INTERNATIONAL STANDARD

ISO/IEC 11770-6

First edition
2016-10-01

Information technology — Security techniques — Key management —

Part 6: Key derivation

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

Partie 6: Dérivation de clés

Reference number
ISO/IEC 11770-6:2016(E)

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

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. 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 on 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.

The committee responsible for this document is 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 website.

Introduction

The establishment of shared secret cryptographic keys is a fundamental key management service. It is a prerequisite for the use of a range of symmetric cryptographic techniques, including symmetric encryption for confidentiality protection, and message authentication codes (MACs) for integrity protection and data origin authentication. Key derivation techniques enable such keys to be generated from pre-existing secrets and have a range of possible applications. Two particularly important applications are as follows.

First, while two (or more) parties might share secret information, this secret information might not be suitable for immediate use as input to an encryption algorithm or a message authentication code scheme. For example, the initial secret information might not be distributed randomly across the entire space of possible values, or an unauthorized third party might have partial information about it. A key derivation function (or a key extraction function) can be used to resolve this issue by taking the secret information as input, perhaps together with other non-secret material, and giving a suitable secret key as output.

Second, a number of secret keys might be required for different purposes, e.g. for different applications or for input to different cryptographic functions. Again, a key derivation function (or a key expansion function) can be used to meet this requirement by taking secret information, perhaps together with other non-secret material, as input, and giving a secret key, or keys, as output. The secret information might, for example, be shared by two or more parties, and the generated secret keys could then be used to protect data exchanged between these parties via untrusted channels; alternatively, the secret information might only be known by a single party, and the generated keys could then be used to protect data stored by that party in untrusted locations.

This document is concerned with such key derivation techniques. Two general classes of key derivation techniques are specified, namely one-step and two-step functions, both of which can be used to generate either a single key or multiple keys. One-step functions transform the input information into one or more keys in a single operation. Two-step functions first transform the input information into a secret MAC key, which is then used in the second step (which can be executed multiple times) to generate one or more secret keys for use in applications.

The choice between one-step and two-step functions depends on two main things: the nature of the available secret input to the key derivation function, and the way in which the secret input is to be used. For example, if the available secret input is already in the form of a secret key, then a one-step function will normally be appropriate. Also, regardless of the nature of the secret input, if the function is to be used only once with a particular set of secret inputs, then again a one-step function will typically be appropriate. However, if the secret input is not in the form of a secret key, and the same secret input is to be used multiple times to generate one or more keys, then a two-step function is likely to be appropriate, where the first step is performed once to generate a MAC key and the second step is performed whenever a new key is, or keys are, to be generated from the MAC key.

This document defines a range of one-step key derivation functions. It also defines examples of both key extraction functions and key expansion functions, where a key extraction function can be combined with a key expansion function to define a two-step key derivation function.

Information technology — Security techniques — Key management —

Part 6: Key derivation

1 Scope

This document specifies key derivation functions, i.e. functions which take secret information and other (public) parameters as input and output one or more "derived" secret keys. Key derivation functions based on MAC algorithms and on hash-functions are specified.

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 9797 (all parts), *Information technology — Security techniques —Message Authentication Codes (MACs)*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*