RLJ Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung

Juridical Analysis of The Strength of Electronic Signatures as Legality Reviewed from The Electronic Transaction Information Law & The Civil Law Book

Ahmad Sholeh
Faculty of Law, Sultan Agung Islamic University (UNISSULA), E-mail: ahmadsholeh.std@unissula.ac.id

Abstract. *The aim of this studyTo find out the regulations regarding making electronic signatures that are valid according to law and to find out the legal force regarding electronic signatures, review the Electronic Transaction Information Law and the Civil Code. The method applied in this writing is carried out using normative juridical legal research, namely by analyzing problems through a legal principles approach and referring to legal norms contained in statutory regulations.The results of this research are regulations regarding the creation of legally valid electronic signatures based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions, electronic signatures can be considered valid in the eyes of the law and have a legal umbrella and making electronic signatures must fulfill several aspects in order to be considered valid in the eyes of the law, namely authentication of the owner of the electronic signature, meaning that the electronic signature is truly owned by the signatory listed on the document digital and document authentication, meaning that digital documents must also be proven authentically after being signed, the document remains true to the original so the document cannot be faked. The legal power regarding electronic signatures is reviewed by the Electronic Transaction Information Law and the Civil Code. The legal power and legality of your electronic signature which is certified based on Article 11 of Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE) is said to be valid in the eyes of the law to fulfill several requirements, especially that the electronic signature must be certified to provide a guarantee of trust for the owner, namely in the form of data authenticity. Data validity and legal certainty can only be provided by an Electronic Certification Organizing Body (PSeE) which has a license from the government, in this case the Ministry of Communication and Information Technology (Kominfo), whereas in the Civil Code after the issuance of Law Number 11 of 2008 concerning Electronic Information and Transactions , then the recognition of electronic documents signed with an electronic signature is an extension of the verification of civil procedural law in*

Indonesia, so that all electronic transactions with electronic signatures can be considered as deeds, even the strength of the proof is the same as an authentic deed made by an authorized official.

Keywords: *Civil Code; Technology; Signature.*

1. Introduction

Indonesia is a country that we know is based on the ideology of Pancasila, where Indonesia is a country that upholds the law. As stated in Article 1 paragraph (3) of the 1945 Constitution which reads "The Indonesian state is a state of law" which means that everyone within the territory of Indonesia must obey and submit to the laws in force in Indonesia.

The entire world is currently experiencing changes towards the era of the information society, especially Indonesia which is required to be able to adapt so as not to fall into the abyss of the digital divide, namely the imbalance in the growth of information and communication technology which results in isolation from global developments because it is unable to utilize information. One form of change that has occurred is the implementation of electronic signatures or digital signatures in documents, whether agreements or contracts.

Progress today is very rapid compared to several years ago. Currently, the development of science has developed quite well, especially with the presence of the internet network. This need to be practical will increasingly support the development of the virtual world. Everyone nowadays needs something fast. To search for something on the internet network, everyone can access and get information easily. Starting from small children to the elderly, they often use internet network services. Any information they need is very fast and easy to get. Using just one button, the information they want can be obtained on the internet network.

The virtual world ensures that we connect with many people. The information we obtain is also increasing, the way we obtain this information is now protected by existing laws and regulations in Indonesia, namely Law Number 11 of 2008 concerning Information and Electronic Transactions. There are so many ways we can obtain information in cyberspace, information about anything can be searched on the internet network in cyberspace, many people often misuse this electronic information, therefore we need legislation to protect it.[1] However, in general, the Indonesian nation is still groping in finding a public policy in building

[1]Nurdin Abdul Halim, Use of Internet Media for Information and Technology Development in Indonesia, RISALAH Journal, Vol. 26, no. 3, September 2015, p. 5.

a reliable infrastructure (National Information Infrastructure) in the face of global information infrastructure (Global Information Infrastructure).[2]

Apart from searching for information, we can also carry out transactions via the internet network. Electronic transactions are now often carried out because people really want it to be practical. In the midst of globalization of communication which is increasingly integrated with the increasing popularity of the internet, it seems that the world is shrinking and the borders of countries and their sovereignty and social order are increasingly blurred. Ironically, the dynamics of Indonesian society, which is still only growing and developing as an industrial society and information society, seems to still be visible premature to accompany these technological developments. The enactment of Law No. 11 of 2008 states that every person can provide information about all things, including providing information regarding the sale of goods or services using this information technology, from this information, if someone is interested in having a product or service being offered then an electronic transaction will occur.

The main problem in legal science is answering questions or providing solutions to problems raised by doubts regarding the application of positive law. Therefore, legal products are urgently needed which aim to increase the security of electronic transactions via electronic networks, as well as to provide recognition of the legal force of electronic evidence and electronic signatures. Based on Article 11 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, the evidentiary power of an electronic document signed with a digital signature is the same as the evidentiary power of an authentic deed made by an authorized public official. The above rule is contrary to Article 1 paragraph (7) of Law Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning the Position of Notary Public. What is meant by a Notarial Deed is an authentic deed made by or before a Notary in the form and procedures specified stipulated in this law.

The view of the definition of an authentic deed based on Article 1868 of the Civil Code is a deed which, in the form determined by law, is made by or in the presence of public officials who have authority for that purpose in the place where the deed is made. As a result of a conflict with these rules, if one of the parties files a lawsuit using electronic documents signed with an electronic signature as evidence.[3], then in resolving disputes in court, the judge is required to have the courage to make legal breakthroughs, because he is the most

[2]Maria Farida Indrati Soepapto, Legislative Science, Basics and Formation, Kanisius, Jakarta, 1998, p. 2
[3]Arrianto Mukti Wibowo, Digital Signature Legal Framework in Electronic Commerce, Digital Research, 2019, p. 3.

powerful in deciding a case and because he is also the one who can give a verdict van de rechter (judge's decision), which cannot be directly based on a legal regulation written or unwritten.

The main evidence inCivil evidence law is written evidence which for trading via electronic commerce becomes an actual problem because electronic commerce uses tools, namely electronic information and electronic signatures. Therefore, this research was carried out by inventorying, systematizing, analyzing and evaluating legal regulations concerning civil evidence issues in Indonesia with the legal implementation of electronic information and electronic signatures. We can see the use of digital signatures in Article 1 number 12 of Law Number 19 of 2016 concerning Electronic Information and Transactions which states that: "Electronic Signatures are signatures consisting of Electronic Information that is attached, associated or related to other Electronic Information that is used as a verification and authentication tool.

The validity of electronic signatures has been regulated by the government issuing several official regulations. Functionally, this electronic signature functions as a tool to verify and authenticate the identity of the signer while ensuring the integrity and authenticity of the document. An electronic signature shows the identity of the signer which is verified based on the electronic signature creation data where the electronic signature maker data is created uniquely and only refers to the signing. Understanding electronic information that covers a broad spectrum is essential in virtual activities, especially e-commerce activities. So electronic information as evidence in civil law is important because it involves the identity of the subject, the substance of the information, the methodology for fixing the storage media to make the information clearly known.

2. Research Methods

Approachcarried out with normative juridical legal research, namely by analyzing problems through a legal principles approach and referring to legal norms contained in statutory regulations[4]. The data analysis technique used in this research is a qualitative descriptive technique, namely a data analysis technique that aims to reveal and extract the truth from studies related to,"Juridical Analysis of the Strength of Electronic Signatures as Legality in View of the Electronic Transaction Information Law (UU ITE) and the Civil Code (KUHPerdata)".

[4]Soerjono Soekanto, Sri Mamudji, Normative Legal Research, Rajawali Press, Jakarta, 2010, p. 12.

3. Results and Discussion

3.1. Regulations Regarding the Creation of Legally Valid Electronic Signatures.

*Digital Signatures*or electronic signatures created using cryptographic techniques, a branch of applied mathematics that deals with changing information into another form that cannot be understood and returned to its original state. Electronic signatures use "public key cryptography", where the algorithm uses two keys, the first is the key to form a digital signature or change data to another form that cannot be understood, and the second key is used to verify digital signatures or return messages to reshape. This concept is known as "asymmetric cryptosystem" (non-symmetric cryptographic system). This cryptographic system uses a private key, which is known only to the signer and is used to form a digital signature, as well as a public key, which is used to verify the digital signature[5].If several people want to verify a digital signature issued by someone, then the public key must be distributed to these people.

The use of an electronic signature (digital signature) requires 2 (two) processes, namely from the signatory and from the recipient. In detail these two processes can be explained as follows[6]:

1. Formation of an electronic signature uses a hash value generated from the document as well as a previously defined private key. To ensure the security of the hash value, there should be a very small possibility that the same electronic signature can be generated from two different documents and private keys.

2. Digital signature verification is the process of checking an electronic signature by referring to the original document and the public key that has been provided, in this way it can be determined whether the electronic signature was created for the same document using a private key that corresponds to the public key.

To sign a document or other piece of information, the signer first delimits exactly which parts are being signed. This restricted information is called "message". Then the electronic signature application will form the hash value into a digital signature using the private key. The digital signature formed is unique for both the message and the private key[7]. Generally a digital signature is included with the document and is also saved with the document as well. However, digital signatures can also be sent or stored as separate documents, as long as they can still be associated with the document. Because digital signatures are unique to

[5]Kevin Yauris, Use of Hash Functions and Digital Signatures in Data Transmission, Journal of Cryptography, Vol. 2, 2016, p. 2

[6]Ibid., p. 3-4
[7]Ibid., p. 5.

the document, separating digital signatures like that is unnecessary. The process of creating and verifying a digital signature fulfills the most important elements expected for a legal purpose, namely[8]:

1. Signer authentication, if the public key and private key pair are associated with a defined legal owner, then the digital signature will be able to connect or associate the document with the signer. The digital signature cannot be forged, unless the signer loses control of his private key.

2. Document authentication, digital signatures also identify signed documents with a much higher level of certainty and accuracy than signatures on paper.

3. Assertion, creating a digital signature requires the use of the signer's private key. This action can confirm that the signer agrees and is responsible for the contents of the document.

4. The efficient, digital signature verification process provides a high level of certainty that the existing signature is the valid and genuine signature of the private key owner. With a digital signature, there is no need for verification by looking carefully (comparing) the signature on the document with an example of the original signature as is usually done in formal signature checks.

This authentication aims to avoid forgery and is an application of the concept of "nonrepudiation" in the field of information security which is a guarantee of the authenticity or delivery of the original document to avoid denial by the signer of the document. This means that electronic signatures have supporting technological capabilities that guarantee the fulfillment of the conditions that have been determined, based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions, electronic signatures can be considered valid in the eyes of the law and have a legal umbrella. If electronic information and documents are intended as authentic documents, then the documents must meet the requirements, the requirement is that electronic document information can be declared as valid evidence of the use of an electronic system that has received electronic certification from the government.[9]

3.2. Legal Strength Regarding Electronic Signatures Reviewed by the ITE Law and the Civil Code

[8]Thamaroni Usman, Validity of Electronic Signatures in Electronic Transactions, Indonesia Private Law Review, Vol. 1 issue 2, 2020, p. 92
[9]Sugeng, Indonesian Telematics Law, Prenadamedia Group, Jakarta, 2020, p. 138- 139

a. Legal Strength Regarding Electronic Signatures Reviewed by the ITE Law

Since the enactment of the Electronic Transaction Information Law in 2008 and then changed to Law Number 19 of 2016, this has been the foundation for the implementation of digital signature technology or electronic signatures in Indonesia. However, in 2012 a new government regulation was issued which was later changed to PP Number 71 of 2019 concerning the implementation of electronic systems and transactions which became the legal basis for online transactions and the implementation of digital signatures or electronic signatures in Indonesia. Based on existing Laws and Government Regulations, digital signatures or electronic signatures must have supporting technological capabilities that guarantee the fulfillment of the conditions that have been determined, where these facilities must have digital signature or electronic signature attributes and verification capabilities.[10].

Related to the digital signature or electronic signature attribute in question is the authentication capability that guarantees the authenticity of the digital signature or electronic signature and also digital documents. Regarding the authenticity of documents, in civil cases it is rare for documents containing original letters to be presented before the court. Usually only a copy is submitted, however, the strength of the proof lies in the original deed[11]. Document signing authentication is a tool to avoid forgery and is an application of the concept of "nonrepudiation" in the field of information security. Nonrepudiation is a guarantee of the authenticity or delivery of the original document to avoid denial from the signer of the document (that he did not sign the document) as well as denial from the sender of the document (that he did not send the document).[12].

Therefore, with the enactment of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions and PP Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions, digital signatures can be considered valid. in the eyes of the law and has a legal umbrella. PP Number 80 of 2019 concerning Trading via Electronic Systems Article 49 paragraph 3 which reads: "Proof of transactions using certified or signed electronic signatures can be considered authentic written evidence." Specifically for this certified electronic signature, it must be carried out by the Indonesian Electronic Certificate Provider (PSrE Indonesia) which has received recognition and has passed an audit that refers to standards issued by the Ministry of Communication and Information (Kominfo) in accordance with Article 1 number 5 of Minister of

[10]Ibid., p. 74
[11]Eddy OS Hiariej, Theory and Law of Evidence, Erlangga Publishers, Jakarta, 2012, p. 69-70
[12]Ibid., p. 1088

Communication and Information Regulation Number 11 of 2018 concerning the Implementation of Electronic Certification, it is stated that an electronic certificate organizer is a legal entity that functions as a party worthy of trust, which provides and audits electronic certificates.

This certified electronic signature based on Article 11 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) is said to be valid in the eyes of the law when it meets several requirements as follows[13]: Electronic signature maker data relates only to the signatory. The data for creating an electronic signature during the electronic signing process is only within the control of the signer. Any changes to the electronic signature that occur after the time of signing can be noted. Any changes to electronic information related to the electronic signature after the time of signing can be known. There are certain methods used to identify who the signatory is. There are certain ways to demonstrate that the signatory has given consent to the relevant electronic information.

b. Legal Strength Regarding Electronic Signatures Reviewed by the Civil Code Law

The law of evidence (which is stated in the fourth book of Burgerlijk Wetboek (BW) or the Civil Law book) which are the provisions regarding Dutch East Indies legal products that were enforced in Indonesia[14]. Contains all the basic rules of evidence in civil law. The evidence in Burgelik Wetboek is solely related to the case. There are several definitions put forward by legal experts that can be used as a reference. According to Pitlo, proof is a method carried out by a party regarding facts and rights related to interests[15]. According to Subekti, what is meant by proving is convincing the judge of the truth of the argument or arguments put forward in a dispute.[16].

Why is proof needed? This proof is carried out to reveal the existence of a fact, or postulate an event. We can see Article 163 HIR (283 RGB) which regulates the matter of proof: "Every person who postulates that he has a right, or in order to confirm his own rights or dispute the rights of others, points to an event and is required to prove the existence of that right or event. ” From this article we can conclude that in proof not only the event argument can be proven, but also the existence of a right. Within the judiciary in Indonesia, there

[13]Explanation of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2006 concerning Electronic Information and Transactions
[14]Nurhilmiyah, Civil Law, CV. Multi Global Makmur, Medan, 2020, p. 11

[15]A. Pitlo, Proof and Expiration According to the Dutch Civil Code, PT. Intermasa, Jakarta, 2014, p. 89
[16]R. Subekti, Law of Evidence, Bala Pustaka, Jakarta, 2018, p. 34

is known as procedural law which functions to regulate matters held in the judicial process. In this case, the existing positive law is the Herzein Inlands Regulation (HIR) or what is known as the updated Indonesian Regulation (RIB), namely the Law contained in Staatsblaad 1941 Number 44. In the minds of ordinary people, this is what is often echoed by legal experts in Indonesia regarding Dutch legal products which are still valid today[17]. As regulated in 164 HIR (283 RGB) and 1903 BW, only 5 (five) types of evidence are known that can be presented at trial, especially in civil proceedings, namely[18]: Written Evidence, Witnesses, Allegations, Confession, Oath.

In order for evidence to be used as evidence in court, several conditions are required as taught by the legal theory of evidence as follows[19]: Permitted by law to be used as evidence. Reliability, namely evidence can be trusted to its validity. Necessity, namely that evidence is needed to prove a fact. Relevance, namely that the evidence has relevance to the facts that can be proven. If the electronic document has the same evidentiary power as an authentic deed, then Law Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning Notary Positions should be revised, because in Article 1 paragraph (7) a notarial deed is an authentic deed made by or before a Notary in accordance with the form and procedures stipulated in this Law. The evidentiary power of the electronic document is only a private deed.

Often the State Body which has the authority to issue Laws, one Law and another Law conflict with each other, such as Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, which is in conflict with Law Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning the Position of Notary Public, then in cases where the legal rules conflict with each other, the judge relies on the principle of lex specialis derogate lex generalis, meaning the Law. Specific laws override general laws, in this case Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions overrides Law Number 2 of 2014 concerning Amendments to Laws. Law Number 30 of 2004 concerning Notary Positions.

4. Conclusion

Regulations regarding the creation of legally valid electronic signatures based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008

[17]Laila M. Rasyid, Introduction to Civil Procedure Law Module, Unimal Press, Lhokseumawe, 2015, p. 11
[18]Ibid., p. 76
[19]H. Sunarto, The Active Role of Judges in Civil Cases, Prenadamedia Group, Jakarta, 2014, p. 167-168

concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions, electronic signatures can be is considered valid in the eyes of the law and has a legal umbrella and making an electronic signature must fulfill several aspects in order to be considered valid in the eyes of the law, namely authentication of the owner of the electronic signature, meaning that the electronic signature is truly owned by the signatory listed on the digital document and document authentication , meaning that digital documents must also be authentically proven after being signed, the document remains in its original form so the document cannot be faked. The legal power regarding electronic signatures is reviewed by the Electronic Transaction Information Law and the Civil Code. The legal power and legality of your electronic signature which is certified based on Article 11 of Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE) is said to be valid in the eyes of the law to fullfil several requirements, especially that the electronic signature must be certified to provide a guarantee of trust for the owner, namely in the form of data authenticity. Data validity and legal certainty can only be provided by an Electronic Certification Organizing Agency (PSeE) that has a license from the government, in this case the Ministry of Communication and Information Technology (Kominfo). Meanwhile, in the Civil Code after the issuance of Law Number 11 of 2008 concerning Information and Electronic Transactions, the recognition of electronic documents signed with an electronic signature is an extension of the proof of civil procedural law in Indonesia, so that all electronic transactions with an electronic signature can be considered as deed, even its evidentiary strength is the same as an authentic deed made by an authorized official.

5. References

A. Pitlo, Proof and Expiration According to the Dutch Civil Code, PT. Intermasa, Jakarta, 2014.

Arrianto Mukti Wibowo, Digital Signature Legal Framework in Electronic Commerce, Digital Research, 2019.

Eddy OS Hiariej, Theory and Law of Evidence, Erlangga Publishers, Jakarta, 2012.

H. Sunarto, Active Role of Judges in Civil Cases, Prenadamedia Group, Jakarta, 2014.

Kevin Yauris, Use of Hash Functions and Digital Signatures in Data Transmission, Journal of Cryptography, Vol. 2, 2016.

Laila M. Rasyid, Introduction to Civil Procedure Law Module, Unimal Press, Lhokseumawe, 2015.

Maria Farida Indrati Soepapto, Legislative Science, Basics and Formation, Kanisius, Jakarta, 1998.

Nurdin Abdul Halim, Use of Internet Media for Information and Technology Development in Indonesia, RISALAH Journal, Vol. 26, no. 3, September 2015.

Nurhilmiyah, Civil Law, CV. Multi Global Makmur, Medan, 2020.

R. Subekti, Law of Evidence, Bala Pustaka, Jakarta, 2018.

Soerjono Soekanto, Sri Mamudji, Normative Legal Research, Rajawali Press, Jakarta, 2010.

Sugeng, Indonesian Telematics Law, Prenadamedia Group, Jakarta, 2020.

Thamaroni Usman, Validity of Electronic Signatures in Electronic Transactions, Indonesia Private Law Review, Vol. 1 issue 2, 2020.