ISO/DTS 24574

ISO/TC 171/SC 1~~/WG12~~

Secretariat: BSI

Date: 2024-10-14

Document management applications~~-~~ — Specification for a digital safe

~~DTS stage~~

~~**Warning for WDs and CDs**~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

~~*To help you, this guide on writing standards was produced by the ISO/TMB and is available at*~~

~~*A model manuscript of a draft International Standard (known as "The Rice Model") is available at*~~

Applications en gestion des documents — Spécification pour un coffre fort numérique

ISO copyright office
CP 401 • Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. Phone: + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail: copyright@iso.org
Website: www.iso.orgwww.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO ~~documents~~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~~ISO draws attention to the possibility that ~~some of~~ the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~use of (a) patent(s). ISO takes 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 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~~.~~. ISO 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).~~

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation ~~on~~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 ~~the following URL:~~ www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 171, ~~*[name of committee]*~~*Document management applications*, Subcommittee SC ~~*##, [name of subcommittee]*~~. 1, *Quality, preservation and integrity of information*.

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~~A list of all parts in the ISO ##### series can be found on the ISO website.~~

Introduction

As part of their activities, public organizations and private companies increasingly use digital content, whether it is produced by these organizations or ~~comes~~by others. Digital content includes documents, data, images and sound that can be referred to as digital objects. These can be natively electronic or result from ~~other organizations.~~ the digitization of printed documents.

To meet legal or management requirements, ~~they~~organizations and companies are expected to use trusted technology to ensure the integrity over time of all types of digital content ~~such as documents, data, images and sound. This digital content can be referred to as digital objects, which can be natively electronic or result from the digitization of printed documents.~~

~~For that reason~~. Thus, there is a need for software that can ensure the integrity, confidentiality and availability of the digital objects over time, including office documents, PDF files, scan results, JPEG pictures, etc.

This document defines the minimum functions of a digital safe:

— ~~maintain~~maintaining the integrity, confidentiality and availability of digital objects over time~~,~~;

— ~~preserve~~preserving the chain of custody~~,~~;

— ~~manage~~managing retention periods or freeze status making it impossible to delete digital objects during a determined period~~,~~;

— defining the minimum elements to allow transfer of digital objects between two different digital safes~~,~~;

— ~~define~~defining the minimum elements of traceability of the software operation~~,~~;

— ~~manage~~managing replication of digital objects~~,~~;

— ~~ensure~~ensuring sustainability of business operations, business continuity~~/~~ and disaster recovery~~, and~~;

— ~~define~~defining encryption requirements.

~~As this~~This document is limited to the functions of integrity, traceability, confidentiality and availability of digital objects of any kind~~, it~~. It does not address sustainability of digital objects (i.e. the component does not control and convert the formats in which digital objects are stored).

In order for users to have confidence in their electronic safe, this software should have the same basic functions and maintain a common minimum of technical metadata, regardless of the software publisher. These fundamental elements are also the necessary condition to ensure interoperability between several electronic safes.

This document is intended for:

— software developers or integrators ~~of a such solution~~ who wish to develop or integrate a digital safe~~,~~;

— service providers ~~like~~, such as trust service providers of digital storages, who ~~is~~are looking for software to support their services~~,~~;

— software ~~publisher~~publishers who wants to have a repository to develop digital safe software~~,~~;

— consultants and auditors~~,~~ who ~~wishes~~wish to have a reference document to build or audit an archiving system ~~or audit this type of system.~~

~~ISO TS 24574 ISO~~This document is intended to complement other ISO documents that deal with electronic archiving. Annex A~~Appendix A~~ provides a list of these documents and ~~ISO TS 24574's links~~their link to ~~them~~this document.

Document management applications — Specification for a digital safe

1 Scope

This document specifies the minimum functional requirements of digital safe software in order to ensure the integrity, confidentiality and availability of the digital objects it stores.

~~A digital safe is a software package operating on one or more hardware platforms.~~

This document does not address system environments ~~that can be necessary~~ for the operation of the digital safe, such as physical security (fire extinguishing system, armoured doors, presence detectors, etc.), power supply security (generators and transformers) or telecommunication lines.

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 8601-1, *Date and time ~~-~~ — Representations for information interchange — Part 1: Basic rules*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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/

3.1 ~~Application~~ application programming interface API

collection of invocation methods and associated parameters used by one piece of software to request actions from another piece of software

[SOURCE: ISO/IEC TR 13066-6:2014, 2.2]

~~3.1~~3.2 audit trail

a record of the activity taking place in an information system over a period of time~~.~~

[SOURCE ISO/IEC TR 10032:2003, 2,7].

~~3.2~~3.3 digital safe ~~(Abbreviation:~~ DS~~)~~

component of an information system consisting of software or a combination of software ~~/~~and hardware for the preservation of digital objects in such conditions as to ensure their long-term integrity~~.~~

3.33.4
digital object
(Abbreviation: DO)
Bitbit stream to be preserved.

EXAMPLE A digital object can contain:

— a file;

— a group of files (for example a single file including several files, possibly compressed);

— a file and metadata describing it;

— a file accompanied by an electronic signature;

— an encrypted file;

— a combination of all the file types listed above.

3.43.5
digital object identifier
(Abbreviation: DO_ID)
identifier assigned unambiguously to a digital object in a digital safe.

3.53.6
digital safe identifier
(Abbreviation: DS_ID)
identifier of the digital safe assigned unambiguously to it by a Technical Administratortechnical administrator during the initial configuration of the digital safe.

3.63.7
hash code
string of bits which is the output of a *hash-function* (3.8*(3.8)*)

[SOURCE: ISO 24534-4:2010, 3.34]

3.73.8
hash -function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output.

[SOURCE: ISO/IEC 11770-4:2012017, 3.9], modified —Note 1 to entry was removed.]

3.83.9
user
(Abbreviation: USR)
person or software that interacts with the digital safe.

Note 1 to entry: to entry There are three types of users: general administrator (USR-G), Functional Administratorfunctional administrator (USR-F) and Standard User standard user (USR-S). Their respective roles are defined in 4.35.6.

3.93.10
user identifier
(Abbreviation: USR_ID)
Identifieridentifier assigned unambiguously to a user of the digital safe

3.103.11
user identifier of the Digital Object (Abbreviation: digital object DO_USR_ID)
identifier assigned to a digital object by a user.

4 Digital safe functional specifications

4.1 Key concepts

The functional specifications of digital safe are bundled into:

— management of users (4.3(4.3),);

— 8 functions that allow the management of digital objects (from 4.44.4 to 4.64.6),);

— additional requirements (from 4.74.7 to 4.174.17),).

The 8 functions on the DOs allow interoperability between digital safes.

The other requirements ensure that digital safe has the minimum characteristics to ensure the protection of DOs, that is to say to ensure their integrity, availability and confidentiality.

Figure 1The diagram on Figure 1 shows the mechanism of functionthe invocation functions and the mechanism of retrieving of results.