International Journal of Engineering & Technology, 8 (1.4) (2019) 606-615

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



A Metadata Schema Design for Global e-Apostille Processing and a Consortium Blockchain-based Certificate and Verification Framework for e-Register Service

Eunjin Yoo[1], Geunseong Jung[1], Jaehyuk Cha[1]*

[1]*Department of Computer Science, Hanyang University, Seoul, Korea*
Corresponding author E-mail:yooidol, aninteger, chajh@hanyang.ac.kr

Abstract

Whenever public underlying documents are required for international legal contracts, such as admissions, petitions, and employment, the document often has complicated authentication process. The most exhaustive part is the proof of origin as most countries' civil laws do not allow foreign documents as is. Therefore, the foreign applicants should prepare their documents such that they are valid in the destination country. The Apostille Convention helps reduce the complexity of the legalisation process. As an agreement to simplify the certification procedure between countries, it allows them to skip many authentication processes between the Apostille member States.
The electronic Apostille program (e-APP) deals with digital documents for the Apostille Convention. However, only a few States support e-APP because of the legislative and procedural differences in electronic documents. For global proliferation of e-APP, the process has to be standardized between States. In this paper, the information for a certificate verification system does not depend on the type of the format of e-Apostille and public documents and design the structure of data sharing and verification system for global e-Register service. The proposed e-Register service consists of a consortium block chain to prevent monopolizing of the data and ensure availability to all.

Keywords: *Apostille; Blockchain; Document verification system; Public document*

1. Introduction

An underlying document for a given contract is formatted in various ways in different countries. Thus, when a document is used in other countries, additional mandatory attachments, such as a translation certificate for the content's accuracy and other documents for proof of origin are also required. The discrepancy between countries' laws causes the documents to generally be confirmed manually, even if the electronic government system can handle the documents in an automated process. These complex processes cause inefficiency in international dealings, contracts, and administration [1].

The origin of documents need not be verified on the principle of "*acta probant sese ipsa*": the origin of the document lies in the document itself. Thus, all documents' origin need not be proved in the issuing country unless they are forged. However, if the document is used abroad, the origin of the documents must be verified as the national laws differ. Fortunately, the Apostille Convention is an agreement to simplify the certification procedure of official documents between the member countries of the Hague Conference on Private International Law (HCCH). All of the 82 HCCH members can reduce costs through the Apostille Convention as it allows several attachments for proving the origin to be replaced by a single Apostille (Fig. 1) [3].

Even though the Apostille simplifies the oversea process, it cannot connect different countries' systems. Though HCCH' Apostille Certificate model was broadly accepted by its members, the model defines what format the Apostille should have and not how it is handled by each government, especially through the Internet. To confirm the document's origin overseas, as mentioned above, numerous foreign diplomatic procedures and preparations such as translations, authentication, signatures, seals, and certifications are needed. This process, called legalization, is essential but difficult to be claimed directly through the government as foreigners are generally prohibited from accessing the e-government because Internet privacy laws are stricter then offline procedures. Eventually, the majority of such overseas requests are forced to use other methods, such as phone call, post (e-mail), foreign agent, or visiting even with proper documents and materials [2][23].

Thus, the Electronic Apostille Program (e-APP) was launched to prepare electronic government system. e-APP consists of e-Apostille that handles issuance of Apostilles in electronic format with a digital certificate and e-Register the online Apostille registers to verify the Apostilles' origin (paper and digital format). Despite the HCCH advising its member States to operate the e-APP system for efficient and modernized Apostille service, only 56 States of its 133 members have installed the e-Register system. The challenge is for the Apostille to have more complicated agreement between parties on digital format and system, such as electronic document, online privacy, and online authentication.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Therefore, many States hesitate to develop e-APP system. Moreover, all information regarding the Apostille Certificate should be provided when a person enquires about issued Apostille. Most e-Register services of member States, however, receive requests only through phone, e-mail, and other manual ways, and not through their online system. Further, as of 2015, only 16 States can provide Apostille information on their e-Register service. Therefore, the Apostille model suggested by HCCH does not guarantee interoperability in electronic document system between countries. For stronger compatibility of international document exchange, the member countries should standardize their rules and laws concerning documents and contracts. Unfortunately, contract laws are one of the most sensitive parts of civil laws in every State and changing these laws is an onerous task for the members. Furthermore, HCCH does not force its members to revise their laws because of their convention or guidelines as long as it exists in the international conference without legal binding power over every member.

Thus, a new standard is needed to satisfy each States' Apostille Certification process without infringing upon their State laws. The current standard of underlying document is therefore, not practical. However, rules on their documents and processes can be defined such that converting States' every original document and Apostille into the proper formats and procedures for other destination States to greatly improve interoperability between the member States. A State, despite having the Apostille Certification that has not supported e-APP because of the cost of establishing e-APP or concern regarding the amendment of their electronic privacy/document related laws can easily adopt the e-APP system by following the predefined rules as system guidelines for their existing document procedure [2].

Even if the standardization of documents and its procedure between the States is established, these documents always consist of greatly sensitive personal information because of which the countries might prevent sharing data to protect their people's privacy even if the person allows his or her information to be used for their own business. In recent years, several governments have operated a public digital archive to resolve the problem of transferring electronic documents from the applicant to the recipient in domestic businesses [5–6][15]. In most countries, the archive can store or access the documents containing personal identification because it belongs to the national institute. In an international situation, on the other hand, the foreigner's identification data is required for allowing them to access the data that must be kept secure at all cost. Thus, every State must establish an agreement to designate a completely safe place for accommodating each citizen's personal information. However, this place is likely to controversial for information monopoly even if proved safe enough.

Consequently, any State participating in the Apostille Convention must install a policy allowing any member States to store or access the Apostille archive at any time even if a State does not want to endure the cost of the e-APP services. All States must have equal rights to the stored global Apostille data. Existing server synchronization, such as cloud computing models, finds it difficult to meet these conditions because each State has exclusive ownership of their servers as well as to the data within. However, blockchain technology can help to resolve this problem. All States can create a blockchain network as a peer-to-peer network data storage, wherein every participant has even rights and bears equal maintenance costs at the beginning. Over time, the States with more users will have to pay more to maintain the network; however, other States' rights to use the network will remain. The blockchain network does not impair the principles of the Apostille Convention and helps any State that is hesitating to establish new e-APP service as it can just allow the State to join the network.

In this paper, we provide a detailed metadata schema to ensure interoperability for every Apostille Convention States' procedure. We also discuss a blockchain-based e-Register service that can involve every Apostille State without having them make major changes to their own government systems for global e-APP use.

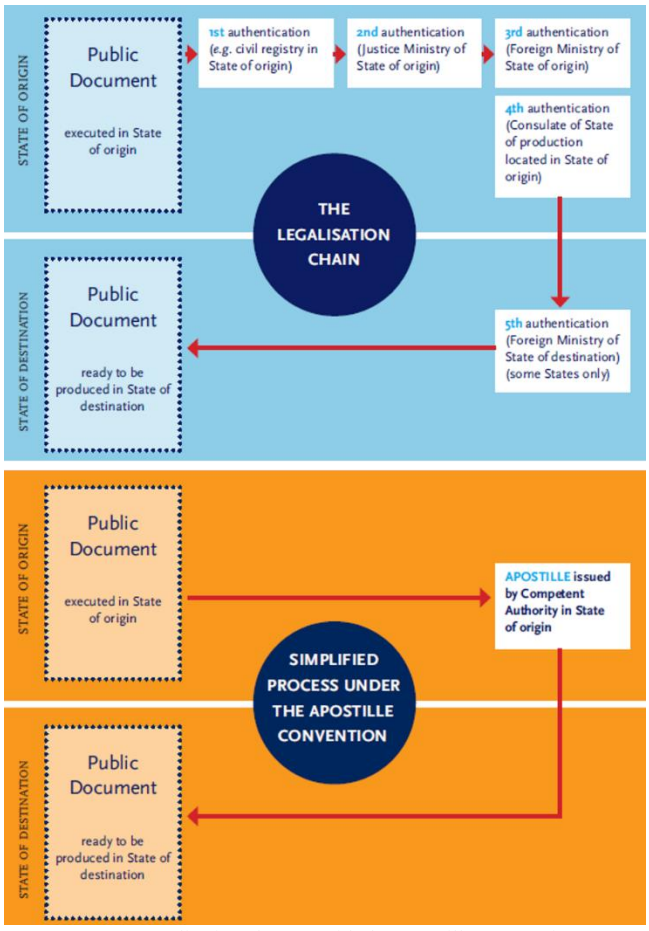


Fig. 1: Legalisation changes with the Apostille Convention

2. Related Work

2.1. The Apostille and e-APP

The Apostille Convention, originally *the Hague Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents*, is an international treaty that specifies that the modalities of a document issued in one of the signatory States (typically, the HCCH members) can be certified in all the other signatory States. The States issuing a document attach a special certificate, called an Apostille, verified by other States. Any recipient of a public underlying document can verify if the document has the right Apostille [1].

The e-APP was launched to keep pace with e-Government initiatives of most modern governments so that more public underlying documents can be used in an electronic form on an electronic government system. Although the e-APP can reduce considerable paperwork with automating issuance of the Apostille Certificate, deploying a new government system is always demanding.

Moreover, the Apostille should inevitably carry significant diplomatic pre-task. The e-APP not only includes the format of the Apostille but also allows access to online operations of Apostille registers, which is exceedingly hard work for most governments. Nonetheless, several States are running the e-APP as it is a more secure, efficient, flexible, and green technology. The e-APP is composed of e-Apostille and e-Register. The e-Apostille issues Apostilles in an electronic format with a digital certificate, while the e-Register handles operations of Apostille registers in an electronic format than can be accessed online to verify the origin of paper and e-Apostilles.

Table 1: Category of e-Register

Functionality	Category	Information displayed
Basic	1	"Yes" or "No"
Additional	2	Category 1 + information on Apostille and/or underlying document (possibly visual check)
Advanced	3	Category 2 + digital verification of Apostille and/or underlying document

The e-Register manages the methods, technology, and services required for Apostilles to be saved in an electronic format and accessed online. As the e-Register
is not necessarily free of the other item, the e-Apostille, in the e-APP, the e-Register was designed to handle both Apostilles in the conventional document format as well as e-Apostilles in electronic form. Thus, if the issuing office has an e-Register, then the concerned parties can use it to verify information in the Apostille regardless of the format. The HCCH categorizes the stages of the e-Register, as shown in Table 1, according to the level of information it provides and recommends that the e-Register be built in compliance with these stages. Stage 1 lets the user know if an Apostille was issued, Stage 2 allows users to verify information on the issuance of an Apostille, and Stage 3 allows users to verify information that guarantees the Apostille's electronic signature and integrity. Countries that offer Stages 1–3, as of 2015, include Spain and seven other countries [2][3].

2.2. e-APP Operational Status by States

2.2.1. Colombia

Colombia introduced e-Apostille in 2007 and launched the online application service in 2008. It provides e-Register in category 3 (advanced). To certify an Apostille, a physical document (paper format) is necessary. Though electronic documents are not allowed, scanned ones are available. The Apostille applicant can visit the office or apply online. When the application is received, the officer checks the content, seal, signature, and other relevant information and sends a payment request to approve the Apostille. The Apostille is then emailed to the applicant after successful payment. Fig. 2 shows the usecase of the Apostille issuing process in Colombia.

2.2.2. Moldova

Moldova joined HCCH and the Apostille Convention in 2007 and launched the e-APP in 2013. Moldova, like Colombia, also provides e-Register in category 3 (advanced). While the issuing process of Moldova is similar to that of Colombia, there are some differences. Though Moldova also accepts only a physical document for issuing Apostille, its government supports electronic signature that enables authentication and signing documents in cyberspace, using a cryptographic USB device, card, or even mobile phone. After the payment, the applicant can download the e-

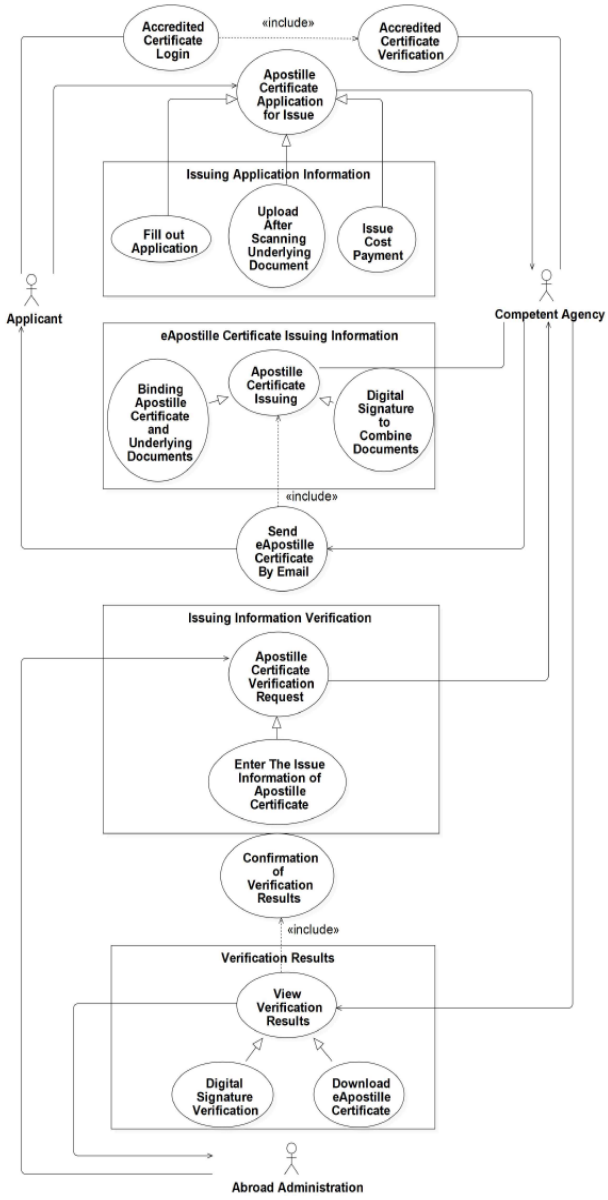


Fig. 2: Usecase of e-Apostille process in Colombia

Apostille from the government's webpage. The Apostille certificate, however, cannot be used without a security code that is sent to the applicant's email. As shown in Fig. 3, Moldova has a more versatile e-APP service than Colombia.

2.2.3. New Zealand

New Zealand launched the e-APP in 2009 with category 3 e-Register. Unlike Colombia and Moldova, New Zealand supports electronic documents as well as physical documents, and thus, New Zealand applicants can send their electronic documents on e-mail directly without printing and scanning. The applicants can also submit the underlying documents by post if they have a physical format of the document. After their issuing request is accepted, the Apostille will be sent to them by e-mail whether the document format is physical or electronic.

2.2.4. Spain

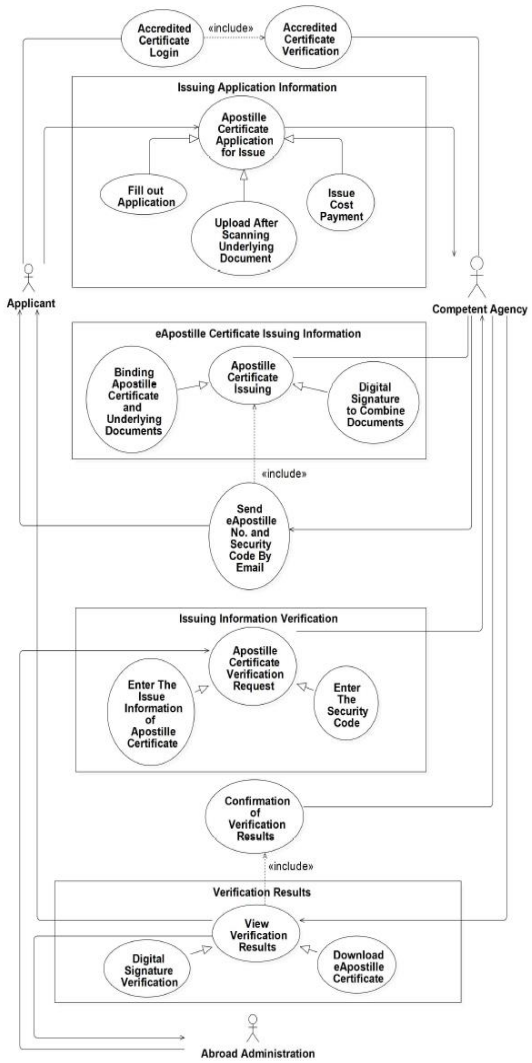


Fig. 3: Usecase of e-Apostille process Moldova

Spain has an operational e-APP and category 3 e-Register system since 2011. Similar to New Zealand, Spain accepts both physical and electronic formats, but every applicant has to attend the office even if they submit the document in electronic format with digital storage and signature. Besides, there is no issuing fee in Spain.

2.2.5. Republic of Korea

Republic of Korea has established an e-APP and category 2 e-Register system since 2016. This allows the Korean applicants to determine whether the Apostille and e-Apostille exists through the Internet but does not allow them to download the Apostille online. The applicants can get by visiting office or print it rather than download it, as Fig. 4.

2.3. Metadata for Public Document and the Apostille

Metadata is data that provides information about other data. There are three types of metadata: descriptive metadata that describes resource for purposes, structural metadata that indicates relations between objects within the data, and administrative metadata that manages the data.

2.3.1. ISO 15836: Dublin Core

Dublin Core is designed to describe both digital and physical resources [2]. The metadata presented by the Dublin core establishes common elements of various digital and physical resource. Table

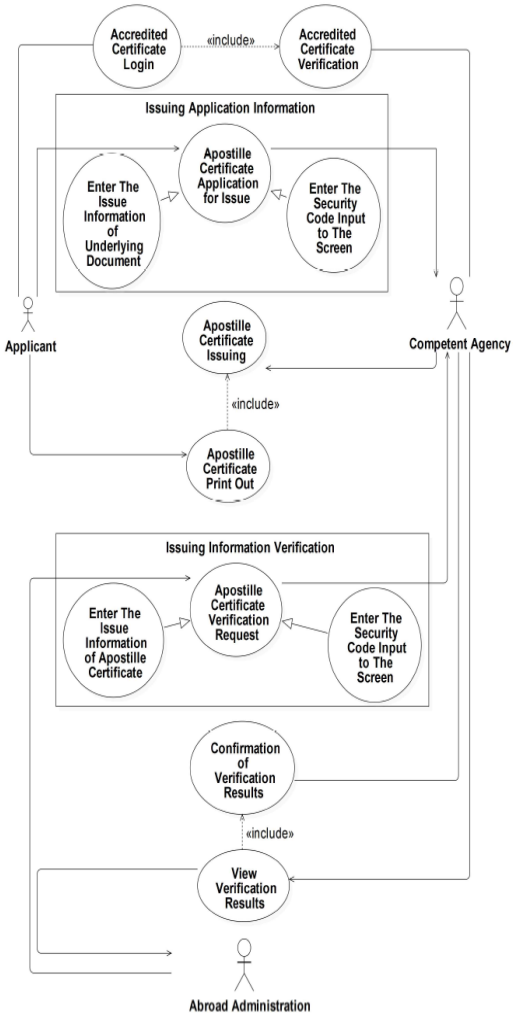


Fig. 4: Usecase of e-Apostille process Republic of Korea

2 shows Dublin Core Metadata Element Set (in italic) and the Dublin Core Metadata Initiative (DCMI) Metadata terms. Each Dublin Core element is optional and may be repeated.

As Dublin Core is simple structuring of any data resource, an author or a publisher can directly create metadata of their own resource. These characteristics, however, may increase ambiguity of metadata and make it difficult to retrieve the data while decreasing interoperability. Despite these minor shortcomings, Dublin Core is a useful base of metadata model for exchange of public document systems.

Table 2: Metadata from Dublin Core

Dublin Core Metadata Element Set and DCMI metadata terms		
abstract	educationLevel	modified
accessRights	extent	provenance
accrualMethod	*format*	*publisher*
accrualPeriodicity	hasFormat	references
accrualPolicy	hasPart	*relation*
alternative	hasVersion	replaces
audience	*identifier*	requires
available	instructionalMethod	*rights*
bibliographicCitation	isFormatOf	rightsHolder
conformsTo	isPartOf	*source*
contributor	isReferencedBy	spatial
coverage	isReplacedBy	*subject*
created	isRequiredBy	tableOfContents
creator	issued	temporal
date	isVersionOf	*title*
dateAccepted	*language*	*type*
dateCopyrighted	license	valid
dateSubmitted	mediator	
description	medium	

2.3.2. ISO 15489: Information and Documentation–Records Management

ISO 15489, developed by the Working Group (WG1) of SC 11 under ISO/IEC 23081, defines the key concepts and principles for generating and managing records [16]. ISO 15489 establishes metadata as "the context and content of records, structure and history of records management over a period of time." It also presents metadata for technology area of records. Metadata for the classification and functional framework required for location of records should be produced within ISO 15489 documents, and thus, Shepherd and West complied with ISO 15489. Table 3 presents the elements of ISO 15489 as per the area.

Table 3: Metadata from ISO 15489

Record Description	Record management and control
Unique identifier	Location
Title	Status
Date/time	Ownership
Extent	Responsibility
Technical requirements	Retention action
Creator(s)	Retention policy
Function	Access conditions
Classification	User history
Relationship(s)	Format/migration action
Indexing	Format/migration policy
Arrangement	Version control
Authorized amendments	

2.3.3. ISO 23081

Similar to ISO 15489, ISO 23081, developed by the Working Group (WG1) of SC 11 under ISOTC 46 (Information and Documentation), defines the principles of controlling metadata in production, management, and utilization of metadata [16]. It provides the metadata management guidelines for records and establishes the standards for defining the content, structure, and properties of records or collections of records.

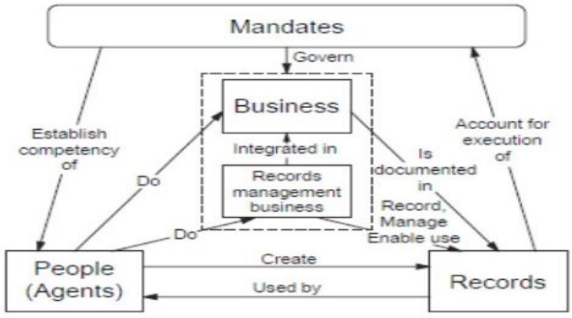


Fig. 3: Process Model from ISO 23081

2.4. Blockchain

Blockchain refers to a peer-to-peer (P2P)-based data storage system or model that is designed to grow continuously as small pieces of data, called blocks, form a list [4]. As the connection between blocks is encrypted, it is impossible to determine without information on the previous block. Thus, the data record list grows continuously in the form of a distributed database so that it cannot be manipulated by users. The most important characteristic of the blockchain is that though anyone can view the information, no one can alter the data without authorization. Therefore, blockchain is utilized not only as a core technology for various cryptocurrencies that use decentralization as their mechanism, but also in various fields as a technology that is independent from cryptocurrency [7][8]. Blockchain can be further classified into public, private, or consortium blockchain. Anyone can participate in a public blockchain, whereas only those with approval for a certain node that monopolizes all rights can participate in a private blockchain [8][9]. On the other hand, a consortium blockchain is operated after distributing rights according to the initial consultative body's intentions and determining the policies regarding the blockchain's operations.

Structurally, the blocks in the blockchain are composed of a header that contains the overall content and the body that expresses the data (transaction) that the block contains. The head must include the results of the previous block (Pre_HASH), and the block's data summary and timestamp can be determine according to the user's request. In the body, the actual data that the block will contain is included as a transaction. The generated blocks share the information from the block with the user or share the integrity of the information.

2.5. Package File

Package file is an Application Programming Interface (API) that installs, manages, controls, and removes a software [18]. It provides a proxy that grants users minimum amount of access required to administer software [19]. Package files not only make it easier to distribute software but also provide a standard format for component management. Moreover, it allows users to perform an appropriate installation process depending on the operating system or other environment. The components of a package file may include program files, folders, COM components, registry keys, and shortcuts.

2.5.1. Microsoft Install Package

Microsoft extended the COM structured storage to develop the Microsoft install package for their install solution called Windows Installer. Windows Installer Version 1.0 was first released in 1999 for Microsoft Office 2000 installer only [20]. Introducing Windows XP in 2000, Version 2.0 was released and was redistributable for Windows 9x, 2000, XP, and Server 2003. The current stable version was released in 2009 as 5.0 for Windows 7 and later. This package contains all the information necessary for Windows installer to run the user interface to install and uninstall applications and consists of the following components [21]:

- *.msi* file and any external source files
  Internal and external source files, cabinet files for installation.
- *Installer database*
  This consists of a relational database of the information required to install a group of applications. The database tables reflect the general layout of the installing applications that includes available features, components, relationship between features and components, necessary registry settings, and user interface.
- *Summary Information Stream*
  This is used to contain information about the package on Microsoft Windows Explorer and other applications and to contain properties used by the installer.
- *Digital signatures*
  This is used for validating the installer and the application.

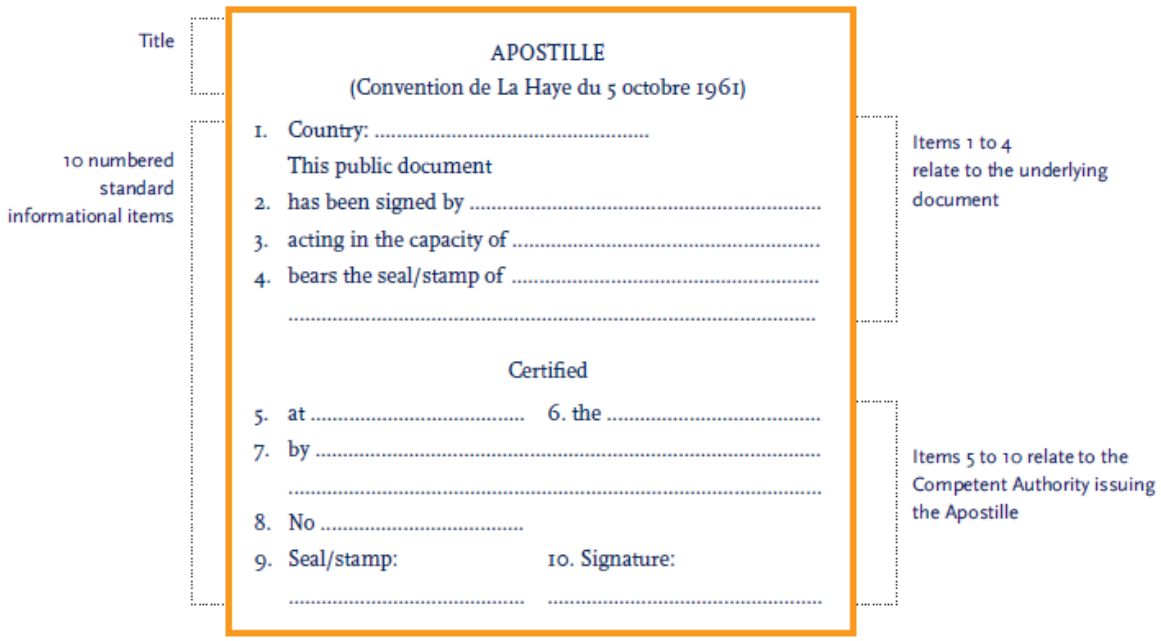


Fig. 6: Model of the Apostille Certificate from the Apostille Convention

2.5.2. Question and Test Interoperability (QTI)

IMS global learning consortium distributed IMS Question & Test interoperability® (QTI) specification, based on the IEEE LTSC P1484.17 standard**,** to enable the exchange of item and test content and results data between online learning applications, platforms, and infrastructures, such as authoring tools, item banks, assessment delivery systems, and scoring/analytics engines [22]. The QTI content package provides searchability, system interchange, and reuse of learning materials. It consists of the flowing components:

- *Top-level Manifest*
  An XML file to describe the entire package.
- *Metadata section*
  An XML file to describe the manifest.
- *Organizations section*
  An XML file to argue the cardinality of organizations.
- *Resources section*
  An XML file to describe metadata of resources and references to external files and media elements.
- *Sub-Manifest*
  Optional manifest properties.
- *File Resources*
  Resources using item such as media, texts, graphics, and other data.

3. e-Apostille Metadata

3.1. e-Apostille Certificate Model

Fig. 6 shows the original Apostille Certificate established by HCCH that was used by the member States. The e-Apostille Certificate model helps the various member States to create their Apostille Certificate such that it is clearly identifiable to all other member States. It consists of data regarding the original document that will be certificated (Items 1 to 4) and the Apostille Certificate (Items 5 to 10). First, the former metadata should contain common properties that any underlying document would have, especially concerning the data that describes where and by whom the document was signed. Next, the Apostille metadata should detail that the State of origin has executed proper process for Apostille Certificate. Furthermore, more metadata must be placed so that each State can verify the document and the Apostille with their own digital document handling process.

3.2. Underlying Document Properties

As shown in Fig. 7, the properties from country that *bears the seal/stamp of* are visible on the paper document or the electronic document on screen. The rest properties, on the other hand, are hidden to human but not to the machines. The rest properties for machine processing will help every State to deploy a digital document format concerning their civil laws even if the State has not established electronic services. The additional properties are easy to standardize as they are based on existing standard documents: Dublin core, ISO 15489, ISO 23081. The details of the properties after *bears the seal/stamp of* are as follows:

- *format*
  It declares the storage type of the underlying documents.
- *uri*
  This property indicates location of the underlying documents and uses well-known electronic identifiers, such as uniform resource number (URN) or digital object identifier (DON).
- *contributor*
  The name of issuer of the underlying documents.
- *contributor position*
  The position of issuer of the underlying documents.
- *validity*
  The validity period of the underlying documents.
- *digital signature hash*
  A hash value of digital signature from the underlying documents validates the digital document and does not substitute a person's signature by hand, like a "wet" signature. The hash function is decided by States' digital encryption laws.
- *language*
  The original language of the underlying documents.
- *issued reason*
  The background written on issuance application when the document is first issued.

- *coverage*
  The number of the issued documents.

3.3. Apostille Certificate Properties

Apostille Certification has properties that indicate the competent authority of Apostille issuance, which are generally diplomatic offices and consulates of the destination State.

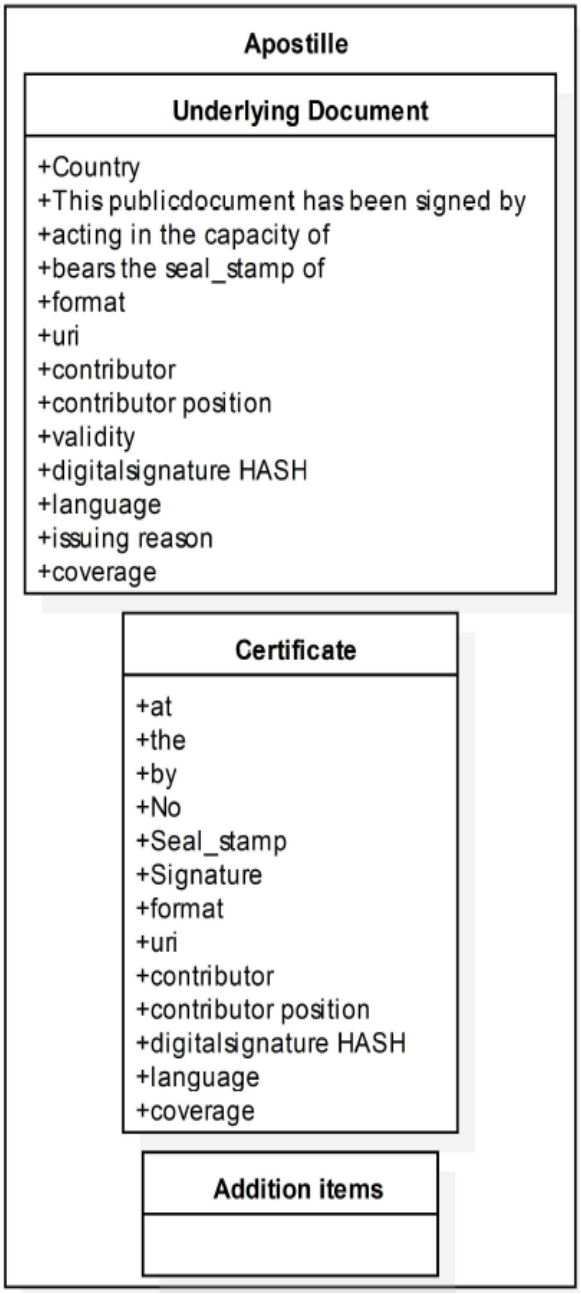


Fig. 4: Metadata for the underlying documents with the Apostille Certificate

- *at*
  The name of the place where the Apostille is issued, such as the city where the authority is located. It responds to the *place* from Dublin Core.
- *the*
  Issuing date. It also responds to the date form Dublin Core, ISO 15489, and ISO 23081.
- *by*
  This property asks who issued the Apostille Certificate, where typically the name or title of the Competent Authority is written though some authorities write the officer's name who issued the certificate. The Convention does not require the authorised officer to be named.
- *No*
  The number of the Apostille. As the Convention does not stipulate a rule to number the Apostilles, each authority must determine it.
- *Seal/Stamp*
  The seal/stamp of the Competent Authority is not a digital signature. If the certificate is issued in a digital format, the image or string data of the seal/stamp will be substituted.
- *Signature*
  The signature of the authorised officer. For most States, the officer issuing the Apostille applies his/her own signature. However, the convention dose not restrict how to sign the document and the signature depends on each State's law.

Other metadata for certificate are the same as the underlying document's properties though altered for the certificate document.

4. e-Apostille Verification System

4.1. e-Register System Requirements

Although HCCH member countries use Apostilles, the method and level of building the e-APP has not been made mandatory, and thus, each country's system is different. Unlike the Apostille Convention that bypasses differences in notarization methods between countries by limiting them to international usage, because building the e-APP is restricted by each country's electronic document format, electronic information protection, electronic signatures, and laws regarding personal information protection, it is more complicated to build a system than it is to apply Apostilles. These restrictions also make it difficult to access the country's electronic services, aside from residents or registered aliens. Though Article 7 of the Apostille Convention requires that Apostille information be shared with all concerned parties, it is practically impossible

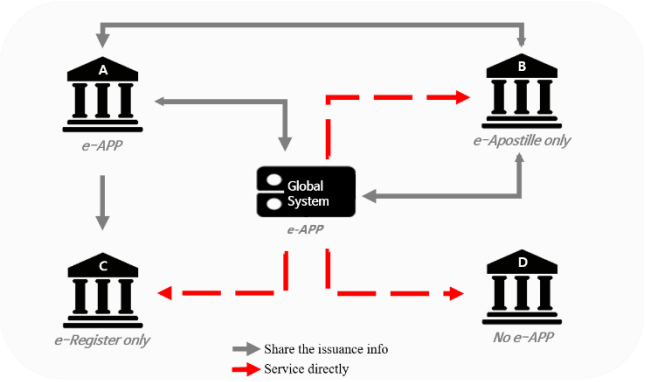


Fig. 8: Service scenario for blockchain based Apostille Verification System

for an overseas party to use the e-Register to verify an Apostille from the country of issuance. To resolve this problem using current methods, each country's system must be integrated and information on the issuance of all Apostilles must be shared and managed accordingly. However, national administrative systems are substantially large in size, complicated, and contain a considerable amount of sensitive information [5]. The majority of the countries prefer not to keep information on their nationals overseas when the managing agent is uncertain. Therefore, to enable the e-APP to become as widely used as Apostilles, it is necessary to build an e-Register that offers the same electronic verification system across all member countries. The first method for building a global e-Register service involved building a shared storage site in a region that can be trusted by all member countries and verifying that the Apostilles were stored at this site. This is advanta-

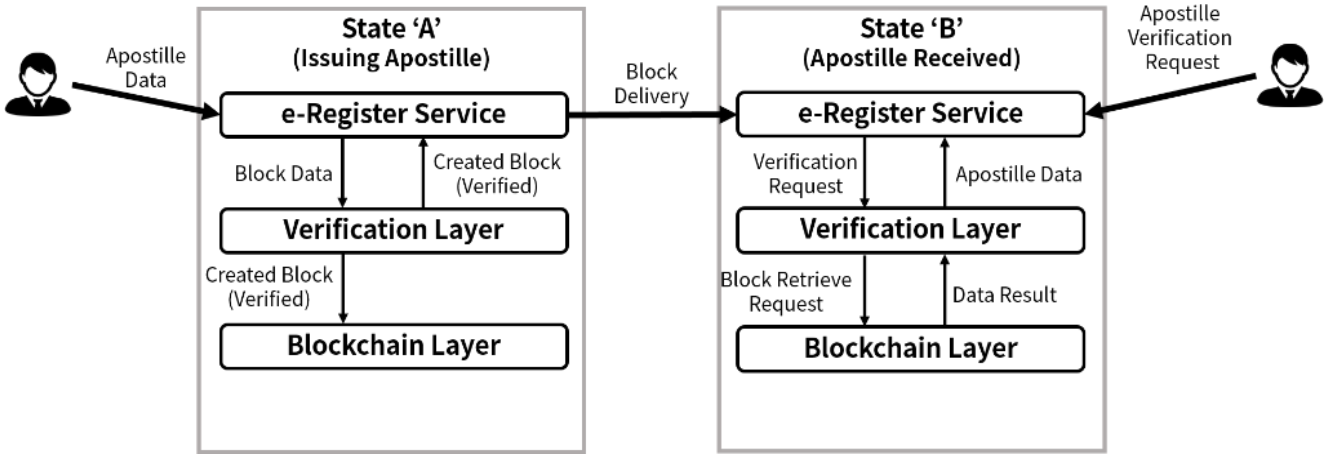


Fig. 9: Blockchain layers in the verification scenario

geous because it will integrate the diverse methods and levels of e-Registers that are built in each country, and help existing e-Register services and technology to be used without modification. However, because the data is concentrated in one location, a public storage site will be vulnerable to hacks; hence, there are difficulties in selecting a reliable location. Moreover, member countries that have already gone through great lengths to build an e-Register may have suspicions and object to building a brand-new system. Therefore, the two methods proposed in this paper are based on a distributed shared storage site based on a consortium blockchain, which is a partially privatized blockchain controlled through a pre-selected node. This can be used to build and manage a network between member countries. As the blockchain has characteristics such as all nodes having all or a portion of the data, anyone can view the blockchain but nobody can alter a blockchain once it has been added. This method can help in resolving complaints regarding information exclusivity by sharing with member countries, improving security, and building an e-Register that satisfies the condition of allowing a concerned party to view the Apostille information. Furthermore, as any data that can be registered in the form of a block in the blockchain can be stored without a fixed storage-site schema, the different e-Register verification methods, official document formats, disclosure levels, and Apostille authentication certificate formats of each member country will still be acceptable. Fig. 8 presents a situation of providing the global e-APP service to member countries A, B, C, and D including countries that have not established electronic services, depending on the level of the e-APP that is supported,. In this scenario, Table 4 shows the participating countries according to the level of e-APP that is supported among Apostille member countries [13].

Table 4: States Roles in the Scenario

Actor	Global service system and member States: A, B, C, and D	
Role	Global Service System	Support full e-APP capabilities
	State A	Support full e-APP capabilities
	State B	Support e-Apostille only
	State C	Support e-Register only
	State D	No electronic Apostille support

The shared blocks in this blockchain system can be defined as shown in Fig. 10. The data required to create a blockchain includes "Sid," "timestamp," and "pre_HASH," and the data for verifying the validity of an Apostille authentication certificate are "data" and "country." The issuing country will package information concerning the facts of issuance for the verification of the validity of an Apostille authentication certificate and turn it into a block, which will be used in the e-Register. In addition, although blockchain does not require revealing the origin of the block's creation and the Apostille system does not need separate information on the country of issue because the country of issue is the one that guarantees the Apostille, the country is differentiated through the 'country' value. Moreover, because there are diverse documents that must be verified according to each country's policies and it is necessary to implement a separate verification procedure, this value also serves as a metadata factor [10]. Each country can connect the necessary information when handling electronic documents in accordance with the country's laws through the data's Uniform Resource Identifier (URI). These may be package files with a bundle of simple values, strings, images, or more complex information as there are various forms of data that are necessary for each country's laws and environment and there must be a method of expression for that metadata. Therefore, because the document expression method that is expressed in the URI and document-verification mechanism may differ for each country, it is necessary to have a design that allows the blockchain registration and the relevant portion to be operated independently [11–13]. Through a separated design, member countries can use a verification mechanism that suits their own environment.

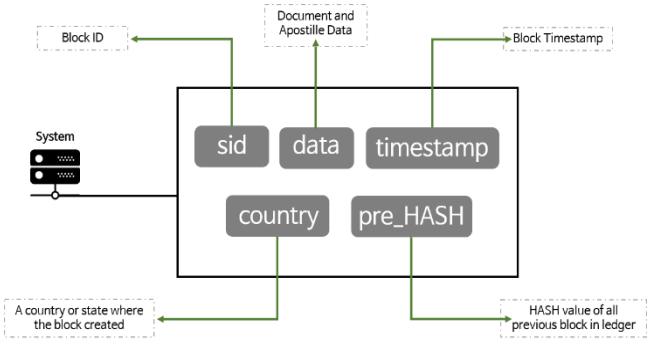


Fig. 10: Block structure

For the global e-APP service that is composed using a consortium blockchain, only approved institutions that are designated by member countries can participate in the network. Each country can perform actions such as create, deliver, add, read, and discard blocks. However, because blocks cannot be discarded in the blockchain technology, a discard flag is used instead of actually discarding data so that the validity of the shared block can be examined. This guarantees that the same product are controls in the database of the institution that will be storing information on Apostille authentication certificates if a separate linked system is created for the administrative convenience of the country [4][14][15]. Therefore, even if the block is in the blockchain, if it was already discarded and does not exist in the system of the country of issuance, it is replaced by a deletion flag in the blockchain.

4.2 The Blockchain Verification System

The system we proposed above has three essential layers: the e-Register Layer that has the e-Register interface, the Verification Layer that verifies Apostilles, and the Blockchain Layer that controls the blockchain ledger. There are two main categories of system users: users who are affiliated with the institution of the country of issuance that can issue Apostilles and concerned parties who want to check Apostille information. The latter category of users can be anyone.

When a user with the rights to issue an Apostille delivers the Apostille authentication certificate, Apostille official document, and the shared data that includes the metadata through the e-Register server, the shared data is verified in the verification layer according to the country of issuance's e-Register stage. After the country of issuance is determined through the block's "*country*" value, the data is verified to match the environment of the country's laws. This procedure can be designated by the country of issuance or modularized and applied through a discussion between countries. Once the data is verified, the block is generated by including values for generation, such as "*Sid*," and the generated blockchain layer containing block is added to the sharing ledger. At the same time, the block is generated to a different e-Register server node through the e-Register server layer. The other e-Register server that receives the block checks whether it is correct through the *pre_HASH* data before adding it to its block chain.

The concerned party will need the issue number and date to verify the authentication certificate of an Apostille or e-Apostille or to make a request to verify the facts of issuance. This data is stored in the block's data area, and the verification layer finds and converts the block with the relevant values through the blockchain layer. The verification layer verifies the integrity of the converted block and returns the relevant information to the e-Register's server up to the level of the e-Register that is supported by the country of issuance based on the block's "*country*" value. Though the global system supports all stages of the e-Register, the information that is shared differs according to the requests of the country of issuance.

4.3 Blockchain Ledger and State ledger

Originally, every user in blockchain from bitcoin shares only one ledger that contains all transactions that have been confirmed on the blockchain. Everyone can check the transaction details if they have valid hash values, even if they are not participants in the network. Fig. 11 shows the bitcoin transaction explorer from 'blockchain.info.' When users send or receive bitcoins, the transaction generated with unique hash value. Basically, the couple of users who made a transaction would know the hash value of theirs. If someone got the hash value for a certain reason, he or she can easily retrieve the information of the transaction: time, total sent, relayed Bitcoin node, and user hash value who's sent or received the Bitcoin.

However, the hash value, typically encrypted hash (e.g., SHA-256 used bitcoin mining 1024 letters in binary or 64 letters in hexadecimal), is inconvenient and not readable to people. It is also much slower than the existing relational database based retrieval service that most governments nowadays use. Furthermore, e-APP must enable the physical (paper) format document, which can also be stored in the digital database in most developed countries where e-government systems are actively used.

Therefore, the verification layer of the abovementioned system is capable of converting the block data to suitable schema for legacy e-Register system. The legacy system and the ledger of the blockchain network are continuously synchronized to provide quick response to the domestic e-APP procedure user. If any State does not have powerful e-Register system, the users in those States can still search and verify their Apostille via global e-APP blockchain network with 32byte long letters which can cause some inconvenience.

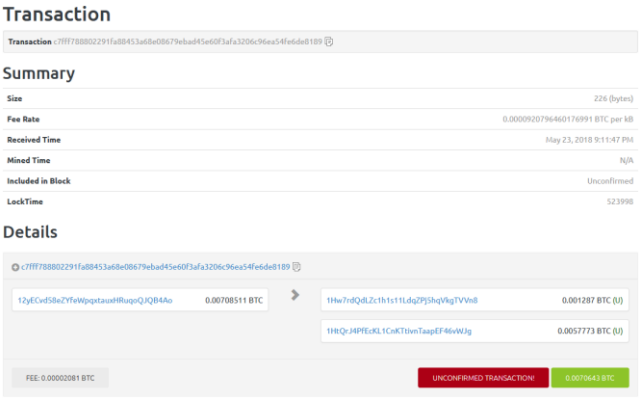


Fig. 51: Bitcoin transaction search with hash value

5. Conclusion

As discussed, some standardization is required to distribute the e-APP though the global e-APP exchange method cannot be unified in practice. Well-defined metadata, however, can allow many States that have not adopted e-APP yet to use the global e-APP system without amending their laws about digital document handling. Therefore, instead of unifying the Apostille's forms and processes, defining the metadata that depicts the real underlying documents and its Apostille can establish the global e-APP service while ensuring the best autonomy for each Apostille parties. This strategy can allow those with long-running Apostille services as well as those with no Apostille services to flexibly create new and high-level e-APP services.

We proposed a design for an interoperable data sharing and verification system structure for building a global e-Register service that is not dependent on the level of the e-Register built by the country of issuance. The proposed design meets all requirements to ensure that data is not monopolized by certain countries, while also preventing forgery and manipulation of official documents, guaranteeing availability to concerned parties, and providing all the verification steps of existing e-Register systems. Thus, the system was designed based on consortium blockchain that accepts different electronic file formats for Apostille authentication certificates and official documents for each member country and provides a verification method for various e-Registers. This will enable member countries to participate through a node and build a global e-Register service so that Apostilles can be verified even by member countries that cannot fully support the e-APP. Blockchain can be used to allow countries that are reluctant to implement the e-APP because of their current legal limitations and systematic issues to implement e-APP with greater ease and bypass or resolve limitations by using an e-Register service that is built through an international network without requiring a complete system.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and ICT) (No. NRF-2016R1A2B4016591).

References

[1] HCCH, The Secretary General, PB response to EU Green Paper 2011, HCCH, pp. 1–24, (2011).
[2] Yoo EJ, Jung GS, Han SJ & Cha JH (2017), A system design based on consortium blockchain for the public document certification, Korea Computer Congress 2017, 1030–1032.
[3] HCCH, Apostille Handbook: A Handbook on the Practical Operation of the Apostille Convention, HCCH, pp.1–139, (2013).

[4] S Nakamoto (2008), Bitcoin: A peer-to-peer electronic cash system. Bitcoin, pp. 1–9.
[5] National Archives of Korea (2007), A Study on Archiving and Management for Administrative Information System.
[6] Cho YH (2003), A Comparative Study on Metadata Formats of Digital Contents, Journal of the Korean Library and Information Science Society, Vol. 37, No. 2, pp.135–152.
[7] Oh S & Lee C (2017), Block Chain Application Technology to Improve Reliability of Real Estate Market. Journal of Society for e-Business Studies, Vol. 22, No. 1.
[8] Andrews C, Broby D, Paul G, & Whitfield I (2017), Utilising financial blockchain technologies in advanced manufacturing.
[9] Bitfury Group, Public versus Private Blockchain, Bitfury, (2015).
[10] Han SJ, Yoo EJ, Kwon D, & J. Cha (2016), A Study on Standardizing for Apostille Certification Data Model, Digital Contents Society Congress 2016, pp. 167–169.
[11] Day M (2001), Metadata for Digital Preservation: A review of Recent Developments, International Conference on Theory and Practice of Digital Libraries, Springer, Berlin, Heidelberg,, pp.161–172.
[12] Seo EG (2005), A Study on Preservation Metadata for Digital Resources, Journal of the Korean Society for Information Management, Vol. 22, No. 3, pp.233–260.
[13] RosettaNet (2002), RosettaNet Implementation Framework: Core Specification, Standards Specification Version, 2.
[14] Gartner Inc., Social Media Governance: An Ounce of Prevention, (2010).
[15] Sung KS, Oh DY, Kim JJ, Na WS & Oh HS (2008), Study on the Efficiency System Design for Minimize the Information Leak of the E-Document Store Service, The Journal of Korean Institute of Communications and Information Sciences, Vol. 33, No. 10, pp.350–358.
[16] Lee YY, Kang EB, Lee JN, & Kim Y (2014), A study on development of the metadata schema for traditional architecture based on FRBR. Journal of the Korean BIBLIA Society for library and Information Science, Vol. 25, No. 3, pp.29–57.
[17] Hung SY, Tang KZ, Chang CM & Ke CD (2009), User acceptance of intergovernmental services: An example of electronic document management system. Government Information Quarterly, Vol. 26, No. 2, 387–397.
[18] Higgins DG & Sharp PM (1988), CLUSTAL: a package for performing multiple sequence alignment on a microcomputer. Gene, Vol. 73, No. 1, pp.237–244.
[19] Bellissimo A, Burgess J, & Fu K. Secure Software Updates: Disappointments and New Challenges. HotSec. 2006.
[20] https://msdn.microsoft.com/en-us/library/aa371185.aspx. Released Versions of Windows Installer. MSDN.
[21] https://msdn.microsoft.com/ko-kr/library/windows/desktop/aa367449(v=vs.85).aspx About Windows Installer, MSDN.
[22] QTI, IMS. IMS Question & Test Interoperability Specification. IMS Global Learning Consortium (2005).
[23] Yoo EJ, Jung GS, Han SJ & Cha JH (2018), A Consortium Blockchain-based Certificate and Verification Framework for Apostille e-Register Service, International Journal of Private Cloud Computing Environment and Management, Vol. 5, No. 2, pp. 1-6.