Advances in Social Science, Education and Humanities Research, volume 391
International Conference on Business, Economic, Social Science, and Humanities – Humanities and Social Sciences Track (ICOBEST-HSS 2019)

Legal Aspects of the Digital Signature in E-Commerce Connected to Law Number 19 Year 2016 about Amendments to Law Number 11 Year 2008 about Information and Electronic Transactions

Hetty Hasanah
Departemen Hukum
Universitas Komputer Indonesia
Bandung, Indonesia
hetty.hassanah@email.unikom.ac.id

Eman Suparman
Departemen Hukum
Universitas Komputer Indonesia
Bandung, Indonesia
eman@unpad.ac.id

***Abstract*— This research aims to find out the legal aspects related to digital signature authentication in e-commerce. The research method used was the normative juridical approach method, and the resulting data analyzed qualitatively juridical. The results obtained are that digital signatures have an important role in the validity of contracts in e-commerce. Based on the legal analysis conducted, the conclusion of this research is that digital signatures that are certified or not certified recognized by law and have legal force, provided the identity of the signatory and all processes of signing known. However, the use of digital signatures can also lead to legal problems. The impact of the research that has done can provide an understanding related to the use of digital signatures, especially in e-commerce, so that people can be more careful in using these digital signatures.**

Keywords— E-commerce, Digital Signature, Legal aspect

I. INTRODUCTION

Digital signatures are very important to examine in terms of legal aspects because digital signatures determine the validity of contracts in e-commerce. In e-commerce there is a digital signature, which is not like a signature that has been known so far, it is by using different methods to mark a document so that the document or data not only identifies the sender, but also to ensure the integrity of the document so as not to change during the transmission process.

There have been some previous researches about the validity of digital signatures in e-commerce agreements, by Rehulina [1], the study only discussed one aspect is the validity of digital signatures in the agreement, without elaborating on other legal aspects related to digital signatures in e-commerce. According to his opinion, the digital signature must accept as a signature with the following reasons. A digital signature is a signature that can be affixed by someone or some person who is authorized by someone else who wishes to be legally bound; using mechanical equipment, such as traditional or conventional signatures; A digital signature is very likely to be safer or more insecure as it is possible this also occurs in traditional or conventional signatures; as in traditional or conventional signatures. In another study, about digital signature there is research about digital signature in e-commerce, but the results of this study only explain that Information technology is a sector which grows rapidly from year to year. The current development of technology has greatly affected human's life globally. Computer and internet have experienced rapid growth so people can access, communicate, and access anything without limit. The internet is the unifier of people around the world. Due to the advancement and development of information technology, many changes happen. One of them is the increased transactions, which carried out through telecommunication media or the internet. In regards to this, digital signature system is developed. Digital signature under Article 1 paragraph (12) of the Electronic Information and Transaction Law is a signature consisting of electronic information attached, associated or related to other electronic information used as a means of verification and authentication [2]. Another study from Kalama M. Lui Kwan explained that digital signatures essentially allow parties to authenticate their document when communicating online. This is particularly useful for parties who want to know that their contract is enforceable, or for companies that want to be assured that customers with whom they are dealing inline truthfully representing themselves [3]. The other opinion such as form Charles R. Merrill stated that digital signature using cryptographic software and the signer of a digital signature will use the sender's private key to transform the message into a digital signature [4]. Paul R. Katz and Aron Schwartz stated that digital signature is a sequence of bits created when a person, intending to sign an electronic document, runs his or her message, through a one way function to create a unique identifier used for sender verification purpose [5]. The current conditions have been new laws governing the internet and cyberspace, namely the promulgation of Law Number 19 Year 2016 About Amendments to Law Number 11 Year 2008 About Information And Electronic Transaction (Then written UU ITE) concerning Information and Electronic Transactions, but have not explicitly regulated criminal acts of digital signature forgery.

This research aims to find out the legal aspects related to digital signature authentication in e-commerce. The research method used a normative juridical approach and the resulting data analyzed qualitatively juridical. The results obtained are that digital signatures have an important role in the validity of contracts in e-commerce. One of the legal requirements of the agreement is the agreement of the parties or the suitability of the parties' wishes, which proven by the signature, so that in electronic trading any agreement between the parties must be proven by the presence of a digital signature. The results of this study can provide an understanding of digital signatures used in e-commerce, so that the public can know the benefits and role of digital signatures, as a sign of contract authentication in e-commerce as well as the public can be more careful in using digital signatures in e-commerce.

II. METHOD

The specification of the research is descriptive analytical, i.e. giving the facts systematically. Approach method used is normative juridical approach method, in this case test and review secondary data about legal aspect of digital signature on e-commerce. All the data obtained are analyzed by qualitative juridical, in this case the analysis is done by considering the hierarchy of legislation so that the one legislation does not contradict other laws and legal certainty.

III. RESULTS AND DISCUSSION

Digital signatures are not manual signatures scanned and affixed to documents or emails that we send. Digital signature is one of the uses of cryptographic methods that aims to detect unauthorized modification of data and to check identity authentication from the sender and non-repudiation (refusing denial) [6]. The purpose of a digital signature in a document is to ensure the authenticity of the document. A digital signature is actually not a signature as it is known so far, digital signatures use different methods to mark a document so that digital signatures not only identify data from the sender, but digital signatures also ensure the integrity of the document, not changing during transmission process. A digital signature based on the contents of the message itself [7]. Giving digital signatures to the electronic data sent will be able to show where the electronic data actually came from. Guaranteed integrity of the message can occur because of the existence of the Digital Certificate. Digital Certificate obtained based on application to Certification Authority by user or subscriber. Digital certificate contains information about users including:

1. *Identity*
2. *Authority*
3. *Legal standing*
4. *Status of the user*

This digital certificate has various levels; the level of the digital certificate determines how much authority the user has. An example of this authority or qualification is if a company wants to do a legal act, then the party authorized to represent the company is the board of directors. Therefore, if a company wants to do a legal action, the Digital Certificate used is a digital certificate owned by the directors of the company.

The existence of this digital certificate, the third party associated with the digital certificate holder can feel confident that a message is true from that user. Integrity related to the integrity of the data sent. A message recipient / data can be sure whether the message received is the same as the message sent. He can feel confident that the data has modified or changed during the shipping or storage process.

The use of digital signatures that are applied to electronic messages or data sent can guarantee that these electronic messages or data do not experience a change or modification by an unauthorized party. It is guarantee of authenticity seen from the hash function in a digital signature system, where data recipients can compare the hash value. If the hash value is the same and is appropriate, then the data is truly authentic, no action has ever taken place to modify the data during the shipping process, so the authenticity guaranteed. Conversely, if the hash value is different, then it should be suspected immediately, it means that the recipient receives data that has been modified.

Non-repudiation or cannot be denied the existence of a message related to the person who sent the message. The message sender cannot deny that he sent a message when he sent a message. He also cannot deny the contents of a message different from what he sent when he sent the message. Non-repudiation is very important for e-commerce if a transaction done through an internet network, electronic contracts, or payment transactions [8]. This non-repudiation arises from the presence of digital signatures that use asymmetric encryption. This asymmetric encryption involves the existence of the private key and public key. A message that has been encrypted using a private key can only be opened or description using the sender's public key. Therefore, if there is a message that has encrypted by the sender using his private key, he cannot deny the existence of the message because it proven that the message can encrypted with the sender's public key. The integrity of the message seen is from the existence of the hash function of the message, noting that the signature data will enter into the digital envelope. The messages in the form of electronic data sent are confidential, so not everyone can find out the contents of electronic data that has signed and entered in the digital envelope. The existence of a digital envelope that includes an integral part of a digital signature causes an encrypted message to open only by the rightful person. The level of confidentiality of a message that has encrypted depends on the length of the key or key used to encrypt. At this time, the standard key length used was 128 bites. Safeguarding data in e-commerce with cryptographic methods through the digital signature scheme is technically acceptable and applied, but if discussed from the point of view of law, it still lacks attention. The lack of attention from legal science is understandable because especially in Indonesia, the use of computers as a means of communication through the internet has only known since 1994. Thus, safeguarding internet networks with digital signature methods in Indonesia is certainly still new to computer users.

Some properties that exist in digital signatures, namely [9]:

1. It is authentic; a message containing a digital signature can also be evidence, so that the party making the ratification (who signed) cannot deny that he never signed it.
2. It is exclusive, only valid for the document (message) or the exact copy. The signature cannot be transferred to another document. This also means that if the document is changed, the digital signature of the message is no longer valid.
3. It is global verification, checks can be done easily, even by people who are not related or have never met with the party who did the ratification (who signed) though

Digital signatures used as contract authentication in e-commerce [10].

UU ITE stipulates that electronic signatures have legal force and legal consequences as long as they comply with the provisions of this law. It means that as long as it can be ascertained the relationship between the electronic signature and the signatory concerned and the electronic signature is made and stored in conditions guarantee integrity with the deed attached to it, then an electronic signature has the same legal value as an ordinary signature.

The rise of cases of electronic crime (cybercrime) has become one of the backgrounds for the use of digital signatures. Now, the Ministry of Communication and Information is actively implementing digital signatures for online transactions. Hopefully, with this technology, the community can carry out various online activities.

In addition to reducing the case of cybercrime, digital signatures also aim to facilitate business activities. The signature can used to authorize documents. For example, you want to sign a business agreement with someone face to face. Digital signatures can substituted for wet signatures. The Ministry of Communication and Information is collaborating with the Financial Services Authority to launch the program. Signature validation questions is submitted to Root CA (Certification Authority). This institution tasked with determining the identity of the digital signature user and continuing the process [11].

Electronic signatures said to be valid if they meet certain requirements stipulated in the law. In the UU ITE, the legal requirements for digital signatures include the following. Manufacturing data is privacy and only known by the owner of the signature. When creating a signature, only the original owner has the power to use it. If there is a change after making an electronic signature, it will be known with certainty. Digital signatures including those used in e-commerce contracts used as electronic evidence, and therefore must obtained in accordance with existing laws and best practices to ensure receipt in court [12].

All related changes to electronic information are known. Have a special way to know for sure the owner of his signature. Have a special way to prove that the signature owner has given legal approval regarding certain electronic information. Signing a document has four main objectives, namely as evidence, a sign of agreement, fulfillment of formality, and efficiency. For this purpose to achieved, there are two attributes of electronic signatures that must met. Signature owner authentication is the electronic signature that not easy to imitate and is able to show the owner's identity also Document authentication. This gives meaning, under an electronic signature must be able to characterize the authenticity of the signed document. Thus, the document not easily faked or changed without known by the author.

In essence, the authentication of the signing and the document must be able to prevent someone from the case of cybercrime, such as forgery. Therefore, electronic signatures must adhere to the concept of nonrepudiation. This is one form of guaranteeing the authenticity of the file to prevent denial from the owner of the signature.

In verification of digital signatures, the hash function needs to consider. Hash is an algorithm used to make a fingerprint type. One hash can usually only be used in one document. The value is smaller than the original file.

There are two elements associated with the hash function, namely:

1. Making an electronic signature uses a hash value that comes from the file and the privacy key (must have defined). Electronic signatures applied to the same two documents, but have different private keys.
2. When verifying digital signatures, the process must be referenced to the original file and public key. Thus, the recipient can access the signature.

Regarding the validity of electronic signatures, the government has issued several official regulations. Guided by these rules, digital signatures have legal powers. Therefore, as if there were frauds or cases of disputes, we can follow up on legal channels.

The results obtained are that digital signatures have an important role in the validity of contracts in e-commerce. Digital signatures that are certified or not certified recognized by law and have legal force, if the identity of the signatory and all processes of signing are known, however the use of digital signatures can also lead to legal problems. The impact of the research that has done can provide an understanding related to the use of digital signatures, especially in e-commerce, so that people can be more careful in using these digital signatures

IV. CONCLUSION

Based on the above legal analysis, Electronic signatures certified as valid status are almost the same as authentic certificates, whereas if not certified in the process of proof requires digital forensic testing. Law recognizes both, but their position is much stronger which is certified. Electronic signatures have legal force and legal consequences with the following conditions. Data on the manufacture of Electronic Signatures related only to Signatories. Data on the manufacture of Electronic Signatures during the electronic signing process is only in the power of the Signatory; all changes to the Electronic Signature that occur after the signing time can be known. There are certain ways to indicate that the signatory has given approval of related electronic information.

ACKNOWLEDGMENT

This project is supported by The Rector of Universitas Komputer Indonesia.

REFERENCES

[1] Rehulina, Keabsahan Digital Signature Dalam Perjanjian E-Commerce, The Journal of Law, Volume 1, P.45, (2019).
[2] Meina Diniari Basani, Perkembangan Tandatangan Elektronik di Indonesia, Jurnal Hukum UNPAD, Volume 1, P. 45, (2017).
[3] Kalama M. Lui Kwan, Recent Developments in Digital Signature Legislation Electronic Commerce, Barkeley Technology Law Journal, Vol 14 No. 1, Annual Review of Law and Technology, P. 463-481. (1999).
[4] Charles R. Merrill, Science & Technology Digital : Signature Guidline For Electronic Commerce, Best ABA Sections Journal, Solo & Smal Firm Section, Vol. 1, No. 2, P. 50-51. (1997).
[5] Paul R. Katz & Aron Schwartz, Electronic Documents and Digital Signaturing : Changing The Way Business is Conducted and Contracts are Formed, Best of ABA Section Journal, Solo & Smal Firm Section, Vol. 1 No. 1, P. 36-37, (1997).
[6] Rahmat Sobari, Penggunaan Tanda Tangan Digital untuk Pengamanan Pertukaran Informasi, Tugas Akhir Proteksi dan Teknik Keamanan Sistem Informasi Bab IV: Cryptography, Program Magister Teknolgi Informasi Fakultas Teknik Komputer Universitas Indonesia, Hlm. 15, (2005).
[7] Edmon Makarim, Kerangka Hukum digital Signature Dalam Electronic Commerce, Makalah Dipresentrasikan di Hadapan Masyarakat Telekomunikasi Indonesia Pada Bulan Juni di Pusat Ilmu Komputer Universitas Indonesia, Depok Jawa Barat, (1999).
[8] Ilja Ponka, Legal Aspects of Digital Signatures and Non Repudiation, The Journal of Information Law and Technology, Vol. 2, P.5, (1999).
[9] Julius Indra Dwipayono Singara, Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia, Sumber Data dari Situs www.legalitas.org pada tanggal 1 Juni (2019).
[10] Ferhi Afifa, Credit Risk and Banking Stability: A Comparative Study between Islamic and Conventional Banks, International Journal of Law and Management, Volume 5, Issue 4, Longdom, Barcelona, Spain, P.1010, (2017).
[11] Anthony J. Diana & David G. Krone, Electronic Signatures : Legal & Practical Considerations for E-Signing On The Virtual Dotted Line, New York Law Journal, Vol. 1 No. 1, P. 2, (2019).
[12] Kancauskiene, Jolita, Computer forensics and electronic evidence in criminal legal proceeding, Digital Evidence & Electronic Signature Law Review Journal, Volume 16, SAS University of London, P.11, (2019).