

Third edition  
2015-08-01

---

---

## Information technology — Security techniques — Key management —

### Part 3: Mechanisms using asymmetric techniques

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

*Partie 3: Mécanismes utilisant des techniques asymétriques*

---

---

Reference number  
ISO/IEC 11770-3:2015(E)





**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2015, 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

This is a preview of "ISO/IEC 11770-3:2015". Click here to purchase the full version from the ANSI store.

## Contents

	Page
Foreword .....	v
Introduction .....	vi
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>2</b>
<b>4 Symbols and abbreviations</b> .....	<b>7</b>
<b>5 Requirements</b> .....	<b>9</b>
<b>6 Key derivation functions</b> .....	<b>9</b>
<b>7 Cofactor multiplication</b> .....	<b>9</b>
<b>8 Key commitment</b> .....	<b>10</b>
<b>9 Key confirmation</b> .....	<b>11</b>
<b>10 Framework for key management</b> .....	<b>12</b>
10.1 General .....	12
10.2 Key agreement between two parties .....	12
10.3 Key agreement between three parties .....	12
10.4 Secret key transport .....	13
10.5 Public key transport .....	13
<b>11 Key agreement</b> .....	<b>14</b>
11.1 Key agreement mechanism 1 .....	14
11.2 Key agreement mechanism 2 .....	15
11.3 Key agreement mechanism 3 .....	16
11.4 Key agreement mechanism 4 .....	18
11.5 Key agreement mechanism 5 .....	18
11.6 Key agreement mechanism 6 .....	19
11.7 Key agreement mechanism 7 .....	21
11.8 Key agreement mechanism 8 .....	22
11.9 Key agreement mechanism 9 .....	23
11.10 Key agreement mechanism 10 .....	24
11.11 Key agreement mechanism 11 .....	25
11.12 Key agreement mechanism 12 .....	26
<b>12 Secret key transport</b> .....	<b>27</b>
12.1 Secret key transport mechanism 1 .....	27
12.2 Secret key transport mechanism 2 .....	28
12.3 Secret key transport mechanism 3 .....	30
12.4 Secret key transport mechanism 4 .....	32
12.5 Secret key transport mechanism 5 .....	33
12.6 Secret key transport mechanism 6 .....	35
<b>13 Public key transport</b> .....	<b>36</b>
13.1 Public key transport mechanism 1 .....	36
13.2 Public key transport mechanism 2 .....	37
13.3 Public key transport mechanism 3 .....	38
<b>Annex A (normative) Object identifiers</b> .....	<b>40</b>
<b>Annex B (informative) Properties of key establishment mechanisms</b> .....	<b>47</b>
<b>Annex C (informative) Examples of key derivation functions</b> .....	<b>49</b>
<b>Annex D (informative) Examples of key establishment mechanisms</b> .....	<b>56</b>
<b>Annex E (informative) Examples of elliptic curve based key establishment mechanisms</b> .....	<b>60</b>

This is a preview of "ISO/IEC 11770-3:2015". [Click here to purchase the full version from the ANSI store.](#)

<b>Annex F (informative) Example of bilinear pairing based key establishment mechanisms</b> .....	<b>68</b>
<b>Annex G (informative) Secret key transport</b> .....	<b>71</b>
<b>Annex H (informative) Patent information</b> .....	<b>76</b>
<b>Bibliography</b> .....	<b>80</b>

This is a preview of "ISO/IEC 11770-3:2015". Click here to purchase the full version from the ANSI store.

## 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.

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 document 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](http://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 and IEC 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](http://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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 11770-3:2008 with ISO/IEC 11770-3/Cor1:2009), which has been technically revised.

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*
- *Part 5: Group key management*
- *Part 6: Key derivation*

Further parts may follow.

## Introduction

This part of ISO/IEC 11770 describes schemes that can be used for key agreement and schemes that can be used for key transport.

Public key cryptosystems were first proposed in the seminal paper by Diffie and Hellman in 1976. The security of many such cryptosystems is based on the presumed intractability of solving the discrete logarithm problem over certain finite fields. Other public key cryptosystems such as RSA are based on the difficulty of the integer factorization problem.

A third class of public key cryptosystems is based on elliptic curves. The security of such a public key system depends on the difficulty of determining discrete logarithms in the group of points of an elliptic curve. When based on a carefully chosen elliptic curve, this problem is, with current knowledge, much harder than the factorization of integers or the computation of discrete logarithms in a finite field of comparable size. All known general purpose algorithms for determining elliptic curve discrete logarithms take exponential time. Thus, it is possible for elliptic curve based public key systems to use much shorter parameters than the RSA system or the classical discrete logarithm based systems that make use of the multiplicative group of some finite field. This yields significantly shorter digital signatures, as well as system parameters, and allows for computations using smaller integers.

This part of ISO/IEC 11770 includes mechanisms based on the following:

- finite fields;
- elliptic curves;
- bilinear pairings.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from those in [Annex H](#).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO ([www.iso.org/patents](http://www.iso.org/patents)) and IEC (<http://patents.iec.ch>) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.