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 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Overview of a TTPR **3**
4.1 Necessity for a TTPR 3
4.2 Requirements for TTPR trustworthiness 4
4.3 TTPR components 5
4.4 Characteristics of a TTPR 6

5 TTPR services **7**
5.1 General 7
5.2 Service procedure 7
5.3 TTPR service agreements 7
5.3.1 Service level agreement (SLA) 7
5.3.2 Service agreement items 8
5.4 TTPR subservices 10
5.4.1 General 10
5.4.2 Acquisition service 11
5.4.3 Repository service 12
5.4.4 Access and use of service 12
5.4.5 Issuance service 13
5.4.6 Conversion service 14
5.4.7 Delivery and/or migration service 14
5.4.8 Disposal service 15
5.4.9 TTPR certification service 16
5.4.10 Non-repository certification service (Remote Certification Service) 18

6 Technological requirements **19**
6.1 General 19
6.2 Digital record repository 20
6.3 Transmitter–receiver 20
6.4 Network system 20
6.5 Time-stamping 20
6.6 Audit trail 21
6.7 Network security system 21
6.8 Access control equipment 21
6.9 Disaster recovery facility 22
6.10 System for certificate issuance and validation of digital records 22
6.11 Backup system 23

7 Operational requirements **23**
7.1 General 23
7.2 Client management 24
7.3 Administrator's role and authority management 24
7.4 Network and security management 25
7.5 Digital records management 25
7.6 Operation of transmitted and received messages 28
7.7 Audit record 29
7.8 Data backup and recovery 29
7.9 Security management 30
7.10 Migration and receipt management 30
7.11 Client system management 31

© ISO 2017 – All rights reserved

Bibliography **33**

 © ISO 2017 – All rights reserved

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*.

© ISO 2017 – All rights reserved

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.

© ISO 2017 – All rights reserved

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)

© ISO 2017 – All rights reserved

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)

© ISO 2017 – All rights reserved

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

© ISO 2017 – All rights reserved