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)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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.

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.

Bibliography

[1] ISO/IEC 9798-5:2009, *Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*

[2] ZKProof Community Reference. Available online from https://docs.zkproof.org/pages/reference/versions/ZkpComRef-0-3.pdf

[3] Verifiable Credentials Data Model v2.0 Available online from https://www.w3.org/TR/vc-data-model-2.0/

[4] Zero Knowledge Proofs applied to auctions. May 16, 2019 Available online from: https://courses.csail.mit.edu/6.857/2019/project/18-doNascimento-Kumari-Ganesan.pdf

[5] The BBS Signature Scheme. July 10, 2023 Available online from: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/ Available online from: https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html

[6] Merkle R.C. "A digital signature based on a conventional encryption function." Conference on the theory and application of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1987. Available from: https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf

[7] Bünz. Benedikt, et al. "Bulletproofs: Short proofs for confidential transactions and more." 2018 IEEE symposium on security and privacy (SP). IEEE, 2018. Available online from: https://eprint.iacr.org/2017/1066.pdf

[8] Pedersen T.P. "Non-interactive and information-theoretic secure verifiable secret sharing." Annual international cryptology conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991. Available online from: https://link.springer.com/content/pdf/10.1007/3-540-46766-1_9.pdf

[9] "Privacy-Preserving Credentials for Self-Sovereign Identity with BBS+ Signatures". Master Degree Thesis. Alessandro Guggino. 2021-2022. Available online from: https://webthesis.biblio.polito.it/24502/1/tesi.pdf

[10] Selective Disclosure for JWTs (SD-JWT) Available online from: https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/

[11] Selective Disclosure CWTs (SD-CWT) Available online from: https://datatracker.ietf.org/doc/draft-prorock-cose-sd-cwt/

[12] ISO/IEC 4922-1:2023, *Information security — Secure multiparty computation — Part 1: General*

[13] ISO/IEC 4922-2:2024, *Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing*

[14] ISO/IEC 29100:2024, *Information technology — Security techniques — Privacy framework*

[15] ISO 31000:2018, *Risk management — Guidelines*

[16] ISO/IEC 29134:2023, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[17] ISO/IEC 24760-1:2025, *Information security, cybersecurity and privacy protection — A framework for identity management — Part 1: Core concepts and terminology*

[18] ISO/IEC 11770-7:2021, *Information security — Key management — Part 7: Cross-domain password-based authenticated key exchange*

[19] ISO/IEC 27551:2021, *Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication*

[20] ISO/IEC TS 29003:2018, *Information technology — Security techniques — Identity proofing*

[21] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*

[22] ISO 12812-1:2017, *Core banking — Mobile financial services — Part 1: General framework*

[23] ISO 17356-1:2005, *Road vehicles — Open interface for embedded automotive applications — Part 1: General structure and terms, definitions and abbreviated terms*

[24] ISO 17573-2:2025, *Electronic fee collection — System architecture for vehicle related tolling — Part 2: Vocabulary*

[25] ISO/IEC TR 27550:2019, *Information technology — Security techniques — Privacy engineering for system life cycle processes*

[26] ISO/IEC 10118-1:2016, *Information technology — Security techniques — Hash-functions — Part 1: General*

[27] ISO/IEC 10118-2:2010, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*

[28] ISO/IEC 10118-3:2018, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

[29] ISO/IEC 10118-4:1998/Amd 1:2014, *Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic — Amendment 1: Object identifiers*

[30] ISO/IEC 20008-2:2013, *Information technology — Security techniques — Anonymous digital signatures — Part 2: Mechanisms using a group public key*

[31] ISO/IEC 20008-3:2024, *Information security — Anonymous digital signatures — Part 3: Mechanisms using multiple public keys*