PEOPLE: International Journal of Social Sciences
ISSN 2454-5899

Siswanto & Surgawiwaha, 2019

Volume 5 Issue 2, pp. 1003-1012

Date of Publication: 22nd October 2019

DOI- https://dx.doi.org/10.20319/pijss.2019.52.10031012

This paper can be cited as: Siswanto, B., & Surgawiwaha, D., (2019). Implementation of Digital Signature for Research Paper Legalization, Authentication and Ratification Case Study: Training Center for National Cyber and Crypto Agency. PEOPLE: International Journal of Social Sciences, 5(2), 1003-1012.

IMPLEMENTATION OF DIGITAL SIGNATURE FOR RESEARCH PAPER LEGALIZATION, AUTHENTICATION AND RATIFICATION CASE STUDY: TRAINING CENTER FOR NATIONAL CYBER AND CRYPTO AGENCY

Budi Siswanto
Training Center For National Cyber and Crypto Agency, Depok, Indonesia
budi.siswanto@bssn.go.id

Dian Surgawiwaha
Training Center For National Cyber and Crypto Agency, Depok, Indonesia
dian.surgawiwaha@bssn.go.id

Abstract

At The Training Center for The National Cyber and Crypto Agency, at the end of every course programs, the students are given a task to write scientific papers. Then those papers must be ratified by the seminar committee using their wet signatures as a sign of ratification of documents. But the drawback of using wet signatures is that often difficult to get committee signatures as they are not always in the office. To overcome this problem, we'll discuss the uses of digital signature for student's papers ratification. This research begins by describing a digital signature and how it can replace a wet signature. Then we present the design of a scheme for implementing a digital signature that can be applied for papers authentication and ratification. Retrieval of the research data is done through in-depth observations in the process of ratifying student's scientific papers at The Training Center for The National Cyber and Crypto Agency.

The result of this study is the application of digital signatures as a substitute solution for wet signatures on student's scientific papers ratification.

Keywords

Digital Signature, Authentication, Verification, Research Paper, Commitee Members

1. Introduction

The use of information and communication technology (ICT) can improve the accuracy and efficiency of the organization in providing its services. The ICT services in the management of organizational documents are realized by providing speed, accuracy, and security for distributed documents. To answer this challenge, document management has now shifted from a manual system to an electronic one. Goverment organization around the world are actively transforming their agency businesses, using digital technologies to diliver agility, efficiency, cost saving and superior constituent experiences(Adobe, 2017). In Indonesia, to encourage the enhancement of public service, the shifting of governance paradigm to electronic-based governance is established through Presidential Regulation Number 95/2018 on Electronic Based Government System. The regulation urges all public institutions to digitalize public services as one of the steps to cutting budgets and resources, including public information requests (OPEN GOVERNMENT INDONESIA, 2018).

The Training Center for The National Cyber and Crypto Agency is one of the supporting elements of the National Cyber and Crypto Agency (BSSN) which has the task of carrying out education and training of cyber and crypto human resources, accreditation of cyber and crypto training institutions, and evaluation and reporting. And as a government organization, the BSSN training center that also conducts administration activities must obey the regulation concerning electronic-based government system.

One of the document administration management systems in an educational institution environment is related to the ratification of the legality and validity of student's scientific paper documents. The ratification of these documents currently done by manually sign it with wet signatures of the seminar committee. In practice, this system has problems. Sometimes the process of ratification becomes constrained because the committee that is supposed to sign is not in place. To overcome this problem, scientific paper documents can be made in the form of electronic files and sent to the committee to be signed electronically. Then are sent back to the organizer of the course program. But the problem is how the electronic signing mechanism is so

we can ensure that the document is signed by the correct person and not a fake signature. Based on the background of the above problem, this paper will discuss how to use digital signatures on the ratification of scientific paper documents.

2. Theoretical Basis

2.1 Information Security

Information security can be defined as an effort to protect information and important elements in it, in the form of systems and hardware used to store and transmit information. (Whitman, 2012).

Information security has four security aspects, namely:

a. Confidentiality: Maintaining the confidentiality of information from all parties except those who have the authority.

b. Integrity: Ensuring that information is not changed by unauthorized or by something else that is unknown (for example poor data transmission).

c. Availability: The information will always be available whenever the information is needed or is used.

d. Non-repudiation: A guarantee that someone cannot deny that he/she has sent the information.

And the application in the implementation of aspects of integrity and non-repudiation is digital signatures.

2.2 Digital Signature

The Digital signature is an asymmetric cryptographic application, commonly referred to as a public-key encryption system. Used to ensure the authenticity of electronic messages and guarantee the integrity of the contents of the message (UNCITRAL, 2009). Digital signatures consist of private keys, public keys, and certificates. Certificates are issued by the certification authority. Using certain algorithms, the Private key associates the messages with the value. The message, value, and certificate that associates the entity are then sent to the recipient of the message. Message Recipient will verify all three elements using the public key. (Mason S, Barrister, 2016).

According to the Republic of Indonesia Law Number 11 of 2008 concerning Electronic Information and Transactions, digital signature is a signature that contains electronic information that is attached to, associated or linked with other electronic information that is used for means of verification and authentication.

A digital signature can assure that the signer is truly the owner of the signature. Digital signatures also can be used to detect whether information has been altered after it has been signed or not (ensuring the integrity of documents) (Liyanti, Hakim AR., 2019). This guarantee can be obtained through verification when data is received or retrieved from storage. An overview of the digital signature process is as follows (eSign, 2017):

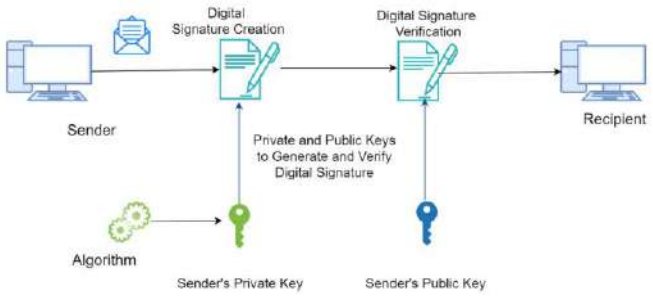

Figure 1: *Digital Signature Scheme*

Digital signature algorithms include the process of generating signatures and verifying signatures. Each signer has a public key and private key or is called the owner of the key pair. The private key will be used to sign and can only be done by the owner of the private key. This private key must keep protected from someone else who has no right to know (secret). While public keys are not secret, their integrity must be protected. Anyone can verify signed documents. This verification process is carried out using a public key.

Public Key Infrastructure (PKI), is a security infrastructure that is implemented using public key cryptographic concepts and techniques. PKI is a security infrastructure that allows users to securely exchange data on public networks, such as the internet, using public and private key pairs that are obtained and distributed through trusted third parties (Rose, 2018). PKI provides digital certificates and directory services that can store digital certificates and if necessary, relocate or revoke the certificates. In other words, PKI is a basic infrastructure that can be used to support secure use of cryptographic public keys, such as digital transactions via the internet. In its application, PKI is built from several integrated components whose aim is to regulate ownership of digital certificates so that they can be implemented effectively and accountably. Some of the main elements of the PKI are as follows (Schmeh, 2001):

1. Certificate Authority (CA) is a trusted entity that has the authority to create, issue and manage electronic certificates.

2. Registration Authority (RA), the PKI component that specifically handles matters related to registration and validation of digital certificate service requests by users.
3. The certificate database stores information about certificates issued, validity periods, PKI validity status.
4. The Certificate storage device, usually in the form of computer memory in which regulates the system of issuance, revocation and certificate status.

3. Discussion

The current system of the student's paper document ratification mechanism is still done manually. The committee can only sign the document directly using a wet signature. Busy committee members outside the office often hamper the process of signing papers. The delay in the signing process will have an impact on the paper documents collection to the course program organizer.

These constraints and problems require a more flexible ratification solution. Flexible in the sense of wherever the committee is, they still can sign the document. Therefore, the mechanism of the signature process must be changed from manual to digital, so that the document that originally had to be printed, now does not need to be printed anymore because it is turned into a digital document.

The digital signature that is applied to complete the solution must fulfill the following:

1. The digital signature has legal force and is equivalent to a wet signature.
2. Ensure that the document is properly digitally signed by the authorized committee so that the digital signature can be authenticated.
3. The committee cannot deny the signature he/she has done.
4. The committee can digitally sign anywhere and anytime, so the management and delivery of the student's paper documents are fast, precise, and valid.

4. Results

The scheme of the digital signature process that will be carried out by the committee is as follows:

1. Submission of a digital certificate to the Digital Certification Center. The resulting output is CA Certificate, Private key, Public key, Electronic certificate file p12, which contains a private key.

2. Installing the P12 electronic certificate file into the reviewer's laptop that will be taken when doing activities outside the office. Installation can be done on a computer or Adobe Reader application.
3. Digital signature process

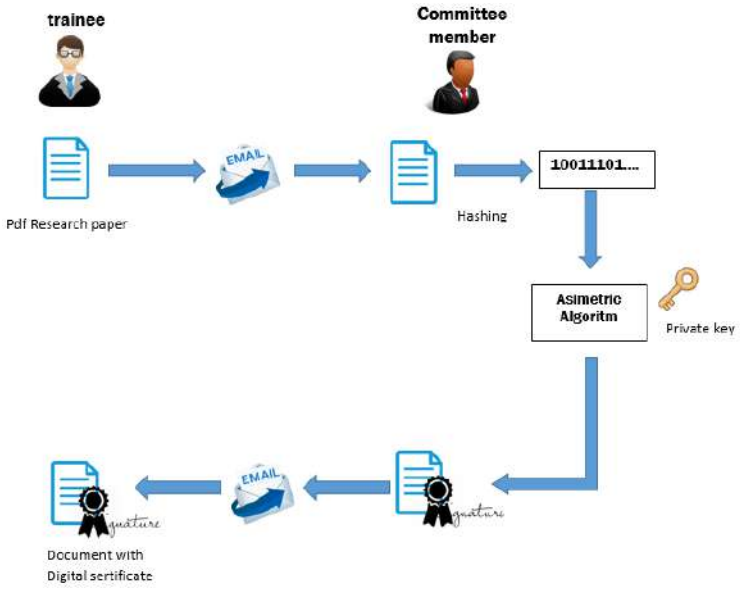

Figure 2: *Digital Signature Process*

The digital signature process is carried out as follows:

a. Students will send their papers through a secure electronic mail network, in the form of the electronic documents or PDF documents, that are ready to be digitally signed by the committee. The electronic documents are the final result of the papers that have been revised after the seminar.
b. The committee as the receiver will open a PDF document using the Adobe Reader DC application, and perform a digital signature.
c. The committee will send back the documents that have been given a digital signature to the students.
d. Students can then send the signed documents to the program course organizer as the final paper documents.

4. Verification process on the user's side

For digitally sign documents, user needs to obtain a Private and Public Key – a one-time process, it's done by Secured Signing Service, while user registered. The Private Key isn't shared and is

used only by user sign documents. The Public Key is available for all, used for validate the signatory's digital signature (Chaudary, Himanshi A, 2017).

Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

Verification needs to be done by the student to ensure that the digital document sent back by the committee is legitimate. Legitimate means that the document comes from the authorized committee, the document is authentic, there are no modifications to the document either before or during transmission, and the digital certificate in a digital signature is issued by a trusted CA. This verification process can be done in 2 ways:

1). Through the website *osd.bssn.go.id*, in the website *https://osd.lemsaneg.go.id*, you can verify the document by selecting the Application menu and then selecting Verifying Digital Document Signature PDF(BSRe, 2018).

Figure 3: *OSD Frotpage*

Users will be asked to enter the file by clicking Search PDF File so the verification results will display three important information, namely the validity of PDF documents, the validity of digital certificates and trusted digital certificates. If it shows a green checklist then the signature is valid or correctly signed by the committee. Recipients of documents from the Center for Education and Training can verify documents. An example of the display of the verification results is as follows:

Figure 4: *Document Verification Result*

2). Aside from using the OSD web, if the user obtains documents from electronic mail opened with a smartphone, the user can verify with the Very DS application. This application is available in the PlayStore.

Figure 5: *Document Verfication Application*

5. Conclusion

Based on the things that have been described several conclusions that can be drawn are:

1. The digital signature mechanism can be used for the ratification of student's scientific papers.
2. The Electronic Certificate Center of the National Cyber and Crypto Agency has provided digital signature services by issuing digital certificates that can be applied by the Seminar Committee to support the acceleration of document signing.
3. The application of digital signatures on the ratification of student's scientific papers at the Training Center for The National Cyber and Crypto Agency has the advantages that it can be done safer, easier, faster, anywhere and anytime as long as there is an internet network.

4. Digital signatures can be developed within the scope of other legalities to be able to support office automation to increase administrative speed and accuracy.

References

Adobe.(2017).,*Electronic and digital signature in adobe sign for goverenment White paper*. Adobe. Retrieved from https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/electronic-digital-signatures-adobe-sign-gov-wp-ue.pdf

BSRe.(2018).Balai Sertifikasi Digital, *Penerbitan Sertifikat Elektronik*. Retrieved from https://osd.lemsaneg.go.id/public/penerbitan

Chaudary, Himanshi A. (2017). *Process, Application and Authenticity of Digital Signature*. International Journal of Scientific Research Engineering & Technology (IJSRET). Volume 6: 882-888. Retrieved from http://scienceandnature.org/IJEMS-Vol3(2)-Apr2012/IJEMS_V3(2)6.pdf

eSign. (2017, june 12). *Electronic Signatures vs Digital Signatures*. Diambil kembali dari https://www.esigngenie.com: https://www.esigngenie.com/blog/electronic-signatures-vs-digital-signatures/

Liyanti, Hakim AR.(2019).*Perancangan Penerapan Tanda tangan Digital Sebagai Pengembangan Sistem Pelayanan Pentashihan Al Quran Digital*. Journal Sistemasi Volume 8 : 41-54. Retrieved from https://www.researchgate.net/publication/fulltext/Perancangan-Penerapan-Tanda-Tangan-Digital-Sebagai-Pengembangan-Sistem-Pelayanan-Pentashihan-Al-Quran-Digital.pdf

Mason S, Barrister. (2016). *Electronic Signatures in Practice*, Elektron. Volume 2 No. 2: 148-162 Retrieved from http://www.ee.co.za/wp-content/uploads/legacy/58.pdf

OPEN GOVERNMENT INDONESIA. (2018, December). *Indonesia Action-Plan 2018-2020*. Diambil kembali dari opengovpartnership: https://www.opengovpartnership.org/wp-content/uploads/2019/01/Indonesia_Action-Plan_2018-2020.pdf

Rose, M. (2018, Desember). *PKI (public key infrastructure)*. Diambil kembali dari Techtarget: https://searchsecurity.techtarget.com/definition/PKI

Schmeh,Klaus.(2001).*Cryptography and Public Key Infrastucture on the Internet*. Chichester. John Wiley

UNCITRAL.(2009). *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*. Uncitral. Retrieved from http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf

Whitman, Michael E. and Mattord, Herbert J.(2012). *Principles of Information Security Fourth Edition*. Boston. Course Technology