INTERNATIONAL STANDARD

ISO/IEC 11770-5

Second edition
2020-11

Information security — Key management —

Part 5: Group key management

Sécurité de l'information — Gestion de clés —

Partie 5: Gestion de clés de groupe

Reference number
ISO/IEC 11770-5:2020(E)

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

Contents

Page

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).

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 http://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.

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

This second edition cancels and replaces the first edition (ISO/IEC 11770-5:2011) which has been technically revised.

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

— the document has been modified to be consistent with use of the key deriviation specifications from ISO/IEC 11770-6;

— the use of a "trapdoor" in key derivation has been removed. Consequently, unlimited forward key chains can no longer be calculated.

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

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.

Introduction

In some applications, it is necessary for a secret cryptographic key to be shared by a group of entities. Moreover, in some cases the exact membership of a group of entities that share a key may change over time.

This document is concerned with techniques that enable a secret key to be shared by all members of a defined group with the assistance of a trusted third party known as a key distribution centre. Provisions for adding and removing members of a group are also made.

Information security — Key management —

Part 5: Group key management

1 Scope

This document specifies mechanisms to establish shared symmetric keys between groups of entities. It defines:

— symmetric key-based key establishment mechanisms for multiple entities with a key distribution centre (KDC); and

— symmetric key establishment mechanisms based on a general tree-based logical key structure with both individual rekeying and batch rekeying.

It also defines key establishment mechanisms based on a key chain with group forward secrecy, group backward secrecy or both group forward and backward secrecy.

This document also 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 specify information that has no relation with key establishment mechanisms, nor does it 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 the initial secret keys required to be shared between each entity and the KDC, nor key lifecycle management. This document also does not explicitly address the issue of interdomain key management.

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 19772, *Information technology — Security techniques — Authenticated encryption*

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