TECHNICAL REPORT

ISO/TR 17068

First edition
2012-11-01

Information and documentation - Trusted third party repository for digital records

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

Reference number
ISO/TR 17068:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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.

ISO/TR 17068 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 electronic and/or digital systems, there is an increasing need to secure the 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 may be 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 may not be ensured. As a result, there is a growing need for certification services 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 of maintaining the integrity of digital records. However, as a digital signature can only ensure integrity within its validity time (generally one to two years or less), most digitally signed records cannot ensure their integrity for longer than this validity time. As a result, it may 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 can be provided by a Trusted Third Party Repository (TTPR) service.

A TTPR is defined as a set of services, systems and personnel that ensure that digital records, entrusted to it by a client, remain and can be 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 should provide trustworthy services for clients, which can 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.

This Technical Report describes the specific requirements for the trustworthy services provided by a TTPR. Its main purpose is to ensure that digital records can retain the relevant evidence and information in an ensured and trusted manner during the required period of retention.

1) UNCITRAL 200t, 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 Technical Report details the authorized custody services of a Trusted Third Party Repository (TTPR) in order to ensure provable integrity and authenticity of the clients' digital records and serve as a source of reliable evidence.

It describes the services and processes to be provided by a TTPR for the clients' digital records during the retention period, to ensure trust. It also details the criteria of "trustworthiness" and the particular requirements of TTPR services, hardware and software systems, and management.

This Technical Report has the limitation that the authorized custody of the stored records is between only the third party and the client.

2 Terms and definitions

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

2.1
client
individual or organization that contracts with the TTPR and obtains permission to use the TTPR services

2.2
client system
hardware and software used by a client to use the service provided by the TTPR

2.3
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

NOTE Adapted from ISO 15489-1:2001.

2.4
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the unit and protect against forgery by, for example, the recipient

NOTE Adapted from ISO 7498-2:1989.

2.5
information package
content information and associated preservation description information which is needed to aid in the identification and preservation of the authentic and reliable digital records

NOTE 1 The information package has associated packaging information used to delimit and identify the content information and preservation description information.

NOTE 2 Adapted from ISO 14721:2012.

2.6
process
series of actions or events taking place in a defined manner leading to the provision of TTPR services

2.7
public key certificate
digitally-signed statement that binds the value of a public key to the identity of the person, device or service that holds the corresponding private key

NOTE 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.

2.8
service level agreement
SLA
written agreement between a service provider and a client that documents services and agreed service levels

NOTE Adapted from ISO/IEC 20000-1:2011.

2.9
system
hardware and software of the TTPR

2.10
trusted archival information package
TAIP
information package, consisting of the content information, creator's digital signature and a TTPR or third party's timestamp, and the associated preservation description information, which is preserved in a TTPR after verification

2.11
trusted dissemination information package
TDIP

information package, derived from one or more TAIPs, received by a client in response to a request to a TTPR

2.12
trusted submission information package
TSIP
information package that is delivered by a client to a TTPR with creator's and sender's digital signature and a TTPR or third party's timestamp, delivering the time and information of the sender

NOTE 1 Herein, the digital signature is prepared using the public key certificate and the time stamp is created in accordance with the time stamping module provided by a TTPR.

NOTE 2 Adapted from ISO/TS 15000-2:2004.

2.13
trusted third party repository
TTPR
set of services, systems and personnel that ensure that the digital records entrusted to it by a client remain and can be asserted to be reliable and authentic

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

2.14
TTPR certificate
digital document issued to authenticate the digital record in the TTPR

2.15
TTPR service
intangible product that is the result of at least one activity performed at the interface between a TTPR and a client

NOTE Adapted from ISO 9000:2005.

2.16
third party
person or body that is recognized as being independent of the parties involved, as concerns the issue in question

2.17
trustworthiness
quality (of a TTPR) of being dependable and reliable

NOTE A trustworthy TTPR can be 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.

3 Overview of a TTPR

3.1 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 electronic 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 can be easily copied, modified and distributed by an unauthorized person. This aspect of documents and records retained in digital formats may create 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 electronic 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 build and 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 should be in a position to trust the third party. To prevent any complications that may 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 contracted service. In addition, the TTPR provides an official source of digital records that are admissible as evidence from a third party in the event of a dispute between parties regarding their records.

TTPRs can play a significant role and provide several benefits to parties involved. A TTPR could provide document digitization services for converting paper documents into digital records with legal admissibility. It could also provide services for managing digital records. A TTPR is endowed with authorized custody over the stored records. A TTPR also provides certification services by authenticating digital documents and issuing certifications on documents 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 can provide 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 electronic 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 can be helpful for effective and efficient management of digital records.

3.2 Requirements for trustworthiness

The trustworthiness requirements of the TTPR should meet the high level requirements in terms of authenticity, reliability and integrity described in ISO 15489 (all parts) and should follow the legal requirements for electronic communications formulated by UNCITRAL. Moreover, these requirements need to extend to information packages driven from the reference model for information archival suggested in ISO 14721 for the purpose of reliable custody.

A TTPR should follow the trustworthiness requirements 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 should be retained. The TTPR should be able to check this.

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

  — The authenticity of digital records created by the client is maintained using the timestamp and digital signature applied at the time of 'freezing' the record. To ensure this, the clients' digital records system should attach the timestamp to created records, sourced from the time stamping module provided by the TTPR. Also it should attach the clients' digital signature to the digital records. Using this digital signature, digital records that have been falsified can be recognized immediately, and consequentially, their authenticity and integrity can be challenged.

— The **reliability** of digital records can be confirmed by verifying the custody of digital records. However, the TTPR should specify only where the custody is between the TTPR and its clients.

  — A client should transfer digital records to the TTPR as a package in the form of a Trusted Submission Information Package (TSIP).

  — The TTPR should confirm 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 should be retained after creation for the period of retention. After confirming the authenticity and reliability requirements from transmitted digital records, the TTPR should maintain the integrity for the period of retention by registering these records as a TAIP package (i.e. the information package of the TTPR's signed registration metadata, the attached clients' digital records and evidential history).

The TTPR should retain and manage the registration metadata, including the time of registration, retention period, client information, the history of digital records, etc. In order to be able to confirm trustworthiness of the stored digital records, the TTPR should be able to document key processes in the management of digital records, such as acquisition, retention, distribution, delivery and migration and disposition, and provide the document to a client as proof when requested.

3.3 TTPR components

A TTPR comprises services, systems and personnel as shown in Figure 1.

Services are provided to a client by the TTPR after the client has been authorized to use the TTPR service through a contract. The TTPR should provide all the services specified in the contract to the client, to the agreed quality level. The client should also fulfil all the obligations in the contract. For example, the client should include the metadata required for validation of the authenticity of digital records into information packages. The TTPR should be able to verify the authenticity of the transmitted digital records. Besides the service provider and the client, there are other parties indirectly related to the TTPR, for example, the inspector, auditor, evaluator. They are referred to as interested parties. The inspector is an individual/organization that reviews technical issues in detail to determine whether the digital records stored in a TTPR have legal evidential admissibility. The auditor is an individual/organization that audits and monitors whether a TTPR is managed according to the defined procedures and guidelines. The evaluator is an individual/organization that mainly judges whether a software/hardware system satisfies the necessary functional requirements. The evaluator checks and verifies the TTPR based on objective and formally established criteria, to provide the basis by which TTPR can secure the confidence of its clients.

The software/hardware system fulfils its role as a tool, allowing the TTPR to maintain trustworthiness and provide different services required by clients. The transmission system, which allows the client's created digital record to be transmitted reliably with integrity, the verification system which automatically validates the metadata required for authenticity check during the acquisition stage, and the repository system for the retention and management of the digital record, are included in such software/hardware system. Also, the client's system is necessary for the TTPR to maintain a safe and reliable transmission channel and use a standardized transmission package.

The TTPR's personnel have two main tasks: management and marketing. The management task operates software/hardware to provide the TTPR services and preserves service quality. The marketing task performs public relations and collects the clients' requirements.

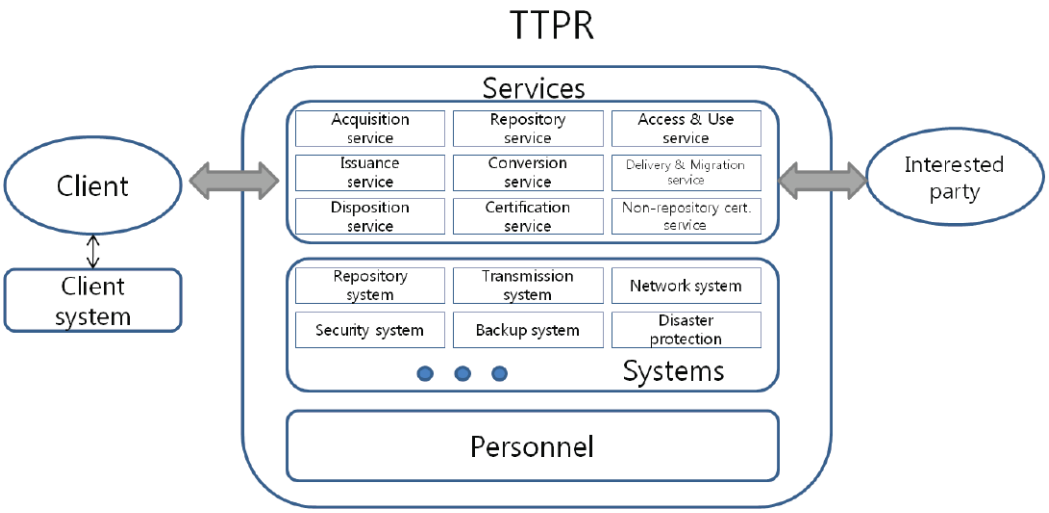

Figure 1 — TTPR Overview

3.4 Characteristics of a TTPR

For a TTPR to be a reliable agent of digital record management for clients, the TTPR should be capable of providing consistent and stable service, have specialized competence to guarantee the evidential admissibility of the digital records, and maintain neutrality toward all parties. The basic characteristics required of the TTPR are divided into three aspects: stability, expertise and neutrality.

Stability: For consistent management of the stored digital records consigned to the TTPR and to provide trustworthiness to the client, a TTPR should ensure stability. A TTPR should have sufficient capital and human resources, a management strategy and execution capability. Furthermore, the TTPR should be able to store, maintain and manage digital records normally, even in an emergency situation. To ensure this capacity, the TTPR should have in place a disaster protection and recovery system.

Expertise: A TTPR should have expertise in coping with all the matters related to digital records. Expertise is the essential attribute of the TTPR in ensuring the authenticity, reliability, integrity and usability of their client's digital records. The maintenance and management of a safe and efficient digital record management system is also based on such expertise. The TTPR should employ experts and be equipped with specialized processes and systems to ensure its own expertise. Specialized procedures should be established for activities related to digital record management, such as acquisition, archiving, certification, delivery and migration and disposition of the digital record. The TTPR should be equipped with a specialized system to provide functions related to digital record management, such as metadata processing, reliable messaging, security, digital signatures, time-stamps, etc.

Neutrality: A TTPR should maintain its neutrality toward all parties. A TTPR will only be recognized within society if its neutrality is maintained. In addition, a TTPR should satisfy the guidelines and requirements proposed in this Technical Report, and should be independent in its performance of reliable digital record management, regardless of any external pressure; political institution, client organization and all the stakeholders.

4 TTPR services

4.1 Service procedure

After the formation of a contract between a client and a TTPR, the client should construct a system by adopting modules or specifications provided by the TTPR, whose functions are packaging digital records, attaching a digital signature and transmitting the digital records. After constructing the client system, the client can transmit digital records packaged in the form of a TSIP to the TTPR through the transmission channel at a specific time or at any time, according to the contract. When the TTPR receives the package, it verifies the package and its integrity. If there are no problems, the TTPR repackages the submitted package into a TAIP and places it in digital storage. The client may request an authenticity certificate or confirmation documents to prove that the digital records have reached each stage of submission without problems.

A TTPR has a facility to migrate the digital records stored in the TTPR to other TTPRs, or to the client who owns the records. When the agreed period of the digital records' storage expires or the client requests the disposition of the records, the TTPR will dispose of the records.

4.2 TTPR service contracts

4.2.1 General

A TTPR should contract with a client to provide services to the client. The contract should specify the engagement of the service type, the service period, the authority and duty of the client, and the responsibility of the TTPR. In particular, a TTPR service contract should clearly state whether the client needs to provide information to the TTPR to prove the authenticity of digital records submitted by them, to enable the TTPR to meet its responsibility as a provider of trustworthy services. It is recommended that the contract includes a service level agreement (SLA) between a client and a TTPR. An SLA should clarify the quality factors and the levels of TTPR services agreed by the client and the TTPR. An SLA

may also describe the method and amount of compensation when the TTPR does not meet the service level agreed in the SLA. The contract may also fix the TTPR's authority or determine the limitation of the client's accountability/responsibility, and provide a reasonable solution for any case or incident which may arise. The client's damages due to TTPR service problems may be minimized through the SLA contract, in which the client may give a penalty or incentive to the TTPR based on the quality of the provided service.

4.2.2 Service contract items

To use the service provided by a TTPR, clients (individuals or organizations) should enter into a service contract with the TTPR. The following should be included in the service contract:

— service fees;

— service period;

— confirmation of digital record's authenticity;

— the procedure and method of digital record transmission;

— the scope of accountability and responsibility of the TTPR and the client;

— the type of service the client is willing to use, pertaining to the management service;

— the client's authority of access and use for consigned digital records;

— issues related to security and data protection of consigned digital records;

— provision of necessary information by the client and the TTPR during the service period;

— issues related to insurance coverage in the event of compensation due to service or disaster; and

— issues related to service quality and evaluation on the quality.

4.2.3 Service level agreement

4.2.3.1 General

The client should consent to the service agreement in order to use the service provided by the TTPR. The TTPR should provide the service based on the agreement to which the client has consented, and the client should also conform to the service agreement and have the right to receive the service. The main items of a SLA are described below.

4.2.3.2 Service period

A TTPR should be obliged to provide the service to the client in accordance with the agreement during the contract period, and the client should have the right to receive the service in accordance with the agreement during the period. The client may specify the following regarding the service period:

— Effective period of service agreement;

— Retention period for each digital record; and

— Available period of non-repository certification service (refer to 4.3.9).