INTERNATIONAL STANDARD

ISO/IEC 11770-2

Third edition
2018-10

IT Security techniques — Key management —

Part 2: Mechanisms using symmetric techniques

Techniques de sécurité IT — Gestion de clés —

Partie 2: Mécanismes utilisant des techniques symétriques

Reference number
ISO/IEC 11770-2:2018(E)

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

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **3**
5 Requirements ... **4**
6 Point-to-point key establishment ... **6**
6.1 General ... 6
6.2 Key establishment mechanism 1 ... 6
6.3 Key establishment mechanism 2 ... 7
6.4 Key establishment mechanism 3 ... 7
6.5 Key establishment mechanism 4 ... 8
6.6 Key establishment mechanism 5 ... 8
6.7 Key establishment mechanism 6 ... 10
7 Mechanisms using a Key Distribution Centre ... **11**
7.1 General ... 11
7.2 Key establishment mechanism 7 ... 11
7.3 Key establishment mechanism 8 ... 12
7.4 Key establishment mechanism 9 ... 14
7.5 Key establishment mechanism 10 ... 15
8 Mechanisms using a Key Translation Centre ... **17**
8.1 General ... 17
8.2 Key establishment mechanism 11 ... 17
8.3 Key establishment mechanism 12 ... 18
8.4 Key establishment mechanism 13 ... 20
Annex A (normative) **Object identifiers** ... **22**
Annex B (informative) **Properties of key establishment mechanisms** ... **24**
Annex C (informative) **Auxiliary techniques** ... **26**
Bibliography ... **28**

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).

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).

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.

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

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.

This third edition cancels and replaces the second edition (ISO/IEC 11770-2:2008), which has been technically revised. It also incorporates ISO/IEC 11770-2:2008/Cor 1:2009.

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

— the list of requirements in Clause 5 has been updated;

— an optional message and mechanism identifier to the encrypted strings sent within each of the mechanisms has been added;

— the set of inputs for calculation of the key in Mechanism 5 has been expanded;

— minor changes have been made to the fourth message in Mechanism 8 and the second message in Mechanism 10.

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

Introduction

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.

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. Besides key establishment, the goals of such a mechanism can include unilateral or mutual authentication of the communicating entities. Further goals can be the verification of the integrity of the established key, or key confirmation.

IT Security techniques — Key management —

Part 2:
Mechanisms using symmetric techniques

1 Scope

This document defines key establishment mechanisms using symmetric cryptographic techniques.

This document addresses three environments for the establishment of keys: Point-to-Point, Key Distribution Centre (KDC), and Key Translation Centre (KTC). It 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.

This document 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 document.

This document does not specify the means to be used to establish initial secret keys; that is, all the mechanisms specified in this document 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 document does not explicitly address the issue of inter-domain key management. This document also does not define the implementation of key management mechanisms; products complying with this document are not necessarily compatible.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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*