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)

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 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.

a) 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.

b) 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.

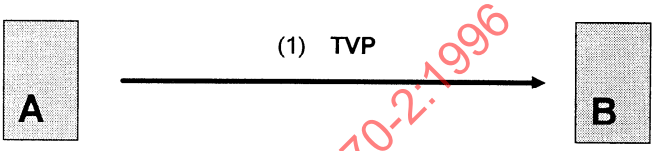

Figure 1 - Mechanism 1

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:

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

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.

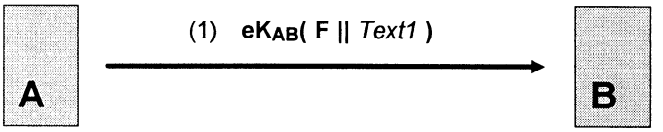

Figure 2 - Mechanism 2

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.

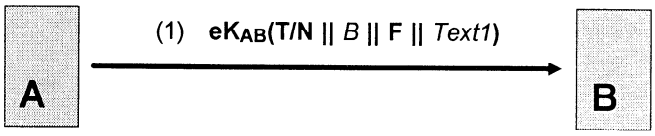

Figure 3 - Mechanism 3

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.

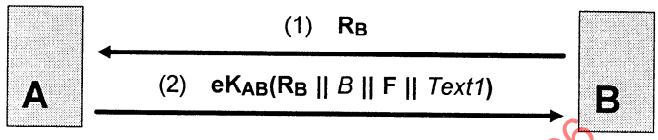

Figure 4 - Mechanism 4

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

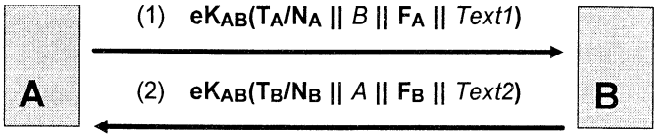

Figure 5 - Mechanism 5

distinguishing identifier B is optional. The data fields are enciphered with K_{AB}.

(1a) On receipt of message (1), B deciphers the enciphered 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 or sequence number T_B/N_B, the distinguishing identifier A, and the keying material F_B. The inclusion of the distinguishing identifier A is optional. The data fields are enciphered with K_{AB}.

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

(2b) Both A and B derive the key K by using a key generating function f with inputs the secret keying material fields F_A and F_B:

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

See Annex B for examples of possible key generating functions.

NOTES

1 - In key establishment mechanism 5, either of the two keying material fields F_A or F_B may be empty, but not both.

2 - Distinguishing identifier B is included in step (1) to prevent the re-use of this message by an adversary masquerading as B. For similar reasons, distinguishing identifier A is present in step (2). In environments where such attacks cannot occur, one or both of the identifiers may be omitted.

5.6 Key Establishment Mechanism 6

Key establishment mechanism 6 is derived from the three pass authentication mechanism of ISO/IEC 9798-2, clause 5.2.2. This mechanism enables both A and B to contribute part of the established key K. Key establishment mechanism 6 provides mutual authentication, i.e., both communicating entities are authenticated by the

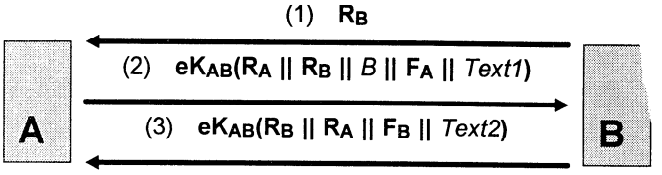

Figure 6 - Mechanism 6

mechanism. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that both A and B are able to generate random numbers.

Steps:

(1) B sends A a random number R_B.

(2) A sends B a random number R_A, the received number R_B, the distinguishing identifier B, and the keying material F_A. 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, 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. The data fields are enciphered with K_{AB}.

(3a) On receipt of message (3), A deciphers the enciphered part and checks that the random number R_A, sent to B in step (2), was used in constructing message (3).

(3b) Both A and B derive the key K by using a key generating function f with inputs the secret keying material fields F_A and F_B:

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

See Annex B for examples of possible key generating functions.

NOTES

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

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

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

6 Key Distribution Centre

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

In this clause, four key establishment mechanisms 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 then can be sent by the requesting entity to the ultimate recipient. For the last mechanism the KDC generates or acquires the key K and sends it directly to each communicating entity. The messages are protected using the keys which the KDC shares with the corresponding entities. If required, authentication of the requesting entity by the KDC may be ensured by the inclusion of a MAC in a plaintext text field of the requesting message.

For all these mechanisms, only the KDC has to have the ability to generate or otherwise acquire keys. Following the distribution of a key by the KDC, the two entities may operate in a point-to-point mode.

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

- There is a trusted third party T, the Key Distribution Centre, with which A and B share secret keys, K_{AT} and K_{BT} respectively. The KDC shall be able to generate or otherwise acquire a key K.
- The KDC is on-line with the entity requesting a key.
- Security requirements are concerned with the confidentiality of K, modification and replay detection, and the detection of substitution attacks.

6.1 Key Establishment Mechanism 7

In key establishment mechanism 7 the key K is supplied by the Key Distribution Centre. The mechanism provides no authentication of the key K established by the mechanism.

Steps:

(1) A requests keying material from the KDC by sending a message to the KDC that contains the distinguishing identifier of the recipient B.

(2) The KDC sends a protected message to A that contains the keying material F (key K and optional data). This message consists of 2 main parts:

(a) $eK_{AT}(F \| B \| \textit{Text1})$

(b) $eK_{BT}(F \| A \| \textit{Text2})$

(2a) On receipt of message (2), A deciphers part (a), checks the correctness of the distinguishing identifier and obtains the key K.

(3) A forwards part (b) of message (2) to B.

(3a) On receipt of message (3), B deciphers the enciphered part, checks the correctness of the distinguishing identifier and also obtains the key K.

6.2 Key Establishment Mechanism 8

Key establishment mechanism 8 is derived from the four pass authentication mechanism of ISO/IEC 9798-2, clause 6.1. In this mechanism the key K is supplied by the Key Distribution Centre. Key establishment mechanism 8 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. 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.

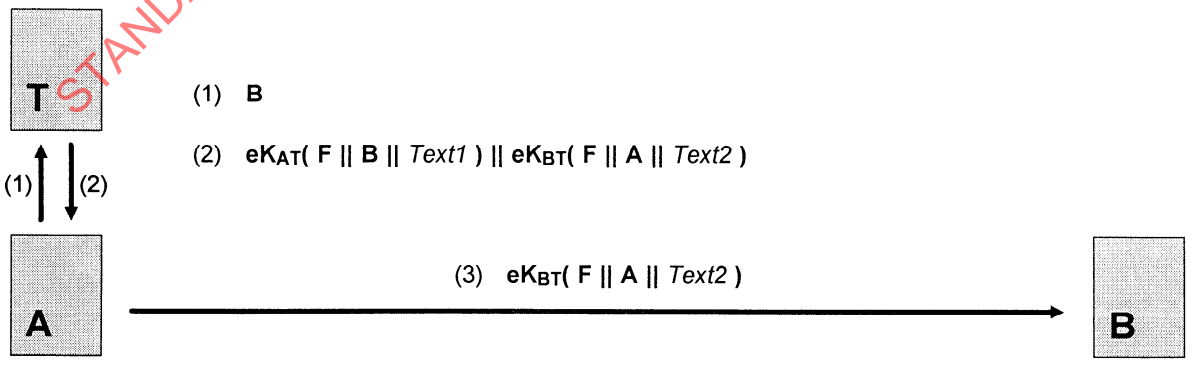

Figure 7 - Mechanism 7

Steps:

(1) A requests keying material from the KDC by sending a message to the KDC that contains a time variant parameter TVP_A (a random number, time stamp, or sequence number) and the distinguishing identifier of the recipient B.

(2) The KDC sends a protected message to A that contains the keying material F (key K and optional data). This message consists of 2 main parts:

(a) $eK_{AT}(TVP_A \| F \| B \| Text1)$

(b) $eK_{BT}(T_T/N_T \| F \| A \| Text2)$

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

(3) A forwards part (b) of message (2) to B. Message (3) optionally contains a data field $eK(T_A/N_A \| B \| Text3)$ which enables B to check the integrity of the key K retrieved from F.

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

(3b) B deciphers the second part of message (3), if present, and checks the correctness of the time variant parameter and of its distinguishing identifier.

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

(4) B returns $eK(T_B/N_B \| A \| Text4)$ to A thereby acknowledging that it shares the key K.

(4a) On receipt of message (4), A deciphers it and checks the correctness of the time variant parameter and of the distinguishing identifier.

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted by e) used for key distribution.

2 - To achieve mutual authentication and conformance with the four pass authentication mechanism specified in ISO/IEC 9798-2 the options in steps (3) and (3b) and optional steps (4) and (4a) need to be included.

6.3 Key Establishment Mechanism 9

Key establishment mechanism 9 is derived from the five pass authentication mechanism of ISO/IEC 9798-2, clause 6.2. In this mechanism the key K is supplied by the Key Distribution Centre. Key establishment mechanism 9 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that A, B and the KDC are able to generate random numbers.

Steps:

(1) B initiates the mechanism by sending a random number R_B to A.

(2) A requests keying material from the KDC by sending a message to the KDC that contains a random number R_A, the random number R_B, and the distinguishing identifier of B.

(3) The KDC sends a protected message to A that contains the keying material F (key K and optional data). This message consists of 2 main parts:

(a) $eK_{AT}(R_A \| F \| B \| Text1)$

(b) $eK_{BT}(R_B \| F \| A \| Text2)$

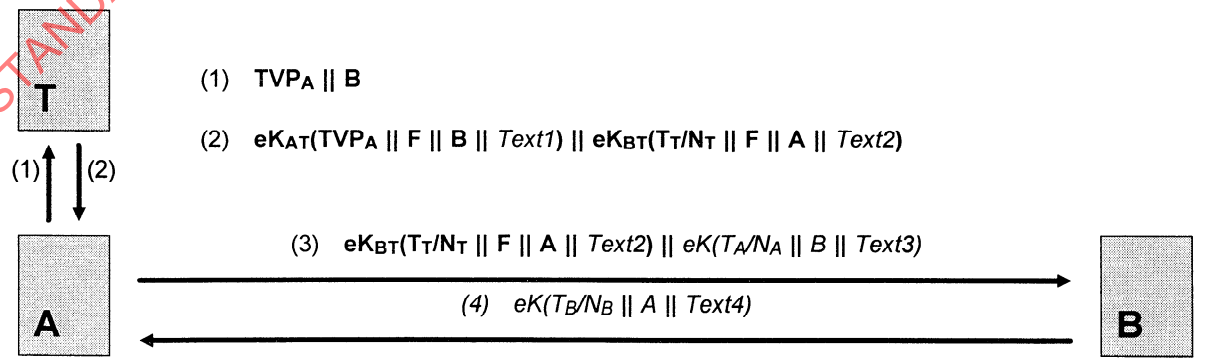

Figure 8 - Mechanism 8

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

(4) A forwards part (b) of message (3) to B. Message (4) optionally contains a data field $eK(R'_A \| R_B \| Text3)$ which incorporates random numbers R_B and R'_A and enables B to check the integrity of the key K retrieved from F.

(4a) 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 message (4), and obtains the key K. The distinguishing identifier indicates to B that the key was requested by A.

(4b) 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).

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

(5) B returns $eK(R_B \| R'_A \| Text4)$ to A thereby acknowledging that it also shares the key K. Step (5) requires the option described in step (4).

(5a) 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).

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted by e) used for key distribution.

2 - To achieve mutual authentication and conformance with the five pass authentication mechanism specified in ISO/IEC 9798-2 the options in steps (4) and (4b) and optional steps (5) and (5a) need to be included.

6.4 Key Establishment Mechanism 10

In key establishment mechanism 10 the KDC distributes the keying material directly to both entities. The mechanism provides mutual authentication between A and the KDC and unilateral authentication from 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 or verifying the validity of time stamps T or sequence numbers N.

Steps:

(1) A requests keying material from the KDC by sending a message to the KDC that contains a time stamp or sequence number T_A/N_A, and the distinguishing identifier of the recipient B. The data fields are enciphered with K_{AT}.

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

(2) The KDC returns a message to A that contains a time time stamp or sequence number T_T/N_T, the distinguishing identifier of B, and the keying material F. The data fields are enciphered with K_{AT}.

(2a) On receipt of message (2), A deciphers it, checks the correctness of the time stamp or sequence number, and obtains the key K.

(3) The KDC sends a message to B that contains a time stamp or sequence number T'_T/N'_T, the distinguishing identifier of A, and the keying material F. The data fields are enciphered with K_{BT}.

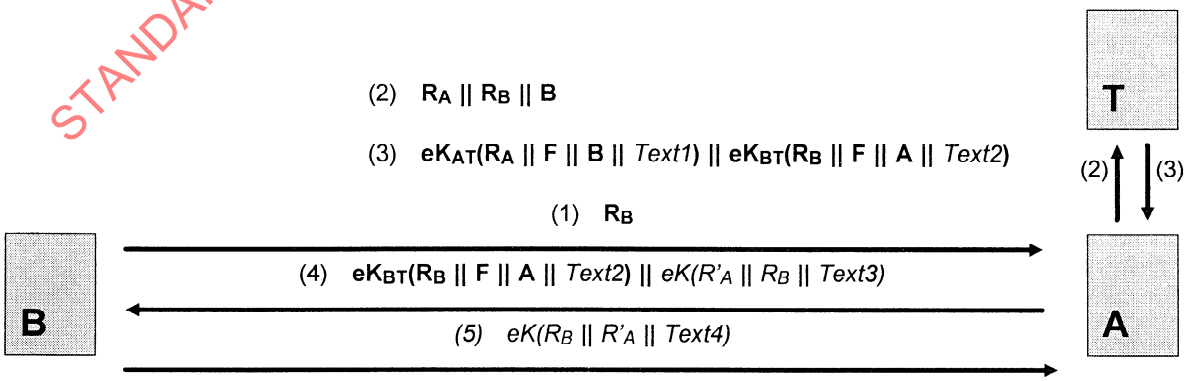

Figure 9 - Mechanism 9

(3a) 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 of A indicates to B that the key was requested by A.

NOTES

1 - The order of steps 2 and 3 is optional.

2 - There is no authentication between A and B. After key establishment, entity authentication can be achieved using one of the mechanisms of ISO/IEC 9798-2 or ISO/IEC 9798-4.

7 Key Translation Centre

The purpose of a Key Translation Centre is to translate keys between entities that each share a key with the KTC. One of the entities (the originator) sends a key K to the KTC enciphered with 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 (the ultimate recipient); this process produces 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.

In an environment where a KTC is used the originator shall have the ability to generate or otherwise acquire keys.

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

- There is a trusted third party, T, the Key Translation Centre, with which A and B share secret keys, K_{AT} and K_{BT} respectively.
- The KTC is on-line with at least one of the entities, usually the originator.
- The originator is able to generate or otherwise acquire a secret key K.
- Security requirements are concerned with the confidentiality of K, modification and replay detection, and the detection of substitution attacks.

7.1 Key Establishment Mechanism 11

In key establishment mechanism 11 the key K is supplied by entity A. The mechanism provides no authentication of the key K established by the mechanism.

Steps:

(1) A requests a key translation by sending a message to the KTC that is enciphered with K_{AT} and contains the distinguishing identifier of the recipient B, and the keying material F (key K and optional data).

(1a) On receipt of message (1), the KTC deciphers F, adds the distinguishing identifier A and re-enciphers both with K_{BT}.

(2) The KTC returns the re-enciphered keying material to A.

(3) A forwards the protected part of message (2) to B.

(3a) On receipt of message (3), B deciphers the enciphered part and thus obtains the key K. The distinguishing identifier of A indicates to B that the key was requested by A.

7.2 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 9798-2:1994, clause 6.1. In this mechanism the key K is supplied by entity A.

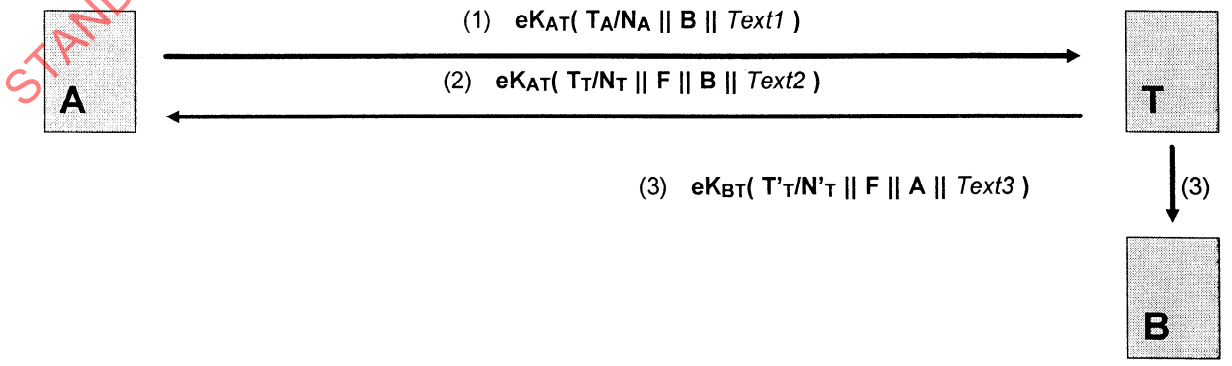

Figure 10 - Mechanism 10

Uniqueness/timeliness is controlled by time stamps or sequence numbers.

Key establishment mechanism 12 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. 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.

Steps:

(1) A requests a key translation by sending a message to the KTC that consists of a time variant parameter TVP_A (a random number, time stamp or sequence number), the distinguishing identifier of the recipient B, and the keying material F (key K and optional data). The data fields are enciphered with K_{AT}.

(1a) On receipt of message (1), the KTC deciphers the enciphered keying material F and re-enciphers it together with additional data fields.

(2) The KTC returns a message to A that consists of 2 main parts:

(a) $eK_{AT}(TVP_A \| B \| \textit{Text2})$

(b) $eK_{BT}(T_T/N_T \| F \| A \| \textit{Text3})$

(2a) On receipt of message (2), A deciphers the first part and checks the distinguishing identifier and that the time variant parameter TVP_A, sent to the KDC in step (1), was used in constructing message (2).

(3) A forwards part (b) of message (2) to B. Message (3) optionally contains a data field $eK(T_A/N_A \| B \| \textit{Text4})$ which enables B to check the integrity of the key K retrieved from F.

(3a) On receipt of message (3), B deciphers the first part, checks the correctness of the time stamp or sequence number, and obtains the key K. The distinguishing identifier indicates to B that the key translation was requested by A.

(3b) B deciphers the second part of message (3), if present, and checks the correctness of the time variant parameter and of its distinguishing identifier.

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

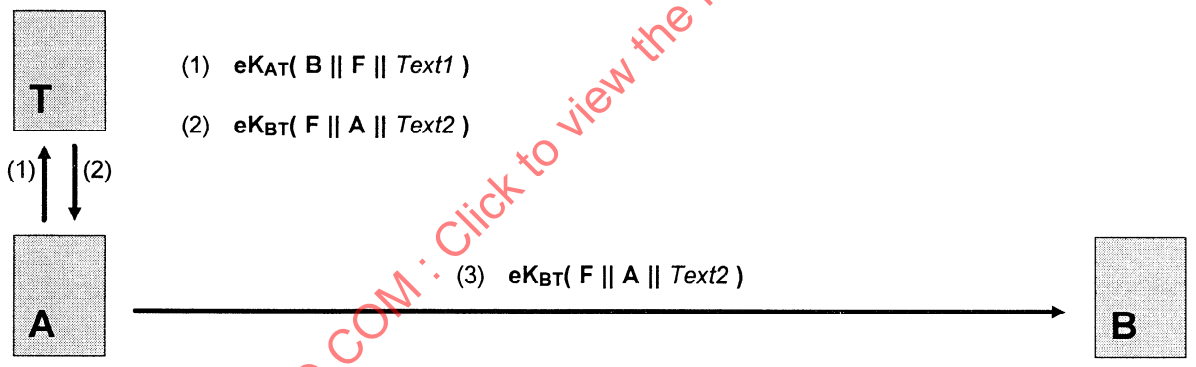

Figure 11 - Mechanism 11

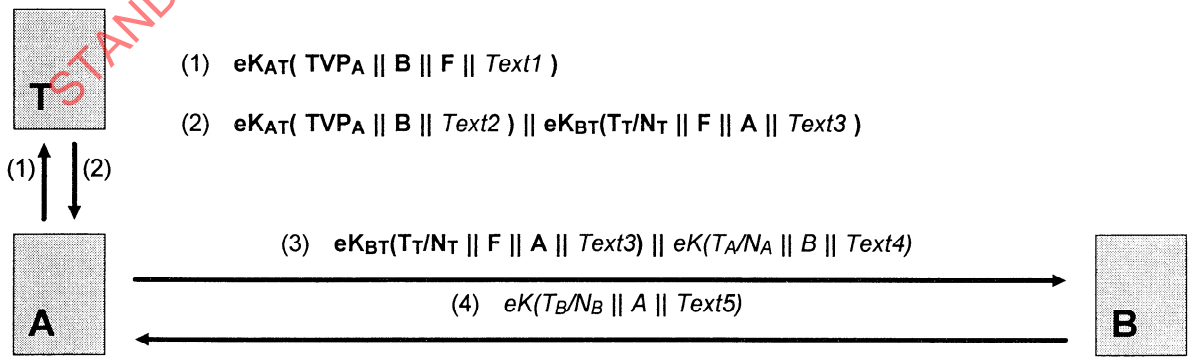

Figure 12 - Mechanism 12

(4) B returns eK(T_B/N_B || A || *Text5*) to A thereby acknowledging that it shares the key K.

(4a) On receipt of message (4), A deciphers it and checks the correctness of the time variant parameter and of its distinguishing identifier.

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted by e) used for key distribution.

2 - To achieve mutual authentication the options in steps (3) and (3b) and optional steps (4) and (4a) need to be included.

7.3 Key Establishment Mechanism 13

Key establishment mechanism 13 is derived from, but is not fully compatible with, the five pass authentication mechanism of ISO/IEC 9798-2:1994, clause 6.2. In this mechanism the key K is supplied by entity A. Key establishment mechanism 13 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that A, B and the KTC are able to generate random numbers.

Steps:

(1) B initiates the mechanism by sending a random number R_B to A.

(2) A requests a key translation by sending a message to the KTC that contains a random number R_A, the random number R_B, the distinguishing identifier of the originator B, and the keying material F (key K and optional data). The data fields are enciphered with K_{AT}.

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

(3) The KTC returns a message to A that consists of 2 main parts:

(a) $eK_{AT}(R_A \| B \| Text2)$

(b) $eK_{BT}(R_B \| F \| A \| Text3)$

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

(4) A forwards part (b) of message (3) to B. Message (4) optionally contains a data field $eK(R'_A \| R_B \| Text4)$ which enables B to check the integrity of the key K retrieved from F.

(4a) On receipt of message (4), B deciphers its first part and obtains the key K. If the random number R_B sent to A in step (1), was used in constructing the first part of message (4), the message indicates to B that it was sent by A as a reply to message (1).

(4b) If present, B deciphers the second part of message (4) and checks that the random number R_B sent to A in step (1), was also used in constructing the second part of message (4).

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

(5) B returns $eK(R_B \| R'_A \| Text5)$ to A thereby acknowledging that it also shares the key K. Step (5) requires the option described in step (4).

(5a) On receipt of message (5), A checks that the random number R'_A sent to B in step (4), was used in constructing message (5).

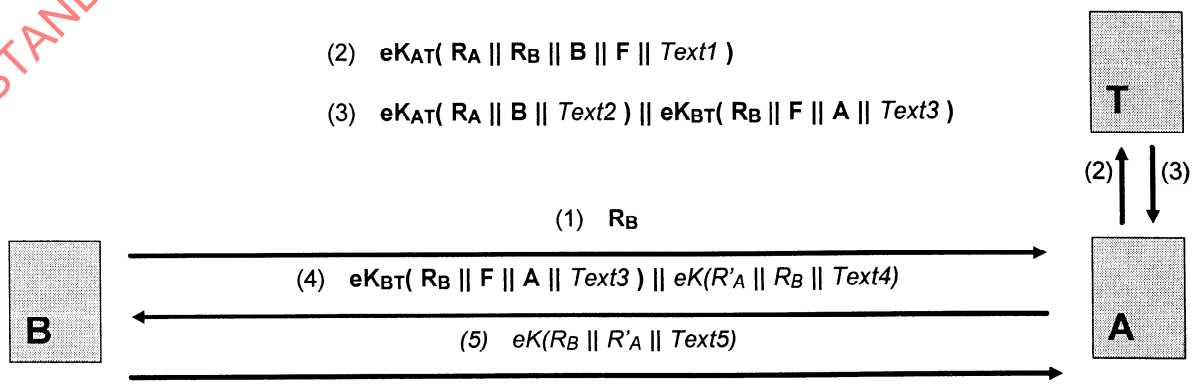

Figure 13 - Mechanism 13

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted by e) used for key distribution.

2 - To achieve mutual authentication the options in steps (4) and (4b) and optional steps (5) and (5a) need to bc included.

Annex A
(informative)

Properties of Key Establishment Mechanisms

Table A.1 summarizes major properties of the key establishment mechanisms specified in this part of ISO/IEC 11770. Options are shown in parenthesis, e.g., mechanism 8 has an optional fourth pass to achieve mutual entity authentication.

Table A.1

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	entity A[1)]	entity A	entity A	entity A	A/B	A/B	KDC	KDC	KDC	KDC	entity A	entity A	entity A
Key authentication[2)]	no	no	yes	yes	yes	yes	yes	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.

NOTES

1 - In case of mechanism 1, the key K is not directly supplied by entity A but derived from a time variant parameter provided by A.

2 - Key authentication in this context refers to explicit key authentication and includes both key integrity and key origin authentication. All the mechanisms offer at least implicit key authentication, because only parties with knowledge of a specific secret key can recover the correct key.

3 - T/N denotes replay detection by using time stamps or sequence numbers while R denotes replay detection by using random numbers.

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

5 - Entity authentication in this context only refers to authentication between entities A and B. In case of mechanisms 8, 9, 12 and 13, unilateral or mutual authentication can optionally be achieved.

Distinguishing identifiers are included in the enciphered parts of messages of some of the mechanisms to protect against certain types of substitution attacks, i.e., the re-use of legitimate messages of 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 one entity (A say) is sent back to that entity by a masquerading third party, in order to convince A that it is communicating with a legitimate entity. In environments where reflection attacks cannot occur, and where the text accompanying the message description makes it clear that this is allowed, distinguishing identifiers may be omitted. One particular case where reflection attacks cannot occur is

when the authenticating 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.