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 19829, *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.

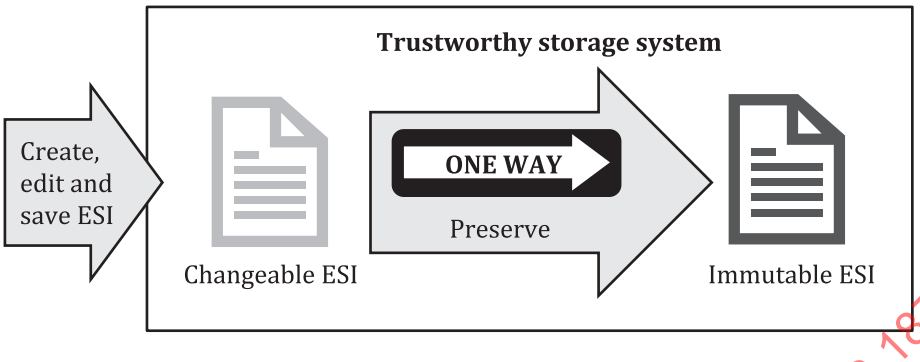

Figure 1 — TSS immutable ESI preservation

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.

The TSS shall not delete ESI, even if it was expired-ESI without any deletion-hold. The TSS role is always to determine deletion eligibility based on evaluating the preservation status of the ESI and whether there is a deletion-hold. The TSS either allows or denies the deletion request typically triggered by an authorized and authenticated user or application.

The TSS provides a deletion-hold mechanism to prevent deletion of any TSS ESI. The deletion-hold applies to both changeable and immutable ESI whose retention period had lapsed and is now expired.

— For expired ESI, this deletion-hold prevents deletion even though the expired ESI may be otherwise eligible for deletion, without having to extend the retention expiration date and time.

— For changeable ESI, the deletion-hold can prevent and prohibit the deletion of the ESI indefinitely until the deletion-hold is removed. This is ideal for environments where there is a need to share changeable ESI in TSS with multiple applications.

In all situations, the TSS is unaware of the motives since that is outside the context of its knowledge and influence. The applications internal processes and workflows along with the users, managers and administrators can determine the reasons, motivation and justification for a deletion-hold. The TSS only knows that it was told to apply the deletion-hold and enforce it accordingly.

4.6 TSS functional requirements

The TSS provides the necessary safeguards to support and enforce:

— records management immutability and retention concepts and principles as specified in ISO 15489-1;

— tamper-resistant storage and ESI preservation of the trusted system policies and procedures as defined in ISO/TR 15801 and ISO/TR 22957;

— ESI lifecycle in ECM systems as specified in ISO 18829 and noted in ISO/TR 22957;

— the preservation, validation, authentication, auditability and security concepts and methodologies identified in both ISO/TR 15801 and ISO/TR 22957;

— the provable immutability and authenticity, retention and deletion-hold, modification-holds, access-holds, lifecycle management and tamper-evident protection and privacy of ESI throughout its lifecycle.

At a minimum, a TSS stores ESI in a tamper-resistant configuration that is redundant and maintains multiple copies of the ESI in an immutable manner that prevents modifications and unauthorized deletions. A TSS meets the requirement of a trusted system to store at least two copies of the ESI written in an unalterable format to two separate TSS storage repositories, each providing the internal write-once controls independent of the physical characteristics of the storage media. The TSS ESI copies should be maintained in different physical locations that take into consideration sufficient geographic separation to avoid the destruction of the copies of information simultaneously due to the same disaster or other vulnerabilities.

NOTE 1 The set of disasters considered depend on the risk or threat model, while scale of geographic separation can be limited if, for example, there is a requirement to store information within the boundaries of specific jurisdictions.

A TSS is not intended to replace the retention and disposition hold management functionality of the applications [such as records management, electronic document management system (EDMS) or ECM] that manage ESI. TSS-enforced immutable protection, retention and deletion-hold controls complement and supplement the records management and ECM application retention and deletion policies of the organization, ensuring that there are no back doors that can be exploited to compromise the integrity and authenticity of the ESI. It should be noted that in the context of the TSS, there are no privileged users or administrators, trusted or otherwise, who can directly or indirectly through ransomware, malware, malicious acts or user error, override, circumvent, or compromise the TSS security protecting the integrity, authenticity and deletion of the ESI in a TSS.

A TSS is not associated with any specific hardware (physical, virtual or hybrid infrastructure) or software configurations, and is independent of whether it is hosted on-premise or in the cloud. The TSS protects the integrity and chain of custody of the trusted ESI, preventing additions, modifications and deletions of the ESI.

A TSS shall meet all of the following requirements:

(a) TSS ESI lifecycle immutability, integrity, reliability and protection:

- creates tamper resistant secure repositories to store ESI which provide the write-once controls and functionality to protect individual ESI;
- provides immutable secure protection for the ESI that prevents tampering and unauthorized destruction;
- maintains multiple identical immutable copies (a minimum of 2) of the ESI. These copies should be maintained in different physical locations that take into consideration sufficient geographic separation to avoid the destruction of the copies of information simultaneously;
- provides mechanisms to validate and authenticate ESI using checksums, hash values and signatures, in conjunction with persistent audit trails and metadata;
- maintains ESI chain of custody and persistence of all ESI properties including the ESI integrity, retention expiration dates and deletion-holds independent of any changes to the underlying TSS storage technologies.

(b) TSS immutable-ESI retention and deletion-hold enforcement:

- enforces immutable preservation of ESI to support organizational requirements of relevant regulations and standards to prevent unauthorized and premature deletions as defined in 5.4;

  NOTE 2 A TSS supports and enforces the persistence of immutable ESI for the duration of the assigned preservation period.

- provide deletion-hold enforcement to prevent ESI deletion without changing the assigned ESI retention expiration;
- provide retention triggers, management interface and programming interface (API) related fields and scripts to enable applications and authorized personnel to set and manage the retention and deletion-hold of any ESI in the TSS.

  NOTE 3 Clause 5 provides additional TSS ESI lifecycle management requirements.

(c) TSS audit control:

- maintains persistent ESI audit logs for ESI creation, modification, availability, authenticity, integrity, retention and deletion, including TSS deletion-holds, access holds, modification holds, retention expiry dates or changes to retention periods;
- maintains persistent security audit logs for ESI access operations or any attempts to modify the ESI or tamper with the security of the TSS;
- enables the persistent logging of ESI read access operations;
- maintains audit logs stored within the TSS and, where warranted, external to the TSS.

  NOTE 4 7.7 provides additional TSS auditing requirements.

(d) TSS administration:

- provide alarms, warnings and notifications that alert authorized personnel to take appropriate action, including replacing components;

— provide a management interface to exclusively administer TSS policies and maintain policy audit logs.

For additional requirements for TSS general, technical methods and requirements, see:

— Clause 7 for TSS integrity, auditing, security requirements;

— Clause 8 for technical methods for trusted storage environments requirements;

— Clause 9 for requirements related to mitigating technical methods.

5 TSS ESI lifecycle management technical requirements

5.1 General

The TSS safeguards the trustworthiness of ESI throughout its lifecycle; enforcing security, write-once immutability, integrity, authenticity, retention, deletion and chain of custody protection to address the requirements of trusted environments.

Due to the nature of the functionality, resiliency and high availability requirements of trusted environments, the TSS shall support and enforce immutable protection to maintain authenticity and integrity of preserved ESI restricting deletion eligibility using a retention period that determines the target preservation expiration date and time and deletion-hold policies on ESI to prohibit exploits and eliminate attempts to compromise chain of custody. At a minimum, the TSS provides the last line of defence to enforce the immutability, security protection requirements for the ESI. The enforcement of the retention and deletion-hold policies within the TSS is the minimal level of security to ensure that protected ESI cannot be compromised, corrupted or deleted outside the controls of the applications as shown in Figure 2.

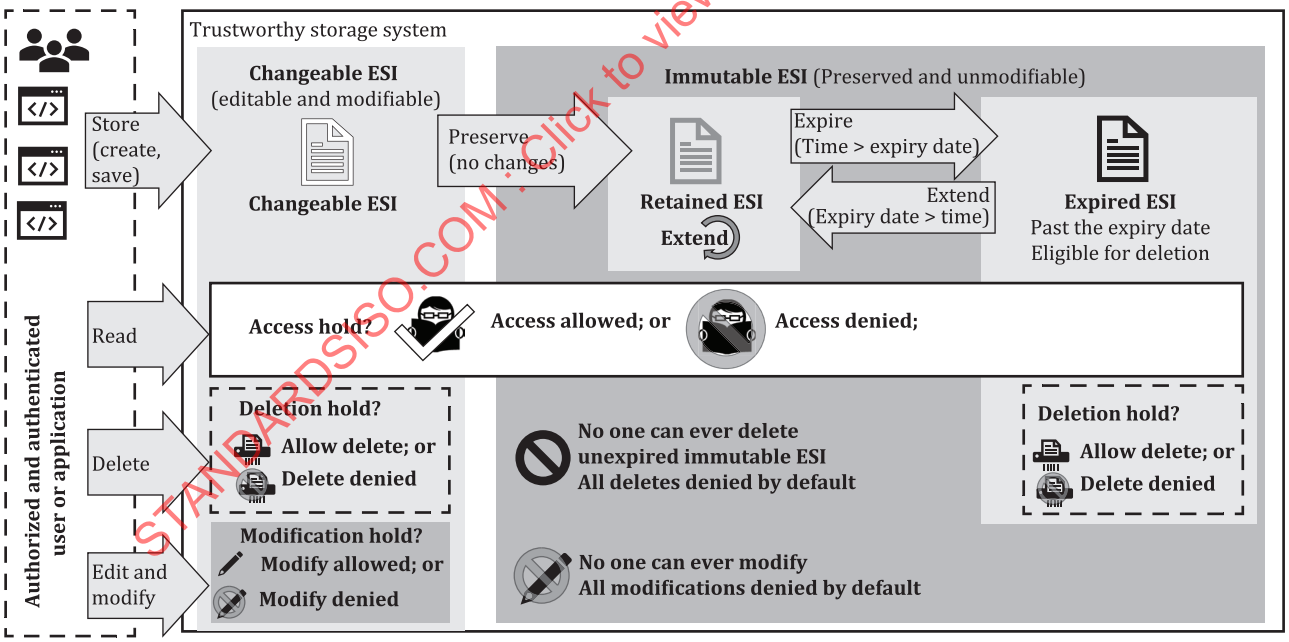

Figure 2 — ESI lifecycle in a TSS

By design, a TSS is not limited to be deployed with an application and may be deployed as a standalone repository to store, protect and preserve unstructured ESI that is not managed by any specific application. The TSS is not intended to be a records management application. Instead, the TSS provides the safeguards and protection required to support the requirements of records management, ECM and other applications. A TSS is the perfect complement for records management and ECM applications to

enforce retention and deletion-hold, and address the immutability and preservation requirements of ESI.

The TSS is also intended to be used in environments where lifecycle is managed by an application such as ECM, or where retention is managed by a record keeping system or both, but where multiple applications may access the information for a variety of purposes. It provides the final authority on the type of access permitted at the time of the access request.

The use of a TSS in support of applications, such as records management and ECM, bridges the security gaps to prevent external tampering or deletion of the application managed ESI to enforce the application retention, deletion-holds, modification-holds, access-holds as well as security and privacy restrictions specified by the application policies on application-managed ESI in the TSS.

Where multiple applications share access to common repositories of managed ESI to derive intelligence and analytics, the ability to secure and preserve the immutability and authenticity of shared ESI is critical. The use of a TSS is not limited to environments where lifecycle is managed by one application such as an ECM or where retention is managed by a record management system, but where multiple applications may access the information for a variety of purposes. It provides the final authority on the type of access permitted at the time of the access request.

The TSS ESI security, protection and privacy restrictions constitute an essential requirement and include the enforcement of holds as defined in greater detail in 5.2. In the context of this document, the general concept of ESI represents a self-contained object of digital information, which can be created, authored, accessed, read, modified, processed or edited, stored and deleted in a TSS. In the context of the TSS there are two types of ESI, changeable ESI (writeable-ESI) and immutable ESI (unmodifiable ESI) that are defined in greater detail in 5.3 and 5.4.

5.2 TSS ESI security, protection and hold restrictions requirements

5.2.1 General

A core requirement of a TSS is based on its ability to enforce various security, protection and hold restrictions to safeguard the integrity and authenticity of ESI and provide the necessary protection to support various application specific content management and records management requirements and regulations.

At a minimum, a TSS shall support the security, protection and hold restriction requirements in 5.2.2, 5.2.3, 5.2.4 and 5.2.5.

5.2.2 TSS ESI security requirements

5.2.2.1 General

A TSS shall support and enforce the security requirements in 5.2.2.2 and 5.2.2.3.

5.2.2.2 TSS user security requirements

A TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support and enforce user credentials authentication to restrict access, modifications and operations to TSS ESI. TSS security limits actions to validated and authenticated users in accordance and compliance with organizational security controls including but not limited to active-directory and domain-based credentials. TSS-authenticated users cannot overrule or supersede the applicable immutable ESI restrictions on modifications as defined in 5.4 which can prohibit changes to immutable ESI name, contents, path and restrict changes to immutable ESI assigned retention period target preservation expiration date and time.

5.2.2.3 TSS application security requirements

A TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support and enforce application authentication and validation to restrict access and modifications of TSS ESI to validated and authenticated applications. Organizational mandates and requirements can apply. It is presupposed that TSS-authenticated applications are aware of the applicable immutable ESI restrictions on modifications as defined in 5.4 which can prohibit changes to immutable ESI name, contents, path and restrict changes to ESI assigned retention period target preservation expiration date and time.

5.2.3 TSS ESI hold restriction requirements

5.2.3.1 General

A TSS shall support and enforce the hold restriction requirements in 5.2.3.2, 5.2.3.3 and 5.2.3.4.

5.2.3.2 TSS stored ESI deletion-hold restriction requirements

The deletion-hold addresses a wide range of requirements for regulations, legal holds and organizational mandates. The primary purpose of applying a deletion-hold to any TSS ESI is to prevent its deletion regardless of whether it is changeable ESI or immutable ESI and independent of the assigned retention period and target preservation expiration date and time. The ESI-deletion-hold prohibits deletion without modifying the immutable ESI assigned retention period target expiration date and time.

A TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support the ability to apply and enforce a deletion-hold as the mechanism to prevent and disallow the deletion of any TSS ESI regardless of whether it is changeable ESI or immutable ESI or whether it has been assigned a retention period with a target preservation expiration date and time that has lapsed and expired; to support applications needs, applicable business operations, and administrative requirements.

The TSS shall enforce the ESI-deletion-hold to determine ESI eligibility for deletion even if the immutable ESI preservation state is expired-ESI. Any changeable or expired ESI in the TSS that has a deletion-hold is ineligible for deletion and cannot be deleted until the deletion-hold is released as shown in Figure 3.

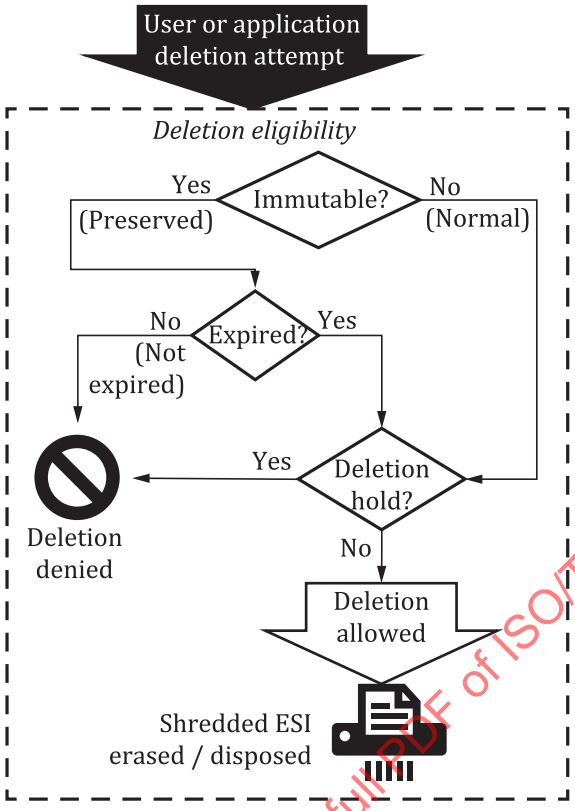

Figure 3 — ESI deletion eligibility in a TSS

The ESI-deletion-hold does not change the immutable ESI assigned retention period target preservation expiration date and time but renders the immutable ESI ineligible for deletion even if its assigned target preservation date and time has lapsed. Any TSS ESI with an assigned deletion-hold is ineligible for deletion unless the deletion-hold is released.

A common use case for an ESI deletion-hold is to address "legal hold" framework requirements, where certain immutable ESI are preserved beyond the target retention expiration date and time maintained for administrative and legal reasons.

5.2.3.3 TSS ESI access-hold restriction requirements

A TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support the ability to apply and enforce a TSS access hold. The access hold prevents the access of any specific TSS ESI for legal or administrative reasons and applies equally to both changeable and immutable ESI.

The TSS shall enforce the ESI-access-hold to determine ESI eligibility for access such as read contents even if the immutable ESI preservation state is expired-ESI as shown in Figure 4. Any TSS ESI that has an access-hold is ineligible for access and cannot be read or accessed until the access-hold is released.

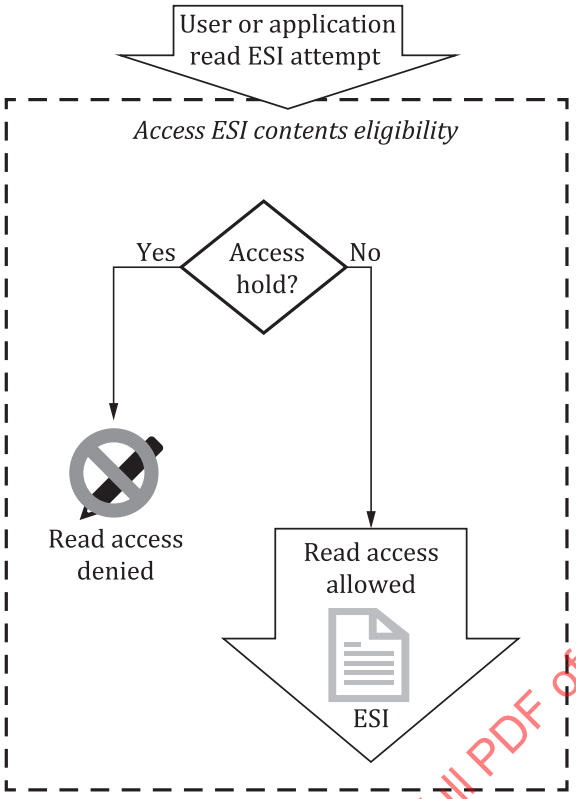

Figure 4 — ESI access eligibility in a TSS

The ESI access-hold may be used as temporary measure to address adhoc-deletion requirements for retained-ESI that is not eligible for deletion. The ESI access-hold may be used to address and complement privacy requirements for managing personally identifiable information, sensitive documents as well as private health information and vital records.

5.2.3.4 TSS ESI modification-hold restriction requirements

A TSS that supports the storing of changeable ESI shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support the ability to apply and enforce a modification-hold for changeable ESI in the TSS. The modification hold prevents the modification of ESI for legal or administrative reasons and applies only to changeable ESI. This hold does not apply to immutable ESI, since all immutable ESI is unmodifiable.

The ESI-modification-hold determines eligibility for changeable ESI modification such as edit, rename, move and overwrite operations. Any changeable ESI in the TSS that has a modification-hold is ineligible and cannot be modified until the modification-hold is released.

Figure 5 shows a common use case for ESI modification-hold to prevent modification of changeable ESI for administrative, procedural mandates, or to support application processes and workflows.

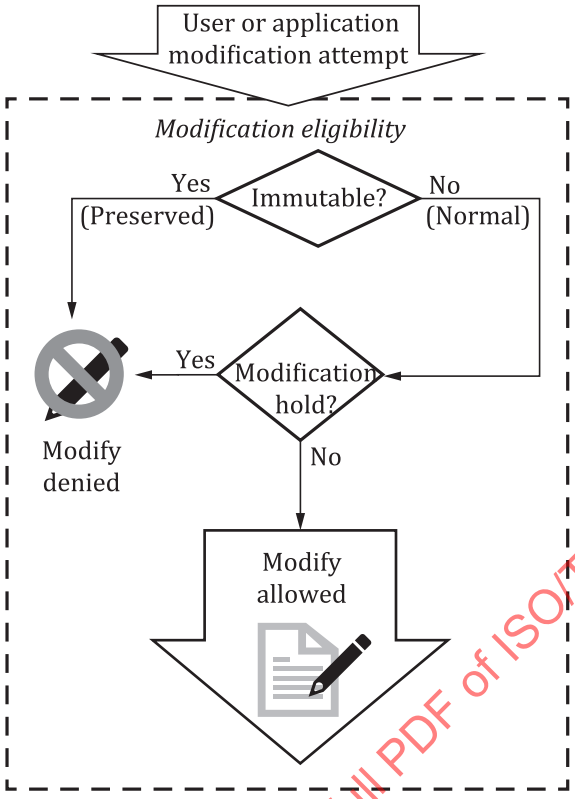

Figure 5 — ESI modification eligibility in a TSS

5.2.4 TSS ESI protection requirements

A TSS may optionally support and enforce the following ESI protection requirements for authorized and authenticated users and applications:

— For all TSS ESI (changeable ESI and immutable ESI):

  — modify-ESI-security-protection enforces and supports the assignment of an ESI protection policy that may allow or deny changing any TSS ESI assigned security access controls and permissions, applied on a per individual ESI basis;

  — execute-ESI-protection enforces and supports the assignment of an ESI protection policy that may allow or deny executing TSS ESI, applied on a per individual ESI basis;

  — delete-ESI-protection enforces and supports the assignment of an ESI protection policy that may allow or deny deleting TSS ESI, applied on a per individual ESI basis to prevent the deletion of the assigned ESI regardless of its state.

— For all TSS changeable ESI, if supported by the TSS:

  — rename-ESI-protection enforces and supports the assignment of an ESI protection policy that may allow or deny renaming TSS changeable ESI, applied on a per changeable ESI basis;

  — move-ESI-protection enforces and supports an ESI protection policy that may allow or deny moving TSS changeable ESI within the TSS, applied on a per changeable ESI basis;

  — overwrite-ESI-protection enforces and supports an ESI protection policy that may allow or deny overwriting TSS changeable ESI, applied on a per changeable ESI basis;

  — overwrite-zero-ESI-protection enforces and supports an ESI protection policy that may allow or deny overwriting zero length TSS changeable ESI, applied on a per changeable ESI basis.

— preserve-ESI-protection enforces and supports an ESI protection policy that may allow or deny the preservation of TSS changeable ESI to become immutable ESI, applied on a per changeable ESI basis.

NOTE The preserve ESI protection is used to support application requirements for the storage of application indexes, transaction files, logs and temporary files that can otherwise break the application if they were persevered as immutable ESI.

5.2.5 TSS ESI deletion requirements

From a TSS security perspective, the deletion of TSS ESI is an essential function of a trustworthy environment. The TSS shall provide trusted storage system defined policies, triggers, scripts, programmatic and management interfaces to allow authorized and authenticated users and applications to manage and initiate the deletion of TSS ESI as follows:

— All TSS ESI delete operations shall conform to the secure delete and erasure requirements as defined in 7.3 to ensure that deleted ESI is destroyed and can never be restored or retrieved.

— The TSS is not required to initiate the deletion of any TSS ESI but enforces the eligibility for deletion based on whether it is changeable ESI or expired immutable ESI subject to applicable deletion-hold and TSS ESI security and protection restrictions.

— The deletion of TSS ESI is initiated by authenticated and authorized individuals or applications that are responsible for approving or triggering the operation.

— All formal application disposition activities and related documentation that occur within the context of records management or other application requirements occur outside the TSS and are not part of the TSS functionality or specification.

— The TSS shall maintain relevant audit logs of ESI deletion operations.

5.3 Changeable ESI requirements

The TSS may support changeable ESI, which by definition is ESI that is modifiable, editable and subject to change within the operational security and protection restrictions enforced by the TSS.

Changeable ESI may remain modifiable for its entire existence. The TSS may apply and enforce security privileges and restrictions.

If the TSS supports the storage of changeable ESI then it shall provide and support the following requirements:

— provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to allow authorized and authenticated users and applications to manage changeable ESI;

— create and store changeable ESI;

— read and access ESI contents and properties (name, path) subject to applicable TSS assigned access-hold restrictions;

— modify, overwrite changeable ESI contents and properties (rename, move) subject to applicable TSS assigned ESI-protection policies and modification-hold restrictions;

— invoke or execute changeable ESI subject to applicable TSS assigned execute-ESI-protection policy;

— modify changeable ESI user access permissions subject to applicable TSS assigned modify-ESI-security-protection policy;

Optionally the TSS may:

— apply or remove a deletion-hold to prevent or allow changeable ESI deletion;

— apply or remove an access-hold to prevent or allow access to changeable ESI contents;

— apply or remove a modification-hold to prevent or allow changeable ESI modification;

— delete the changeable ESI at any time provided there is no deletion-hold;

— preserve the changeable ESI to become immutable ESI subject to applicable TSS assigned changeable ESI preserve-ESI-protection policy;

— maintain the changeable ESI as modifiable for its entire existence and at a minimum the TSS may apply security privileges, protection and restrictions enforced by the TSS.

5.4 TSS immutable ESI requirements

Immutable ESI is unmodifiable ESI on a TSS with write-once immutable protection that permanently prevents changes to ESI (contents, size, properties, attributes and hashes or checksums) to safeguard ESI with provable immutability, integrity and authenticity. Immutable-ESI may be created and stored in the TSS as immutable upon creation or transition from changeable ESI upon being preserved to become immutable ESI.

For the immutable ESI to be trusted, the TSS shall provide and enforce the necessary long-term storage for ESI immutability, validation, authentication and auditability and the security provisions and recommendations in ISO 14641 and ISO/TR 15801. The lifecycle of ESI shall be supported in accordance with ISO 18829 and ISO/TR 22957. Immutable ESI is no longer modifiable for its entire existence. It cannot be deleted unless it is assigned a retention period that assigns a target preservation expiration date and time after which the immutable ESI becomes eligible for deletion. Immutable ESI can only have one of two states that determine eligibility of deletion:

— retained ESI where the immutable ESI target preservation expiration date and time has not lapsed;

— expired ESI where the immutable ESI retention target preservation expiration date and time has lapsed.

A TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support the following immutable ESI requirements:

— preserve a TSS ESI to assign an immutable ESI write protection state;

— enforce ESI write protection to permanently prevent all modifications of immutable ESI contents and properties (including name, size and path);

— enforce the TSS-defined immutable ESI target preservation (or retention) target expiration date and time as the only means for the TSS to determine that an immutable ESI retention has expired which determines its deletion eligibility;

— assign a retention period as defined in 5.7 to determine the target preservation expiration date and time which is used by the TSS to regulate eligibility for deletion from the TSS;

— apply and enforce one of two immutable ESI states based on the assigned target preservation expiration date and time:

  — retained ESI where the immutable ESI retention target preservation expiration date and time has not lapsed and the ESI is ineligible for deletion; or

  — expired ESI where the immutable ESI retention target preservation expiration date and time has lapsed and expired and the ESI is eligible for deletion.

— maintain TSS internally stored metadata and audit trails about the immutable ESI chain of custody including:

  — creation date and time which reflects when the immutable ESI was created in the TSS;

  - last modification date and time which reflects when the immutable ESI was last modified;
  - preservation date and time which reflects when the ESI was preserved to be immutable ESI;
  - preservation user which reflects the user credentials used to preserve the immutable ESI;
  - checksum which is a hash code or digital signature of the contents of the immutable ESI upon preservation.
- apply and enforce the immutable ESI assigned retention period requirements and restrictions as defined in 5.7;
- prevent and prohibit retained ESI deletion where the assigned target preservation expiration date and time has not lapsed;
- only allow the deletion of expired ESI if there is no deletion-hold assigned to the immutable ESI whose assigned target preservation expiration date and time has expired. When the target preservation expiration date and time has expired, the immutable ESI changes state from retained ESI to expired ESI and is eligible for deletion provided it is not on deletion-hold;
- prevent and prohibit expired ESI deletion if deletion-hold is set as defined in 5.2.3.2;
- applying an ESI access-hold restriction prohibits access to the immutable ESI contents as defined in (5.2.3.3);
- applying an ESI modification-hold restriction to the immutable ESI has no effect since immutable ESI is unmodifiable for its entire existence in the TSS;
- prohibits changes to the retention of any immutable ESI that violates the assigned retention period as defined in 5.7;
- internally stores and maintains the audit trail of the immutable ESI within the TSS;
- enforces and demonstrates that all copies of expired ESI that are not under deletion-hold are securely erased once a valid delete request is received and accepted using a trusted interface or application;
- enforce applicable TSS immutable ESI security, protection and hold restriction requirements as defined in 5.2
- maintain immutable ESI persistence and immutability enforcing any applicable target preservation expiration date and time independent of any refresh of underlying changes to TSS infrastructure over time.

5.5 TSS retained ESI requirements

Retained ESI is immutable ESI whose assigned target preservation expiration date and time has not lapsed or expired. The immutable ESI assigned retention period establishes a target preservation expiration date and time that determines the eligibility for deletion, subject to the restrictions and requirements specified for immutable ESI as defined in 5.4.

No matter how the immutable ESI retention period was assigned, a TSS, at a minimum, shall support the following retained ESI requirements:

- enforce the retained ESI status on any TSS immutable ESI whose assigned target preservation expiration date and time has not lapsed or expired;
- prevent retained ESI deletion unconditionally;
- transition the immutable ESI from retained ESI to expired ESI automatically once the assigned retention period target preservation expiration date and time has lapsed and expired;

— enforce all immutability, preservation and persistence requirements and restrictions of immutable ESI (5.4);

— enforce the assigned retention period that determines the permitted changes to the immutable ESI assigned target preservation expiration date and time;

NOTE Fundamentally, the target preservation expiration date and time can be increased.

— prohibit the reduction of the assigned target preservation expiration date and time as defined by the assigned retention period.

5.6 TSS expired-ESI requirements

Expired ESI is immutable ESI on a TSS whose retention-period has reached the assigned target preservation expiration date and time and is eligible for deletion unless it is on deletion-hold.

A TSS shall support the following expired ESI requirements:

— enforce all requirements and restrictions of immutable ESI as defined in 5.4;

— transition the immutable ESI from retained ESI to expired ESI automatically once the assigned retention period target preservation expiration date and time has lapsed and expired;

— allow the extension of the expired ESI assigned target preservation expiration date and time independent of any deletion-hold or access-hold restrictions, which may result in transitioning the status from expired-ESI to retained-ESI provided that the new target preservation expiration date and time has not lapsed;

— allow the deletion of expired ESI, if not on deletion-hold.

5.7 Immutable ESI retention period

5.7.1 General

The immutable ESI retention period defines the length of time for which an immutable ESI in a TSS is to be preserved, prohibiting its deletion. This retention period determines the immutable ESI assigned preservation target expiration date and time, which is used by the TSS to enforce the minimum preservation duration of the immutable ESI before it is eligible for deletion.

5.7.2 Immutable ESI retention period requirements

The TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support the following immutable ESI retention period requirements:

— immutable ESI retention period determines the target preservation expiration date and time at a minimum which is used by the TSS to determine whether any individual immutable ESI is eligible for deletion or not;

— immutable ESI assigned retention period shall be enforced on an individual immutable ESI basis by the TSS;

— immutable ESI in the TSS shall have an assigned immutable ESI retention period;

— immutable ESI retention period modifications are governed by the restrictions associated with the immutable ESI assigned retention period type which can be either permanent (5.7.3), fixed (5.7.4), hybrid (5.7.5) or indefinite (5.7.6) retention.

Regardless of the assigned retention period, the immutable properties of the immutable ESI (contents, size, properties, attributes and hashes or checksums) shall never be modifiable or alterable throughout its existence.

A TSS shall support at least two or more of these immutable ESI retention periods to qualify as conforming to this document. Specific TSS solutions have different names or different methods to accomplish these retention periods. For the purposes of this document, these retention period definitions define the key functionality supporting an organization's different types of ESI retention lifecycles with differing types of needs and requirements.

Since immutable ESI is unchangeable by definition, the only possible allowable action is to delete or destroy it, provided that its retention period has lapsed and there are no deletion-hold restrictions.

5.7.3 Immutable ESI permanent retention period

With the assignment of this ESI permanent retention period, the immutable ESI shall be retained forever with a target preservation (or retention) expiration date and time that shall never expire.

The TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support and assign an immutable ESI with a permanent-retention period with the following requirements:

— enforce all requirements and restrictions of immutable ESI as defined in 5.4;

— immutable ESI with a permanent retention period shall be assigned an explicit target preservation expiration date and time that shall never expire;

— immutable ESI with a permanent retention period shall remain in a retained ESI state and shall never expire or be eligible for deletion;

— immutable ESI with a permanent retention period shall never be eligible to change to another retention period.

5.7.4 Immutable ESI fixed retention period

With the assignment of an immutable ESI fixed retention period, the immutable ESI shall be retained and preserved for an explicit period after which it may become eligible for deletion.

The TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support and assign an immutable ESI with a fixed-retention period with the following requirements:

— enforce all requirements and restrictions of immutable ESI as defined in 5.4;

— immutable ESI with a fixed retention period shall be assigned an explicit target preservation expiration date and time which may be extended but never reduced;

— extending the target preservation expiration date and time of an expired ESI with a fixed retention period may change the status to retained ESI;

— immutable ESI with a fixed retention period whose assigned target preservation expiration date and time has not lapsed is assigned a retained ESI status and governed as defined in 5.5;

— immutable ESI with a fixed retention period whose assigned target preservation expiration date and time has lapsed and expired is assigned an expired ESI status and governed as defined in 5.6;

— immutable ESI with a fixed retention period may be assigned to one of the following retention periods:

  — permanent retention period as defined in 5.7.2; which effectively extends the target preservation expiration date and time which shall not expire;

  — hybrid retention period as defined in 5.7.5; which at a minimum shall maintain the existing target preservation expiration date and time

— immutable ESI with fixed retention period can never be reassigned to an indefinite retention period.

5.7.5 Immutable ESI hybrid retention period

The hybrid retention period extends the fixed retention period functionality by incorporating a maximum preservation date and time. With this hybrid retention period, the immutable ESI shall be assigned both a minimum preservation expiration date and time as well as a keep-until maximum preservation date and time which at a minimum is greater than or equal to the minimum retention expiration date and time.

The hybrid retention assigned to an immutable ESI can determine the target preservation expiration date and time by applying the keep-until maximum preservation date and time. By default, the hybrid-retention period can only allow the immutable ESI to expire once the keep-until maximum preservation date and time has lapsed.

The hybrid-retention period allows the target preservation expiration date and time to be reduced but never less than the minimum preservation expiration date and time. The expiration date may be extended at any time or shortened as long as it is greater than the ESI's explicit minimum retention date. Both dates are set when the ESI becomes immutable ESI with the hybrid retention period.

The hybrid retention period provides some flexibility for managing the preservation target expiration data and time. It sets a short minimum preservation expiration date and time, and allows the maximum preservation expiration date and time to fluctuate according to the records management needs of the application such ECM and records management systems.

The TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support and assign an immutable ESI with a hybrid-retention period with the following requirements:

— enforce all requirements and restrictions of immutable ESI as defined in 5.4;

— assign a preservation expiration range based on both:

  — minimum preservation expiration date and time which can never be reduced and can be extended but never greater than the keep-until maximum preservation date and time;

  — keep-until maximum preservation date and time which can be increased or reduced but never less than minimum preservation expiration date and time;

— assign a target preservation expiration date and time based on the keep-until maximum preservation date and time;

— reduce the keep-until maximum preservation date and time of an immutable ESI with a hybrid retention period which effectively shortens the preservation target date and time, changing the immutable ESI status from retained ESI to expired ESI;

— increase the keep-until maximum preservation date and time of an immutable ESI with a hybrid retention period which effectively extends the preservation target date and time, changing the immutable ESI status from expired ESI to retained ESI.

— immutable ESI with a hybrid-retention period whose assigned target preservation expiration date and time has not lapsed is assigned a retained ESI status and governed as defined in 5.5;

— immutable ESI with a hybrid retention period whose assigned target preservation expiration date and time has lapsed and expired is assigned an expired ESI status and governed as defined in 5.6;

— immutable ESI with a hybrid retention period may be assigned to one of the following retention periods:

  — permanent retention period as defined in 5.7.2; which effectively extends the target preservation expiration date and time which shall not expire;

— fixed retention period as defined in 5.7.4; which at a minimum shall maintain the existing minimum preservation expiration date and time as the target preservation expiration date and time;

— immutable ESI with a hybrid retention period can never be reassigned to an indefinite retention period.

5.7.6 Immutable ESI indefinite retention period

Immutable ESI that has an assigned indefinite retention period remains as retained ESI and does not expire unless it is assigned a different retention period that has a defined target preservation expiration date and time which may expire. The indefinite retention period provides the flexibility to preserve the ESI in an immutable state to support various scenarios where the ESI is considered a record by the application. In certain instances, the event to assign the target preservation expiration date and time may not have occurred and is triggered at a later stage. In other instances, the assignment of an indefinite retention to the immutable ESI enables the applications including ECM and records management systems to manage the retention expiration where the TSS simply maintains the preservation state of the ESI until the managing application determines it is time for disposition and assigns a target expiration date and time by assigning a fixed retention period (5.7.3) to the immutable ESI that renders it expired and eligible for deletion.

The TSS shall provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support and assign an immutable ESI with an indefinite retention period with the following requirements:

— enforce all requirements and restrictions of immutable ESI (5.4);

— immutable ESI with an indefinite retention period shall never have an assigned expiration date and time;

— immutable ESI with an indefinite retention period shall remain in a retained ESI status;

— immutable ESI with an indefinite retention period shall never expire;

— immutable ESI with an indefinite retention period shall never be deleted or destroyed;

— immutable ESI with an indefinite retention period may be reassigned to a permanent retention (5.7.3), fixed retention (5.7.4) or hybrid retention (5.7.5) period at which point, the immutable ESI status, capabilities and restrictions of the newly assigned retention period apply independent of any deletion-hold or access-hold restrictions.

6 TSS integration and management interfaces

An integral part of the TSS is its ability to provide the necessary immutable protection to enforce the trustworthiness of the ESI throughout its lifecycle, as well as the ability to extend this security and integrate with external applications in a trusted environment.

TSS shall provide a mechanism to enable the applications to set the appropriate retention expiration and associated deletion-holds on the ESI in the TSS.

TSS integrated and management interfaces enable the applications and authorized personnel that manage the retention and deletion-hold of the ESI to trigger retention and set an expiration date, apply deletion-holds and accessibility restrictions to TSS ESI, leveraging the TSS retention enforcement capabilities.

The TSS shall support and provide the following interfaces and management capabilities:

— provide TSS-defined policies, triggers, scripts, programmatic and management interfaces to support and manage the ESI throughout its lifecycle as defined in Clause 5:

  — programmatic interface to support and enable TSS-aware applications to integrate TSS ESI lifecycle protection, restrictions and applicable deletion;

  — scripting interface to enable authorized and authenticated personnel to manage the ESI lifecycle as defined in Clause 5;

  — automated retention policy engine that applies immutable ESI retention period enabling non-TSS-aware applications to store unstructured ESI in the TSS and leverage TSS ESI lifecycle protection and preservation, applicable restrictions and permitted deletions;

  — file system interface to support and enable organizations to store unstructured ESI in the TSS and leverage ESI lifecycle protection, restrictions, and applicable deletion;

  — administrative interface (in the form of applications or tools or both) enable authorized and validated personnel to manage ESI lifecycle protection, restrictions and applicable deletion.

— The TSS shall provide the following management and administrative capabilities using any of the abovementioned interfaces to:

  — configure, manage and administer TSS retention periods and triggers as defined in Clause 5;

  — manage the entire ESI lifecycle from creation to applicable deletion;

  — modify immutable ESI expiration and trigger ESI retention and the assignment of a retention period;

  — modify immutable ESI expiration and associated retention period as defined in 5.7;

  — apply and remove ESI deletion-holds, access-holds, modification-holds and restrictions.

7 TSS integrity, auditing, security requirements

7.1 Storage security

Direct access to the underlying storage device shall be limited. Administrative actions to the storage device shall be auditable. There should be no mechanism for anyone, including privileged users and administrators, to violate the security and the integrity of the ESI on a TSS. At a minimum, the TSS should maintain ESI-at-rest encryption using industry standard encryption methodologies (on the underlying storage volumes, to prohibit all external access and tampering with the contents of the ESI on the TSS). All internal ESI operations to migrate, transfer, copy and store ESI on the TSS shall be encrypted to maintain the same levels of security and to prevent unauthorized access to sensitive ESI.

7.2 ESI encryption

ESI on a TSS may be encrypted individually to provide additional security controls and measures. Encrypting individual ESI creates complexity for the applications and tools attempting to store, access and retrieve the ESI. Caution should be exercised when implementing ESI encryption to ensure that the application provides the proper safeguards to minimize ESI loss or corruption.

7.3 Secure delete and erasure

The TSS shall prohibit deletion or destruction of immutable ESI adhering to the strict retention enforcement controls as defined in 5.7. Eligible expired-ESI where the retention period has expired and is not under deletion-hold may be deleted by authorized personnel using a validated trusted interface or application as defined in the retention enforcement in 5.7. The TSS shall demonstrate complete and

irreversible destruction (expungement) of all copies of the deleted expired ESI in the system. ESI on magnetic media should be overwritten using a procedure conforming to the applicable standard or best practice for ESI deletion. Logs of approval of ESI deletion or destruction shall be maintained for a minimum of one year following the retention period. Best practice is to keep the logs of ESI deletion and destruction permanently.

7.4 Immutable ESI integrity checks

The TSS shall provide a mechanism to validate the authenticity of the contents of the immutable ESI to determine that it has not been modified, altered, tampered or corrupted. The creation of one or more hash values is the most commonly accepted method to validate and authenticate the contents of any ESI object. Hash values or checksums should be created and stored for immutable ESI. Each ESI content should be audited or checked on a periodic basis by the storage device against the specific hash values of the relevant ESI. The storage device should either automatically correct the ESI to its original state, as with corruption or ESI degradation, or notify the system administrator of any variances.

Multiple hash values are often used to avoid collisions. A collision is a rare occurrence where a single hash value may have different content yet produce the same hash value. That risk is mitigated by using more than one hash value to validate the integrity and authenticity of each individual ESI. An alternative to hash values is a checksum. It is recommended to select a TSS that uses one or more hash values to audit each ESI's integrity versus its original content when ingested into the TSS.

7.5 Redundancy and replication

The motivation for redundancy and replication is to eliminate any single point of failure in the context of the TSS that may result in the loss of data. At a minimum, a TSS shall support storing immutable ESI at two separate and safe locations, which shall remain protected and accessible. Preferably separate and safe locations may imply the use of independent resources including power, storage and infrastructure. While greater geographic diversity typically results in less risk, local regulations may restrict where certain types of ESI can be stored. All ESI that is moved between the two storage locations shall be encrypted for data privacy.

The TSS shall provide trustworthy replication of ESI to meet and address redundancy and availability requirements. The TSS cannot rely nor depend on external replication mechanisms whether through software or hardware to address the resiliency and redundancy requirements.

The TSS can enforce security restrictions that can limit and control who and which applications can access the ESI, to potentially restrict the access to authorized or validated applications and user credentials as defined in 5.2.

7.6 Storage migration and upgrades

Given the TSS support for the storage of both immutable and changeable ESI, the TSS shall accommodate changes, migration or an upgrade of the underlying storage technologies while maintaining the chain of custody and without compromising the security measures, including signatures. The TSS should accommodate changes to infrastructure to keep the ESI on current supportable technologies while ensuring the continuity and sustainability of each individual ESI in its lifecycle.

7.7 Auditability

7.7.1 General

All actions related to the ESI shall be audited. This requires some level of logging on both the application and storage side that differ depending on the architecture of the system. Auditing is required to ensure the reliability and trustworthiness of ESI and to permit forensic or practical investigation of changes, additions and deletions. A TSS shall track and support an audit of its own history of accesses and changes and shall do so in a way that is reliable and trustworthy. This function of the trusted storage is

independent of the auditability of the user applications. Auditability shall include chain of custody for the ESI.

7.7.2 TSS audit capabilities

TSS audit capabilities are mandatory to support investigations and forensic audits and to discourage those who may otherwise attempt to alter ESI. A TSS should store information about accesses, changes, time stamps and other meaningful actions in a way that is:

— sufficiently detailed to support audit and other analysis;

— structured to permit easy manual and automatic analysis of operations, preferably without interfering with current use of the storage system;

— as current (real-time updates) as possible;

— in itself impossible to alter.

7.7.3 TSS audit trail

All actions on the storage system, including reviews of logs and formal audits, accesses and writes of expired ESI, and attempts to alter metadata or ESI, shall be logged with time stamping. The time stamp should be tied to an independent time source and not the local system time source. Each log entry shall contain the following information for each action:

— nature of the action, e.g. access (read), write, audit, attempt to alter metadata or main ESI;

— ID or location of affected ESI;

— time and date;

— origin of the request for action, including at least one of the following: IP address, internal network address, username or ID of originating or otherwise responsible person;

— outcome of the action, e.g. normal granting of the request, blockage of the request, alert or alarm sent to monitor or authority, validation discrepancy, any further action correlated with the initial action.

8 TSS technical methods for trusted storage

8.1 General

While using an immutable storage system prevents intentional modification of content outside of the immutable preservation protection, there is a risk with any storage media that ESI can experience ESI degradation over time. To mitigate against the risk of ESI degradation, a TSS shall provide the capability to validate that the ESI being retrieved from the system has not changed since it was originally written to the TSS.

8.2 Security

For security requirements, reference should be made to ISO/IEC 27002, ISO/IEC 27040 and associated standards. The organization may implement and demonstrate security measures as specified in ISO 14641 or ISO/TR 15801, depending on the methodology selected by the organization.

Accordingly, organizations shall have management procedures to enforce their ESI security within a TSS that mitigates the security risks of storing organizational ESI data on non-TSS storage.

By contrast, non-TSS storage can easily be compromised and result in tampering by malicious users. Non-TSS compliant storage has no means of enforcing the application retention and deletion-holds. A

privileged user or malware can bypass the application. The application cannot protect and is not aware of the non-TSS data tampering or unauthorized destruction.

The TSS shall provide no less than two auditable copies of the data preferably stored on separate infrastructures or in geographically separate locations. This ensures the integrity and availability of each ESI at both sites even in the event of the loss of a data centre.

Independent time sources, date and time stamps, integrity and retention shall be maintained even when the underlying storage technologies of the TSS are refreshed.

8.3 Validate and detect corruption

The TSS shall maintain its own unique identifiers that can be used to independently validate the integrity of the immutable ESI, regardless of whether the state is expired ESI or retained ESI. To validate that ESI has not changed, the TSS shall create one or more checksums or other content validation value for each immutable ESI which can be used to confirm that the TSS ESI contents have not been modified or changed and to validate that the TSS managed copies of the ESI are identical. A digital signature can also be used since it includes a hash of the corresponding ESI contents as well as an associated identity. At a minimum, the hash value(s) shall be generated when the ESI is preserved. These hashes should be stored on the TSS and maintained as part of the audit logs. The ESI should be validated again on demand or automatically at an interval defined internally within the TSS. The hash value validation should re-generate the hash value(s) from the contents of the ESI on the TSS and compare it to the hash value(s) stored on the TSS. If the validation fails, the failure should be logged in the TSS audit logs and the TSS should try to correct the corruption by restoring a copy of the ESI from one of the replicated copies maintained by the TSS. All access to the corrupted or suspect ESI should be prevented (except the access for investigation or maintenance purposes by authorized persons) until the proper copy of the ESI is restored.

When ESI is found to be untrustworthy, the organization should have in place a policy to automatically or manually quarantine the corrupted ESI and replace the altered content with a trusted copy of the same content from the replicated store of the ESI. The system should alert the administrator when this event happens. The TSS should use at least one of the industry standard hash value methodologies, or any other hash or checksum methodologies available in the future, that minimize the risk of collisions and spoofing.

NOTE For examples of standard hash functions and methodologies, see the ISO/IEC 10118 series.

8.4 Ransomware protection

The TSS implementation's redundant underlying storage configurations and validations of each ESI's content against its original hash value shall also be able to detect and correct any ransomware impact at the application server or file server level. The files protected in the TSS shall be ransomware resistant by protecting the file's integrity and not allowing overwrites over the known good state of the files by ransomware and other malware.

8.5 Error correction

The TSS should be implemented using redundant underlying storage configurations. It shall incorporate mechanisms including hash or checksum validation to authenticate the integrity of the immutable ESI in the TSS. If corruption is detected, or the checksum validation fails, the TSS should report it with alerts and audit logs and should take corrective measures to restore a valid copy from one of the replicated copies maintained internally.

8.6 Monitoring, notifications and alerts

To the extent that the TSS can determine any functional or reliability issues that can impact the availability, integrity or authenticity of the ESI, it shall provide mechanisms to provide alerts, warnings and notifications in the context of system event logs and email messages. The TSS should provide