

ISO/IEC 27565:2026-02 (E)

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

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 |
| 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 |