Talent Development & Excellence
Vol.12, No.1, 2020, 1624-1629

Application Of Digital Signature To Increase Investment In Indonesia

Firman Freaddy Busroh, Fatria Khairo, Jauhariah
Sumpah Pemuda School of Law, Palembang, Sumatera Selatan, Indoinesia.

Abstract

One investment problem in Indonesia is the complexity of managing procedures for investment. So many licenses and signatures are required by the authorities with the necessity to be done in person or face to face. Although many policy packages and deregulation efforts for investment acceleration have been made, implementation of policies in the field is still weak and has not yet fully adopted the digital system in investment management services. The study aims to analyze how to optimizing the digital signature in improving the investment climate in Indonesia. The study used method normative juridical research method or library research is to examine a legal problem and make the settlement through the legislation in Indonesia. The results showed that the adoption of digital signatures is expected to optimize the investment climate in Indonesia, especially related to regulations, making it easier for investors to develop their investments in Indonesia.

Keywords: digital signatures, investment, regulations, doing business.

1. Introduction

One of investment problem in Indonesia procedure is set to invest still too complicated with the obligation of investment form filling quite thick and requires so many signatures by the authorities and must be done in person or face to face. It is very slow the process of legality in the administration (Butt, 2012). These conditions pose a problem of trust. Although a great deal of policy packages and deregulation efforts have been made and some regions have made great advancement (Von Luebke et al., 2009), however, the implementation of policies in the field is still weak (Harjono, 2007). One of investment problem in Indonesia is a procedure established for investing still too complicated with the obligation of filing a considerable investment thick and requires so many signatures by the authorities and must be done in person or face to face. Of course, it is very slow the process of legality in the administration. These conditions pose a problem of trust. While a great deal of policy packages and deregulation efforts, however, if the information on the implementation of policies in the field is still weak, it remains challenging to accelerate investors.

Regarding the regulation should be optimized to increase investment in Indonesia, the authors are interested in creating a regulation that must be followed a world increasingly emphasizes patterns of software technology, such as e-commerce, digital signatures. In developed countries, such as in the United States, some states already apply the rules on digital signatures (see, for instance, Stern, 2001). Some states make a very comprehensive regulation, but there is also very quick to make regulations. Even some countries that incorporate the regulation on the internet and multimedia information, such as in Malaysia (Chong, 1998). Moreover, the actual digital signature regulations regarding already exist in Indonesia, namely Law No. 11/2008 on information and electronic transactions. However, because of the limited budget to support the infrastructure of the digital signature then it is not optimal in practice, especially in supporting the investment climate in Indonesia. Related about the regulations that

ISSN 1869-0459 (print)/ ISSN 1869-2885 (online)

http://www.iratde.com

must be optimized to increase investment in Indonesia, the authors are interested in creating a regulation that should be able to follow the pattern of the world are increasingly prioritizing device technology software, such as e-commerce, digital signatures, the study aims to analyze how to optimizing the digital signature in improving the investment climate in Indonesia.

2. Methodology

In order to collect data for this study, the authors use a method normative juridical research method or library research is to examine a legal problem and make the settlement through the legislation in Indonesia. The author uses secondary data to support this research. Data is obtained from the library that includes books, reports, scientific papers, expert opinion, and the law applicable to the problems studied.

3. Digital Signature

Based on history, the use of digital signatures is originated from the use of cryptographic techniques used to secure information to be transmitted/communicated to others that have been used for hundreds of years ago (see also for current perspective, Sinha & Singh, 2003). In a cryptographic an encrypted message (encrypted) is using a key. The results of this encryption is a form of ciphertext is then transmitted/submitted to destination pleases. The ciphertext is then opened/decrypted with a key to getting the information that has been encrypted. There are two ways of doing encryption by using symmetric cryptography (symmetric cryptography/cryptography secret key) and symmetric cryptography (asymmetric cryptography), which later became known as public key cryptography (Acemoglu, & Linn, 2006).

Cryptography and secret key is known as symmetric cryptography uses the same key to encrypt and decrypt on a message , where the sender and receiver use the same key so they must keep the secret (Piper, 2002). Cryptography public key, otherwise known as symmetric cryptography, uses two keys: one key is used for encrypting a message, and the other key is used to decrypt against the message. Two keys have a mathematical relationship so that a message encrypted with one key can only be decrypted with a key partner. A user has two keys, a private key and a public key. User then distribute/disseminate his public key. Because there is a relationship between the two key, the user and someone who accepts public key will be confident that the data it receives and has successfully decrypted only be derived from users that have a private key. Certainty/confidence is only there for the private key is not known by others. The second key is derived or created by the user. One of the best-known algorithms for this is RSA (named for its creators Rivest, Shamir, Adleman) (see, Cohen & Parhi, 2011).

When two people want to communicate or exchange data/messages securely, they then each sent one keydipunyainya, namely the public key. While they keep the keys private as a pair of public key distributed, because the data/message can only be encrypted and decrypted by using a key partner, then this data can be transmitted securely over a relatively insecure network (via the internet). Digital signature in a data/messages will be encrypted using the symmetric key that is created at random (randomly generated symmetric key). This key is then encrypted using the public key of the prospective recipient of the message.

ISSN 1869-0459 (print)/ ISSN 1869-2885 (online)

The results of this encryption then known /are referred to as a "digital envelope" which will then be sent with a message/data that has been encrypted. After receiving the digital envelope, the recipient will then open/decrypt with key lock bu using privately key. The results he got from the decryption is a symmetric key that can be used to unlock the data/messages.The combination of a digital signature with the message digest cause a user can "digitally signed" a data/messages. The purpose of digitally signing is giving a characteristic to a message (Abidin et al., 2014).

Recipient of the digital signature will be able to trust that the data/messages from the sender's right. Moreover, because if there are changes in a data/message will cause the message digests will change in a way that can not be predicted (in an unpredictable way) then the recipient will feel confident that the data/messages never changed after the message digest created. Before both parties (sender/receiver) want to perform communication such as by using public key cryptography, each party must feel confident of their trust. They will then be authenticated on the existence of each party. Then they appoint a third party that will provide basic public authentication against them. These third parties are known as authority of certification. This authority certification will then provide a certificate (certificate) containing the identity of the user (e.g., Alice); this certificate is digitally signed by the certification authority. The contents of the certificate in addition to the identity it also contains a public key of the owner. A digital signature will cause the electronic data that is sent via the open network be guaranteed.

4. Implementation of Digital Signature in Investment Contract

In the implementation of paperless systems, traditional signature and stamp still cannot be separated from the practice of everyday documents (Civelek et al., 2017). Signature and stamp still be the determining authenticity of a document, so it is often the limiting factor to the implementation of a paperless system. In practice still required time-consuming manual processes long as distribute the document to the signing, the examination paper documents, and document signing process and then re-done digitizing documents.

Increasingly convergency development of information technology and telecommunications today has resulted in increasingly diverse also a variety of services (features) the existing telecommunications facilities, as well as the increasing sophistication of information technology products capable of integrating all the media information. Amid the growing globalization of unified communications (global communications network) with the growing popularity, internet has made the shrinking world and even eclipsed the following national borders and sovereignty society state. Ironically, the dynamics of the new Indonesian society still growing and developing as an industrial society and information society, as still seems premature to accompany the development of these technologies. The pattern of Indonesian society dynamics as they move irregularly amid a desire to reform all areas of life rather than a compelling idea to formulate a policy or the right settings for it. Although the community has been widely used of products to information technology and telecommunications services in his life, the Indonesian nation outline is still groping in the search for public policy in building a reliable infrastructure in the face of the global information infrastructure.

ISSN 1869-0459 (print)/ ISSN 1869-2885 (online)

The personal computer as a tool supported the development of information technology has helped the network access to the public network in the transfer of data and information. In e-commerce transactions, for example, the cryptographic device most commonly used is the digital signature. If the sender of the message affixing a digital signature in the message, the recipient can feel confident that once signed by the sender, the message that no one manipulates. By providing digital signatures on electronic data that is sent, it will be it can be shown some advantaged regarding the electronic data, among others, authenticity, integrity, and confidentiality.

Ensuring the integrity of the message could occur because of the existence of a Digital Certificate. Digital certificate is obtained on the basis certification application to the Authority by the user/subscriber. The digital certificate contains information about the user such as identity, authority, no legal status, and the status of the user. Digital certificate has different levels/levels, the level of this digital certificate to determine how much authority possessed by the user. So if a company wishes to perform an act of law, the Digital certificate that was used is a digital certificate owned by the directors of the company. In the presence of this digital certificate then the third party associated with the digital certificate holders can be confident that a message/messages honestly comes from the user.

Related to the issue of the integrity of the data submitted, A recipient of the message/data can be sure whether the message received is equal to the message that was sent. He can feel confident that the data is never modified or changed during the shipping process or storage. Messages in the form of electronic data that is sent the confidential/confidential, so not everyone can know the contents of electronic data that has been digitally signed and included in the envelope. The existence of the digital envelope includes an integral part of the digital signature causes an encrypted message can only be opened by a person who is entitled. The level of confidentiality of a message which has been encrypted, depending on the length of the key/key used for encryption (Busroh, 2018).

Data security in e-commerce with these methods are technically acceptable and applied (Roland, 2001), but when we discussed from the standpoint of the law are still not getting the attention. Lack of attention from the science of law is understandable since, particularly in Indonesia, the use of computers as a means of communication via the new internet network is known since 1994. Thus internet network security with the digital signature method in Indonesia, of course, is still a new thing for computer users, especially in terms of speed and ease of transactions in the global interaction without limitation of place and time. In this regard, the need for confidentiality of information and custody of the authenticity of the information is increasing so that the Government of the Republic of Indonesia issued Law No. 11 of 2008 on Information and Electronic Technology (referred to as Law 11/2008).

One point to note in electronic transactions is the implementation of digital signatures(digital signatures)that aims to legalize documents/results in an electronic transaction. Related to that Law 11/2008 regulates the rights and obligations authentication in an electronic document that is digitally signed(digital signature).

In making digital signature, electronic Information, to be signed must be known and understood by marker hand. (Article 56 paragraph (2) PP 82/2012). Approval Hands Markers

ISSN 1869-0459 (print)/ ISSN 1869-2885 (online)

on Electronic Information that will be signed with the Electronic Signatures must use the mechanism of affirmation and other mechanisms that show the purpose and objective markers Hands to be bound in an electronic transaction (Article 56 (2) PP 82/2012). Electronic Signatures for identity verification electronically Hands Markers are required to apply a combination of at least two (2) authentication factors (Article 58 paragraph (2) PP 82/2012). In terms of power of digital signature law, by referring to Article 5 Paragraph (1) of Law 11/2008, Electronic information and electronic documents and prints with valid legal evidence. It is an extension of the valid evidence.

5. Conclusion

It is hoped that the adoption of digital signatures can optimize the investment climate in Indonesia, especially related to regulations, making it easier for investors to develop their investments in Indonesia. In the end, the goal to absorb a lot of labor can be achieved. Characteristics of properties owned by digital are authentic signatures can not be difficult / written / copied by others, and only applies to sending documents messages and can be checked easily. In general, digital signatures use important known cryptographic techniques, symmetric keys, and one-way hash functions. It is worth noting that a digital signature is not the signature of someone scanned or entered into a computer using a stylus or mouse, but many mathematical calculations to encrypt data, e.g., with cryptography.

Another terminology for the digital signature is 'digitally ensured document ' so that its meaning is not ambiguous. So it can be likened to a document that is 'locked' and can not be manipulated contents. In developed countries, like the United States, some states already apply the rules on digital signatures. Some states make a very comprehensive regulation, but there is also very quick to make regulations. Even some countries that incorporate the regulation on the Internet and multimedia information, such as in Malaysia. Moreover, regarding the actual digital signature regulations already exist in Indonesia, namely Law No. 11/2008 on information and electronic transactions. However, because of the limited budget to support the infrastructure of the digital signature then it is not optimal in practice, especially in supporting the investment climate in Indonesia.

References

1. Abidin, I. S. Z., Bakar, N. A. A., & Haseeb, M. (2014). An empirical analysis of exports between Malaysia and TPP member countries: Evidence from a panel cointegration (FMOLS) model. *Modern Applied Science*, *8*(6), 238.
2. Acemoglu, D., & Linn, J. (2004). Market size in innovation: theory and evidence from the pharmaceutical industry. *The Quarterly journal of economics*, *119*(3), 1049-1090.
3. Busroh, F. F. (2018). Assessing the Role of IPR Legislations for Technology, Innovation and Economic Growth in Indonesia. *Int. J. Manag. Bus. Res*, *8*(3), 227-236.

ISSN 1869-0459 (print)/ ISSN 1869-2885 (online)

4. Butt, S. (2012). Foreign investment in Indonesia: The problem of legal uncertainty. In *Foreign investment and dispute resolution law and practice in Asia* (pp. 132-154). Routledge.
5. Chong, J. (1998). A primer on digital signatures and Malaysia's digital signatures act 1997. *Computer Law & Security Review*, *14*(5), 322-333.
6. Civelek, M. E., Çemberci, M., Uca, N., Çelebi, Ü., & Özalp, A. (2017). Challenges of Paperless Trade Redesign of the Foreign Trade Processes and Bundling Functions of Traditional Documents. *International Business Research*, *10*(2).
7. Cohen, A. E., & Parhi, K. K. (2011). Architecture optimizations for the RSA public key cryptosystem: A tutorial. *IEEE Circuits and Systems Magazine*, *11*(4), 24-34.
8. Harjono, D.K. (2007). *Hukum Investasi*. PT. RajaGrafindo Persada.
9. Piper, F. (2002). Cryptography. *Encyclopedia of Software Engineering*.
10. Roland, S. E. (2001). Uniform Electronic Signatures in Global and National Acommerce Act: Removing Barriers to E-Commerce of Just Replacing Them with Privacy and Security Issues. *Suffolk UL Rev.*, *35*, 625.
11. Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics communications*, *218*(4-6), 229-234.
12. Stern, J. E. (2001). The electronic signatures in global and national commerce act. *Berk. Tech. LJ*, *16*, 391.
13. Von Luebke, C., McCulloch, N., & Patunru, A. A. (2009). Heterodox reform symbioses: the political economy of investment climate reforms in Solo, Indonesia. *Asian Economic Journal*, *23*(3), 269-296.

ISSN 1869-0459 (print)/ ISSN 1869-2885 (online)