



DPC: 24/30456460 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 17 December 2024

Origin: International

Latest date for receipt of comments: 09 February 2025

Project No. 2022/01096

Responsible committee: IST/33 Information security, cybersecurity and privacy protection

Interested committees:

Title: Draft BS EN ISO/IEC 27565 . Information security, cybersecurity and privacy protection. Guidelines on privacy preservation based on zero knowledge proofs.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 09 February 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 27565

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

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-12-17

Voting terminates on:
2025-03-11

This document is circulated as received from the committee secretariat.

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.

Reference number
ISO/IEC DIS 27565:2024(en)

Full document details: 24/30456460 DC



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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	5
5.1 Interactive and Non-interactive ZKP	6
5.1.1 General	6
5.1.2 Interactive zero-knowledge proofs	6
5.1.3 Non-interactive zero-knowledge proofs	7
5.2 Components of a ZKP system	7
5.2.1 Setup module	7
5.2.2 Prover module	9
5.2.3 Verifier module	9
5.3 Characteristics of ZKPs	10
5.4 ZKP performance	11
6 Use cases of ZKPs	11
6.1 Requirements for implementing ZKPs	11
6.1.1 Attribute providers	11
6.1.2 Subject binding	12
6.1.3 Replay attack detection or protection	13
6.2 Proving some properties of a hidden attribute	13
6.3 Proving the contents in an authoritative document	14
6.4 Proving the contents across several authoritative documents	15
6.5 Selective disclosure of attributes	15
6.5.1 Pre-generation of digital credentials	16
6.5.2 On-demand generation of digital credentials	16
7 Privacy Preservation using Zero Knowledge Proofs	17
7.1 General	17
7.2 Privacy Principles in the context of ZKP	17
7.3 Privacy Risk Assessment	17
7.4 Privacy Functional Requirements for ZKP	18
7.4.1 General	18
7.4.2 Collection limitation	18
7.4.3 Data minimization	18
7.4.4 Options and choice	19
7.4.5 Selective disclosure	19
7.4.6 Purpose legitimacy and specification	19
7.4.7 Anonymity of the authority that has issued the attestation	19
7.4.8 Non-disclosure of the identity of the verifiers to the attribute issuer	19
7.4.9 Use, retention and disclosure limitation	19
7.4.10 Accuracy and quality	19
7.4.11 Openness, transparency and notice	19
7.4.12 Individual participation and access	19
7.4.13 Accountability	19
7.4.14 Information security	20
7.4.15 Unlinkability	20
7.5 Security Considerations	20
7.5.1 Alice and Bob collusion attack	20
7.5.2 Use of an authoritative document or of a trusted authority	21
8 Functional Use Cases	21

8.1	Functional use examples	21
8.2	Selection of ZKP models	21
9	Business Use Examples	22
9.1	Age Verification	22
9.2	Fraud Prevention	22
9.3	Auction	23
9.4	Disability Proof	23
9.5	Distributed Ledger Technologies (DLT) and blockchains	23
9.6	Central Bank Digital Currencies (CBDCs)	24
Annex A (informative) Factors facilitating or hindering ZKP developments		25
Annex B (informative) An example of a consistency check between two documents		26
Annex C (informative) An example of selective disclosure		28
Annex D (informative) An example of secure comparison of two numbers		30
Annex E (informative) A ZKP usage example using digital credentials		32
Bibliography		37

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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 Technical Committee ISO/TC JTC1, *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.

Introduction

The world is witnessing unprecedented data-driven innovation and growth in digital technologies that include use of Big Data, IoT, AI, Blockchain etc all of which are providing societal and economic benefits, as well as improving efficiency, user experience and convenience. But there is a corresponding increase in privacy risks that requires appropriately stronger privacy preserving measures when designing and implementing solutions. Legislators are introducing new data privacy laws and regulations, and they are strengthening existing ones, to make organisations accountable and compliant regarding data privacy protection, with steep penalties for contraventions. However, they also require support for investigation and regulatory enforcement, where privacy protections are being misused to harm society.

A number of new technologies enable organisations 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 the desired function. ZKP is a privacy enhancing technology, and can be used to adhere to the principles of "collection limitation", "user consent and choice" and "disclosure limitation" as mentioned in ISO 29100.

This technology also allows the validation of data held by an authoritative or an authentic source of the data if it is known to both the prover and the verifier. This results in greater regulatory compliance with the disclosure of data that is only necessary.

This document begins with an explanation of ZKP and its features. The privacy and functional requirements that ZKP can address are then described, so guidelines for using ZKP can then be described in a way that is most useful for a privacy practitioner.

To clarify, ZKP functional requirements means the functional requirements of the system to be fulfilled using ZKP, rather than the functional requirements of ZKP.

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 organisations 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

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 29100:2024, *Information technology — Security techniques — Privacy framework*

ISO 31000:2018, *Risk management — Guidelines*

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

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 attestation

confirmation to a server that it is communicating with an instance of its genuine application that has specific characteristics and running in a trusted environment

3.2

attribute

characteristic or property of an entity

[SOURCE: ISO/IEC 24760-1:2019]

Note 1 to entry: For example, an entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes.

3.3

attribute provider

authority trusted by one or more users and one or more relying parties to issue or verify attributes related to an entity

[SOURCE: ISO/IEC 27551:2021]

3.4

authoritative document

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

3.5

completeness

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

3.6

computed attribute

attribute that is computed from one or more attributes and public information

3.7

data principal

entity to which data relates

Note 1 to entry: The term “data principal” is broader than “PII principal” (or “data subject” as used elsewhere), and can denote any entity such as a person, an organization, a device, or a software application.

3.8

dataset

collection of data

3.9

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

3.10

digital credential issuer

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

3.11

digital wallet

application that stores and manages digital credentials and keys and is able to use them upon request using either online or near-field communication (NFC) technology

Note 1 to entry: an application is a software component that can be installed and run on some hardware, like a smartphone, a tablet, or other electronic device.

3.12

domain

environment where an entity can use a set of attributes for identification and other purposes

[SOURCE: ISO/IEC 24760-1:2019]

3.13

dynamic attribute

attribute that changes quite often over time

Note 1 to entry: For example, the GPS coordinate of the person changes quite frequently.

3.14

distinguishing identifier

information which unambiguously distinguishes an entity within a given context

[SOURCE: ISO/IEC 11770-7:2021, 3.5 with the addition of "within a given context"]

3.15

identifying attribute

attribute that contributes to uniquely identifying a subject within a context

[SOURCE: ISO/IEC TS 29003:2018]

3.16

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]

3.17

mobile device

personal device with mobile communication

[SOURCE: ISO 12812-1:2017, 3.24]

3.18

personal attribute

attribute of a person that describes certain aspects of that person

Note 1 to entry: For example, name, date of birth, location, blood pressure, domicile address, employer, phone number, email address, etc

3.19

personal data

information relating to an identified or identifiable natural person

[SOURCE: ISO/TS 17573-2:2020, 3.136]

3.20

proof verification

process where a verifier checks that a proof is valid

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

3.21

prover

entity that presents a proof to a verifier

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

3.22

public coin ZKP protocol

interactive ZKP protocol where the verifier's messages are uniformly random and independent of the prover's messages

3.23

record

set of attributes concerning a single data principal

3.24

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

3.25

static attribute

attribute that does not change over time

Note 1 to entry: For example, name at birth or date of birth does not change.

3.26

data subject

natural person to whom data refer

[SOURCE: ISO/IEC 25237:2017,3.18]

3.27

subject binding

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

3.28

trusted execution environment

aspect of the mobile device comprising hardware and/or software 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]

3.29

unlinkability

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

[SOURCE: ISO/IEC TR 27550:2019, 3.25]

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.

3.30

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.

3.31

verified attribute

personal attribute that has been successfully verified by an entity to be correctly associated either with an individual or with an individual account

3.32

zero-knowledge proof

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

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	OCSF
Personally identifiable information	PII
Public key certificate	PKC
Trusted execution environment	TEE
Trusted third party	TTP
Zero-knowledge Proof	ZKP

5 Introduction to Zero-knowledge Proofs

In the digital world, not collecting or exposing personal information is the best possible way to preserve 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, one may need 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 national laws.

Sometimes, it is possible to avoid the collection of personal information using ZKP techniques since the knowledge of some property about it may be sufficient. Instead of sharing confidential personal information in order 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. The personal information is not revealed to the verifier, only the proof is communicated, thereby eliminating the potential harm that may be caused by exposing the personal information.

When making a PII-based decision, personal information (attributes) have to be associated with the correct subject. Using ZKPs, the prover can prove that the relevant attributes satisfy certain criteria and those attributes are associated with the correct subject in a privacy-preserving manner.

ZKP is an important privacy-enhancing tool based on cryptography. Every ZKP system involves at least a prover and a verifier. A ZKP system is a protocol specification for how a prover and verifier(s) can interact so that the prover can convince the verifier(s) that a given statement or a set of statements is true. ZKPs were initially developed by the academic community in the 1980s and have seen tremendous improvements since then. They are now of practical feasibility in multiple domains of interest across different industries and to a large community of developers and researchers. ZKPs can have a positive impact in industries, agencies and for personal use, by allowing privacy-preserving applications, where permitted, to learn some properties or characteristics of or about private data, despite not disclosing their values.

A ZKP makes it possible to prove that a statement or a set of statements is true while preserving confidentiality of secret information. This makes sense when the veracity of the statement or a set of statements is not obvious on its own, but the prover knows relevant secret information that enables a proof to be made.

A ZKP protocol must support the following three properties:

- 1) completeness: If the prover's statement is true, then the verifier will accept it with overwhelming probability.
- 2) soundness: If the prover's statement is false, then no matter how the prover behaves, the verifier will reject it with overwhelming probability.
- 3) zero-knowledge: if the statement is true, no verifier learns any information other than the fact that the statement is true.

For more details on ZKP: See [2] ZKProof Community Reference.

In addition to the three well-known properties applicable to ZKP protocols, a Non-Interactive Zero-knowledge Proof (NIZKP) protocol should support the following two additional properties:

- 1) replay detection / protection against the same verifier: If a user saves a previously sent NIZKP exchange and replays it to the same verifier, that verifier shall be able to reject it with high probability.

This can be resolved by including a challenge sent by the verifier or a date and time in the ZKP.

- 2) replay detection / protection against a different verifier: If a user saves a previously sent NIZKP exchange and replays it to a different verifier, that verifier shall be able to reject it with high probability.

This can be resolved by including an identifier of the designated verifier in the ZKP.

This document only focuses on privacy preservation using ZKPs.

Note In some applications, zero-knowledge techniques are used during an authentication process (see ISO/IEC 9798-5:2009 Entity authentication — Part 5: Mechanisms using zero-knowledge techniques[1]).

The mechanisms described in ISO/IEC 9798-5:2009 are constructed using the principles of zero-knowledge techniques, but are not necessarily strictly zero-knowledge according to the definition of ZKP made in this document, because ISO/IEC 9798-5:2009 states that “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”.

5.1 Interactive and Non-interactive ZKP

5.1.1 General

ZKP can be divided into two categories: (a) interactive ZKP and (b) non-interactive ZKP. An interactive ZKP requires several rounds of interaction between the prover and the verifier before a decision can be made. Whereas, for a non-interactive ZKP, the prover can just send one-message proof to the verifier; in practice, the verifier does not need to be online when the proof was produced.

5.1.2 Interactive zero-knowledge proofs

To establish such proofs, both the verifier and the prover need to be online at same time. In order to prove the same statement again to another verifier, the prover needs to interact with another verifier again.

During an interactive ZKP protocol, three or more messages need to be exchanged between the prover and the verifier. If the verifier's messages are uniformly random and independent of the prover's messages, we say that this ZKP is a public coin protocol.

A special type of public coin interactive ZKP is the Sigma protocol, which involves the exchange of three values:

- 1) During the commitment phase, a first message is sent from the prover to the verifier that contains an element **a**,
- 2) During the challenge phase, a second message (fresh random value) is sent from the verifier to the prover that contains a challenge **c**, and
- 3) During the response phase, a final message **z** is computed by the prover and sent from the prover to the verifier.

At the end of the interaction, the verifier makes a decision whether a statement **x** is true or false based on the values of (**a,c,z**).