INTERNATIONAL STANDARD

ISO/IEC 11770-3

Third edition
2015-08-01

AMENDMENT 1
2017-11

Information technology — Security techniques — Key management —

Part 3: Mechanisms using asymmetric techniques

AMENDMENT 1: Blinded Diffie-Hellman key agreement

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

Partie 3: Mécanismes utilisant des techniques asymétriques

AMENDEMENT 1: Accord de clés Diffie-Hellman aveugle

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

Reference number
ISO/IEC 11770-3:2015/Amd.1:2017(E)

© ISO/IEC 2017

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 11770 series can be found on the ISO wesite.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

© ISO/IEC 2017 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

Information technology — Security techniques — Key management —

Part 3:
Mechanisms using asymmetric techniques

AMENDMENT 1: Blinded Diffie-Hellman key agreement

Normative references

Add the following normative references:

ISO/IEC 11770-6, *Information technology — Security techniques — Key management — Part 6: Key derivation*

ISO/IEC 19772, *Information technology — Security techniques — Authenticated encryption*

10.2, first sentence

Modify the first sentence to be as follows:

The provisions in this subclause apply to key agreement mechanisms 11.1 to 11.11, 11.13 and 11.14, all of which specify mechanisms for key agreement between two parties.

Clause 11

Add the following after 11.12:

11.13 Key agreement mechanism 13

This key agreement mechanism, known as "2-pass blinded Diffie-Hellman", establishes a shared secret key in two passes between entities A and B with unilateral implicit key authentication. The following requirements shall be satisfied.

— Entity A has a private key agreement key h_A in S_1 and a public key agreement key $P_A = \mathrm{F}(h_A, G)$ in S_2, where S_1 and S_2 are the sets introduced in 10.2.

— Entity B has access to the credentials necessary to authenticate the public key agreement key of entity A. This may be achieved using the mechanisms described in Clause 13, but to ensure the privacy property of unlinkability, any identifiers of entity A and any credentials unique to entity A that are sent from entity A to entity B are sent encrypted using a key derived from the shared key, for example, as shown in Text1 in the description below.

— Key derivation shall comply with ISO/IEC 11770-6 (see also Annex C) and encryption shall use an authenticated encryption method chosen from ISO/IEC 19772.

— Random number generation shall comply with ISO/IEC 18031.

Key token construction (B1) Entity B randomly and secretly generates r_B in S_1, computes its ephemeral public key $P_B = \mathrm{F}(r_B, G)$ in S_2, constructs the key token $KT_{B1} = P_B$, and sends it to entity A.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

© ISO/IEC 2017 – All rights reserved

Key token construction, key construction and encryption (A1) Entity A randomly and secretly generates r_A in S_1, and constructs the key token $KT_{A1} = F(r_A, P_A)$.

Entity A computes the shared secret key as $K = F(r_A, F(h_A, KT_{B1}))$.

Entity A derives key K_{AB} from K using an agreed key derivation function and uses an authenticated encryption algorithm AuthEnc to compute $E = \text{AuthEnc\_}K_{AB}(r_A, P_A, \text{Text1})$ and sends this and the key token KT_{A1} to entity B.

Key construction, decryption and checking (B2) Entity B computes the shared secret key as $K = F(r_B, KT_{A1})$.

Entity B derives key K_{AB} from K using the agreed key derivation function and uses AuthEnc and E to recover r_A and P_A and check that $KT_{A1} = F(r_A, P_A)$.

NOTE 1 A security proof for the 3-pass protocol (Mechanism 14) is provided in Reference [38], and is extended to a proof for the 2-pass protocol in Reference [41]. The security proof requires the use of unidirectional authenticated encryption keys and the inclusion of state information such as message counters.

NOTE 2 A cryptographic analysis of the impact of using a small blinding factor (i.e. in step A1 selecting r_A from a small subset of S_1) is provided in Reference [39].

NOTE 3 An analysis in an enhanced security model is given in Reference [40].

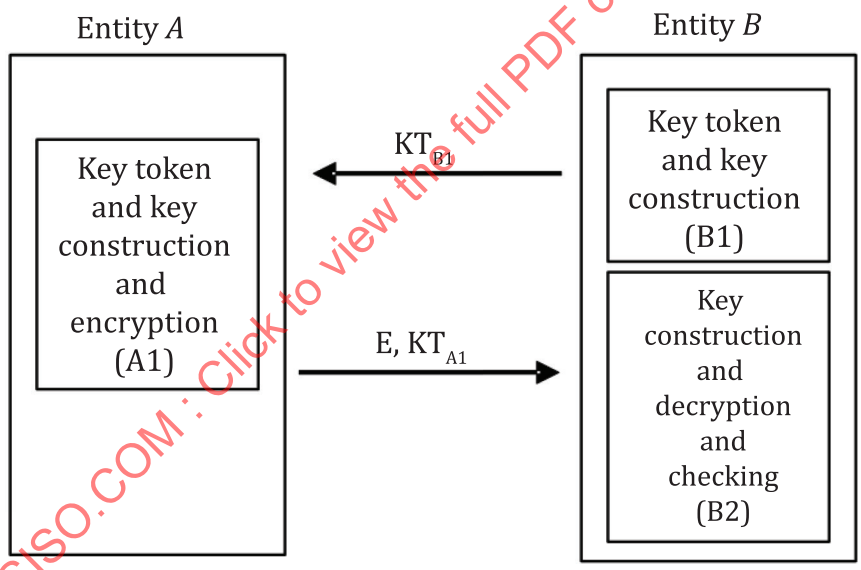

Figure 9a — Key agreement mechanism 13 (2-pass)

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

11.14 Key agreement mechanism 14

This key agreement mechanism, known as "3-pass blinded Diffie-Hellman", establishes a shared secret key in three passes between entities A and B with unilateral implicit key authentication. The following requirements shall be satisfied.

© ISO/IEC 2017 – All rights reserved

— Entity A has a private key agreement key h_A in S_1 and a public key agreement key P_A= F(h_A, G) in S_2, where S_1 and S_2 are the sets introduced in 10.2.

— Entity B has access to the credentials necessary to authenticate the public key agreement key of entity A. This may be achieved using the mechanisms described in Clause 13, but to ensure the privacy property of unlinkability any identifiers of entity A and any credentials unique to entity A that are sent from entity A to entity B are sent encrypted using a key derived from the shared key, for example, as shown in Text1 in the description below.

— Key derivation shall comply with ISO/IEC 11770-6 (see also Annex C) and encryption shall use an authenticated encryption method chosen from ISO/IEC 19772.

— Random number generation shall comply with ISO/IEC 18031.

Key token construction (A1) Entity A randomly and secretly generates r_A in S_1, constructs the key token KT_{A1} = F(r_A, P_A), and sends it to entity B.

Key token construction and key construction (B1) Entity B randomly and secretly generates r_B in S_1, computes its ephemeral public key P_B = F(r_B, G) in S_2, constructs the key token KT_{B1} = P_B, and sends it to entity A.

Entity B computes the shared secret key as K = F(r_B, KT_{A1}).

Key construction and encryption (A2) Entity A computes the shared secret key as K = F(r_A, F(h_A,KT_{B1})).

Entity A derives key K_{AB} from K using an agreed key derivation function and uses an authenticated encryption algorithm AuthEnc to compute E = AuthEnc_K_{AB} (r_A, P_A, Text1) and sends this to entity B.

Decryption and checking (B2) Entity B derives key K_{AB} from K using the agreed key derivation function and uses AuthEnc and E to recover r_A and P_A and check that KT_{A1} = F(r_A, P_A).

NOTE 1 A security proof for the 3-pass protocol is provided in Reference [38]. The security proof requires the use of unidirectional authenticated encryption keys and the inclusion of state information such as message counters.

NOTE 2 A cryptographic analysis of the impact of using a small blinding factor (i.e. in step A1 selecting r_A from a small subset of S_1) is provided in Reference [39].

NOTE 3 An analysis in an enhanced security model is given in Reference [40].

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

© ISO/IEC 2017 – All rights reserved

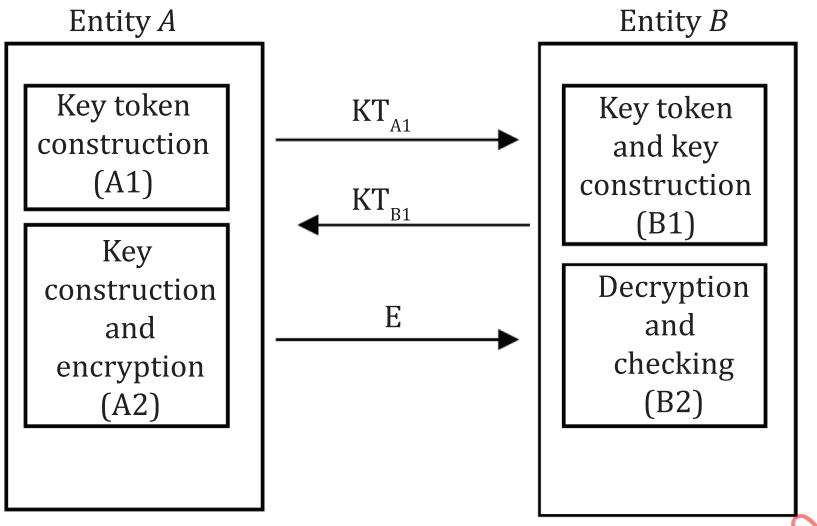

Figure 9b — Key agreement mechanism 14 (3-pass)

Annex A

On page 40, insert a reference to ISO/IEC 8824 and ISO/IEC 8825 in the opening sentence:

> This annex lists the object identifiers (see References [42] and [43]) assigned to the key management mechanisms specified in this document.

On page 40, insert the following between id-km-at-kAM-12 and id-km-at-kTM-1:

```
id-km-at-kAM-13 OID ::= { id-km-at keyAgreementMechanism13(22) }
id-km-at-kAM-14 OID ::= { id-km-at keyAgreementMechanism14(23) }
```

On page 43 insert the following before -- Key Transport Mechanism 1 –:

```
-- Key Agreement Mechanism 13 --
keyTokenConstruction-13-B1 OID ::= {
   id-km-at-kAM-13 keyTokenConstruction (1)  }
keyKeyTokenConstructionEncryption-13-A1 OID ::= {  id-km-at-kAM-13 kKTCE (2)  }
-- Key Agreement Mechanism 14 --
keyTokenConstruction-14-A1 OID ::= {
   id-km-at-kAM-14 keyConstruction (1)  }
keyKeyTokenConstruction-14-B1 OID ::= {
   id-km-at-kAM-14 keyKeyTokenConstruction (2)  }
keyConstructionEncryption-14-A2 OID ::= {
  id-km-at-kAM-14 keyConstructionEncryption (3)  }
```

Annex B

Insert the following paragraph before Table B.1:

> Having the property of being unlinkable provides privacy in the sense that a passive eavesdropper is unable to determine if two instances of the protocol involve the same entity or not. Note that the property of being unlinkable for entity A necessarily provides anonymity for entity A, for if it did not then it would not be unlinkable. Mechanisms that require an entity's plaintext public key to be sent to the other entity do not provide the property of unlinkability for that entity. For the purposes of Annex B, mechanisms which assume that an entity's public key is already shared are not considered to provide the property of unlinkability.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

 © ISO/IEC 2017 – All rights reserved

Table B.1

Replace Table B.1 with the following:

Table B.1 — Properties of key agreement mechanisms

Mechanism	Number of Passes	Implicit key authentication	Key confirmation	Entity authentication	Public key operations	Forward secrecy	Key freshness	Unlinkable
1	0	A, B	No	No	(1F, 1F)	No	No	No
2	1	B	No	No	(2F, 1F)	A	A	A
3	1	A, B	B	A	(2F/1S_A, 1F/1V_A)	A	A	No
4	2	No	No	No	(2F, 2F)	MFS	A,B	A,B
5	2	A, B	Opt	No	(3F, 3F)	A,B	A,B	No
6	2	A, B	Opt	B	(1V_B/1D_A, 1S_B/1E_A)	B	A,B	No
7	3	A, B	A, B	A, B	(2F/1V_B/1S_A, 2F/1S_B/1V_A)	MFS	A,B	No
8	1	A, B	No	No	(2F, 1F)	A	A	No
9	2	A, B	No	No	(2F, 2F)	MFS	A,B	No
10	3	A, B	A, B	A, B	(2F, 2F)	MFS	A,B	No
11	4	B	A, B	B	(1V_{CA}/1E_B, 1D_B)	MFS	A,B	A
12	0	A, B, C	No	No	(1FP,1FP,1FP)	No	No	No
13	2	A	(A), B	A	(2F,3F)	A	A, B	A, B
14	3	A	(A), B	A	(2F,3F)	A	A, B	A, B
F.3	2	A, B	No	No	(3F+2FP, 3F+2FP)	A, B	A, B	No
F.4	2	A, B	No	No	(3F+2FP, 3F+2FP)	A, B	A, B	No

Annex E

Add the following after E.13:

E.14 Key agreement of Diffie-Hellman type with blinded public key

This example adopts the form and notation of E.8.

This is an example of key agreement mechanism 13. Key agreement mechanism 13 establishes a shared secret between entities *A* and *B* in two passes and enables entity *B* to obtain entity *A*'s public key (and other information that might be unique to entity *A*) without revealing it to eavesdroppers.

The example uses elliptic curve cryptography with an elliptic curve group with generator *G* of order *n*. In the notation of 10.2 and 11.13, S_2 is the set of points on the elliptic curve generated by *G* and S_1 is the set of integers in the range {2,..., *n*-1}.

Prior to the process of agreeing upon a shared secret, in addition to the common information, the following is established:

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-3:2015/Amd 1:2017

© ISO/IEC 2017 – All rights reserved