Digital Academic Transcript Development for Thai University

Sorapong Ruanmanee[1], Sasithorn Suchaiya[2]*, Neranuch Pachanatip[2] and Jitti Niramitranon[2]

[1]Educational Administration, Kasetsart University, Bangkok, 10900, Thailand.

[2]Department of Computer and Information Science, Department of Computer and Information Science, Faculty of Science and Engineering, Kasetsart University, Sakon Nakhon, 47000, Thailand.

* Corresponding author. E-mail address: ssrithon.s@ku.th

Received: 18 April 2023; Revised: 3 August 2023; Accepted: 9 August 2023; Available online: 26 August 2023

Abstract

The Electronic Transactions Development Agency (ETDA), one of the public organizations under the control of the Thai government, and related departments such as the Ministry of Digital Economy and Society together with University Delegations, jointly developed an electronic message standard for educational transcripts that defines, to international standards, the data structure of electronic messages in XML format, following the UN/CEFACT Guidelines and based on ETDA Recommendation on ICT Standards for Electronic Transactions 25-2563. These standards include XML Naming and Design Rules for CCTS 2.01 Version 2.1 and Postsecondary Electronic Standards Council (PESC). The objective of this standard is to provide Thai educational institutions with internationally accepted standards for effective Academic Digital Transcript preparation and to develop a design methodology and an academic digital transcript (ADT) application to facilitate the production of transcripts and the exchange of data and documents among academic institutions in Thailand. The format of exchanged documents is PDF/A3 files which consist of transcript XML data. These PDF files are signed by digital signature based on PAdES-LTV, the standard method for signing PDF files with a digital signature, and XML files are signed based on the XML Advanced Electronic Signature (XAdES) standard for electronically signing XML documents. This standard was issued in addition to the XML Digital Signature standard issued by the W3C to enable signatures to provide long-term validation and conformity to the format and implementation of XML. The application developed in this project was used to generate 143,160 academic digital transcripts from February 2021-December 2022. The system had 30 (0.02%) error counts, with 99.98% effectiveness, and 5.66 Kbps efficiency of service rates.

Keywords: Transcript, PDF/A3, PAdES-LTV, XML, XAdES

Introduction

The project received Cabinet preliminary approval in compliance with the April 2, 2019 decision on the issuance of official papers via digital technology. The Office of the Public Sector Development Commission, as the primary agency, collaborates with the Ministry of Digital Economy and Society, the Electronic Transactions Development Agency (ETDA), the Digital Government Development Agency (public organization), and other related agencies to gather input from all related agencies. They also authorised the transitioning of government operations to an electronic service system and are responsible for the issuance of official papers using operationally standardized digital formats.

At a meeting of a working group with representatives from universities, the organizations indicated above issued guidelines to higher education institutions for creating significant educational papers in digital format (digital transcripts). The purpose was to make it easier for students, the general public, government organizations, and the commercial sector to access and examine appropriate educational materials that adhere to uniform standards and can effectively share information swiftly and easily.

A transcript is a documented record (inventory) of a student's academic progress that includes their complete enrollment history, all courses (or subjects) they have attempted, grades they have received, and any degrees

and awards they have received. Originally, the transcripts were first provided in paper form, with a signature from an authorized person. If graduates or students wanted a transcript, they could either pick it up in person or have it delivered by post. These processes had many drawbacks including a lack of timeliness in issuing the documents to the recipient. Additionally, reliability problems are a major issue because paper transcripts can easily be counterfeited. If the recipient wants to check the transcript, they must contact the university or educational institution which will issue the document endorsement, which will enable confirmation of the legitimacy of the document.

New technologies have been applied to digital academic transcripts, according to research studies, including blockchain technology to confirm the authenticity of transcript documents, electronic signatures, the use of QRCodes and RFID, and the use of XML to exchange information. These new technologies are presented in the Literature Review below.

The Electronic Transactions Development Agency (ETDA) proposed information and communication technology standards (ETDA, 2020) to apply to electronic transactions on electronic communications for academic transcripts. The proposed ETDA standards were congruent with international standards (European Telecommunications Standards Institute, 2016) set forth by UN/CEFACT, including the Postsecondary Electronic Standards Council and XML Naming and Design Rules for CCTS 2.01 Version 2.1, that provide the data structure of electronic messages in XML format (PESC, 2016, p. 10).

UN/CEFACT defines XML Naming and Design Rules Technical Specification describes and specifies the rules and guidelines that will be applied by UN/CEFACT when developing XML schema. This technical specification provides a way to identify, capture and maximize the reuse of business information expressed as XML schema components to support and enhance information interoperability across multiple business situations. All UN/CEFACT business information and business process modelling employ the methodology and model described in CCTS. CCTS defines both context-neutral and context-specific information building blocks. Context-neutral information components are defined as Core Components (ccts : CoreComponents).

Documents are produced as PDF files and have XML attachments. Document content includes institution logos and names, person names, score reports, signatures and other necessary information. For the destination computer system, the digital data is stored as XML files. Data belonging to the recipient can be read and processed immediately on production and transmission. Both PDF and XML files have digital signatures that are encrypted to avoid fraud and enable immediate verification of the document issuer via the international PKI system. To exchange educational digital transcripts between institutions, DGA and ETDA collaborated to create an electronic message standard for educational transcripts. This standard will serve as the recommendation for all Thai educational institutions starting in 2023.

However, this recommendation posed challenges for the development of the applications, and for the practical implementation of the systems, which was complicated, there being no established models or methods for developing applications based on a standard for electronic messages for transcripts of education. The developers needed to identify and gain experience in using and applying the tools correctly to ensure successful outcomes based on the standards, enabling document exchange between institutions.

The objective of this research was therefore to propose a methodology and a set of tools for producing digital educational transcripts that conform to the DGA requirements and ensure that the digital document produced is not only a reliable PDF file but also based on DGA recommendations.

Academic Transcript

An academic transcript (Lutton, Regan, & Geoff, 2009) is a detailed record of a student's academic performance. The subjects studied and the grades or marks the student attained are included as part of the evidence of their education. When a student applies for admission to a foreign institution of higher learning or seeks employment, the educational institution provides them with their academic transcripts, for all courses that the student undertook, Undergraduate or Graduate. Information about the university, the student, the course title, the grades and results of the course, the year the course was attempted, the degree, and any awards are all included in the document. The procedure used at present is to generate and print a transcript needed for a graduation ceremony or as requested by a single student.

A representative case study for Thai universalities was undertaken at Kasetsart University (Kasertsart University, 2020). The system developed in this case study follows a process with the following procedural steps:

1) Students make their requests for educational documents and identification verification using online channels or web services provided.

2) The requested document will be issued electronically in PDF format which will be sent to a specified email as requested by the applicant. Some institutions may charge a fee.

3) The student is then able to print the document as often as they wish or transmit the electronic document as required to destinations of their choice.

Some significant problems were discovered through the investigation of the processes outlined above:

Integrity: The recipient may get a transcript that has been changed along the way (the MITM or 'Man in the Middle' attack), making it impossible for the recipient to identify whether the data is accurate. If the receiver wishes to ensure it was created by the university they must obtain formal confirmation directly from the university. This requires time.

Interoperability: If the recipient receives a paper transcript printed from a PDF file and needs to input the information into a computer system for processing, such as entering the data manually into another system that can only receive the data manually, this is a time-consuming task and data input errors may occur (human error).

Numerous studies have been conducted to develop efficient and trustworthy processes for providing academic transcripts. Lokhandwala (Lokhandwala, Mandal, Raj, Sagar, & Acharya, 2021) researched the use of blockchain to confirm the validity of academic transcripts. Blockchain provides a method for assessing the reliability of documents through participant distribution and opinion sharing. Oyerinde (Grace & Oyerinde, 2015) used indexing information technology to quickly access transcripts that match the search term. In this research, the academic transcripts are structured in an uncomplicated format which accordance with XML schema which is defined in the electronic message structure (Grace & Oyerinde, 2015). Somdip Dey (Dey, 2013) suggests using QR codes to confirm the accuracy of the transcript. In their process a QR code is created and printed on the transcript, providing an encoded ID. Users can scan the QR for confirmation of identity. (Lutton, Regan, & Geoff, 2009) used RFID technology to verify the accuracy of transcripts. Mona (Al-Maharri, Al-Ammal, & Aljasmi, 2018) (Al-Mahari, Al-Ammal, & Aljasmi, 2019) presented an easy way to present useful transcription content. Imad (Shaikhli, Zeki, Makarim, & Pathan, 2012) studied how to hide electronic

signatures in PDF files to verify data ownership. The Postsecondary Electronic Standard Council (PESC) (PESC, 2014) provided an XML data structure for college and high school transcripts.

UN/CEFACT XML Naming and Design Rules

XML Name and Design Guidelines are defined by UN/CEFACT. The criteria and specifications that UN/CEFACT will use for creating an XML schema are described and specified in the technical specification. This technical definition offers a means to enable and improve information interoperability across various business settings by identifying, capturing, and maximizing the reuse of business information defined as XML schema components. The approach and model specified in CCTS are used in all UN/CEFACT business information and business process models. Information building blocks that are context-neutral and context-specific are defined by CCTS. The term "Core Components" refers to context-neutral information components (ccts : CoreComponents).

All design guidelines in (UNECE, 2014) were created based on the guiding ideas listed below:

- Relationship to UMM – UN/CEFACT XML Schema Definition Language (XSD) Schema will be based on UMM metamodel adherent Business Process Models.
- Relationship to Information Models – UN/CEFACT XSD Schema will be based on information models developed in accordance with the UN/CEFACT – Core Components Technical Specification.
- Schema Creation– UN/CEFACT XML design rules will support schema creation through handcrafting as well as automatic generation.
- Interchange and Application Use – UN/CEFACT XSD Schema and instance documents are intended for business-to-business and application-to-application use.
- Tool Use and Support – The design of the UN/CEFACT XSD Schema will not make any assumptions about sophisticated tools for creation, management, storage, or presentation available.
- Legibility – UN/CEFACT XML instance documents should be intuitive and reasonably clear in the context for which they are designed.
- Schema Features – The design of UN/CEFACT XSD Schema should use the most commonly supported features of W3C XSD Schema.
- Technical Specifications – UN/CEFACT XML Naming and Design Rules will be based on Technical Specifications holding the equivalent of W3C recommended status.
- Schema Specification – UN/CEFACT XML Naming and Design rules will be fully conformant with W3C XML Schema Definition Language.
- Interoperability – The number of ways to express the same information in a UN/CEFACT XSD Schema and UN/CEFACT XML instance document is to be kept as close to one as possible.
- Maintenance – The design of UN/CEFACT XSD Schema must facilitate maintenance.
- Context Sensitivity – The design of UN/CEFACT XSD Schema must ensure that context-sensitive document types are not precluded.
- Relationship to Other Namespaces – UN/CEFACT XML design rules will be cautious about making dependencies on other namespaces.
- Legacy formats – UN/CEFACT XML Naming and Design Rules are not responsible for sustaining legacy formats.

Message standard for an academic transcript

The Cabinet approved the issuance of government documents via digital system in principle in its resolution of April 2, 2019, (ETDA, 2020). The committee assigned the Office of the Public Sector Development Commission (OPDC) as the main organization to collaborate with the Digital Government Development Agency (Public Organization) (DGA), the Electronic Transactions Development Agency (ETDA), and related agencies to develop an electronic service system for the digital issuance of government documents for government services. In partnership with the committee, a working group on standards for producing significant educational records in digital format (digital transcripts) was created that included representatives from universities. They attended a meeting to discuss the preparation of important educational documents in digital format for higher education institutions that would enable students, government organizations, and the commercial sector to easily access electronic documents, which are based on a single standard. In addition, such electronic documents would be exchanged more efficiently in the future. The ETDA proposed information and communication technology standards that must be followed for electronic transactions on electronic communications for academic transcripts. They serve the electronic message data structure in XML format in compliance with global standards established by UN/CEFACT (European Telecommunications Standards Institute, 2016), such as the Postsecondary Electronic Standards Council and the XML Naming and Design Rules for CCTS 2.01 Version 2.1 (PESC). The data structure model of the electronic message consists of a standard data set provided in the academic digital transcript as shown in Figure 1.

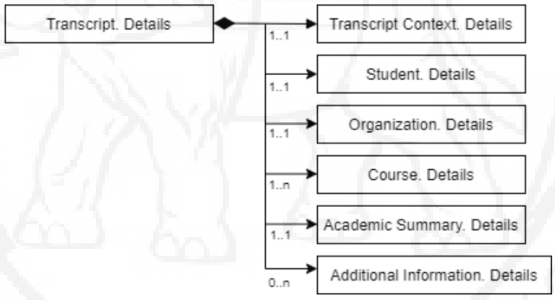

Figure 1 The data set in academic transcripts (ETDA, 2020)

The process of electronic messages in XML format generator

Figure 2 depicts the process of electronic messaging in XML format. The electronic formatting of data is the first step in the creation of electronic messages in XML format. The second step uses XML Schema files and Schematron Schema files to check data structures and usage rules. The result of the action conducted in the second step is a structured electronic message in XML format that complies with this standard recommendation.

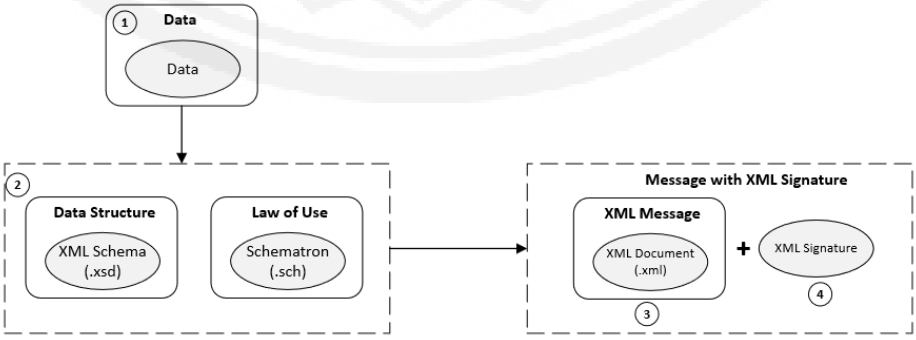

Figure 2 The process of electronic messages in XML format generator (ETDA, 2020)

In the third step, users can then use this XML message to create an electronic signature. In this step, users can then use this XML message to create an electronic signature and send an XML message with an electronic signature to those involved in the process of issuing the transcript in Step 4.

Guidelines and approaches were developed for improving the reliability of academic transcripts, increasing the speed of data access, and develop the structure of the transcript into XML to support data exchange. However, the reliable use of digital transcripts among students, educational institutions, and entrepreneurs has not been presented yet. Although Thailand has established standards for the interchange of academic digital transcripts, this recommendation makes it challenging to develop practical applications. Because there is no recognized model or approach for creating applications based on a standard for electronic messaging for transcripts of education, the implementation of program development was hard. Developers must understand and correctly use the tools for the documents to meet the criteria to be exchanged with other institutions. The objective of the current study was to design a methodology and development approach for an academic digital transcript (ADT) application to increase transcript creation and exchange data/documents among academic institutions in Thailand based on ETDA Recommendation on ICT Standard for Electronic Transactions 25-2563

Methods and Materials

The methodology to produce a digital transcript consists of the procedure shown in Figure 3. The procedure to create a digital academic transcript can be separated into two stages: 1. Keypair—the stage to prepare a pair of keys resulting in a private key and an X509v3 certificate for storing in the system. This stage will be repeated every 1 or 2 years, depending on the age of the given electronic certificate. Build PDF—The stage to build a PDF file according to ETDA standard 25-2563 is depicted in steps 8 and 9 and includes a certified timestamp from the Timestamp Authority as a third-party result as a time-trustable PDF to ensure the integrity of the document signing time.

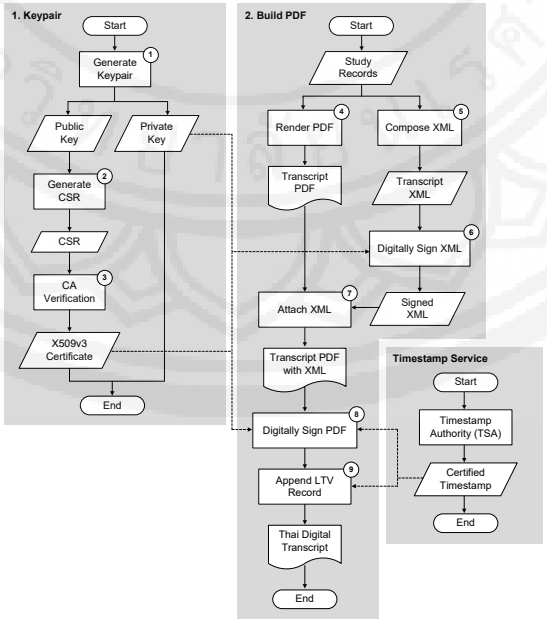

Figure 3 Digital academic transcript creation process

Results and Discussion

Keypair and certificate preparation

First, we need to build keypair, private and public keys, and request an electronic certificate from CA that includes the following inputs:

- Algorithm and key size, for example, RSA 2048 bytes
- University name, organization name, country, city, and email
- University legal certificate, for example, a legal juristic registration document and power of attorney from the chancellor

Users (Universities or agencies) keep the private key secret and make the CSR (Certificate Signing Request) from the public key, sending the CSR and legal documents to CA. The stage will be completed as follows after the CA formally identifies the organization and provides the X509v3 certificate with a typical 1-2-year expiration.

- Private key file according to PKCS7 in PEM format
- Certificate file according to PKCS8 in PEM format

These two files are typically kept securely together in a PKCS12 compliance keystore file with password protection.

PDF production

The following inputs will be used to create a PDF file commensurate with the ETDA 25-2563 standard, which will contain individual educational information.

- Student and university information, semester study results, and a summary of the studies.
- Private key and certificate for creating an electronic signature
- URL to request certified time from the Time Stamp Authority (TSA)

When the processing is complete, the PDF files will be generated as a result and include the key characteristics below.

- The XML file attachment within, including student, university, and study information
- A PDF is unmodifiable with an electronic signature
- An electronic signature is included in the XML file
- As long-term verification (LTV), a PDF contains a certified timestamp; the PDF will remain valid in the future even if the electronic certificate has expired

A PDF will be a valid result and trustworthy when verified with a DGA web application or an ETDA 25-2563 compliance university application.

Data structure

The data structure in the attached XML accompanying the digital academic transcript is based on a defined XML schema (Figure 4)

- Transcript – title, description, date of issue, date of entrance, and date of completion,
- Student – personal information such as given and family name,
- Organization – university, campus, and faculty,

- Course – curriculum, subject, and transfer subject,
- AcademicSummary – study summary for each semester and year,
- AdditionalInformation – thesis, project, and honors,
- signature – electronic signature based on XadES.

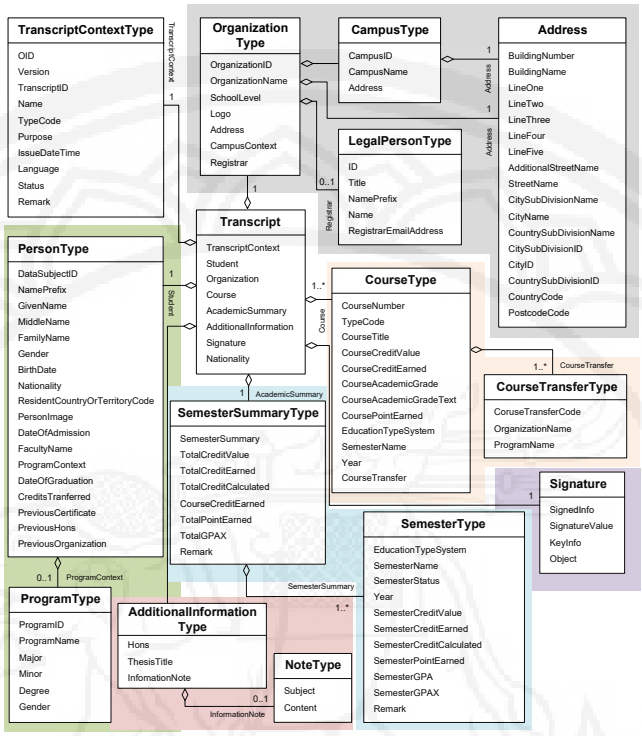

Figure 4 The data structure of a digital academic transcript

System Processes and Technology Requirements

The system will be used by primary actors including students who request the document for admission to higher education or in a work application. The digital document will be verified by the entrepreneurs by opening it in Acrobat Reader or submitting it to the DGA web application.

To prove the organization′s identity, the issuer academy will request an electronic certificate from an intermediate certificate authority, as shown in Figure 5. The private key and its associated certificate will be stored in the system and later used to sign the XML of educational information attached to the PDF with the signing time. The students will give a PDF file to a higher educational institute or company that recruits them. PDF recipients can open the document in Acrobat Reader and verify the apparent signature displayed on the pop-up signature panel. If the operating system trusts the top-level certificate authority, the Acrobat Reader will immediately recognize the signature as valid; otherwise, it will issue a warning.

Furthermore, the provided PDF can be verified with the DGA website, demonstrating that each valid item results in an immediate approval decision without contacting the university of origin.

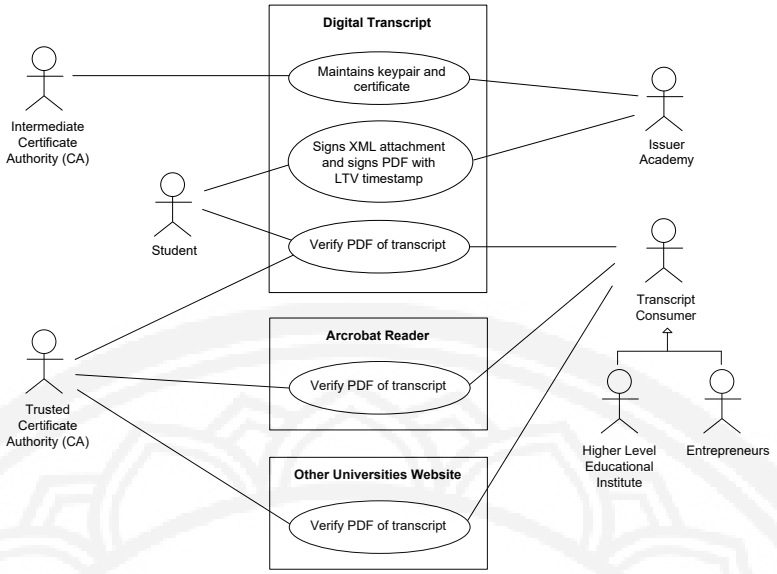

Figure 5 Usecase of digital academic transcript system

Tools and technologies

Tools and technologies will be used to achieve the system requirements shown in Figure 6.

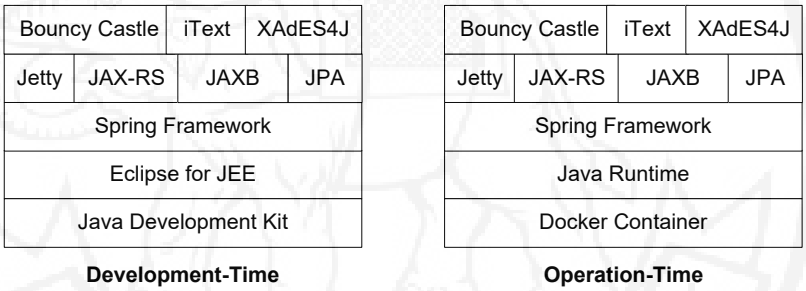

Figure 6 The software development tools and technologies

The tools depicted in Figure 6 served the following functions:

- Spring Framework – component-based software integration and inversion of control (IoC)
- Jetty – Embedded HTTP server as a microservice
- JAX-RS – Java API for REST, to use JSON over HTTP.
- JAXB – Java API for XML data binding, to convert XML data to an object and also revert based on the XML schema.
- JPA – Java Persistence API, to handle object-relational mapping (ORM) over the relational database.
- Bouncy Castle – to support many securities algorithms such as PKCS12, RSA, SHA, and CMS.
- iText – PDF manipulation such as handle attachment and electronic signature.
- XAdES4J – XML-based advanced electronic signature for Java, to verify whether a signature is valid or not.

The tools described above are open source and can be downloaded with a legal distribution license; the author uses these tools to develop software systems that meet the requirements.

Application structure

The digital academic transcript system was designed as a microservice that provided the API for use by related systems. Figure 7 illustrates participant classes.

The SignPdfSystem class acts as a system façade to list all core functions. An instance of PdfSigning will be created for each client request to produce a digital transcript. It will act as temporary session data during request fulfilment. The other class contains utility functions such as Marshaller, which manages objects for XML conversion, and PdfSigner, which is in charge of creating PDF signatures. XadesVerifier will be the provider signature verification functionality.

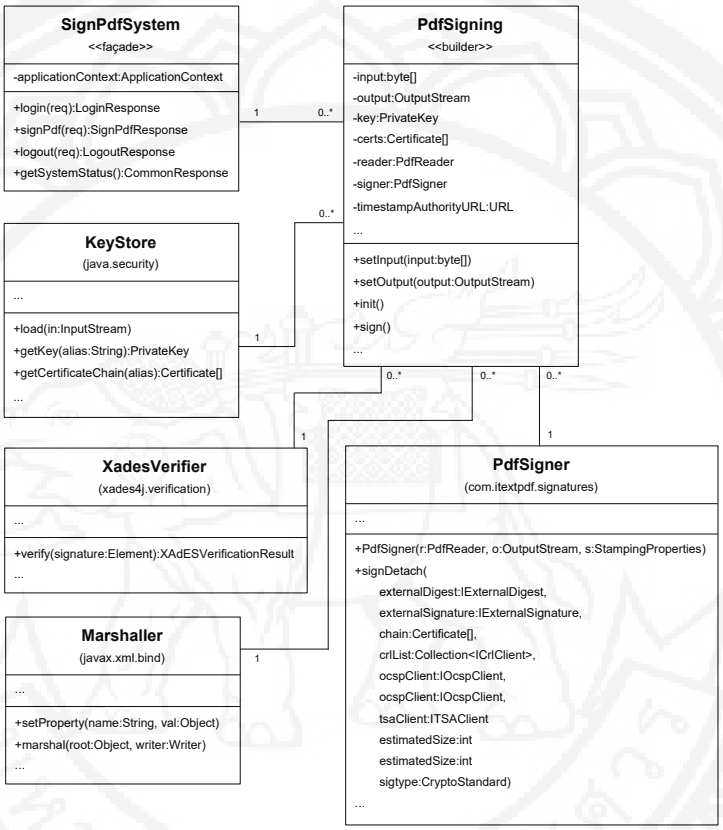

Figure 7 The class diagram for application structure

Sequence of messages

When clients request that the system generate a digital transcript via API, the sequence of object messages and delegation is shown in Figure 8. The API signPdf function operates by instantiating PdfSigning to keep session data. The given original PDF content, which was encoded in Base64 format, will be decoded into a byte array for subsequent processing. Also, the original plain XML will be generated and signed by XAdESSigner, which will later be attached to the PDF by the addAttachmentRaw() function. The KeyStore will be initialized to get the private key and certificate for calling the signDetach() function of PdfSigner. The signDetach() function composes a PDF signature and inserts it into a PDF document. The addLTV() function generates long-term verification with a certified timestamp added to the PDF also. The completed PDF will be Base64 encoded and returned to the client as a JSON string.

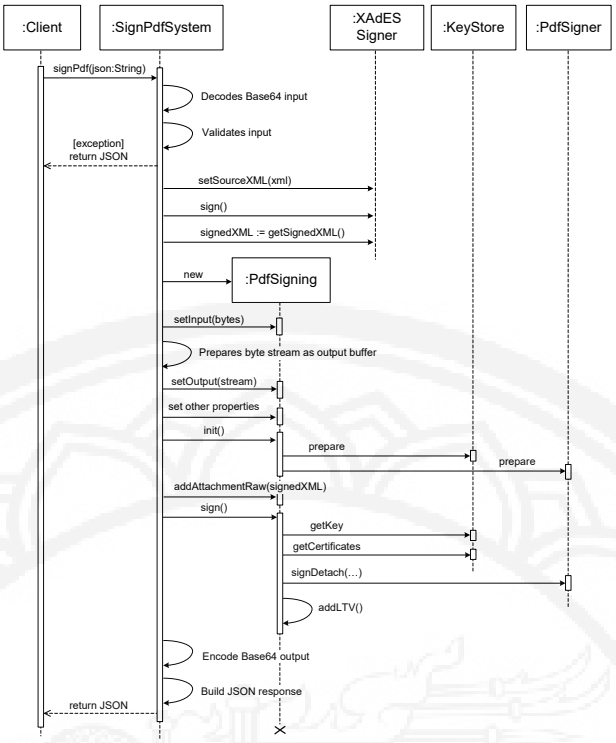

Figure 8 Sequence diagram of the proposed application

API for System Integration

Institutional administrative staff will produce a certificate in PDF format and occasionally print it out as a hard copy when a student completes the curriculum plan. To create the ETDA 25-2563 compliance PDF file, the system will receive the certificate PDF file and any accompanying XML data through an API. The API interface exposed as web services includes both SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) as the following operations (Figure 9):

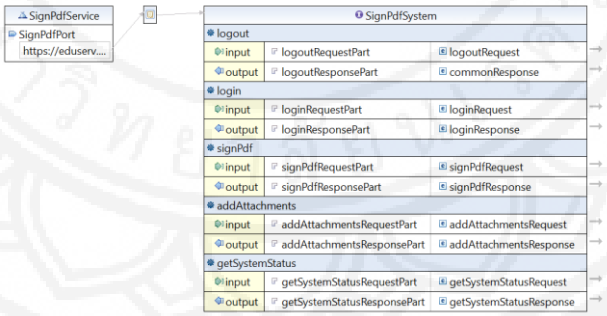

Figure 9 API for academic digital transcript

As shown in Figure 9, consumers use the service by initially sending an HTTP POST to URL /signpdf/login to get an access token, then uploading a plain PDF file with XML data to URL /signpdf/signPdf. For example, some portions of the JSON request used to generate a signed PDF can be shown in Figures 10 and 11.

The benefit of exposing APIs is that private keys, which are a crucial idea in PKI applications, are securely stored only in the central system. Private keys are not transferred to other parties. Moreover, APIs will make it very convenient for third-party IT systems to perform cross-platform interoperability.

```
{
  "sign" : {
    "apiVersion" : "1.0",
    "username" : "user1",
    "token" :
"s3zpKUeQMZAYIy4BccTmeZw22rcwapheGtSxYL+2NJI=",
    "pdfPassword" : "Ff0Upp",
    "pdfData" : "JVBERi0xL ... VPRgo=",
    "docIssuer" : "Kasetsart University",
    "docType" : "Transcript",
    "docName" : "Academic Transcript",
    "docNo" : "123456789",
    "signatureName" : "Demonstration only",
    "reason" : "E-Transcript",
    "location" : "Kasetsart University",
    "certifiedLabel" : "Kasetsart University",
    "enableQr" : true,

    "pageNumber" : 1,
    "qrData" : "https://registrar.ku.ac.th/",
    "x" : 288,
    "y" : 77,
    "width" : 65,
    "height" : 65
  },
  "attachments" : {
    "attachment" : [
      {
        "display" : "student.xml",
        "description" : "Student information",
        "content" : "SGVsbG8sIFdvcmxk..."
      }
    ]
  }
}
```


Figure 10 Sample JSON request used to generate a compliance PDF data


```
{
    "valid": true,
    "result": {
        "valid": true,
        "duration": 6242,
        "success": true,
        "endTime": "2021-09-01T01:07:52.364+07:00",
        "resultId": 1617,
        "resultType": "Sign"
    },
    "downloadTimeout": 0,
    "pdfData": "JVBERi ... SVFT0YK"
}
```


Figure 11 Sample JSON response containing compliance PDF data

Testing and AND Evaluation

The academic digital transcript system, which was designed and developed in Section 3, was implemented, tested, and used to create an ETDA 25-2563 compliance PDF with the results and evaluations detailed below.

Testing with Acrobat Reader

The signature panel will appear when opening an academic digital transcript PDF file with Acrobat Reader. The compliance PDF file will be verified and shown as valid based on the following apparent factors (Figure 12):

1) The signature panel appears and is shown to be valid.

2) There is the message "Signer's identity is valid."

3) There is the message "Signature is LTV enabled."

4) At the timestamp portion, there is a "Signature is valid."

5) At the timestamp portion, there is a "timestamp signature."

6) At the timestamp portion, there is a "Signature is LTV enabled."

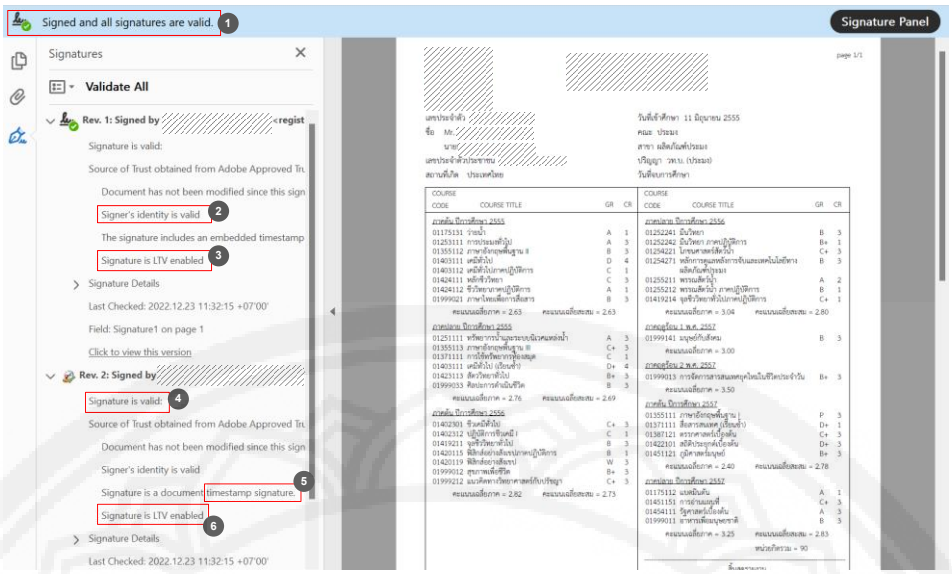

Figure 12 Result when opening an academic digital transcript with Acrobat Reader

Testing with DGA website

Users who upload their digital academic transcripts to the DGA website receive the following verification results (Figure 13):

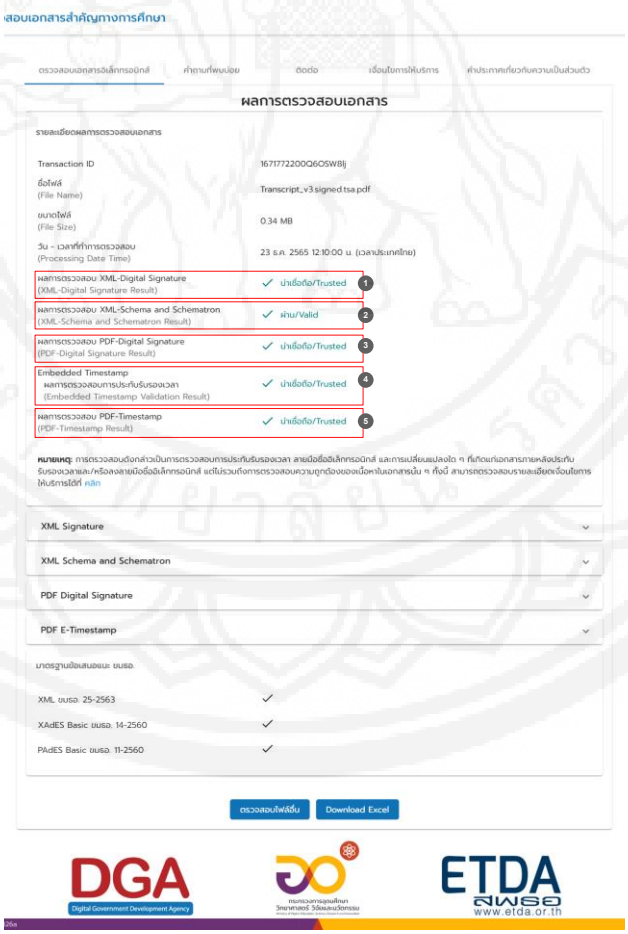

Figure 13 Result when opening an academic digital transcript with DGA website

As illustrated in Figure 13, we can determine whether a PDF is trustworthy if it meets the following key criteria:

- "XML-Digital Signature" appears to be trusted.
- "XML-Schema and Schematron" appear to be valid.
- "PDF-Digital Signature" appears to be trusted.
- "Embedded Timestamp" appears to be trusted.
- "PDF-Timestamp" appears to be trusted.

Usages Statistic

The academic digital transcript has been available as an API service since February 2021, with 146,246 digital transcripts generated as of December 2022, and monthly usage statistics can be shown in Figure 14.

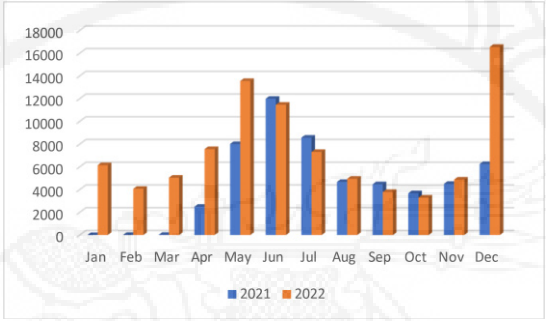

Figure 14 Monthly usage statistic chart

According to this chart, the system errors recorded 30 times can be classified into four types (Figure 15).

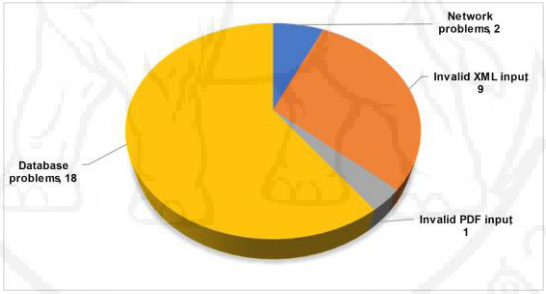

Figure 15 System errors experienced

As a result, the system error was as low as 0.02%, and the system effectiveness is 99.98%. After 23 months and 146,246 transactions, the system running on a VM emulated as an Intel® Xeon® Gold 5120 at 2.2 GHz with 16 CPU cores and 32 GB of RAM can be evaluated for efficiency by running the following SQL command (Figure 16 and 17):

```
SELECT
  COUNT(d.id) numOfDocs,
  AVG(d.duration) avgDurationInMs,
  AVG(s.SIZE) avgSizeInBytes,
  ((AVG(s.size)*8)/(AVG(d.duration)/1000))/1024/1024
avgEffInMbps,
  ((STD(s.SIZE)*8)/(STD(d.duration)/1000))/1024/1024
stdEffInMbps
FROM
  snp sign d INNER JOIN
  stg_doc_size s ON (s.id = d.id)
WHERE
  d.docName = 'ทรานสคริปต์'
```

Figure 16 The SQL command for calculating system efficiency

```
Name           |Value             |
---------------+------------------+
numOfDocs      |146246            |
avgDurationInMs|572.3541          |
avgSizeInBytes |424539.9208       |
avgEffInMbps   |5.6590538855021269|
stdEffInMbps   |0.3228041955118523|
```

Figure 17 The system efficiency evaluation

The summary of an average PDF data size of 414.59 KiB and a time consumption per document of 572.35 milliseconds, the average system speed is 5.66 Mbps with a standard deviation of 0.32 Mbps.

The academic digital transcript experiments referenced in Section 2.1 demonstrate that (Lokhandwala, Mandal, Raj, Sagar, & Acharya, 2021), (Dey, 2013), (Lutton, Regan, & Geoff, 2009) and (Shaikhli et al., 2012) have as their goals the resolution of issues with data reliability. Speeding up data access and storing study results in an XML structure for data exchange are the issues of (Grace & Oyerinde, 2015) and (Al-Maharri, Al-Ammal, & Aljasmi, 2018). The reliable use of digital transcripts by college students, educational institutions, and businesses is not the purpose of those articles.

Conclusion and Suggestions

In this research, we focused on the system implementation by applying contemporary technologies and tools for the development of a practical academic digital transcript system based on the ETDA 25-2563 standard for the provision of reliable digital transcripts for students applying for admission at higher education institutions, nationally or internationally, and similarly applying for employment. The recipient educational institute or company will be able to immediately verify and import the digital transcript into their digital system in a timely and trusted manner.

The strength of this paper is that the methodology is highly reliable. There are 3 levels of data security confirmation, which are a digital signature of XML data, a digital signature of PDF data and TSA signing time verification. The security confirmation made it difficult to counterfeit. In addition, this paper also used techniques that were international open standards and general tools such as Adobe Acrobat Reader™ which other agencies can follow.

Improvements should be made in the areas where the root certificate was excluded from earlier procedures. It is necessary to only use CAs that are directly or indirectly certified by a limited number of root certificates because when administrative personnel accessed the PDF file, the system alerted that it was not trusted. The recipient application will need to manually extract the XML and validate it because Adobe Acrobat Reader does not offer validation for digital signatures embedded in XML. Although it is a universal technique, there are particular computer languages and libraries that might be misused to create digital transcripts that cannot be shared around departments.

Future research should use a platform-neutral approach to digital transcription, and on what may be termed an Anywhere/AnyTime/AnyDevice basis. The use of the PAdES and XAdES approaches with additional programming languages beyond Java, such as Python, PHP, NodeJS requires further research. It is also important to learn how to deploy the system to run on Kubernetes or in the cloud so that it can support higher-performance applications. Network errors, which have repeatedly occurred, will also be resolved with the aid of this method.

References

Al-Mahari, M., Al-Ammal, H., & Aljasmi, L. (2019). *Prototyping a Visual Academic Transcript.* Sakhier, Bahrain: Institute of Electrical and Electronics Engineers. http://dx.doi.org/10.1109/3ICT.2019.8910270

Al-Maharri, M., Al-Ammal, H., & Aljasmi, L. (2018). Usability of the Academic Transcript. *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 18-20 November 2018* (pp. 1-7). Sakhier, Bahrain: Institute of Electrical and Electronics Engineers.

Dey, S. (2013). New generation of digital academic-transcripts using encrypted QR code™: Use of encrypted QR code™ in mark-sheets (academic transcripts). *International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)* (pp. 313-317). Kolkata, India: Institute of Electrical and Electronics Engineers.

Electronic Transactions Development Agency. (2020). ETDA *Recommendation.* Bangkok: Electronic Transcation Development Agency, Telecommunications Policy.

Besen M., S. (1990). The European Telecommunications Standards Institute: A preliminary analysis

Grace, O., & Oyerinde, Y. (2015). Information Retrieval and Indexing For a Digital Academic Transcript System. *Researchjournali's Journal of Information Technology, 2*, 1-11.

Kasertsart University. (2020, April 1). *Announcement by Office of Educational Administration Subject: Guidelines for Requesting Educational Documents in Electronic Format Outbreak of the Communicable Disease Coronavirus(COVID-19)*

Lokhandwala, T. T., Mandal, A., Raj, J., Sagar, S., & Acharya, V. (2021). Blockchain based Transcript Processing. *4th International Conference on Recent Trends* (pp. 257-262). Jamshedpur, India: Institute of Electrical and Electronics Engineers.

Lutton, E., Regan, B., & Geoff, G. (2009). RFID Authentication of Academic Transcripts: In the Context of a RFID Rationale and Deployment Methodology. *Fourth International Conference on Systems and Networks Communications.* Newcastle: Institute of Electrical and Electronics Engineers. http://dx.doi.org/10.1109/ICSNC.2009.87

Grace, O., & Oyerinde, Y. (2015). Information Retrieval and Indexing For a Digital Academic Transcript System. *Researchjournali's Journal of Information Technology, 2*, 1-11.

Postsecondary Electronic Standards Council. (2016). *XML Technical Specification.* United States: P20W Education Standards Council (PESC).

Shaikhli, I., Zeki, M., Makarim, R. A., & Pathan, A.-S. (2012). Protection of Integrity and Ownership of PDF Documents using Invisible Signature. *14th International Conference on Modelling and Simulation, 28-30 March 2012* (pp. 533-537). Cambridge, UK: Institute of Electrical and Electronics Engineers.

UNECE. (2014, May 27). *XML Naming and Design Rules For2 CCTS 2.01.* Retrieved from https://unece.org/DAM/cefact/xml/XML-Naming-And-Design-Rules-V2_1.pdf