PD ISO/TR 17068:2012

BSI Standards Publication

# Information and documentation — Trusted third party repository for digital records

## National foreword

This Published Document is the UK implementation of ISO/TR 17068:2012.

The UK participation in its preparation was entrusted to Technical Committee IDT/2/17, Archives/records management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 74392 4

ICS 01.140.20

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2013.

**Amendments issued since publication**

| Date | Text affected |
|---|---|

PD ISO/TR 17068:2012

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.

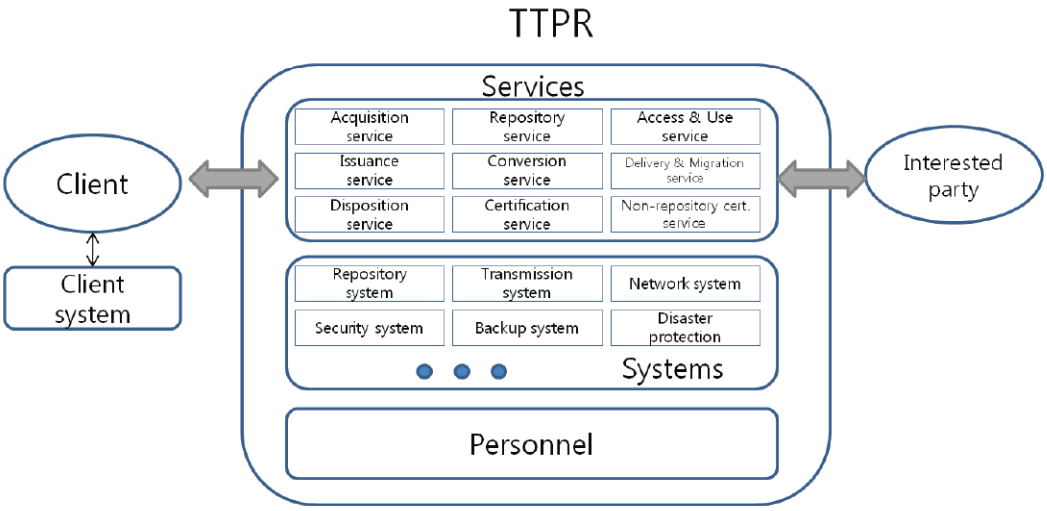

**Figure 1 — TTPR Overview**

### 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).

#### 4.2.3.3 Transmission procedure and method

Agreement on the procedure and method for acquisition and transmission of digital records between the TTPR and the client should be settled. The following should be consented to regarding the transmission procedure and method:

- Decide on an online or offline method;
- Decide whether the record will be saved in the TTPR whenever a nonrecurring record such as transaction takes place, or whether to save certain quantities of data as a batch;
- Decide whether an encrypted transmission channel will be used; and
- Decide which reliable transmission method (e.g. At Least Once delivery, At Most Once delivery, Exactly Once delivery and In Order delivery) will be used.

#### 4.2.3.4 Types of repository service

The TTPR should clarify the type and characteristics of each of its services to clients in a manner that the client can clearly understand. Types and characteristics of TTPR services are as follows:

— *Simple repository service:*

> The TTPR provides repository services for the digital records of the client during the period of time specified in the agreement. However, no evidential document is provided for the records. Unless there is an extension, the consigned digital records are disposed of in a manner preventing their physical recovery.

— *Delivery and migration service:*

> When a client requests the delivery and migration of the consigned digital records, the TTPR acts as a mediator transmitting the records to a TTPR or another assigned client. When the client only uses the delivery and migration service but not the repository service, and wishes to migrate the digital records to a certain party, the TTPR migrates the digital records to the second party through a series of processes and disposes of the digital records afterwards.

— *Repository and certification service:*

> The TTPR provides a repository service for the digital records of the client during the period of time specified in the SLA. Based on the stored record, it is possible for the TTPR to authenticate whether it is original, check the result for authenticity and integrity, and certify that the authenticated copy has been issued. Unless there is an extension, the consigned digital record is disposed of in a manner preventing its physical recovery.

— *Non-repository certification service (Remote Certification Service):*

> The TTPR only stores the metadata trail of the digital record by hashing, without storing the original digital record in the TTPR's repository. Using the stored metadata trail, the TTPR remotely determines the authenticity and integrity status of the digital record.

#### 4.2.3.5 Security and data protection

To secure the system integrity and protect the digital record and relevant data, the following security provisions should be established and conformed to:

- protect against unauthorized access to the digital record and its metadata;
- validate data and information in the digital record;
- encrypt the transmission channel;

— maintain a backup copy to replace a digital record when there has been data loss or error;

— retain and dispose of a digital record for which the retention period and disposition requirements specified in the contract with the consigner have been satisfied, and documentation of conformance to such requirements and any relevant disposition schedule;

— develop a business continuity plan for digital records and relevant records, including production of off-site copies of records, operating system (OS) and application programs; and

— maintain security for all transmission and receipt procedures.

Access levels to the TTPR and usage procedures for internal records of the TTPR should be documented in detail in accordance with the security policy. Access guidelines, change of authorized personnel, notification of unauthorized access and records of countermeasures to such access should be included.

To improve security and ensure integrity, encryption and a digital signature should be applied to the digital record stored in the TTPR. Also, the TTPR should establish procedures and technology for encryption and authorization management.

#### 4.2.3.6 Information provision

The TTPR and the client should specify the information and type of certification documentation to be provided during the period stated in the service agreement to provide and receive the service.

#### 4.2.3.7 Compensation

Means of compensation for loss, calculation of compensation amount, scope of compensation, etc. should be agreed upon in order to prepare for any damage to the client due to service suspension of the TTPR or loss of the stored digital record due to unexpected disaster, human error or a service quality problem.

## 4.3 TTPR services

### 4.3.1 Acquisition service

This is a mandatory service in order for a TTPR to receive an information package including digital records from a client. The TTPR should register the received records in repository storage after verifying the whole information package. Requirements for providing the acquisition service are as follows:

— a client who is willing to store digital records in the TTPR should be authorized as a member of the TTPR;

— the client system should be able to package the digital record as a TSIP in preparation for transmitting the record to the TTPR;

— the authenticity of digital records to be stored in the TTPR should be verifiable, using creator’s digital signature and timestamp of creation;

— the TTPR should inspect the consigned digital record during the acquisition, on normal registration, in the event of registration failure, virus infection and/or errors.

The TTPR’s acquisition service should maintain service quality as follows:

— integrity should be maintained by receiving a digital record bundle as a TSIP;

— the process of packing the digital record in the form of a TSIP in the client system should be processed within an acceptable time. In the event of a problem, the TTPR should notify the client with the cause and solution; and

— the following requirements should be complied with in order to maintain security during the transmission and receipt of digital records between the TTPR and the client:

  — use a reliable transmission protocol with a transmission and receipt check function;

  — process only using a secure transmission method;

  — process confidentiality and integrity requirements for the transmitted and received digital record; and

  — perform denial protection for the transmitted and received digital record.

The procedures of the TTPR's acquisition service are as follows:

a) Discuss and establish an acquisition plan with the TTPR for digital records to be stored by the client in the TTPR. The acquisition plan should include the acquisition date, the selection of digital records, the acquisition method (online or offline), and the type of digital record.

b) The client selects the digital records and ensures that they use one of the agreed file formats (if not, the client implements a file conversion procedure).

c) The selected digital records are converted into a TSIP and transmitted to the TTPR.

d) The TTPR verifies the following prior to moving the TSIP to a digital record repository:

  — whether the digital record in the TSIP has been successfully converted;

  — whether the digital record is infected by virus or has an error; and

  — whether the format of TSIP is compliant.

e) After the acquisition of the digital records is complete, documentation of the received data should be completed by the TTPR.

f) Upon the client's request, the TTPR should issue the acquisition certificate and add it to the certificate issuance list.

g) The client receives and confirms the certificate issued by the TTPR and provided that there is no problem with the certificate, stores it by selecting an appropriate storage method.

### 4.3.2 Repository service

This is a mandatory service for the TTPR to store the digital records consigned by the client. Requirements for providing the service are as follows:

— the TTPR should have in place a process and system for the stable management of the digital record; and

— a TAIP should be produced at the point when the digital record is registered at the TTPR system, and the system should manage the TAIP with a unique identifier assigned.

The TTPR's repository service should maintain service quality as follows:

— the TTPR should create an audit trail for the completed management tasks, which will be used to prove the authenticity and integrity of the stored record;

— the TTPR should prevent loss of the digital record due to disaster, system failure, etc.

The procedures of the TTPR's repository service are as follows:

a) The TTPR should verify the following when the client requests registration of the digital record:

  — check the client's registration authority;

  — check whether the digital record is included in the TSIP; and

  - check whether the format for the TAIP is correct.

b) The TTPR should store the digital record in a TAIP, after the completion of verification of the registration request of the client.

c) After the completion of registration of the digital record, the TTPR should issue a registration certificate to the client upon the client's request, and add it to the certificate issuance list.

d) The client receives and confirms the certificate issued by the TTPR and provided there is no problem with the certificate, stores it by selecting an appropriate storage method.

### 4.3.3 Access and use of service

This is a mandatory service to enable a client to access and search the consigned digital record. Requirements for providing the service are as follows:

- The TTPR should establish principles for the authority to access, any conditions and restrictions regarding the stored digital record, and provide the client with various search tools using metadata and classification systems.
- Browsing of access-restricted digital records should be possible using appropriate access controls or by special request.
- Access restriction can be applied during specified periods of time.
- Technical measures to prevent illegal copying, leaks, falsification, etc., should be taken when allowing browsing on a computer.

The TTPR's access/use service should maintain service quality as follows:

- Browsing or searching of the digital record by the client should be allowed within the specified periods of time.
- Browsing or searching of the digital record should be allowed subject to the agreed and authorized access authority.
- The storage and browsing/issuing service should always be available for the client to use, subject to any specific access timing agreements.

The procedures of the TTPR's access/use service are as follows:

- The client should be allowed to use and search the digital record in the TTPR, using the agreed search tools.
- The TTPR should verify the following prior to fulfilling the browse request of the client:
  - check the client's access authority; and
  - check whether the browse function is supported for the file type requested by the client.
- Forgery and falsification of the digital records through actions such as amend or copy should be prevented when the client browses the digital record.
- If the client is unable to browse a particular digital record, the TTPR should assist the client in determining the cause of failure and should recommend a solution.

### 4.3.4 Issuance service

This is a mandatory service for the TTPR to issue the digital record consigned by the client. Requirements for providing the service are as follows:

— the TTPR should issue digital records only to the client with issuance authority for the stored records; and

— the TTPR should issue authentic digital records and should document the issuance of the records.

The TTPR's issuance service should maintain service quality as follows:

— issuance of the digital record to the client should be allowed within the specified periods of time; and

— the TTPR should always be ready for the client to use the issuance service.

The TTPR should provide the service when the client requests the issuance of the stored digital record. The procedures are as follows:

a) The TTPR should issue the digital record with an authenticity certificate when the issuance of a digital record is requested by the client.

b) The TTPR should verify the following prior to fulfilling an issuance request for a digital record by the client:

   — Check the client's authority; and

   — Check whether the client is the recipient of the requested digital record.

c) The TTPR should issue the digital record to the client in a Trusted Dissemination Information Package (TDIP).

d) The TTPR should issue an authenticity certificate to the client and add it to the certificate issuance list after providing the digital record.

e) The client receives and confirms the certificate issued by the TTPR and provided there is no problem with the certificate, stores it by selecting an appropriate storage method.

### 4.3.5 Conversion service

This is an optional service provided by a TTPR to convert the format of the digital record consigned by the client for long-term storage purposes. Requirements for providing the service are as follows:

— the TTPR should only provide a conversion service to the client who has demonstrable authority to request conversion of the digital record;

— the TTPR should notify clients about which digital record file types are available from the conversion service; and

— the TTPR should not allow alteration of the digital record during the conversion process, and the client should be able to browse the converted digital record upon request.

The TTPR's conversion service should maintain service quality as follows:

— the conversion service should be performed within a specified period of time; and

— digital records should not be altered during the conversion process.

The procedures of the TTPR's conversion service are as follows:

a) The client requests the digital records conversion.

b) The TTPR should verify the following upon a request by the client for the digital record's conversion:

— Check the client’s authority; and

— Check whether the digital record is convertible.

c) Convert the digital record.

d) The TTPR should save the converted digital record in a TSIP format.

e) The TTPR should document and save the metadata about the conversion process, and any changes to the record’s metadata, e.g. format, time, log.

f) After completing the conversion of the digital record, issue a non-alteration certificate upon the client’s request and add it to the certificate issuance list.

g) The client receives and confirms the non-alteration certificate issued by the TTPR, and, provided that there is no problem with the certificate, stores it by selecting an appropriate storage method.

#### 4.3.6 Delivery and migration service

This is an optional service which could be provided by the TTPR according to the client’s requirement to migrate the stored digital record to another TTPR or other nominated party. Requirements for providing the delivery and migration service are as follows:

- the client who requests the delivery and migration service of the digital records should identify a recipient;
- when the digital record is received for the purpose of providing the delivery and migration service, the TTPR should store the received digital record, then convert it to the TTPR’s issuance format and transmit the digital record to the recipient in a timely manner;
- the clients who transmits and receives the digital record should become a member of the TTPR in advance;
- the TTPR and the parties involved in the transaction should have systems installed with the module for delivery and migration.

The TTPR’s delivery and migration service should maintain service quality as follows:

- The completion of the delivery and migration service should be undertaken within the specified period of time after the delivery and migration request has been received by the TTPR.
- The delivery and migration scope should be checked to confirm that the requested digital records have been delivered and migrated. The TTPR should issue the certificate for the delivery and migration. When digital records outside the requested scope have been delivered and/or migrated, the TTPR should determine the cause and notify it to the client.
- When migrating the digital records stored in the TTPR to another TTPR, the relevant digital record should be completely transmitted.
- The following requirements should be complied with in order to maintain security during the transmission and receipt of a digital record between the TTPR and the client:
  - use a reliable transmission protocol with a transmission and receipt check function;
  - process only using a secure transmission method;
  - process confidentiality and integrity for both the transmitted and the received digital record, and
  - perform denial protection for both the transmitted and the received digital record.

The procedures of the TTPR's delivery and migration service are as follows:

a) When the client changes their TTPR or the digital record is to be migrated to another TTPR, the TTPR should move the information relevant to the digital record and issue a delivery and migration certificate.

b) The TTPR should verify the following upon receiving a request for digital record delivery and migration:

— Check the client's delivery and migration authority; and

— Check whether it is possible to move the record to the recipient TTPR.

c) Delivery and migration of the digital record should be performed using an online or offline method.

d) The TTPR should save the metadata for the delivery and migration, e.g. format, time, and log etc.

e) The recipient TTPR should receive the digital record and register and store the record. Then, the registration certificate is provided upon the client's request, and added to the certificate issuance list.

f) The client confirms the delivery and migration certificate and registration certificate from the migration and recipient TTPR, and provided that there is no problem with the certificate, stores it by selecting an appropriate storage method.

g) The TTPR should self-migrate in accordance with the following, upon the client's request for self-migration:

- move the digital record to a different storage media or platform, and discard the digital record in the original storage media, so that it cannot physically be recovered; and
- after the self-migration of the digital record, the TTPR provides a non-alteration certificate to the client and adds it to the certificate issuance list.

### 4.3.7 Disposal service

This is a mandatory service for a TTPR to dispose the digital record stored in the TTPR. Requirements for providing the disposal service are as follows:

- The digital record is disposed of when the retention period expires or upon the client's request regardless of the expiration date.
- The digital record for which disposal has been approved should be disposed of in a manner preventing its physical recovery; disposal is only to be performed on the authority of a senior TTPR employee.
- Documentation of the disposal process should be made, in case it is necessary after the disposal to prove the legitimacy of the disposal and to confirm the disposal of the digital record. At a minimum, metadata such as when and by whom the disposition was reviewed and the record was disposed should be produced and maintained for future needs.

The TTPR's disposal service should maintain service quality as follows:

- Disposal should be completed within the specified period of time, upon the client's request to the TTPR for disposal.
- In the event of failure during processing the digital record which is being disposed, all relevant data should be disposed of in accordance with the transaction process.
- No record related to the disposed digital record should be left, other than the certificate of disposal.
- To maintain security and reliability, disposal should only be performed on the authority of a senior TTPR employee.

The procedures of a TTPR's disposal service are as follows:

a) The TTPR checks the following, upon receiving the client's request for disposal of a digital record:

— the client’s authority; and

— the previously nominated retention period of the digital record.

b) If the retention period of the digital record is decided by the client, the TTPR should notify the client of the expiration of the retention period one month prior to the expiration date.

c) A digital record may be disposed of upon the client’s request, regardless of the retention period.

d) The TTPR should dispose of the digital record in accordance with the following, upon the client’s request for disposal:

— destroy the digital record so that it cannot be physically recovered;

— after the disposal of the digital record, issue a disposal certificate to the client; and

— add the disposal information to the certificate issuance list.

e) The TTPR should allow for the extension of the retention period, if requested by the client.

f) The client confirms the disposition certificate or non-alteration certificate issued by the TTPR, and provided that there is no problem with the certificate, stores it by selecting an appropriate storage method.

#### 4.3.8 TTPR certification service

This is a mandatory service for the TTPR to issue certificates for the stored digital record. Requirements for providing the certification/confirmation service are as follows:

— The TTPR should be able to produce an authentic copy of the digital record upon the client’s request.

— The TTPR should establish a procedure for issuing an authentic copy by confirming the authenticity and by producing the copy requested.

— The TTPR should issue a certificate proving the authenticity of the digital record copy, be responsible for documentation of the issuance and provide a function confirming the issuance itself and verifying the integrity.

— The TTPR should provide a function to verify format, expiration date, disposition issue, digital signature and signature certificate of the issued authentic copy and certification document.

The TTPR’s certification service should maintain service quality as follows:

— The TTPR should be able to issue a certification document within the specified period of time, upon the client’s request.

— Documentation for issuance of all the certification documents should be made to ensure the reliability of the issued certificate.

— The client should always be able to receive certificates from the TTPR, upon request.

— To maintain security during the transmission and receipt of the certificate between the TTPR and the client, the following should be conformed to:

— use a reliable transmission protocol with a transmission and receipt check function;

— process only using a secure transmission method;

— process confidentiality and integrity for transmitted and received certificate; and

— perform denial protection for transmitted and received certificate.

The procedures of a TTPR's certification service are as follows:

- The TTPR provides certification documents as follows:
  - issue a registration certification document to prove the registration and deposit of the digital record requested by the client, in the TTPR;
  - issue an issuance certification document to prove the issuance of a digital record with an authenticity certificate to the client;
  - issue a delivery and migration certification document to prove the transmission of the digital record to another TTPR;
  - issue a disposition certification document to prove the complete disposition of the digital record requested by the client;
  - issue a non-alteration certification document to prove that the content of the digital record has not been modified after the change of file type or storage media;
  - issue an authenticity certification to prove that the digital record issued to the client is identical to the authentic digital record stored in the TTPR;
  - when it is required to issue a new type of certification document during the process of providing the digital record management service, the TTPR may define the function, purpose and format for usage.
- The TTPR should include the following information in the certification document:
  - name of the certification document requestor (for organizations, the name of the company);
  - unique identifiers of the certification document requestor (for organizations, the business licence number);
  - serial number of the certification document;
  - time and date of request for the certification document;
  - expiration date of the certification document;
  - purpose of the certification document;
  - information showing the TTPR, e.g. title of the TTPR.
- The TTPR should produce the certification document as follows:
  - produce certificates based on a standardized certificate format;
  - record time information from the TTPR's system on the certification document;
  - produce a security report demonstrating the integrity of the digital record and attach it to the certification document;
  - attach the TTPR's digital signature.
- Issuance of the certification document of the digital record should proceed as follows:
  - check the client's certification document request authority;
  - issue an electronic certification document based on a standardized certificate format.
- The TTPR should retain the list of issued certificates/confirmation documents and record the following certification document list information:
  - serial number of the certification document;

- issued date and time of the certification document;
- expiration date of the certification document;
- purpose of the certification document;
- other necessary information.

### 4.3.9 Non-repository certification service (Remote Certification Service)

This is a service, which could be optionally provided for client convenience, by which a TTPR can remotely certify a digital record not stored in the TTPR by only storing information about the digital record (for example, its hash tag). Requirements for providing the non-repository service are as follows:

- The client who is willing to use the non-repository certification service should be a member of the TTPR.
- The TTPR should be able to extract the information for identifying the relevant digital record (such as the hash tag).
- The TTPR should be able to determine whether there has been forgery and/or falsification of a digital record by using the information about the digital record for comparison purposes. Furthermore, the certification for comparison should be issued to the client.
- Information about the digital record should be disposed of after the expiration of a specified period based on the service agreement.

The TTPR's non-repository certification service should maintain service quality as follows:

- Information about the extraction of the digital record which the client requests from the remote certification service should be processed within the specified period of time.
- A client should always be able to use the remote certification service.
- The process by which remote certification service determines the forgery and/or falsification of a digital record should be completed within the specified period of time.
- Documentation for issuance of all certificates should be made for the reliability of the issued certificate.
- The following should be conformed to, in order to maintain the security during the transmission and receipt of a digital record between the TTPR and the client:
  - to use a reliable transmission protocol with a transmission and receipt check function;
  - to process only using secure transmission methods;
  - to process confidentiality and integrity information about the digital record; and
  - to perform denial protection for the information about the digital record.

The procedures of a TTPR's non-repository service are as follows:

- The client transmits the digital record to the TTPR that will be used for non-repository certification service.
- The TTPR extracts the information (such as the hash tag) for the received digital record, and then discards the digital record.
- The TTPR provides remote certification using the information about the digital record as follows:
  - issue a registration certificate to prove the storage of the digital record's information requested by the client;

- issue an authenticity certificate to prove that the information about the digital record stored in the TTPR and the digital record requested for comparison are identical;
- issue a certificate to prove that the digital record certified by the TTPR and the digital record requested for comparison is not forged and/or falsified; and
- issue a disposition certificate to prove the complete disposition of the information stored about the digital record as requested by the client.

The TTPR should include the following information in the certificate:

- name of the certificate requestor (for organizations, the name of the company);
- unique identifiers of the certificate requestor (for organizations, the business licence number);
- serial number of the certificate;
- time and date of request for the certificate;
- expiration date of the certificate;
- purpose of the certificate; and
- information identifying the TTPR, e.g. the title of the TTPR.

## 5 System requirements

### 5.1 General

To maintain reliable and useful TTPR services, it is necessary to establish software and hardware systems which are secure and reliable. The system should protect managed digital records in the event of any disaster, such as earthquake, fire or intrusion by an unauthorized person, etc. As the TTPR is exposed on public networks, it should employ a security system to defend against any threats to the TTPR. This chapter presents the types and requirements of TTPR systems that should be considered from the time of establishment.

### 5.2 Digital record repository system

The digital record repository system of a TTPR should be equipped with the following functions:

- registration, browsing and searching of the digital records;
- issuance of certificates and digital records;
- migration and receipt of the digital record;
- conversion of the digital record;
- integrity check of the digital record; and
- termination and disposition of the digital record.

### 5.3 Transmitter-receiver system

The TTPR's transmitter-receiver system should satisfy the following functions to transmit or receive messages, including the digital record:

- function to transmit and receive the messages according to the standardized procedure and method;
- function to process confidentiality and integrity for the transmitted or received message;

- function to ensure transmission security;
- function to check the transmission or receipt of the sent or received message; and
- denial protection functions for transmitted or received message.

## 5.4 Network system

The TTPR's network system should satisfy the following functions for the connection between the client system and the TTPR and between TTPRs:

- function to create and distribute the digital record;
- function supporting the use of the service, such as the management of digital records from an outside system; and
- function supporting check of the process result within the repository from the outside system.

## 5.5 Time-stamping system

The TTPR should be equipped with a system that records and manages the date and time of transmission. Such equipment should perform the following functions:

- function enabling time transmitter to send the time from the time source;
- function to inform the administrator when time transmitter has an error;
- function to provide the exact date and time over a full 24 h period when time transmission from time source has been completed;
- function that corrects the time of the time-stamping system using the time from the time transmitter;
- function that initiates the time-stamping function after the exact correction of the time for the time-stamping system;
- function that provides a continuous time correction function;
- function that automatically ceases the time-stamping service, immediately after there has been a failure of the time correction function and the error message has been output;
- function that checks whether the time recorded on the time checking token received by the client matches the issuance time; and
- function that provides the time-stamping service using the digital signature.

## 5.6 Trail management system

The TTPR should create and retain an audit record for the following information related to services such as the digital record repository, through system managing the audit record, which should include:

- registration history of the digital record;
- issuance history of the digital record;
- repository migration history of the digital record;
- disposition, self-migration and recovery histories of the digital record;
- conversion history of the digital record;
- transmission and receipt histories of the digital record; and
- certificate issuance history of the digital record.

## 5.7 Security system of network system

The TTPR's network system security system should provide the following in order to realize network security:

- function to provide consistent services, such as digital record repository, in the event that one of the transmission systems fails;
- dual intrusion protection systems and access control protocols required for services such as digital record repository; and
- real-time system or equipment with access control function, which checks the network status and records and maintains the access histories created from the network system.

## 5.8 Access control equipment

The TTPR should be equipped with access control equipment that satisfies the following requirements, to control access to the system operation room:

- physical access control function that restricts access by unauthorized persons to the repository system;
- audit record function for information such as serial number, type of incident and whether system has succeeded or failed, and if it has failed, the cause of failure, access date and time and information on intruder;
- access control function with biometric based identification function such as fingerprint or iris recognition and possession based identification function such as key or card combined together;
- safe access to the operation room during power outage should be ensured;
- implementation of access controls based on the role of the administrator, at operation system level;
- implementation of program or process appropriate for the goal of system operation; and
- creation and retention of audit record for the information of repository system operation.

## 5.9 Disaster protection facility

The TTPR should provide business continuity and disaster prevention processes in line with industry best practice for the operation of the TTPR.

## 5.10 System for certificate issuance and validation of digital record

The TTPR should be equipped with a certificate issuance and validation system satisfying the following functions for creation/issuance of certificates:

- the function to create the unique identifier of the certificate;
- the function to create the security value assuring the integrity of the digital record;
- the function to attach the digital signature of the repository to prove the identity of the issuing TTPR;
- the function to attach the correct time, transmitted from the time-stamp system;
- the function to create the certificate according to a standardized format; and
- the encryption function to ensure the confidentiality of specific information in the certificate.

The TTPR's certificate system should have the following to set the certificate creation policy:

- the expiration date of the certificate,

- the applicable scope or purpose of use of the certificate, and
- the extension field of the certificate.

The TTPR's certificate validation and issuance system should have a function to allow the issuance of certificates for the following:

- the registration certificate to prove the registration of the digital record by the client;
- the migration certificate to prove the migration of the digital record to another repository;
- the disposition certificate to prove the disposal of the digital record;
- the non-alteration certificate to prove that the content of the digital record has not been modified after a change of file type or storage media;
- the authenticity certificate to prove that the issued digital record is identical to the authentic digital record stored in the repository; and
- any additional type of certificate required during the performance of the services, such as the digital record repository.

The TTPR's certificate service should have functions that allow enquiry on the following items:

- The applicant's information: The certificate should include personal identification and status.
- The certificate information: Verifiable information related to certifying the validity of the certificate, such as time and date of request for issuance, time and date of issuance, information on the record being issued, type and purpose of the certificate and the expiration date.
- Information of issuing TTPR: Information confirming the identity of the issuing TTPR.
- Any other information related to legal effect, validation, etc. of the certificate.

The TTPR's certificate system should have the following functions to validate the certificate:

- the function of validating the certificate according to a standardized certificate format;
- the function of validating through validation route written on the certificate;
- the function of validating by checking the certificate issuance list of the repository;
- the function of validating the integrity of the certificate by checking the digital signature, security value, etc. written on the certificate; and
- the function of notifying the client when the validation on the certificate has failed.

The TTPR's certificate system should have the following functions for audit on the certificate:

- maintenance of the information related to the created/issued certificate for a limited time period after the extinction date of the certificate;
- the function of creating and maintaining the audit record on the details of certificate issuance and backup function for the audit record;
- the protection from the threat of forgery/falsification and deletion of audit record;
- the protection from the illegal use of certificate creation/issuance software; and
- the role classification and access control function of the policy administrator, operation administrator and audit administrator. When there is any other administrator role assigned, role classification and access control function should be provided.

### 5.11 Backup system

The TTPR's backup system should have the following functions:

- a separate function enabling the backup system to protect digital records in the repository, and to ensure their stable retention;
- a function that allows complete backup of the record in the system;
- a function that allows the backup of the database that will be applied to the repository, under nonstop status;
- a function that allows backup for different types of platform such as Linux, Unix, Windows, etc.;
- a function that allows backup of digital records, databases and other management information used by the TTPR for management and access purposes; and
- a function preventing the forgery and falsification of backup data.

### 5.12 Remote repository system

The TTPR's remote repository system should have the following functions:

- a remote repository system operating at a distance which maintains the digital record, certificate and management information of the repository;
- physical access control device and locking system for the remote repository system, such as security cabinet;
- audit recording and maintaining the access details of the remote repository system;
- backup function for digital records, databases and other management information according to the backup cycle proposed in the working principles; and
- intrusion surveillance device for the remote repository system.

## 6 Management requirements

### 6.1 General

The following management requirements should be satisfied for the stable and reliable operation of a TTPR.

### 6.2 Client management

The following should be managed for client information registration:

- client's identification and authentication processes needs to be available when the client is registered;
- client's registration date, name, certification, etc. should be entered accurately; and
- client's information should be deleted only when no longer needed for legitimate purposes.

The following should be managed for client's authority management and control:

- provide a client's authority management function;
- if the authority given to the client is deleted or changed arbitrarily, no error should occur when managing the information or relevant document of the client to whom the authority was given;
- when the TTPR administrator performs management of the client's authority, the basis of the client's request should be retained;

— the TTPR service should be provided or controlled based on the client's authority; and

— a client's authority management history and histories of requests for and responses to each service should be recorded in the audit record.

## 6.3 Administrator's role and authority management

The roles and authority of the TTPR administrator should be managed as follows:

— roles of all TTPR administrators are defined, and access to TTPR data are controlled based on the role;

— each administrator should be assigned a role, and collected history should be maintained and managed;

— access to records of unauthorized activities should be restricted to authorized personnel; and

— all processes including activities performed by the administrator and records of unauthorized activities should be recorded in the audit record.

The following should be managed for access control at the operation system level:

— when an unauthorized administrator attempts to access a system, access authority will not be given by the operating system of the system; and

— all access histories should be recorded in the log, etc., including illegal access by an administrator.

Illegal use of certification creation/issuance software should be handled as follows:

— access should be controlled so that only the administrator with proper authority will have access to the certification creation/issuance software;

— when blocking the access, warning message should be displayed simultaneously;

— the complete access history should be recorded in the log, including the illegal access by an administrator; and

— if the certification creation/issuance software's structure consists of server and client, confirm the access control function on both sides.

## 6.4 Network and security management

The network equipment and network security system should be managed as follows:

— identification checks should be performed on individuals or other systems seeking access to stored digital records or system functions, particularly the function to control access to the network facilities, such as network switches and routers;

— identification checks should be performed on individuals or other systems seeking access to system functions controlling access to the network security systems, such as intrusion blocking system and an intrusion detection system; and

— history of access to the network equipment and network security system should be recorded in the audit record or log.

Authority control for the management system of the operation room security system should be managed as follows:

— access to the security system management system, such as access control system management system, intrusion detection system, surveillance camera management system, etc. should be controlled;

— access password of security system management system should be protected;

- password protection system should not show the typed password when logging in, and should have an encryption function to safely protect the password saved in the system; and
- access history of the administrator to the security system management system should be recorded in the audit record or log.

### 6.5 Digital record management

Management of registration confirmation and notification should be performed as follows:

- after the client registers the digital record, a process result message should be sent to report the normal registration of the record;
- when the registration of the digital record fails, an error message should be sent to report the failure;
- if the error is due to the client's system, the specific cause should be included in the error message;
- if the error is due to the TTPR, the error message should specify that it is the TTPR's error; and
- registration and registration failure histories of the digital record should be recorded in the audit record.

Virus/error inspection and notification functions should be managed as follows:

- the TTPR should determine whether the transmitted digital record is infected by a virus or other malicious software, and notify the client of the result if an infection is detected;
- the TTPR should determine whether there is any error in the Trusted Submission Information Package (TSIP), and notify the client of the result if any error is detected; and
- infection and/or error inspection histories should be recorded in the audit record.

The validation function of the TSIP format regarding client's digital records should be performed as follows:

- the client should be able to select or enter the format of TSIP when registering the record; and
- the client's TSIP should be validated, and errors reported in the event of failure.

The following should be managed for searching using the digital record's metadata items:

- provide a search function using digital record's metadata items;
- digital record search from the client's system is allowed only for records with authorization; and
- digital record search by the administrator is allowed for all digital records. However, this is only for the purpose of digital record management, and access (browsing and issuance) to the digital record is not allowed.

The following should be managed for converting the record to a type supported by the TTPR that allows the browsing or long-term storage of a digital record without alteration of the record:

- the TTPR should have a policy for conversion file type, and should specify the policy in the terms and conditions for the client to acknowledge;
- the TTPR should propose a policy for the browsing support service in case of exceptional file types, where software not normally available on the TTPR systems is required for record rendition;
- the TTPR should be able to convert the registered authentic digital record to the file type specified in the policy.

The function to issue the digital record based on the client's request should satisfy the following requirements:

- issue the record in the file format requested by the client; and

- issuance history of the original digital record and the converted version should be recorded in the audit record.

When a digital record is issued, the forgery/falsification protection function should satisfy the following requirements:

- when Trusted Dissemination Information Package (TDIP) is created, the integrity of the digital record and property included in the TAIP should be verified;
- this function is provided separately from the integrity check function provided by the storage media; and
- integrity verification history should be recorded in the audit record.

The function to issue the digital record and its authenticity certificate to the designated individual or organization should satisfy the following requirements:

- when a digital record issuance function is implemented using the registration certificate, digital record and authenticity certificate may be issued to the individual / organization to which the client of the digital record repository has entrusted the issuance request authority;
- when the digital record is issued to a third party, the digital record and an authenticity certificate may be issued to the party who is assigned to be the recipient of the digital record; and
- the TTPR should provide the validity verification function for the certificate of the digital record recipient, or specify in the client's terms and conditions that the client needs to attach valid certification.

When the retention period for the digital record is fixed, the function to notify the client prior to the expiration date should satisfy the following requirements:

- notify the client prior to the expiration of digital record's destruction date;
- notify the administrator, when there has been failure to notify due to any reason;
- record the notification and failure histories of the digital record retention period in the audit record; and
- if the expiry notification fails, detailed background including cause of failure should be recorded in the audit record.

The function to self-migrate the digital record to other storage media or platforms should satisfy the following requirements;

- self-migration to other storage medium or platforms supporting storing function should be possible; and
- self-migration history of the digital record should be recorded in the audit record.

The function to recover the digital record migrated to other storage medium or platforms should satisfy the following requirements:

- recovery of the digital record migrated to another storage medium or platforms to operating storage media is possible;
- the method of self-migration may be the same as that for backup. However, the function should be implemented separately from the backup function, and also be distinguished in the audit record;
- digital record recovery history should be recorded in the audit record; and
- if self-migration fails, detailed background including cause of failure, etc. should be recorded in the audit record.

The digital record disposition function should satisfy the following requirements:

- dispose of the digital record upon the client's request;
- the disposition response message of the digital record includes the TDIP along with the digital record;
- dispose of the digital record internally, when the retention period of the digital record has expired;
- upon completion of migration and receipt of the digital record, the migrated record should be disposed of immediately; and
- the disposition history of the digital record should be recorded in the audit record.

The function of creating and transferring the digital record information package (TDIP) should satisfy the following requirements:

- registration, retention and issuance of the digital record should conform to the determined processes;
- when security level of the digital record is set, the ability to issue the digital record should be confirmed through a check on the security level of the digital record and the client's authority;
- when the client requests the issuance of the digital record, the content of the record should be encrypted, and the record attached to the issued TDIP should be encrypted using the client's public key;
- individual files should be encrypted when the attached record is being encrypted; and
- unsuccessful and successful histories of the digital record's issuance based on the security level should be recorded in the audit record.

The function supporting and allowing confirmation of the result of the TTPR's internal process from the outside system should satisfy the following requirement:

- results of digital record acquisition, repository, migration, disposition, certification and non-repository certification processed in the TTPR need to be able to be checked from external systems.

## 6.6 Management of transmitted and received messages

The function to transmit and receive the messages via a standardized procedure and method based on the standard transmission and receipt protocol should satisfy the following requirements:

- Basic factors should be included in the transmitted and received messages:
  - for the digital record registration, the TSIP should be included in the request message and the initial registration certificate should be included in the response message;
  - for digital record issuance (when requested for encryption), the public key certificate should be included in the request message and the TDIP should be included in the response message;
  - for digital record issuance by a third person (if implemented), the recipient's email and public key certificate should be included in the request message;
  - for digital record issuance with certificate (if implemented), the certificate should be included in the request message and its dissemination should be included in the response message;
  - for the digital record disposition, the TDIP, i.e. original digital record, should be included in the request message;
  - for certificate issuance, the certificate requisition form should be included in the request message and the certificate should be included in the response message.
  - for the renewal of the certificate, the certificate should be included in the request message and the renewed certificate should be included in the response message.

The client certificate verification function should satisfy the following requirements:

— the client's certificate should be a standards-based public key certificate;

— when the client logs into the TTPR, it should be determined whether the owner of the certificate is a proper TTPR client, through the certificate and through verification on the log in certificate; and

— history of verification of the client's certificate should be recorded in the audit record.

The function to process the confidentiality and integrity of the transmitted and received messages should satisfy the following requirements:

— encrypt the message using a standardized encryption algorithm for communication with the client system, to secure the confidentiality of the transmitted and received messages (including client's information registration message); and

— apply hash and digital signature technology to standards-based transmission and receipt protocol to maintain the integrity of the transmitted and received messages (including the client's information registration message).

Denial protection function for the transmitted and received messages should satisfy the following requirements:

— request and response for each service should be performed for the denial protection of the transmitted and received messages; and

— the TTPR should store the transmitted and received messages, and a denial protection function that verifies the signature of the message should be realized, if necessary.

The function to check the transmission and receipt of the transmitted and received messages through message transmission and receipt history should satisfy the following requirements:

— transmission and receipt of the message should be checked by recording the identifier of transmitted and received messages, information for checking the receiver or transmitter (e.g. identifier), time of the message transmission and receipt and transmitted and received message, etc. in the audit record; and

— audit record for the TTPR's transmission message (response message) should be able to be checked at transmission system.

Confidentiality process function for the messages transmitted and received between the TTPR and a remote repository system should satisfy the following requirements:

— secure confidentiality of the messages transmitted and received between the TTPR and the remote repository system online;

— recommend standard protocols for confidentiality protection, and all encryption sessions to be based on mutual authentication between the client and server; and

— message encryption to use a standard algorithm.

## 6.7 Audit record management

Management of the audit record for handling forgery/falsification and threat of deletion should be performed as follows:

— forgery/falsification and deletion of each service history stored in the history management system should be prevented or detected;

— forgery/falsification and deletion of audit record or log created during the process of activities performed within the TTPR should be prevented or detected; and

- protection method through authorization control may be used as a supplementary means, but fundamental protection function using storing function or detection method using the TTPR digital signature needs to be applied.

## 6.8 Data backup and recovery management

Data backup and recovery function should satisfy the following requirements:

- data backup and recovery procedures, such as backup schedule and method, etc. should be specified in detail in the working principles and internal regulations, to prevent activities infringing integrity, such as data forgery/falsification, deletion, etc., or other disasters;
- backup equipment with proper function should be used to perform backup and recovery procedures;
- backup report for recording the backup activities should be managed;
- backup function satisfying the backup requirements should be provided;
- real-time backup should be performed in case of remote backup;
- recovery function satisfying the recovery requirements should be provided;
- time for emergency recovery should be within the mirror site standard; and
- histories of backups performed and recovery activities should be recorded in the audit record, log, etc.

The system management of a TTPR's storage should satisfy the following requirements:

- system management should ensure the integrity of the TTPR's stored data, by using the appropriate storage system;
- the system function to disable the deletion or modification of data during its retention period should be managed;
- the administrator of storage system should not be able to modify or delete the stored data during its retention period, which itself should be set when the data are stored,;
- access to storage equipment or system should be allowed only when authorized;
- any stored data should not be modified or deleted through improper activities caused from storage system;
- integrity of the stored data should be checked and observed regularly; and
- failure of integrity verification should be reported to the administrator.

Systems or facilities operated by backup servers in case of error in the TTPR server should satisfy the following requirements:

- back-up facilities should use redundant systems so that the backup server is activated for operation in the event of an error in the TTPR server;
- consistent service should be provided when one piece of the redundant equipment fails to operate; and
- redundant structure of each system refers to parallel composition of network flow.

Setting of access control rules required for services such as digital record storage, etc. and maintenance of the handling process should satisfy the following requirements:

- the function of setting the rule for controlling the rule for access to the TTPR through the network should be provided;

- access permission and restriction histories should be recorded in the audit record based on the TTPR’s regulation; and
- in the event of the creation, modification or deletion of the access control regulation, certain details, including by whom and when the activity was performed and the content of the performed activity, should be recorded in the audit record.

## 6.9 Security management

Infringement detection and notification functions should satisfy the following requirements:

- inspection and infringement detection on all traffic;
- detection and renewal of new infringement patterns continuously;
- the notification of an administrator when an infringement is detected; and
- histories of infringement detection by the infringement detection system and renewed infringement patterns recorded in the audit trail, in detail.

A separate operation room equipped with a backup system should satisfy the following requirements:

- access of unauthorized persons to the operation room to be physically restricted;
- access control equipment that audits or records information such as serial number, type of incident and whether access controls succeeded or failed, and in the event of failure, gives the cause of failure, access date and time and intruder;
- to provide an access control function with biometrics-based identification function such as fingerprint or iris recognition and possession-based identification function such as key, card, etc. combined together; and
- safe access to the operation room ensured during a power outage.

## 6.10 Migration and receipt management

The function of querying and checking the availability of transfer of a digital record to the recipient TTPR should satisfy the following requirements:

- proper migration and receipt procedures specified in the TTPR’s working principles or internal regulations;
- requirements for migration and receipt, i.e. inquiry and confirmation procedures for the availability of migration and receipt, identity of the digital records to be migrated, details of online and offline migration and receipt procedures, etc., included in the migration and receipt procedures; and
- migration and receipt processes in principle performed in a manner that minimizes any inconvenience or loss for the client.

The function to migrate and receive digital records between TTPRs should satisfy the following requirements:

- to provide digital record migration and receipt functions that interface with each other;
- to provide functions satisfying the security requirements of the TTPR and client;
- for online and offline request and response messages for migration and receipt, technical verification of TTPR certification and of the integrity of the messages should be performed through hash value and digital signature value, and a denial protection function should also be implemented;

- to ensure confidentiality for online and offline request and response messages for migration and receipt, a session encryption method should be used for online requests and an encryption method should be used for digital records migrated offline;
- confidentiality for an offline migration request message and an encryption function to the transmitted digital record;
- standard algorithms for message hashes;
- standard algorithms for digital signatures; and
- standard algorithms for encryption.

### 6.11 Client system management

The following should be performed for the management of digital record packages from the client system:

- TSIP creation and digital record registration function, TAIP issuance request function, and TSIP and TDIP retention function;
- to provide a function to view the contents of a digital record package;
- to provide a function to support digital record browsing;
- to provide a prevention function for change, copy, save, print screen, etc., if browsing the digital record (change, copy, save and print screen refers to conditions when browsing format is maintained); and
- to provide output and verification functions for the digital record package.

The certificate management function should satisfy the following requirements:

- to provide a request function for certificate issuance and certificate storage function;
- to provide a function for viewing the content of the certificate; and
- to provide a certificate's print and verification functions.

The public key certificate management function should satisfy the following requirements:

- to provide a safe management function by encrypting the client's private key;
- to provide an interface for public key certificate management;
- to use standard algorithms for encryption of private key; and
- to provide the TTPR's public key certificate verification function and management function for the validation data.

The client system management function should satisfy the following requirements:

- to provide access control function for the client system;
- to provide a version check, and a version management and update function for the client system;
- that the version information should include a client system version, an applicable version of this Technical Report and distributor's information, and should be presented in a manner that enables a visual check;
- to include an internet URL in the distributor's information containing the name of the distributor and the details of the client system and the distributor;
- when the client system is updated, a function to report the update to the client should be provided; and

— when the client system is updated, verification of client system's integrity and distributor's reliability should be performed.

# Bibliography

[1] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 13008:2012, *Information and documentation — Digital records conversion and migration process*

[4] ISO/TR 13028:2010, *Information and documentation — Implementation guidelines for digitization of records*

[5] ISO 14721:2012, *Space data and information transfer systems — Open archival information system (OAIS) — Reference model*

[6] ISO/TS 15000-2:2004, *Electronic business eXtensible Markup Language (ebXML) — Part 2: Message service specification (ebMS)*

[7] ISO 15489-1:2001, *Information and documentation — Records management — Part 1: General*

[8] ISO 15489-2:2001, *Information and documentation — Records management — Part 2: Guidelines*

[9] ISO/TR 15801:2009, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*

[10] ISO 16363:2012, *Space data and information transfer systems — Audit and certification of trustworthy digital repositories*

[11] ISO 16919, *Space data and information transfer systems — Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*[2)]

[12] ISO/TR 18492:2005, *Long-term preservation of electronic document-based information*

[13] ISO 20652:2006, *Space data and information transfer systems — Producer-archive interface — Methodology abstract standard*

[14] ISO 21188:2006, *Public key infrastructure for financial services — Practices and policy framework*

[15] ISO/IEC TR 14516:2002, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

[16] ISO/IEC 20000-1: 2011, Information technology — Service management — Part 1: Service management system requirements

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

[2)] To be published.

**ICS 01.140.20**

Price based on 32 pages

*This page deliberately left blank*

# British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

## About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

## Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

## Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

## Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

**PLUS** is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

## Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

## Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

## Useful Contacts:

**Customer Services**
**Tel:** +44 845 086 9001
**Email (orders):** orders@bsigroup.com
**Email (enquiries):** cservices@bsigroup.com

**Subscriptions**
**Tel:** +44 845 086 9001
**Email:** subscriptions@bsigroup.com

**Knowledge Centre**
**Tel:** +44 20 8996 7004
**Email:** knowledgecentre@bsigroup.com

**Copyright & Licensing**
**Tel:** +44 20 8996 7070
**Email:** copyright@bsigroup.com

**BSI Group Headquarters**

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™