



Recognition of Electronic Signatures in Proving Civil Procedure Law in Indonesia

Syaiful Bahri ¹, Moh. Zeinudin ², Miftahul Munir ³

^{1,2,3} Master of Law Study Program, Universitas Wiraraja, Indonesia

Jl. Raya Sumenep Pamekasan KM.5 North Panitian, Patean, Batuan sub-district,
Sumenep district (69451), East Java, Indonesia

Author's correspondence: bahri.sya80@gmail.com

Abstract. *This research is normative legal research that uses a normative judicial approach. The research results show that: (1) There are differences of opinion between judges, e-commers and notaries. regarding the strength of proof of a signature on an electronic document in proving civil procedural law in Indonesia. Judges and e-commers are of the opinion that electronic documents that have been signed with an electronic signature have the same evidentiary power as authentic deeds made by authorized officials, after the issuance of Law Number 11 of 2008 concerning Electronic Information and Transactions. Meanwhile, the notary is of the opinion that an electronic document signed with an electronic signature only has the power of proof under the hand, because it does not meet the requirements as an authentic deed, that is, it does not appear before an authorized official; and (2) Settlement of disputes resulting from non-fulfillment of the agreement can be resolved using a court or an institution outside the court, but e-comers generally use institutions outside the court because it is considered easier and faster to resolve and the costs are cheaper. The use of an electronic signature on an electronic document can guarantee the security of an electronic information message, which uses a public network, because electronic signatures are created based on asymmetric cryptography technology. From this research, there are differences of opinion regarding the evidentiary power of electronic documents signed with electronic signatures that are used as evidence in trials. The use of an electronic signature on an electronic document can guarantee the security of an electronic information message, which uses a public network, because electronic signatures are created based on asymmetric cryptography technology. From this research, there are differences of opinion regarding the evidentiary power of electronic documents signed with electronic signatures that are used as evidence in trials. Furthermore, electronic signatures need to be certified so that they have evidentiary power such as authentic deeds and there is no need to carry out digital forensic tests in the evidentiary process at trial.*

Keywords: *Electronic Documents, Signatures, Evidence, Proof.*

1. BACKGROUND

The rapid development of information technology and telecommunications has resulted in an increasing variety of existing telecommunication facilities, as well as the increasingly sophisticated information technology products that are able to integrate all information media. Computers as a human aid tool supported by the development of information technology, have helped access to public networks in transferring data and information, with computer capabilities and access that are increasingly developing, then trade transactions are carried out in the communication network. Public networks have advantages compared to private networks with cost and time efficiency, this makes trade with electronic transactions (electronic Commerce) an option for business people to facilitate their trade transactions, because of the nature of public networks that are easy to access by everyone or companies that are carried out with electronic systems.

Electronic systems are used to explain the existence of information systems which are the application of information technology based on telecommunication networks and electronic media, which functions to design, process, analyze, display, and transmit or disseminate electronic information. Information systems, technically and management, are actually the embodiment of the application of information technology products into a form of organization and management in accordance with the characteristics of the needs of the organization and in accordance with the purpose for which it is intended. On the other hand, information systems are technically and functionally the integration of systems between humans and machines, which includes hardware components, software, procedures, human resources, and information substances whose utilization includes input, process, output, storage, and communication functions.

Everyone can provide information about everything, including providing information on the sale of goods or services using this information technology, from this information, if someone is interested in owning a product of goods or services offered, then an electronic transaction will occur.

Electronic transactions are non-face, non-signature (without using an original signature) and without territorial boundaries (a person can make electronic transactions with other parties even though they are in different countries) using information technology. Electronic transaction activities that are no longer limited by the territory of a country facilitate access to transactions anytime and from anywhere. The advantages offered by advances in electronic transactions are inseparable from the negative aspect, where losses can occur, both to the transaction perpetrator and to other people who have never made a transaction. In addition, the proof in the dispute arising from the transaction is a very important factor, considering that electronic transactions are not only accommodated in the Indonesian procedural law system comprehensively, but also turn out to be very easy to forge and abuse.

In its development, the security aspect of information has begun to be considered. When this information becomes damaged or there will be risks that must be borne by people who send, need, or just see it, due to the use of this electronic information, using a public network, where everyone can know the electronic information, or if one party does not carry out the achievements of the electronic transaction that has been agreed with the other party, this is detrimental to interested parties who use information technology for the sale of a good or service.

New technologies and media are increasingly used in trade practices, both at the national and international levels, so that international organizations are increasingly thinking about legal recognition of electronic documents and electronic signatures. Finally, the impetus came from the United Nations Commission on International Trade Law, the Model Law on Electronic Commerce (hereinafter referred to as UNCITRAL), issuing the UNCITRAL Model Law on Electronic Commerce on December 16, 1996.

This Model Law is actually proposed to offer a legal model to countries that already or do not have laws and regulations on this material. However, model law is free, meaning that countries are left free to follow it or not. Thanks to this model law, many countries in the world have improved themselves, they see that traditional law of proof is no longer able to adapt to the model of electronic commerce, electronic government and rapid exchange of information. Therefore, there is a great need for legal products that aim to increase the security of electronic transactions through electronic networks, as well as to provide recognition of the legal power of electronic evidence and electronic signatures.

In fact, cyber activities are no longer simple, because their activities are no longer limited by the territory of a country, which is easily accessible anytime and from anywhere. Losses can occur, both to the transaction perpetrator and to other people who have never made a transaction. In addition, proof is a very important factor, considering that electronic information has not only not been accommodated in the Indonesian procedural legal system comprehensively, but it also turns out to be very easy to forge, and sent to various parts of the world within seconds. Thus, the resulting impact can be so complex and complicated.

Since 1999 this Bill has been discussed by the Legislative Body, finally Indonesia has a legal rule to regulate the issue with the issuance of Law Number 11 of 2008, concerning "Information and Electronic Transactions" which was passed on April 21, 2008.

Based on Article 18 juncto Article 7 juncto Article 11 of Law Number 11 of 2008, the evidentiary power of the 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 30 of 2004 which means a notary deed is an authentic deed made by or before a Notary in accordance with the form and procedures stipulated in this Law. Meanwhile, the definition of an authentic deed based on Article 1868 of the Civil Code is a deed that is in the form

prescribed by the Law, made by or in the presence of public officials who have authority for it in the place where the deed is made.

An electronic document signed with a digital signature, can be categorized as written evidence. However, there is a legal principle that makes it difficult to develop the use and use of electronic documents or digital signatures, namely the requirement that the document must be viewable, sent and stored in paper form.

2. RESEARCH METHODS

2.1 Type of Research

This thesis research seeks to combine normative legal research and empirical legal research by conducting an inventory of a number of articles in laws and regulations and exploring several documents that are empirically signed electronically. Normative legal research is carried out to identify legal concepts and principles used in legal construction that govern electronic signatures on an electronic document. Meanwhile, empirical legal research was also carried out to get an overview of how the concepts and ideas related to electronic signatures have been carried out in the world *of e-commers* so far. Because according to Johnny Ibrahim, a meaningful explanation of legal phenomena is needed that is interpreted factually speaking. As for legal facts that can be explained with the help of law, similarly legal rules can be explained with the help of legal facts

2.2 Problem Approach

This thesis research uses a statute approach, a case approach and a socio-legal approach. The approach to laws and regulations is used to identify a number of articles in laws and regulations that are used in understanding the concept of signatures in the world of e-commerce. The case approach is used, because several relevant cases related to electronic signatures on electronic documents are used as evidence of transactions in the world of e-commerce. And the socio-legal approach is used to conduct a direct exploration of how electronic signatures on electronic documents are practiced as evidence in various transactions in the world of e-commerce.

2.3 Source of Legal Materials

In accordance with the focus of the study, this thesis research uses data and legal materials. The data used is in the form of interviews from competent experts in their fields such as notaries, judges, and other practitioners, while the legal materials used

include primary legal materials, secondary legal materials, and tertiary legal materials. The ricias are as follows:

1. Primary legal materials, namely binding legal materials, namely:
 - a. Basic norms or rules , namely the Preamble to the 1945 Constitution;
 - b. Laws and regulations, namely Law No. 11 of 2008 concerning Information and Electronic Transactions , Law No. 30 of 2004 concerning Notary Positions;
 - c. Legal materials from the colonial era that are still in force today, for example the Civil Code.
2. Secondary legal materials , which provide an explanation of the primary legal materials, as follows :
 - a. Research results and scientific works related to electronic documents (*e-contract/online-contract*) and electronic commercial transactions (*e-commerce*);
 - b. Books related to electronic commercial transactions (*e-commerce*);
 - c. Draft Government Regulation on Electronic Signatures, and Draft Government Regulation on Electronic Certification.
3. Tertiary legal materials or supporting legal materials, including:
 - a. Materials that provide instructions and explanations for primary and secondary legal materials. For example: Legal dictionary and English dictionary.
 - b. Primary, secondary and tertiary (supportive) materials outside the field of law, for example those from the fields of sociology and philosophy and so on, which can be used to complement or support field data.

2.4 Legal Materials Collection Techniques

1. Literature Studies

Literature study , carried out by conducting research on documents related to signatures on an electronic document (*e-contract/online-contract*), in electronic commercial transactions (*e-commerce*) including browsing through internet sites.

2. Interview

Field data collection will be carried out by means of interviews, both structured and unstructured. Structured interviews, conducted guided by a list of questions that have been provided by the researcher, while unstructured interviews, namely

interviews conducted without being guided by a list of questions related to signatures in electronic commercial transactions (*E-commerce*).

2.5 Legal Material Processing Techniques

The legal materials that have been successfully collected are processed in the following stages:

1. Inventory of regulations that reflect the government's policy in the field of laws and regulations related to electronic documents and electronic commerce;
2. Analyze the laws and regulations that have been inventoried to find out the extent to which the above laws and regulations are synchronous both vertically and horizontally.

In addition, the author also uses the opinions and views of the parties who carry out the transaction electronically, and the opinions of the Notary, regarding the signing that is not directly attended by the interested parties in the preparation of electronic documents, as well as the opinions of the judges regarding the recognition of signatures on electronic documents in the law of proof in Indonesia, with the main consideration that the normative juridical approach is still not enough to can find out the reality that occurs in society, especially regarding the recognition of signatures in the law of proof in Indonesia.

2..6 Analysis of Legal Materials

As a way to draw conclusions from the collected research results, a qualitative normative analysis analysis method will be used . Normative, because this research is based on existing regulations as positive legal norms. While qualitative means data analysis that starts from efforts to discover principles and information that is monographic expressions from respondents.

3. RESULTS AND DISCUSSION

Electronic commercial transactions (e-Commerce), are a form of modern business that is non-face and non-sign (without face-to-face and without signature). Electronic commercial transactions (e-commerce) have several special characteristics, including that these transactions are paperless (without written documents), borderless (without geographical boundaries) and the parties who make transactions do not need to be face-to-face. Electronic commercial transactions (e-commerce), refer to all forms of commercial transactions that are based on electronic processes and data transmission

through electronic media. Therefore, there is no definition of the concept of electronic commercial transactions that applies internationally.

A similar thing was also stated by UNCITRAL which defines e-commerce as follows, "Electronic commerce. Which involves the use of alternatives to paper-based of communication and storage of information".

Black's Law Dictionary, as quoted by Ridwan Khairandy, defines e-commerce as follows:

"The practice of buying and selling goods and services through online consumer services on the internet. The a shortened form of electronic, has become a popular prefixes for other terms associated with electronic transaction".

Vladimir Zwass, defines electronic commercial transactions (e-commerce) as the exchange of business information, maintaining business relationships and conducting business transactions through communication networks.

Observing this, electronic commercial transactions (e-commerce) are trade transactions for the purchase and sale of goods and services that are carried out by exchanging information/data using alternatives other than written media, which is meant by transaction media here is electronic media, especially the internet.

Electronic Transactions based on Article 1 paragraph (9) of Law Number 11 of 2008 concerning Electronic Transaction Information states that electronic transactions are legal relationships carried out through computers, or other electronic media.

Based on these various definitions, there are several similarities, namely:

- 1) There is a transaction between two or more parties;
- 2) There is an exchange of goods and services;
- 3) Using the internet as the main medium to make transactions.

Electronic commercial transactions (e-commerce), in principle, are legal relationships in the form of exchanges of goods and services between sellers and buyers which have the same basic principles as conventional transactions, but are carried out by exchanging data through intangible media (the internet), where the parties do not need to meet face to face physically.

Broadly speaking, the types of electronic commercial transactions (e-commerce) are divided into 5, namely:

- a. Business to Business (B2B) is a transaction, where both parties to the transaction are a company.

- b. Business to Consumer (B2C) is a transaction between a company and a consumer/individual. B2C transactions include the purchase of products directly by consumers via the internet.
- c. Customer to Customer (C2C) is a transaction, where individuals sell goods to each other.
- d. Customer to Business (C2B) is a transaction that allows individuals to sell goods to a company.
- e. Customer to Government (C2G) is a transaction, where individuals can make transactions with the government.

According to Tan Thong Kie, a signature is a statement of the will of the signatory, that he by affixing his signature under a writing wants the writing to be considered in the law as his own writing.

The meaning of a signature in a general sense, is a signature that can be defined as an arrangement (letter) of a sign in the form of writing from the signatory, with which the person who makes the statement/information can be individualized. The definition includes an assumption that a statement made in writing must be affixed with the signature of the person concerned. A digital signature is a security for digital data created with a private signature key, whose use depends on the public key that is the partner.

According to Julius Indra Dwiparyo, an electronic signature is an electronic identity that functions as a sign of approval of the obligations attached to an electronic deed. The definition of electronic signature, based on Article 1 paragraph (12) of Law Number 11 of 2008 concerning Information and Electronic Transactions is as follows:

"A signature consisting of electronic information that is attached, associated with or related to other electronic information used as a verification and authentication tool"

Meanwhile, the existence of electronic signatures in an electronic document must be recognized as having the same legal force and legal consequences as signatures on other written documents. This departs from the understanding that electronic documents have the same legal force as evidence and legal consequences as other written documents. An electronic signature that uses asymmetric cryptography technology, using two keys, namely the private key and the public key, then there is evidence that the electronic document is the sender's own will.

The purpose of a signature in an electronic document is as follows:

- a. To ensure the authenticity of the document;

- b. To accept/agree convincingly the content of a writing.

Electronic documents signed with electronic signatures in the law of proof in Indonesia, are recognized in essence after being regulated in the ITE Law that electronic information/electronic documents and/or printed results are valid legal evidence, and are an extension of valid evidence in accordance with the procedural law applicable in Indonesia, this is based on the provisions of Article 5 paragraph 2 of the ITE Law. Based on Article 164 of the Criminal Procedure Code and Article 284 of the Criminal Procedure Code, valid evidence consists of written evidence, evidence with witnesses, suspicions, confessions and oaths, while according to Article 184 of the Criminal Procedure Code, valid evidence consists of witness statements, expert statements, letters, instructions and statements of the defendant. Therefore, evidence according to the above procedural law made in the form of electronic information/electronic documents, and electronic information/electronic documents themselves, are valid evidence according to the Electronic Information and Transaction Law.

Electronic transactions that use electronic signatures are certainly very convenient, especially if both parties are in different countries, for example, American citizens make agreements with Indonesian citizens. However, if one party commits a default, the parties will find it difficult to resolve the case because they have two different legal systems, namely the legal system in America and the legal system in Indonesia. So to avoid this, before making an agreement, the parties made a Memorandum of Understanding (MoU). An MoU is a memorandum or letter where each party signs an MoU as an initial guideline for a sign of an understanding between them. The MoU only contains the main things and is a preliminary agreement, which will regulate and describe the details of the content that will be included in the contract or agreement. The MoU can also contain a form of settlement such as which legal system the parties will use. So that if a case occurs, it can be easily resolved in accordance with the legal system contained in the MoU.

Along with the development of advances in the field of information technology and telecommunications, there are also things or ways that can be used as evidence in civil relations that occur in modern society with the emergence of various kinds of modern transactions. Proof is the most important stage in resolving cases in court, because it aims to prove that an event or certain legal relationship has occurred that is used as the basis for filing a lawsuit to the court. Through the proof stage, the judge will obtain the basics to make a decision in resolving a case.

Electronic evidence is increasingly appearing in practice in the community, for example, e-mail, witness examination using video teleconference, short message service system (SMS), closed circuit television (CCTV), electronic information, electronic tickets, electronic data/documents and other electronic means as data storage media. An instrument that can be used to determine the authenticity or validity of an electronic evidence in the form of an electronic document or information is an electronic signature. Electronic signatures aim to ensure the authenticity of a document in an electronic transaction and ensure that the integrity of the contents of the document does not change during the delivery process.

The guarantee of authenticity can be seen from the existence of a hash function in the electronic signature system, so that data recipients can compare hash values. If the hash value is the same and appropriate, then the data is completely authentic and there has never been an action that changes the data during the transmission process, so that its authenticity is guaranteed. On the other hand, if it is not the same or there is a change in the hash value, then it is suspicious and it can be immediately concluded that the recipient received the modified data.

Electronic signatures have the same legal force as conventional signatures that use wet ink and seals. In the ITE Law Article 11, it is stated that electronic signatures have legal force and legal consequences as long as they meet the following requirements:

- a. The relevant Electronic Signature creation data is only to the Signatory.
- b. The data on the creation of an Electronic Signature during the electronic signing process is only within the authority of the Signatory.
- c. Any changes to the Electronic Signature that occur after the signing time can be known.
- d. Any changes to the Electronic Information related to the Electronic Signature after the time of signing can be known.
- e. There is a certain way to identify who the signatories are.
- f. There are certain ways to indicate that the Signatory has given consent to the relevant Electronic Information.

If the electronic signature is in accordance with the requirements and procedures mentioned in Article 11 of the ITE Law, the signature already has legal force and legal consequences.

The trading system by utilizing internet facilities (interconnection networking), hereinafter referred to as e-commerce has changed the face of the Indonesian business

world. In addition to being caused by the development of information technology, e-commerce was born on the guidance of the community towards fast-paced, easy and practical services. Through the internet, people have a wider space to move in choosing products (goods and services) to be used, of course, with various qualities and quantities as desired.

E-commerce is one of the forms of trade transactions that is most influenced by the development of information technology. Through these trade transactions, the concept of the traditional market (where sellers and buyers physically meet) changes to the concept of telemarketing (remote trade using the internet). E-commerce has also changed the way buyers get the products they want.

Through e-commerce, all formalities that are commonly used in conventional transactions are reduced, besides of course, buyers also have the ability to collect and compare information such as goods and services more freely without being restricted by territory (borderless).

An e-commerce agreement made by interested parties in the form of an electronic document, if one of the parties violates the agreement/default from one of the parties, then the aggrieved party can sue the Court with electronic document evidence.

The settlement of a dispute or an absolute case only based on the judge's conviction is a very risky thing because it can raise concerns that the judge's conviction will be subjective, so that it will give rise to arbitrary actions from the judge which does not provide a sense of justice for the parties to the case, so it is natural if the postulates put forward by the parties to the dispute are also the basis for consideration for the judge to be able to an objective decision is reached.

Proof is an aspect that plays a central role in a judicial process. In criminal cases, the fate of the defendant will be determined at this stage, if there is not enough evidence, the defendant will be declared innocent and must be acquitted, and vice versa. Meanwhile, in civil cases, in this stage of proof, the parties are given the opportunity to show the truth about the legal facts that are the main point of the dispute. Thus, the judge who examines and decides the case will be based on the evidence submitted by the parties to the dispute.

Proving is an effort to collect facts that can be analyzed from a legal point of view and related to a case that is used to give the judge confidence in making a decision, while proof is the process of proving a case accompanied by facts that can be analyzed from a legal point of view to give the judge confidence in making a decision.

3.1 The Power of Proof of Electronic Documents with Electronic Signatures in the Civil Trial Process

Electronic documents signed with electronic signatures in the law of proof in Indonesia, are recognized in essence after being regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions that electronic information/electronic documents and/or printed results are valid legal evidence, and are an extension of valid evidence in accordance with the procedural law applicable in Indonesia, this is based on the provisions of Article 5 paragraph 2 Law Number 11 of 2008. Based on Article 164 of the Criminal Procedure Code and Article 284 of the Criminal Procedure Code, valid evidence consists of written evidence, evidence with witnesses, suspicions, confessions and oaths, while according to Article 184 of the Criminal Procedure Code, valid evidence consists of witness statements, expert statements, letters, instructions and statements of the defendant. Therefore, evidence according to the above procedural law made in the form of electronic information/electronic documents, and electronic information/electronic documents themselves, is valid evidence according to the Electronic Information and Transaction Law.

Electronic documents are declared valid if they use a security system that can be accounted for in accordance with the development of information technology, and meet the minimum requirements as follows:

- a. Can display information and/or electronic documents in their entirety in accordance with the retention period stipulated by laws and regulations;
- b. Can protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the implementation of the electronic system;
- c. Be able to operate in accordance with procedures or instructions in the implementation of the electronic system;
- d. Equipped with procedures or instructions announced in language, information, or symbols that can be understood by the party concerned with the implementation of the electronic system; and
- e. Have an ongoing mechanism to maintain the freshness, clarity, and accountability of procedures or instructions.

Electronic documents are documents that occur as a result of an electronic commercial transaction (e-commerce). To determine when an agreement occurs in an electronic commercial transaction (e-commerce).

According to Hikmahanto Juwana, the documents in electronic commercial transactions (e-commerce) are valid legally and binding when the buyer clicks the sent button and in this case the buyer is considered to have agreed and agreed to the terms and conditions listed in the offer.

Regarding when this agreement will occur, the actors of electronic commercial transactions give different opinions. Mia Lestari, said that so far she has carried out electronic commercial transactions by utilizing websites and emails. Furthermore, he said that the agreement occurs when the prospective buyer agrees to the price proposed by the seller in the event that there are several prospective buyers, then the prospective buyer with whom the agreement will be made, is selected based on the time listed in the email containing the approval of the prospective buyer requested by the seller and the selected prospective buyer will receive confirmation via email while the other prospective buyers will receive an email with a notification that The item you want to buy has been sold.

Ahmad Hidayat argued that determining when the agreement occurred for the buyer was more difficult because the final decision was in the hands of the seller, the buyer could only wait for confirmation from the seller to the buyer which contained confirmation that the order of goods and payment had been received by the seller showing that there had been an agreement between the seller and the buyer.

A similar opinion was expressed by Thamrin who said that the email from the seller to the buyer containing confirmation that the order for the goods and the payment had been received by the seller showed that there had been an agreement between the seller and the buyer.

As a commercial transaction actor, Ahmad Hidayat said that the non-face and non-signature nature of an electronic contract should not prevent the use of electronic documents as evidence in the event of a dispute. During electronic commercial transactions, he has never experienced problems with the seller. Furthermore, he suggested that to minimize the possibility of disputes, an actor in electronic commercial transactions should only make transactions with trusted and reputable parties and store or print out all documents related to the transaction.

Abu Bakar Munir stated that a data message can be considered as written information if the information can be accessed and can be used as a reference for the future. Furthermore, he said that if the law requires a signature, then this can be fulfilled by using a reliable identification method, for example, by using an electronic signature.

According to Nursiah Sianipar, electronic documents if submitted as evidence at trial, in the law of proof in Indonesia will be considered as valid evidence, in the law of proof in Indonesia. Where the electronic document is used as evidence after the document is printed/photocopied and put together in the case file.

The print out of an electronic document produced in the exchange of information should have the same evidentiary value as other written evidence. In deciding a case, of course, the judge must base on the provisions of procedural law that govern the issue of proof. Moreover, almost all countries, including Indonesia, recognize letter evidence as one of the evidence for those that can be submitted to court.

The evidentiary power of the electronic document signed with an electronic signature, can be categorized as written evidence, but there are exceptions, electronic documents as valid legal evidence do not apply to:

- a. A letter that according to the Law must be made in written form; and
- b. Letter and its documents which according to the Law must be made in the form of a notary deed or a deed made by the deed-making official

According to Jusuf Patrianto Tjahjono, the evidentiary power of the electronic document is the same as the authentic deed made by the authorized public official, such as a Notary, this is based on Article 18 juncto Article 7 juncto Article 11 of Law Number 11 of 2008 has affirmed that the electronic transaction outlined in the electronic document binds the parties which gives rise to rights and obligations for each party, provided that it is signed electronically by the parties in accordance with the provisions of the applicable laws and regulations.

According to Toni Iskandar, although electronic documents can be used as evidence in trials, which is an expansion of the law of proof in Indonesia after the existence of Law Number 11 of 2008, it only has the power of proof as a deed under hand.

According to Leanni Bharline, the electronic document, even though it has been signed with a digital signature, does not meet the requirements of an authentic deed determined by Article 1868 of the Civil Code: "A deed in the form prescribed by law, made by or in the presence of public officials who are authorized to do so at the place where the deed is made".

Article 165 of the HIR and Article 285 of the Civil Code regulate the definition of an authentic deed, i.e. a letter made by or before a public official in power shall make it, manifest sufficient evidence for both parties and their heirs and all persons entitled to it, i.e. about all things, which are mentioned in the letter and also about those contained

in the letter as a notice only, But the one who was then only informed was directly related to the subject of the act.

According to Desi Arisanti, in the Notary Position Law, facing a notary, is an absolute requirement for certain legal acts, even though the person represents the interests of others, so that the provisions of Law Number 11 of 2008 are contrary to Law Number 30 of 2004.

According to Toni Iskandar, authentic deeds made by notaries come in 2 forms:

- a. A deed of relaas is a deed made by a notary based on everything seen, heard, witnessed by the events that occurred at that time.
- b. A partij deed is an authentic deed made in front of a notary based on the request of the parties.

Although there is one form of authentic deed, there is an exception, namely not appearing before a notary, but the notary hears and witnesses an event, so facing a notary is one of the main requirements for an authentic deed.

According to Thamrin, if the electronic document has the same evidentiary power as the authentic deed, then the Notary Position Law Number 30 of 2004 must be revised, because in Article 1 paragraph (7) the notary deed is an authentic deed made by or before a Notary according to the form and procedures stipulated in this Law.

The evidentiary power of the electronic document is only the deed under the hand, where the form of the deed under the hand is made in a form that is without intermediaries or not intermediaries or not in the presence of authorized public officials, has the power of proof as long as the parties admit it or there is no denial from one of the parties. If one of the parties does not admit it, the burden of proof is left to the party who denies the deed, and the judgment of the repudiation of the evidence is left to the judge.

There is one thing that should be considered in the recognition of an electronic document signed with an electronic signature, namely the security of a system and the involvement of the person with the computer system.

According to Arianto Mukti Wibowo, the evidentiary power of an electronic document can be equated with an authentic deed, on the grounds that for an electronic information and/or electronic document that has been signed electronically means for electronic information and/or an electronic document that has been signed electronically means that the electronic information and/or electronic document has been verified and authenticated.

Meanwhile, the existence of electronic signatures in an electronic document must be recognized as having the same legal force and legal consequences as signatures on other written documents. This departs from the understanding that electronic documents have the same legal force as evidence and legal consequences as other written documents.

An electronic signature that uses asymmetric cryptography technology, using two keys, namely a private key and a public key, then there is evidence that the electronic document is the sender's own will.

According to Arianto Mukti Wibowo, in order for an electronic signature on an electronic document to have the power of proof in court, it must register the electronic signature with the Certification Authority (CA), then the CA can act as a public official, so that by utilizing the infrastructure provided by the CA, especially the ability to know when the electronic transaction is signed, the signed electronic transaction is equalized with an authentic deed made in the presence of an authorized official.

Digital signatures that have obtained a certificate from the Certification Authority institution, then the authentication of a document will be more guaranteed, and digital signatures are very difficult to forge and uniquely associated with a combination of documents and private keys, if they have implemented the provisions stipulated by the relevant laws and regulations, then there are actually no rules of the Law that are contrary.

According to Nursiah Sianipar, often the State Agency that has the authority to issue laws, between one law and another law contradicts each other, such as Law Number 11 of 2008, which is contrary to Law Number 30 of 2004, so for cases where the legal rules are contrary to each other, the judge is based on the principle of *lex specialis derogate lex generalis*, This means that special laws are set aside laws of a general nature, in this case Law Number 11 of 2008 is set aside Law Number 30 of 2004. Therefore, the evidentiary power of an electronic document signed with an electronic signature is the same as an authentic deed.

Based on the opinions mentioned above, the recognition of documents that have been signed using digital signatures, after the issuance of Law Number 11 of 2008 concerning Information and Electronic Transactions, the recognition of electronic documents signed with digital signatures, is an extension of the proof of civil procedure law in Indonesia, so that all electronic transactions with electronic signatures can be considered as deeds, In fact, the power of proof is the same as an authentic deed made by an authorized official. Except as specified in Article 5 paragraph (4) of Law Number

11 of 2008, namely the provisions regarding electronic information and/or electronic documents as referred to in paragraph (1) do not apply to:

- a. A letter that according to the Law must be made in written form; and
- b. Letter and its documents which according to the Law must be made in the form of a notary deed or a deed made by the deed-making official.

Explanation of Article 5 paragraph (4) of Law Number 11 of 2008, that the letter that according to the Law must be made in written form includes but is not limited to securities, valuable letters, and letters used in the process of law enforcement of civil, criminal and state administrative procedures.

The use of electronic signatures in the process of forming agreements or contracts (e-commerce) will facilitate the evidentiary mechanism in civil cases. This is because by giving an electronic signature to the electronic data sent, it will be possible to show where the electronic data actually came from. The integrity of the message can be guaranteed because of the existence of an electronic certificate (digital certificate).

An electronic certificate contains information about the user, including; identity, authority, legal standing, and status of the user. Electronic certificates have various levels that determine how much authority the user has. For example, if a company is going to do a legal act, the electronic certificate used is owned by the company's board of directors. With the existence of an electronic certificate, a third party who is in contact with the electronic certificate holder can feel confident that a message is true from the user.

The obligation to use electronic certificates in public services has been mandated in Government Regulation Number 82 of 2012 concerning Electronic Certification Providers (PP PSTe) Article 59 paragraph (1) that Electronic System Operators for public services are required to have an Electronic Certificate. Furthermore, in accordance with the mandate of PP PSTe (Article 64 paragraph (2)), the Main Electronic Certification Operator (PSrE) as a "trust anchor" for the issuance of online identities or electronic certificates is organized by the Ministry of Communication and Information. Then the Parent PSrE guarantees the identity of the Parent PSrE by issuing an electronic certificate for the Parent PSrE that meets the technical requirements. Then the Parent PSrE guarantees the identity of the community and the government by issuing electronic certificates (electronic identities) for them. An electronic certificate is obtained on the basis of an application to the Certification Authority (CA) by the user (subscriber).

Certificate Authority (CA) is an institution that plays a role in issuing electronic certificates. The users of the certificate include companies, agencies, or individuals after going through the verification process. The CA is responsible for the storage of information. Each CA is equipped with a Certification Practice Statement (CPS). In addition, the CA also authorized the person's public key pair and private key. The certification process to get approval from a CA can be divided into three stages:

- 1) Customers or subscribers create their own private and public key pairs using the software on their computers.
- 2) Show proof of his identity in accordance with the requirements of the CA.
- 3) Prove that he has a private key that can be paired with a public key without having to show his private key.

4. CONCLUSIONS AND SUGGESTIONS

There are differences of opinion between judges, e-commers, and notaries. regarding the power of proving signatures on an electronic document in proving civil procedure law in Indonesia. Judges and e-commers actors argued that electronic documents that have been signed with electronic signatures have the same evidentiary power as authentic deeds made by authorized officials, after the issuance of Law Number 11 of 2008 concerning Electronic Information and Transactions. Meanwhile, the notary argued that electronic documents signed with electronic signatures only have the power of proof under their hands, because they do not qualify as authentic deeds, that is, they do not face the authorized officials. In practice, electronic signatures on electronic documents need to be certified by a certification body based on the Law in order to have the same evidentiary power as authentic evidence; and

The government in issuing a law should look at other laws that are related to each other, so that one law and another law do not contradict each other.

The Government should immediately grant a License to a legal entity as a Certification Authority institution, both government and private, so that the implementation of electronic transactions, with electronic documents as agreements between the parties that have been signed electronically has the same evidentiary power as an authentic deed in a trial in a court.

5. REFERENCE LIST

- Aaron, R. (1999). Electronic commerce: Enablers and implications. *IEEE Communication Magazine*.
- Adjie, H. (2008). *Sanksi Perdata Dan Administratif Terhadap Notaris Sebagai Pejabat Publik*. Bandung: Refika Aditama.
- Khairandy, R. (2001). Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi Electronic Commerce. *Jurnal Hukum Bisnis*, 16.
- Mudiardjo, D. (2008). Telekomunikasi Dan Teknologi Hukum E-commerce. Diakses dari www.google.com.
- Soekanto, S., & Mamudji, S. (1990). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: Rajawali Press.
- Soemitro, R. H. (1990). *Metodologi Penelitian Hukum Dan Judimetri*. Jakarta: Ghalia Indonesia.
- Supancana, I. B. R. (2008). Kekuatan Akta Elektronik Sebagai Alat Bukti Pada Transaksi E-commerce Dalam Sistem Hukum Indonesia. *Jurnal Hukum Bisnis*, 22.
- Wawancara dengan Ahmad Hidayat, Pamekasan, 11 Desember 2023.
- Wawancara dengan Desi Arisanti, Pamekasan, 12 Desember 2023.
- Wawancara dengan Leanni Bharline, Pamekasan, 12 Desember 2023.
- Wawancara dengan Mia Lestari, Pamekasan, 13 Desember 2023.
- Wawancara dengan Nursiah Sianipar, Pamekasan, 12 Desember 2023.
- Wawancara dengan Thamrin, Pamekasan, 13 Desember 2023.
- Wawancara dengan Toni Iskandar, Pamekasan, 12 Desember 2023.
- Wibowo, A. M. (1999). Kerangka Hukuum Digital Signature Dalam Electronic Commerce. Diakses dari amwibowo@caplin.cs.ui.ac.id.