InterPARES 3 Project

International Research on Permanent Authentic Records in Electronic Systems

Trusted 3rd Party Digital Repositories

Brazil Summit International Symposium
September 30, 2009

Eun Park
IP3 TEAM Korea
McGill University
School of Information Studies

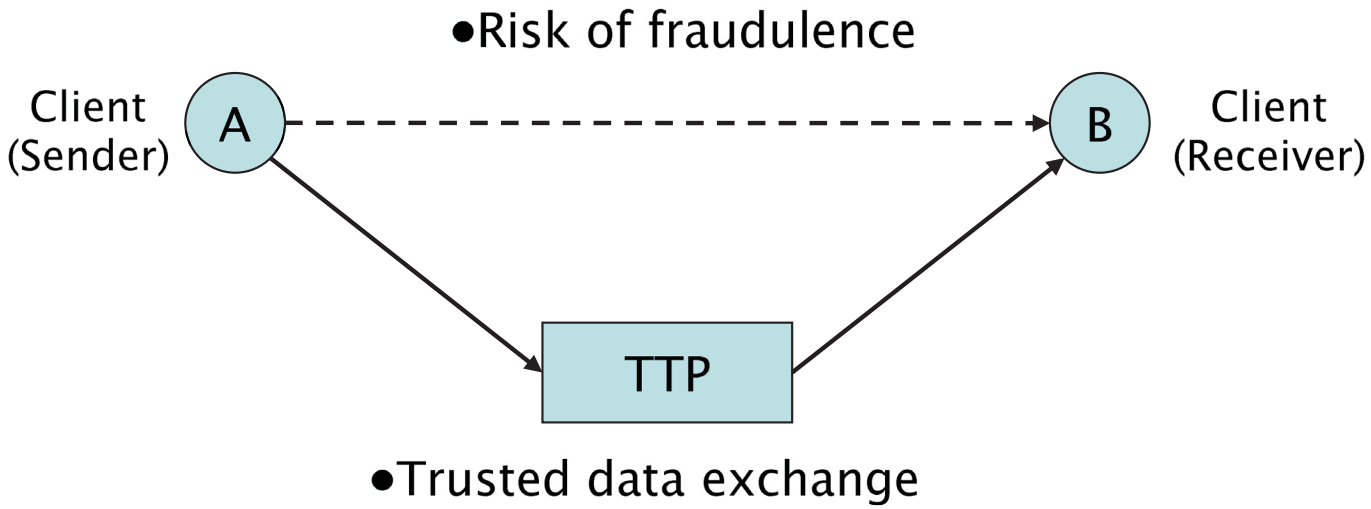
Contents

- Overview
- Background of trusted 3rd party digital repositories
- Types of Trusted 3rd party digital repositories
- Case 1. Archives model
- Case 2. e-Notary model
- Case 3. Combination model
- Issues and questions

Overview

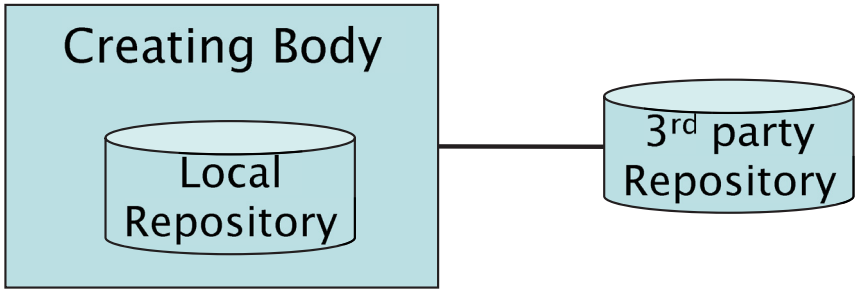
- **What is 'Trusted Third Party Digital Repository' ?**

- **Trusted Third Party (TTP)**
  - An authority that acts as an intermediary between participating parties for trustworthy interactions between the parties
  - A trusted third party authority that is trusted by both parties (A, B)



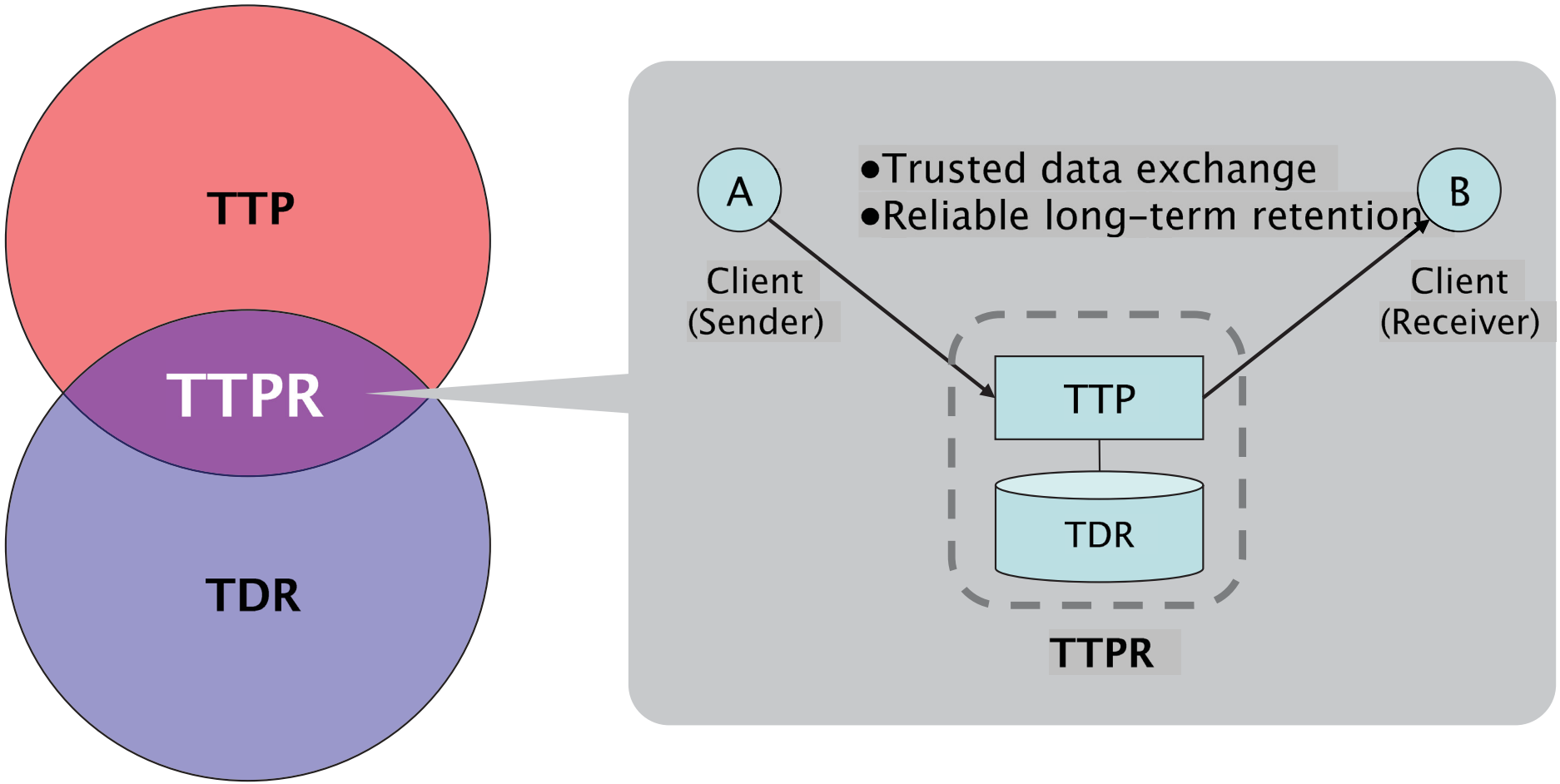
Overview

- **What is 'Trusted Third Party Digital Repository' ?**
- **Trusted Digital Repository (TDR)**
  - "A trusted digital repository provides reliable, long-term access to managed digital resources to its designated community, now and in the future." (OCLC/RLG, 2002, p. 5)
    - Accept responsibility for the long-term maintenance of digital documents
    - Demonstrate fiscal responsibility and sustainability
    - Design its system in accordance with standards
    - Establish methodologies for system evaluation
    - Have policies, practices, performances that can be audited and measured
    - Can be either local repository or third-party repository



Overview

- What is 'Trusted Third Party Digital Repository' ? (TTPR)



Background of trusted 3rd party digital repositories

Industrial

- Ensuring e-document's reliability and authenticity
- Building trust between e-document exchange parties
- Promoting e-business and improving business efficiency and speed

Legal

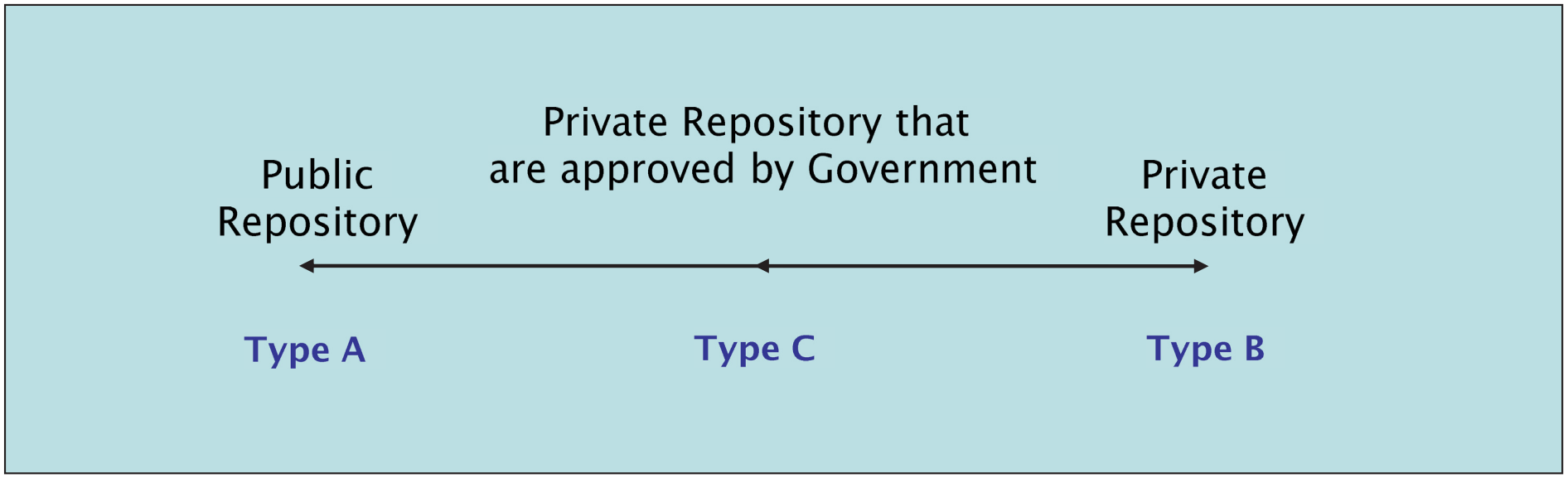
- Resolving relevant laws and regulations into unified requirements in dealing with e-documents
- Offering legal, procedural and technical standards in establishing digital repository
- Endowing scanned documents with legal authority

Technical

- Based on development of security technology and storage technology
- Supporting electronic document exchange and sharing

Types of trusted 3rd party digital repositories

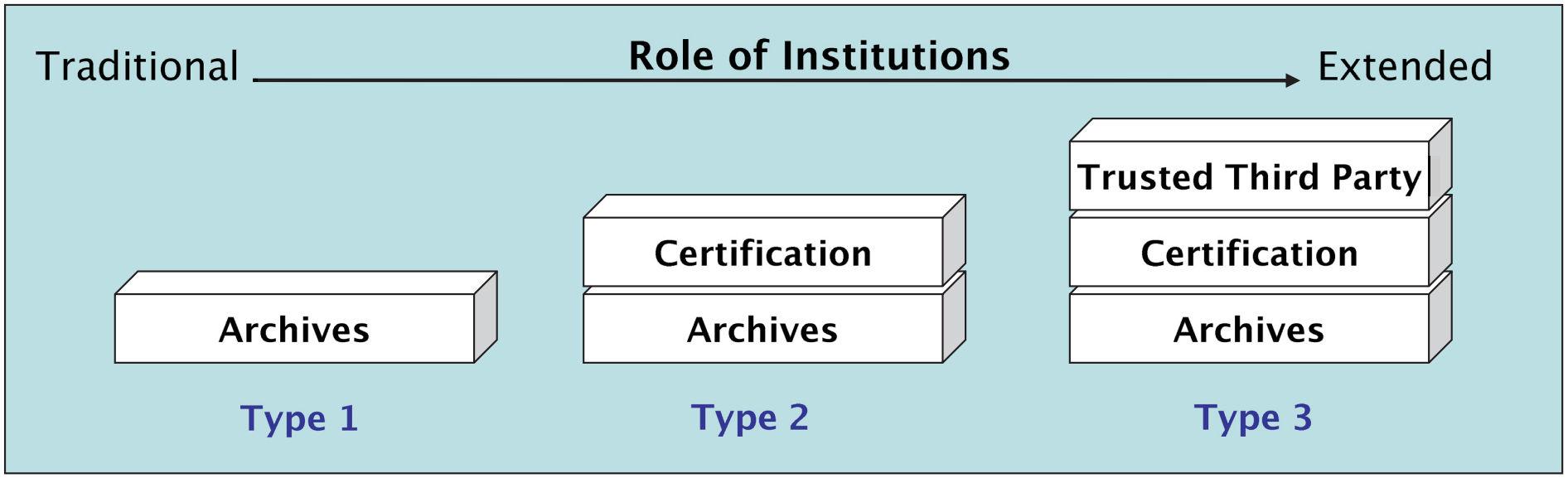
◆ By Types of Institutions



- Type A: Official repositories that are governed and operated by Government (e.g. US, Spain)
- Type B: Commercial repositories (e.g. US, Iron Mt.)
- Type C: Commercial repositories that are approved by Government (e.g. Korea, Japan)

Types of trusted 3rd party digital repositories

◆ By Major Role



- Type 1: Archives retaining and preserving e-documents (e.g. US Iron Mt., Spain)
- Type 2: Archives + Certification or Notarization of e-documents (e.g. US, Japan)
- Type 3: Archives + Certification + Trusted Third Party (e.g. Korea)

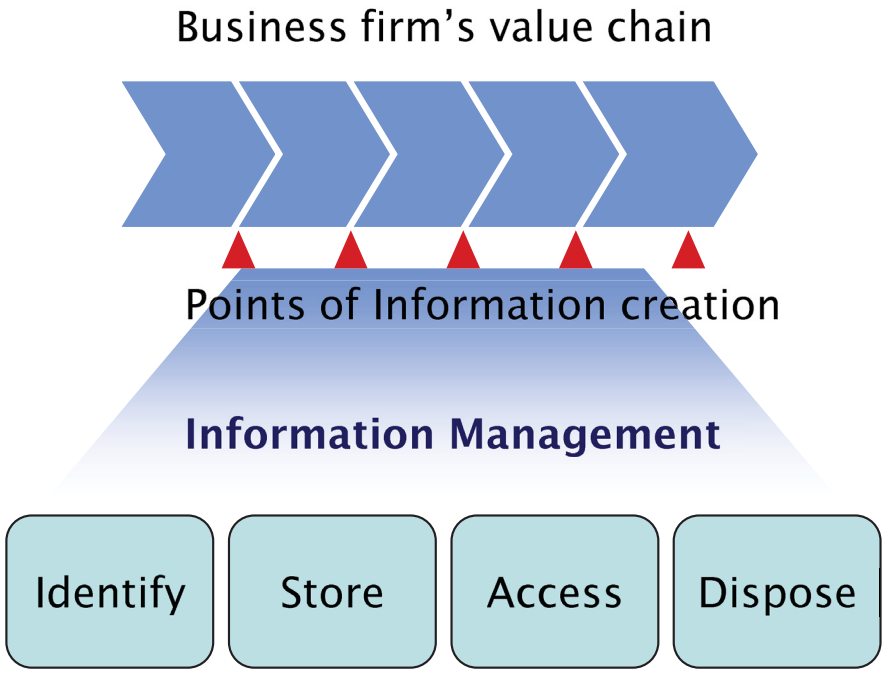
Types of trusted 3rd party digital repositories

- **Matrix of Roles and Institution Type**

Roles		Types of Institutions	
TTP + Certification + Archives		Certified e-Document Authority (Korea)	
Certification + Archives		e-Notary by notary assc. (Japan)	e-Notary by lawyers (US)
Archives	Gov agencies (Spain, US?)		corporations (US)
	Public		Private

Case 1. Archives model

◆ Iron Mountain, US: secure storage and destruction



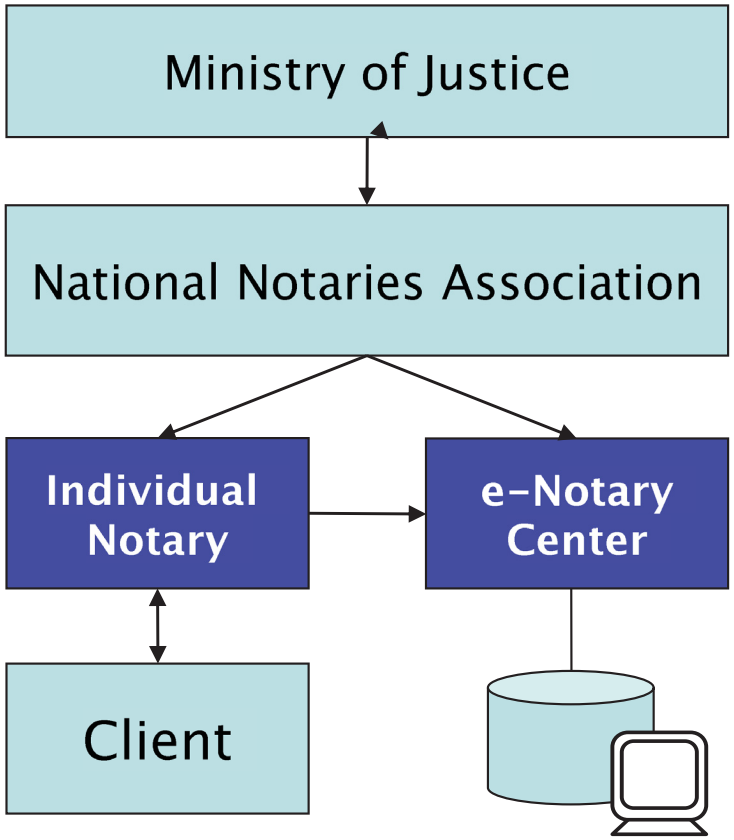
IRON MOUNTAIN®

- **Founded in 1951**
- **Offices in 37 countries**

- **Records Management & Shredding**
  - Records Management (paper, digital)
  - Secure Destruction
- **Data Protection & Recovery**
  - Server Data protection
  - PC Data protection
- **Digital Services & Software**
  - e-Discovery
  - e-mail Management
- **Fulfillment Services**
  - Inventory Management
  - On-time document delivery

Case 2. e-Notary model

◆ National e-Notary System, Japan

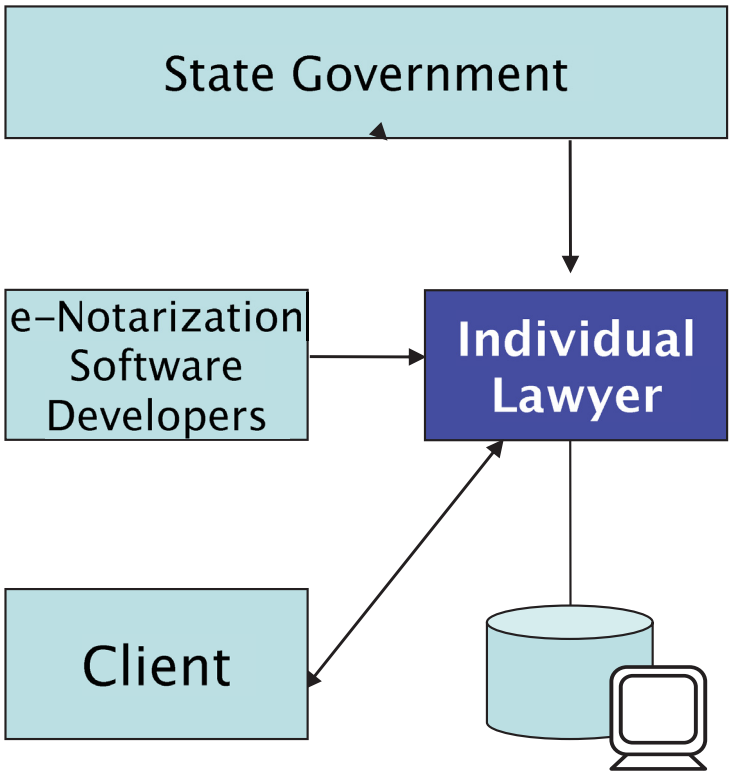


- **Amendment of Notary law in 2000**
- **Started in 2002**

- **Ministry of Justice**
  - Established rules and regulations on electronic notary
  - Issues electronic certificates
  - Authorize and supervise notaries
- **National Notaries Association**
  - Runs 'e-Notary Center'
- **Individual Notary**
  - Create electronic notaries
  - Notarize electronic private document
- **e-Notary Center**
  - Retain e-notarized documents for 20 years
  - Outsourced by Hitachi Co.

Case 2. e-Notary model

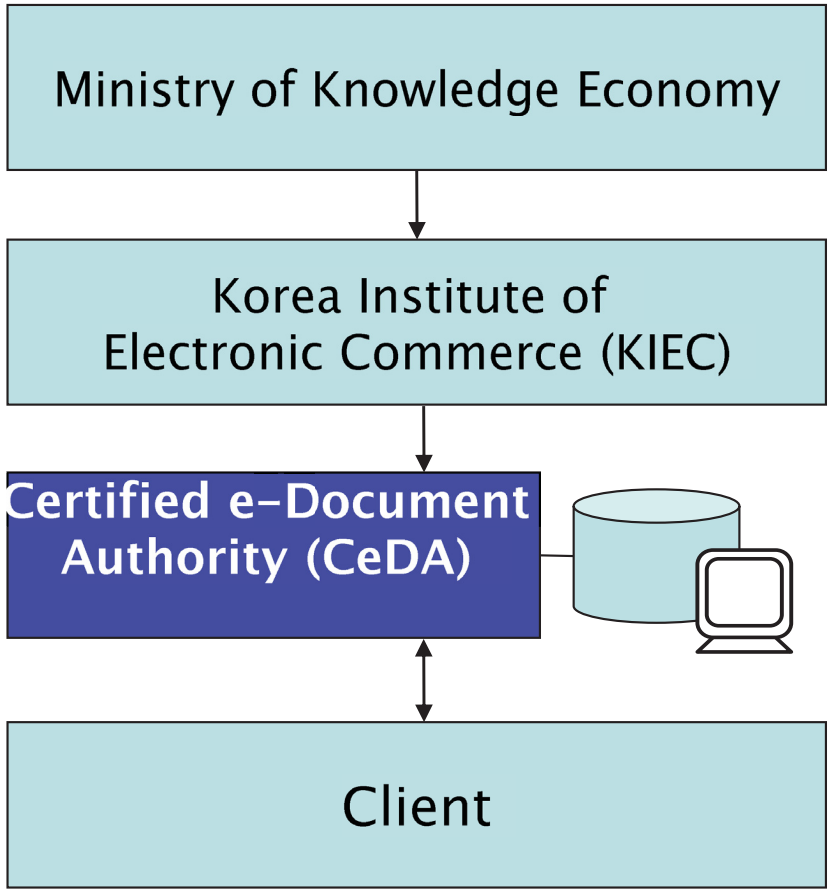
◆ e-Notary, US



- **State Governments**
  - Amend rules and regulations on notarization for electronic documents
  - Specify procedural, technical standard regarding e-notary
  - Many states are in operation or in progress of e-notary planning
- **e-Notarization software developers**
  - Develop e-notarization software in accordance with standards
  - Provide the software to each lawyer
- **Individual Lawyer**
  - Create electronic notaries for private document
  - Store e-notarized documents in their computer systems

Case 3. Combination model

◆ Governance of CeDA



- Establishing relevant acts and regulations
- Supervising KIEC's activities
- Authorizing each repository as the Certified electronic document authority (CeDA)

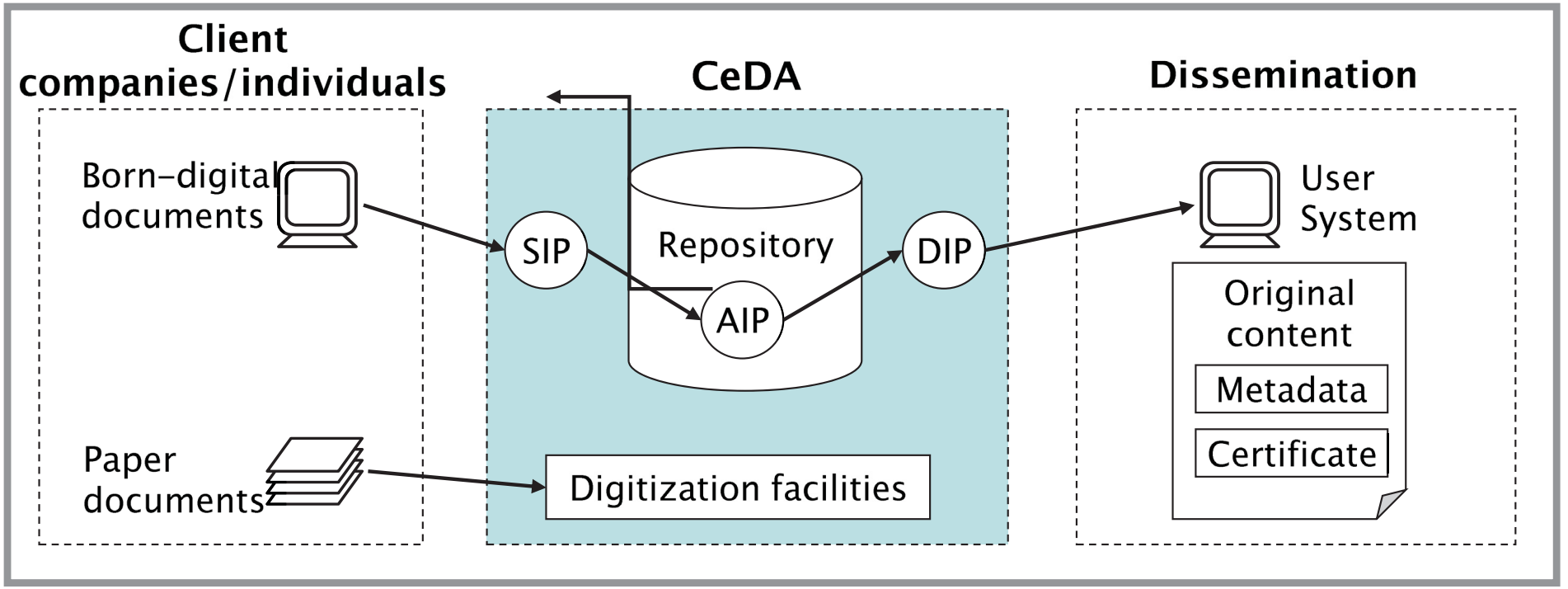
- Evaluating potential candidates for private service provides
- Setting up technical standards and guidelines

- Archiving e-documents
- Exchanging secure e-documents
- Certificating the retained e-documents

- Private businesses
- Individuals

Case 3. Combination model

◆ **Certified e-Documents Authority (CeDA), Korea**



- **Official repository that ensures e-document's reliability**
  - Preserving born-digital and digitized documents
  - Ensuring legal authority of all retained documents
  - Certifying the lifecycle of e-documents
  - Being as an Intermediary for secure e-document exchange between parties

Issues

- Repositories may vary in their major role, organizational structure and governing body by each country's contexts.
- Each repository seems to have some ways to ensure authenticity, reliability and integrity of electronic documents by:
  - legal requirements;
  - technical specifications; and
  - operational procedures.
- However, we have some questions.
  - Do the repositories function appropriately?
  - Do the current methods to ensure authenticity, reliability and integrity of electronic documents appropriate?
  - How do they deal with loss of retained documents?

Further questions

1. **Governance**
   - Are laws and regulations appropriate for establishing repositories?
   - Do government agencies monitor and auditor repositories on a regular basis?
2. **Management**
   - Do the repositories contain sufficient capability in technical expertise, managerial and operational expertise, and human resources?
3. **Budget**
   - Who finances for establishing and operating the repositories?

InterPARES 3 Project

International Research on Permanent Authentic Records in Electronic Systems

Thank you!

For questions, contact:
Eun Park at eun.park@mgill.ca