Prototype of E-Document Application Based on Digital Signatures to Support Digital Document Authentication

I Afrianto¹*, A Heryandi², A Finandhita³, S Atin⁴

¹,²,³,⁴ Program Studi Teknik Informatika, Universitas Komputer Indonesia, Indonesia.

Email: *irawan.afrianto@email.unikom.ac.id

Abstract. The purpose of this research is to develop a prototype of a web-based application that can be used to provide digital signatures on files or digital documents. This prototype uses a digital signature mechanism issued by the Ministry of Communication and Information of the Republic of Indonesia (KOMINFO). The results of the research conducted by using the alpha test showed that all functionalities in the application have been able to run well. While the authentication test shows that any changes made to a document that has a digital signature will invalidate the digital signature, which means that there are attempts to falsify documents and their authenticity can be identified. This is because in documents that have the digital signature will have a certain hash value which if the document is changed or modified, then the hash value will change. This is what determines whether a document is still original or has been modified its contents, namely by comparing the hash value contained in the document.

1. Introduction

Electronic documents (e-document) are part of public services that are used to replace paper documents because they have more flexible characteristics, easier searching, save space, digital archiving, easier document transfer and better and easier security in data restoration. [1]. In order to improve the security of data in a digital document, a mechanism is needed to protect it [2]. Digital signatures are solutions that can be attached to digital documents to maintain the authenticity of electronic documents [3]. Digital signatures are created with the help of cryptographic methods, with the aim of such a regular signature being place an author authentication on documents [4] [5].

Three basic things in the digital signature process are checking the signature authentication, document authentication, and verification of digital signatures [6]. The strength of a digital signature depends on the cryptographic method used and the key length [7]. Several algorithms are used in the development of digital signatures such as Elgamal, Schnorr [8], and RSA [9].

The purpose of this research is to build a prototype for an e-document system based on digital signatures where the models and designs that were built were measured using a Blackbox approach and usability test from the prospective user side.

2. Method

This research began with the literature review stage which aimed to summarize similar studies as initial identification of research to be conducted, and followed by analyzing and modeling the system using UML to determine the functional and non-functional requirements of the system [10]. The third stage was developing the prototype e-document system and concluded with testing of the prototype system that had been built (Figure 1).
3. Results and Discussion

The e-document system is used as a solution to reduce the number of paper documents (files, letters or certificates) that are usually signed by the leader/official in charge. The authentication of digital files and certificates uses digital signatures developed by the Ministry of Communication and Information of the Republic of Indonesia. The flow of business processes carried out in the system process to be designed includes the procedure for requesting letters/certificates to be signed, as well as the process of signing digital documents using digital signatures.

Procedure for requesting letters or certificates or other securities starts from the community or division or part of the scope of the agency, where users must upload the data needed to make the letter or digital certificate. Figure 2 shows the procedure for requesting digital documents (e-documents).

Meanwhile, to verify the authenticity of the digital document, a verification procedure is needed to authenticate the electronic document into the e-document system. The user uploads a digital document to verify its authenticity, then the system will verify and validate the authenticity of the document. If there is no change in the contents of the document, then the document is said to be original, while if the content is changed in the document, then the document can be called fake. The flow of the digital document verification business process can be seen in Figure 3.
3.1 Systems analysis and modeling

The system model was developed to show the functions and of the interrelated entities in order to produce good system performance. The e-document system model developed can be seen in Figure 4.

In the e-document system architecture model, a system interface is provided to facilitate the needs and functions of each user. Technologies such as web servers, database servers, web services and APIs are used to run systems online, and to connect to the internet as part of public services to be developed (Figure 5).
One tool that can be used to model software functional requirements is to use UML (Unified Modeling Language). Modeling is done using a use case diagram (Figure 6).

3.2 Prototype Testing

Testing the e-document system is carried out in accordance with the functional in the system.

1. Open the e-document application with the site address: https://tt-el.my.id. Figure 7 shows the landing page of the prototype of the digital signature application.
2. Uploading files to be signed. This menu is used to display the feature of sending files to be signed to the server. If this menu is clicked, it will display the file filling page that will be sent which can be seen in Figure 8.

3. Checking files in the system is to see whether the file is actually stored on the server. Figure 9 shows the files to be signed are in the application server.
4. Downloading files: To carry out digital (electronic) signature, users can click on the button to the right of the file. If the digital signature is successful, then the user will be given a dialog screen for inputting the location of the downloaded file to be saved (Figure 10). While the results of files that have been digitally signed can be seen in Figure 11.

5. Checking the authenticity of documents that have been digitally signed. To identify the authenticity of the document, you can access the site https://tte.kominfo.go.id/verifyPDF. The site can confirm the authenticity of a document (if it hasn't changed), as shown in Figure 12, and can show invalidity of the digital signature when the document changes, and this can be indicated by the falsification of the document (Figure 13).
4. Conclusion
The results of this study indicate that the prototype e-document system can be used to perform document data management activities. The prototype was able to digitally sign documents using the KOMINFO Republic of Indonesia's digital signature scheme. Test results show that documents that have been digitally signed can be authenticated, while efforts to falsify documents can be demonstrated by invalid digital signatures contained in these documents. Future research certainly tries to apply this prototype for public services in government agencies so that it is faster, more accurate, and safe [11].

Acknowledgment
The research was funded by a grant from the Ministry of Research and Higher Education (KEMENRISTEKDIKTI) Republic of Indonesia - Directorate General of Research and Development Strengthening, with Decree Number 7 / E / KPT / 2019 and Agreement / Contract Number 047 / SP / LPPM / UNIKOM / III / 2019 on the Applied Research scheme for 2019-2020.
References

[1] Hassan, R.G. & Khalifa, O.O. 2016. E-Government-an Information Security Perspective. *International Journal of Computer Trends and Technology (IJCTT)*, 36(1), pp. 1-9.

[2] Pappel, I., Pappel, I., Tepandi, J. & Draheim, D. 2017. Systematic digital signing in estonian e-government processes. In *Transactions on large-scale data-and knowledge-centered systems XXXVI* (pp. 31-51). Springer, Berlin, Heidelberg.

[3] Rifauddin, M. 2016. Pengelolaan Arsip Elektronik Berbasis Teknologi. *Khizanah al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, 4(2), pp. 168-178.

[4] Finandhita A., & Afrianto I. 2018. Development of E-Diploma System Model with Digital Signature Authentication. In *IOP Conference Series: Materials Science and Engineering*, 407(1), p. 012109. IOP Publishing

[5] Smael, A. & Okumus, I. 2017. Design and Implementation of an Electronic Document Management System. *Mehmet Akif Ersoy Üniversitesi Uygulamali Bilimler Dergisi (MAKUUBD)*, 1(1), pp. 9-17.

[6] Buccafurri, F., Fotia, L. & Lax, G. 2016. Implementing advanced electronic signature by public digital identity system (SPID). In *International Conference on Electronic Government and the Information Systems Perspective* (pp. 289-303). Springer, Cham.

[7] Afrianto, I., Suryana, T., & S Atin, S. 2015. Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009. *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, 6(1), pp. 43-49.

[8] Pooja, Mamta Y. 2018. Digital Signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCEIT)*, 3(6), pp. 71-75

[9] Shaker, S.H. & Jumaa, G.G. 2017. Digital Signature Based on Hash Functions. *International Journal Of Advancement In Engineering Technology, Management and Applied Science (IJAETMAS)*, 4(1), pp. 88-99.

[10] Heryandi, A., & Afrianto, I. 2019. Online Diploma Supplement Information System Modelling for Indonesian Higher Education Institution. In *IOP Conference Series: Materials Science and Engineering* 662(2), p. 022092. IOP Publishing.

[11] Afrianto, I., Heryandi, A., Finandhita, A. & Atin, S., 2018. *E-Document Authentification With Digital Signature For Smart City: Reference Model*. 407, pp. 1-6.