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)

© ISO/IEC 2024



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 Symbols and conventions **3**
4.1 Symbols 3
4.2 Conventions 4

5 General **5**

6 Generic construction from signature schemes and hash-functions **5**
6.1 Parameters 5
6.2 Construction 6
6.2.1 Key generation process 6
6.2.2 Redactable attestation process 6
6.2.3 Redaction process 7
6.2.4 Verification process 8

7 Scheme SBZ02-MERSAProd **8**
7.1 Parameters 8
7.2 Construction 9
7.2.1 Key generation process 9
7.2.2 Redactable attestation process 9
7.2.3 Redaction process 10
7.2.4 Verification process 11

8 Scheme BBDFFKMOPPS10 ..... **12**
8.1 Parameters 12
8.2 Construction 12
8.2.1 Key generation process 12
8.2.2 Redactable attestation process 12
8.2.3 Redaction process 14
8.2.4 Verification process 15

9 Scheme DPSS15 ..... **17**
9.1 Parameters 17
9.2 Subroutine: RSA Accumulators 17
9.3 Construction 18
9.3.1 Key generation process 18
9.3.2 Redactable attestation process 19
9.3.3 Redaction process 20
9.3.4 Verification Process 20

10 Scheme MHI06 ..... **21**
10.1 Parameters 21
10.2 Construction 22
10.2.1 Key generation process 22
10.2.2 Redactable attestation process 22
10.2.3 Redaction process 23
10.2.4 Verification Process 24

11 Scheme MIMSYTI05 ..... **25**
11.1 Parameters 25
11.2 Construction 25
11.2.1 Key generation process 25
11.2.2 Redactable attestation process 25

© ISO/IEC 2024 – All rights reserved

11.2.3 Redaction process 26
11.2.4 Verification Process 27

Annex A (normative) **Object identifiers** **29**

Annex B (informative) **Overview of properties of redactable signature schemes based on asymmetric mechanisms** **30**

Annex C (informative) **Criteria for inclusion of schemes in this document** **33**

Annex D (informative) **Numerical examples** **34**

Bibliography **57**

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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

© ISO/IEC 2024 – All rights reserved

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 23264-1 and the following 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/

© ISO/IEC 2024 – All rights reserved