FINAL DRAFT
Technical Specification

ISO/DTS 24574

Document management applications — Specification for a digital safe

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

ISO/TC **171**/SC **1**

Secretariat: **BSI**

Voting begins on:
2024-10-28

Voting terminates on:
2024-12-23

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.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/DTS 24574:2024(en)

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) 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 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).

ISO draws attention to the possibility that the implementation of this document may involve the 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.

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 Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 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.

Introduction

As part of their activities, public organizations and private companies increasingly use digital content, whether it is produced by these organizations or 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 the digitization of printed documents.

To meet legal or management requirements, organizations and companies are expected to use trusted technology to ensure the integrity over time of all types of digital content. 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:

- maintaining the integrity, confidentiality and availability of digital objects over time;
- preserving the chain of custody;
- 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;
- defining the minimum elements of traceability of the software operation;
- managing replication of digital objects;
- ensuring sustainability of business operations, business continuity and disaster recovery;
- defining encryption requirements.

This document is limited to the functions of integrity, traceability, confidentiality and availability of digital objects of any kind. 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 who wish to develop or integrate a digital safe;
- service providers, such as trust service providers of digital storages, who are looking for software to support their services;
- software publishers who wants to have a repository to develop digital safe software;
- consultants and auditors who wish to have a reference document to build or audit an archiving system.

This document is intended to complement other ISO documents that deal with electronic archiving. Annex A provides a list of these documents and their link to 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.

This document does not address system environments 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 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]

3.2
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].

3.3
digital safe
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

3.4
digital object
DO
bit 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.

3.5
digital object identifier
DO_ID
identifier assigned unambiguously to a digital object in a digital safe

3.6
digital safe identifier
DS_ID
identifier of the digital safe assigned unambiguously to it by a technical administrator during the initial configuration of the digital safe

3.7
hash code
string of bits which is the output of a *hash-function* (3.8)

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

3.8
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 11770-4:2017, 3.9, modified —Note 1 to entry was removed.]

3.9
user
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 administrator (USR-F) and standard user (USR-S). Their roles are defined in 4.3.

3.10
user identifier
USR_ID
identifier assigned unambiguously to a user of the digital safe

3.11
user identifier of the 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);
- 8 functions that allow the management of digital objects (from 4.4 to 4.6);
- additional requirements (from 4.7 to 4.17).

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 1 shows the mechanism of the invocation functions and the mechanism of retrieving results.

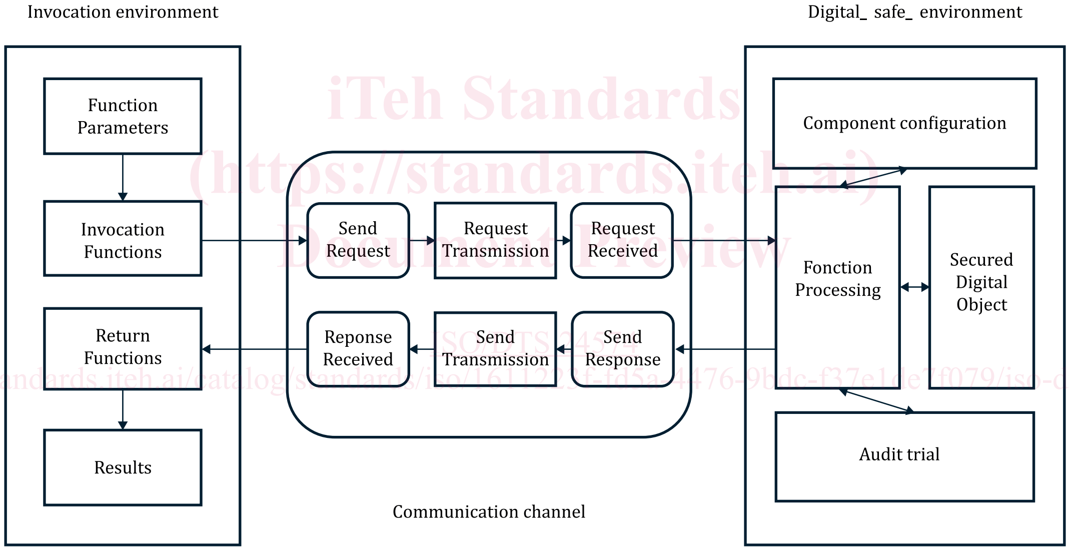

Figure 1 — Functional entities of a digital safe

4.2 Implementation functions

All functions can be implemented either with a human interface or with an application programming interface (API).

4.3 Users management

4.3.1 General

The digital safe shall be able to manage, at a minimum, the three types of users in 4.3.2, 4.3.3 and 4.3.4.

4.3.2 General administrator (USR-G)

A general administrator is authorized to create or remove functional administrators (USR-F).

A USR-G shall not be able to access DOs stored in the digital safe.

At least one USR-G shall exist when the digital safe is created.

The digital safe may contain multiple users with USR-G role.

4.3.3 Functional administrator (USR-F)

The functional administrator (USR-F) is only authorized to create, modify and remove standard users (USR-S).

A USR-f shall not be able to access DOs stored in the digital safe.

The digital safe may contains multiples users with USR-F role.

4.3.4 Standard user (USR-S)

Each USR-S shall have a profile.

A profile indicates, for each function of the digital safe linked to DOs, whether a user is allowed to perform this function.

For each function of the digital safe linked to DOs, Table 1 describes the basic profile.

Table 1 — USR-S profile

Functions	Authorization
Write	Yes / No
Read	Yes / No
Delete	Yes / No
Read technical metadata	Yes / No
Verify	Yes / No
Read audit trail	Yes / No
List	Yes / No
Count	Yes / No

By default, when creating a USR-S, all authorizations shall be set to “No”.

4.3.5 Management of functional administrator (USR-F)

This function is used to create, deactivate and reactivate a functional administrator (USR-F).

Only the general administrator (USR-G) shall be able to perform this function.

4.3.6 Management of standard user (USR-S)

This function is used to create, deactivate and reactivate a USR-S.

Only the functional administrator (USR-F) shall be able to perform this function.

4.3.7 Users management environment

The user management should be independent from the operating system.

4.4 Digital safe mandatory functions

At a minimum, a digital safe shall have the 8 functions listed in Table 2:

- functions 1 to 5 relate to a single DO;
- functions 6 to 8 can relate to one, more than one, or all DOs in a digital safe.

Table 2 — Digital safe functions

	N°	Function	Description
Functions that apply to one DO only	1	Write	This function is used to write a DO in the digital safe after verification of the user write rights.
	2	Read	This function is designed to retrieve a full copy of a DO held in the digital safe.
	3	Delete	This function is used to render inaccessible a DO preserved in the digital safe and to remove it from digital safe. This function includes: — destruction of the DO without any possibility of reconstruction; — destruction of technical metadata and any link within the digital safe to or from this DO. The DO_ID shall not be used for another DO. All records in the audit trial linked to this destroyed DO are not affected by this destruction (all records in the audit trail for this DO are retained).
	4	Read technical metadata	This function is used to retrieve the technical metadata, as defined in 4.4, associated with a DO preserved in the digital safe.
	5	Verify	This function is used to verify the existence and integrity of a preserved DO in the digital safe. Verification concerns the existence of a DO in the digital safe and non-alteration from its time of write in the digital safe.
Functions that apply to one or more DOs	6	Read audit trail	This function is used to retrieve some or all audit trail records of the digital safe associated with a DO preserved or having been preserved in the digital safe. Filters may be used to limit the operation's scope.
	7	List	This function is used to retrieve a list of DO_IDs assigned to DOs preserved in the digital safe. DO_IDs may be filtered using the technical metadata associated with DOs. If no filter is used, this function returns all DO_IDs of DOs preserved in the digital safe.
	8	Count	This function is used to retrieve a number of DOs preserved in the digital safe at a specific moment. DOs may be filtered using the technical metadata associated with the objects. If no filter is used, this function returns the total number of DOs preserved in the digital safe. It is possible that this number does not reflect an accurate count at one instance in time.

4.5 Invoke functions parameters

4.5.1 General

There may be filters on technical metadata. At a minimum, a filter displays a range defined by a lower limit and an upper limit (limits included).

This document does not define filtering for functions that relate to one DO only.

Some functions may allow for ranges for parameters.

4.5.2 Write function

The parameters listed in Table 3 shall be transmitted when the write function is invoked.