TECHNICAL SPECIFICATION

ISO/TS 18759

First edition
2022-08

Document management — Trustworthy storage system (TSS) — Functional and technical requirements

Gestion des documents — Système de stockage fiable (TSS) — Exigences fonctionnelles et techniques

Reference number
ISO/TS 18759:2022(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) 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 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 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).

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 2, *Document file formats, EDMS systems and authenticity 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

The trustworthy storage system (TSS) provides a secure storage framework to preserve and protect all types of electronically stored information (ESI) independent of the application and is not intended to be limited to the use cases of content and records management applications. It provides a unified tamper-resistant storage repository for the preservation and protection of ESI for various environments. In a digital world where information is created, authored and captured electronically, the TSS provides the vital security, protection and preservation of ESI against an ever-growing list of evolving vulnerabilities including accidental and malicious acts, malware and ransomware as well as operational and application errors.

Organizations designing and implementing information and content management systems need guidance on how to select and implement a trustworthy storage system to safeguard the trustworthiness, reliability, authenticity, integrity and immutability of ESI throughout its entire lifecycle. A trusted system needs a TSS in order to maintain ESI trustworthiness ensuring chain of custody, compliance with organizational mandates, legal and regulatory requirements and admissibility standards, including enforcement of retention requirements and deletion-holds. The TSS also benefits organizations that do not have a formal records programme or application, but are responsible for protecting, managing and securing information for their organization.

Readers are advised to use this document taking into account their local jurisdictions and applicable liabilities, paying special attention to legal, regulatory and other organizational requirements, obligations and expectations.

Document management — Trustworthy storage system (TSS) — Functional and technical requirements

1 Scope

This document specifies the functional, technology-neutral requirements for trustworthy storage systems (TSS) that ensure storing and managing electronically stored information (ESI) in a protected and secure fashion during the lifecycle of the information. The TSS as specified in this document is storage technology neutral and accordingly does not specify any specific storage media types or configurations.

This document is applicable to all information systems in which users and applications must manage the protection, preservation and security of stored ESI throughout its entire lifecycle to meet organizational and regulatory requirements to enforce:

— immutability, authenticity and trustworthiness of the stored ESI;

— protection of application managed ESI and other stored ESI against tampering, malicious acts and ransomware;

— organizational ESI preservation and retention policies;

— protection for unstructured and unmanaged data.

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 12651-1, *Electronic document management — Vocabulary — Part 1: Electronic document imaging*

ISO 13008, *Information and documentation — Digital records conversion and migration process*

ISO 14641, *Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications*

ISO 15489-1, *Information and documentation — Records management — Part 1: Concepts and principles*

ISO/TR 15801, *Document management — Electronically stored information — Recommendations for trustworthiness and reliability*

ISO 18829, *Document management — Assessing ECM/EDRM implementations — Trustworthiness*

ISO/TR 22957, *Document management — Analysis, selection and implementation of enterprise content management (ECM) systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12651-1, ISO 14641, ISO 15489-1 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/

3.1
trusted system
information technology system with the capability of managing *electronically stored information (ESI)* (3.2) in a trustworthy manner

Note 1 to entry: A trusted system demonstrates authenticity, integrity and availability of ESI over time.

3.2
electronically stored information
ESI
information created, used, edited, modified and stored in digital form

Note 1 to entry: Electronically stored information (ESI) includes documents and records (unstructured and structured data) created or managed by the organization in the course of business and requiring a computer or other device for access.

3.2.1
changeable electronically stored information
changeable ESI
writeable ESI
electronically stored information (ESI) (3.2) stored on a trustworthy storage system (TSS) without any write-once immutable protection, allowing all changes to electronically stored information (ESI) (contents, size, properties, attributes and checksums)

3.2.2
immutable electronically stored information
immutable ESI
electronically stored information (ESI) on a trustworthy storage system (TSS) with write-once immutable protection that permanently prevents changes to ESI (contents, size, properties, attributes and checksums)

3.2.3
immutable ESI preservation period
immutable ESI retention period
period that defines the length of time for which an *immutable ESI (electronically stored information)* (3.2.2) in a trustworthy storage system (TSS) is to be preserved, prohibiting its deletion

3.2.4
retained ESI
preservation state of an *immutable ESI (electronically stored information)* (3.2.2) in a trustworthy storage system (TSS) that has been assigned a preservation target expiration date and time, which has not lapsed and is therefore ineligible for deletion

3.2.5
expired ESI
preservation state of an *immutable ESI (electronically stored information)* (3.2.2) in a trustworthy storage system (TSS) that has been assigned a preservation target expiration date and time, which has lapsed and expired and is therefore eligible for deletion

3.2.6
preservation expiration date and time
retention expiration date and time
preservation date and time that the *immutable ESI (electronically stored information)* (3.2.2) be retained and preserved at a minimum prohibiting deletion

Note 1 to entry: The immutable ESI (electronically stored information) minimum retention expiration date and time may be increased but can never be reduced.

3.2.7
preservation target expiration date and time
immutable ESI (electronically stored information) (3.2.2) in a trustworthy storage system (TSS) assigned preservation target expiration date and time that is used by the TSS to determine eligibility for deletion

Note 1 to entry: The *immutable ESI* (3.2.2) is eligible for deletion any time after the assigned preservation target expiration date and time has lapsed, provided that the *immutable ESI* (3.2.2) does not have a *deletion hold* (3.3). The assigned preservation target expiration date and time can never be reduced.

Note 2 to entry: Alternatively, reference preservation target expiration date and time or retention period target expiration date and time.

3.3
deletion-hold
trustworthy storage system (TSS) preventing the destruction of any specific electronically stored information (ESI) within a TSS

3.4
access-hold
trustworthy storage system (TSS) preventing the access of any specific electronically stored information (ESI) within a TSS

3.5
modification-hold
trustworthy storage system (TSS) preventing the modification of any specific changeable electronically stored information within a TSS

3.6
application
system for collecting, saving, processing, and presenting data by means of a computer

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.167, definition 1]

3.7
legal hold
litigation hold
operation that tags or otherwise cues special access management and destruction suspension for record [electronically stored information (ESI)] entries deemed relevant, consistent with organization policy under the legal doctrine of "duty to preserve", also notifying records ESI owners and other designated parties of the special data controls on access, retention, and destruction processes

Note 1 to entry: The Add Legal Hold Record ESI Lifecycle Event occurs when an agent causes the system to tag or otherwise indicate special access management and suspension of ESI entry deletion or destruction, if deemed relevant to a lawsuit or which are reasonably anticipated to be relevant to fulfil organizational policy under the legal doctrine of "duty to preserve".

[SOURCE: ISO/TS 21089:2018(en), 3.82, modified — added electronically stored information (ESI) to the definition.]

3.8
ransomware
malicious software that infects computer systems, restricts access to the victim's data and requires a ransom

[SOURCE: ITU-T X.1215 (01/2019), 7.1]

4 TSS concepts and functional requirements

4.1 Overview

The trustworthy storage system (TSS) in conformity with the technical and functional requirements of this document provides a storage environment capable of ensuring and maintaining the trustworthiness and reliability of electronically stored information (ESI) throughout its lifecycle independent of the application or the underlying storage technology. The primary purpose of a TSS is to protect and preserve ESI in a manner that reliably ensures security, immutability, integrity and authenticity. The TSS maintains and safeguards ESI against tampering and corruption in conformity with relevant laws, regulations and business requirements as well as with international standards associated with trustworthy storage environments (ISO/TR 15801, ISO/TR 22957, ISO 18829, ISO 14641, ISO 15489-1 and other related standards).

A TSS is the key component of any trusted environment that manages and maintains the trustworthiness of ESI from creation to deletion. The TSS is designed to enforce provable immutability, integrity, authenticity, retention, security, privacy, tamper-evident protection, enforcing destruction and access holds. The TSS allows the deletion of TSS-stored ESI based on determining deletion eligibility.

Using a non-TSS platform leaves the ESI at risk since the integrity and viability of the entire lifecycle of the ESI cannot be independently secured and protected with provable immutability. There are fundamental limitations to the extent any individual component of a trusted environment can address the requirements without employing the immutability protection and the deletion restrictions of a TSS.

Application-defined security controls are limited to the context of operations performed within the internal components of the application. Modifications to application-managed ESI executed outside the context of the application-defined security can jeopardize the trustworthiness of the entire solution. In a non-TSS platform, any privileged user or privileged process may directly modify, encrypt or delete application-managed ESI bypassing all the security provisions of the application-defined security. Applications cannot prevent, prohibit, inhibit or detect any changes to application-managed ESI on non-TSS storage.

For example, malicious users or malware can manipulate, corrupt or destroy the application-managed ESI without the application's knowledge by simply bypassing the application and modifying the application-managed ESI on a non-TSS platform.

To compensate for the application-managed ESI security and protection, the operating system standard access controls and permissions shall be used. Though deemed a necessity in the context of any trusted environment, operating system enforced access controls and permissions are limited to enforcing privileges without taking into consideration the status of the ESI and associated requirements of a TSS. Without a TSS to protect and safeguard the trustworthiness of ESI, an authenticated process, a privileged user, rogue administrator or anything executing in their context, whether ransomware, malicious code, or any accidental act, can destroy, encrypt and modify any application-managed ESI.

In the age of ransomware, malicious and accidental acts, a TSS should be included when implementing any trusted environment to ensure the trustworthiness of ESI and protection of its authenticity and immutability against internal and external vulnerabilities and exploits that can compromise ESI in a non-TSS or application-managed environment.

In many instances, an application can contain many different types of applications within it, or share ESI with other applications and organizational entities, resulting in a complex schema of controls on individual ESI. In such situations, the TSS provides an additional level of support to protect the data beyond the individual controls of the relevant applications. This is important in a collaborative environment where access can be granted from a variety of methods and from a variety of access roles.

Any application on its own cannot guarantee the authenticity or enforce the retention and deletion-hold of application-managed ESI unless it is coupled with the TSS for immutable security, protection, retention and deletion-hold enforcement. A TSS enables organizations to augment their applications to provide end-to-end protection, preserving ESI integrity and authenticity, chain of custody and immutability in compliance with governance and regulatory requirements. The combination of a TSS

with any application provides the end-to-end immutability, security and protection of ESI to prevent external manipulation, eliminating potential exploits and circumventing any possible risks to integrity and authenticity of the ESI from creation through deletion.

Organizations that implement a TSS should have a defined process to review and evaluate their ESI before simply committing it to a TSS. Professional experts and analysis tools are available to assist organizations in identifying the operational state and the appropriate retention policies. Not all ESI is equal and the guidelines for protecting, preserving and destroying various types of ESI vary. This document defines the functional requirements, taking into consideration that the underlying implementations and technologies may differ between various solutions, that should be available to deploy and use a TSS.

The nature of the ESI in a TSS, whether it is unstructured or structured ESI, is irrelevant to the fundamental functional control defined within the TSS. The requirements identified in this document focus on the features and capabilities of the TSS that support compliance with security, preservation and retention requirements, independent of the source of the ESI or the applications used to access the information.

4.2 TSS concepts

4.2.1 General

There is a clear line of delineation that shall be defined in terms of the functionality of the TSS and how it collaborates with applications such as enterprise content management (ECM) and records management. These applications provide context, reasoning, motives and justification. The principles that govern the functionality of the TSS are simple and in many cases appear to be primitive in contrast with the capabilities and context maintained by applications such as records and document management applications. In the most simplistic concept, the TSS provides a trustworthy repository that can allow ESI to be created, preserved and destroyed on demand.

The TSS creates a trusted storage environment capable of ensuring and maintaining the trustworthiness and reliability of the ESI throughout its lifecycle independent of the application or the underlying storage technology. As a common storage repository, the TSS may support the ability to store both modifiable and unmodifiable ESI to enable organizations and their applications to maintain and manage ESI without having to relocate, transfer or migrate the ESI throughout its lifecycle.

The TSS provides the ability to store and manage two distinct types of ESI.

4.2.2 Immutable ESI

At a minimum, the TSS provides the ability to store unmodifiable ESI on a TSS with write-once immutable protection that permanently prevents changes to ESI (contents, size, properties, attributes and checksums) for the duration of its existence in the TSS. The TSS also provides the ability to safeguard the trustworthiness of ESI with provable immutability, integrity and authenticity that can at some point be assigned retention expiration date and time. The support for the storage of immutable ESI is a core requirement for any TSS.

4.2.3 Changeable ESI

Optionally, the TSS provides the ability to store generic modifiable ESI on a TSS without any write-once immutable protection; allowing all changes to ESI (contents, size, properties, attributes and checksums) for the duration of its existence in the TSS; subject to applicable TSS-defined hold restrictions for modification, access and deletion. A changeable ESI is eligible to be preserved to become an immutable ESI. The TSS may support the creation and management of changeable ESI to allow some organizations to use a common trustworthy repository to manage the lifecycle of all ESI, eliminating the need to migrate managed ESI between different repositories over its lifecycle. For such TSS environments that support changeable ESI, the TSS provides additional controls to help manage and secure various aspects of the changeable ESI lifecycle.

4.3 ESI preservation

The TSS has a basic core requirement to preserve ESI in an immutable and unmodifiable state and only allow deletion if it expires. The TSS never allows a preserved immutable ESI to become a changeable or modifiable ESI as shown in Figure 1.

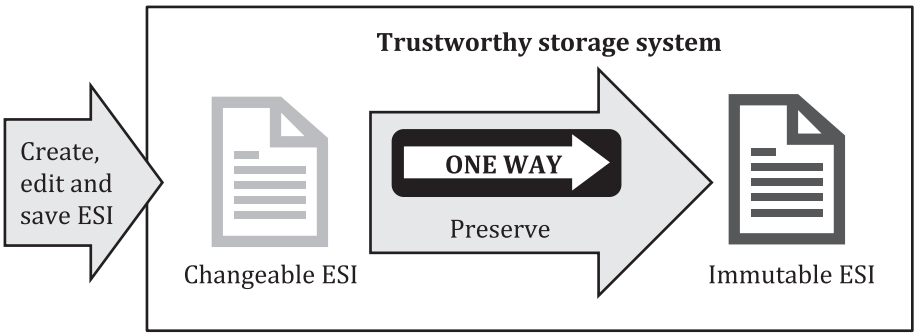

Figure 1 — TSS immutable ESI preservation

From a TSS perspective, once ESI is preserved, it is immutable and can never be modified for the remainder of its existence within the TSS. The only mechanism available to allow the preserved ESI to be eligible for deletion is to expire the ESI. It is important to note that the TSS does not automatically destroy or delete any ESI. The TSS only evaluates the eligibility of the deletion of the ESI when an authorized and authenticated user or application triggers and attempts a delete operation against the ESI.

4.4 Immutable ESI preservation period

4.4.1 Overview

The immutable ESI preservation period is an assigned period that defines the length of time for which an immutable ESI in a TSS is to be preserved, during which the immutable ESI is ineligible for deletion. This period is better known as the retention period which determines the immutable ESI assigned preservation target expiration date and time. Modifications to this period are governed by the restrictions associated with the immutable ESI assigned retention period type.

The TSS can allow a stored ESI to be marked as preserved, which renders the ESI unmodifiable as immutable ESI, prohibiting all modifications to ESI contents and properties and only allowing deletion once the TSS determines that the stored immutable ESI is expired. The immutable ESI expiration is assigned by the authorized user and application or by TSS internal policies. The ESI preservation expiration date and time are key components in enforcing the necessary protection and preservation requirements that are mandated for stored immutable ESI; to ensure that it cannot be deleted or destroyed unless expired.

The TSS can simply act as a slave to the application or the designated authorized user, manager or administrator where it is told to preserve an ESI to prevent deletion. The TSS is only notified to allow deletion once the immutable ESI is expired by the application or authorized user assigning a preservation expiration date and time. This enables organizations to implement the ability to notify the TSS when files are eligible for deletion only after the applicable retention period is satisfied. It enables the organization to have more flexibility in managing changes to its retention policies.

The TSS is not intended to replace the functionality of ECM or records management applications, which can determine and associate context, employ reasoning and invoke processes based on motives and intent.

— The TSS cannot provide the level of context available through a records management or ECM application and is not intended to derive such context either. The reason and motivation to preserve any particular ESI as immutable ESI is not specifically known from the TSS perspective. The role

of the TSS is to preserve the integrity and authenticity and enforce immutability to prohibit all modifications in a manner that safeguards the trustworthiness of stored ESI to address the requirements of a trusted environment. The applications maintain context and manage the relationship between individual ESI. The applications can determine the reasons and motives behind the need to preserve any specific ESI as immutable ESI.

— The TSS is unaware of the motives and reasons why specific ESI is not eligible for deletion. At the TSS level, it does not know whether there is one single reason or several. The reasons are determined at the application level. The TSS is designed to prohibit deletion of immutable ESI until the TSS can independently determine that an assigned preservation target expiration date and time has lapsed. Any immutable ESI that has not been assigned a preservation target expiration date and time is not be eligible for deletion. The immutable ESI assigned retention period controls when the immutable ESI becomes eligible for destruction by an authorized and authenticated application or individual.

— The TSS immutable ESI retention period determines the target preservation (or retention) target expiration date and time. The assigned retention expiration date and time can never be reduced but can always be extended. In other words, from a TSS retention perspective, the assigned immutable ESI retention expiration date and time denotes the retention period.

— The TSS immutable ESI retention may be assigned an indefinite-retention period where an immutable ESI may be assigned an explicit retention period that determines the immutable ESI retention expiration at a later date when triggered to do so. This allows organizations to designate immutable ESI as permanent in the context of applications or processes while maintaining the flexibility to expire on demand or assigning an explicit retention period to accommodate a change in their record keeping policies.

— The TSS immutable ESI retention period may be governed by a hybrid retention period that determines two parameters: the immutable retention expiration date and time and a maximum retention expiration date and time. In other words, the assigned immutable ESI retention expiration date and time sets a period of obligatory retention, while the maximum immutable ESI retention expiration sets a “can keep until” period which is greater than the assigned retention expiration date and time. This allows organizations to designate immutable ESI as permanent in the context of applications or processes, while maintaining the flexibility to expire on demand by reducing the maximum immutable ESI expiration or assigning an explicit retention period to accommodate a change in their record keeping policies.

— The TSS immutable ESI retention period may assign a never expiration designation, making it permanently retained and consequently never eligible for deletion and destruction.

— In all cases, the TSS immutable ESI retention enforcement control eligibility for destruction allows organizations to address and conform to applicable rules, guidelines, regulations and mandates.

4.5 ESI deletion

The TSS supports the ability to delete ESI solely based on the ESI eligibility for the deletion. ESI deletion is critical in a trustworthy environment and the TSS is responsible for independently determining the eligibility of deletion of any specific ESI. This allows the TSS to be resilient, eliminating back doors and other vulnerabilities that can otherwise be exploited in a non-TSS storage environment. In non-TSS environments, user credentials and other application security measures can simply be bypassed or in other instances user credentials and authentication may be compromised allowing ESI to be leaked, encrypted, corrupted or hijacked. The TSS ability to independently validate deletion eligibility of any ESI provides the failsafe scrutiny and security to prevent the destruction of TSS ESI.

TSS ESI deletion eligibility is governed by the status of the ESI, where immutable ESI is only eligible for deletion if it is expired, and changeable ESI is by default eligible for deletion. To support the necessary requirements of various organizational preservation mandates and hold requirements for records management, ECM and other applications, the TSS provides support for deletion-holds that can prohibit deletion of otherwise deletion eligible ESI.