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 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.