DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 11770-6

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on:
2015-09-07

Voting terminates on:
2015-12-07

Information technology — Security techniques — Key management —

Part 6:
Key derivation

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

ICS: 35.040

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 11770-6:2015(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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 11770-6 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

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*

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.

Firstly, whilst 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.

Secondly, 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 part of ISO/IEC 11770 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: firstly the nature of the available secret input to the key derivation function, and secondly 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 part of ISO/IEC 11770 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 part of ISO/IEC 11770 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 referenced documents are indispensable for the application 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*

ISO/IEC 11770-1, *Information technology — Security techniques — Key management — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 11770-1 and the following apply.

3.1
entropy
measure of the disorder, randomness or variability in a closed system

Note 1 to entry: The particular measure of entropy that is used in the document is discussed in ~~clause~~ 5.1.

3.2
hash-function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits

Note 1 to entry: Cryptographic requirements on hash-functions employed for the purposes of this document are considered in ~~clause~~ 6.1.

3.3
key derivation function
KDF
function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm(s) and applications

Note 1 to entry: Cryptographic requirements on key derivation functions are specified in ~~clause~~ 5.1 of this document.

Note 2 to entry: Key derivation functions are also sometimes known as key generating functions.

3.4
key expansion function
KPF
function which takes as input a number of parameters, at least one of which shall be a secret key, and which gives as output keys appropriate for the intended algorithm(s) and applications

Note 1 to entry: Cryptographic requirements on key expansion functions are specified in ~~clause~~ 7.1 of this document.

Note 2 to entry: All the KPFs specified in this document are based on a MAC algorithm.

3.5
key extraction function
KTF
function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output a key suitable for use as input to a key expansion function

Note 1 to entry: Cryptographic requirements on key extraction functions are specified in ~~clause~~ 7.1 of this document.

3.6
Message Authentication Code
MAC
string of bits which is the output of a MAC algorithm

[SOURCE: ISO/IEC 9797-1, 3.9]

3.7
Message Authentication Code algorithm
MAC algorithm
algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

- for any key and any input string, the function can be computed efficiently;
- for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of a set of input strings and corresponding function values, where the value of the i th input string might have been chosen after observing the value of the first i -1 function values (for integers $i > 1$)

Note 1 to entry: A MAC algorithm is sometimes called a cryptographic check function.

Note 2 to entry: Computational feasibility depends on the user's specific security requirements and environment.

Note 3 to entry: Additional cryptographic requirements for MAC algorithms employed for the purposes of this document are specified in ~~clauses~~ 6.1 and 7.1.

3.8
Message Authentication Code key
MAC key
bit string suitable for use as a key input to a MAC algorithm

3.9
one-step key derivation function
OKDF
key derivation function which operates in a single stage, in contrast to key derivation functions involving separate key-extraction and key-expansion stages (cf. 3.12)

3.10
salt
value used as input to a key derivation function, a key expansion function or a key extraction function, which might not be secret

3.11
secret information
bit string used as input to a KDF or a KTF, which shall be known only to entities which are authorized to agree upon the key or keys, and possibly to one or more other entities trusted for the purposes of key establishment

3.12
two-step key derivation function
TKDF
key derivation function which involves two stages, namely the use of a key extraction function followed by a key expansion function

4 Symbols and abbreviations

4.1 Symbols

a algorithm identifier

b bit string output by a KDF

c counter

f MAC algorithm, where $f_k(d)$ denotes the MAC obtained when f is given as input the key k and the data d (a bit string)

h hash-function

k secret key

k_m secret MAC key

L_b bit-length of the output b of a KDF

L_c bit-length of the binary encoding of the counter c

L_f bit-length of the output of the MAC algorithm f used as part of a KDF

L_h bit-length of a hash-function h used as part of a KDF

L_k bit-length of a secret key k

p label employed to 1) indicate how a bit string is to be partitioned into one or more keys, and 2) identify the algorithm(s) with which the resulting key(s) should be used

s secret information

t salt value

u auxiliary secret information

y bit string

z bit string

4.2 Abbreviations

KDF Key Derivation Function

KPF Key exPansion Function

KTF Key exTraction Function

MAC Message Authentication Code

OKDF One-step KDF

TKDF Two-step KDF

4.3 Notation

|| concatenation, where $x||y$ denotes the bit string obtained by concatenating the bit strings x and y in the order specified

$\lceil\ldots\rceil$ if x is a real number, $\lceil x \rceil$ denotes the smallest integer greater than or equal to x

[...] if x is a bit string, [x] indicates that the inclusion of x is optional

5 Key derivation techniques

5.1 Model

A KDF is a function which can be used to generate one or more secret keys, given a range of possible inputs. In general, a KDF has the following inputs and outputs.

Inputs:

- Mandatory inputs:

  - s secret information possessed by the party or parties using the KDF, and which shall be generated from a random source with sufficient entropy to support the security requirements of the user(s) of the intended application(s) of the generated key(s) (see B.1.2 for guidance).

    NOTE 1 The entropy of a (discrete) random variable X is a mathematical measure of the uncertainty associated with the possible outcomes of an observation, which serves as an estimate of the information that may be gained from an observation of X. Entropy is at its highest if all possible outcomes are equally likely. Entropy is lessened if the distribution on X is such that some outcomes are more likely than others; entropy is at its lowest (zero) if each observation is certain to be a particular (predetermined) value.

    NOTE 2 There are various notions of entropy that are relevant to cryptographic applications, but in this document entropy is measured using min-entropy, as defined in [ISO 18031, 3.22]. When the unit of measurement is bits, the min-entropy of a (discrete) random variable X is the largest value m for which the probability of observing any particular value of X is at most 2^{-m}. The min-entropy of X is a lower bound for other commonly used measures of entropy.

- Optional/mechanism-dependent inputs:

  - a algorithm identifier employed by the OKDF2 mechanism, which specifies the algorithm with which its single generated key should be used;

  - p label, used with certain KDFs to indicate how the output bit string should be partitioned into secret keys and the intended use for each such secret key;

  - t salt value, i.e. a (not necessarily secret) value that can be used, for example, to make the generated key(s) specific to a particular application and/or to ensure that the output key(s) will vary with each execution of a key derivation function; used as a MAC key by the KTF1 mechanism;

  - t' salt value, i.e. a (not necessarily secret) value that is used as a MAC key by the OKDF6 mechanism and used as an initialization value by the KPF3 mechanism

- *u* auxiliary secret information possessed by the party or parties using the KDF; the entropy provided by the choice of *u* may be used to supplement that provided by the choice of *s,* in support of the security requirements of the user(s) of the intended application(s) of the generated key(s).

Outputs:

- *b* bit string that is either equal to a single secret key or can be partitioned to obtain a number of secret keys.

The instantiation of a key derivation function specified in this document requires a number of critical choices, including the selection of a hash-function or MAC algorithm(s), the type and source of various input parameters, etc. Appropriate choices will provide assurance that the resulting KDF satisfies the following requirement.

Given no prior knowledge of *s*, it shall be computationally infeasible to predict the value of an (as-yet-unseen) output *b* with a probability of success that is a significant improvement over simply guessing either the value of *b* or the value of *s*. This shall be the case even when given knowledge of a (bounded) number of KDF outputs which were computed using the same (unknown) *s*, but with other (possibly known and adaptively chosen) input parameters that are not identical to those used to generate *b*.

NOTE Computational feasibility and the significance of the probability of successfully predicting *b* depend on the KDF user's specific security requirements and environment.

5.2 Types of key derivation function

In this part of ISO/IEC 11770 two types of KDF are specified.

- **One-step KDFs (OKDFs)** are KDFs which transform input information into one or more keys in a single operation.

- **Two-step KDFs (TKDFs)** are KDFs which transform input information into one or more keys in two operations. A TKDF consists of a combination of two functions: a key extraction function (KTF), and a key expansion function (KPF). In some cases the KTF can be the identity function (i.e. a function whose output is always the same as the input), i.e. the TKDF is simply a KPF, in which case the secret information input to the TKDF shall take the form of a MAC key suitable for use with the MAC algorithm on which the KPF is based.

Six OKDFs (OKDF1-OKDF6) are specified in Clause 6. In Clause 7, one key extraction function (KTF1), four key expansion functions (KPF1-KPF4), and four TKDFs (TKDF1-TKDF4) are specified, where the TKDFs are defined as specific combinations of a KTF and a KPF.

The KDFs specified in this part of ISO/IEC 11770 are built upon existing cryptographic functions, namely either hash-functions, as specified in ISO/IEC 10118, or Message Authentication Code algorithms, as specified in ISO/IEC 9797.

5.3 Relationship to key management lifecycle

Clause 4 of ISO/IEC 11770-1 specifies a model for key management, including, in 4.3, a model for the lifecycle of a key. Key derivation forms part of the first step in this lifecycle, namely the *Generation* step. Key derivation could also be used in the *Active* state for a key, when an existing active key is used to generate additional keys.

5.4 Use of a key derivation function

The inputs to and outputs from a KDF are permitted to take a variety of forms.