Korespondensi Artikel :
E-Document Autentification With Digital Signature Model For Smart City In Indonesia
(B.A.3)

REVIEWER INFORMATION FORM

Title of Paper:	**E-DOCUMENT AUTENTIFICATION WITH DIGITAL SIGNATURE MODEL FOR SMART CITY IN INDONESIA**
Manuscript ID:	**MPM_00X_IRAWAN AFRIANTO**

Reviewer 1:	
Full Name:	Asep Bayu Dani Nandiyanto
Institution Name:	Universitas Pendidikan Indonesia
Area(s) of Specialisation:	Engineering; Chemistry; Education
Email (s):	nandiyanto@upi.edu
Full Mailing Address of the Reviewer:	
Telephone Numbers:	
Date Sent To Reviewer:	
Date Returned By Reviewer:	
Total Time Taken By Reviewer to Review the Article:	

Specific Comments by the Referee [for the Author(S)]:

1. Result in abstract should more clear (tambahkan hasil uji)
2. In the last pharagraph at introduction should be writter method and purpose (ada tujuan di baris akhir pendahuluan) .
3. Figure 3 should be more detail about the users
4. Need more information about the flow of system
5. Position of explanation figure 6 above the picture.
6. Information about modification document
7. Result confirm the testing

Reviewer 2:	
Full Name:	Lia Warlina
Institution Name:	Universitas Komputer Indonesia
Area(s) of Specialisation:	Engineering; Urban and Rural Planning
Email (s):	lia@unikom.ac.id
Full Mailing Address of the Reviewer:	
Telephone Numbers:	

Date Sent To Reviewer:	
Date Returned By Reviewer:	
Total Time Taken By Reviewer to Review the Article:	

Specific Comments by the Referee [for the Author(S)]:

1. Need more explanation result in abstract
2. Introduction conduct more relevant research
3. To Many explanation about SIVION
4. Need explanation detail about the system in flowchart
5. More clear in conclution

Reviewer #1

1. Result in abstract should more clear .

Response to the Reviewer #1:

We agree. We already added the result into abstract :

"The test results show that e-document inserted with digital signature can be shown authenticity, as well as modified e-documents can be shown that the document is falsified document"

Reviewer #1:

2. In the last paragraph at introduction should be written method and purpose.

Response to the Reviewer #1:

We agree. We already added method and purpose in the last paragraph of introduction.

"The objectives of this study 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."

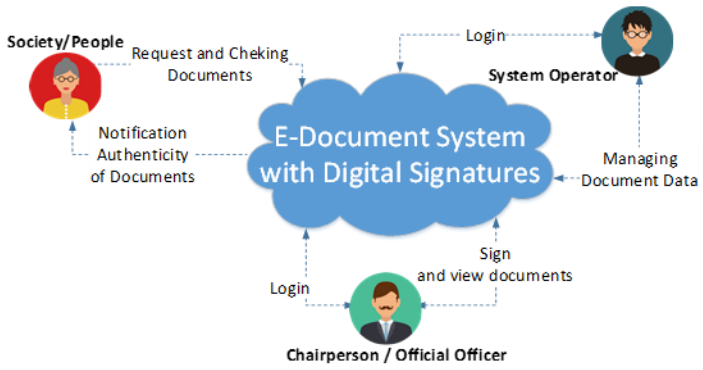
Reviewer #1:

3. Figure 3 should be more detail about the users

Response to the Reviewer #1:

We agree. We already changed the figure 3 with user desription

"The e-document system model, there are entities that interact with each other. From the user side, there are three users who will later use this system, namely the society/citizen, the chairperson/office officer and system operators."



Reviewer #1:

4. Need more information about the flow of system

Response to the Reviewer #1:

We agree. We already added flow of the system

“The concept model consists of 2 main modules namely, digital document requesting and digital document checking. The document request module is used to create digital documents as shown in Figure 4., while checking digital documents is used to determine the authenticity of the documents, shown in Figure 5 ”

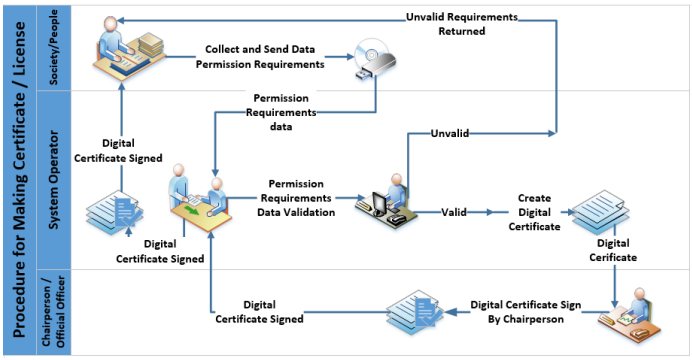


Fig. 4. Flowchart of create e-document.

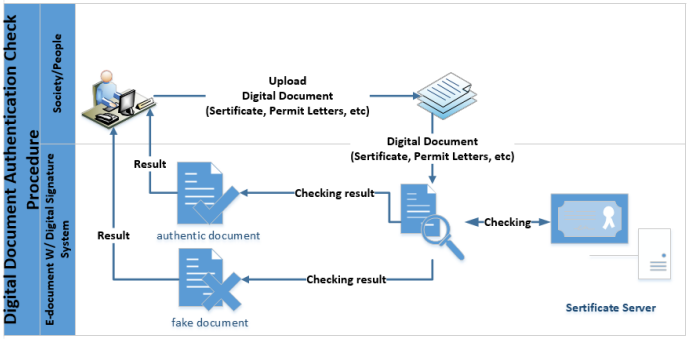


Fig. 5. Flowchart of cheking autentication e-document.

Reviewer #1:

5. Position of explanation figure 6 above the picture.

Response to the Reviewer #1:

We already change the position of explanation above the picture

“Technologies such as web servers, database servers and APIs are used to run systems online, and are connected to the internet as part of the public services that will be developed. Digital signatures generated in the e-document system, use the .p12 format which officially comes from the Indonesian Ministry of Communication and Information which acts as a Certificate Authority (CA) digital certificate and digital signature in Indonesia. P12 Algorithm is a digital signature algorithm developed by the Ministry of Communication and Information Technology Republic of Indonesia, using a combination of RSA Algorithm (Rivest-Shamir-Adleman) and SHA 256 (Secure Hash Algorithm). With a Key Public Key Length of 4096 bits. The meaning of the key area to look for is 2 4096, so that the attackers will find it very difficult to solve. Figure 6 shows the e-document system architecture.”

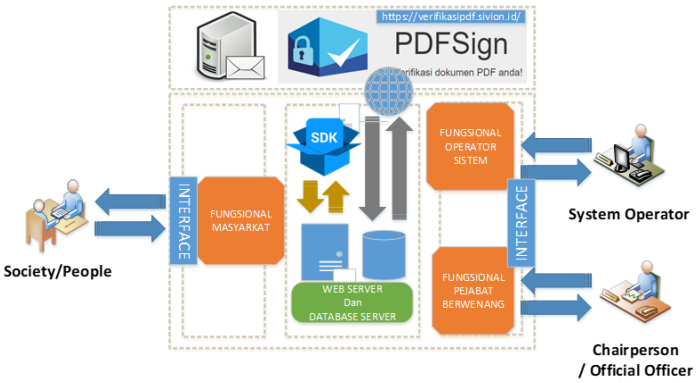


Fig. 6. Architecture e-document system.

Reviewer #1:

6. Information about modification document

Response to the Reviewer #1:

We agree. We already added information about modification document

"Meanwhile, if there is a change in the content of the document (such as text changes and document crops) , the system will indicate that the digital signature is no longer valid."

Reviewer #1:

7. Result confirm the testing

Response to the Reviewer #1:

We agree. We already added information about testing in result

"The result of tests conducted, has been able to provide authentication to digital documents, changes made to the document, causing a digital signature to be invalid and this indicates the existence of attempts to falsify the document".

Reviewer #2:

1. Need more explanation result in abstract

Response to the Reviewer #2:

We agree. We already added the result into abstract :

"The test results show that e-document inserted with digital signature can be shown authenticity, as well as modified e-documents can be shown that the document is falsified document"

Reviewer #2:

2. Introduction conduct more relevant research

Response to the Reviewer #2:

We agree. We already added more references

"Some algorithms are used in the development of digital signatures such as elgamal, Schnorr [14], and RSA [15]. In order to maintain the integrity of electronic documents, cryptographic algorithms are combined with several message digest methods such as MD5, SHA 256, SHA 521 and Base64 [16] [17] [18]".

Reviewer #2:

3. To Many explanation about SIVION

Response to the Reviewer #2:

Thank you for the suggestion. We already creduced the teory

"At this time the Ministry of Communication and Information of Indonesia through the Directorate General of Information Applications has a program in the framework of using national digital signatures. Through the Online Verification System (SiVION), the digital certificate validation will be done immediately (real time) on each Electronic Certification Operator (PsrE) with a certificate issuer (Root Certification Authority / Root CA) [20]. The National Identity Verification System (SiVION) provides a digital certificate to the applicant which becomes a validation for him 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. The aim is to maintain the validity of a document and show the legal status of the parties in the transaction [21]."

Reviewer #2:

4. Need explanation detail about the system in flowchart

Response to the Reviewer #2:

We agree. We already added flow of the system

"The concept model consists of 2 main modules namely, digital document requesting and digital document checking. The document request module is used to create digital documents as shown in Figure 4., while checking digital documents is used to determine the authenticity of the documents, shown in Figure 5 "

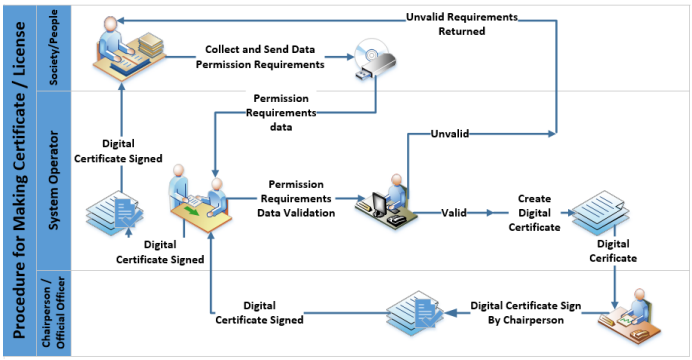


Fig. 4. Flowchart of create e-document.

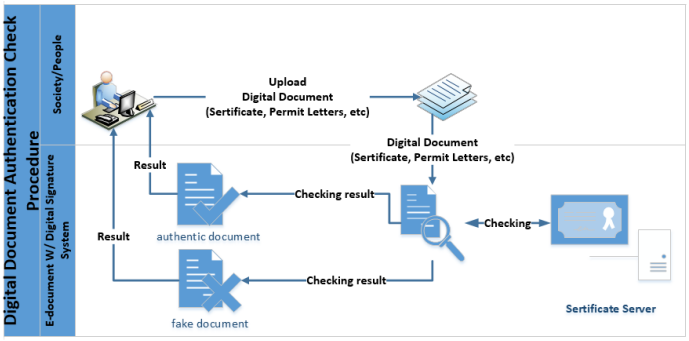


Fig. 5. Flowchart of cheking autentication e-document.

Reviewer #2:

5. Should more clearand need discussion in conclution

Response to the Reviewer #2:

We agree. We already added the result discussion.

"This research has produced a model for e-document systems with digital signatures where the system developed has adapted to the needs of the users. The result of tests conducted, has been able to provide authentication to digital documents, changes made to the document, causing a digital signature to be invalid and this indicates the existence of attempts to falsify the document. In the future, the integration of the system model developed must be able to be implemented with public services contained in the smart city perspective"

Journal of Engineering Science and Technology
Vol. XX, No. Y (Year) PPP - QQQ

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

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

[1,2,3,4]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 has an effect on public services. This raises the spirit of turning paper documents that are commonly used into digital documents. Important letters such as certificates, permit letters and so on began to be developed towards digital documents. But to be used as a valid document, an authentication mechanism needs to be inserted in it. This authentication is a mechanism to replace the signature known as digital signature. Digital signature is a mechanism used to guarantee the authenticity of a digital document when the document is used for various things.The purpose and objective of this study is to provide an overview of e-document systems in the form of digital files as documents that have the same validity as paper documents through authentication of these documents with digital signatures. The test results show that e-document inserted with digital signature can be shown authenticity, as well as modified e-documents can be shown that the document is falsified document.

Keywords: E-document, Digital Signature, Public Services, p12, Smart City, Indonesia

1. Introduction

Smart city is a city that can manage all resources effectively and efficiently in solving various challenges, using innovative, integrated and sustainable solutions[1]. Smart city includes six aspects, namely governance, environment, economy, mobility, people, and living. The final result of smart city is the creation of efficiency, sustainability and quality of life [2][3]. One part of smart city services is e-government. E-government denotes the strategic, co-ordinated use of information and communication technologies (ICT) in public administration and political decision-making. The benefits it is expected to deliver are greater efficiency of the institutions concerned, improvements in public services, and political participation and transparency [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 must also provide transparency in order 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 characteristics are more flexible, search is easier, the possibility of missing is small, save space, archiving digitally, transfer documents more easily, improve security and easy in data recovery[7].

However, digital documents require a marker that can guarantee authenticity like other important paper documents. Digital signature is a solution that can be attached to a digital document to maintain the authenticity of the document [8]. Digital signatures are made with the help of cryptographic methods, with the aim of such an ordinary signature that is 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 are used in the development of digital signatures such as elgamal, Schnorr [14], and RSA [15]. In order to maintain the integrity of electronic documents, cryptographic algorithms are combined with several message digest methods such as MD5, SHA 256, SHA 521 and Base64 [16] [17] [18].

The objectives of this study 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.

2. Methods

The research method used in this study is a quantitative approach using descriptive methods, namely conducting a comparative study to compare the phenomena found and make classifications that are sourced from a standard. The research starts from the formulation of the problem, data collection (primary and secondary), data processing and analysis, and system modeling design that will be developed. Figure 1 shows the descriptive quanitative method used to develop the model [19].

Fig. 1. Research methods.

3. Result and Discussion

A document is an important work letter and usually signed by a leader or an authorized official. The signature indicates that the document is authentic and can be used for the purposes of the document. The disadvantages of paper documents are that they are easily damaged and lost, and the signatures attached to them 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 Ministry of Communication and Information of Indonesia through the Directorate General of Information Applications has a program in the framework of using national digital signatures. Through the Online Verification System (SiVION), the digital certificate validation will be done immediately (real time) on each Electronic Certification Operator (PsrE) with a certificate issuer (Root Certification Authority / Root CA) [20]. The National Identity Verification System (SiVION) provides a digital certificate to the applicant which becomes a validation for him 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. The aim is to maintain the validity of a document and show the legal status of the parties in the transaction [21]. Figure 2 shows the arcitecture of SiVION system.

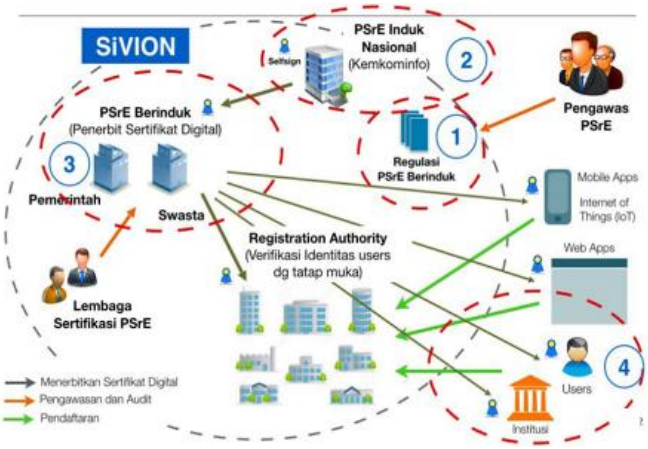


Fig. 2. The national identity verification system (SiVION)

The system model that will be developed is web-based with the site portal concept. The main function of the e-document system is to produce a digital document digitally signed (digital certificates are inserted in it) so that the digital document has the same strength as paper documents. The e-document system model, there are entities that interact with each other. From the user side, there are three users who will later use this system, namely the society/citizen, the chairperson/office officer and system operators. The system interface is provided to facilitate the needs and functions of each user. Figure 3 shows the concept model of e-document system.

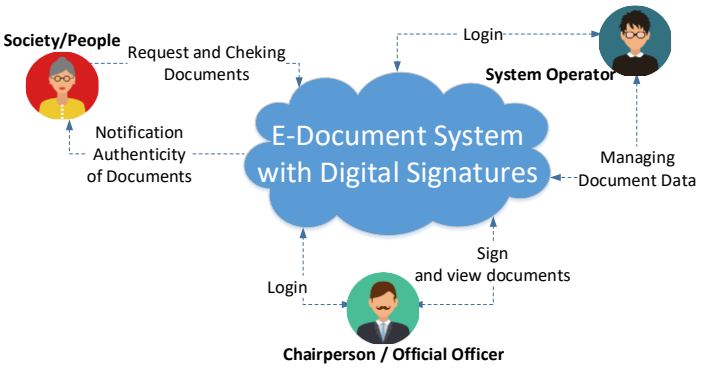


Fig. 3. E-document concept model.

The concept model consists of 2 main modules namely, digital document requesting and digital document checking. The document request module is used to create digital documents as shown in Figure 4., while checking digital documents is used to determine the authenticity of the documents, shown in Figure 5.

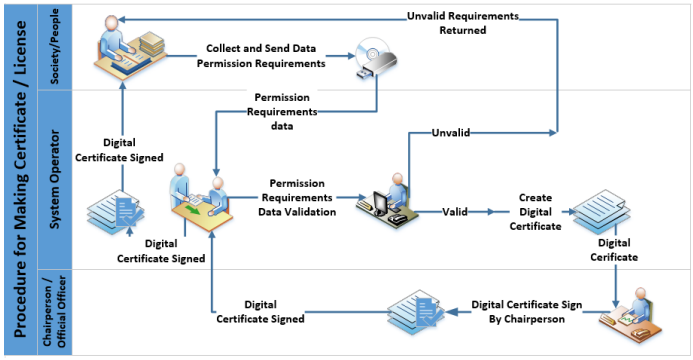


Fig. 4. Flowchart of create e-document.

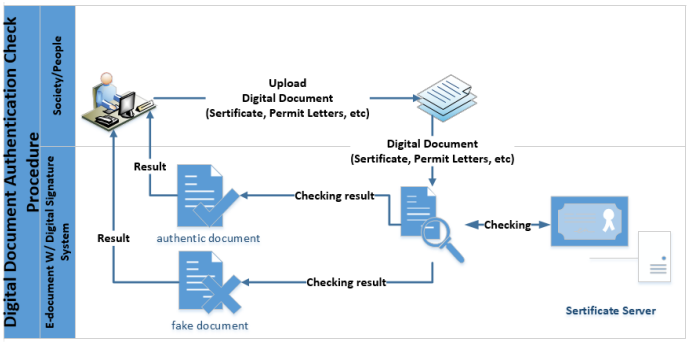


Fig. 5. Flowchart of cheking autentication e-document.

Technologies such as web servers, database servers and APIs are used to run systems online, and are connected to the internet as part of the public services that will be developed. Digital signatures generated in the e-document system, use the .p12 format which officially comes from the Indonesian Ministry of Communication and Information which acts as a Certificate Authority (CA) digital certificate and digital signature in Indonesia. P12 Algorithm is a digital signature algorithm developed by the Ministry of Communication and Information Technology Republic of Indonesia, using a combination of RSA Algorithm (Rivest-Shamir-Adleman) and SHA 256 (Secure Hash Algorithm). With a Key Public Key Length of 4096 bits. The meaning of the key area to look for is 2 4096, so that the attackers will find it very difficult to solve. Figure 6 shows the e-document system architecture.

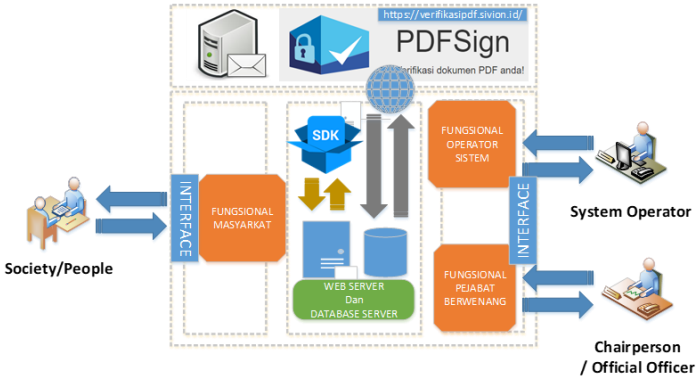


Fig. 6. Architecture e-document system.

Implementation carried out involves an example of a digital document that is legalized with a digital signature inside. The digital signature is embedded in the chairperson section as proof that the document has been legalized from the chairperson and the document is saved in the .pdf format. Figure 7 shows a digital document that is given a digital signature.


Nomor : 0011/S1/IJZ/UMARA/2017

UNIVERSITAS MADANGKARA

IJAZAH

Diberikan Kepada
Tempat Tanggal Lahir
Nomor Induk Mahasiswa
Program Pendidikan
Fakultas
Program Studi
Tanggal Lulus
Status

Ijazah ini diserahkan setelah yang bersangkutan memenuhi semua persyaratan yang ditentukan dan kepadanya dilimpahkan segala wewenang dan hak yang berhubungan dengan Ijazah yang dimilikinya serta berhak menyandang gelar akademik .....

Bandung,.....

DEKAN,

Alif Finandhita , S.Kom, M.T.

REKTOR

Irawan Afrianto

Irawan Afrianto, S.T, M.T.

Fig. 7. Digital document with digital signature.

For original documents (without any changes), the test results indicate that the digital signature in the document is valid. It is shown by the notification that the certificate is trusted, the certificate is verified and valid signature (three checklist in figure 8) , which mean it's indicated the authenticity of the document.

Fig. 8. Valid digital signature confirmation.

Meanwhile, if there is a change in the content of the document (such as text changes and document crops) , the system will indicate that the digital signature is no longer valid. The system will provide information that the document has changed, the signer's identity is not verified, the document does not have a time stamp and the document does not support LTV (four crosses in figure 9). This can be interpreted that the document has undergone a trial of forgery, which indicates that the document is a falsified document.

Fig. 9. Invalid digital signature confirmation.

4. Conclusions

This research has produced a model for e-document systems with digital signatures where the system developed has adapted to the needs of the users. The result of tests conducted, has been able to provide authentication to digital documents, changes made to the document, causing a digital signature to be invalid and this indicates the existence of attempts to falsify the document. In the future, the integration of the

system model developed must be able to be implemented with public services contained in the smart city perspective.

Acknowledgments

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 Strengthening, with contract numbers between L2DIKTI4 and Universitas Komputer Indonesia No. 2898/L4/PP/2019 in the Applied Research scheme for 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*, Waseda University. No 32, pp 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), pp.3-21.
3. Schipper R.; and Silvius A. (2018). Characteristics of Smart Sustainable City *Development: Implications for Project Management. Smart Cities*, 1(1), pp.75-97.
4. Von Haldenwang C. (2004). Electronic government (e-government) and development. *The European Journal of Development Research*, 16(2), pp.417-432.
5. Vukelich, S.R.; and Jenkins, J.E. (1982). Evaluation of component buildup methods for missile aerodynamic prediction. *Journal of Spacecraft and Rocket*, 19(6), 481-488.
6. López-López V.; Iglesias-Antelo S.; Vázquez-Sanmartín A.; and Connolly R., Bannister, F. (2018). e-Government, Transparency & Reputation: An Empirical Study of Spanish Local Government. *Information Systems Management*, 35(4), pp.276-293.
7. Rifauddin M. (2016). Pengelolaan Arsip Elektronik Berbasis Teknologi. *Khizanah al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, 4(2), pp.168-178.
8. Warasart M.; and Kuacharoen P. (2012). Based document authentication using digital signature and QR code. In *4TH International Conference on Computer Engineering and Technology ICCET* .
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), pp.39-46
10. Azdy R.A. (2016). Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 5(3), pp.184-191.
11. Pooja; and Mamta Y. (2018). Digital Signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, ISSN : 2456-3307, Volume 3 Issue 6, pp. 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 & Management*, 41(5), pp.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), p.3949.
14. Handley, M. (2018). Schnorr's Digital Signature and its Applications. Review of Computational Science and Engineering, 4(1), p.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), pp.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. *In Journal of Physics:* Conference Series (Vol. 978, No. 1, p. 012116). IOP Publishing.
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, pp.31630-31643.
18. Rajendran B.; Misbahuddin M.; Kaviraj S.; and Bindhumadhava B.S. (2018). Digital Tokens: A Scheme for Enabling Trust Between Customers and Electronic Marketplaces. In *Intelligent Computing and Information and Communication*, pp. 491-503.
19. Finandhita A.; and Afrianto I. (2018) : Development of E-Diploma System Model with Digital Signature Authentication. In *IOP Conference Series: Materials Science and Engineering*, vol. 407, no. 1, p. 012109. IOP Publishing.
20. Aptika A. Root CA dan Sertifikat Digital. 20 October 2018. [Online]. Avaliable: https://aptika.kominfo.go.id/2018/10/sertifikat-digital/ [Accessed : 1 Mei 2019].
21. Thasia. Sistem Verifikasi Online Nasional (SiVION). 27 October 2016. [Online]. Avaliable: https://aptika.kominfo.go.id/2016/10/841/ [Accessed : 1 Mei 2019].

Journal of Engineering Science and Technology
Vol. XX, No. Y (Year) PPP - QQQ

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

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

[1,2,3,4]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 has an effect on public services. This raises the spirit of turning paper documents that are commonly used into digital documents. Important letters such as certificates, permit letters and so on began to be developed towards digital documents. But to be used as a valid document, an authentication mechanism needs to be inserted in it. This authentication is a mechanism to replace the signature known as digital signature. Digital signature is a mechanism used to guarantee the authenticity of a digital document when the document is used for various things.The purpose and objective of this study is to provide an overview of e-document systems in the form of digital files as documents that have the same validity as paper documents through authentication of these documents with digital signatures. The test results show that e-document inserted with digital signature can be shown authenticity, as well as modified e-documents can be shown that the document is falsified document.

Keywords: E-document, Digital Signature, Public Services, p12, Smart City, Indonesia

1. Introduction

Smart city is a city that can manage all resources effectively and efficiently in solving various challenges, using innovative, integrated and sustainable solutions[1]. Smart city includes six aspects, namely governance, environment, economy, mobility, people, and living. The final result of smart city is the creation of efficiency, sustainability and quality of life [2][3]. One part of smart city services is e-government. E-government denotes the strategic, co-ordinated use of information and communication technologies (ICT) in public administration and political decision-making. The benefits it is expected to deliver are greater efficiency of the institutions concerned, improvements in public services, and political participation and transparency [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 must also provide transparency in order 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 characteristics are more flexible, search is easier, the possibility of missing is small, save space, archiving digitally, transfer documents more easily, improve security and easy in data recovery[7].

However, digital documents require a marker that can guarantee authenticity like other important paper documents. Digital signature is a solution that can be attached to a digital document to maintain the authenticity of the document [8]. Digital signatures are made with the help of cryptographic methods, with the aim of such an ordinary signature that is 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 are used in the development of digital signatures such as elgamal, Schnorr [14], and RSA [15]. In order to maintain the integrity of electronic documents, cryptographic algorithms are combined with several message digest methods such as MD5, SHA 256, SHA 521 and Base64 [16] [17] [18].

The objectives of this study 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.

2. Methods

The research method used in this study is a quantitative approach using descriptive methods, namely conducting a comparative study to compare the phenomena found and make classifications that are sourced from a standard. The research starts from the formulation of the problem, data collection (primary and secondary), data processing and analysis, and system modeling design that will be developed. Figure 1 shows the descriptive quanitative method used to develop the model [19].

Fig. 1. Research methods.

3. Result and Discussion

A document is an important work letter and usually signed by a leader or an authorized official. The signature indicates that the document is authentic and can be used for the purposes of the document. The disadvantages of paper documents are that they are easily damaged and lost, and the signatures attached to them 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 Ministry of Communication and Information of Indonesia through the Directorate General of Information Applications has a program in the framework of using national digital signatures. Through the Online Verification System (SiVION), the digital certificate validation will be done immediately (real time) on each Electronic Certification Operator (PsrE) with a certificate issuer (Root Certification Authority / Root CA) [20]. The National Identity Verification System (SiVION) provides a digital certificate to the applicant which becomes a validation for him 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. The aim is to maintain the validity of a document and show the legal status of the parties in the transaction [21]. Figure 2 shows the arcitecture of SiVION system.

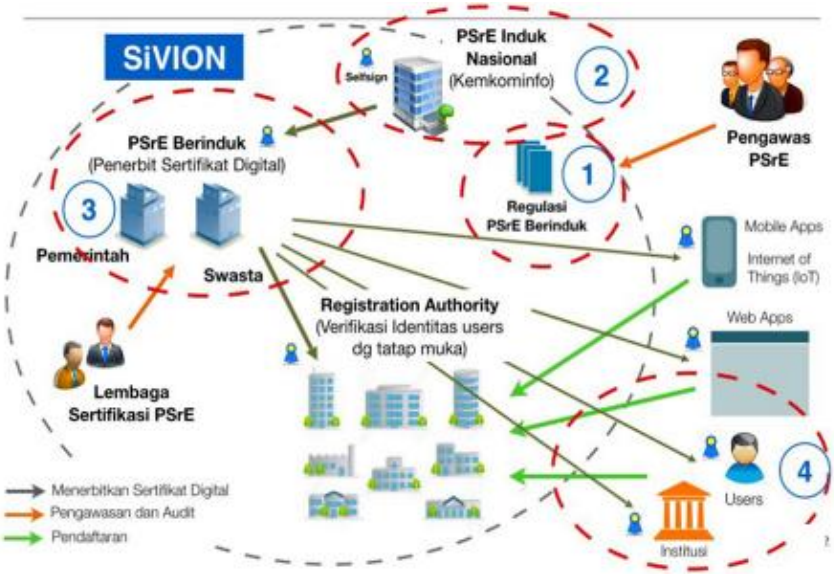


Fig. 2. The national identity verification system (SiVION)

The system model that will be developed is web-based with the site portal concept. The main function of the e-document system is to produce a digital document digitally signed (digital certificates are inserted in it) so that the digital document has the same strength as paper documents. The e-document system model, there are entities that interact with each other. From the user side, there are three users who will later use this system, namely the society/citizen, the chairperson/office officer and system operators. The system interface is provided to facilitate the needs and functions of each user. Figure 3 shows the concept model of e-document system.

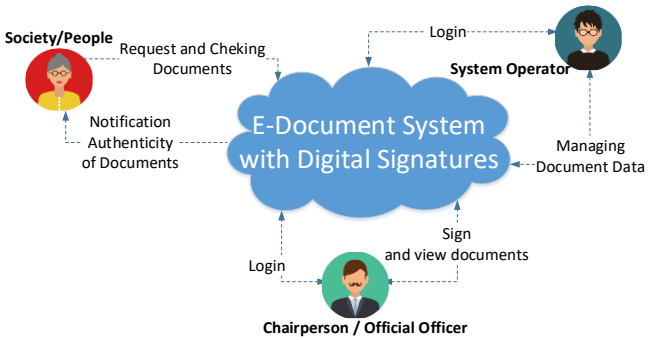


Fig. 3. E-document concept model.

The concept model consists of 2 main modules namely, digital document requesting and digital document checking. The document request module is used to create digital documents as shown in Figure 4., while checking digital documents is used to determine the authenticity of the documents, shown in Figure 5.

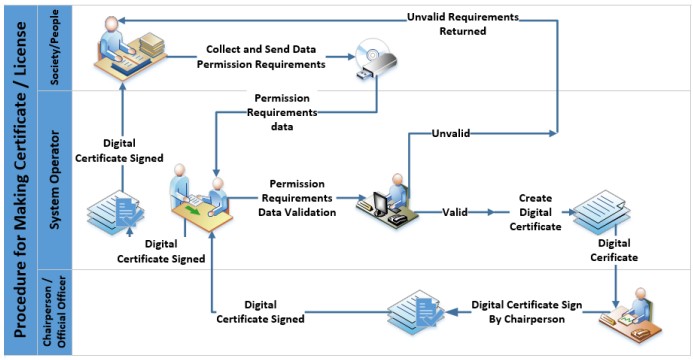


Fig. 4. Flowchart of create e-document.

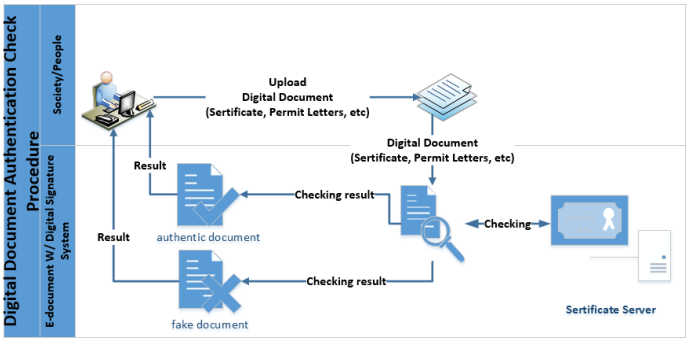


Fig. 5. Flowchart of cheking autentication e-document.

Technologies such as web servers, database servers and APIs are used to run systems online, and are connected to the internet as part of the public services that will be developed. Digital signatures generated in the e-document system, use the .p12 format which officially comes from the Indonesian Ministry of Communication and Information which acts as a Certificate Authority (CA) digital certificate and digital signature in Indonesia. P12 Algorithm is a digital signature algorithm developed by the Ministry of Communication and Information Technology Republic of Indonesia, using a combination of RSA Algorithm (Rivest-Shamir-Adleman) and SHA 256 (Secure Hash Algorithm). With a Key Public Key Length of 4096 bits. The meaning of the key area to look for is 2 4096, so that the attackers will find it very difficult to solve. Figure 6 shows the e-document system architecture.

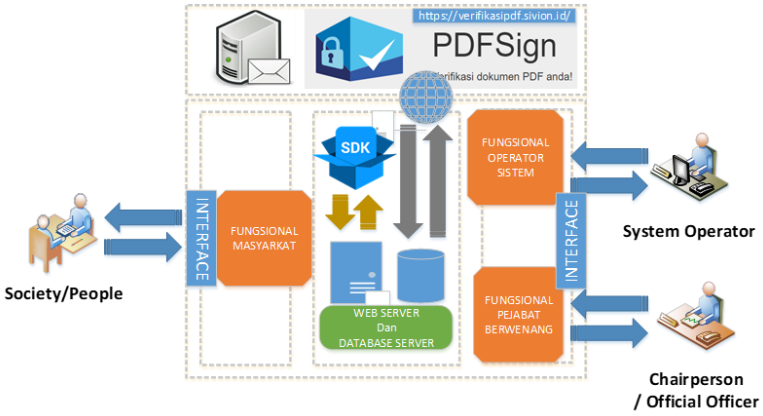


Fig. 6. Architecture e-document system.

Implementation carried out involves an example of a digital document that is legalized with a digital signature inside. The digital signature is embedded in the chairperson section as proof that the document has been legalized from the chairperson and the document is saved in the .pdf format. Figure 7 shows a digital document that is given a digital signature.


Nomor : 0011/S1/IJZ/UMARA/2017

UNIVERSITAS MADANGKARA

IJAZAH

Diberikan Kepada
Tempat Tanggal Lahir
Nomor Induk Mahasiswa
Program Pendidikan
Fakultas
Program Studi
Tanggal Lulus
Status

Ijazah ini diserahkan setelah yang bersangkutan memenuhi semua persyaratan yang ditentukan dan kepadanya dilimpahkan segala wewenang dan hak yang berhubungan dengan Ijazah yang dimilikinya serta berhak menyandang gelar akademik .....

Bandung,.....

DEKAN,

Alif Finandhita , S.Kom, M.T.

REKTOR

Irawan Afrianto

Irawan Afrianto, S.T, M.T.

Fig. 7. Digital document with digital signature.

For original documents (without any changes), the test results indicate that the digital signature in the document is valid. It is shown by the notification that the certificate is trusted, the certificate is verified and valid signature (three checklist in figure 8) , which mean it's indicated the authenticity of the document.

Fig. 8. Valid digital signature confirmation.

Meanwhile, if there is a change in the content of the document (such as text changes and document crops) , the system will indicate that the digital signature is no longer valid. The system will provide information that the document has changed, the signer's identity is not verified, the document does not have a time stamp and the document does not support LTV (four crosses in figure 9). This can be interpreted that the document has undergone a trial of forgery, which indicates that the document is a falsified document.

Fig. 9. Invalid digital signature confirmation.

4. Conclusions

This research has produced a model for e-document systems with digital signatures where the system developed has adapted to the needs of the users. The result of tests conducted, has been able to provide authentication to digital documents, changes made to the document, causing a digital signature to be invalid and this indicates the

existence of attempts to falsify the document. In the future, the integration of the system model developed must be able to be implemented with public services contained in the smart city perspective.

Acknowledgments

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 Strengthening, with contract numbers between L2DIKTI4 and Universitas Komputer Indonesia No. 2898/L4/PP/2019 in the Applied Research scheme for 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*, Waseda University. No 32, pp 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), pp.3-21.
3. Schipper R.; and Silvius A. (2018). Characteristics of Smart Sustainable City *Development: Implications for Project Management. Smart Cities*, 1(1), pp.75-97.
4. Von Haldenwang C. (2004). Electronic government (e-government) and development. *The European Journal of Development Research*, 16(2), pp.417-432.
5. Vukelich, S.R.; and Jenkins, J.E. (1982). Evaluation of component buildup methods for missile aerodynamic prediction. *Journal of Spacecraft and Rocket*, 19(6), 481-488.
6. López-López V.; Iglesias-Antelo S.; Vázquez-Sanmartín A.; and Connolly R., Bannister, F. (2018). e-Government, Transparency & Reputation: An Empirical Study of Spanish Local Government. *Information Systems Management*, 35(4), pp.276-293.
7. Rifauddin M. (2016). Pengelolaan Arsip Elektronik Berbasis Teknologi. *Khizanah al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, 4(2), pp.168-178.
8. Warasart M.; and Kuacharoen P. (2012). Based document authentication using digital signature and QR code. In *4TH International Conference on Computer Engineering and Technology ICCET* .
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), pp.39-46
10. Azdy R.A. (2016). Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 5(3), pp.184-191.
11. Pooja; and Mamta Y. (2018). Digital Signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, ISSN : 2456-3307, Volume 3 Issue 6, pp. 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 & Management*, 41(5), pp.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), p.3949.
14. Handley, M. (2018). Schnorr's Digital Signature and its Applications. Review of Computational Science and Engineering, 4(1), p.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), pp.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. *In Journal of Physics:* Conference Series (Vol. 978, No. 1, p. 012116). IOP Publishing.
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, pp.31630-31643.
18. Rajendran B.; Misbahuddin M.; Kaviraj S.; and Bindhumadhava B.S. (2018). Digital Tokens: A Scheme for Enabling Trust Between Customers and Electronic Marketplaces. In *Intelligent Computing and Information and Communication*, pp. 491-503.
19. Finandhita A.; and Afrianto I. (2018) : Development of E-Diploma System Model with Digital Signature Authentication. In *IOP Conference Series: Materials Science and Engineering*, vol. 407, no. 1, p. 012109. IOP Publishing.
20. Aptika A. Root CA dan Sertifikat Digital. 20 October 2018. [Online]. Avaliable: https://aptika.kominfo.go.id/2018/10/sertifikat-digital/ [Accessed : 1 Mei 2019].
21. Thasia. Sistem Verifikasi Online Nasional (SiVION). 27 October 2016. [Online]. Avaliable: https://aptika.kominfo.go.id/2016/10/841/ [Accessed : 1 Mei 2019].