DRAFT International Standard

ISO/IEC DIS 9798-5

Information security — Entity authentication —

Part 5: Mechanisms using zero-knowledge techniques

ICS: 35.030

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

Secretariat: **DIN**

Voting begins on:
2026-09-17

Voting terminates on:
2026-12-10

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS 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.

This document has not been edited by the ISO Central Secretariat.

Reference number
ISO/IEC DIS 9798-5:2026(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 Notation, symbols and abbreviated terms ... **4**
5 Mechanisms based on identities ... **7**
5.1 Security requirements for the environment ... 7
5.2 Key production ... 8
5.2.1 Asymmetric key pair ... 8
5.2.2 Asymmetric pair(s) of numbers ... 9
5.3 Unilateral authentication exchange ... 11
6 Mechanisms based on integer factorization ... **13**
6.1 Security requirements for the environment ... 13
6.2 Key production ... 13
6.3 Unilateral authentication exchange ... 14
7 Mechanisms based on discrete logarithms with respect to prime numbers ... **16**
7.1 Security requirements for the environment ... 16
7.2 Key production ... 17
7.3 Unilateral authentication exchange ... 17
8 Mechanisms based on discrete logarithms with respect to composite numbers ... **19**
8.1 Security requirements for the environment ... 19
8.2 Key production ... 19
8.2.1 General ... 19
8.2.2 First mode of use (GPS1) ... 20
8.2.3 Second mode of use (GPS2) ... 20
8.3 Unilateral authentication exchange ... 20
9 Mechanisms based on asymmetric encryption systems ... **22**
9.1 Security requirements for the environment ... 22
9.2 Unilateral authentication exchange ... 23
9.3 Mutual authentication exchange ... 24
10 Mechanism based on discrete logarithms with respect to elliptic curves ... **26**
10.1 Security requirements for the environment ... 26
10.2 Key production ... 26
10.3 Unilateral authentication exchange ... 27
Annex A (normative) **Object identifiers** ... **29**
Annex B (informative) **Principles of zero-knowledge techniques** ... **31**
Annex C (informative) **Guidance on parameter choice and comparison of the mechanisms** ... **34**
Annex D (informative) **Numerical examples** ... **47**
Bibliography ... **61**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 had 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. ISO 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.

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

This fourth edition cancels and replaces the third edition (ISO/IEC 9798-5:2009), which has been technically revised.

The main changes are as follows:

— Updated guidance for short, medium and long term security in Annex C.

— Clarifications and updated presentation throughout.

A list of all parts in the ISO/IEC 9798 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.

© ISO/IEC 2026 – All rights reserved

Introduction

This document specifies authentication mechanisms that involve exchanges of information between a claimant and a verifier.

In accordance with the types of calculations that need to be performed by the claimant and the verifier, the mechanisms can be classified into the following four main groups (see Annex C).

— The first group (see the Clause and Clause 5) is characterized by the performance of short modular exponentiations. The challenge size needs to be optimized since it has a proportional impact on workloads.

— The second group (see Clause 6, Clause 7 and Clause 8) is characterized by the possibility of a “coupon strategy” for the claimant. A verifier can authenticate a claimant who has very limited computational power. The challenge size has no practical impact on workloads.

— The third group (see 9.2) is characterized by the possibility of a coupon strategy for the verifier. A verifier with very limited computational power can authenticate a claimant. The challenge size has no impact on workloads.

— The fourth group (see 9.3) has no possibility of a coupon strategy.

© ISO/IEC 2026 – All rights reserved

Information security — Entity authentication —

Part 5:
Mechanisms using zero-knowledge techniques

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using zero-knowledge techniques:

— mechanisms based on identities and providing unilateral authentication;

— mechanisms based on integer factorization and providing unilateral authentication;

— mechanisms based on discrete logarithms with respect to numbers that are either prime or composite, and providing unilateral authentication;

— mechanisms based on asymmetric encryption systems and providing either unilateral authentication or mutual authentication;

— mechanisms based on discrete logarithms on elliptic curves and providing unilateral authentication.

These mechanisms are constructed using the principles of zero-knowledge techniques, but they are not necessarily zero-knowledge according to the strict definition for every choice of parameters.

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 8825-1, *Information technology — ASN.1 encoding rules — Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 9798-1, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 18033-1:2021, *Information security — Encryption algorithms — Part 1: General*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules — Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
accreditation exponent, noun
secret number related to the verification exponent and used in the production of private keys

© ISO/IEC 2026 – All rights reserved

3.2
adaptation parameter, noun
public key specific to the modulus and used in the definition of public keys in the GQ2 mechanisms

3.3
asymmetric cryptographic technique, noun
cryptographic technique that uses two related transformations, a public transformation [defined by the *public key* (3.23)] and a private transformation [defined by the *private key* (3.21)]

Note 1 to entry: The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. Computational feasibility depends on the specific security requirements and environment.

[SOURCE: ISO/IEC 18033-1:2021, 3.1]

3.4
asymmetric encryption system, noun
system based on asymmetric cryptographic techniques whose public operation is used for encryption and whose private operation is used for decryption

3.5
asymmetric pair, noun
two related data items where the private data item defines a private transformation and the public data item defines a public transformation

3.6
challenge, noun
procedure parameter used in conjunction with secret parameters to produce a response

3.7
claimant, noun
entity whose identity can be authenticated, including the functions and the private data necessary to engage in authentication exchanges on behalf of a principal

3.8
claimant parameter, noun
public data item, number or bit string, specific to a given claimant within the domain

3.9
coupon, noun
pair of pre-computed numbers to be used only once; one is kept secret and the other remains secret until its use by an entity

3.10
decryption, noun
reversal of a corresponding encryption

[SOURCE: ISO/IEC 9798-1:2010, 3.10]

3.11
domain, noun
collection of entities operating under a single security policy

Note 1 to entry: For example, a collection of entities possessing public key certificates created either by a single certification authority, or by a collection of certification authorities using the same security policy.

3.12
domain parameter, noun
public key, or function, agreed and used by all entities within the domain

© ISO/IEC 2026 – All rights reserved

3.13
encryption, noun
reversible operation by a cryptographic algorithm converting data into ciphertext, so as to hide the information content of the data

[SOURCE: ISO/IEC 9798-1:2010, 3.13]

3.14
entity authentication, noun
corroboration that an entity is the one claimed

[SOURCE: ISO/IEC 9798-1:2010, 3.14]

3.15
exchange multiplicity parameter, noun
number of exchanges of information involved in one instance of an authentication mechanism

3.16
hash-function, noun
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]

3.17
identification data, noun
set of public data items (e.g. an account number, an expiry date and time, a serial number, etc.) assigned to an entity and used to identify it

3.18
mutual authentication, noun
entity authentication which provides both entities with assurance of each other's identity

[SOURCE: ISO/IEC 9798-1:2010, 3.18]

3.19
number, noun
natural number, i.e. a non-negative integer

3.20
pair multiplicity parameter, noun
number of asymmetric pairs of numbers involved in one instance of an authentication mechanism

3.21
private key, noun
data item of an asymmetric pair, that shall be kept secret and should only be used by a claimant in accordance with an appropriate response formula, thereby establishing its identity

3.22
procedure parameter, noun
transient public data item used in an instance of an authentication mechanism, such as a witness, challenge or response

3.23
public key, noun
data item of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity

© ISO/IEC 2026 – All rights reserved

3.24
random number, noun
time variant parameter whose value is unpredictable

[SOURCE: ISO/IEC 9798-1:2010, 3.29]

3.25
response, noun
procedure parameter produced by the claimant, and processed by the verifier for checking the identity of the claimant

3.26
secret parameter, noun
number or bit string that does not appear in the public domain and is only used by a claimant, e.g. a private key

3.27
token, noun
message consisting of data fields relevant to a particular communication and which contains information that has been produced using a cryptographic technique

3.28
unilateral authentication, noun
entity authentication which provides one entity with assurance of the other's identity but not vice versa

[SOURCE: ISO/IEC 9798-1:2010, 3.39]

3.29
verification exponent, noun
public key used as exponent by the claimant and the verifier

3.30
verifier, noun
entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication

3.31
witness, noun
procedure parameter that provides evidence of the claimant's identity to the verifier

4 Notation, symbols and abbreviated terms

For the purposes of this document, the following notation, symbols and abbreviated terms apply.

($a \mid n$) Jacobi symbol of a positive integer a with respect to an odd composite integer n

NOTE 1 By definition, the Jacobi symbol of any positive integer a with respect to any odd positive composite integer n is the product of the Legendre symbols of a with respect to each prime factor of n (repeating the Legendre symbols for the repeated prime factors). The Jacobi symbol [1][2] can be efficiently computed without knowledge of the prime factors of n.

($a \mid p$) Legendre symbol of a positive integer a with respect to an odd prime integer p

NOTE 2 By definition, the Legendre symbol of any positive integer a with respect to any odd positive prime integer p is equal to $a^{(p-1)/2} \mod p$. This means that $(a \mid p)$ is zero if a is a multiple of p, and either +1 or –1 otherwise, depending on whether or not a is a square modulo p.

$|A|$ if A is a number then the number of bits in its binary representation (i.e. the unique integer i so that $2^{i-1} \leq A < 2^i$ if $A > 0$, or 0 if $A = 0$, e.g. $|65\,537 = 216 + 1| = 17$), or if A is a bit string then its bit length.

© ISO/IEC 2026 – All rights reserved