INTERNATIONAL STANDARD

ISO/IEC 23264-1

First edition
2021-03

Information security — Redaction of authentic data —

Part 1: General

Sécurité de l'information — Rédaction de données authentifiées —

Partie 1: Généralités

Reference number
ISO/IEC 23264-1:2021(E)

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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 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 website.

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

Digital attestation schemes, in particular digital signature schemes or message authentication codes, can be used to provide data integrity and data origin authentication. A redactable attestation scheme enables the attestation of a message in such a way that, if certain parts of the attested message (known as fields) are redacted (erased, blanked out or permanently removed), the attestation of the redacted message can still be verified. More precisely, upon attesting a message, the attestor knowing the private attestation key can define which parts of the message can later be redacted (in the sense of ISO/IEC 27038) by any entity only knowing the message, the attestation, and the attestor's redaction key. Any other modification of the attested message (e.g. redaction of other message parts or insertion/modification of any parts) invalidates the attestation.

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

The goal of the ISO/IEC 23264 series is to remedy existing incompatibilities or inconsistently defined properties in existing specifications of such schemes, and to ease the real-world adoption of this technology. Specifically, the goal of this document is to lay the foundations for subsequent parts (e.g. focusing on concrete algorithms for the authenticity-preserving redaction of specific document formats like text, pictures, video, etc.) by specifying and defining common terminology and properties for such schemes.

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

Information security — Redaction of authentic data —

Part 1: General

1 Scope

This document specifies properties of cryptographic mechanisms to redact authentic data. In particular, it defines the processes involved in those mechanisms, the participating parties, and the cryptographic properties.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
admissible changes
description of all possible modifications of a *message* (3.12) attested with a *redactable attestation scheme* (3.16) that can be applied within the *redaction process* (3.23) without invalidating the resulting *redacted attestation* (3.18)

Note 1 to entry: The set of admissible changes is called non-trivial, if the admissible changes allow for at least one modification of the original message yielding a redacted message different from the original message.

Note 2 to entry: In the context of this document, the possible modifications of a message are limited to removal of some fields of a message.

3.2
attestation key
private attestation key
secret data item specific to an *attestor* (3.4) and usable only by this entity in the *redactable attestation process* (3.15)

Note 1 to entry: Except for the term "redactable attestation process" instead of "signature process", this definition is consistent with "signature key" as defined in ISO/IEC 14888-1:2008, 3.13.

3.3
attested message
set of data items consisting of the *redactable attestation* (3.14), the *admissible changes* (3.1) and the *fields* (3.10) of the *message* (3.12) which are attested

Note 1 to entry: Depending on the instantiation, if not all admissible changes are part of the attested message, then at least those admissible changes that are relevant for the verification process can be reconstructed from the redactable attestation in combination with the fields of the message which are attested and the verification key.