INTERNATIONAL STANDARD

ISO 17068

First edition
2017-10

Information and documentation — Trusted third party repository for digital records

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

Reference number
ISO 17068:2017(E)

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

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 46, *Information and documentation*, Subcommittee SC 11, *Archives/records management*.

Introduction

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

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

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

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

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

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

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

Information and documentation — Trusted third party repository for digital records

1 Scope

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

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note 2 to entry: See ISO 14721.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 Overview of a TTPR

4.1 Necessity for a TTPR

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

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

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

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

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

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

4.2 Requirements for TTPR trustworthiness

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

TTPR trustworthiness shall be achieved by meeting the high level requirements in terms of authenticity, reliability and integrity described in ISO 30300, ISO 30301, ISO 30302 and by following the requirements for electronic communications formulated by UNCITRAL. Moreover, TTPR trustworthiness extends to information packages described by the open archival information system suggested in ISO 14721 for the purpose of reliable custody.

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

- The **authenticity** of the client's digital records is accounted for in a business context, for example, the creators' place of business at time of creation of the record is retained. The TTPR shall check this.
    - The TTPR agrees with the client regarding the client's role and responsibility for authenticity during the service agreement period. When the TTPR checks the state of authenticity of the clients' records, the client is able to account for this. If a client can't account for the authenticity of its digital records, the TTPR is unable to classify those digital records as authentic.
    - The authenticity of digital records created by the client can be managed at the time of "freezing" the record by using authentication technology such as the timestamp, digital signature, etc. To manage this, the clients' digital records system can attach the timestamp to create records, sourced from the time stamping module provided by the TTPR. It can also attach the clients' digital signature to the digital records. Using this digital signature, digital records that have been falsified can be recognized.
- The **reliability** of digital records can be confirmed by verifying the custody of digital records. However, the TTPR specifies only where the custody is between the TTPR and its clients. The TTPR and the client shall check this.
    - A client transfers digital records to the TTPR as a package in the form of a trusted submission information package (hereinafter referred to as "TSIP").
    - The TTPR confirms the reliable custody of clients' digital records by validating received clients' TSIP regarding any change in the digital records and/or any transmission errors.
- The **integrity** of digital records shall be managed after creation for the period of retention. After verifying the authenticity and reliability requirements of transmitted digital records, the TTPR shall allow to verify the integrity for the period of retention by registering these records as a TAIP package.
- The **availability** of digital records shall be confirmed by TTPR's robustness with backup and recovery policy and system. TTPR shall provide adequate security and resilience for ensuring the availability of digital records.

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

4.3 TTPR components

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

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

Besides the TTPR and the client, there are other parties indirectly related to the quality assessment, for example, the inspector, auditor and 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 can be demonstrated as authentic. 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.

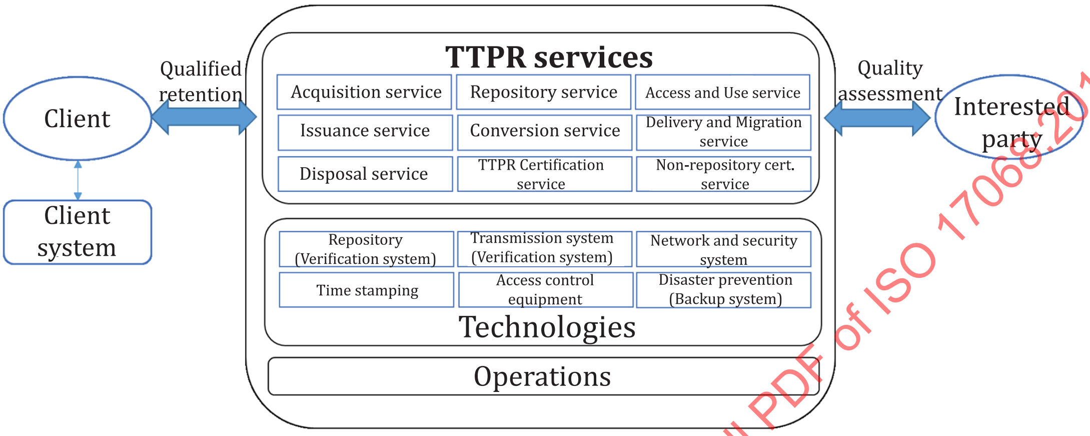

Figure 1 — TTPR overview

The technology 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, its verification system which automatically validates the metadata required for authenticity check during the acquisition stage, and the repository and its verification system for the retention and management of the digital record, are included in such technology. Also, the client’s system is necessary for the TTPR to establish a safe and reliable transmission channel and use a standardized transmission package.

The TTPR’s operations are performed by a TTPR expert, who understands the process of TTPR and is capable of coping with various situations. Operations cover software/hardware management to provide the TTPR services and preserves service quality and public relationship and clients’ requirements collection.

4.4 Characteristics of a TTPR

For a TTPR to be regarded as a reliable agent to clients, the TTPR shall have the capability of providing qualified service to safeguard the authenticity of the digital records, and maintain neutrality toward all parties. The TTPR requires three characteristics: stability, expertise and neutrality.

Stability: For trustworthy management of the stored digital records, a TTPR shall ensure stability; it has sufficient capital and human resources, a management strategy and execution capability. Furthermore, the TTPR is able to manage digital records normally, even in an emergency situation. To ensure this capacity, the TTPR has in place a disaster prevention and recovery system.

Expertise: A TTPR shall have expertise in coping with all the matters which cause risks in managing 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 trustworthy management is also based on such expertise. The TTPR employs experts and is equipped with specialized processes and systems to ensure its own expertise. Specialized procedures are established for activities related to digital record management, such as acquisition, archiving, delivery and/or migration and disposition of the digital record. The TTPR is equipped with a specialized system to provide functions related to digital record management, such as metadata processing, reliable messaging, security, digital signatures and time-stamps.

Neutrality: A TTPR shall maintain its neutrality toward all parties. A TTPR is only recognized within society if its neutrality is maintained. In addition, a TTPR satisfies the requirements in this document, and is independent in its performance of trustworthy digital record management, regardless of any external pressure; political institution, client organization and all the stakeholders.

5 TTPR services

5.1 General

This clause specifies the detailed requirements for qualified retention service.

5.2 Service procedure

TTPR service procedure shall be provided to the client as follows.

The client shall construct a system by adopting modules or specifications provided by the TTPR. Those functions are packaging digital records, where applicable attaching a digital signature and a timestamp token and transmitting the digital records. After constructing the client system, the client transmits digital records packaged in the form of a TSIP to the TTPR through the transmission channel at a specific time or at any time. 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 can request confirmation documents to demonstrate that the digital records have reached each stage of submission without problems.

A TTPR shall have a facility to transfer the digital records stored in the TTPR to other TTPRs, or to the client who owns the records. When the agreed retention period expires or the client requests the disposition of the records, the TTPR shall implement the agreed disposition process.

5.3 TTPR service agreements

5.3.1 Service level agreement (SLA)

A TTPR service shall be pre-described and agreed in order to clarify the liability between the client and the TTPR in the event of a dispute from alteration, forgery, leak, loss, etc. of digital records and quality, procedures, etc. of service.

A TTPR shall agree with a client to provide services to the client. The agreement specifies 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 agreement clearly states how the client needs to provide information to the TTPR to demonstrate the authenticity of digital records submitted by them. In cases where it is necessary to demonstrate the authenticity of the client's record, the agreement shall include the authenticity certificate in issuance service (refer to 5.4.4). It is required that the agreement includes a service level agreement (SLA) between a client and a TTPR. An SLA clarifies the quality factors and the levels of TTPR services agreed by the client and the TTPR. An SLA shall also describe the method and amount of compensation when the TTPR does not meet the service level agreed in the SLA. The agreement shall also fix the TTPR's authority or determine the limitation of the client's responsibility, and provide a reasonable solution for any case or incident which shall arise. The client's damages due to TTPR service problems shall be minimized through the SLA. The SLA may allow for the client to give a penalty or incentive to the TTPR based on the quality of the provided service quality.

5.3.2 Service agreement items

To use the TTPR service, clients (individuals or organizations) shall enter into a service agreement with the TTPR. The following shall be included in the service agreement:

- service fees;
- service period;
- the procedure for confirmation of digital record's authenticity;
- the procedure and method of TSIP(or TDIP) transmission;
- the scope of accountability and responsibility of the TTPR and the client;
- the method of security and data protection;
- the file type/format by which conversion shall be allowed;
- the type of service the client is required to use, e.g. an issuance service or a conversion service;
- the client's authority of access and use for consigned digital records;
- requirements for security related to consigned digital records;
- provision of necessary information by the client and the TTPR during the service period;
- requirements for insurance coverage in the event of compensation due to service or disaster;
- requirements for service quality and evaluation on the quality.

The client shall be able to cancel the service agreement in case of the fault due to a TTPR. In this case, the agreement item for cancellation shall include post service such as temporal retention, return, or disposal and the compensation related to the damage.

The client shall consent to the service agreement in order to use the TTPR service. The TTPR shall provide the service in compliance with the agreement to which the client has consented, and the client also shall conform to the service agreement and have the right to receive the service. The main items of an SLA are described below.

5.3.2.1 Service period

A TTPR is obliged to provide the service to the client in accordance with the agreement during the agreed period, and the client has the right to receive the service in accordance with the agreement during the period. The client shall specify the following regarding the service period:

- effective period of service agreement;
- period of renewals;
- period of reporting to the client;
- period of monitoring target services;
- retention period for each digital record;
- available period of optional non-repository certification service (refer to 5.4.9).

5.3.2.2 Transmission procedure and method

The transmission procedure and method of digital records shall be specified in the TTPR's acquisition service and agreed by the client. The following items shall be included in the agreement:

— transmission method, whether online or offline;

— transmission interval, whether a record is transmitted to the TTPR whenever it takes place, or transmitted at period;

— transmission security, whether an encrypted transmission channel is used, or what kind of encryption algorithm is used;

— protocol for reliable transmission, whether At Least Once delivery, At Most Once delivery, Exactly Once delivery and/or In Order delivery is used.

In case of any failure of transmission, records shall be retransmitted to assure that they are transmitted at least once, at most once, exactly once or in order.

5.3.2.3 Types of service

The agreement describes the types and characteristics of each of its services to clients in a manner that the client can clearly understand. In the agreement the client can select subscribing types of service as follows.

—	*Acquisition service type*:
	This service is to receive an information package including digital records from a client. The TTPR shall register the received records in its repository storage after verifying the validity of the whole information package.
—	*Access and use of service type*:
	This service is to enable a client to access and search the client's consigned digital records.
—	*Issuance service type*:
	This service is to issue the digital record consigned by the client.
—	*Conversion service type*:
	This service is to convert the format of the digital record consigned by the client in formats suitable for long-term storage purposes. This conversion service is optional according to the client's request.
—	*Simple retention service type*:
	The TTPR provides retention service for the digital records of the client during the time period specified in the agreement. However, no certificate is provided for the records. Unless there is a time extension, the consigned digital records can be returned in the TDIP package to the client and/or disposed of in a manner preventing their physical recovery.
—	*Delivery and/or migration service type*:
	When a client requests the delivery and/or migration of the consigned digital records, the TTPR acts as a mediator transmitting the records to another TTPR or another assigned client. When the client only uses the delivery and/or migration service but not the retention service, and wishes to migrate the digital records to a certain party's storage, the TTPR migrates the digital records to the second party's storage through a series of processes and disposes of the digital records afterwards.
—	*Retention and certification service type*:
	The TTPR provides a retention service for the digital records of the client during the time period specified in the SLA. Based on the stored record, it is possible for the TTPR to manage the authenticity of the record, 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 shall be disposed of in a manner preventing its physical recovery.

—	*Non-repository certification service (Remote certification service)type*:
	The TTPR only stores the metadata trail of the digital record by hashing which generates unique digital code, 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.
—	*Disposal service type*:
	This service is to dispose the digital record stored in the TTPR.

5.3.2.4 Security and data protection

To secure the system integrity and protect the digital record and relevant data from unauthorized access or data loss, the following security provisions shall be established and conformed to:

- protect against unauthorized access to the digital record and its metadata;
- validate the integrity of data and information in the digital record by digital signature;
- encrypt the data on the transmission channel;
- retain and dispose of a digital record regarding the retention and disposition requirements, relevant 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;
- ensure all security procedures are in compliance with the service agreement.

In accordance with above security provision, access levels to the TTPR and usage procedures for digital records in TTPR shall be documented in detail. It includes access guidelines, change of authorized personnel, notification of unauthorized access and records of countermeasures to such access.

To improve security and manage integrity, encryption and either a digital signature and/or trusted stamp token issued by a trusted time stamping authority shall be applied to the digital record stored in the TTPR. If the client has applied itself a digital signature and/or a time stamping token, the TTPR may not need to apply its own digital signature or a time stamping token.

5.3.2.5 Information provision

The service agreement shall include information verifying the validity and reliability of the TTPR's PKI certificate being provided for the client. The TTPR and the client specify the information and type of certificate to be provided during the period stated in the service agreement.

5.3.2.6 Compensation

The service agreement shall include the compensation item from any damage or risks. Means of compensation for loss, calculation of compensation amount or scope of compensation shall 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.

5.4 TTPR subservices

5.4.1 General

Each service function is referred to as a "service" in this document. This subclause describes the requirements, the quality and the procedures of each service.

5.4.2 Acquisition service

This service is to receive an information package including digital records from a client. The TTPR shall register the received records in its repository storage after verifying the validity of the whole information package.

The requirements of the acquisition service are as follows.

- A new TTPR client shall be authorized as a member of the TTPR after requesting registration and being identified.
- The client system shall be able to package the digital record into a TSIP in preparation for transmitting the record to the TTPR.
- In case the client requests a printing service about the authenticity certificate, the authenticity of client's records to be stored in the TTPR shall be managed, by checking creator's digital signature, timestamp of creation or other evidence related to authenticity.
- The acquisition service shall examine whether the consigned digital record gets damaged during the acquisition, on registration, in the event of registration failure, virus infection and/or errors.

The quality of the acquisition service shall be maintained as follows.

- Integrity shall be managed by receiving a digital record bundle packaged into the form of a TSIP.
- In the client system, the process of packing the digital records in the form of a TSIP shall be processed within an acceptable time. In the event of a problem, the TTPR shall notify the client with the cause and solution.

  Reliable transmission shall be able to notify the problem or error of transmission, in case the receiver does not send its confirmation of receipt within an acceptable time which is predefined for the purpose of checking the transmission error.
- The following requirements shall be complied with in order to maintain security during the transmission and its confirmation of digital records between the TTPR and the client.
  - Use a reliable transmission protocol with a transmission and its confirmation check function.
  - Process only using a secure transmission method.
  - Process confidentiality and integrity requirements for the well-transmitted digital records.
  - Perform denial protection for the well- transmitted digital records.

The procedures of the acquisition service are as follows:

a) the TTPR and client discuss and establish an acquisition plan. The acquisition plan includes 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 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 repository

   - whether the digital record in the TSIP has been successfully converted into client's digital records,
   - whether the digital record is infected by a virus or has discord, and
   - whether the format of TSIP is compliant;

e) after the acquisition is complete, the digital records received from the client update the acquisition audit trail by the TTPR;

f) upon the client's request, the TTPR confirms the acquisition from the client and updates the acquisition list;

g) confirmation of acquisition is accepted by the client and the TTPR stores the confirmation.

5.4.3 Repository service

This service is to store the digital records consigned by the client.

The requirements of the repository service are as follows:

- the TTPR shall have in place a process and systems for the trustworthy management of TAIP; and
- a TAIP shall be produced at the point when the digital record is registered at the TTPR system, and the system shall manage the TAIP with a unique identifier assigned.

The quality of the repository service shall be maintained as follows:

- the TTPR creates an audit trail for the completed management tasks of the stored record, which will be used to prove the authenticity and integrity of it;
- the TTPR shall recover from any disaster or error situation to ensure that authenticity is not compromised.

The procedures of the repository service are as follows.

a) The TTPR shall verify the following items when the client requests registration of digital records:

   - the client's authority;
   - whether the digital records are included in the TSIP;
   - whether the format can be accepted/is suitable for building the TAIP is correct.

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

c) After the completion of registration of the digital records, the TTPR shall confirm registration to the client as specified in the agreement, and add it to the registration list.

d) Confirmation of registration is accepted by the client and TTPR stores the confirmation.

5.4.4 Access and use of service

This service is to enable a client to access and search the client's consigned digital records.

The requirements of the access and use service are as follows.

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

The quality of the access and use service shall be maintained as follows.

- Browsing or searching shall be allowed within the specified time periods.
- Browsing or searching shall be allowed subject to the agreed and authorized access authority.
- The storage and browsing/issuing service shall always be available for the client, subject to agreement.

The procedures of the access and use service are as follows.

- The client shall be allowed to use and search the digital record in the TTPR, using the agreed search tools.
- The TTPR shall verify the following prior to fulfilling the browse request of the client.
- The client’s access authority is checked.
- The browsing digital record requested by the client is checked.
- Forgery and falsification of the digital records through actions such as "modify" or "copy" shall be prevented when the client browses the digital record.
- If the client is unable to browse a particular digital record, the TTPR shall assist the client in determining the cause of failure and shall recommend a solution.

5.4.5 Issuance service

This service is to issue the digital record consigned by the client.

The requirements of the issuance service are as follows.

- The TTPR shall issue digital records only to the client with issuance authority for the stored records.
- The TTPR shall issue authentic digital records and document the issuance of the records.

The quality of the issuance service shall be maintained as follows.

- The issuance service shall be allowed within the specified time periods.
- The TTPR shall always be ready for the client to use the issuance service.

The procedures of the issuance service are as follows.

a) The TTPR shall issue the authenticity certificate of a digital record when an authorized client requests it.

b) The TTPR shall verify the following prior to fulfilling an issuance request:

   - the client’s authority;
   - whether the client is the recipient of the requested digital record.

c) The TTPR shall issue the digital record to the client in a trusted dissemination information package (TDIP).

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

e) Confirmation of issuance is accepted by the client and TTPR stores the confirmation.

5.4.6 Conversion service

This service is to convert the format of the digital record consigned by the client in formats suitable for long-term storage purposes. This conversion service is optional according to the client's request.

The requirements of the conversion service are as follows.

- The TTPR shall provide a conversion service only to the authorized client who requests conversion of the digital record.
- The TTPR shall notify clients about available file types from the conversion service.
- The TTPR shall not allow any alteration of the digital record's content, structure and presentation during the conversion process, and the client shall be able to browse the converted digital record upon request.

The quality of the conversion service shall be maintained as follows.

- The conversion service shall be performed within a specified time period.
- Digital record's authenticity is not be compromised during the conversion process.

The procedures of the conversion service are as follows.

a) The TTPR shall convert the digital record when an authorized client requests it.

b) The TTPR shall verify the following upon a conversion request:

  - the client's authority;
  - whether the digital records are convertible.

c) Conversion of the digital records.

d) The TTPR shall save the converted digital records in a TSIP format.

e) The TTPR shall 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, the TTPS shall issue a non-alteration certificate upon the client's request and add it to the certificate issuance list.

g) Confirmation of conversion is accepted by the client and TTPR stores the confirmation.

5.4.7 Delivery and/or migration service

This service is to migrate the stored digital record to another TTPR or other nominated party. This service is optional according to the client's request.

The requirements of the delivery and/or migration service are as follows.

- The client of this service shall identify a recipient for delivery and/or migration.
- When the digital records to be delivered or migrated are requested, at first the TTPR shall store the target records, then convert them to the TTPR's issuance format and transmit them to the recipient in a timely manner.
- The client who transmits and receives the digital records shall be a member of the TTPR in advance.
- The TTPR and the clients involved in this transaction shall have systems installed with the functionality for delivery and/or migration.

The quality of the delivery and/or migration service shall be maintained as follows.

- The completion of this service shall be undertaken within the specified time period after the request.
- Both scopes of the request and the delivery and/or migration shall be checked. In the case of concordance, the TTPR shall issue the confirmation of delivery and/or migration. In the case of discordance, the TTPR shall determine the cause and notify it to the client.
- In the case of the migration service to another TTPR, the relevant digital records shall be completely transmitted.
- The following requirements shall be complied with in order to maintain security during transmission.
- Use a reliable transmission protocol with a transmission and its confirmation check function.
- Process only using a secure transmission method.
- Ensure confidentiality and integrity for both the transmitted and the received digital record.
- Perform denial protection for both the transmitted and the received records.

The procedures of delivery and/or migration service are as follows.

a) When a client changes a TTPR or the digital record is to be migrated to another TTPR's storage, a TTPR shall move the information relevant to the digital record and issue a confirmation of delivery and/or migration.

b) The TTPR shall verify the following upon receiving a request for the delivery and/or migration service:

   - check the client's authority regarding delivery and/or migration;
   - check whether it is possible to move the record to the recipient TTPR.

c) The delivery and/or migration service shall be performed using an online or offline method.

d) The TTPR shall save the metadata for the delivery and/or migration, e.g. format, time, and log.

e) The recipient TTPR shall receive the digital record and then register and store the record.

f) The TTPR shall 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 shall not physically be recovered;
   - after the self-migration of the digital record, the TTPR shall provide a non-alteration certificate to the client and adds it to the confirmation list.

5.4.8 Disposal service

This service is to dispose the digital record stored in the TTPR.

The requirements of 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 client of this service shall be authorized.
- Target records of this service shall be disposed of in a manner preventing it's their physical recovery; disposal is only to be performed on the authority of a senior TTPR employee.

— Documentation of the disposal process shall be made. In case after the disposal, this document is necessary 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 shall be produced and maintained for future needs.

The quality of the disposal service shall be maintained as follows.

— Disposal process shall be completed within the specified time period, upon the client's request.

— In the event of failure during processing the digital record which is being disposed, all relevant data shall be disposed of in accordance with the transaction.

— No record related to the disposed digital record shall be left, other than the confirmation of disposal.

— To maintain security and reliability, disposal shall only be performed on the authority of a senior TTPR expert.

The procedures of the 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 allowed to disposal request;

  — 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 shall notify the client of the expiration of the retention period as agreed in the service agreement to the expiration date.

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

d) The TTPR shall dispose of the digital record in accordance with the following, upon the client's request for disposal.

  — Destroy the digital record and the related TAIP information so that it shall not be physically recovered.

  — After the disposal, issue the confirmation of disposal to the client.

  — Add the disposal information to the disposal list.

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

f) The confirmation of disposal is accepted by the client and TTPR stores the confirmation.

5.4.9 TTPR certification service

This service is to issue certificates for the stored digital records in the TTPR.

The requirements of the certification/confirmation service are as follows.

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

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

— The TTPR shall issue a authenticity certificate 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 shall provide a function to verify format, expiration date, disposition issue, digital signature, signature certificate and time stamp tokens of the issued authentic copy and certificate.

The quality of the certification service shall be maintained as follows.

- The TTPR shall be able to issue a certificate within the specified time period, upon the client's request.
- Documentation for issuance of all the certificates shall be made to ensure the reliability of the issued certificate.
- The client shall always be able to receive certificates from the TTPR, upon request.
- To maintain security during the transmission of the certificate to the client, the following shall be conformed to:
  - use a reliable transmission protocol with a transmission and its confirmation check function;
  - process only using a secure transmission method;
  - process confidentiality and integrity for transmitted certificate; and
  - perform denial protection for transmitted certificate.

The procedures of the certification service are as follows.

a) The TTPR provides the certificate and/or the confirmation as follows.

- Issue a registration confirmation to prove the registration and deposit of the digital record requested by the client, in the TTPR.
- Issue an issuance confirmation to prove the issuance of a digital record with an authenticity certificate to the client.
- Issue a delivery and/or migration confirmation to prove the transmission of the digital record to another TTPR.
- Issue a disposition confirmation to prove the complete disposition of the digital record requested by the client.
- Issue an authenticity certificate 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 the certificate and/or the confirmation during the process of providing the digital record management service, the TTPR should define the function, purpose and format for usage.

b) The TTPR shall include the following information in the certificate and/or the confirmation:

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

c) The TTPR shall produce the certificate and/or the confirmation as follows:

- produce certificates and/or the confirmation based on a standardized format;
- record time information from the TTPR's system on the certificate;
- produce a security report demonstrating the integrity of the digital record and attach it to the certificate;
- attach the TTPR's digital signature.

d) Issuance of the certificate and/or the confirmation shall proceed as follows:

- check the client's authority allowed to the certificate and/or the confirmation;
- issue an electronic certificate based on a standardized format.

e) The TTPR shall retain the list of issued certificates/confirmation documents and record the following certificate list information:

- serial number of the certificate and/or the confirmation;
- issued date and time of the certificate;
- expiration date of the certificate;
- purpose of the certificate;
- other necessary information.

5.4.10 Non-repository certification service (Remote Certification Service)

This service stores only some distinctive elements of client's digital records (for example, their digests calculated via a hashing algorithm). A TTPR shall remotely certify a digital record not stored in the TTPR. This service is optionally provided for client convenience.

The requirements of the non-repository service are as follows.

- The client who is willing to use the non-repository certification service shall be a member of the TTPR.
- The TTPR shall be able to extract the information for identifying the relevant digital record (such as the hash code).
- The TTPR shall 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 shall be issued to the client.
- Information about the digital record shall be disposed of after the expiration of a specified period based on the service agreement.

The quality of the non-repository certification service shall be maintained as follows.

- Information about the extraction of the digital record which the client requests from the remote certification service shall be processed within the specified time period.
- A client shall 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 shall be completed within the specified time period.
- Documentation for issuance of all certificates shall be made for the reliability of the issued certificate.

- The following shall be conformed to, in order to maintain the security during the transmission of a hash code between the TTPR and the client:
  - to use a reliable transmission protocol with a transmission and its confirmation check function;
  - to process only using secure transmission methods;
  - to process confidentiality and integrity information about the digital record;
  - to perform denial protection for the information about the digital record.

The procedures of the non-repository service are as follows.

a) The client transmits the digital record to the TTPR that will be used for non-repository certification service.

b) The TTPR extracts the information (such as the hash tag) for the received digital record, and then discards the digital record.

c) The TTPR provides remote certification using the information about the digital record as follows:

  - issue a registration confirmation 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 Time Stamp Token on the digest calculated on the stored digital object;
  - 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;
  - issue a confirmation to prove the complete disposition of the information stored about the digital record as requested by the client.

d) The TTPR shall include the following information in the certificate and/or the confirmation:;

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

6 Technological requirements

6.1 General

To maintain reliable and useful TTPR services, it is necessary to make use of software and hardware which are secure and reliable. The technology shall protect managed digital records in the event of any disaster, such as earthquake, fire or intrusion by an unauthorized person. As the TTPR is exposed on public and open networks, it shall employ a security system to defend against any threats to the TTPR.

This clause specifies the types and requirements of TTPR technology that shall be considered from the time of establishment.

6.2 Digital record repository

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

- registration, browsing and searching of the digital records;
- issuance of certificates and digital records;
- migration and confirmation of the digital record;
- conversion of the digital record;
- integrity check of the digital record;
- disposal of the digital record.

6.3 Transmitter–receiver

The TTPR's transmitter–receiver system shall satisfy the following functions to transmit or receive messages (such as TSIP, TDIP), including the digital record:

- function to transmit and receive the messages according to a 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;
- denial protection functions for transmitted or received messages.

6.4 Network system

The TTPR's network shall 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;
- function supporting check of the process result within the repository from the outside system.

6.5 Time-stamping

The TTPR can be equipped with a system that records and manages the date and time of transmission, while making use of external functions. Such equipment shall perform the following functions:

- function enabling time transmitter to send the time from a time source;
- function to inform the administrator when a time transmitter has an error;
- function to provide the accurate date and time over a full 24 h period when time transmission from the 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 automatically ceases the time-stamping service, immediately after there has been a failure of the time correction function and after the error message has been put out;
- function that checks whether the time received by the client matches the issuance time;
- function that provides the time-stamping service using the digital signature.

6.6 Audit trail

The TTPR shall create and retain an audit record for the following information related to services such as the digital record repository which shall include:

- acquisition history of the digital record;
- repository history of the digital record;
- access and use history of the digital record;
- issuance history of the digital record;
- conversion history of the digital record;
- delivery and/or migration history of the digital record;
- disposal history of the digital record;
- certification history of the digital record;
- non-repository certification history of the digital record.

6.7 Network security system

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

- function to provide consistent services in the event that one of the transmission systems fails;
- intrusion protection systems and access control protocols;
- 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.

6.8 Access control equipment

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

- physical access control function that restricts access by unauthorized persons to the repository system;
- audit record function for information such as type of incident and whether the system has succeeded or failed, and if it has failed, the cause of failure, access date and time and information on intruder;
- under two or three ways authentication where the three authentication methods are: 1) something one knows(e.g. PIN), 2) something one has(e.g. OTP token), 3) something one is (e.g. biometrics);
- safe access to and safe exit from the operation room during power outage shall be ensured;
- implementation of access controls based on the role of the administrator, at operation system level;
- implementation of a program or process appropriate for the goal of system operation;
- creation and retention of an audit record for the information of repository system operation.

6.9 Disaster recovery facility

The TTPR shall provide business continuity and disaster prevention processes in line with, for example ISO 22301, for the operation of the TTPR.

The TTPR's remote repository shall have the following functions:

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

6.10 System for certificate issuance and validation of digital records

The TTPR shall 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 hash code assuring the integrity of the digital record;
- the function to attach the public-key certificate to prove the identity of the issuing TTPR;
- the function to attach the time-stamping token, transmitted from the time-stamp system;
- the function to create the expiration date of the authenticity certificate;
- the function to create the authenticity certificate;
- the encryption function to ensure the confidentiality of specific information in the certificate.

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

- the registration confirmation to prove the registration of the digital record by the client;
- the migration confirmation to prove the migration of the digital record to another repository;
- the disposition confirmation to prove the disposal of the digital record;
- the non-alteration certificate to prove that the content, structure and presentation of the digital record after a change of file type or storage media has been preserved;
- the authenticity certificate to prove that the issued digital record is not compromised to the authentic digital record stored in the repository.

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

- client information: the certificate and/or the confirmation shall include personal identity information;
- 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; and
- any other information related to legal effect or validation of the certificate.

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

- the function of validating the authenticity certificate format;
- the function of validating through a 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 or hash code written on the certificate;
- the function of notifying the client when the validation on the certificate has failed.

The TTPR's certificate system shall 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 the audit record;
- the protection from the illegal use of certificate creation/issuance software;
- 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 shall be provided.

6.11 Backup system

The TTPR's backup system shall 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 digital records that will be applied to the repository, under nonstop status;
- a function that allows backup for different types of OS platform such as Linux, Unix or Windows;
- a function that allows backup of digital records, databases and other management information used by the TTPR for management and access purposes;
- a function preventing the forgery and falsification of backup data;
- reference to ISO/IEC/TR 10032.

7 Operational requirements

7.1 General

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

7.2 Client management

The following shall be managed for client information registration:

- client's identification and authentication processes shall be available when the client is registered;
- client's registration date and name, as well as any other information that uniquely identifies the client, shall be entered accurately;
- client's information shall be deleted only when no longer needed for legitimate purposes.

The following shall 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 shall 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 shall be retained;
- the TTPR service shall 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 shall be recorded in the audit record.

7.3 Administrator's role and authority management

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

- roles of all TTPR administrators are defined, and access data to TTPR shall be controlled based on the role;
- each administrator shall be assigned a role, and collected history shall be maintained and managed;
- access to records of unauthorized activities shall be restricted to authorized personnel;
- all processes including activities performed by the administrator and records of unauthorized activities shall be recorded in the audit record.

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

- when an unauthorized administrator attempts to access a system, alarms shall be triggered for notification to an authorized administrator and access authority will not be given by the operating system of the system;
- all access histories shall be recorded in the log including illegal attempts by an administrator.

Use of certification creation/issuance software shall be handled as follows:

- access shall be controlled so that only the administrator with proper authority will have access to the certification creation/issuance software;
- when blocking the access, a warning message shall be notified simultaneously to the administrator;
- the complete access history shall be recorded in the log, including the illegal access by an administrator;
- if the certification creation/issuance software's structure consists of server and client, confirm the access control function on both sides.

7.4 Network and security management

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

- unidentified access to the TTPR equipment shall be filtered out by a firewall system. Intrusion trials with an unidentified data packet shall be prevented and detected by an IPS/IDS (Intrusion Prevention System/Intrusion Detection System);
- identification checks shall 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 shall 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;
- history of access to the network equipment and network security system shall be recorded in the audit record or log.

Access control for the operation room security system shall be managed as follows:

- a person who accesses the security system shall be identified via personal information such as ID/password or biometric based authentication.
- access to the security system, such as access control system, intrusion detection system and surveillance camera system, shall be controlled;
- password protection system shall not show the typed password when logging in, and shall have an encryption function to safely protect the password saved in the system;
- access history of the administrator to the security system shall be recorded in the audit record or log.

7.5 Digital records management

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

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

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

- the TTPR shall determine whether the transmitted digital record is infected by a virus or other malicious software, and not store the record and notify the client of the result if an infection is detected;
- the TTPR shall determine whether there is any virus error in the TSIP, and notify the client of the result if any error is detected;
- infection and/or error inspection histories shall be recorded in the audit record.

The validation function of the TSIP format regarding the client's digital records shall be performed, and errors shall be reported if there is a failure.

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

- provide a search function using digital record's metadata items and digital records;
- digital record search from the client's system is allowed only for records owned by the client;
- digital record search by the administrator is allowed for all digital records stored in TTPR, and access (browsing and issuance) to the digital record is not allowed without the permission of the client.

The following shall 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:

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

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

- issue the record in the file format requested by the client because the original file may have been converted, because it was not in a format accepted by the TTPR, or the client may require that a record is given back in a format different from the one used for archiving;
- the history log for the digital record issuance and the converted version shall be recorded in the audit record.

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

- when a trusted dissemination information package (TDIP) is created, an authenticity certificate and authenticity information is added to TAIP; and the integrity of the digital record and property included in the TAIP shall be verified;
- this function is provided separately from the integrity check function provided by the storage media; and
- integrity verification history shall be recorded in the audit record.

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

- When a digital record is issued, an authenticity certificate for it shall be also issued to the individual/organization to which the client of the digital record repository has entrusted the issuance request authority.
- When a TTPR issues the digital record to another TTPR, it shall issue the digital record with an authenticity certificate.
- The TTPR shall provide the verification function for validating the public key certificate of the digital record recipient, or specify in the client's terms and conditions that the client needs to attach a valid public key certificate.

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

- Notify the client prior to the expiration of the digital record's destruction date. Such notification shall be provided in advance of time, so that the client has sufficient time to decide on the action to be taken.