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)

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.

3.4
attestor
entity using its *private attestation key* (3.2) to perform the *redactable attestation process* (3.15), producing an *attested message* (3.3)

3.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[SOURCE: ISO/IEC 7498-2:1989, 3.3.16, modified — The article has been removed.]

3.6
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/IEC 7498-2:1989, 3.3.21, modified — The article has been removed.]

3.7
digital attestation
data appended to, or a cryptographic transformation of, a *message* (3.12) that allows a recipient of the data to verify the source and *data integrity* (3.6) of the *message* (3.12)

3.8
domain
set of entities operating under a single security policy

Note 1 to entry: In the context of this document, a domain contains all participating attestors, redactors and verifiers.

[SOURCE: ISO/IEC 14888-1:2008, 3.4, modified — Note 1 to entry has been added.]

3.9
domain parameter
data item which is common to and known by or accessible to all entities within the *domain* (3.8)

[SOURCE: ISO/IEC 14888-1:2008, 3.5, modified — The article has been removed.]

3.10
field
sub-string of any length of the *message* (3.12)

3.11
key generation process
process for generating cryptographic keys

3.12
message
string of bits of any length

Note 1 to entry: In the context of this document, the message is always composed of one or several field(s). The exact composition and a decomposition is always obtainable from the message.

[SOURCE: ISO/IEC 14888-1:2008, 3.10, modified — Note 1 to entry has been added.]

3.13
modification instruction
instruction that describes the message redaction, i.e. how a *message* (3.12) is to be redacted by the *redactor* (3.24) within a *redaction process* (3.23)

Note 1 to entry: Modification instructions are called non-trivial if the message input to, and the message obtained by, the redaction process are not identical.

3.14
redactable attestation
redactable digital attestation
data resulting from the redactable attestation process that is appended to a *message* (3.12) that allows a recipient of this data to verify the source and integrity of the *message* (3.12)

Note 1 to entry: This string of bits may have an internal structure that is specific to the attestation mechanism.

3.15
redactable attestation process
process which takes as inputs the *message* (3.12), the *private attestation key* (3.2), the *admissible changes* (3.1) and the *domain parameters* (3.9), and which outputs a *redactable attestation* (3.14)

3.16
redactable attestation scheme
set of processes that achieves *digital attestation* (3.7) and supports the creation and verification of *redactable attestations* (3.14) together with a *redaction process* (3.23)

3.17
redacted admissible changes
admissible changes (3.1) that are the output of the *redaction process* (3.23)

Note 1 to entry: The redacted admissible changes are derived during the redaction process from the given admissible changes by applying modification instructions.

3.18
redacted attestation
redacted digital attestation
attestation resulting from applying the *redaction process* (3.23) at least once with some *modification instructions* (3.13)

Note 1 to entry: This string of bits may have an internal structure that is specific to the attestation mechanism.

3.19
redacted attested message
set of data items resulting from the *redaction process* (3.23) which consists of the *redacted attestation* (3.18), the *redacted admissible changes* (3.17) and the *redacted message* (3.20) composed from those *fields* (3.10) that have not been subject to any redaction

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

3.20
redacted message
message (3.12) that is the output from the *redaction process* (3.23)

3.21
redaction
removal of a *field* (3.10) such that it results in the irreversible and permanent removal of information contained within that field from the *message* (3.12)

Note 1 to entry: The removal of a field only removes the information contained within that field. Information that can be derived from other fields of the message or from other sources is not removed.

3.22
redaction key
set of public data elements which is related to an *attestor's* (3.4) *private attestation key* (3.2) and which is used by the *redactor* (3.24) in the *redaction process* (3.23)

Note 1 to entry: Depending on the instantiation, the redaction key may be private or public. In any case, knowledge of the redaction key does not result in information about the attestor's private attestation key.

3.23
redaction process
process which takes as inputs the *attested message* (3.3), the *domain parameters* (3.9), the *redaction key* (3.22) and the *modification instructions* (3.13), and which outputs a *redacted attested message* (3.19) by applying the given modification instructions

Note 1 to entry: The input to the redaction process may be an attested message or a redacted attested message obtained by one (or potentially multiple) previous application(s) of a redaction process.

Note 2 to entry: The admissible changes are implicitly provided as inputs as part of the attested message.

Note 3 to entry: It is only possible to create a redacted attestation which will be verifiable using the attestor's verification key, if a given set of modification instructions are in accordance with the attestor-specified admissible changes.

3.24
redactor
entity that carries out the *redaction process* (3.23)

3.25
verification key
set of data elements which is related to an attestor's *private attestation key* (3.2) and which is used by the *verifier* (3.27) in the *verification process* (3.26)

Note 1 to entry: Depending on the instantiation, the verification key may be private or public. In the case of a public verification key, knowledge of the verification key cannot be used to deduce information about the attestor's private attestation key.

3.26
verification process
process which:

- takes as input the *attested* (potentially redacted) *message* (3.13), consisting of the (potentially redacted) *message* (3.12), the (potentially redacted) *admissible changes* (3.1) and the (potentially redacted) *redactable attestation* (3.14), the *verification key* (3.25) and the *domain parameters* (3.9);
- checks whether the given attestation is a valid attestation for the given message under the given verification key; and
- gives as output the result of the attestation verification: valid or invalid

Note 1 to entry: It is only possible to output valid if the modification instructions that have been applied in one (or potentially many) application (s) of the redaction process are in accordance with the attestor-specified admissible changes.

Note 2 to entry: Depending on the instantiation, if not all the (potentially redacted) admissible changes are part of the attested (potentially redacted) message, then at least those (potentially redacted) admissible changes that are relevant for the verification process can be reconstructed from the (potentially redacted) attestation in combination with the (potentially redacted) message and the verification key.

3.27
verifier
entity that performs the *verification process* (3.26)

4 Symbols and conventions

4.1 Symbols

adm	description of redacted or original admissible changes
adm’	description of redacted admissible changes
ak	attestation key
att	redactable or redacted attestation
att’	redacted attestation
m	redacted or original message
m’	redacted message
$m_1, \ldots, m_n$	individual fields of a message
mod	description of modification instructions
n	number of fields in a message
rk	redaction key
vk	verification key
Z	set of one or more domain parameters

4.2 Conventions

A triple of a message, an attestation and a list of admissible changes is denoted by (*m*, *att*, *adm*). In the same way, a triple of a redacted message, a redacted attestation and redacted admissible changes is denoted by (*m’*, *att’*, *adm’*).

Specific values of a symbol (e.g. *sym*) are distinguished using superscripts (e.g. *sym**, *sym***, etc.)

5 General model and processes

5.1 General

Digital attestation schemes such as digital signature schemes or message authentication codes can be used to prove data origin authentication and data integrity for entire messages. In particular, they do not support any subsequent modification of a message without invalidating the digital attestation. In contrast, redactable attestation schemes enable the attestation of message in a way which allows the subsequent redaction (erasure or permanent removal) of certain parts of the attested message (known as fields), while protecting against any other modification. This redaction can be carried out by any entity only knowing the message, the attestation, and the attestor’s redaction key, but not the private attestation key.

5.2 Parties and processes

The parties participating in a redactable attestation scheme are:

a) an attestor;

b) a redactor;

c) a verifier.

A redactable attestation scheme is defined by the specification of the following processes:

a) a key generation process;

b) a redactable attestation process;

c) a redaction process;

d) a verification process.

NOTE The mechanism used by the involved parties to agree on a specific redactable attestation scheme is outside the scope of this document.

5.3 General model

The following parties perform processes relating to a redactable attestation scheme.

a) An attestor shall:

   1) obtain the attestation key *ak*, the domain parameters *Z*, and admissible changes *adm*;

   2) use the private attestation key *ak*, the domain parameters *Z*, and the admissible changes *adm* to attest the message *m*;

   3) obtain a redactable attestation *att* possibly containing some information about the admissible changes *adm*.

b) A redactor shall:

   1) obtain the attestor's redaction key *rk*, the domain parameters *Z*, the (potentially redacted) message *m*, the (potentially redacted) redactable attestation *att*, the (potentially redacted) admissible changes *adm*, and modification instructions *mod*;

   2) if not provided as input, use the redaction key *rk*, the domain parameters *Z*, the (potentially redacted) message *m* and the (potentially redacted) redactable attestation *att* to reconstruct the (potentially redacted) admissible changes *adm*;

   3) use the modification instructions *mod* to redact the message *m*, and adapt (if necessary) the admissible changes *adm*;

   4) use the attestor's redaction key *rk*, the domain parameters *Z*, and the modification instructions *mod* to redact the redactable attestation *att*;

   5) obtain a redacted message *m'*, redacted admissible changes *adm'* and a redacted attestation *att'*.

c) A verifier shall:

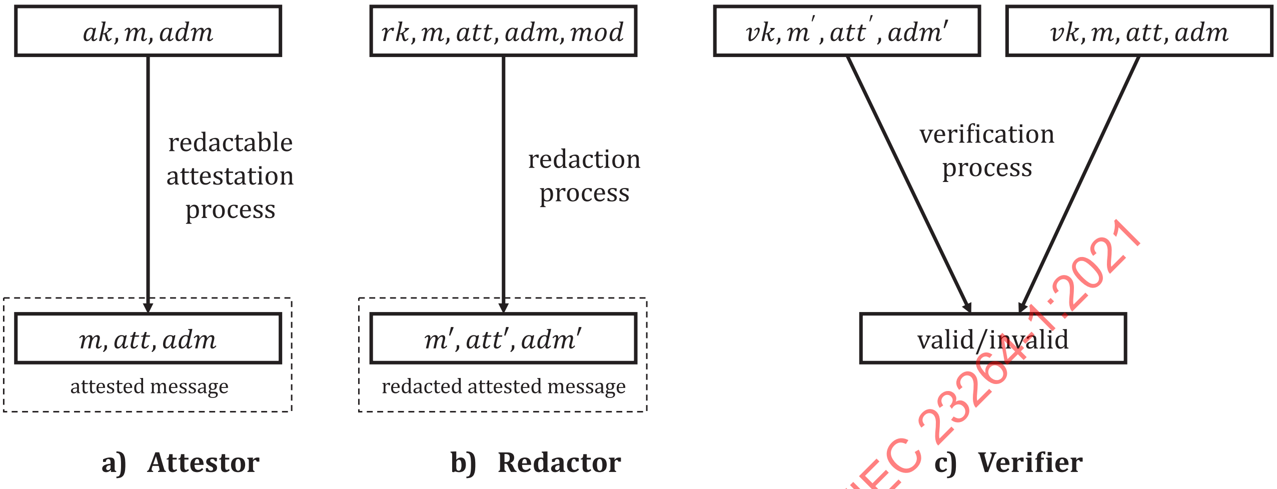
   1) obtain the attestor's verification key *vk*, the domain parameters *Z*, the (potentially redacted) message *m*, the (potentially redacted) redactable attestation *att*, and the (potentially redacted) admissible changes *adm*;

   2) if not provided as input, use the verification key *vk*, the domain parameters *Z*, the (potentially redacted) message *m* and the (potentially redacted) redactable attestation *att* to reconstruct the (potentially redacted) admissible changes *adm*;

   3) use the verification key *vk*, the domain parameters *Z*, the (potentially redacted) message *m* and the (potentially redacted) admissible changes *adm* to verify the (potentially redacted) redactable attestation *att*;

   4) obtain *valid* or *invalid*.

Figure 1 provides an overview of the processes executed by the parties in a redactable attestation scheme. For brevity, Figure 1 does not show the domain parameters *Z*. The input to the redaction process as well as the verification process can be an original (i.e. an attested message) or redacted attested message (i.e. the output of a previous redaction process).



a) Attestor

b) Redactor

c) Verifier

Figure 1 — Overview of processes in a redactable attestation scheme

5.4 Specification of processes

5.4.1 Key generation process

The key generation process of a redactable attestation mechanism consists of the following two procedures:

a) generating the domain parameters *Z*;

b) generating the attestation key *ak*, the redaction key *rk*, and the verification key *vk*.

The first procedure is executed once when the domain is set up. The resulting domain parameters are needed in subsequent processes and functions. The second procedure is executed for each attestor within the domain.

NOTE 1 Validation of domain parameters and keys can be required. However, how this is achieved is outside the scope of this document.

NOTE 2 Key distribution is outside the scope of this document.

5.4.2 Redactable attestation process

In the redactable attestation process, the attestor computes its redactable attestation for a given message and a given definition of admissible changes based on a given decomposition of the message into fields. The redactable attestation (including necessary information for its verification and redaction) is appended to the message to form the attested message.

Specifically, the following data items are required for the redactable attestation process:

- the domain parameters *Z*;
- the attestation key *ak*;
- the message *m*;
- the admissible changes *adm*.

The process generates a redactable attestation *att* that binds the message *m* to the admissible changes *adm* and to the verification key *vk* corresponding to the attestation key *ak*.

5.4.3 Redaction process

In the redaction process the redactor produces a redacted attestation of a given redacted attested or attested message according to given modification instructions. The input to the redaction process may be an attested message or a redacted attested message. The output of the redaction process is a redacted message and a corresponding redacted attestation including information about the redacted admissible changes. This means that a redacted attested message may be subject to multiple consecutive redactions.

NOTE 1 Whether or not any previous application(s) of a redaction process are detectable by a verifier or subsequent redactor depends on the security properties of the scheme (see 6.2.1).

The following data items are required for the redaction process:

- the domain parameters *Z*;
- the redaction key *rk*;
- the original or redacted message *m*;
- the redactable or redacted attestation *att*;
- the original or redacted admissible changes *adm*;
- the modification instructions *mod* that are in accordance with the admissible changes *adm*.

If the admissible changes *adm* are not directly provided as input, the redaction process first reconstructs them using the redaction key *rk*, the domain parameters *Z*, the message *m* and the redactable attestation *att*.

The process produces as output a redacted attestation *att'* that corresponds to the redacted message *m'* obtained by applying the modification instructions *mod* to the input message *m*. If the input attestation *att* is valid on *m* under *vk* and the applied modification instructions *mod* are within the limits of the attestor-authorized admissible changes *adm*, then the resulting deducted (*m'*, *att'*) yields a positive output when input to the verification processes together with the verification key *vk* corresponding to the attestor's attestation key *ak*. In addition, the process produces *adm'* as a potentially modified version of *adm*.

This process does not require access to the attestor's attestation key *ak* or verification key *vk* in order to function correctly. Access to the redaction key *rk* does not yield information about the attestor's attestation key *ak* nor the verification key *vk*.

NOTE 2 To allow the redaction process to be a public operation the attestor's redaction key *rk* can be made public, e.g. by distributing it alongside the attested message. This has no effect on the confidentiality of the attestor's attestation key *ak* nor of the verification key *vk*. Thus, secure schemes with a public or empty *rk* still achieve digital attestation of the attested message.

5.4.4 Verification process

The following data items are required for the verification process:

- the domain parameters *Z*;
- the verification key *vk*;
- the original or redacted message *m*;
- the redactable or redacted attestation *att*;