SLOVENSKI STANDARD
SIST ISO 17068:2018

01-oktober-2018

Nadomešča:
SIST-TP ISO/TR 17068:2013

Informatika in dokumentacija - Repozitorij za digitalne zapise zaupanja vredne tretje strani

Information and documentation - Trusted third party repository for digital records

Information et documentation -- Référentiel tiers de confiance pour les enregistrements électroniques

Ta slovenski standard je istoveten z: ISO 17068:2017

ICS:

01.140.20	Informacijske vede	Information sciences

SIST ISO 17068:2018 **en,fr,de**

INTERNATIONAL STANDARD

ISO 17068

First edition
2017-10

Information and documentation — Trusted third party repository for digital records

Information et documentation — Référentiel tiers de confiance pour les documents d'activité électroniques

Reference number
ISO 17068:2017(E)

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

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 46, *Information and documentation*, Subcommittee SC 11, *Archives/records management*.

Introduction

As digital records are the inevitable by-products of various business activities in digital systems, there is an increasing need to secure the authenticity and legal admissibility of digital records during their period of retention. It is internationally agreed that "digital records shall not be denied validity or enforceability of legal recognition by reason of their format alone"[1)]. Despite this, it is very difficult for an organization to assert that its digital records are authentic and able to act as effective evidence of business action over a long period. In many cases, legal admissibility of digital records managed by organizations' records systems is not ensured. As a result, there is a growing need for services safeguarding these characteristics for digital records by neutral third parties.

In order to protect digital records from business disputes during the period they are required for sustaining legal obligation and ongoing retention, it is essential to ensure that the authenticity, reliability and integrity of digital records endures.

Digital signatures are a well-known means to ascertain if digital records have been tampered with. However, as a digital signature only safeguards integrity within its validity time (generally one to two years or less), most digitally signed records do not ensure their integrity for longer than this validity time. It may thus be very difficult for an individual record system to prove the integrity of their digital records for the period of retention obligation, where this is longer than the validity period of the digital signature.

A possible solution is provided by a Trusted Third Party Repository (TTPR). A TTPR is defined as a third party's qualified retention service that ensure that digital records, entrusted to it by a client, remain and are asserted to be reliable and authentic, with the aim of providing reliable access to managed digital records to its clients for the period of obligation for retention. A TTPR for digital records provides trustworthy services for clients, which should be examined by interested parties (i.e. inspector, auditor, evaluator). These TTPR services are helpful to identify the evidence admissibility of clients' digital records as a source of evidence.

Clause 4 provides an overview of a TTPR including rationale for the criteria and the mechanism of trustworthiness and characteristics and components of TTPR.

Clause 5 specifies the services to be provided by a TTPR for the clients' digital records during the retention period. Clause 5 specifies the technological requirements of hardware and software systems and Clause 6 provides the operational processes requirements.

1) Article 8, Chapter 3, UNCITRAL 2007, United Nations Convention on the Use of Electronic Communication in International Contracts.

Information and documentation — Trusted third party repository for digital records

1 Scope

This document specifies requirements for a trusted third party repository (TTPR) to support the authorized custody service in order to safeguard provable integrity and authenticity of clients' digital records and serve as a source of reliable evidence.

This document is applicable to retention or repository services for digital records as a source of evidence during the retention periods of legal obligation in both the private and the public sectors.

This document has the limitation that the authorized custody of the stored records is between only the TTPR and the client.

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 30300, *Information and documentation — Management systems for records — Fundamentals and vocabulary*

ISO 30301, *Information and documentation — Management system for records — Requirements*

ISO 30302, *Information and documentation — Management systems for records — Guidelines for implementation*

UNCITRAL 2007, *United Nations Convention on the Use of Electronic Communications in International Contracts*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
authenticity certificate
document issued to authenticate the digital record in the TTPR

3.2
authenticated copy
digital copy of a *digital record* (3.5) for which authenticity has been verified before

3.3
client
individual or organization that has an agreement with the *TTPR* (3.15)

3.4
client system
hardware and software used by a client to use the service provided by the *TTPR* (3.15)

3.5
digital record
information in any format created, received and maintained by digital means, used as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business, which is packaged with necessary data for submission, dissemination, and archive

[SOURCE: ISO 15489-1:2016, 3.14, modified]

3.6
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the digital record to prove integrity of the *digital record* (3.5)

Note 1 to entry: A data unit is a binary block created cryptographically from original data record.

[SOURCE: ISO 7498-2:1989, 3.3.26, modified]

3.7
information package
digital record (3.5) and associated description information which is needed to aid in the identification and operation for the authentic and reliable digital records, consisting of the digital record, creator's *digital signature* (3.6) and/or a *TTPR* (3.15) or third party's timestamp, and the associated preservation description information

Note 1 to entry: The information package has associated packaging information used to delimit and identify the digital record and description information of operation such as submission, preservation or dissemination for the authentic and reliable records.

Note 2 to entry: See ISO 14721.

3.8
process
series of actions or events taking place in a defined manner leading to the provision of *TTPR services* (3.16)

3.9
public key certificate
public key of a user, together with some other information, rendered unforgeable by *digital signature* (3.6) with the private key of the certification authority which issued it

Note 1 to entry: Public key certificates are issued and signed by a certification authority (CA). The entity that receives a certificate from a CA is the subject of that certificate.

3.10
service level agreement
SLA
written agreement between a service provider and a client that documents services and agreed service levels

[SOURCE: ISO/IEC 20000-1:2011, 3.29, modified]

3.11
system
hardware and software of the *TTPR* (3.15)

3.12
trusted archival information package
TAIP
information package (3.7) which is preserved in a *TTPR* (3.15) after verification of *TSIP* (3.14)

3.13
trusted dissemination information package
TDIP
information package (3.7), derived from one or more *TAIP*s (3.12), received by a client in response to a request to a *TTPR* (3.15)

3.14
trusted submission information package
TSIP
information package (3.7) that is delivered by a client to a *TTPR* (3.15) with creator's and/or sender's *digital signature* (3.6) and a TTPR or third party's timestamp, delivering the time and information of the sender

Note 1 to entry: Herein, the digital signature is prepared using the *public key certificate* (3.9) and the time stamp is created in accordance with the time stamping module provided by a TTPR.

[SOURCE: ISO/TR 17068:2012, 2.12]

3.15
trusted third party repository
TTPR
third party's qualified retention service that ensure that the *digital records* (3.5) entrusted to it by a client remain and are asserted to be reliable and authentic

Note 1 to entry: This has the goal of providing reliable access to managed digital records to its clients in the period of obligation for retention.

3.16
TTPR service
intangible product that is the result of at least one activity performed at the interface between a *TTPR* (3.15) and a client

[SOURCE: ISO/TR 17068:2012, 2.15]

3.17
third party
person or body that is recognized as being independent of the parties involved, as concerns the issue in question

3.18
trustworthiness
quality [of a *TTPR* (3.15)] of being dependable and reliable

Note 1 to entry: A trustworthy TTPR is trusted to deliver its services in an authentic manner by following documented policies and processes and ensuring the accuracy, reliability and authenticity of the records in the repository over time.

4 Overview of a TTPR

4.1 Necessity for a TTPR

With the development and advancement of information and communication technology (ICT) over the last two decades, the use of digital records has increased greatly. Accordingly, the number of electronic transactions carried out by individuals and organizations in their daily activities has increased. For example, in international transactions, many documents and records in digital formats are exchanged in order to initiate, process and complete transactions between importers and exporters. Banks are also involved in digital records exchanges to confirm credit or payment. In the health industry, treatment records are exchanged between clinics or patients and insurance companies; order of treatment records are exchanged between general clinics and specialized clinics. These kinds of individual or organizational transactions are very common within one sector or across several industries. During these transactions, digital records is easily copied, modified and distributed by an unauthorized

person. This aspect of documents and records retained in digital formats creates the risk of alteration or forgery, and has raised awareness of the need for the secure management and transaction of digital records.

To help prevent possible risks, some countries have enacted laws and regulations requiring provable authenticity, reliability, integrity and accessibility as a precondition for legal effect and enforceability of digital records. These regulations explain the requirements for adopting secured digital records and for judging their evidential admissibility. However, these requirements only typically describe the mandatory characteristics that retained digital records need to have, regardless of an organization's records management capability. While many organizations have implemented a records system for themselves, implementation of digital records exchange across organizations often faces a number of challenges. Individuals are also limited in their ability to comply with legal requirements for the admissibility of their digital records. This limitation might cause social problems, delay operational processes, reduce efficiency and prevent electronic exchange.

Therefore, as the exchange of secure records becomes more significant for individual and/or organizational collaboration, the social demand for a trustworthy electronic transaction environment has emerged as one of the major issues in digital environments today. Protecting information in digital records is beginning to be regarded as an indispensable precondition for operational efficiency and economic benefit in organizations across all sectors and industries.

One way of resolving this situation is to use a TTPR. A third party is an independent individual or organization that is separate from the direct interests of mutual parties, and that acts as an intermediary when two parties are exchanging digital information in a secure manner. Society and governments shall be in a position to trust the third party. To prevent any complications that can arise during electronic transactions, a TTPR operates systems and facilities and follows well-defined procedures according to the principles and guidelines for managing digital records in a secure manner. During these processes, the TTPR ensures the authenticity, reliability, integrity and usability of digital records, for the period of the agreed service. In addition, the TTPR shall provide an official source of digital records that can be admissible as evidence from a third party in the event of a dispute between parties regarding their records.

TTPRs play a significant role and provide several benefits to parties involved. A TTPR could provide document digitization services for converting paper documents into authentic digital records. It could also provide services for managing digital records. A TTPR is endowed with authorized custody over the stored records. A TTPR also provides services by issuing certificates on digital records processed and retained by the TTPR. Furthermore, a TTPR works as an intermediary to provide a secure exchange of digital records between creators, senders and receivers in many forms of electronic transactions (e.g. one-to-one party, one-to-many parties, many-to-many parties in business transactions and operational workflows). As such, a TTPR provides a public service for secure electronic information exchange between individuals or organizations.

As a result, a TTPR can have a role in the management of digital records produced or received in both the public and the private sector. The TTPR helps reduce the cost of constructing and operating internal repositories by enabling the outsourcing aspects of digital records management. Recently, with the increasing popularity of cloud computing service environments, the shift from traditional records management to service-oriented approaches is appropriate. Therefore, TTPR services are helpful for effective and efficient management of digital records.

4.2 Requirements for TTPR trustworthiness

A TTPR is provided by an independent organization as a service for its clients. This organization, as any other, should have its own management system, which may be based on ISO Management Systems Standards. Dealing with digital records of clients, the implementation of a Management System for Records compliant with ISO 30301 requirements for their own records is an extra factor of trustworthiness.

TTPR trustworthiness shall be achieved by meeting the high level requirements in terms of authenticity, reliability and integrity described in ISO 30300, ISO 30301, ISO 30302 and by following the requirements

for electronic communications formulated by UNCITRAL. Moreover, TTPR trustworthiness extends to information packages described by the open archival information system suggested in ISO 14721 for the purpose of reliable custody.

The trustworthiness requirements are broken down into the attributes of authenticity, reliability and integrity described below.

— The **authenticity** of the client's digital records is accounted for in a business context, for example, the creators' place of business at time of creation of the record is retained. The TTPR shall check this.

  — The TTPR agrees with the client regarding the client's role and responsibility for authenticity during the service agreement period. When the TTPR checks the state of authenticity of the clients' records, the client is able to account for this. If a client can't account for the authenticity of its digital records, the TTPR is unable to classify those digital records as authentic.

  — The authenticity of digital records created by the client can be managed at the time of "freezing" the record by using authentication technology such as the timestamp, digital signature, etc. To manage this, the clients' digital records system can attach the timestamp to create records, sourced from the time stamping module provided by the TTPR. It can also attach the clients' digital signature to the digital records. Using this digital signature, digital records that have been falsified can be recognized.

— The **reliability** of digital records can be confirmed by verifying the custody of digital records. However, the TTPR specifies only where the custody is between the TTPR and its clients. The TTPR and the client shall check this.

  — A client transfers digital records to the TTPR as a package in the form of a trusted submission information package (hereinafter referred to as "TSIP").

  — The TTPR confirms the reliable custody of clients' digital records by validating received clients' TSIP regarding any change in the digital records and/or any transmission errors.

— The **integrity** of digital records shall be managed after creation for the period of retention. After verifying the authenticity and reliability requirements of transmitted digital records, the TTPR shall allow to verify the integrity for the period of retention by registering these records as a TAIP package.

— The **availability** of digital records shall be confirmed by TTPR's robustness with backup and recovery policy and system. TTPR shall provide adequate security and resilience for ensuring the availability of digital records.

The TTPR retains and manages metadata for the registration event, including the time of registration, retention period, client information and history of digital records. In order to be able to confirm trustworthiness of the stored digital records, the TTPR shall document key processes in the management of digital records, such as acquisition, retention, distribution, delivery and/or migration and disposition, and provide the document to a client as proof when requested.

4.3 TTPR components

A TTPR comprises services provided by technology and operations as shown in Figure 1.

TTPR services are provided to a client after the client has been authorized to use the TTPR service through an agreement. The TTPR guarantees all the qualified retention service specified in the agreement to the client, to the agreed level of service quality. The client makes a service level agreement (SLA) (see 5.3) with the TTPR, which includes the service item and the quality level maintained by TTPR. The client also fulfils all the obligations in the agreement. For example, the client provides the metadata required for validation of the authenticity of digital records into information packages. The TTPR is able to verify the authenticity of the transmitted digital records. The client shall have social credit which can be estimated quantitatively by a reliable organization.

