanism 8 ... 11
7.3 Key Establishment Mechanism 9 ... 12
7.4 Key Establishment Mechanism 10 ... 14

8 Mechanisms using a Key Translation Centre ... 15
8.1 Key Establishment Mechanism 11 ... 16
8.2 Key Establishment Mechanism 12 ... 16
8.3 Key Establishment Mechanism 13 ... 18

Annex A (normative) **ASN.1 module** ... 21

Annex B (informative) **Properties of key establishment mechanisms** ... 23

Annex C (informative) **Auxiliary techniques** ... 25

Bibliography ... 27

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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*

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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*

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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].

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

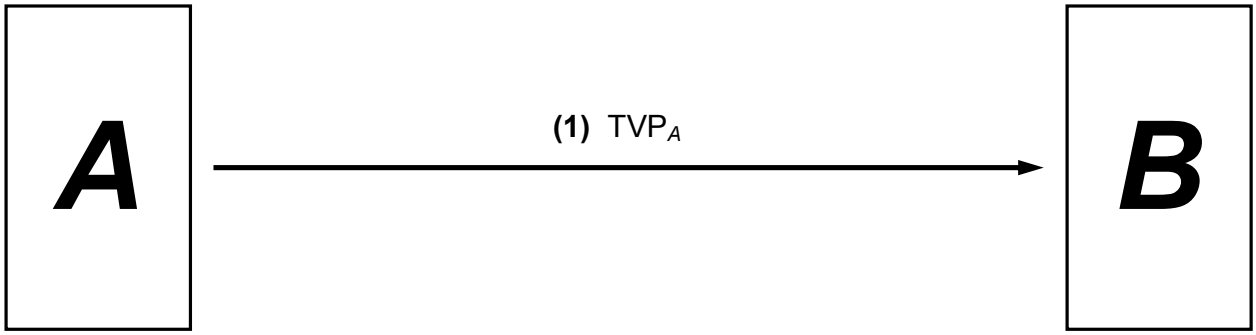

Figure 1 — Mechanism 1

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.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

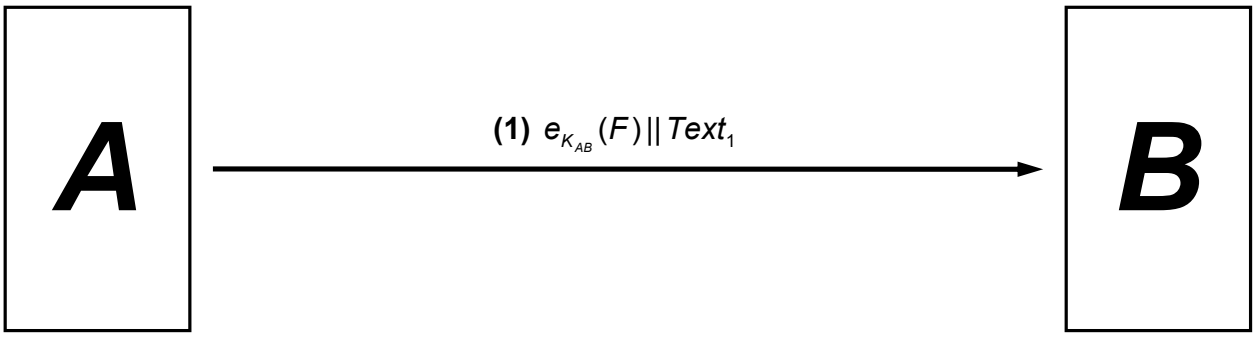

Figure 2 — Mechanism 2

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.

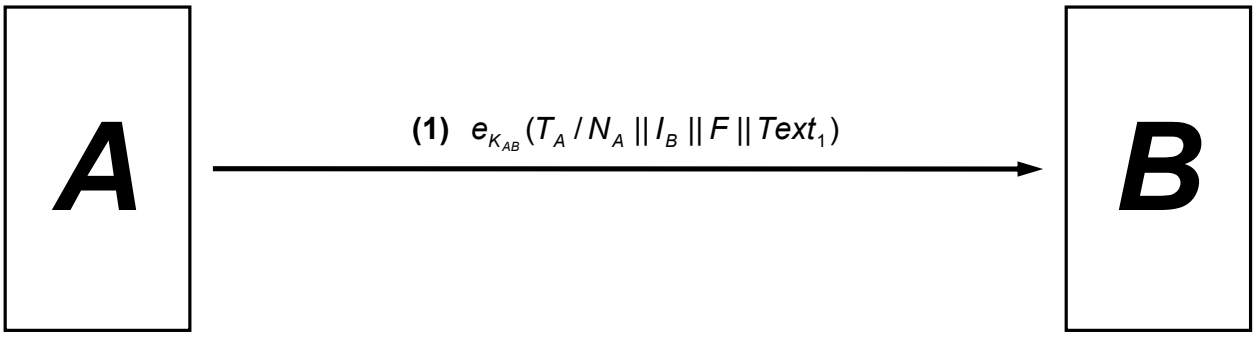

Figure 3 — Mechanism 3

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.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

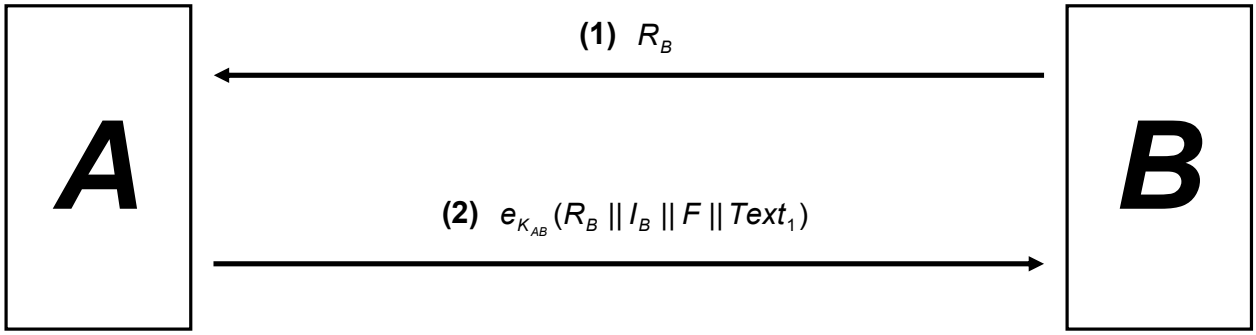

Figure 4 — Mechanism 4

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*.

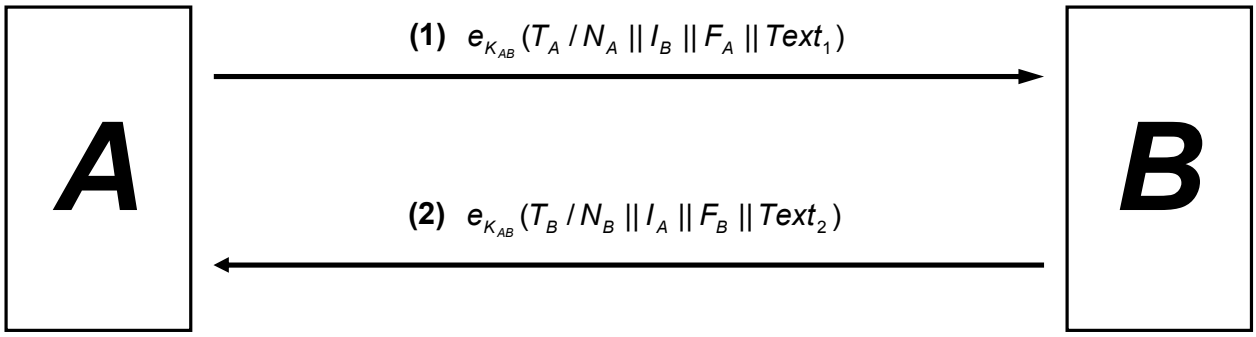

Figure 5 — Mechanism 5

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

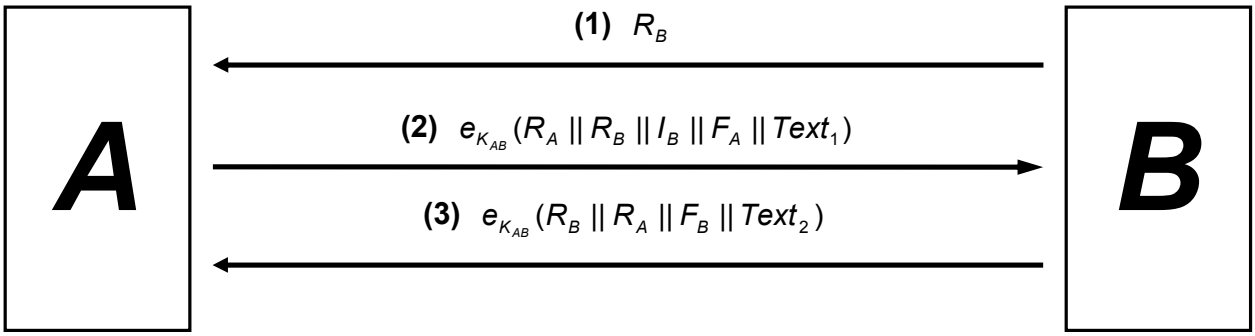

Figure 6 — Mechanism 6

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The mechanism involves the following steps (see Figure 6):

1) *B* sends *A* a random number R_B in message 1.

2) *A* sends *B* a random number R_A, the received number R_B, the distinguishing identifier I_B, and the keying material F_A in message 2. 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, and checks that the random number R_B, sent to A in step 1, was used in constructing message 2.

3) *B* sends *A* the random numbers R_B and R_A, and the keying material F_B in message 3. The data fields are encrypted using the key K_{AB}.

   i) On receipt of message 3, *A* deciphers the encrypted part and checks that the random numbers R_B and R_A, sent in messages 1 and 2, respectively, were used in constructing message 3.

   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.

NOTE 1 In key establishment mechanism 6, either of the two keying material fields F_A and F_B may be empty, but not both.

NOTE 2 Distinguishing identifier I_B is included in step 2 to prevent reflection attacks (see Annex B). In environments where such attacks cannot occur, the identifier may be omitted.

NOTE 3 A variant of key establishment mechanism 6 can be constructed from two parallel instances of key establishment mechanism 4, one started by entity *A* and the other by entity *B*.

7 Mechanisms using a Key Distribution Centre

The purpose of a Key Distribution Centre (KDC) is to first generate or acquire and then distribute a key to a pair of entities that both share a key with the KDC.

In this clause, four key establishment mechanisms using a KDC are specified.

— In the first three mechanisms one of the two entities requests a key *K* from the KDC for later distribution to the other entity. The KDC generates or acquires the key *K*, and sends a message to the requesting entity protected by a key shared with this entity. This message contains a second message protected by a key shared between the KDC and the second entity, which can then be forwarded by the requesting entity to the ultimate recipient.

— In the fourth mechanism the KDC generates or acquires the key *K*, and sends it directly to both communicating entities. The two messages are protected using the key that the KDC shares with the corresponding entities.

For all of these mechanisms, only the KDC is required to have the ability to generate or otherwise acquire keys. Following the distribution of a key by the KDC, the two entities may use this key to support the use of a point-to-point key establishment mechanism.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

a) Entities *A* and *B* share secret keys K_{AP} and K_{BP}, respectively, with a trusted third party *P* that acts as a KDC. The KDC shall be able to generate or otherwise acquire a key *K*.

b) The KDC shall have a means of communication with the entity requesting a key.

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

7.1 Key Establishment Mechanism 7

Key establishment mechanism 7 does not provide authentication of the key *K* established by the mechanism.

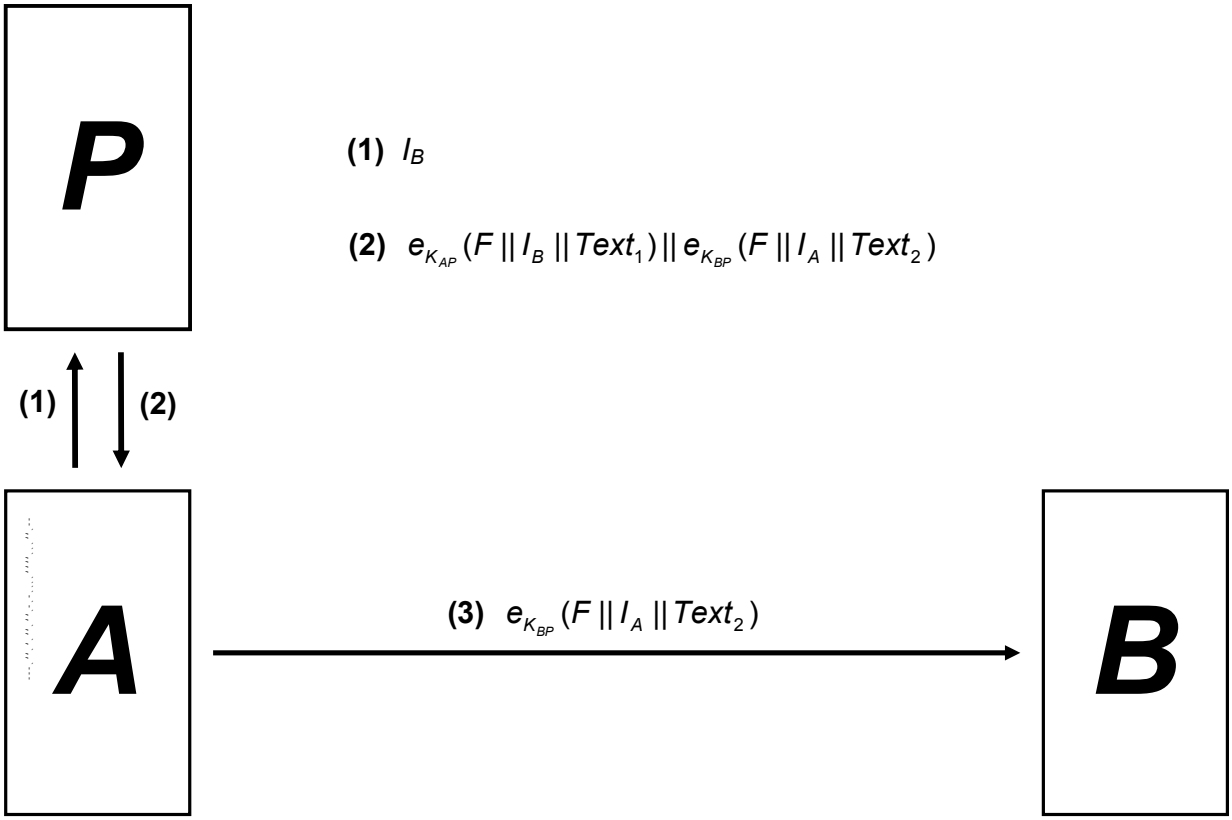

Figure 7 — Mechanism 7

The mechanism involves the following steps (see Figure 7):

1) *A* requests keying material from the KDC by sending message 1 to the KDC containing the distinguishing identifier I_B of the second entity *B*.

2) The KDC sends message 2 to *A* containing the keying material *F* (made up of a key *K* together with optional data). This message consists of two main parts:

   — $e_{K_{AP}}(F \,||\, I_B \,||\, Text_1)$;

   — $e_{K_{BP}}(F \,||\, I_A \,||\, Text_2)$.

   i) On receipt of message 2, *A* deciphers the first part, checks the correctness of the distinguishing identifier I_B, and obtains the key *K*.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3) *A* forwards the second part of message 2 to *B* in message 3.

   i) On receipt of message 3, *B* deciphers the encrypted part, checks the correctness of the distinguishing identifier I_A, and obtains the key *K*.

7.2 Key Establishment Mechanism 8

Key establishment mechanism 8 is derived from the four-pass mutual authentication mechanism specified in ISO/IEC 9798-2. Key establishment mechanism 8 optionally provides mutual authentication between *A* and *B*. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that *A*, *B* and the KDC are able to maintain mechanisms for generating and verifying the validity of time stamps *T* or sequence numbers *N*.

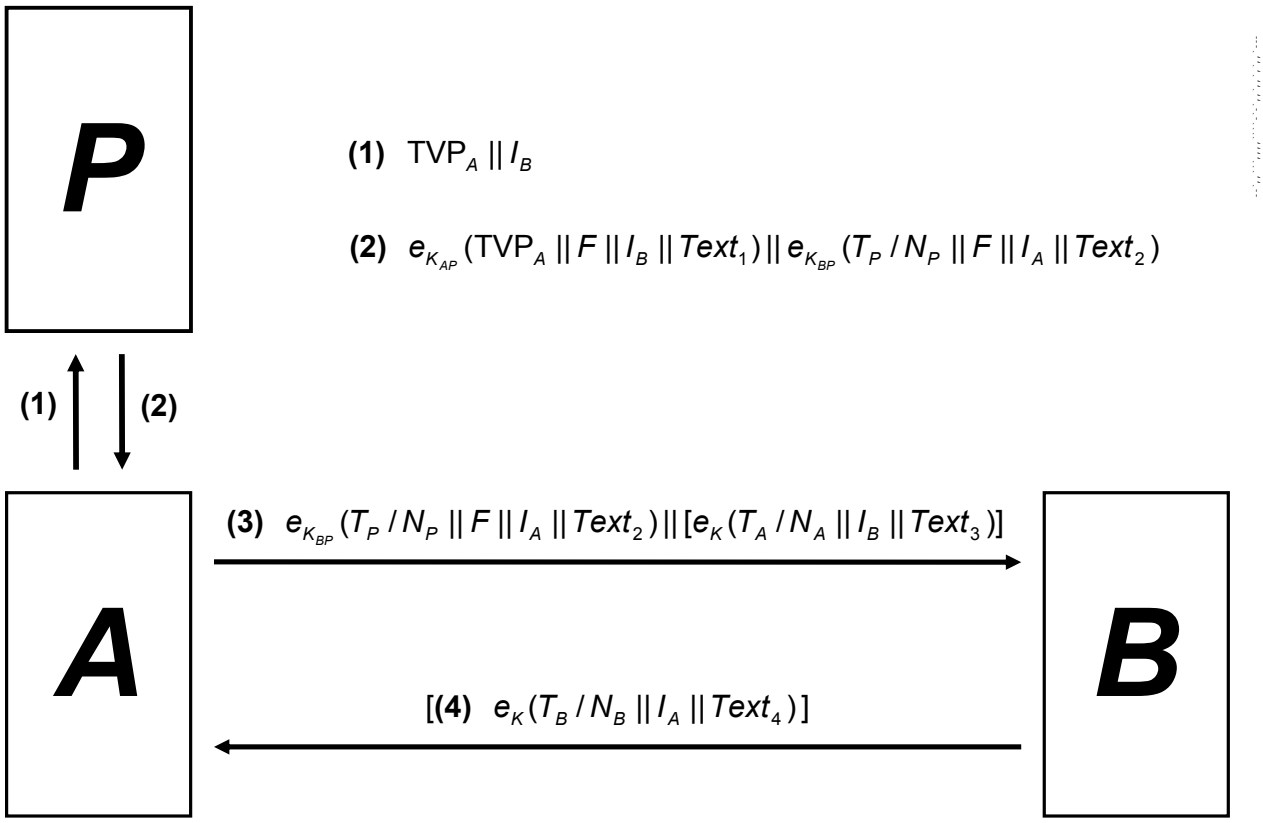

Figure 8 — Mechanism 8

The mechanism involves the following steps (see Figure 8):

1) *A* requests keying material from the KDC by sending message 1 to the KDC containing a time variant parameter TVP_A (which can be a random number, a time stamp, or a sequence number) and the distinguishing identifier I_B of the second entity *B*.

2) The KDC sends message 2 to *A* containing the keying material *F* (made up of a key *K* together with optional data). This message consists of two main parts:

   — $e_{K_{AP}}(\mathrm{TVP}_A \,||\, F \,||\, I_B \,||\, Text_1)$;

   — $e_{K_{BP}}(T_P / N_P \,||\, F \,||\, I_A \,||\, Text_2)$.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

i) On receipt of message 2, *A* deciphers the first part, checks that the time variant parameter TVP_A, sent to the KDC in step 1, was used in constructing the first part of message 2, checks the correctness of the distinguishing identifier I_B, and obtains the key *K*.

3) *A* forwards the second part of message 2 to *B* in message 3. Message 3 optionally also contains a second part, a data field

$$e_K(T_A / N_A \,||\, I_B \,||\, Text_3)$$

which enables *B* to check the integrity of the key *K* retrieved from *F*.

NOTE The timestamp T_A or sequence number N_A included in message 3 is unrelated to the time variant parameter TVP_A included in message 1.

i) On receipt of message 3, *B* deciphers the first part, checks the correctness of the time stamp or sequence number, checks the correctness of the distinguishing identifier I_A, and obtains the key *K*.

ii) *B* deciphers the second part of message 3, if present, and checks the correctness of the time stamp or sequence number and of the distinguishing identifier I_B.

The fourth step given below is optional; it can be omitted if either no entity authentication or only unilateral authentication is required.

4) *B* returns $e_K(T_B / N_B \,||\, I_A \,||\, Text_4)$ to *A* in message 4, thereby acknowledging that it shares the key *K*.

i) On receipt of message 4, *A* deciphers it and checks the correctness of the time stamp or sequence number and of the distinguishing identifier I_A.

NOTE 1 The encryption algorithm *e* used in the optional key confirmation process (i.e., part 2 of message 3 and message 4) may differ from the encryption algorithm (also denoted by *e*) used for key distribution.

NOTE 2 In order to achieve mutual authentication and conformance with the four-pass entity authentication mechanism specified in ISO/IEC 9798-2, the optional message (parts) in steps 3 and 4 need to be included.

NOTE 3 If required, authentication of the requesting entity by the KDC may be provided by the inclusion of a MAC, computed over TVP_A using a secret key shared by *A* and the KDC, in a plaintext text field of message 1. This can only work correctly if TVP_A is of a form (e.g. a time stamp) whose correctness can be verified by the KDC.

7.3 Key Establishment Mechanism 9

Key establishment mechanism 9 is derived from the five-pass mutual authentication mechanism specified in ISO/IEC 9798-2. Key establishment mechanism 9 optionally provides mutual authentication between *A* and *B*. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that *A*, *B* and the KDC are able to generate random numbers.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

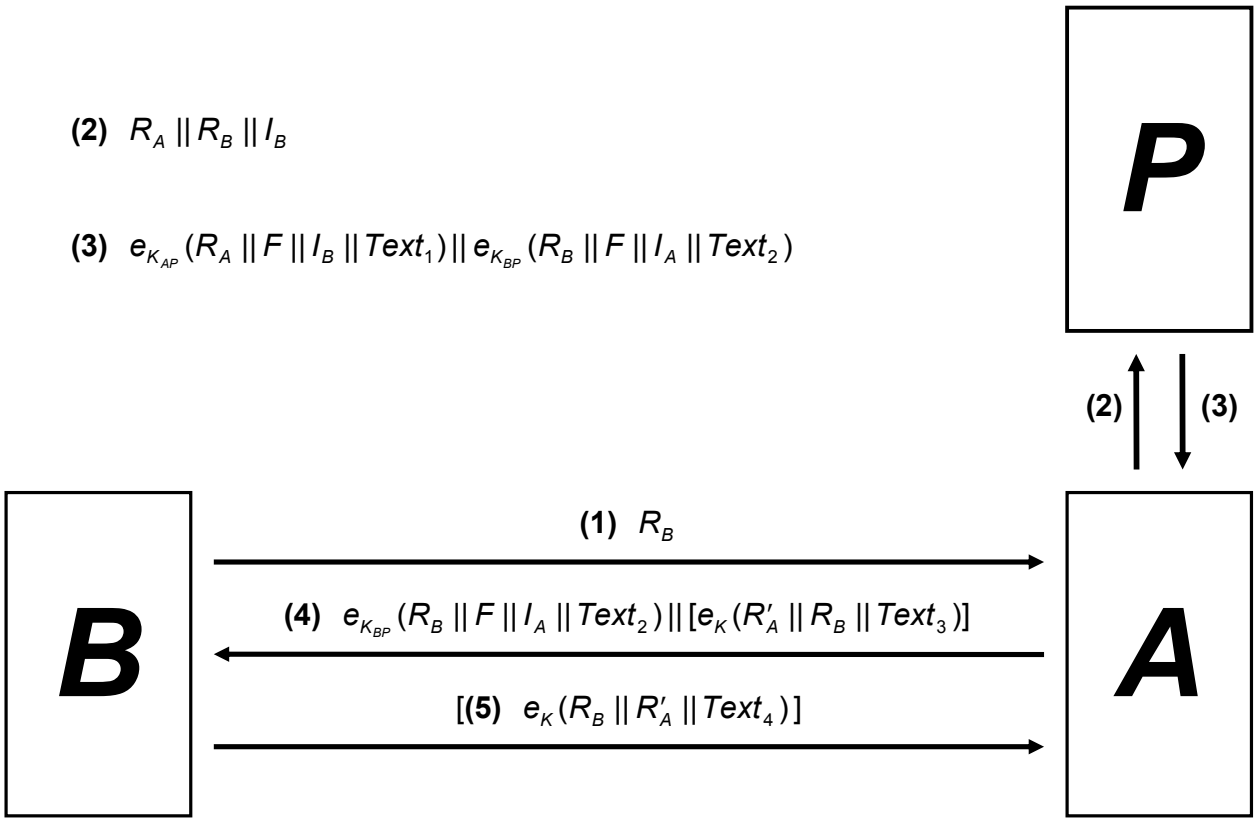

Figure 9 — Mechanism 9

The mechanism involves the following steps (see Figure 9):

1) *B* initiates the mechanism by sending a random number R_B to *A* in message 1.

2) *A* requests keying material from the KDC by sending message 2 to the KDC containing a random number R_A, the random number R_B sent in message 1, and the distinguishing identifier I_B of *B*.

3) The KDC sends message 3 to *A* containing the keying material *F* (made up of a key *K* together with optional data). This message consists of two main parts:

   — $e_{K_{AP}}(R_A \,||\, F \,||\, I_B \,||\, Text_1)$;

   — $e_{K_{BP}}(R_B \,||\, F \,||\, I_A \,||\, Text_2)$.

   i) On receipt of message 3, *A* deciphers the first part, checks that the random number R_A, sent to the KDC in step 2, was used in constructing the first part of message 3, checks the correctness of the distinguishing identifier I_B, and retrieves the key *K*.

4) *A* forwards the second part of message 3 to *B* in message 4. Message 4 optionally also contains a second part, a data field

   $$e_K(R'_A \,||\, R_B \,||\, Text_3)$$

   which incorporates random numbers R_B and R'_A, and enables *B* to check the integrity of the key *K* retrieved from *F*.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

i) On receipt of message 4, *B* deciphers the first part, checks that the random number R_B sent to *A* in step 1 was used in constructing the first part of message 4, checks the correctness of the distinguishing identifier I_A, and obtains the key *K*.

ii) *B* deciphers the second part of message 4, if present, and checks that the random number R_B, sent to *A* in step 1, was used in constructing the second part of message 4.

The fifth step given below is optional; it can be omitted if either no entity authentication or only unilateral authentication is required. This fifth step can only be used if the second part of message 4 is also sent.

5) *B* returns $e_K(R_B \,||\, R'_A \,||\, Text_4)$ to *A* in message 5, thereby acknowledging that it shares the key *K*.

i) On receipt of message 5, *A* deciphers it and checks that the random number R'_A, sent to *B* in step 4, was used in constructing message 5.

NOTE 1 The encryption algorithm *e* used in the optional key confirmation process (i.e., part 2 of message 4 and message 5) may differ from the encryption algorithm (also denoted by *e*) used for key distribution.

NOTE 2 In order to achieve mutual authentication and conformance with the five-pass entity authentication mechanism specified in ISO/IEC 9798-2, the optional message (parts) in steps 4 and 5 need to be included.

7.4 Key Establishment Mechanism 10

Key establishment mechanism 10 provides mutual authentication between *A* and the KDC and unilateral authentication of the KDC to *B*. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that *A*, *B*, and the KDC are able to maintain mechanisms for generating and/or verifying the validity of time stamps *T* or sequence numbers *N*.

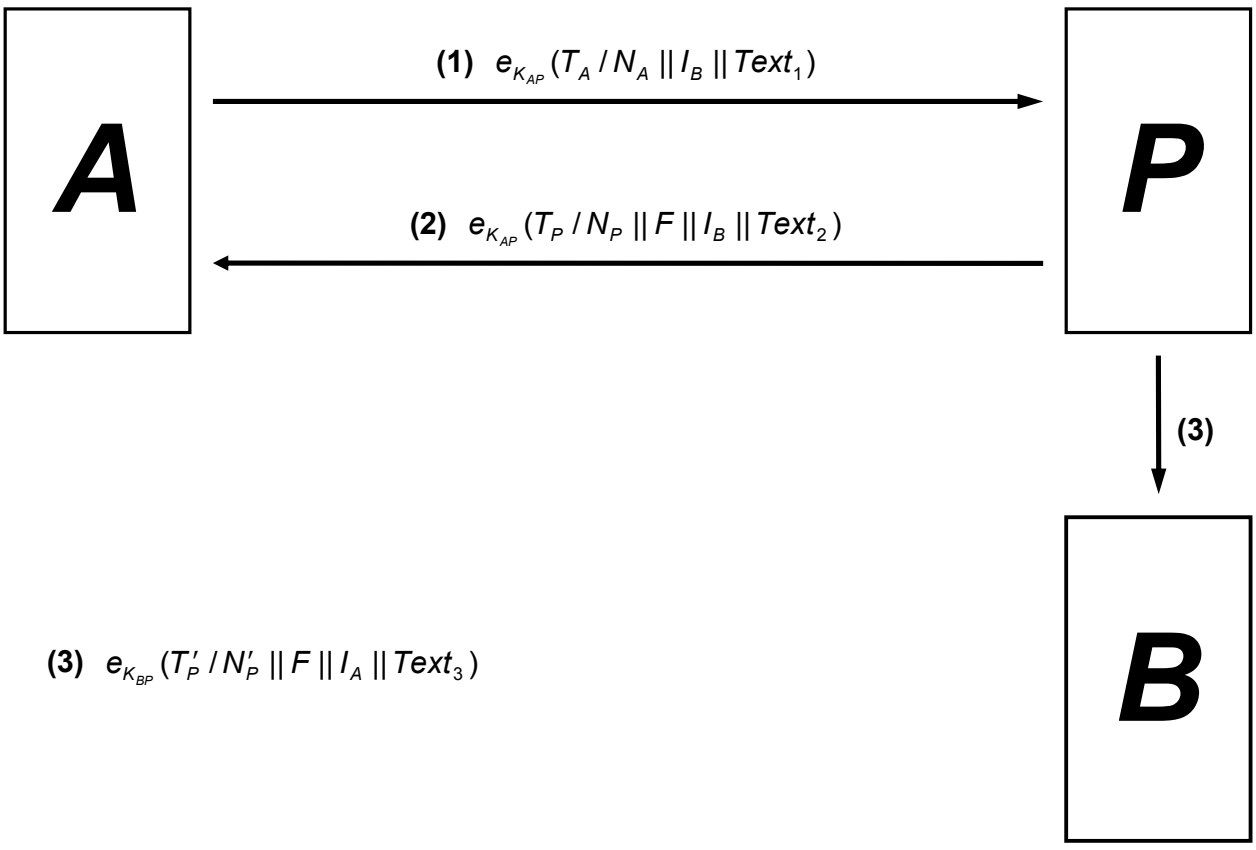

Figure 10 — Mechanism 10

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The mechanism involves the following steps (see Figure 10):

1) *A* requests keying material from the KDC by sending message 1 to the KDC containing a time stamp T_A or sequence number N_A, and the distinguishing identifier I_B of *B*. The data fields are encrypted using the key K_{AP}.

   i) On receipt of message 1, the KDC deciphers it and checks the correctness of the time stamp or sequence number.

2) The KDC sends message 2 to *A* containing a time stamp T_P or sequence number N_P, the distinguishing identifier I_B, and the keying material *F* (made up of a key *K* together with optional data). The data fields are encrypted using the key K_{AP}.

   i) On receipt of message 2, *A* deciphers it, checks the correctness of the distinguishing identifier I_B, checks the correctness of the time stamp or sequence number, and obtains the key *K*.

3) The KDC sends message 3 to *B* containing a time stamp T'_P or sequence number N'_P, the distinguishing identifier I_A, and the keying material *F*. The data fields are encrypted using the key K_{BP}.

   i) On receipt of message 3, *B* deciphers it, checks the correctness of the time stamp or sequence number, and obtains the key *K*. The distinguishing identifier I_A indicates to *B* that the key was requested by *A*.

NOTE 1 The order in which steps 2 and 3 are executed is at the discretion of the implementer.

NOTE 2 Entity authentication between *A* and *B* is not achieved by this mechanism. If entity authentication between *A* and *B* is required, it can be achieved using the key *K* established by the mechanism with one of the mechanisms specified in ISO/IEC 9798-2 or ISO/IEC 9798-4.

NOTE 3 Entity authentication of the requesting entity by the KDC is provided.

8 Mechanisms using a Key Translation Centre

The purpose of a Key Translation Centre (KTC) is to enable a key to be transferred between a pair of entities that both share a key with the KTC.

In this clause, three key establishment mechanisms using a KTC are specified. In each of these mechanisms, one of the two entities (the originator) sends a key *K* to the KTC, encrypted using a key shared between the originator and the KTC. The KTC deciphers the key *K*, and re-enciphers it with a key shared with the second entity (i.e. the ultimate recipient) – this process produces what is known as the translated key. The KTC then either

a) sends the translated key back to the originator who then forwards it to the ultimate recipient, or

b) forwards the translated key to the ultimate recipient directly.

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

a) Entities *A* and *B* share secret keys K_{AP} and K_{BP}, respectively, with a trusted third party *P* that acts as a KTC.

b) The KTC shall have a means of communication with the entity requesting key translation (the originator).

c) The originator shall be able to generate or otherwise acquire a key *K*.

d) Security requirements are concerned with the confidentiality of *K*, and the detection of modification, substitution or replay of keys and messages.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.1 Key Establishment Mechanism 11

In key establishment mechanism 11 the key *K* is provided by entity *A*.

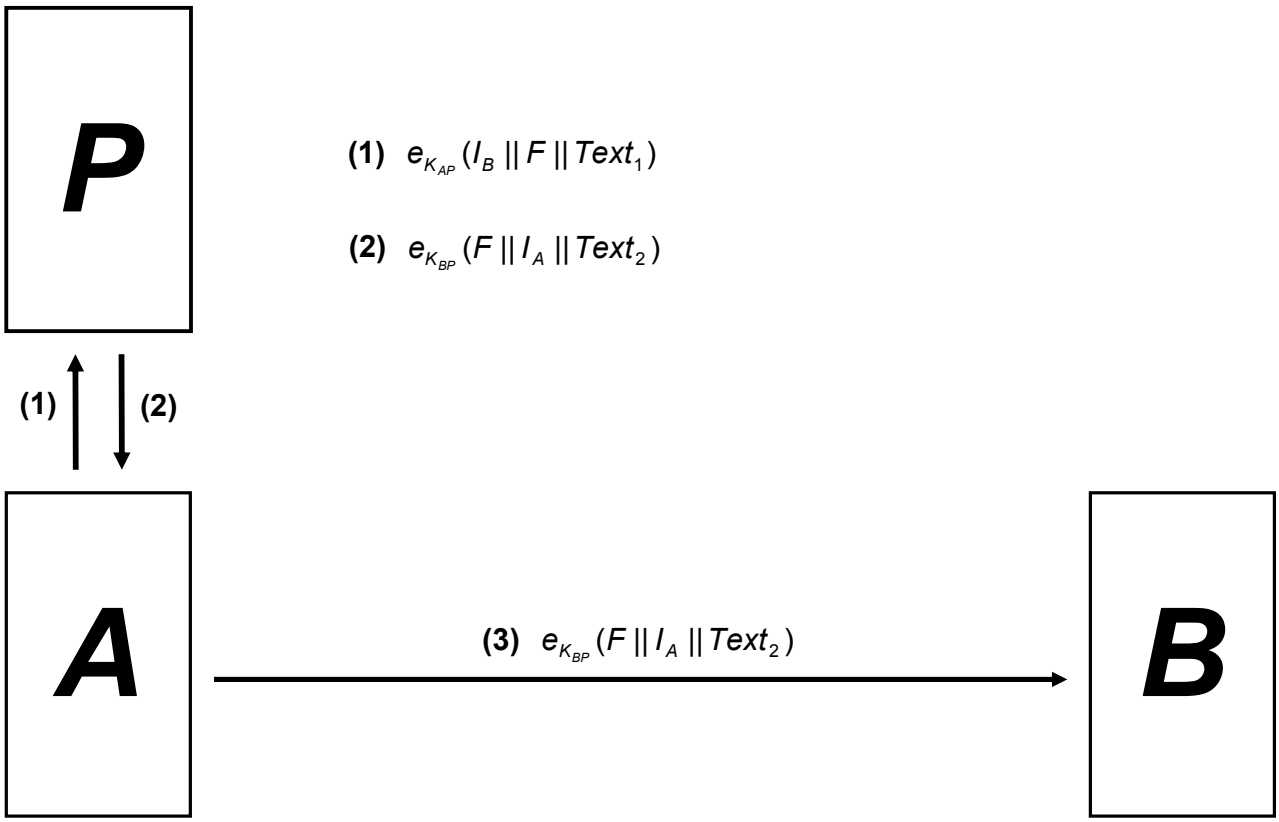

Figure 11 — Mechanism 11

The mechanism involves the following steps (see Figure 11):

1) *A* requests key translation by sending message 1 to the KTC, consisting of $e_{K_{AP}}(I_B \,||\, F \,||\, Text_1)$, encrypted using the key K_{AP}, containing the distinguishing identifier I_B of the second entity *B*, and the keying material *F* (made up of a key *K*, together with optional data).

   i) On receipt of message 1, the KTC deciphers it to obtain *F*, adds the distinguishing identifier I_A, and re-enciphers both using the key K_{BP} to obtain $e_{K_{BP}}(F \,||\, I_A \,||\, Text_2)$.

2) The KTC returns the re-enciphered keying material to *A* in message 2.

3) *A* forwards $e_{K_{BP}}(F \,||\, I_A \,||\, Text_2)$ to *B* in message 3.

   i) On receipt of message 3, *B* deciphers the encrypted part, checks the correctness of the distinguishing identifier I_A, and thus obtains the key *K*.

8.2 Key Establishment Mechanism 12

Key establishment mechanism 12 is derived from, but is not fully compatible with, the four pass authentication mechanism of ISO/IEC 9798-2:1999, clause 6.1. In this mechanism the key *K* is supplied by entity *A*. Uniqueness/timeliness is controlled by time stamps or sequence numbers.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Key establishment mechanism 12 optionally provides mutual authentication between *A* and *B*. The mechanism requires that A, B and the KTC are able to maintain mechanisms for generating and verifying the validity of time stamps *T* or sequence numbers *N*.

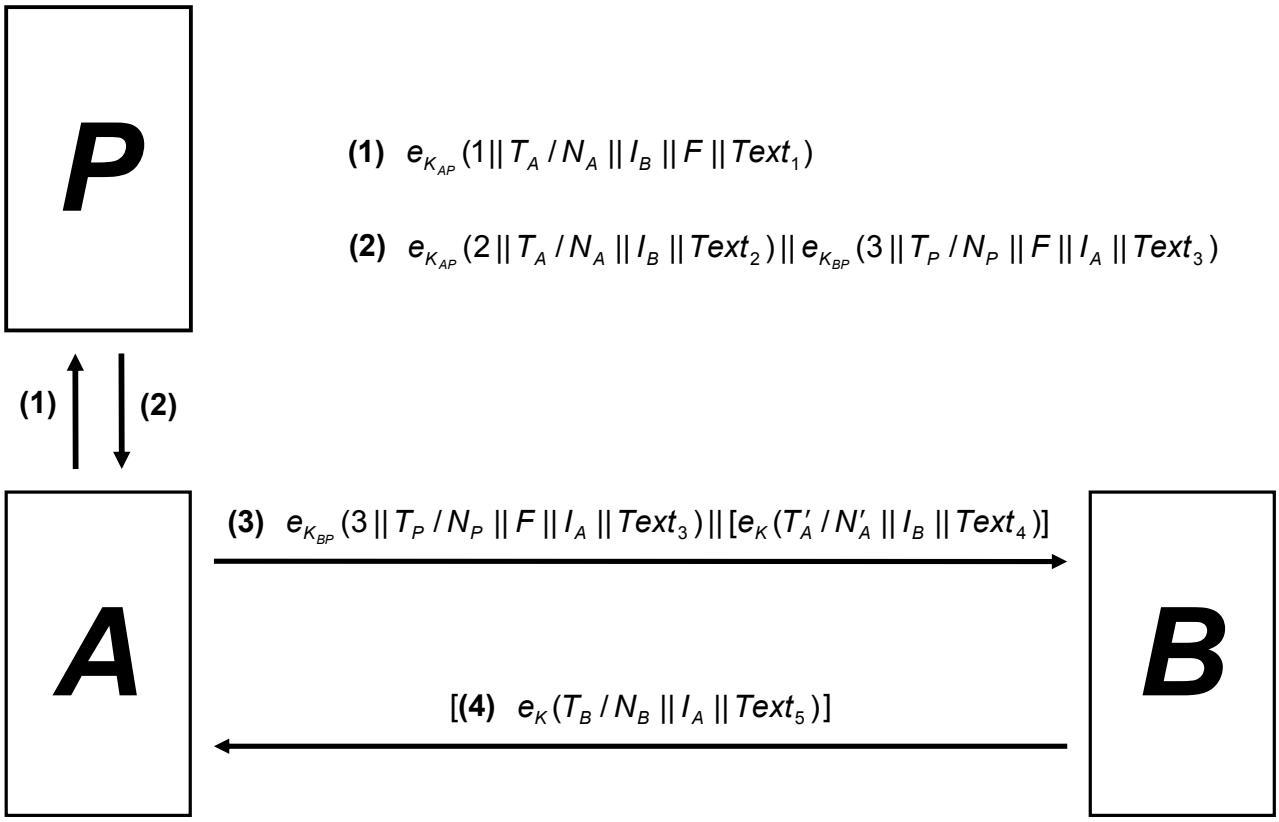

Figure 12 — Mechanism 12

The mechanism involves the following steps (see Figure 12):

1) *A* requests key translation by sending message 1 to the KTC, containing the number 1, a time stamp T_A or sequence number N_A, the distinguishing identifier I_B of *B*, and the keying material *F* (made up of a key *K*, together with optional data). The data fields are encrypted using the key K_{AP}.

   i) On receipt of message 1, the KTC deciphers it, checks the presence of the number 1, checks the time stamp T_A or sequence number N_A, and recovers the encrypted keying material *F*.

2) The KTC sends message 2 to *A*, that consists of two main parts:

   — $e_{K_{AP}}(2 \| T_A / N_A \| I_B \| Text_2)$;

   — $e_{K_{BP}}(3 \| T_P / N_P \| F \| I_A \| Text_3)$.

   i) On receipt of message 2, *A* deciphers the first part, and checks the presence of the number 2 and the distinguishing identifier I_B, and that the time stamp T_A or the sequence number N_A, sent to the KTC in step 1, was used in constructing the first part of message 2.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3) *A* forwards the second part of message 2 to *B* in message 3. Message 3 optionally also contains a second part, a data field

$$e_K(T'_A / N'_A \,||\, I_B \,||\, Text_4)$$

which incorporates a time stamp T'_A or sequence number N'_A, and enables *B* to check the integrity of the key *K* retrieved from *F*.

i) On receipt of message 3, *B* deciphers the first part, checks the presence of the number 3 and the distinguishing identifier I_A, and obtains the key *K*.

ii) *B* deciphers the second part of message 3, if present, and checks the time stamp T'_A or sequence number N'_A and the presence of the distinguishing identifier I_B.

The fourth step given below is optional; it can be omitted if either no entity authentication or only unilateral authentication is required. This fourth step can only be used if the second part of message 3 is also sent.

4) *B* returns $e_K(T_B / N_B \,||\, I_A \,||\, Text_5)$ to *A* in message 4, thereby acknowledging that it shares the key *K*.

i) On receipt of message 4, *A* deciphers it and checks the time stamp T_B or sequence number N_B and the presence of the distinguishing identifier I_A.

NOTE 1 The encryption algorithm *e* used in the optional key confirmation process (i.e., part 2 of message 3 and message 4) may differ from the encryption algorithm (also denoted by *e*) used for key distribution.

NOTE 2 In order to achieve mutual authentication, the optional message (parts) in steps 3 and 4 need to be included.

8.3 Key Establishment Mechanism 13

Key establishment mechanism 13 is derived from, but is not fully compatible with, the five-pass mutual authentication mechanism specified in clause 6.2 of ISO/IEC 9798-2:1999. Key establishment mechanism 13 optionally provides mutual authentication between *A* and *B*. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that *A*, *B* and the KTC are able to generate random numbers.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

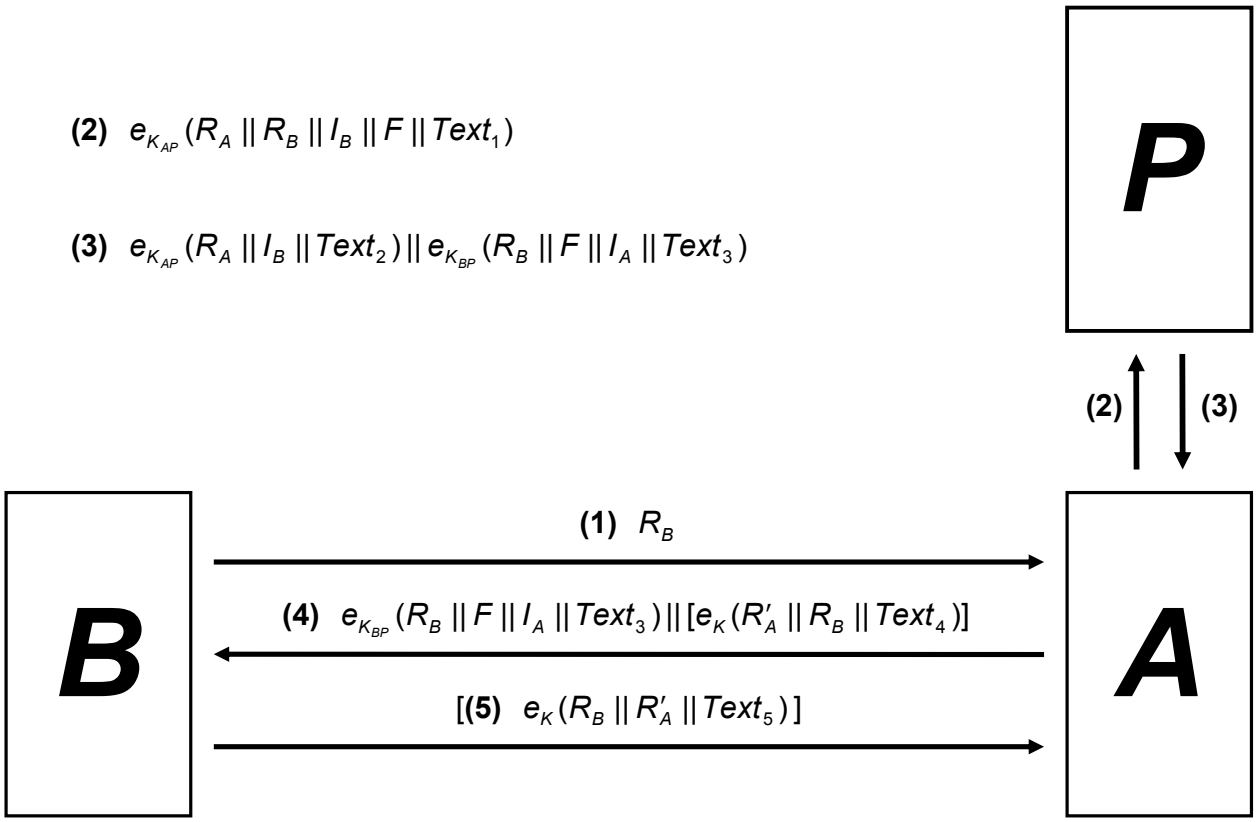

Figure 13 — Mechanism 13

The mechanism involves the following steps (see Figure 13):

1) *B* initiates the mechanism by sending a random number R_B to *A* in message 1.

2) *A* requests key translation by sending message 2 to the KTC containing a random number R_A, the random number R_B sent in message 1, the distinguishing identifier I_B of *B*, and the keying material *F* (made up of a key *K*, together with optional data). The data fields are encrypted using the key K_{AP}.

   i) On receipt of message 2, the KTC deciphers the encrypted keying material *F*, and re-enciphers it together with additional (optional) data fields.

3) The KTC sends message 3 to *A*, that consists of two main parts:

   — $e_{K_{AP}}(R_A \| I_B \| Text_2)$;

   — $e_{K_{BP}}(R_B \| F \| I_A \| Text_3)$.

   i) On receipt of message 3, *A* deciphers the first part, and checks the distinguishing identifier I_B and that the random number R_A, sent to the KTC in step 2, was used in constructing the first part of message 3.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4) *A* forwards the second part of message 3 to *B* in message 4. Message 4 optionally also contains a second part, a data field

$$e_K(R'_A \,||\, R_B \,||\, Text_4)$$

which incorporates random numbers R_B and R'_A, and enables *B* to check the integrity of the key *K* retrieved from *F*.

i) On receipt of message 4, *B* deciphers the first part, checks the distinguishing identifier I_A and that the random number R_B sent to *A* in step 1 was used in constructing the first part of message 4, checks the correctness of the distinguishing identifier I_A, and obtains the key *K*.

ii) *B* deciphers the second part of message 4, if present, and checks that the random number R_B, sent to *A* in step 1, was used in constructing the second part of message 4.

The fifth step given below is optional; it can be omitted if either no entity authentication or only unilateral authentication is required. This fifth step can only be used if the second part of message 4 is also sent.

5) *B* returns $e_K(R_B \,||\, R'_A \,||\, Text_5)$ to *A* in message 5, thereby acknowledging that it shares the key *K*.

i) On receipt of message 5, *A* deciphers it and checks that the random numbers R'_A and R_B, sent to *B* in step 4, were used in constructing message 5.

NOTE 1 The encryption algorithm *e* used in the optional key confirmation process (i.e., part 2 of message 4 and message 5) may differ from the encryption algorithm (also denoted by *e*) used for key distribution.

NOTE 2 In order to achieve mutual authentication, the optional message (parts) in steps 4 and 5 need to be included.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(normative)

ASN.1 module

A.1 Formal definition

```
KeyManagementSymmetricTechniques {
  iso(1) standard(0) key-management(11770) part(2) asn1-module(0)
   key-management-mechanisms(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER

KeyEstablishmentMechanism ALGORITHM ::= {
  ke-mechanism1   |
  ke-mechanism2   |
  ke-mechanism3   |
  ke-mechanism4   |
  ke-mechanism5   |
  ke-mechanism6   |
  ke-mechanism7   |
  ke-mechanism8   |
  ke-mechanism9   |
  ke-mechanism10   |
  ke-mechanism11   |
  ke-mechanism12   |
  ke-mechanism13
}

-- Synonyms --

is11770-2 OID ::= { iso(1) standard(0) key-management(11770) part2(2) }
mechanism OID ::= { is11770-2 mechanisms(1) }

-- Point-to-point key establishment --

ke-mechanism1 OID ::= { mechanism 1 }
ke-mechanism2 OID ::= { mechanism 2 }
ke-mechanism3 OID ::= { mechanism 3 }
ke-mechanism4 OID ::= { mechanism 4 }
ke-mechanism5 OID ::= { mechanism 5 }
ke-mechanism6 OID ::= { mechanism 6 }

-- Mechanisms using a key distribution centre –

ke-mechanism7 OID ::= { mechanism 7 }
ke-mechanism8 OID ::= { mechanism 8 }
ke-mechanism9 OID ::= { mechanism 9 }
ke-mechanism10 OID ::= { mechanism 10 }

-- Mechanisms using a key translation centre –

ke-mechanism11 OID ::= { mechanism 11 }
ke-mechanism12 OID ::= { mechanism 12 }
ke-mechanism13 OID ::= { mechanism 13 }

END -- KeyManagementSymmetricTechniques --
```

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.2 Use of subsequent object identifiers

Each of the authentication mechanisms uses either an encryption algorithm or a key generating function (or both) and any associated parameters. Therefore, the authentication mechanism object identifier may be followed by one of the authentication encryption mechanism algorithm identifiers specified in ISO/IEC 19772 and any associated parameters.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(informative)

Properties of key establishment mechanisms

Table B.1 summarizes the main properties of the key establishment mechanisms specified in this part of ISO/IEC 11770. Options are shown in square parentheses, e.g. mechanism 8 has an optional fourth pass to achieve mutual authentication. The superscripted numbers refer to the list of numbered notes following the table.

Table B.1 — Properties of mechanisms

Mechanism	1	2	3	4	5	6	7	8	9	10	11	12	13
Role of third party	–	–	–	–	–	–	KDC	KDC	KDC	KDC	KTC	KTC	KTC
Number of passes	1	1	1	2	2	3	3	3[4]	4[5]	3	3	3[4]	4[5]
Key control	*A*[1]	*A*	*A*	*A*	*A*/*B*	*A*/*B*	KDC	KDC	KDC	KDC	*A*	*A*	*A*
Key authentication[2]	no	no	yes	yes	yes	yes	no	yes	yes	yes	yes	yes	yes
Replay detection[3]	no	no	*T*/*N*	*R*	*T*/*N*	*R*	no	*T*/*N*	*R*	*T*/*N*	no	*T*/*N*	*R*
Key confirmation[4]	no	no	no	no	no	no	no	opt.	opt.	no	no	opt.	opt.
Entity authentication[5]	no	no	*A*	*A*	*A*&*B*	*A*&*B*	no	opt.	opt.	no	no	opt.	opt.
Complexity[6]	*A*: 1K *B*: 1K	*A*: 1E *B*: 1E	*A*: 1E *B*: 1E	*A*: 1E *B*: 1E	*A*: 1K+2E *B*: 1K+2E	*A*: 1K+2E *B*: 1K+2E	*A*: 1E *B*: 1E *P*: 2E	*A*: 1E [3E] *B*: 1E [3E] *P*: 2E	*A*: 1E [3E] *B*: 1E [3E] *P*: 2E	*A*: 2E *B*: 1E *P*: 3E	*A*: 1E *B*: 1E *P*: 2E	*A*: 2E [4E] *B*: 1E [3E] *P*: 3E	*A*: 2E [4E] *B*: 1E [3E] *P*: 3E

NOTE 1 In mechanism 1, the key *K* is not directly supplied by entity *A*, but is derived from a TVP supplied by *A*.

NOTE 2 Key authentication here means explicit key authentication. All the mechanisms offer at least implicit key authentication, because only parties with knowledge of a specific secret key can recover the key established by the mechanism. However, note also that explicit key authentication does not guarantee that the established key is 'fresh', i.e. not a replay of an 'old' key – in order to achieve key freshness, replay detection is also required.

NOTE 3 *T*/*N* indicates that the mechanism achieves replay detection using time stamps or sequence numbers, and *R* indicates that the mechanism achieves replay detection using random numbers.

NOTE 4 Key confirmation can optionally be achieved for every mechanism using the technique specified in Annex C.

NOTE 5 Entity authentication here only refers to authentication between *A* and *B*. For certain of the mechanisms in Clauses 7 and 8, unilateral or mutual authentication can optionally be achieved.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NOTE 6 Complexity here refers to the number of cryptographic operations to be performed by each entity. After the name of the entity (*A*, *B* or *P*), the number of required applications of a key generating function (K) and/or an encryption/decryption function (E) is listed. The numbers in square brackets indicate the complexity if all the optional steps are performed (otherwise it is assumed that optional steps are not performed).

Distinguishing identifiers are included in the enciphered parts of messages of some if the mechanisms in order to protect against certain types of substitution attacks, i.e. the re-use of legitimate messages sent by *A* or *B* by a third party wishing to masquerade as one of A or *B*. More specifically, in some cases the inclusion of distinguishing identifiers is used to protect against reflection attacks, which are a specific form of substitution attack where a message sent by entity *A* to entity *B* (or vice versa) is sent back to entity *A* by a masquerading third party, in order to convince *A* that it is talking to *B*. In environments where reflection attacks cannot occur, distinguishing identifiers may be omitted. One particular case where reflection attacks cannot occur is when entities *A* and *B* share two different secret keys (unidirectional keys) used separately for messages sent from *A* to *B*, and for messages sent from *B* to *A*.

For further details of such attacks and countermeasures see, for example, [10] or [11].

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(informative)

Auxiliary techniques

C.1 Data integrity

C.1.1 Integrity of individual messages

In the key establishment mechanisms specified in this part of ISO/IEC 11770, the text fields may be used to ensure data integrity. If a hash-function is used for this purpose, then the hash-code shall either be appended to the data before encryption or placed in a plaintext field. If a message authentication code is used, then the MAC may be calculated with an additional (distinct) key established by the mechanism. In all cases, the recipient of K can check the integrity of the received message and of the retrieved key.

More specifically, if a hash-function h is used to ensure the data integrity of the message

$$e_{K_{AB}}(... \,||\, K \,||\, \text{Text1}),$$

then the field Text1 may be instantiated as

$$\text{Text1}^* \,||\, h(... \,||\, K \,||\, \text{Text1}^*)$$

where $h(X)$ denotes the hash-code computed on data X. Alternatively, if a MAC function is used to ensure the data integrity of this message, then the plaintext field

$$\text{MAC}_{K^*}(e_{K_{AB}}(... \,||\, K \,||\, \text{Text1}))$$

may be appended to the message, where K^* denotes a key distinct from K.

However, it is recommended that an authenticated encryption mode (as standardised in ISO/IEC 19772) should be used to instantiate e, in which case no separate integrity mechanism is needed.

C.1.2 Integrity of two-part messages

When two concatenated enciphered data fields are returned by a KDC or KTC (as in mechanisms 7, 8, 9, 12 and 13), assumptions a)1) and a)2) of clause 5 are not always equivalent. Assumption a)1) can only guarantee the integrity of the two individual parts, whereas assumption a)2) can, in addition, guarantee the integrity of the message as a whole. Only in this latter case is it possible to unambiguously detect the link on which an active attack is being performed.

As an example, consider a mechanism where a message of the form

$$e_{K_{AP}}(X) \,||\, e_{K_{BP}}(Y)$$

is sent from the trusted third party P to A. In order to detect a modification of any part of the message whilst in transit between P and A, a plaintext field of the form:

$$\text{MAC}_{K^*_{AP}}(e_{K_{AP}}(X) \,||\, e_{K_{BP}}(Y)) \,||\, \text{MAC}_{K^*_{BP}}(e_{K_{BP}}(Y))$$

may be appended to the message, where K^*_{AP} and K^*_{BP} denote keys distinct from K_{AP} and K_{BP}.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.2 Key calculation

Key calculation is a technique for obtaining a key from two or more data items, at least one of which is secret, using a key generating function *f* (which may be publicly known). Examples of such functions are as follows:

a) The bitwise modulo 2 sum of two secret data items F_1 and F_2, i.e.

$$K = f(F_1, F_2) = F_1 \oplus F_2.$$

b) Applying a hash-function *h*, as defined in ISO/IEC 10118, to the concatenation of two data items F_1 and F_2, i.e.

$$K = f(F_1, F_2) = h(F_1 \,||\, F_2).$$

In some situations it is desirable for a key generating function to be one-way, i.e. given knowledge of the output it shall be computationally infeasible to obtain any information regarding the secret input parameter(s). Note that example function a) above is not one-way in this sense, since knowledge of the output *K* immediately yields potentially useful information regarding the two secret input parameters F_1 and F_2. In key establishment mechanism 1 it is necessary for the key generating function *f* to have the one-way property, so that if the key *K* established using this mechanism is compromised, then the shared secret key K_{AB} (which may be a 'long term' shared secret) is not compromised.

Further information on key derivation functions can be obtained from NIST SP 800-57 Part 1, section 8.2.4. This document can be found at:

http://www.csrc.nist.gov/publications/nistpubs.

C.3 Key confirmation

Key confirmation is the property whereby one entity has assurance that another identified entity is in possession of the correct key. An example of how entity *X* may provide key confirmation to entity *Y* regarding key *K*, is for *X* to send to *Y* the message

$$e_K(\text{TVP} \,||\, \text{Text})$$

where TVP denotes a time variant parameter that can be verified by entity *Y*.

C.4 Combination of key establishment and entity authentication

In order to provide entity authentication, the key establishment mechanisms in this part of ISO/IEC 11770 may be combined with an entity authentication mechanism as specified in ISO/IEC 9798-2 or ISO/IEC 9798-4. The example given below shows the result if the combination of key establishment mechanism 1 with the two-pass unilateral authentication mechanism specified in clause 5.1.2 of ISO/IEC 9798-4:1999.

The mechanism involves the following steps:

1) *B* generates a random number R_B and transfers it to *A* in message 1.

   i) Both A and B then derive the key *K* from R_B using a MAC function *v* with key K_{AB}:

$$K = v_{K_{AB}}(R_B).$$

2) *A* returns $v_{K_{AB}}(R_B \,||\, I_B)$ to *B* in message 2, i.e. a MAC computed on the received random number R_B and the distinguishing identifier I_B.

   i) On receipt of message 2, *B* checks that its distinguishing identifier I_B and the random number R_B, sent to *A* in step 1, were used in constructing message 2.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO 8732:1988, *Banking — Key management (wholesale)*

[2] ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

[3] ISO/IEC 9798 (all parts), *Information technology — Security techniques — Entity authentication*

[4] ISO/IEC 10116:2006, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

[5] ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

[6] ISO 11568-2:2005, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

[7] ISO/IEC 18031:2005, *Information technology — Security techniques — Random bit generation*

[8] ISO/IEC 18033 (all parts), *Information technology — Security techniques — Encryption algorithms*

[9] ISO/IEC 19772 (to be published), *Information technology — Security techniques — Authenticated encryption*

[10] BOYD, C. and MATHURIA, A. *Protocols for Authentication and Key Establishment*. Springer, 2003

[11] MENEZES, A., VAN OORSCHOT, P. and VANSTONE, S. *Handbook of Applied Cryptography*. CRC Press, 1997

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 27 pages

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale