IOP Conf. Series: Materials Science and Engineering **407** (2018) 012109 doi:10.1088/1757-899X/407/1/012109

Development of E-Diploma System Model with Digital Signature Authentication

A Finandhita* and I Afrianto

Program Studi Teknik Informatika, Universitas Komputer Indonesia, Jl. Dipatiukur No. 112 – 116, Bandung 40132, Indonesia

*alif.finandhita@email.unikom.ac.id

Abstract. The purpose of developing an e-diploma system model is to provide an overview of digital files that can be used as documents that have the same validity as paper documents. The validity is obtained through digital signature authentication so that in the future the use of e-diploma can be synchronized with a paper-based diploma. The method used to develop the model is a descriptive qualitative. The result of the research is a model. A printed diploma has a vulnerability that must be considered. Basically, paper documents are easily lost and damaged. Digital signatures are the mechanisms used to guarantee the authenticity of digital documents in the form of digital certificates. Digital certificates issued by the state to maintain its authenticity and integrity. Digital signatures are attached to digital documents. An E-Diploma is given as a companion of the original diploma. The model is developed to show that an E-Diploma may be considered as a valid document in the future, as long as it is authenticated by digital signatures.

1. Introduction

A diploma is a document of recognition of learning achievement and/or completion of a higher education after complete a particular course of study held by a college or university [1]. A diploma is recognized or is legally valid if it is provided by a university [2]. Today most educational institutions issue diplomas in a printed form [3]. This can be understood because the diploma must be printed to maintain its authenticity. Printed documents have vulnerabilities that must be considered [4]. Basically, paper documents are easily damaged and lost [5, 6]. Meanwhile, to reprint the diploma requires a fairly complicated procedure, starts from submission of a copy of the diploma until it is given [7]. In addition, when a copy of the diploma needs to be legalized, the owner of the diploma is required to come directly to the educational institution that issued the diploma [8]. A digital signature is one of the technologies used to improve network security and it has a function as a marker on data that ensures that the data is real (nothing has changed). It can meet at least two network security requirements, Authenticity and Non-repudiation, works by utilizing two keys, public key and private key [9].

In this paper, we propose an electronic model of diploma (E-Diploma) in the form of digital files as documents that have the same legitimacy as paper documents through digital signature authentication. The model to be developed is an additional model of the original diploma (paper-based diploma). E-Diploma is given as a companion that has digital signatures included. In fact, there have been several studies related to digital signature authentication, as conducted by Dhagat et al. [10], Pereira et al. [11], and Adi et al. [12]. However, there has been no specific implementation of digital signature

authentication on e-diploma system. In addition, e-diploma system model for use in college or university at this time has not been found.

Therefore, an e-diploma system model is developed to provide an overview of digital files that can be used as documents that have the same validity as paper documents through digital signature authentication, so that in the future the use of e-diploma can be synchronized with a paper-based diploma. The method used to develop the model is a descriptive qualitative. The result is an e-diploma model.

2. Methods

Figure 1 shows the descriptive qualitative method used to develop the model.

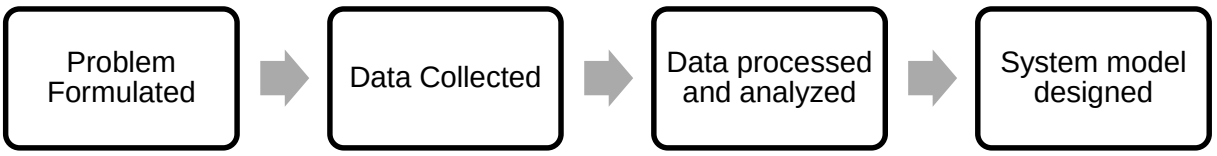

Figure 1. Research method.

3. Results and discussion

The data used include the supporting data of diploma and current diploma data management procedures. The reference data of the diploma based on previous research [13], consist of the following data as in (Table 1)

Table 1. Reference data.

No	Data
1	*Nomor Seri Ijazah* (Diploma Serial Number)
2	*NIM* (Student ID Number)
3	*Nama Lulusan* (Graduate's Name)
4	*Tempat Tanggal Lahir* (Date of Birth)
5	*Jenjang* (Study Level)
6	*Fakultas* (Faculty)
7	*Program Studi* (Department)
8	*Tahun Masuk* (Year of Entry)
9	*Tanggal Kelulusan* (Graduation Date)
10	*Gelar Akademik* (Academic Degree)

Figure 2 shows that the data format of the diploma can be obtained from the basic data of the student, the graduate candidate's data, and the diploma data itself. (Figure 2)

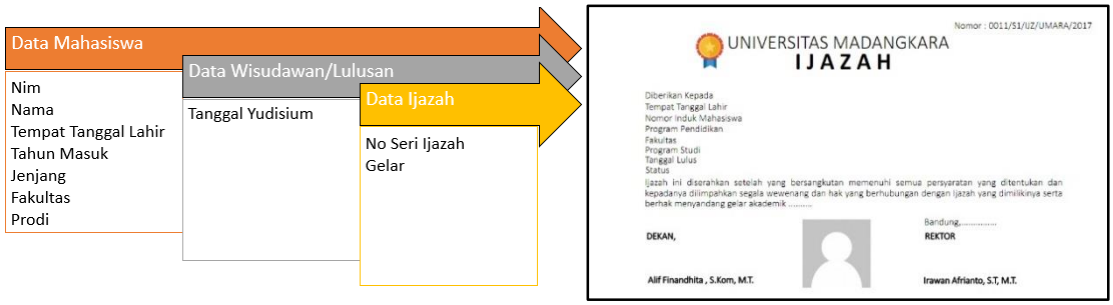

Figure 2. Diploma data flow.

The mechanism of issuing diplomas in some universities is usually done through several stages and involves several sections within the college. The procedures commonly used by universities associated with the management of diplomas is the procedure of diploma issuance and legalization.

Referring to the current procedure, the diploma is issued using paper. This certainly creates vulnerability to the current document, because the paper-based diploma can be lost or damaged for one reason [4-6]. Meanwhile, to do the replacement of diploma takes a long time and complicated process [7]. Digital documents are an alternative solution that can be developed to address the problem [11]. It's just that the digital document must be equipped with an identity marker such as a signature that is recognized for its validity [12]. Protection and verification of digital diplomas are essential to avoid abuse by irresponsible parties [9]. It can be facilitated by digital signature technology provided by a trusted party (The Certification Authority) [14]. Currently, in Indonesia, the certification authority (CA) is held by the Ministry of Communications and Informatics (*Kominfo*) through the *SiVion (Sistem Verifikasi Identitas Online Nasional)* service for digital signature platforms in Indonesia [15].

The e-diploma system is developed based on the web. The main function of the e-diploma system is to produce a digital diploma document that is digitally signed so that the digital diploma has the same power as a paper-based diploma. Digital signatures generated in the e-diploma system using the official .p21 format derived from CA Kominfo Republik Indonesia [15]. Users in the system have the function and role as needed [16]. There are 4 users involved in this e-diploma system: system operators, head of the university, alumni, and visitors. E-diploma will be made in a digital form that is authenticated with a digital signature from the head of the university. People who need authentication or want to know the authenticity of the digital diploma can check into the e-diploma system by uploading digital diploma files into the system to obtain information related to the correctness of the document. If the system detects a digital signature in the file, it can be ascertained that the digital diploma is authentic (no change since it was signed), but if the system does not detect a digital signature in the diploma file, it can be categorized as a fake diploma.

Table 2 shows the users of an E-Diploma system with digital signature authentication divided into 4 categories according to the permissions they have in the system. For data security, system operators, head of university and alumni are granted access to be able to enter and manage data in the system with usernames and passwords, while visitors can directly access the system. (Figure 2)

Table 2. E-Diploma user requirements.

Users	Requirements	Skills to be Owned
System Operators	• Login • Register Users • Process Alumni Data • Process Diploma Data • Check E-Diploma Status	have the ability to use the internet and understand data management
Alumni	• Login • Request E-Diploma • Input Diploma Data • Download E-Diploma	have the ability to use the internet
Visitors	• Check the authenticity of E-Diploma • View alumni profile	have the ability to use the internet
Head of University	• Login • View E-Diploma Data • Sign E-Diploma	have the ability to use the internet

Figure 3 shows the overview of e-diploma system model. (Figure 3)

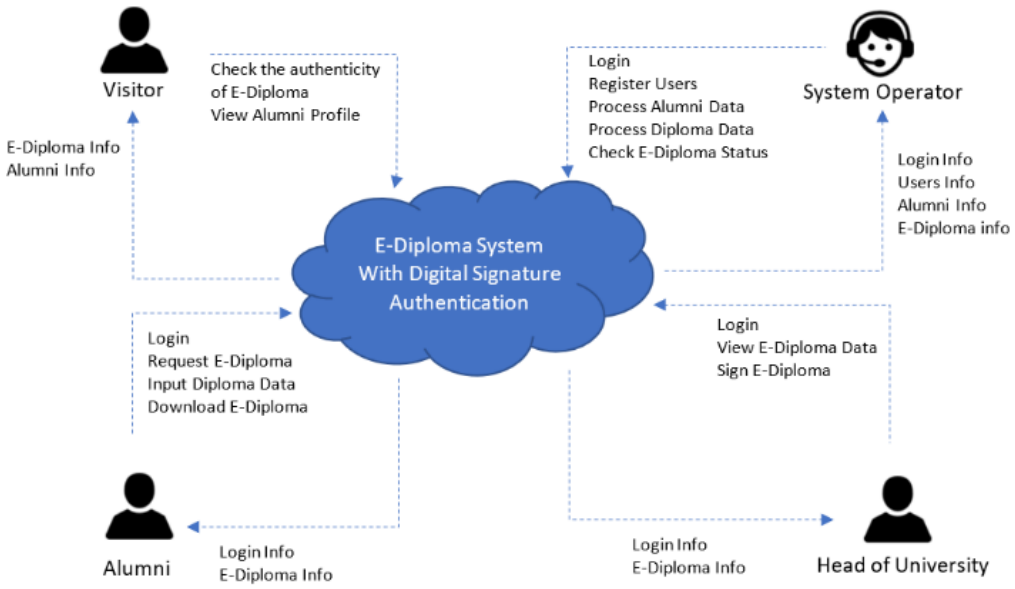

Figure 3. E-Diploma system model overview.

The architecture of e-diploma system model can be seen in Figure 4, involving interrelated entities to produce good system performance. The sections of the e-diploma system model architecture include functional, interface, web server, database server, SDK / API, External System (https://verifikasipdf.sivion.id) [17, 18] using PDFSign [19], and users. (Figure 4)

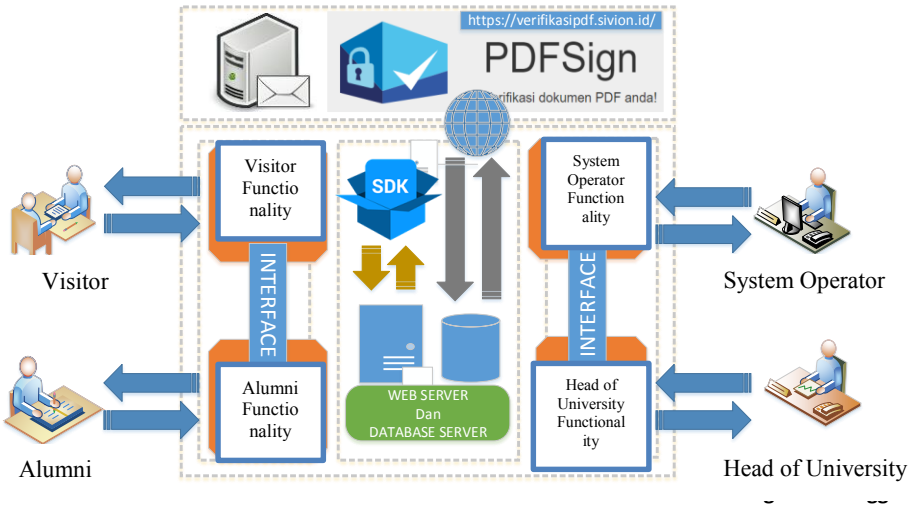

Figure 4. E-Diploma system model architecture.

The e-diploma system model will produce the output of a digital diploma file in .pdf format model. The digital diploma contains data such as the original diploma with digital signature authentication

affixed by the head of the university (Rector and Dean). The example of digital diploma produced in the e-diploma system can be seen in Figure 5.

Figure 5. E-Diploma format model.

4. Conclusions

The present study has given an overview of E-Diploma system model with digital signature authentication using an external system called SiVION. The developed model has a functional system that allows the operator to manage the data of graduates, alumni, and diplomas. It will make the head of the university easier to sign diplomas digitally. The developed model also will make it easier for graduates to get diploma replacement that has the same authentication value with a paper-based diploma. Communities will more easily detect the authenticity of a digital diploma by accessing the official E-Diploma system.

Acknowledgments

Authors acknowledged Universitas Komputer Indonesia and Kementerian Komunikasi dan Informatika Republik Indonesia for supporting this research by providing the required data.

References

[1] Diploma [Internet]. En.wikipedia.org. 2018 [cited 15 March 2018]. Available from: https://en.wikipedia.org/wiki/Diploma.
[2] Abraham D 2017 "Is a university competent to confer a "Recognized" medical degree or diploma in India," *Current Medical Issues* **15** (4) 295-300.
[3] Credentialing in Higher Education: Current Challenges and Innovative Trends [Internet]. Educause Review. 2015 [cited 9 April 2018]. Available from: https://er.educause.edu/articles/2015/3/credentialing-in-higher-education-current-challenges-and-innovative-trends.
[4] Lax G, Buccafurri F and Caminiti G 2015 "Digital Document Signing: Vulnerabilities and Solutions," *Information Security Journal: A Global Perspective* **24** (1-3) 1-14.
[5] After the Disaster: Replacing Lost or Damaged Documents | FEMA.gov [Internet]. Fema.gov. 2015 [cited 10 April 2018]. Available from: https://www.fema.gov/news-release/2015/06/19/after-disaster-replacing-lost-or-damaged-documents.

[6] T Olexa M and Grant L 2016 Replacing Lost or Damaged Documents [Internet]. Florida: IFAS Extension University of Florida; 2016 [cited 11 April 2018]. Available from: http://edis.ifas.ufl.edu/pdffiles/DH/DH21500.pdf.
[7] Reissued Diploma [Internet]. Registrar.psu.edu. 2017 [cited 11 April 2018]. Available from: https://www.registrar.psu.edu/graduation/reissued_diploma.cfm.
[8] Procedure for issuing diplomas, diploma supplements and certificates at the Estonian Academy of Music and Theatre [Internet]. Ema.edu.ee. 2016 [cited 11 April 2018]. Available from: http://www.ema.edu.ee/wp-content/uploads/2016/11/Diplomi-statuut-2016_EN-1.pdf.
[9] Katz J 2014 *Digital signatures* (Place of publication not identified: Springer).
[10] Dhagat R and Joshi P 2016 "New approach of user authentication using digital signature," *Symposium on Colossal Data Analysis and Networking (CDAN).*
[11] Pereira C, Barbosa L, Martins J and Borges J 2018 "Digital Signature Solution for Document Management Systems - The University of Trás-os-Montes and Alto Douro," *Advances in Intelligent Systems and Computing* **12** 16-25.
[12] Prasetyo A A and Adi W P P 2015 "Design Validation System and Legalized Document Using E-Certificate Application," *Information Systems International Conference (ISICO).* **12** 12-14.
[13] Afrianto I, Heryandi A and Finandhita A 2012 "Pemanfaatan QRCode Sebagai Akses Cepat Ijazah," *Prosiding Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM)* **23** 17-24.
[14] Scheitle Q, Chung T, Hiller J, Gasser O, Naab J, van Rijswijk-Deij R, Hohlfeld O, Holz R, Choffnes D, Mislove A and Carle G 2018 "A First Look at Certification Authority Authorization (CAA)," *ACM SIGCOMM Computer Communication Review* **48**(2) 1-3.
[15] SiVION – SOLUSI IDENTITAS DIGITAL TERPERCAYA [Internet]. Aptika.kominfo.go.id. 2016 [cited 14 April 2018]. Available from: https://aptika.kominfo.go.id/index.php/artikel/134-sivion-solusi-identitas-digital-terpercaya.
[16] Norman D A 2014 "Some observations on mental models," *In Mental models* **14** (12) 15-22. Psychology Press.
[17] Official Tanda Tangan Digital Indonesia [Internet]. Sivion.id. [cited 14 April 2018]. Available from: https://www.sivion.id.
[18] PDFSign [Internet]. Verifikasipdf.sivion.id. [cited 14 April 2018]. Available from: https://verifikasipdf.sivion.id.
[19] Sojka P and Hatlapatka R 2010 "PDF Enhancements Tools for a Digital Library: pdfJbIm and pdfsign," *Brno, Czech Republic* **12** 45-55.