International Standard

ISO/IEC 27565

First edition
2026-02

Information security, cybersecurity and privacy protection — Guidelines on privacy preservation based on zero-knowledge proofs

Sécurité de l'information, cybersécurité et protection de la vie privée — Lignes directrices relatives à la préservation de la vie privée basée sur des preuves à divulgation nulle de connaissance

Reference number
ISO/IEC 27565:2026(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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **4**
5 Introduction to zero-knowledge proofs **4**
5.1 General 4
5.2 Interactive and Non-interactive ZKP 5
5.2.1 General 5
5.2.2 Interactive zero-knowledge proofs 5
5.2.3 Non-interactive zero-knowledge proofs 6
5.3 Components of a ZKP system 7
5.3.1 General 7
5.3.2 Setup module 7
5.3.3 Prover module 9
5.3.4 Verifier module 9
5.4 Characteristics of ZKPs 10
5.5 ZKP performance 11
6 Considerations of implementing ZKPs for attribute verification **11**
6.1 Attribute providers 11
6.2 Replay attack detection or protection 11
6.3 Prevention of collusions between users 12
6.4 Use of an authoritative document or of a trusted authority 12
7 Use cases of ZKPs **12**
7.1 Proving some properties of a hidden attribute 12
7.2 Proving the contents in an authoritative document 13
7.3 Proving the contents across several authoritative documents 14
7.4 Selective disclosure of attributes 14
7.4.1 General 14
7.4.2 Pre-generation of digital credentials 14
7.4.3 On-demand generation of digital credentials 15
8 Privacy preservation using zero-knowledge proofs **15**
8.1 Privacy principles in the context of ZKP 15
8.2 Privacy risk assessment 15
8.3 Privacy functional requirements for ZKP 16
8.3.1 General 16
8.3.2 Collection limitation 16
8.3.3 Data minimization 16
8.3.4 Options and choice 17
8.3.5 Selective disclosure 17
8.3.6 Purpose legitimacy and specification 17
8.3.7 Anonymity of the authority that has issued the attestation 17
8.3.8 Non-disclosure of the identity of the verifiers to the attribute issuer 17
8.3.9 Use, retention and disclosure limitation 17
8.3.10 Accuracy and quality 17
8.3.11 Openness, transparency and notice 17
8.3.12 Individual participation and access 17
8.3.13 Accountability 17
8.3.14 Information security 18
8.3.15 Unlinkability 18
8.4 Security considerations 18

© ISO/IEC 2026 – All rights reserved

9 Functional use cases **18**
9.1 Functional use examples 18
9.2 Selection of ZKP models 19

10 Business use examples **20**
10.1 Age verification 20
10.2 Fraud prevention 20
10.3 Auction 20
10.4 Disability proof 20
10.5 Distributed ledger technologies and blockchains 21
10.6 Central bank digital currencies 21

Annex A (informative) **Factors facilitating or hindering ZKP developments** **22**

Annex B (informative) **Subject binding** **23**

Annex C (informative) **Example of a consistency check between two documents** **24**

Annex D (informative) **Example of ZKP for selective disclosure** **26**

Annex E (informative) **Examples of selective disclosure without using ZKPs** **28**

Annex F (informative) **Example of secure comparison of two numbers** **29**

Annex G (informative) **Implementing digital credentials with ZKP** **31**

Bibliography **36**

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

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

The world is witnessing unprecedented data-driven innovation and growth in digital technologies that include use of big data, AI and blockchain. These technologies are providing societal and economic benefits, as well as improving efficiency, user experience and convenience. At the same time, there is a corresponding increase in privacy risks that requires stronger privacy preserving measures to minimize such risks when designing and implementing solutions. Legislators are introducing new data privacy laws and regulations, and strengthening existing ones, to make organizations accountable and compliant with data privacy protection requirements. They also require support for investigation and regulatory enforcement, where privacy protections are being misused to harm society.

A number of new technologies enable organizations to operate and do business in new ways that are compliant with many regulations, while still protecting privacy. These privacy-enhancing technologies (PETs) apply data protection principles intended to minimize the exposure and use of personal data.

Zero-knowledge proof (ZKP) technology is one such PET, which preserves privacy by eliminating the need to expose or share personal information and personally identifying information (PII), while achieving its desired function. ZKP is a privacy-enhancing technology that can be used to adhere to the principles of collection limitation, user consent and choice and disclosure limitation as mentioned in ISO/IEC 29100.

ZKP allows the validation of data held by an authoritative or an authentic source if it is known to both the prover and the verifier. This results in greater compliance with the data minimization principle of ISO/IEC 29100, since only necessary data are disclosed.

This document begins with an explanation of ZKP and its features. It then describes the privacy and functional requirements that ZKP can address and provides guidelines for using ZKP in a way that is most useful for privacy practitioners.

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection — Guidelines on privacy preservation based on zero-knowledge proofs

1 Scope

This document provides guidelines on using zero-knowledge proofs (ZKP) to improve privacy by reducing the risks associated with the sharing or transmission of personal data between organizations and users by minimizing unnecessary information disclosure. It includes several ZKP functional requirements relevant to a range of different business use cases, then describes how different ZKP models can be used to meet those functional requirements securely.

2 Normative references

There are no normative references in this document.

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
application
software component that issues commands and receives responses to the commands within a system

[SOURCE: ISO/IEC 15961-1:2021, 3.1.1]

3.2
application attestation
confirmation to a server that it is communicating with an instance of its genuine *application* (3.1) that has specific characteristics and is running in a trusted environment

3.3
attribute
characteristic or property of an entity

EXAMPLE An entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes.

[SOURCE: ISO/IEC 24760-1:2025, 3.1.3]

3.4
attribute provider
authority trusted by one or more users and one or more relying parties to issue or verify *attributes* (3.3) related to an entity

[SOURCE: ISO/IEC 27551:2021, 3.2]

© ISO/IEC 2026 – All rights reserved

3.5
authoritative document
document known to be reliable because its authority or authenticity is widely recognized or it bears a signature or seal attesting its validity

3.6
completeness
property where a trusted verifier can be convinced by a trusted prover that a statement is true with overwhelming probability

3.7
computed attribute
attribute (3.3) that is computed from one or more attributes and public information

3.8
digital credential
set of identity attributes and associated data about an individual, cryptographically signed in advance by a credential issuer which includes key information that allows to demonstrate the possession of it

3.9
digital credential issuer
authoritative source that registers subscribers and subsequently issues digital credentials to its subscribers

3.10
digital wallet
application (3.1) that stores and manages digital credentials and keys and can use them upon request

3.11
domain
environment where an entity can use a set of *attributes* (3.3) for identification and other purposes

[SOURCE: ISO/IEC 24760-1:2025, 3.2.3, modified — notes to entry and example have been removed.]

3.12
distinguishing identifier
information which unambiguously distinguishes an entity within a given context

[SOURCE: ISO/IEC 11770-7:2021, 3.5, modified —"within a given context" has been added.]

3.13
identifying attribute
attribute (3.2) that contributes to uniquely identifying a subject within a context

[SOURCE: ISO/IEC TS 29003:2018, 3.8]

3.14
linkability
property for a dataset that it is possible to associate (by linking) a record concerning a data principal with a record concerning the same data principal in a separate dataset

[SOURCE: ISO/IEC 20889:2018, 3.20]

3.15
online
normal state of the data link layer where both application and network management communication are possible

[SOURCE: ISO 17356-1:2005, 2.80]

© ISO/IEC 2026 – All rights reserved

3.16
personal data
information relating to an identified or identifiable natural person

[SOURCE: ISO 17573-2:2025, 3.142]

3.17
proof verification
process where a verifier checks that a proof is valid

Note 1 to entry: Checks can include the cryptography and digital signature.

3.18
prover
entity that presents a proof to a verifier

Note 1 to entry: The prover may be an authoritative source or a trusted intermediary.

3.19
public coin interactive zero-knowledge proof
public coin interactive ZKP
interactive *zero-knowledge proof (ZKP)* (3.26) where the verifier's messages are uniformly random and independent of the prover's messages

3.20
record
set of attributes concerning a single data principal

3.21
soundness
property where a malicious prover, if the statement is false, has only a negligible chance in convincing a verifier that the statement is true

3.22
subject binding
property that assures that a claim is associated with the correct natural person

3.23
trusted execution environment
TEE
aspect of the mobile device comprising either hardware or software, or both, which provides security services to the mobile device computing environment, protects data against general software attacks and isolates hardware and software security resources from the operating system

[SOURCE: ISO 12812-1:2017, 3.60]

3.24
unlinkability
property that ensures that an individual may make multiple uses of resources or services without others being able to link these uses together

Note 1 to entry: There is a distinction between the following two cases: (i) multiple uses of the same services, and (ii) the uses of multiple different services.

[SOURCE: ISO/IEC TR 27550:2019, 3.25, modified — note 1 to entry has been added.]

3.25
verifier
entity relying on a verified proof to prove that a statement is true

Note 1 to entry: The verifier is often the relying party seeking proof that a claimed attribute or statement made by an individual is true.

© ISO/IEC 2026 – All rights reserved

3.26
zero-knowledge proof
ZKP
method involving one or more exchanges between a prover and a verifier where the prover is able to convince the verifier that a statement is true, without revealing to the verifier any additional information beyond that knowledge

3.27
zero-knowledge proof functional requirement
ZKP functional requirement
functional requirements of a system to be fulfilled using *zero-knowledge proof (ZKP)* (3.26)

4 Abbreviated terms

anti-money laundering	AML
central bank digital currency	CBDC
certification revocation list	CRL
common reference string	CRS
counter terrorist financing	CTF
distributed ledger technology	DLT
multi-party computation	MPC
national institute of standards and technology	NIST
non-interactive zero-knowledge proof	NIZKP
online certificate status protocol	OCSP
personally identifiable information	PII
public key certificate	PKC
trusted third party	TTP

5 Introduction to zero-knowledge proofs

5.1 General

In the digital world, not collecting or exposing personal information is the best possible way to preserve the privacy of an individual. However, this is not always practically possible due to the need to use or validate personal information for various business and legal purposes during the course of a business process or the provision of a public service. For instance, it can be necessary for individuals to validate a claimed bank statement to determine eligibility for a loan; or to verify the age of a visitor to a nightclub to ensure compliance to legal requirements.

Sometimes, it is possible to avoid the overcollection of personal information using ZKP techniques since the knowledge of some property about it can be sufficient. Instead of oversharing confidential personal information to satisfy a factual criterion, it is possible to use ZKP to convince the verifier that a certain statement or a set of statements is true. During the proof, only very limited personal information is revealed to the verifier, thereby eliminating the potential harm that can be caused by exposing the personal information.

© ISO/IEC 2026 – All rights reserved