

Fourth edition
2021-10

Information security — Key management —

Part 3: Mechanisms using asymmetric techniques

Sécurité de l'information — Gestion de clés —

Partie 3: Mécanismes utilisant des techniques asymétriques



Reference number
ISO/IEC 11770-3:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

This is a preview of "ISO/IEC 11770-3:2021". [Click here to purchase the full version from the ANSI store.](#)

Contents	Page
Foreword	5
Introduction	6
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Symbols and abbreviations	8
5 Requirements	10
6 Key derivation functions	11
7 Cofactor multiplication	11
8 Key commitment	12
9 Key confirmation	12
10 Framework for key management	13
10.1 General	13
10.2 Key agreement between two parties	14
10.3 Key agreement between three parties	14
10.4 Secret key transport	15
10.5 Public key transport	15
11 Key agreement	15
11.1 Key agreement mechanism 1	15
11.2 Key agreement mechanism 2	17
11.3 Key agreement mechanism 3	17
11.4 Key agreement mechanism 4	19
11.5 Key agreement mechanism 5	20
11.6 Key agreement mechanism 6	21
11.7 Key agreement mechanism 7	23
11.8 Key agreement mechanism 8	24
11.9 Key agreement mechanism 9	25
11.10 Key agreement mechanism 10	26
11.11 Key agreement mechanism 11	27
11.12 Key agreement mechanism 12	28
11.13 Key agreement mechanism 13	29
11.14 Key agreement mechanism 14	30
11.15 Key agreement mechanism 15	31
12 Secret key transport	32
12.1 Secret key transport mechanism 1	32
12.2 Secret key transport mechanism 2	34
12.3 Secret key transport mechanism 3	35
12.4 Secret key transport mechanism 4	37
12.5 Secret key transport mechanism 5	38
12.6 Secret key transport mechanism 6	41
13 Public key transport	42
13.1 Public key transport mechanism 1	42
13.2 Public key transport mechanism 2	43
13.3 Public key transport mechanism 3	44

This is a preview of "ISO/IEC 11770-3:2021". [Click here to purchase the full version from the ANSI store.](#)

Annex A (normative) Object identifiers	46
Annex B (informative) Properties of key establishment mechanisms	55
Annex C (informative) Examples of key derivation functions	58
Annex D (informative) Examples of key establishment mechanisms	66
Annex E (informative) Examples of elliptic curve based key establishment mechanisms	70
Annex F (informative) Example of bilinear pairing based key establishment mechanisms	80
Annex G (informative) Secret key transport	84
Bibliography	88

This is a preview of "ISO/IEC 11770-3:2021". 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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see patents.iec.ch).

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 11770-3:2015), which has been technically revised. It also incorporates Technical Corrigenda ISO/IEC 11770-3:2015/Cor1:2016 and ISO/IEC 11770-3:2015/Amd.1:2017.

The main changes compared to the previous edition are as follows:

- the blinded Diffie-Hellman key agreements are added as key agreement mechanism 13 and 14 and examples of the mechanisms are included in Annex E;
- key agreement mechanism 15 is added and the SM9 key agreement protocol as an example of the mechanism is included in Annex F.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document 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 document 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 document may involve the use of a patent.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from the patent database available at www.iso.org/patents and <http://patents.iec.ch>.

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