DRAFT INTERNATIONAL STANDARD

ISO/DIS 18759

ISO/TC **171**/SC **2**	Secretariat: **ANSI**
Voting begins on: **2018-09-25**	Voting terminates on: **2018-12-18**

Document management — Trusted Storage Sub-System (TSS) functional and technical requirements

Gestion des documents — Exigences fonctionnelles et techniques du sous-système de stockage fiable (TSS)

ICS: 37.080

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 18759:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC *171*, Document management applications, Subcommittee SC 2, Document file formats, EDMS systems and authenticity of information.

Introduction

Organizations storing digital content or ESI (Electronically Stored Information) need guidance on how to select design, implement and manage information and content management systems in such a way as to guarantee the reliability, authenticity, and integrity of the ESI contained within the system throughout its entire lifecycle. In addition to the business or organization's internal requirements to demonstrate the trustworthiness of its ESI, there are also externally mandated legal and regulatory trustworthiness requirements in the form of statutes, regulations and admissibility standards.

Both the ISO/TC 171, Document Management Applications and ISO/TC 46/SC11 Archives and Records Management committees have been working on the development of standards and best practices associated with developing and implementing a "Trusted Storage Sub-System" (TSS). The primary motive of this work is to provide clear, concise, vendor neutral requirements for information and content management systems responsible for retaining and delivering reliable and legally admissible ESI. As defined by ISO 15801, a trusted system is "information technology system with the capability of managing ESI in a trustworthy manner."

This document addresses the requirements for storage systems with regards to non-alterability, security, and verification, as are expressed in authoritative documents such as ISO 15801, ISO 22957, and ISO 18829. Historically, the concept of unalterable storage was referred to as WORM Write-Once Read Many and was primarily focused on the physical characteristics of the storage media. The intent of this document is to focus on preserving the integrity of the ESI independent of the actual underlying storage technology or its physical characteristics.

The title of this document, "Trusted Storage Sub-System (TSS) Functional and Technical Requirements," is meant to reflect the objective of the standard, which is to provide comprehensive details on the characteristics of trustworthy ESI storage solutions. It is meant to define the functional and technical requirements for any storage solution regardless of the actual nature of solution. The solutions implementing this document may rely on specific hardware and/or software features. It is not meant to suggest what constitutes a compliant storage device but rather focuses on the functional requirement and capabilities that in themselves are sufficient for a system to be designated a Trusted Storage Sub-System (TSS).

At a minimum, a TSS stores ESI in a tamper-proof configuration that is redundant and shall maintain multiple copies of the ESI in an unalterable secure format that prevents unauthorized deletions and that are ideally maintained in different physical locations. In particular, the Trusted Storage Sub-System meets the following criteria:

— Maintains at least two copies of the ESI in a minimum of two independent tamper-proof repositories that do not share any physical, virtual or hybrid infrastructure regardless of whether the TSS is on-premise or cloud and ideally is maintained in separate physical locations. For example:

  — Two storage arrays in the same server or storage chassis would not be compliant with this document

  — Two storage arrays in two separate servers or storage chassis along with the other TSS properties defined in this document would be a TSS. If those two independent systems are geographically separated, it provides greater redundancy.

— Supports storage of the ESI in an immutable form, demonstrates and monitors its integrity.

— Demonstrates that the ESI is retained until a policy-defined deletion point.

— Enforces that all policies are managed exclusively through the Trusted Storage Sub-System Management Interface (TSSMI) and are logged by the TSS.

— Maintains archive audit logs for ESI creation, retention and disposition, including litigation hold or changes to retention periods.

— Maintains security audit logs for attempts to tamper or compromise ESI integrity or the security of the TSS.

— Enables the logging of ESI read, write, and modify operations, though auditing access operations may become a burden to maintain and store.

— Monitors the underlying storage technology or infrastructure to provide alerts and notifications that would enable authorized personnel to take appropriate action including replacing components or migrating to alternate storage technologies.

Changes in the legal and technological landscape, the evolution and possible obsolescence of storage technologies should be taken into consideration and constantly monitored. We shall take into consideration that over the lifetime of the data the underlying storage has evolved in certain instances such technologies have literally become extinct. Some hardware manufacturers have gone out of business, shutdown divisions, or discontinued offering citing various reasons from lack of adoption to other business reasons.

The primary focus has always been the viability and reliability of the data and that is dependent on the fundamental need to keep it accessible, verifiable, valid and authentic, taking into consideration that over time the physical storage may have to change without impacting the trustworthiness of the data itself. This document is motivated by the evolution of storage technologies. The de facto paradigm for trusted storage has been writable but non-rewritable optical media, which are "write-once" by virtue of the nature of the media and the method of writing to them. However, new non-optical storage systems have evolved that accomplish "write-once" objectives through a combination of hardware and software controls. Understanding what specific functionality is required of these systems to meet TSS requirements is the primary motivation for this document.

The ISO 15801 definition of a trusted system contains two elements. The first element is the requirement that any ESI retrieved from the system can be proven to be authentic and having integrity (complete and unaltered). The second element is that during the lifecycle of the system itself, it can be demonstrated that the TSS demonstrates authenticity, integrity, usability and confidentiality of all the ESI it contains during the ESI's lifecycle. These two elements of the definition of a trusted system correspond to the admissibility of ESI as evidence into legal proceedings, and the obligations of both public and private organizations to maintain reliable and accurate electronic documents for purposes of accountability and transparency. This document for trusted storage environments addresses both these criteria and shall therefore provide guidance to organizations seeking to meet their own internal requirements and in addition, also meet diverse legal requirements and mandates relative to the production, preservation, security and management of their electronic documents.

The ISO 14641 provides a reference framework for organizations implementing secure information systems and identifies characteristics such as optimization of long-term electronic document preservation, archiving and integrity and more importantly in principle do not conflict with the objectives of this document. This document extends the specifications "intended to demonstrate that all documents to be managed by the information system are captured, stored, retrieved and accessed in a way that guarantees that the archived document is an authentic rendition of the original document for the duration of preservation" [SOURCE ISO 14641] combined with the trustworthiness provisions of the Trusted Storage Sub-System in this document. For the purposes of this document, "an authentic rendition means that the rendered document corresponds to the source document as it was at the time of input in the information system in respect of criteria of fidelity and integrity, and that this state is maintained for the duration of preservation" [SOURCE ISO 14641].

The primary difference in the scope of this document versus the definitions identified in the ISO 14641 is this document focuses on the functional requirement of what constitutes a Trusted Storage Sub-System rather than the focus on the physical characteristics of the archival media (physical WORM, logical WORM and rewritable media) as defined in ISO 14641. It should be noted that requirements for archival integrity of the electronically stored information on a Trusted Storage Sub-System do not conflict with those identified in ISO 14641 including the use of "encryption-like techniques, in particular with checksum calculation or hash function, date and time stamp or digital signature" [SOURCE ISO 14641]. Where possible this document will leverage the applicable definitions identified

in the ISO 14641 as well as other referenced standards to establish a common more comprehensive framework for a Trusted Storage Sub-System.

Organizations that are implementing a TSS should have a defined process to review and analyse their ESI before simply committing it to a TSS. Consult a professional or use an analysis tool that may assist you 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. In this document, we are defining the various functional requirements; bearing in mind 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 stored in a TSS whether it is unstructured or structured ESI is irrelevant to the fundamental functional control defined within the TSS. The requirements identified herein will focus on the features and capabilities of the TSS that would support compliance with security, preservation and retention requirements independent of the source of the ESI or the applications used to access the information.

Recognizing that storage technologies will continue to mature and morph over time, this document is based on the concept that the overall TSS does not rely on specific storage technologies or media. Rather, this document specifies functional requirements for storage technologies/media allowing organizations to maintain their information in a secure fashion.

This environment shall operate regardless of the underlying storage technology, whether optical, magnetic, solid state storage technologies, or whatever else. This document is based on the concept that access to the ESI stored in a TSS is secured from any external access and once configured can only be accessed via the TSS audited interface. This document will also identify reporting requirements for these storage systems that shall manage access control and provide information on other aspects of TSS integration related requirements.

Document management — Trusted Storage Sub-System (TSS) functional and technical requirements

1 Scope

This document specifies the functional and technical requirements associated with storage systems storing and managing organizational documents, in a protected and secured fashion, during the lifecycle of the information. This document does not specify specific storage media types or configurations.

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

ISO 14641:2018, *Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications*

ISO 15489-1:2016, *Information and documentation — Records management — Part 1: Concepts and principles*

ISO/TR 15801:2017, *Document management — Electronically stored information — Recommendations for trustworthiness and reliability*

ISO 17068:2017, *Information and documentation — Trusted third party repository for digital records*

ISO/TR 17797:2014, *Electronic archiving — Selection of digital storage media for long term preservation*

ISO 18829:2017, *Document management — Assessing ECM/EDRM implementations — Trustworthiness*

ISO/TR 22957, *Document management—Analysis, selection and implementation of electronic document management systems (EDMS)*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
Trusted Storage Sub-System (TSS)
a Trusted Storage Sub-System (TSS) demonstrates storage of Electronic Stored Information (ESI), in compliance with the functional and technical requirements of this document

Note 1 to entry: A TSS meets the requirement of a trusted system to store two copies of the ESI written in an unalterable format to two separate TSS storage repository locations, each providing the write-once controls independent of the physical characteristics of the physical storage media used. A TSS is one that provides write once functionality by the internal controls within the system and not strictly only the nature of its media.

3.2
Trusted Storage Sub-System Management Interface (TSSMI)
a Trusted Storage Sub-System management interface is the only mechanism that can manage and administer the security and retention policies of a TSS.

3.3
WORM state
describes a writable functional state of ESI stored in a TSS whose contents and properties (name, size) can never be modified or altered for its during its lifecycle as defined by the retention schedule.

Note 1 to entry: This immutable write protection affords the assurance that the data contained within the document cannot be tampered with once it is in this WORM state for the entire remainder of the ESI lifecycle.

3.4
trusted ESI (tESI)
ESI stored on a TSS which is in a WORM state and whose contents and properties (name, size) can never be modified or altered for its entire existence.

Note 1 to entry: to entry: Alternatively, we can reference immutable ESI (iESI)

3.5
retained ESI (rESI)
an immutable ESI stored on a TSS which may at some point in the future become eligible for disposition based on an assigned minimum retention period.

4 Retention requirements for trusted storage environments

4.1 Overview

To demonstrate ESI integrity and protect the chain of custody of the trusted ESI -- shall prevent additions, modifications and deletions of stored ESI as well as track all accesses. This is not possible by simply writing to a standard storage system. Instead, it requires a storage system that can accept and enforce the retention rules, disposition policies and security policies assigned to stored ESI maintained within the internal controls of the TSS.

4.2 Electronically Stored Information (ESI)

In the context of this document, we refer to the general concept of ESI to represent an ESI object that is a self-contained container of ESI that represents a digital form of information which can be created, authored, accessed, read, modified, processed or edited. Under various circumstances:

(i) ESI stored on a TSS may remain modifiable for its entire existence and only possible restrictions that would apply would be related to security privileges and restrictions enforced by the TSS.

(ii) Once ESI stored on a TSS is finalized, it will be considered as Trusted ESI and is no longer modifiable for its entire existence and is eligible to become a Retained ESI once a retention is assigned.

4.3 Retained ESI

A retained ESI is protected ESI that has met certain criterion to become an immutable ESI, which is designated as no longer modifiable for its entire retained life span and may be assigned an explicit minimum retention period upon which the disposition and destruction is allowed once the minimum retention period has lapsed and expired. In other words, retained ESI contents and properties including name can no longer be modified for the duration of the defined retention period. Once an immutable ESI is retained, the only possible actions are to extend or assign an expiry period, apply a legal hold or delete it once the retention period has expired.

All retained ESI stored on a TSS shall remain unmodifiable for the entire duration of their existence on the TSS and the only possible modification would be to delete them once they are eligible for disposition.