



InterPARES 3 Project

International Research on Permanent Authentic Records in Electronic Systems

TEAM Korea

Status: Draft

Version: 1.0

Submission Date: November 2009

Release Date: November 2009

Author: The InterPARES 3 Project, TEAM Korea

Writer(s): Eun G. Park
School of Information Studies,
McGill University, Montréal, Québec

Project Component: Research

URL:

http://www.interpares.org/rws/display_file.cfm?doc=ip3_korea_cs02_finale_report-v4f.pdf

A. Overview

The Certified e-Document Authority (CeDA) is a trusted third party (TTP) institution for the secure retention and exchange of electronic documents between its clients. The CeDA was originally established to provide secure infrastructure for retaining e-documents, and for promoting e-business by offering a transparent and reliable e-document exchange environment.

Unlike traditional or digital archives that aim to archive documents for certain document-creating bodies and serve the general public, CeDA's main role is to enhance national e-document management and support business firms in digital innovation. Any business or individual client can submit either e-documents or paper documents to the CeDA, and the CeDA then retains them in a secure form of digital (or digitized) information package for a certain period specified in the contract with the business or client. These retained e-documents can be shared with other parties that are authorized by each client. CeDA guarantees the authenticity, reliability, and security of retained documents for the users.

This study examines the e-document management and digitization practices of CeDA as an official service provider of digital archiving and a trusted third party of e-document exchange.

B. Statement of Methodology

Case study survey questions regarding policy, records, and systems were distributed to three major CeDA service providers. The research team also interviewed managerial-level personnel in those three CeDAs and in the Korea Institution for Electronic Commerce (KIEC). KIEC is an affiliated organization of Ministry of Knowledge Economy of Korea, which established guidelines and technical standards of CeDA's operation and IT systems.

Since CeDA should operate according to rules, guidelines, and technical standards set by Korean government, those rules and regulations were reviewed. These documents include 3 acts that define fundamental roles and regulations of CeDA; 5 notices that regulate CeDA's facilities requirements, standard work processes, and qualification criteria for their personnel; 4 guides that relate to the evaluation and auditing of CeDA's operations; 5 technical standards that deal with information packages and certificates, metadata, and CeDA's IT systems and user system specifications.

C. Description of Context

1. Provenancial:

Since the CeDA is a third-party institution for e-document archiving and exchange, various organizations can become clients of the CeDA, and submit their documents in digital or paper format. All documents retained in the CeDA officially retain legal authority as original, authentic, and reliable. The Korean government legislated the '*Framework Act on Electronic Commerce*' in 2005 as amendment to establish 'Certified e-Document Authorities (CeDA)' and to endow legal authority upon the e-documents retained in the CeDA. Since all the e-documents in CeDA are recognized as legal and authentic, the client's paper documents that are submitted to and digitized in CeDA can be disposed of after they are successfully digitized and retained in CeDA unless the paper documents must be kept by the client.

As mentioned above, a client of CeDA can submit either e-documents or paper documents. There are two methods of submitting e-documents. First, the client can bring hard disks or CD-ROMS that store e-documents to be archived to the CeDA facility, and the CeDA then registers those e-documents to the digital archiving system. Second, the client can connect its own IT systems to CeDA's digital archiving system. Once connected, all the data of the client's can be sent to CeDA's system and automatically registered and archived.

When the clients want to archive paper documents, they can bring them to the CeDA facility. These paper documents are digitized in the digitization room in the CeDA according to official digitization procedure by authorized digitization experts of the CeDA. It has been controversial whether scanned and digitized documents can be recognized as originals and thus have legal authority. This controversy has been one of the obstacles of digitization and for offices going paperless. To solve this, the Korean government enacted new rules defining the legal status of digitized documents. According to the '*Regulation on Digitization Procedures and Methods*' legal authority can only be endowed upon digitized documents that are digitized by the CeDA.

2. Juridical-administrative:

In this study, CeDA is regarded as a creating body of digital entities. Even though the original paper or e-documents are created by clients, the CeDA encapsulates the original documents into new information packages by attaching proper metadata and certificates of the documents' status. As a creating and archiving body of digital entities, the CeDA is subject to rules, regulations, and standards regarding its establishment, operation, and evaluation.

The governance of the CeDA is formed by three organizations: Ministry of Knowledge Economy (MKE), Korea Institute for Electronic Commerce (KIEC), and Certified e-Document Authority (CeDA). MKE establishes the relevant acts, notices, and regulations that the CeDA adheres to, and it officially approves new CeDA service providers. KIEC sets up practical guidelines and technical standards for the CeDA. It also evaluates and screens IT services companies that are potential CeDA service providers. Actual CeDA service providers are IT service companies who can afford to establish proper digital archiving facilities according to CeDA technical standards and operate their facilities according to government regulations.

There are several acts, regulations, and notices, but the major ones are as follows:

- *Framework Act on Electronic Commerce*: this act defines the fundamental roles and responsibilities of CeDA.
- *Regulation on the CeDA Facilities and Equipments*: this act addresses the detailed requirements for facilities and equipment for the CeDA, such as required systems with mandatory functions, equipment for network time protocol, security systems of the network and required facilities for certificates.
- *Regulation for Standard Work Process*: this defines the CeDA's management process, work process, security management process and other processes.
- *Regulation on Digitalization Procedures and Methods*: this deals with the environment of the authorized workplace and the detailed specifications of all digitalization systems and scanning equipment.
- *Detailed Regulation on Digitization Facilities and Equipments*: this standardizes the authorized workplace, IT systems, scanning equipments and all the digitalization facilities.
- *Notice of the CeDA Personnel Qualification*: this provides the required qualifications and responsibilities for authorized personnel of the CeDA.

3. Procedural & Documentary:

The CeDA has four areas of work management: document management, digitization management, operation management, and security management. These processes are defined in the *'Regulation for Standard Work Process'*. The document management process deals with how to register, preserve, retrieve, reformat, transfer, and dispose of e-documents. The regulation provided a detailed checklist about the roles of the CeDA and the client in each step of the work process. In the digitization management process, digitization protocols and steps are defined. Through the digitization management process, the CeDA can develop proper digitization protocol before each digitization, and the digitization process can ensure that the digitized documents have the same contents as the originals. Operation management and security management processes deal with daily work at the CeDA, regular system inspection, and physical, procedural, organizational, technical security requirements.

Once e-documents are submitted to the CeDA or paper documents are digitized in the CeDA, they are converted into an 'information package' based on the OAIS reference model (ISO14721). The purpose of using an information package is to prevent forgery of e-documents, and to ensure the e-documents' reliability and integrity. In order to preserve contents, structure, and context of the e-documents, each information package consists of actual contents and metadata. The metadata has information about registration, classification, preservation, and structure of the e-documents retained in the CeDA. The metadata has been developed based on ISO standard for records management (ISO15489) and ISO RM metadata standard (ISO23081).

The CeDA registers, preserves, retrieves, reformats, disposes of, and transfers e-documents for the clients. At each activity, the CeDA creates a history log and audit trail of information as evidence. The certificate is a record of this evidence that is given to clients when they ask for certificates to verify the reliability of certain e-documents.

4. Technological:

The CeDA services are provided with proper IT infrastructure, facilities and equipment, which are all regulated by *'Guideline of CeDA Facilities and Equipments Evaluation'*. This guideline specifies every technical requirement of the CeDA, such as e-document management, certificate management, reliability assurance, security management, audit trail management,

access control, message exchange protocol, system operation and protection, backup and restoring.

CeDA should create and retain three types of information package (Submission Information Package (SIP), Archival Information Package (AIP), and Dissemination Information Package (DIP)), as specified in OAIS model. Metadata is created and packaged in these information packages at each step of e-document management from registration through retrieval and reformatting to disposal or preservation. The regulation requires CeDA's IT system to create and issue certificates at each step of e-document management. This certification stores each document's date history and timestamp, which ensures the reliability and authenticity of the document.

For secure document management, user identification with digital signature is required. The prevention of message forgery is necessary in CeDA's IT system. The IT system should also create and manage proper audit trail data which stores the history of every action taken in every retained document in CeDA, as well as the general system's operational data. This audit trail data should be preserved for five years.

Access control related to users, IT system and data, and physical facilities should be established in CeDA. Roles and access rights of all personnel in CeDA should be pre-defined. This information should be continuously managed in the access profile. All data in the CeDA should be backed up according to pre-defined backup policies and schedule, and a recovery plan should be prepared and practiced in case of data loss.

D. Narrative answers to the applicable set of studies questions.

Not applicable

E. Narrative answers to the applicable project research questions.

Since the first CeDA was implemented in 2005, the number of CeDAs has increased to eight sites in 2009, and the diversity of clients has widened from international trading to financial, health, and energy industries. For small and medium-sized companies, it is not easy or cheap to establish their own archival organization. When they don't have internal competency in digital archiving, it is necessary for them to outsource services of third-party digital repositories. Before CeDA was initiated, there was a lack of national standards or integrated rules and regulation on scanning, retaining, and exchanging e-documents in Korea. After the amendment and enactment of related rules and regulations, e-documents that are scanned, registered, and retained in CeDA can be recognized as authentic and reliable digital documents.

As government-approved official digital repositories, CeDAs have created a standard digital archiving environment and provided cost-effective services. For many clients companies of CeDAs, it is better to outsource their archiving jobs to professional service providers in terms of document management, technology, security, and cost. Maintaining close relationship with trusted third-party digital repository such as CeDAs, client companies can focus their energy on their core competencies.

CeDAs and client companies share a mutual trust. It is the most important factor in this relationship. Since client companies entrust document management to CeDA, nothing will be secure without trust. This relationship is usually set through long-term contracts that last a minimum of five years and up to more than ten years.

To create reliable third-party digital repository, the Korean government started by establishing amendments of existing laws on e-documents. There were three issues related to how to establish CeDA: how can one ensure authenticity and reliability of retained e-documents, how can one endow legal authority to scanned (digitized) paper documents, and how can one promote secure e-documents exchange between multiple parties? To solve these issues, CeDA

created 3 kinds of major services: archiving service with official digitizing, intermediary service for e-document exchange, and certification service.

Archiving service is offered based on the OAIS model. Each document is registered and packaged in SIP, stored in AIP, and accessed in DIP. Necessary metadata is created at each stage of the document lifecycle and packaged in the information packages together with original e-document.

A great number of paper documents are created through daily business operations, and they became barriers in moving to paperless offices. Companies could digitize their paper documents with any scanning software and hardware. However, an important issue was the these scanned documents had no legal authority. In other words, many companies had to retain scanned paper documents in case they were necessary. To solve this problem, the Korean government endowed e-documents that are officially digitized in CeDA legal authority and authenticity. When documents are digitized under the supervision of CeDA, newly digitized documents have legal authenticity and one can dispose of old paper documents.

Clients of CeDA can allow other business partners to access retained documents. CeDA offers intermediary service for the secure exchange of e-documents. By using CeDA's user identification system and encryption technology based on Public Key Infrastructure (PKI), clients can send and receive e-documents without the risk of unauthorized data change, unwanted data loss, or repudiation.

E-documents created and retained in CeDA, one can be certain that that they have not been forged. To ensure authenticity and reliability of the retained documents, CeDA provide clients with certificates at each stage of document's lifecycle. All documents retained in CeDA are quality-ensured with these certificates.

CeDA's roles and responsibilities, work process, and detailed technical specifications are defined and described in various acts, government notices, guidelines and technical standards. Every CeDA service provider should establish and maintain infrastructure according to these rules and regulations. CeDAs' operational soundness is examined and evaluated by regular government auditing each year. Even though actual CeDA services are offered by private IT companies, CeDAs have official authority and reliable quality. Korea's approach can be applied to countries that don't have infrastructure of managing e-document management but need to formulate national e-document management policy, technical environment, and IT infrastructure.

Since CeDA's work process, information structure, and IT system's functional requirements are based on international standards, this type of digital repository model can be a model for similar cases. However, every country has different juridical contexts where laws and regulations related to e-document, customization of law and regulations should be carefully considered.

F. Bibliography.

Not applicable

G. Glossary

Not applicable

H. An IDEF0 model

Not applicable

I. Diplomatic analysis of records

According to diplomatic analysis, the examined digital entities in the CeDA (i.e., the transferred digital documents, the digitized documents, and the certificates of integrity) are qualified as records. Since the CeDA's role is limited to preserving clients' documents, it has no control over deciding the retention period for the documents it possesses. The documents should be disposed of according to the client body's record retention schedule. However, as long as the documents are in the custody of the CeDA, they should be preserved intact. To fulfill this requirement, the CeDA has such methods as a regular backup procedure, security facilities, and an emergency plan. In summary, considering technological obsolescence, the CeDA also must prepare for necessary conversion or migration.

J. Findings and Conclusion

This case study can be summarized with the following four kinds of steps: 1) background of establishing CeDA sites; 2) method of creating trust; 3) delivery services; and 4) quality control.

1) Background of establishing CeDA sites

Unlike traditional or digital archives that aim to archive documents for certain document-creating bodies and to serve to the general public, CeDA's main role is to enhance national e-document management capacity and to enable business firms to innovate their digital processes. The CeDA was established to provide secure infrastructure for retaining e-documents and to promote e-business by offering a transparent and reliable environment for e-document retention and exchange.

2) Method of creating trust

To create trustworthiness for the retained e-documents, the Korean government developed acts, regulations, and technical standards that specify policies, processes, organizational and technical requirements of the CeDA facilities, work processes, and operations. Potential CeDA service providers should be equipped with the required facilities and show the operational capabilities to be appointed and approved as new CeDA service providers. Once appointed and approved as a CeDA service provider, they should maintain the regulations and technical standards to offer their services. In maintaining these regulations and standards, the CeDA can provide secure retention and access for the e-documents.

3) Delivery services

For the delivery of CeDA service, there is a three-tiered structure. The government creates the fundamental rules and regulations; KIEC develops and implements the necessary technical standards and guidelines for the CeDA service. It also reviews and approves IT service providers, who may then apply to be official CeDA service providers. Any IT service providers who can comply with these regulations and technical standards can apply to be appointed and approved as a CeDA service provider. The government evaluates the capabilities of each applicant and appoints a proper applicant as a new CeDA service provider.

4) Quality control

Since CeDA service is offered by private IT companies that need to comply with their rules and regulations, it is important to check and control if they ensure service quality as required in the rules and regulations. The Korean government regulates the annual auditing of service quality and the soundness of each operation. Its auditing has two parts: functional inspection, and

operational & management inspection. In the functional inspection, overall e-document management functions are evaluated from registration through retention to disposal. In the operational & management inspection, technical issues such as management of the facilities and equipment, IT systems and network security, and disaster prevention are evaluated. In addition to annual auditing, immediate and random inspections can be conducted when there is an IT system change, a facilities change, or any other significant change that could impact the current e-document management.

This case study shows unique methods of applying a digital repository into a new industry's environment. In this case, the role of the digital repository is extended from institutional digital archives to national infrastructure. As it is becoming more common and prevalent to create and exchange e-documents in every business operation, it is necessary to create infrastructure for secure retention and reliable e-document exchange between parties. Reliable digital repositories are necessary in every organization, but not all organizations have the capability to establish their own archives and manage their e-documents. CeDA can be a good business partner for organizations looking for trustworthy third-party digital repositories.

The traditional role of digital archives has been limited to maintaining custody of e-documents, but CeDA has the additional role of being an intermediary for e-document exchange, which is valuable to more organizations. By establishing a trusted document management environment, CeDA creates reliable social infrastructure of e-document exchange.