Journal of Engineering Science and Technology
Special Issue on INCITEST2019, February (2020) 28 - 35

E-DOCUMENT AUTENTIFICATION WITH DIGITAL SIGNATURE MODEL FOR SMART CITY IN INDONESIA

IRAWAN AFRIANTO*, ANDRI HERYANDI,
ALIF FINANDHITA, SUFA ATIN

Departement of Informatic Engineering, Universitas Komputer Indonesia, Jl. Dipatiukur no 112-116, Bandung 40123, Indonesia
*Corresponding Author: irawan.afrianto@email.unikom.ac.id

Abstract

The increasing number of smart cities in Indonesia affected public services. Important letters such as certificates and permit letters began its development into digital documents. However, to be approved as a valid document, an authentication mechanism needs to be inserted in it. This authentication is a mechanism to replace the written signature, also known as a digital signature which used to guarantee the authenticity of a digital document when it is used for various things. This study aimed to provide an implementation model of digital signature p12 developed by the Indonesian Ministry of Communications and Information Technology as well as providing an overview of e-document systems. In addition, the validity of the e-document is authenticated by the digital signature. This study used a quantitative approach using descriptive methods, namely conducting a comparative study to compare the phenomena found and make classifications that sourced from a standard. Experimental results showed that the p12 digital.

Keywords: Digital signature, E-document, Indonesia, p12, Public services, Smart city.

1. Introduction

Smart city is indicated through the effective and efficient management of resources to solve challenges by innovative, integrated, and sustainable way [1]. A smart city includes six aspects, namely governance, environment, economy, mobility, people, and living. The final result of the smart city is the creation of efficiency, sustainability, and quality of life [2, 3]. One of the smart city services is e-government. E-government represents the utilization of information and communication technologies (ICT) in the sector of public administration and politic. Indeed, it may influence political decision making. ICT is expected to contribute a better services in public sector, improve political participation and transparency. In short, it will increase efficiency in these sectors [4]. Smart city governance is about crafting new forms of human collaboration through the use of ICTs to obtain better outcomes and more open governance processes [5]. E-Government also provides transparency to maintain the reputation of public services provided to the community [6]. Electronic documents are part of public services used to replace paper documents because they have better characteristics such as more flexible, easy to search, small possibility of missing, saving space, archiving digitally, easy to transfer documents, improve security, and easy in-data recovery [7].

However, digital documents required a marker that can guarantee authenticity like other important paper documents. The digital signature is a solution that can be attached to a digital document to maintain the authenticity of the document [8]. Digital signatures were made with the help of cryptographic methods, to put the author's authentication on the document [9, 10]. Three basic things in the digital signature process are checking signatory authentication, document authentication, and digital signature verification [11, 12]. Digital signature strength depends on the cryptographic method used and the key length [13]. Some algorithms were used in the development of digital signatures such as ElGamal, Schnorr [14], and RSA [15]. In maintaining the integrity of electronic documents, cryptographic algorithms were combined with several message algorithm digest methods such as MD5, SHA 256, SHA 521, and Base64 [16-18].

The objectives of this study were to provide an overview of the e-document model in the form of a digital file that has the same validity as a paper document through authentication of the document with a digital signature, so that paper documents can be reduced by converting them to digital documents that have been authenticated with digital signatures shape of a projectile is generally selected on combined basis.

2. Methods

This study used a quantitative approach using descriptive methods, namely conducting a comparative study to compare the phenomena found and make classifications that sourced from a standard. The research started with the formulation of the problem, data collection (primary and secondary), data processing and analysis, and integrating system modeling design. Figure 1 shows the descriptive quantitative method used to develop the model [19].

Fig. 1. Research methods.

3. Results and Discussion

A document is an important work letter and usually signed by a leader or an authorized official. The sign indicated that the document is authentic and can be used for any purpose. One of the disadvantages of paper documents is that they can be easily damaged and lost. Moreover, the attached signatures are easy to fake. Currently, documents have been made using computer devices called digital documents or electronic documents (e-documents). The ITE Law in Indonesia has stated that electronic documents can be used as legitimate documents if there is a mechanism for signatures that are digital in them.

At this time, the Indonesian Ministry of Communication and Information has a program in the framework of using national digital signatures through the Directorate General of Information Applications. Through the National Identity Verification System (SiVION), the Directorate General of Informatics Applications provided digital certificates to the applicants which become a validation for them to use digital signatures in the transactions in the organizer system of e-document. SiVION provided digital certificates for individuals, organizations, and servers belonging to the public and the government. The digital certificate validation appeared immediately in real-time on each Electronic Certification Operator (PsrE) with a certificate issuer (Root Certification Authority / Root CA) [20]. SiVION has provided a digital certificate to the applicant which becomes a validation for them to use digital signatures in conducting transactions in electronic system organizer systems. Digital certificates contain a person's signature and identity or the web electronically which intended to maintain the validity of a document and show the legal status of the parties in the transaction. SiVION provides digital certificates for individuals, organizations, and servers that belong to the public and the government. Digital certificate validation appeared immediately in real-time on each Electronic Certification Operator (PSrE) with a certificate issuer (Root Certification Authority or Root CA) [21]. Figure 2 shows the architecture of the SiVION system.

The developed system model was web-based with site portal concept. The same validity of the digital document is become the main purpose of e-document. It is conducted by providing digital documents with a digital certificates. p12 format that is provided by the Indonesian Ministry of Communication and Information is used for digital signature in e-document. This form acts as a Certificate Authority (CA), digital certificate, and digital signature in Indonesia. The p12 Algorithm is a digital signature algorithm developed by the Indonesian Ministry of Communication and Information Technology using a combination of RSA Algorithm (Rivest-Shamir-Adleman) and SHA 256 (Secure Hash

Algorithm) with a Public Key Length of 4096 bits so that the attackers find it very difficult to solve. Figure 3 shows the conceptual model of the e-document system.

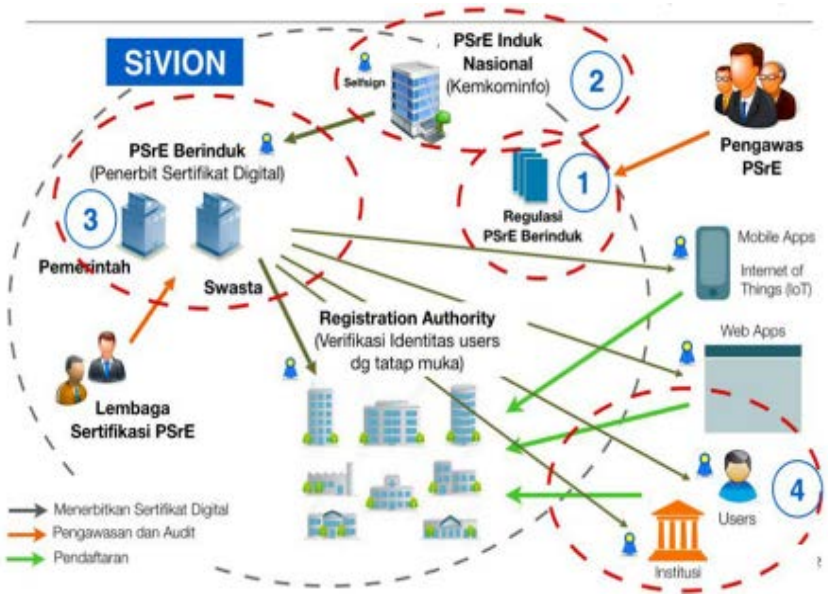

Fig. 2. The national identity verification system (SiVION)
Source: Ministry of Communication and Information RI.

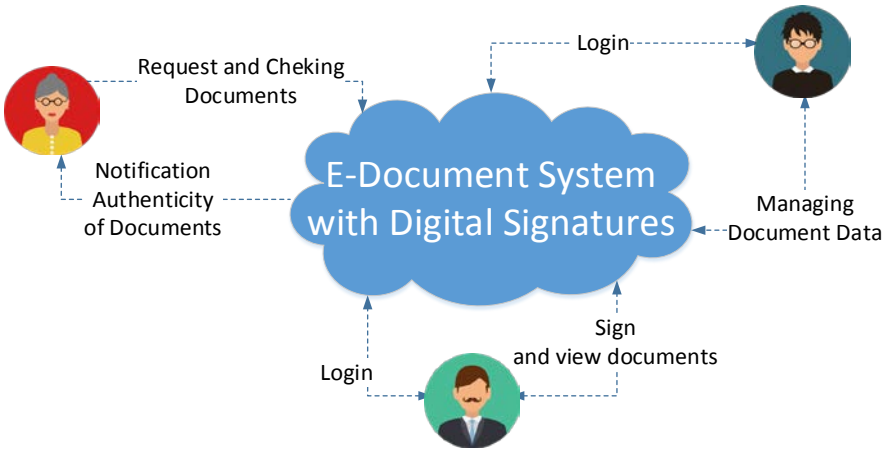

Fig. 3. E-document concept model.

When the e-document system architecture model was integrated, documents in digital form can be authenticated with digital signatures by the chairperson or officials. User who need authentication or authenticity checking of digital documents can visit the e-document system by uploading the digital document into the system. If the system detected a digital signature in the digital document, the system checks whether the digital signature is valid or not. If the system stated that the digital signature is valid, it means that the document is original or there has been no change since it was signed, but if the system detected that the digital

signature in the document is invalid, the document can be categorized as a falsified document. Figure 4 shows the architecture of the e-document system.

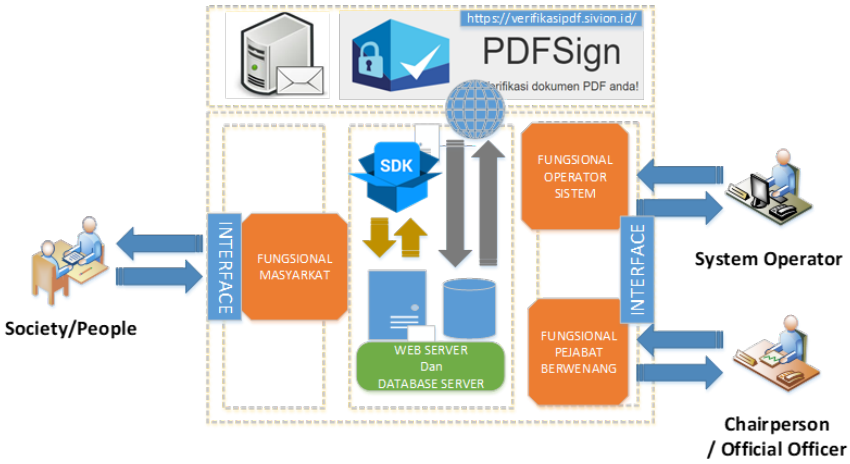

Fig. 4. Architecture e-document system.

In the e-document system model architecture, users can interact with each other. Three types of users can use this system, namely the society or citizen, the authorities or leaders, and system operators. The system interface was provided to facilitate the needs of each user. Technologies such as web servers, database servers, and APIs were used to run systems online as a part of the public services.

The implementation involved an example of a digital document that was legalized with a digital signature inside. The embedded digital signature in the chairperson section acted as proof that the chairperson legalized the document. Figur 5 shows a digital document signed with a digital signature.

Fig. 5. Digital document with the digital signature.

For original documents, the test results indicated that the digital signature in the document is valid. It is shown by the notification that the certificate is trusted, verified, valid as shown by three checklists in Fig. 6. It means the document is indicated as authentic or original (Fig. 6).

Fig. 6. Valid digital signature confirmation.

Meanwhile, if the contents of the document have changed, the system tells that the digital signature is no longer valid. The system provided information about why it is invalid such as the unverified signer's identity, the inexistence of timestamp, or does not support LTV; Four crosses in Fig. 7 can be interpreted that the document has gone through a trial of falsification, which indicates that the document is a falsified document.

Fig. 7. Invalid digital signature confirmation.

In Fig. 7 is a test result of a digital signature, about the validity and security system of the digital signature, so that the results of this trial can be used as an example. In this study also looked at previous research to research the results of research and comparison with previous research that discusses research [22-24].

4. Conclusion

This research produced a model for e-document systems with digital signatures where the system has adapted to the needs of the users. Experimental results showed that the P12 digital signature algorithm was able to provide authentication to digital documents. Changes made to the document can cause the digital signature to be invalid. So, an attempt of falsifying the document will fail.

Acknowledgements

This research was funded by the grant from the Ministry of Research and Higher Education (KEMENRISTEKDIKTI) Republic of Indonesia - Directorate General of Research and Development, with contract numbers between L2DIKTI4 and Universitas Komputer Indonesia No. 2898/L4/PP/2019 in the Applied Research scheme for the fiscal year 2019.

References

1. Supangkat, S.H.; Arman, A.A.; Nugraha, R.A.; and Fatimah, Y.A. (2018). The implementation of garuda smart city framework for smart city readiness mapping in Indonesia. *Journal of Asia Paific Studies*, 32, 169-76.
2. Albino, V.; Berardi, U.; and Dangelico, R.M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, 22(1), 3-21.
3. Schipper, R.; and Silvius, A. (2018). Characteristics of smart sustainable city *development*: Implications for project management. *Smart Cities*, 1(1), 75-97.
4. Von, H.C. (2004). Electronic government (e-government) and development. *The European Journal of Development Research*, 16(2), 417-432.
5. Hashem, I. A. T.; Chang, V.; Anuar, N. B.; Adewole, K.; Yaqoob, I.; Gani, A.; and Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, 36(5), 748-758.
6. López-López, V.; Iglesias-Antelo, S.; Vázquez-Sanmartín, A.; and Connolly R., Bannister, F. (2018). e-Government, Transparency and reputation: An empirical study of Spanish local government. *Information Systems Management*, 35(4), 276-293.
7. Rifauddin, M. (2016). Pengelolaan arsip elektronik berbasis teknologi. *Khizanah al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, 4(2), 168-178.
8. Warasart, M.; and Kuacharoen, P. (2012). Based document authentication using digital signature and QR code. *Proceedings of the 4th International Conference on Computer Engineering and Technology ICCET* . Bangkok, Thailand, 1-5.

9. Chyan, P. (2018). Penerapan sistem kriptografi enkripsi jamak dan tanda tangan digital dalam mendukung keamanan informasi. *TEMATIKA: Journal of Informatics and Information Systems*, 6(1), 39-46.
10. Azdy, R. A. (2016). Tanda tangan digital menggunakan algoritme keccak dan RSA. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 5(3), 184-191.
11. Pooja.; and Mamta, Y. (2018). Digital signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3(6), 71-75.
12. Gupta A.; Tung, Y.A.; and Marsden, J.R. (2004). Digital signature: Use and modification to achieve success in next generational e-business processes. *Information and Management*, 41(5), 561-575.
13. Mezher, A.E. (2018). Enhanced RSA cryptosystem based on multiplicity of public and private keys. *International Journal of Electrical and Computer Engineering*, 8(5), 3949.
14. Handley, M. (2018). Schnorr's digital signature and its applications. *Review of Computational Science and Engineering*, 4(1), 47.
15. Zahhafi, L.; and Khadir, O. (2018) A digital signature scheme based simultaneously on the DSA and RSA protocols. *Gulf Journal of Mathematics*, 6(4), 37-43.
16. Rachmawati, D.; Tarigan, J.T.; and Ginting, A.B.C. (2018). A comparative study of message digest 5 (MD5) and SHA256 algorithm. *Journal of Physics*, 978(1), 012116.
17. Mughal, M.A.; Luo, X.; Ullah, A.; Ullah, S.; and Mahmood, Z. (2018). A lightweight digital signature based security scheme for human-centered Internet of Things. *IEEE Access*, 6, 1630-31643.
18. Rajendran, B.; Misbahuddin, M.; Kaviraj, S.; and Bindhumadhava, B.S. (2018). Digital tokens: A scheme for enabling trust between customers and electronic marketplaces. *Proceedings of the Intelligent Computing and Information and Communication*, Singapore, 491-503.
19. Finandhita, A.; and Afrianto, I. (2018) : Development of e-diploma system model with digital signature authentication. *IOP Conference Series: Materials Science and Engineering*, 407(1), 012109.
20. Aptika, A. root CA dan sertifikat digital. Retrieved on October 20, 2018, from https://aptika.kominfo.go.id/2018/10/sertifikat-digital/.
21. Thasia. Sistem verifikasi online nasional (SiVION). Retrieved on October 27, 2016, from https://aptika.kominfo.go.id/2016/10/841/.
22. Agilandeeswari, L.; and Ganesan, K. (2016). An efficient hilbert and integer wavelet transform based video watermarking. *Journal of Engineering Science and Technology* (*JESTEC*), 11(3), 327-345.
23. Mathi, S.; and Valarmathi, M. L. (2018). An enhanced binding update scheme for next generation internet protocol mobility. *Journal of Engineering Science and Technology* (*JESTEC*), 13(3), 573-588.
24. Firdaus, C.; Wahyudin, W.; and Nugroho, E. P. (2017). Monitoring system with two central facilities protocol. *Indonesian Journal of Science and Technology*, 2(1), 8-25.