ICIC Express Letters
Part B: Applications
Volume **12**, Number **11**, November **2021**

ICIC International ©2021 ISSN 2185-2766
pp. **987–993**

THE USE OF DIGITAL SIGNATURES IN THE BUSINESS WORLD IN THE INDUSTRIAL REVOLUTION 4.0 ERA

Wahyu Sardjono[1], Wowon Priatna[2], Pardiyo[3], Gustian Rama Putra[4] and Hanny Juwitasary[5]

[1]Information Systems Management Department, BINUS Graduate Program – Master of Information Systems Management
[5]Information Systems Department, School of Information Systems
Bina Nusantara University
Jl. K. H. Syahdan No. 9, Kemanggisan, Palmerah, Jakarta 11480, Indonesia
wahyu.s@binus.ac.id; hjuwitasary@binus.edu

[2]Informatics Engineering
Engineering, Bhayangkara University
Jl. Harsono RM No. 67 Ragunan Pasar Minggu, South Jakarta, DKI Jakarta 12140, Indonesia
wowon.priatna@dsn.ubharajaya.ac.id

[3]Master of Management, Faculty of Economics and Business
Gadjah Mada University
Yogyakarta 55281, Indonesia
pardiyo@ugm.ac.id

[4]Computer Science Study Program, Faculty of Mathematics and Natural Sciences
Pakuan University
Jl. Pakuan, Tegallega, Bogor 16129, Indonesia
gustian.rama@unpak.ac.id

Received January 2021; accepted April 2021

Abstract. *The industrial revolution 4.0 is marked by the development and use of technology that is very broad, covering all fields from education, transportation, health, communication, government, defense and security, business, and other areas connected to the Internet. Along with these technological advances, the use of the Internet is a necessity. So that in the industrial era 4.0, it is also marked by the use of the Internet in many aspects and the Internet has become a necessity or a condition called the Internet of Things. The use of the Internet, which is very broad in all fields, is beneficial in the process of daily activities. In the field of communication, it is certainly very helpful in conveying information quickly so that it can get information in real time. One of the uses of technologies that are supported by the Internet in the business world is the use of digital signatures. Using a digital signature, the parties who will sign a document do not have to meet face to face in a location. They just sign through the system. This kind of process will make it easier in the business process. To maintain the confidentiality and security of using digital signatures, it is necessary to pay attention to terms and conditions so that these documents' authentication is guaranteed. For this reason, the use of digital signatures should be done by using a signature in a certified system. This research provides an overview of the importance of maintaining confidentiality and security in the use of digital signatures.*

Keywords: Industry 4.0, Technology, Internet, Digital signature, Business

1. **Introduction.** In the industrial era 4.0, all computers are connected to a shared network or commonly known as being connected to the Internet. The Internet of Things or IoT is what drives technological progress in all fields and encourages efficiency in life processes. With the use of the Internet combined with the capabilities of computer

DOI: 10.24507/icicelb.12.11.987

technology, it is possible to make computers small in size but can process data faster and larger. The rapid development of technology today can simplify various jobs, one of which is by searching for and using digital signatures or e-signatures. We can sign many files or documents via electronic devices such as smartphones or computers connected via the Internet network. Breakthroughs like this are certainly very helpful in jobs that require a lot of document signatures or correspondence. This condition was made possible during the Covid-19 pandemic by carrying out work from home. Companies do many international transactions and require file signing and no longer need to come to the file storage location. Various banking risks in using the Internet really need anticipation and alternative solutions to overcome the risk of uncertainty that occurs. The existence of an electronic signature (e-signature) is one of the answers to this condition and is no exception including digital signatures [1]. Electronic signature is one of the authentication technologies that are considered safe enough to be used [2], to replace conventional hand gestures, this is understandable because of the rapid development of technology in line with digitization in the 4.0 industrial revolution which of course demands changes in the process of signing of important document [3]. Currently, digital signature is part of the message which confirms the correct source and indicates that the message has not changed during the course of the document [4]. The data is encrypted uniquely and identifies the sender by ensuring proper document integrity because technically only recipients with the right software can read the signature code [5]. So that the recipient of a document with a digital signature can ensure that the document does not change on the way [6].

2. **Literature Review.** Literature review of this paper is sourced from various literature on which the writing is based. Literature comes from papers, journals, and articles on blogs or websites from the Internet. The digital signature is a unique combination of hash function and encryption with asymmetric methods [7]. To be able to sign an electronic document, the document will be used as an input to the hash function. The hash function is a one-way function that produces a specific function on every data entered in the hash function [8]. The process starts from the sender of the message, namely the party who signed the document signed the signature then processed through the hash function and encrypted. The result of the encryption process is a digital signature sent to the recipient. Every difference that occurs in one bin in a documented content that has been generated will have a certain hash value [9]. Digital signature processing can be seen in Figure 1.

Electronic signatures can verify the authenticity of the received documents. The use of communication information technology in government agencies is expected to be one of the drivers in realizing environmentally friendly offices [11]. Digital signatures in Indonesia are regulated in Government Regulation No. 82/2012 concerning the Implementation of Electronic Systems and Transactions, which functions as an authentication and verification tool. A digital signature is an ordinary signature that is made electronically which has the same function as an ordinary signature on a document or file [12]. Signature is data if it is not faked, it can function that the person whose name is listed on a document or file agrees with what is stated on the file and the document that is signed. According to Law No. 19 of 2016 of the Republic of Indonesia concerning Electronic Transactions and Information (UU ITE), which is an amendment to the ITE Law No. 11 of 2008, an electronic signature is a signature consisting of electronic information that is attached, associated or related to other electronic information that is used as a verification and authentication tool [13].

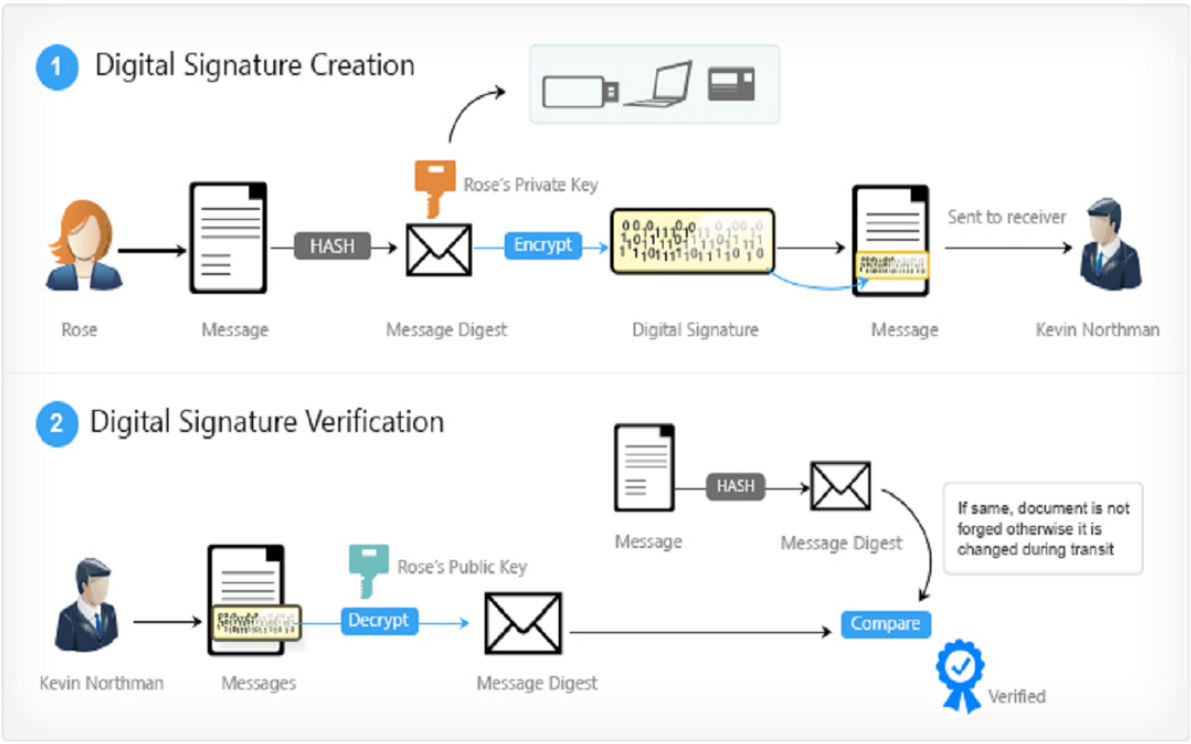

FIGURE 1. Process for creating and verifying electronic signatures [10]

3. **Methodology.** The methodology used in writing this paper is by collecting various literature from the Internet, such as journals, papers, articles related to the topic as a source of information. Furthermore, the various sources are analyzed and processed further as a reference and enrich the material and examine the linkages between these sources that support the writing of this paper. In summary, the methodology is

1) Collecting various sources of information in the form of journals, papers and articles from the Internet;
2) Identify various sources of information that has been collected that are relevant to the topic discussed;
3) Analyze the linkage of the identified information;
4) Compile and rewrite in a structured manner from various literature sources that have been identified as relevant as the paper presented.

4. **Result and Discussion.** Digital signature is one of the ways used to guarantee the authenticity of the document, so that the recipient of the document gets a guarantee that the document received from the other party is the original document [14]. Digital signatures can serve as a tool to verify and authenticate the identity of the party, signing a document as well as to gain confidence in the authenticity of the signature stated on the document. The signature can be in the form of a certified signature. Electronic certification of a digital signature is carried out by the Electronic Certification Operator. It is easy to prove the authenticity of a digital signature when the signature is certified. Conversely, if the digital signature is not certified, it will have reverse proof properties where the party who signed the signature must prove that the digital signature does not belong to him.

4.1. **Legal basis.** In Indonesia, the use of digital signatures has begun to be regulated in Government Regulation (PP) No. 82 of 2012, concerning the Implementation of Electronic Systems and Transactions. This PP applies to all electronic system operators. Whereas what is meant by the operator here is every person, state administrator, business

entity, and society who provides, manages and/or operates electronic systems individually or jointly to electronic system users for their own needs and/or the needs of other parties (Electronic Transaction and System Administration, 2012). In this PP, every public service is required to use an electronic certificate. This Government Regulation is strengthened by the ITE Law, which also protects digital signatures.

Online Verification System (SiVION) provides digital certificates for applicants who use digital signatures to conduct transactions electronically. SiVION also provides digital certificate validation to applicants. Digital certificate validation is carried out to the respective Electronic Certificate Providers (PSrE), and its parent is the certificate issuer (Root Certification Authority/Root CA). Kominfo also prepares a National Root CA by legalizing Government CA and Private CA and provides education to the public because there are additional business processes in online transactions [15]. The government is also very supportive of improving public services to the community in this case that are electronic-based for all parties, both for individuals, the private sector, community groups and the government itself. Ministry of Technology and Information as of the Root Certification Authority (CA) can provide authority in the form of a CA as a guarantor of public identity. Along with the development of technology, especially in the conditions of the Covid-19 pandemic, it is hoped that more parties will be able to issue digital certificates so as to increase the use of digital signatures (paperless). This process is no longer affixing or pasting a manual signature that is affixed to digital documents but using a certified digital signature because this will get a guarantee of confidentiality, and safeguard the message content from unauthorized parties [16].

The legal basis for the use of digital signatures in Indonesia is regulated in Law No. 19 of 2016 of the Republic of Indonesia concerning Electronic Transactions and Information (UU ITE) which is an amendment to the ITE Law No. 11 of 2008. The law states the meaning and signs of digital hand. In contrast, a digital signature is a signature consisting of digital information that is embedded associated or related to other digital information which functions as a verification and authentication tool. Before implementing a digital signature, it is necessary to delve deeply into this digital signing process. Because if you do not understand properly and correctly, digital signatures will also be vulnerable to forgery. According to the Government Regulation of the Republic of Indonesia No. 82 of 2012 paragraph 3, the following are the conditions that must be met in the use of digital signatures.

1) The confidentiality of the manufacturing process must be guaranteed. This is very important so that it is kept confidential and is not misused by other parties.
2) Using a special cryptographic lock so that it is not easily penetrated. As explained above that for the security of digital signature storage, it must be very strict.
3) Storage media must also be ensured that it is safe from use and susceptibility to viruses. Because if the file is infected with a virus and the virus steals important data, including digital signatures, the hackers can use the stolen file for a crime.
4) The owner of the signature has full rights to store the digital signature because otherwise, it can be dangerous and very vulnerable to being misused by other parties.
5) Digital signature storage media is also ensured to be able to detect or detect any irregularities that occur in the file. The slightest change will have a negative impact on digital signature holders because it is very risky if there is a fraud because the signed document is an electronic document.
6) Parties involved in the digital signature process must be trusted to maintain.

The PP also states that the digital signature also functions as a tool for verification and assessing the authenticity of the signer's identity, integrity and authenticity of electronic information. In addition, for every digital document that is distributed through electronic

media, the approval is in the form of the digital signature, not a wet-signature scanned from a scanner.

4.2. **Digital signs in business.** Businesses in modern economic development today are heavily influenced by technological innovations that significantly change customer behavior [17]. Electronic commerce transaction is a trade transaction conducted between the seller and the buyer in meeting the needs of goods, services, by transferring rights through electronic media so that the parties do not need to be physically present but the transaction using the Internet network [18]. To make transactions with the Internet the signature in the transaction document that is done can be done with a digital signature. Digital signatures done directly today have been in demand by businesses, especially those who need transaction practically [19]. The use of digital signatures in business in the industrial era 4.0 is very important because it can simplify the process of signing a document. Using a digital signature is also very efficient in terms of both time and cost because the parties who will sign the signature do not have to come or meet at the location where the document is located [20]. However, with current technological advances which are supported by the very widespread use of the Internet in the industrial era 4.0, the use of a digital signature that is certified in a document can be verified the authenticity of the document. The process of using a digital signature that is certified for business purposes can be illustrated in the example used or issued by the Public Printing Company of the Republic of Indonesia or PERURI. Companies that will use a digital signature in order to be certified for authenticity can register the use of that signature on a system issued by PERURI [21]. After registering for the use of the system, the company will be given access. The examples of this process are as follows [22].

1) Access the web portal with a browser (Chrome or Mozilla), and click the "Account Registration" button shown in Figure 2.

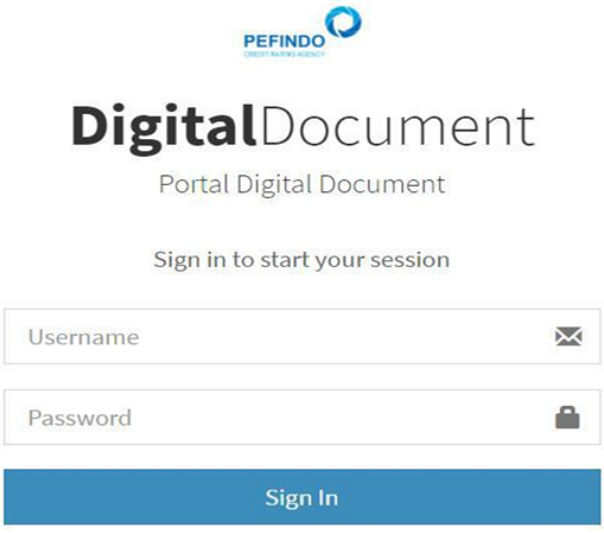

FIGURE 2. Login page – https://e-form.peruri.co.id/perisai-pefindo/login

After that, a form will appear to upload the ID Card.

2) Upload ID card (max 1 MB in .jpg, .jpeg or .png format) shown in Figure 3.

Fill in the fields according to the data on the ID Card. Make sure that the field "Email address" is filled with a work email address. Make sure the field "Handphone number" is filled with cellular phone numbers that can receive SMS (Do not forget to top up your credit). Field "Organization unit" must be filled in with the name of your respective division. The field "Front View Employee Card Photo" must be filled in by uploading image of each company ID Card.

FIGURE 3. Upload form image ID card (https://e-form.peruri.co.id/perisai-pefindo/login)

If successfully registered, a confirmation message will appear that the registration was successful with specific username and password. After successful sign-in, you can set the initial specimen by clicking "Change Specimen". Furthermore, you can try out the digital signing procedure according to the given guidelines.

5. **Conclusion.** In the industrial era 4.0 which is marked by the widespread use of the Internet in the field of public life or what is known as the Internet of Things, it also has a huge impact on all areas. One of the positive effects in the business world is the use of digital signatures. Especially in the current Covid-19 pandemic situation where everyone is trying to maintain their distance, reducing face-to-face meetings, the use of digital signatures is felt to be very important. Digital signatures can also provide more assurance about the security of a document than a regular signature. The party receiving the digitally signed document can check whether the document is a document that came from the correct sender and can check whether the document has been altered after being affixed with the digital signature, whether intentionally or unintentionally.

So, it can be concluded that using a digital signature will simplify and speed up the process of signing a document because the parties do not have to meet in one location. Using a digital signature will be very efficient in business processes. This conclusion also supports the research that has been done previously, which states the need to apply an electronic signature or e-signature to government electronic documents. Electronic signatures can verify the authenticity of the received documents. Besides, the use of digital signatures can reduce paper usage.

However, what needs to be considered to maintain confidentiality and security in the use of digital signatures is that we must pay attention to the terms and processes for using the digital signature. To the identity of the signature owner to be verified, the digital signature needs to be registered with the document certification agency. If the signature has been certified, the document affixed with the signature can be verified for authenticity so that its authenticity will be guaranteed. If the document that has a certified digital signature is changed after being affixed with a digital signature, data and messages will appear regarding the change in the document.

REFERENCES

[1] S. Crook, Get the full e-signature picture to avoid falling foul of the law, *Computer Fraud & Security*, vol.2018, no.8, pp.12-14, 2018.

[2] P. Dutta, T. Choi and R. Butala, Blockchain technology in supply chain operations: Applications, challenges and research opportunities, *Transportation Research Part E: Logistics and Transportation Review*, vol.142, article no.102067, 2020.
[3] S. Mason, Documents signed or executed with electronic signatures in English law, *Computer Law & Security Review*, vol.34, no.4, pp.933-945, 2018.
[4] C. Eduard, M. Yoland and N. Daries, Rural cooperatives in the digital age: An analysis of the Internet presence and degree of maturity of agri-food cooperatives' e-commerce, *Journal of Rural Studies*, vol.74, pp.55-66, 2019.
[5] G. M. Abdulfattah, M. N. Ahmad and R. R. A. Asaad, A reliable binarization method for offline signature system based on unique signer's profile, *International Journal of Innovative Computing, Information and Control*, vol.14, no.2, pp.573-586, 2018.
[6] L. Zhang, H. Zhang and H. Xian, Blockchain-based two-party fair contract signing scheme, *Information Sciences*, vol.535, pp.142-155, 2020.
[7] J. F. Gomila and M. F. Hinarejos, A 2020 perspective on a fair contract signing protocol with blockchain support, *Electronic Commerce Research and Applications*, vol.42, article no.100981, 2020.
[8] H. Saripan and Z. Hamin, The application of the digital signature law in securing Internet banking: Some preliminary evidence from Malaysia, *Procedia Computer Science*, vol.3, pp.248-253, 2011.
[9] J. H. Lee, W. G. Lim and J. I. Lim, A study of the security of Internet banking and financial private information in South Korea, *Mathematical and Computer Modelling*, vol.58, nos.1-2, pp.117-131, 2013.
[10] B. Machkour and A. Abriane, Industry 4.0 and its implications for the financial sector, *Procedia Computer Science*, vol.177, pp.496-502, 2020.
[11] A. Nugraha and A. Mahardika, Application of electronic signatures in government electronic systems to support e-government, *National Seminar on Indonesian Information Systems*, Sesindo, 2016.
[12] F. Z. Abraham, P. I. Santosa and W. W. Winarno, Digital signature as a green information and communication technology (ICT) solution, *Journal of the Telematics and Information Society*, vol.9, no.2, pp.111-124, 2018.
[13] S. S. Al-Gahtani, Modeling the electronic transaction acceptance using an extended technology acceptance model, *Applied Computing and Informatics*, vol.9, no.1, pp.47-77, 2021.
[14] J. Domashova and E. Kripak, Identification of non-typical international transaction on bank cards of individuals using machine learning methods, *Procedia Computer Science*, vol.190, pp.178-183, 2021.
[15] B. K. Hutasuhut, S. Efendi and Z. Situmorang, Digital signature to maintain data authenticity with MD5 algorithm and RSA algorithm, *National Journal of Informatics and Networking Technology (Infotekjar)*, vol.3, no.2, pp.164-169, 2019.
[16] L. D. Hollebeek and K. Macky, Digital content marketing's role in fostering consumer engagement, trust, and value: Framework, fundamental propositions, and implications, *Journal of Interactive Marketing*, vol.45, pp.27-41, 2019.
[17] H. Choi, M. J. Park, J. J. Rho and H. Zo, Rethinking the assessment of e-government implementation in developing countries from the perspective of the design-reality gap: Application in the Indonesian e-procurement system, *Telecommunications Policy*, vol.40, no.7, pp.644-660, 2016.
[18] E. Turban, C. Pollard and G. Wood, *Information Technology for Management*, 11th Edition, John Wiley & Sons, Wiley Custom, 2018.
[19] R. Sitepu, Digital signature insurance in e-commerce agreement, *Journal of Lawa*, vol.1, no.1, pp.46-55, 2018.
[20] A. Delvia, Use of electronic signature in financing application based on sharia principles, *Journal of Business and Economic Accounting*, vol.5, no.1, 2019.
[21] C. Kabengele and R. Hahn, Institutional and firm-level factors for mobile money adoption in emerging markets – A configurational analysis, *Technological Forecasting and Social Change*, vol.171, DOI: 10.1016/j.techfore.2021.120934, 2021.
[22] Gupta, Y. A. Tung and J. R. Marsden, Digital signature: Use and modification to achieve success in next generational e-business processes, *Information & Management*, vol.41, no.5, pp.561-575, 2004.