International Standard

ISO/IEC 23264-2

First edition
2024-08

Information security — Redaction of authentic data —

Part 2: Redactable signature schemes based on asymmetric mechanisms

Sécurité de l'information — Rédaction de données authentifiées —

Partie 2: Schémas de signature éditable basés sur des mécanismes asymétriques

Reference number
ISO/IEC 23264-2:2024(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*.

A list of all parts in the ISO/IEC 23264 series can be found on the ISO and IEC websites.

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

This document specifies cryptographic mechanisms to redact authentic data where the redactable attestation scheme is based on asymmetric mechanisms.

Attestation schemes, in particular digital signature schemes or message authentication codes, can be used to provide data integrity and data origin authentication. Redactable attestation can be used to blank out parts, herein called fields, of an attested message without invalidating the attestation on the remaining contents of the message. This redaction process requires a redaction key. The redaction key computationally does not reveal the attestation key, by which schemes can allow for public redactions. Any other modification of the document (e.g. redaction of other message parts, or insertion/modification of any parts) will invalidate the attestation. Schemes can have specific additional security properties, which are described in ISO/IEC 23264-1. The achievable properties for each scheme are stated in this document.

Redactable attestation schemes are a basic building block in many privacy-preserving applications, such as privacy-preserving data sharing or authentication, where a party may decide to forward only necessary information to a receiver, while the latter is still assured that the received information was previously attested, for example, by a public authority.

The objective of the ISO/IEC 23264 series is to remedy existing incompatibilities or inconsistently defined properties found in academic literature, and to ease the real-world adoption of this technology. Specifically, the goal of this document is to focus on algorithms that enable the authenticity-preserving redaction of general data structures like sets or ordered lists based on asymmetric cryptography. It adheres to the common terminology and description of cryptographic properties for redactable attestation schemes given in ISO/IEC 23264-1.

The ISO/IEC 23264 series complements ISO/IEC 27038, which specifies the redaction of digital documents without considering the authenticity of the data.

This document contains the following algorithms based on asymmetric cryptography:

— generic construction from signature schemes and hash-functions

— scheme SBZ02-MERSAProd

— scheme BBDFFKMOPPS10

— scheme DPSS15

— scheme MHI06

— scheme MIMSYTI05

Information security — Redaction of authentic data —

Part 2:
Redactable signature schemes based on asymmetric mechanisms

1 Scope

This document specifies cryptographic mechanisms to redact authentic data. The mechanisms described in this document offer different combinations of the security properties defined and described in ISO/IEC 23264-1. For all mechanisms, this document describes the processes for key generation, generating the redactable attestation, carrying out redactions and verifying redactable attestations.

This document contains mechanisms that are based on asymmetric cryptography using three related transformations:

— a public transformation defined by a verification key (verification process for verifying a redactable attestation),

— a private transformation defined by a private attestation key (redactable attestation process for generating a redactable attestation), and

— a third transformation defined by the redaction key (redaction process) allowing to redact authentic information within the constraints set forth during generation of the attestation such that redacted information cannot be reconstructed.

This document contains mechanisms which, after a successful redaction, allow the attestation to remain verifiable using the verification transformation and attest that non-redacted fields of the attested message are unmodified. This document further details that the three transformations have the property whereby it is computationally infeasible to derive the private attestation transformation, given the redaction and or the verification transformation and key(s).

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 23264-1, *Information security — Redaction of authentic data — Part 1: General*

Bibliography

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

[2] ISO/IEC 2382:2015, *Information technology — Vocabulary*

[3] ISO/IEC 27038:2014, *Information technology — Security techniques — Specification for digital redaction*

[4] C. Brzuska, H. Busch, O. Dagdelen, M. Fischlin, M. Franz, S. Katzenbeisser, M. Manulis, C. Onete, A. Peter, B. Poettering, and D. Schröder. *Redactable Signatures for Tree-Structured Data: Definitions and Constructions*. In ACNS, 2010.

[5] D. Derler, H. C. Pöhls, K. Samelin, and D. Slamanig. *A General Framework for Redactable Signatures and New Constructions*. In ICISC, 2015.

[6] T. Izu, N. Kunihiro, K. Ohta, M. Takenaka, and T. Yoshioka. *A Sanitizable Signature Scheme with Aggregation*. In: ISPEC, 2007.

[7] T. Izu, N. Kunihiro, K. Ohta, M. Sano, and M. Takenaka. *Sanitizable and Deletable Signature*. In: WISA, 2008.

[8] T. Izu, N. Kanaya, M. Takenaka, and T. Yoshioka. *PIATS: A Partially Sanitizable Signature Scheme*. In: ICICS, 2005.

[9] R. Johnson, D. Molnar, D. Song, and D. Wagner. *Homomorphic signature schemes*. In CT-RSA, 2002.

[10] A. Kundu and E. Bertino. *Structural Signatures for Tree Data Structures*. In PVLDB, 2008.

[11] K. Miyazaki, G. Hanaoka, and H. Imai. *Digitally signed document sanitizing scheme based on bilinear maps*. In ASIACCS, 2006.

[12] R. Steinfeld, L. Bull, and Y. Zheng. *Content extraction signatures*. In ICISC, 2001.

[13] K. Samelin, H. C. Pöhls, A. Bilzhause, J. Posegga, and H. de Meer. *Redactable signatures for independent removal of structure and content*. In ISPEC, 2012.

[14] K. Miyazaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura, S. Tezuka, and H. Imai. *Digitally Signed Document Sanitizing Scheme with Disclosure Condition Control.* In IEICE Transactions 88-A(1): pp. 239-246, 2005.

[15] Pöhls H.C., Samelin K. *On Updatable Redactable Signatures*. In Proc. of the 12th International Conference on Applied Cryptography and Network Security (ACNS 2014), Springer, 2014.

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

[17] R. C. Merkle. *A digital signature based on a conventional encryption function*. In: CRYPTO, 1987.

[18] ISO/IEC 14888 (all parts), *Information security — Digital signatures with appendix*

[19] ISO/IEC 15444-1, *Information technology — JPEG 2000 image coding system — Part 1: Core coding system*

[20] ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

[21] ISO/IEC 15946-5, *Information security — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

[22] ISO/IEC 18033-5, *Information technology — Security techniques — Encryption algorithms — Part 5: Identity-based ciphers*

[23] Faz-Hernandez A., Scott S., Sullivan N., Wahby R.S., Wood C.A. *Hashing to Elliptic Curves*. https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/ or https://github.com/cfrg/draft-irtf-cfrg-hash-to-curve/, version 16, 2023.

[24] Wahby, R.S. and D. Boneh. *Fast and simple constant-time hashing to the BLS12-381 elliptic curve.* Trans. on Cryptographic Hardware and Embedded Systems, 2019.

[25] Mitchell C., Chen L. *WG 2 SD7 — Conversion functions (2nd Edition)*. https://www.din.de/en/meta/jtc1sc27/downloads

[26] ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

[27] ISO/IEC 9804:1998, *Information technology — Open Systems Interconnection — Service definition for the Commitment, Concurrency and Recovery service element*

[28] ISO/IEC 9796-2, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

[29] RFC 8017, *PKCS #1: RSA Cryptography Specifications Version 2.2*

[30] ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

[31] F. Hess, N. Smart, F. Vercauteren, *The Eta Pairing Revisited*. IEEE Trans. Information Theory, 52(10): 4595-4602, 2006.

ICS 35.030
Price based on 58 pages

iso.org