FINAL DRAFT
International Standard

ISO/IEC
FDIS
11770-8

Information security — Key management —

Part 8: Password-based key derivation

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2026-09-21

Voting terminates on:
2026-11-16

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.

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.

Reference number
ISO/IEC FDIS 11770-8:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols ... **2**
5 Use of password-based key derivation functions ... **4**
6 Argon2i ... **4**
6.1 General ... 4
6.2 Input values and parameters ... 4
6.3 Specification of Argon2i ... 5
6.3.1 Argon2i State ... 5
6.3.2 Argon2i Flow ... 6
7 PBKDF2 ... **8**
7.1 General ... 8
7.2 Input values and parameters ... 8
7.3 Specifications ... 9
Annex A (normative) **Object identifiers** ... **10**
Annex B (normative) **Compression function**, *G* ... **12**
Annex C (normative) **Blake2b** ... **14**
Annex D (informative) **Guidance on parameter choice** ... **18**
Annex E (informative) **Criteria for inclusion of functions in this document** ... **19**
Annex F (informative) **Numerical examples** ... **21**
Bibliography ... **22**

© ISO/IEC 2026 – All rights reserved

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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 Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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 and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

Despite well-known shortcomings, secret, human-memorized, passwords remain widely used for user authentication. It is often the case that such passwords have very limited entropy, i.e. a password can be guessed using heuristic techniques, including using tables of likely passwords, in a relatively small number of trials. As a result, it can be hazardous to derive a cryptographic key from a password, since in general keys are expected to be chosen from a set large enough to ensure that guessing attacks are not practical.

However, in practice it is nevertheless sometimes necessary to derive a key from a password. In such cases, the method of deriving the key from the password should be designed very carefully to try to ensure guessing attacks are very costly computationally. This involves making the key derivation function, which is used to derive the key from the password, difficult to compute quickly.

This document is concerned with specifying key derivation functions of this type, i.e. those designed specifically to derive keys from passwords. In particular, the functions known as Argon2i and PBKDF2 are specified.

© ISO/IEC 2026 – All rights reserved

Information security — Key management —

Part 8:
Password-based key derivation

1 Scope

This document specifies password-based key derivation functions, namely key derivation functions designed to take human-memorable passwords as input. This document is applicable to environments where it is necessary to derive a cryptographic key from a password.

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*

ISO/IEC 9834-1, *Information technology — Procedures for the operation of object identifier registration authorities — Part 1: General procedures and top arcs of the international object identifier tree*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
hash-function
function which maps strings of bits of variable (but usually upper-bounded) length to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output

[SOURCE: ISO/IEC 10118-1:2016, 3.4, modified — Note 1 to entry has been deleted.]

3.2
key derivation function
KDF
function which takes as input a number of parameters, at least one of which is secret, and which gives as output keys appropriate for the intended algorithm(s) and applications

[SOURCE: ISO/IEC 11770-6:2016, 3.3, modified — Notes to the entry have been deleted.]

© ISO/IEC 2026 – All rights reserved

3.3
weak secret
secret that can be conveniently memorized by a human being

Note 1 to entry: Typically, this means that the entropy of the secret is limited, so that an exhaustive search for the secret (or, a dictionary attack) can be feasible, given knowledge that would enable a correct guess for the secret to be distinguished from an incorrect guess.

[SOURCE: ISO/IEC 11770-4:2017, 3.38]

3.4
password
secret word, phrase, number, or character sequence used for entity authentication, which is a memorized *weak secret* (3.3)

[SOURCE: ISO/IEC 11770-4:2017, 3.27]

3.5
salt
value used as input to a key derivation function, which is possibly not a secret

[SOURCE: ISO/IEC 11770-6:2016, 3.10, modified — "a key expansion function or a key extraction function" has been removed from the definition.]

4 Symbols

a, b, c, d	64-bit strings
a_L	32-bit string made up of the 32 least significant bits of the 64-bit string a
$B[i][j]$	1024-byte values computed during Argon2i key derivation ($0 \le i < p$, $0 \le j < m/p$)
f	parameter for F equal to TRUE or FALSE
H	Blake2b function
H'	variable-length hash-function which is built upon H
G	fixed-input-length compression function that maps a pair of 1024-byte values to a single 1024-byte value and is based on Blake2b's internal permutation
F	Blake2b component function
G^*	Blake2b component function
H_0	64-byte value computed during Argon2i key derivation
h	8-word vector used as a parameter for F (where a word is a 64-bit value)
IV	8-word constant used by Blake2b (where a word is a 64-bit value)
$k_1, \ldots, k_4$	integers satisfying $0 \le k_i \le 15$, $1 \le i \le 4$, used as parameters for G^*
L	integer equal to the number of bytes in the input to H
L^*	integer equal to $\lceil L/128 \rceil$
Λ	integer defining the length of the output of H in bits
m^*	16-word vector used as a parameter for F

© ISO/IEC 2026 – All rights reserved