Journal of Social Research

P-ISSN: 2827-9832
E-ISSN: 2828-335x
http://ijsr.internationaljournallabs.com/index.php/ijsr

IMPLEMENTATION, ADVANTAGES AND BARRIERS AND LEGAL PROTECTION AGAINST THE USE OF ELECTRONIC SIGNATURES

Muhammad Nova Haikal[1*], Siti Mahmudah[2]
Universitas Diponegoro, Indonesia
muhammadnovahaikal@gmail.com

ABSTRACT

The Government has promulgated Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions as first amended by Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and amended again by Law Number 1 of 2024 concerning Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions and Government has also made derivative regulations in the form of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Currently, the Government through the Ministry of Communication and Information Technology has also granted permission to agencies or legal entities authorized as Electronic Certification Providers (PSrE) that provide electronic certificate and electronic signature services. However, the fact is that today people still rarely or do not know how to use electronic signatures or electronic transactions in every agreement. Often people also do not know about the difference between electronic signatures or signature scans. People today also still doubt the legal consequences and legal risks that occur if electronic transactions and/or electronic documents are signed through electronic signatures. With the existing facilities and infrastructure made by the current government, people should be able to use electronic signatures in electronic transactions, both in buying and selling transactions, accounts receivable or the implementation of other agreements that are often carried out in the community. Therefore, this study aims to discuss and elaborate the implementation of provisions regarding the use of Electronic Signatures in electronic transactions and electronic contracts and also to provide an understanding of legal protection to facilitate and convince the public to be able to carry out transactions and agreements electronically.

Keywords: Electronic Signature, Electronic Transaction, Electronic Certification Operator (PSrE), Electronic Transaction System Operator

INTRODUCTION

The development of digitalization today forces society to be able to transform where information and traditional business processes are converted into digital form. It's a growing trend in various sectors of human life, including business, education, healthcare, government, entertainment, and more. The development of digitalization will continue rapidly along with technological innovations that continue to grow. This will have a huge impact on various aspects of our lives, both positively and negatively, and will require constant adjustments in terms of regulation, cybersecurity, and data management.

The era of digitalization has also changed the way and implementation of the use of signatures, where in the past signatures were known as signs or markings which were usually done with a pen or other stationery by someone to mark or certify official documents or letters. Signatures are also often used as a way to identify a person or indicate agreement, conformity, or agreement in a legal or business context. But now signatures have experienced rapid development over the past few years, where signatures can be implemented electronically to sign documents or transactions digitally, without the need to use pen or paper.

The growing era of digitalization is also coupled with the conditions of the COVID-19 pandemic, electronic signatures are becoming more important as many businesses and government agencies turn to remote working to avoid physical contact, so electronic signatures can be a very useful tool to carry out various business and government activities efficiently and securely, especially when physical meetings must be limited.

Electronic signatures are currently a method of granting approval, authorization, or verification of documents or transactions using digital or electronic signatures, rather than traditional signatures on paper. Some of the characteristics and benefits of electronic signatures in the era of digitalization are more convenience, efficiency, security, digital footprint, cost savings and flexibility. However, although electronic signatures have many benefits, there are still challenges that need to be addressed, including issues of security, privacy, authenticity and cost.

The development of electronic signatures has experienced rapid development over the past few years. Developers and service providers have worked hard to improve the security and reliability of electronic signatures. This includes the use of strong encryption technology, Multi-factor authentication, and traceable audit trails. Various methods and technologies are used for electronic signatures, including digital signatures, biometric signatures (such as fingerprints or faces), and more. This allows people to choose a method that suits their needs. Electronic signatures have been integrated into various business software and services. It allows users to sign documents directly from applications they use daily, such as email or document management applications.

The use of electronic signatures is not only applied in the public environment between state officials but is also commonly practiced in aspects of business and commerce. Effectiveness, efficiency, fast and cheap are the reasons for business people and public agencies to optimize this method. But this practice is still faced with legal standing if needed as evidence. The weakness of digital innovation is the ease of hacking from various regions so that it is impossible to misuse the signature.

The regulations governing the use of electronic signatures are eIDAS (Electronic Identification and Trust Services Regulation) in the European Union and UETA (Uniform Electronic Transactions Act) in the United States which you regulate and are widely adopted by other countries. This regulation provides a legal basis for the use of electronic signatures in many legal contexts. The Government of the Republic of Indonesia has promulgated regulations/provisions related to electronic signatures, among others, through (i) Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions, (ii) Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, (iii) Law Number 11 of 2008 concerning Electronic Information and Transactions, and (iv) Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

The Law on Information and Electronic Transactions (UU ITE) is the first law in the field of Information Technology and Electronic Transactions as a much-needed legislation product and has become a pioneer that laid the foundation of regulation in the field of utilization of Information Technology and Electronic Transactions. However, in reality, the implementation journey of the ITE Law has encountered problems. Some of the issues that arise related to the implementation of the use of electronic signatures are (i) regarding the validity of procedures and forms of electronic signatures in electronic documents, electronic contracts and electronic transactions, (ii) electronic documents, electronic contracts and electronic transactions using electronic signatures whether they can be accepted as valid evidence based on laws and regulations and (iii) How legal protection and security data against the parties to the agreement using electronic signatures. In fact, due to lack of socialization and there are many unanswered problems in society, until now only a few Indonesians use electronic signatures as a means of approving electronic documents, electronic transactions and/or electronic contracts.

Based on this background, the author is interested in examining the issue of how to implement, barriers and legal protection against the use of electronic signatures in electronic transactions and electronic contracts. This study tries to examine and analyze various laws and regulations governing electronic signatures with problem formulations (i) how are the arrangements, implementation and obstacles arising from the use of electronic signatures in transactions and electronic contracts? and (ii) What is the legal protection for the use of electronic signatures in electronic transactions and contracts?

Facts show that there have not been many research results related to the object of research, including in the form of journals. However, specifically for legal research, with the author's limited ability to trace the results of research in the field of law, there are several studies on the application of the doctrine of equality in research conducted by Annisa Noor El Izzaha and Wasis Sugandhaa entitled "The Use of Electronic Signatures in the Implementation of E-Government to Realize Efficient Public Services". The research is more focused on the use of electronic signatures, only focusing on the implementation of E-Government (Izzah & Sugandha, 2021).

Based on the search results, the author got a second study conducted by Sulaiman, Nur Arifudin and Lily Triyana with the title "The Power of Digital Signature Law as Legal Evidence in Review of Civil Procedural Law". This study also only emphasizes electronic signatures as evidence for civil trials in Indonesia (Sulaiman, Nur Arifudin, & Lily Triyana, 2020)..

This article will be elaborated and discussed based on the theory of freedom of contract. Where the Indonesian Positive Law regulates freedom of contract as stipulated in Article 1338 paragraph 1 jo. Article 1320 of the Civil Code. Freedom in contract gives the parties can regulate the rights and obligations in the contract they agree. Freedom of contract theory refers to the principle that provides for everyone to make an agreement or contract with the content of any agreement agreed by the parties, provided that the content is in accordance with the provisions of legislation, public order and decency. Freedom of contract is necessary to understand and elaborate on how parties can use electronic signatures in every agreement, electronic contract and electronic transaction.

This article will also be reviewed and discussed by referring to theories in other theories such as the theory of legal objectives and the theory of legal certainty that are relevant to the discussion of this article. Based on Gustav Radbruch, said that there are three objectives of law, namely expediency, certainty, and justice. In carrying out these three purposes, the law must use the principle of priority. Justice may take precedence and sacrifice benefits for the wider community. Gustav Radbruch said that there is a scale of priorities that must be carried out, where the first priority is always justice, then expediency, and finally legal certainty. Law performs its function as a means of conservation of human interests in society. Legal objectives have objectives to be achieved that divide rights and obligations between individuals in society. The law also gives authority and regulates how to solve legal problems and maintain legal certainty (Sudikno Mertokusumo, 2003, hlm. 77).

When related to the function of law as the protection of human interests, law has goals and objectives to be achieved. The basic purpose of law is to create an orderly and balanced society in social life. The achievement of order in society is expected to protect human interests. In achieving its goals, the law is tasked with dividing rights and obligations between individuals in society, dividing authority, and regulating how to solve legal problems and maintain legal certainty Soedjono Dirdjosisworo argued that in the association of human life, human interests can always conflict with one another, so the purpose of law is to protect those interests (Soedjono Dirjosisworo, 1983). Meanwhile, Muchsin once revealed that actually the law is not as an end but he is only a tool, who has a purpose is man, then what is meant by the purpose of law is man with law as a tool to achieve that goal. Van Apeldoorn said that the purpose of the law is to regulate peaceful association. This means that the law requires peace, which all boils down to an atmosphere of peace. Rudolf Von Jhering said that the purpose of law is to maintain a balance between various interests. Aristotle said the purpose of law is to provide the greatest happiness for as many members of society as possible, as in line with Roscoe Pound's opinion that law is a tool of social engineering, which means the purpose of law is as a tool to build society (Muchsin, 2006, hlm. 11).

Theories related to the theory of legal objectives in this study are also related to legal certainty. Legal certainty means that everyone knows which and how much his rights and obligations are. Legal certainty contains two meanings, namely first, the existence of general rules that make individuals know what actions can or cannot be done, and second, in the form of legal security for individuals from government arbitrariness due to the rule of law carried out by the state against individuals. Legal certainty is not only in the form of articles in the law but also there is consistency in judges' decisions between one judge's decision and another judge's decision for similar cases that have been decided (Pengantar ilmu hukum, 2008). In addition, this research is also related to the theory of legal expediency. The benefit of law is that order and tranquility can be achieved in people's lives, because of the existence of orderly laws. Satjipto Raharjo revealed that the theory of legal expediency (usefulness) can be seen as a tool of society to create order and order. Therefore it works by providing instructions about behavior and in the form of norms (legal rules). Basically, legal regulations that bring benefits or legal uses are for the creation of order and tranquility in people's lives, because of the existence of orderly law (rechtsorde) (Satjipto Rahardjo, 1991). A series of theories presented above, will be used to analyze how the implementation and legal protection of the use of electronic signatures.

Based on the description and presentation of the background and theoretical framework above, this article will discuss and describe how the arrangement, implementation and obstacles arising from the use of electronic signatures in electronic transactions and contracts. The novelty of this study is a previous researcher who has a similar discussion to this study but has different material from this study, namely the research conducted by Annisa Noor El Izzaha and Wasis Sugandhaa with the title "The Use of Electronic Signatures in the Implementation of E-Government to Realize Efficient Public Services". The research is more focused on the use of electronic signatures, only focusing on the implementation of E-Government (Izzah & Sugandha, 2021). The second research was conducted by Sulaiman, Nur Arifudin and Lily Triyana with the title "The Power of Digital Signature Law as Legal Evidence in Review of Civil Procedural Law". This study also only emphasizes electronic signatures as evidence for civil trials in Indonesia (Sulaiman dkk., 2020).

Based on the studies mentioned above which have the same theme or subject matter as this journal but have a different research focus where the author focuses this journal related to implementation, obstacles and legal protection and protection against the use of Electronic Signatures. That way, it can be concluded that the journal written by the author with the title "Implementation, Advantages and Obstacles and Legal Protection Against the Use of Electronic Signatures" can be accounted for its authenticity.

METHOD

This legal research is carried out to produce arguments, theories and new concepts as prescriptions in solving the problems at hand. The research was conducted using a type of research approach by examining all laws and regulations related to the legal theme being handled, namely normative juridical which is regulated systematically. The approach method used in this study is a normative juridical approach. The term 'approach' is something (deed, effort) approaching or approaching. The juridical approach in this study is an approach in terms of applicable laws and regulations. While the normative approach in this case is intended as an effort to bring the problem under study closer to the normative nature of law. The normative approach includes legal principles, legal systematics, legal synchronization, comparative law or legal history (Hilman Hadikusuma, 2013).

Normative juridical approach which means a legal research approach carried out by examining the main legal materials, namely laws and regulations, legal principles, legal theories, and legal doctrines. This approach is also known as the literature approach, because the data used in this study are secondary data derived from books, journals, articles, and other sources related to law. This approach is carried out to analyze and understand the law as a norm prevailing in society.

The normative juridical approach focuses on the study of the application of positive legal rules governing electronic signatures, among others: Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions ("Law No. 11/2008") as first amended by Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions ("Law No. 19/2016") and amended again with Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions ("Law No. 1/2024") (hereinafter Law No. 11/2008, Law No. 19/2016 and Law No. 1/2024 called "ITE Law") jo. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Personal Data Protection in Electronic Systems ("Regulation No. 20/2016"), Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems ("Regulation No. 20/2016") jo. Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 11 of 2018 concerning the Implementation of Electronic Certification ("Regulation No. 11/2018") jo. Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions ("PP No. 71/2019") jo. Regulation of the Minister of Communication and Information Technology Number 5 Year 2020 concerning Private Scope Electronic System Operators ("Regulation No. 5/2020") jo. Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 10 of 2021 concerning Amendments to the Regulation of the Minister of Communication and Information Number 5 of 2020 concerning Private Scope Electronic System Operators ("Regulation No. 10/2021").

The discussion of problems in this article uses the approach of (i) Law (statue approach), and (ii) Conceptual (conceptual approach). The legal approach is carried out by describing and reviewing laws and regulations related to the legal theme discussed. Conceptual approach, which departs from a thought and doctrine that grows in the science of law itself. By analyzing the thoughts and doctrines in the science of law, this Article contains concepts and ideas that can realize relevant legal understandings, concepts, and principles and to answer the problems in this Article.

RESULTS AND DISCUSSION

A. Electronic Signatures

In general, a signature is a tool or method used as an endorsement and as an identity in the agreement made between the parties. However, along with the times, where human needs are increasingly complex and technology is growing rapidly so that it can carry out various activities instantly. The occurrence of this development then brought many changes, one of which was the birth of electronic signatures. Based on the ITE Law that an electronic signature is a signature that includes electronic information attached or interrelated with each other where the signature is used as a means of confirmation and guarantees the truth of the information.

An electronic signature is not a signature affixed to paper as is common for a signature or convention a signature using a scanning machine, Julius Indra Dwipayono defines, an electronic signature is an identity that functions as a sign of agreement on an obligation contained in an electronic deed (Julius Indra Dwipayono Singara, 2004). Soemarno Partodihardjo said that an electronic signature is a data item related to a digital message encoding to ensure that the data is original and unmodified data (Soemarno Partodihardjo, 2008). According to Efa Laela Fakhriah, an electronic signature is electronic information which consists of the identity of the signing parties and notifies that their status as legal subjects in an electronic information they sign (Efa Laela Fakhriah, 2017). If summarized, then electronic signature is a tool used to ensure the purity of electronic evidence in the form of electronic documents or electronic information.

Based on Article 2 of the UNCITRAL (United Nations Commission on International Trade Law) Model Law on Electronic Signatures, electronic signatures are defined as follows (United Nations, 2002):"Electronic signature means data in electronic form in, affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data messages and to indicate the signatory's approval of the information contained in data message."

The free translation is:

Electronic signature means data in electronic form, attached to or relating to a message, which can be used to: (i) identify the signatory; and (ii) to indicate the signatory's consent to the information contained in such data.

In general, electronic signatures are not the same as signatures in general, electronic signatures are made in different ways or methods to mark a document or data where the signature not only recognizes data from the sender but the electronic signature can ensure the completeness of the document where the document does not undergo any changes during the transmission process (transmission). The use of electronic signatures certainly has benefits, as well as if the electronic signature is applied to a message or electronic data sent, it can be used as a guarantee that the electronic data sent does not experience changes made by parties who do not have rights.

The ITE Law defines electronic signatures in Article 1 number 12 and in Article 11 of the ITE Law, namely signatures consisting of Electronic Information embedded, associated or related to other Electronic Information used as verification and authentication tools. Electronic signatures will have legal force and effect with a record that they must be able to meet certain conditions, including the creation of an electronic signature that must only include data from the signatory, a notification stating that the signer agrees to provide related electronic information. While Article 12 of the ITE Law determines the obligations of the parties who take part in the process of making electronic signatures, they must be able to provide security at least be able to guarantee that the system is difficult to access by others, ensure the authenticity of electronic certificates used to support the authenticity of electronic signatures, and if there is a data leak, they must immediately report to the supporting parties of electronic signature services. Furthermore, regarding the scope of electronic signatures, Edmon Makarim stated that like conventional signatures, an electronic signature at least shows several things, namely (Edmon Makarim, 2020):

a. Serves as a symbol of one's authority where by affixing the identity of a legal subject who is responsible for what is conveyed or written in addition to representing the identity characteristics of a person and also his authority;

b. Serves as authentication regarding electronic data provided a signature has been read and known and ends with including the name concerned as a key;
c. Serves as an agreement that the need for a signature is a manifestation of an act on the agreement or acceptance of information available through electronic media in it;
d. Serves as proof that the content of the information that has been affixed with the signature will be legal evidence for the parties who use it.

Basically, an electronic signature has the same function as a signature affixed to paper or commonly known as a conventional signature. However, keep in mind and know that an electronic signature is not a signature placed on paper like a signature in general. Because before finally getting an electronic signature, you must first create a code generated from the encryption process and then sent through cyberspace or cyberspace (Soemarno Partodihardjo, 2009). The encryption process is a process used to protect electronic information so that it cannot be read by just anyone, so to be able to read the information requires the help of a special knowledge (Rifkie Primartha, 2011). Thus, basically this electronic signature is a guarantee related to the integrity of a message and as a guarantee that the sender of the message is a party who does have rights to the content of the message. So, an electronic signature is a code sent in the form of an electronic message with the aim of providing certainty about purity and ensuring that in a data or document there is no change whatsoever (Soemarno Partodihardjo, 2009). Also, the electronic signature contained in an electronic document aims to provide certainty about the authenticity or authenticity of the document and provide confidence agreement about the content of the document.

B. Terms, Elements and Classification of Electronic Signatures

The legal basis for the use of Electronic Signatures is regulated in article 11 paragraphs (1) and (2) of the ITE Law. In the explanation, it is explained that in essence it states that even though the electronic signature is in the form of a code, the electronic signature still has the same position as the signature in general. Therefore, the issuance of the Electronic Information and Transaction Law, especially Article 11 of the ITE Law, states that electronic signatures will have legal force and consequences as long as they can continue to implement and fulfill the conditions that have been determined (Sugeng, 2017).

Likewise, it is explained in PP No. 71/2019, where the regulation regarding Electronic Signatures is regulated in Paragraph 2 of articles 59-60, then in articles 61-64. The articles in the Government Regulation are essentially the same as the articles in the Electronic Information and Transaction Law regarding Electronic Signatures. Based on the understanding of electronic signatures that have been explained earlier, from this understanding there are several basic elements about an electronic signature, the first is that an electronic signature is an electronic information. As stated in Article 1 number 1 of the ITE Law, namely electronic data sets but not only fixated on written form which means it can also be in the form of pictures, numbers and others. Electronic information is important in the use of electronic signatures, because electronic information is the basis of electronic signatures (Ahmad Redi, 2010).

The second element is tied to other information. This means that related to the existence of a unity between information with one another or simply referred to as integrity, with this integrity, every party who receives a message will feel confident that the message that has been sent by the other party will be received in a safe state or there has never been any change. In this case, an electronic signature is needed to ensure the integrity and security of the message to be sent. The recipient of the data can check the integrity of the data it receives by comparing the hash value, namely if the hash value is really the same, it means that the data received is the original data and there is no change whatsoever. Meanwhile, if there is a difference in the value of the value, it is necessary to be vigilant because it does not rule out the possibility if the data received has changed (Efa Laela Fakhriah, 2017).

The use of an electronic signature in the process of making an electronic agreement, will provide its own convenience if one day a dispute occurs, namely during the evidentiary process. Because, using an electronic sign in the contract will provide information on where the electronic data comes from. To further strengthen the validity of electronic signatures in the proof process, an electronic certificate or Certification Authority (CA) issued by a body that has been appointed by the Government and authorized to issue the electronic certificate is needed.

Third, electronic signatures are tools that can be used to verify and authenticate. With this verification and authentication, electronic data can be known where it came from. This verification or validation aims to test the correctness of the electronic data. While authentication to ensure the integrity of the electronic data (Ahmad Redi, 2010).

Electronic signatures have a function that is no different from signatures in general, which can be used as approval of receipts or approvals regarding important information in an agreement, document, or transaction tool. Basically, an electronic signature has several properties, including that an electronic signature is Authentic, which means that it is difficult to write and cannot be imitated by others. Therefore, this authentic electronic signature can be used as evidence so that the person who affixes the signature cannot avoid or deny the electronic signature. Other than that, electronic signatures also have properties that will only be valid for one particular message or document and their copies are exactly the same. An electronic signature cannot be transferred to another message or document even if the message or document has only a slight difference, which means that if there is a change in the message or document then the electronic signature is automatically invalid. Finally, an electronic signature is easy to check. Electronic signature checks can also be done by people who have never met directly with the party who put the signature (Titi S. Slamet & Marianne Masako Paliling, 2019).

An Electronic Signature can be classified into two parts, First is Electronic Signature (Ordinary) which means that the signature is made with the help of electronic media but the process is the same as doing a signature in general which is made and then scanned. The scan results of the signature will become electronic information in the form of an image file which is then glued to the intended electronic document. This is one of the scopes of the ordinary electronic signature class. The second is a guaranteed Electronic Signature or Electronic Signature, is an electronic signature that is required to meet all the conditions that have been determined, so that it can then be equated with signatures in general or conventional signatures. Secure electronic signatures are provided to collect all kinds of technological advances that may develop in the field of security of technology. In terms of electronic signature security, this is not only addressed to the signer or signer but also for the security and integrity of the electronic information embedded. One of the secure electronic signatures is a digital signature. In addition, it is mentioned in article 60 paragraph

(2) of Government Regulation No. 71/2019 concerning the Implementation of Electronic Systems and Transactions which mentions two types of electronic signatures, namely those with certificates from trusted parties and without certificates. Currently, in Indonesia Electronic Certificate Providers consist of ten (10) companies, namely (https://tte.kominfo.go.id/listpsrenew):

a. PT Privy TIdentientity Digital (PrivyID), is a company that organizes electronic signature creation services that have received recognition from the Ministry of Communication and Information Technology with a Parent Recognition Decree No. 2 of 2023 with the type of Non-Agency PSrE. PrivyID has a website that can be accessed easily if we need more information, which is through https://privy.id/;
b. PT. Net Internusa solutions, by elevating the Digisign platform, is a company engaged in technology, namely as an electronic certificate provider or Certification Authority (CA), a certified electronic signature creation service that has been recognized by the Ministry of Communication and Information Technology with a Parent Recognition Decree No. 212 of 2022 with the type of Non-Agency PSrE. Further information about Digisign can be accessed through the official website, namely https://digisign.id/;
c. The Public Company of the Republic of Indonesia Money Printing or Peruri is an electronic certificate service provider that has been recognized based on the Parent Recognition Decree No. 340 of 2022 with the type of Non-Agency PSrE. Peruri has an official website that can be accessed by anyone who wants to know more, namely https://ca.peruri.co.id/;
d. PT. Indonesia Digital Identity (VIDA), is an electronic certificate provider company that has been recognized by the Ministry of Communication and Information as the issuance of the Parent Recognition Decree No. 1 of 2023 with the type of Non-Agency PSrE and has a https://vida.id/ website;
e. PT. Djelas SignatureBersama is an electronic certificate organizer that has been recognized by the Ministry of Communication and Information with a Parent Recognition Decree No. 109 of 2023 with the type of Non-Agency PSrE and its website, namely, https://djelas.id/;
f. PT Tilaka Nusa Teknologi, is a company that organizes electronic signature manufacturing services that have received recognition from the Ministry of Communication and Information Technology with a Parent Recognition Decree No. 107 of 2023 with the type of Non-Agency PSrE and its website, namely, https://tilaka.id/;
g. PT Digital Signature Asli, is a company that organizes electronic signature manufacturing services that have received recognition from the Ministry of Communication and Information Technology with a Parent Recognition Decree No. 551 of 2021 with the type of Non-Agency PSrE and its website, namely, https://www.xignature.co.id/;
h. The Agency for the Assessment and Application of Technology, which uses the iAUTHENTIC platform, is an agency that has the authority to accept registration, verify, and issue electronic certificates and electronic signatures for state civil apparatus, TNI and Polri. This iAUTHENTIC has been recognized by Kominfo with the Parent Recognition Decree No. 969 of 2018.39; and

i. Electronic Certification Center (BSre) of the National Cyber and Encryption Agency (BSSN). BSrE is a unit that carries out technical activities at BSSN with the authority it has, namely to provide electronic certificate issuance and management services. This BSrE was formed based on the Regulation of the Head of the State Encryption Institute Number 15 of 2016 concerning the Organization and Work Procedures of the Electronic Certification Center. This BSreBSSN company has obtained a Parent Recognition Decree Number 103 of 2022 with the type of PSrE Agency from the Ministry of Communication and Information and has a https://bsre.bssn.go.id/ website.

Based on information from the Indonesian Certificate Center, which is included in electronic signatures without electronic certificates, namely in the form of QR CODES, BARCODES, scanned wet signatures, making signatures using a pencil scanner (scanner), and in the form of OTP codes which are usually sent via SMS, or registered email. Meanwhile, electronic signatures that have electronic certificates are made using devices that are used to create electronic signatures. So, the electronic signature is made with a special device and the manufacture is done by the service that also issues electronic certificates (https://bsre.bssn.go.id).

In addition, Edmon Makarim in his book mentions that along with the rapid development of technology, then arises what is known as an electronic signature. Based on his opinion, there are several kinds of technology patterns related to electronic signatures including the use of keys (passwords) or a combination of several things or commonly called hybrid methods, a signature that is scanned electronically (scanned signature) or names typed in an information (typed names), the use of button features as a sign of agreement or as a sign of acceptance electronically (such as ok buttons, or accept button) which is assisted by a secure communication channel (secure socket layer), then the use of unique signatures on limbs or commonly called biometrics, and the last is the use of digital signatures based on encryption of a message or digital signatures. All types of electronic signatures have different levels or evidentiary values in accordance with the rules applicable in secured communication (Edmon Makarim, 2020).

C. Implementation of electronic signatures in electronic documents

Electronic Signature is a digital signature based on a public key infrastructure and based on biometrics (Edmon Makarim, 2020). Before reaching the recipient, the electronic signature goes through several processes First, as the party who sends and makes the signature will make a message digest taken from an original message, this message digest has identical and unique characteristics so it is difficult to fake. The tool used to create a message digest is a hash (function dechange). Second, after the message digest is signed by utilizing the private key of the sender, the original message that has been signed is then sent to the destination, namely the recipient of the electronic document (Ahmad Redi, 2010).

According to Edmon Makarim, the creation of a digital signature used to sign an electronic document or electronic information has several procedures that must be passed, the first is that each signer must limit each document or information that will be given a signature, the second is to compress the message using the help of softaware, the third is to encrypt the core message or document using a key private owned by the signer to produce a digital signature, and the last is the sending of a digital signature along with the message or document that has been signed. Based on the procedure above, a digital signature is unique so that it is difficult to be opened by other parties who do not have a pair of private keys, namely public keys so that the existence of two paired keys can guarantee the security of messages or documents from the sender to the recipient (Edmon Makarim, 2020).

Technically, the creation of electronic signatures has been determined as stipulated in Article 61 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Based on the essence of the article, the technical creation of electronic signatures must contain a unique code and can recognize the identity of the signature maker, the data is made by the electronic certificate operator, and must meet conditions such as not easily known by other parties, the data is in an electronic device controlled by the signature maker, and must be stored in a place that can only be accessed by authorized parties, can check the authenticity of the signatory's identity, and the signatory must maintain confidentiality and be responsible for the electronic signature generation data.

To ensure a method of work used in the use of making electronic signatures in terms of proving the identity of the signatory, at least two authentication factors are applied, this is as specified in article 63 paragraph (3) letter c. What is meant by authentication factors is what you know, for example a PIN number or password, then what you have for example electronic signatures, magnetic cards that have chips, tokens and the last is in what form for example in the form of fingerprints and retinas. In terms of the use of cryptographic methods, there are two forms of cryptography that are quite popular in the general public, namely symmetric and asymmetric cryptography. However, usually what is used in an Electronic signature is asymmetric cryptography (Ahmad Redi, 2010). Symmetric Cryptography or Symmetric Key is a common type of cryptography when compared to cryptography or asymmetric keys. Symmetric cryptography is an encryption that is used only one key where the key serves to lock and unlock an electronic signature. While asymmetric cryptography has two different keys, there is a key used to lock the electronic signature and also a key to unlock it (Edmon Makarim, 2020).

Electronic signature affixing can only be placed in a document or message in electronic form. The affixing of the electronic signature is an effort or process so that the purpose of the signer can be conveyed, the electronic signature must have two attributes, First, Signer Authentication means that the signature affixed must be able to identify the signer of the document or electronic message and is difficult to imitate by others. Second, Document Authentication, i.e. a Signature must identify what is signed so that it is difficult or even impossible to forge or change without being noticed by the owner.

A document authentication and signatory authentication is a tool used to avoid forgery and is an application of the concept of non-repudiation in the field of information security. Non-repudiation is a guarantee of the authenticity or delivery of an original document to avoid denial from the signatory of the document as if he did not admit to having affixed the signature and to avoid a refutation from the sender of the document where he said he did not send the document.

Stephen Mason in his book mentions that there are several attributes needed in every use of electronic signatures, namely first, electronic signatures must be authentic. That is, an electronic signature must be able to guarantee the authentication of the original data and the integrity of the message. Second, in an electronic signature, technical methods must be available to prevent parties who have signed the electronic document from claiming or refuting that the parties did not sign it. Third, that an electronic signature must have a public key as a security key so that it cannot be forged by unauthorized persons or parties. Fourth, when an electronic signature is added in an electronic message or document, the electronic signature and related messages or documents can be verified for legal purposes. Fifth, electronic signatures that have been affixed to an electronic message or document cannot be reused or re-used (Stephen Mason, 2003). Electronic Signatures used in Electronic Transactions can be generated through various signing procedures. In the case of the use of Electronic Signatures on behalf of Business Entities, the Electronic Signature is called the electronic seal. According to article 11 paragraph (1) of the ITE Law jo Article 59 Paragraph (3) of PP No. 71/2019 explains that an Electronic Signature is considered valid if it meets the following requirements:

a. Electronic Signature generation data relates only to the Signatory;
b. Electronic Signature creation data during the electronic signing process is only in the power of the Signatory;
c. Any changes to the Electronic Signature that occur after the time of signing can be noticed;
d. Any changes to Electronic Information related to such Electronic Signatures after the time of signing may be noticed;
e. There are certain methods used to identify who the Signatories are;
f. There are certain ways to indicate that the Signer has given consent to the relevant Electronic Information.

The implementation of the process of making electronic signatures can be summed up into three main stages, namely:

a. Registration
   This stage is carried out by the applicant for an electronic signature to the Electronic Certification Provider (PSrE) which has been accredited by the Ministry of Communication and Information Technology (KOMINFO). The applicant must fill out the registration form and submit the required documents, such as a photocopy of ID card, photocopy of NPWP, and photocopy of passport.
b. Verification
   At this stage, PSrE will verify the applicant's data to ensure the validity of the data. Verification can be done in various ways, such as manual data verification, electronic data verification, or data verification through third parties.
c. Publication
   Once the applicant's data is verified, PSrE will issue an Electronic Certificate. The Electronic Certificate contains the applicant's public key and the applicant's identity information. This Electronic Certificate is used to perform electronic signatures. Once you receive your Electronic Certificate, you can start using electronic signatures for various purposes.

D. Security of the Use of Electronic Signatures

As mentioned above, an electronic signature is a signature that is affixed to an electronic message or document as well. Security of electronic data or information becomes a very important thing for parties who use Information technology facilities because, there are important data from messages or electronic documents that have been signed. Security of a data or information either directly or indirectly certainly has an important role for the parties interested in it. The more data or information from parties stored, the more risk of damage, loss or disclosure of data and information to those who are not even entitled to that data and information.

Security in information systems has several understandings, one of the understandings conveyed by G.J. Simons that a security of information systems is an action like what can be done as a prevention of the occurrence of fraudulent acts or at least can find out if there is fraud in an information system that has no physical meaning. Based on the above opinion, the security in this information system serves to prevent, protect and overcome all kinds of risks from the occurrence of unauthorized actions that come from the parties who use it without permission from the owner, avoid infiltration, and destruction of various information owned by the parties (Farida Dewi, 2012).

The basics of information security have two major areas, namely Physical Information Security and Logical Information Security. Physical information security is defined as an effort to protect an organization's system from physical attacks which includes all physical elements such as protecting the machine on which the application is run, protecting a room where the machine is operated, protecting the building in which there is a machine used installed, and protecting an area that is where the company stands. The elements mentioned must be safeguarded and protected from all kinds of interference and threats that may occur. Not only that, physical security also means that communication channels must be protected both via cable and waves or wireless to avoid eavesdropping and cable damage.

While information security logically is information security that is connected to IT security solutions and problems (IT Architecture), applications and processes. As mentioned above, the Internet network must also be logically protected because almost all organizations and individuals are connected to public networks on the Internet, which means that data can be accessed remotely. Thus, it is very necessary to protect important and sensitive data or information so that it cannot be accessed by parties who are not entitled to it. In short, the existence of information security includes several things, namely Authentication and Identification, access restrictions, confidentiality or privacy, data integrity, accountability, configuration or policy, assurance or monitoring, information security management, and cryptography.

It has been explained earlier, that in an electronic signature can use cryptographic methods. Technically, the security system for electronic signature data is to use cryptography. The use of cryptography that is relative or commonly used in asymmetric electronic signatures is by realizing the implementation of digital signatures accompanied by support in the form of digital certificates based on public key infrastructure operators. The circuit involves two keys called the private key and the public key. This private key is held by the electronic signature generator, this private key is used to create the digital signature and must be kept as a secret. While the public key or public key is a key pair provided to the public that is used to verify messages scrambled with the private key (Edmon Makarim, 2015).

E. Legal Protection of the Use of Electronic Signatures

Along with the rapid development of the times, as happened in people's lives accompanied by increasingly modern and sophisticated technology, this is also an introduction to the presence of developments regarding evidence that had previously been regulated in HIR / RBg. The development of evidence includes the emergence of photocopy evidence, to the use of electronic evidence in court. The rapid development of technology and information among the public, there is also an increase in legal actions carried out through internet media channels. With this, it does not rule out the possibility of increasingly varied disputes in the future. For example, disputes in electronic transactions where the dispute resolution is known as document evidence or electronic mail which certainly has a relationship with electronic signatures.

Currently, there are several laws governing electronic evidence, such as the Law on Company Documents, the Law on Information and Electronic Transactions. The use of electronic signatures in civil evidence can be used as a tool to ensure the purity and validity of documents and electronic messages. In order for an electronic signature on electronic data or messages to have strong legal force in proof, the electronic signature must be registered with the company that issued the electronic certificate. Every digital signature that has obtained an electronic certificate will be more guaranteed about authentication than an information or electronic document that has been signed (Efa Laela Fakhriah, 2017).

Julius Indra Dwipayono said that an electronic signature will get the same legal power and consequences as a conventional signature if it can fulfill or guarantee the integrity of the electronic deed and is able to identify who signed the electronic deed. An electronic signature will have valid legal force and effect provided that all conditions specified in article 11 paragraphs (1) and (2) of the Electronic Information and Transaction Law must be fulfilled (Julius Indra Dwipayono Singara, 2004). Given the types of evidence available in the HIR / Rbg, as well as the formal and material requirements for electronic evidence as mentioned in article 1 point 4, article 5 paragraph (3), articles 6 and 7, based on this a Judge can examine and carry out electronic evidence, one of which is in the form of electronic signatures as evidence in the Trial, namely with the help of expert testimony who understands and understands in the Electronic field. In addition, in the case of proving this electronic signature, the Judge can use the evidence of the Allegations at the Trial.

The presence of experts, does not rule out the possibility that the explanations presented by him at the Court will provide knowledge or increase knowledge for the judge about an electronic evidence, one of which is in the form of an electronic signature and can be used as a basis for assessing electronic evidence in the form of electronic signatures. Meanwhile, the strength of proof was then fully handed over to the Panel of Judges (Farida Dewi, 2012). So, although electronic signatures have been recognized as having valid legal force, the civil procedural law itself has not explicitly regulated so that if the electronic signature is used as evidence against a dispute in Court it would be better if the physical form can be presented in the Court as a backup of evidence that can certainly be used to strengthen evidence such as presenting experts in the field of technology.

F. Benefits and Barriers of Electronic Signatures

The use of electronic signatures can certainly help us to reduce the use of paper in every making agreements, contracts, or other things as mentioned above that the affixing of electronic signatures is not done in printed documents but the document is electronic as well.

Thus, an Electronic Signature certainly provides its own benefits for its users. These advantages include First, authenticity (Ensured) or the authenticity of a message that serves to show where electronic data comes from. Authenticity assurance is known from the existence of a hash function in the Electronic Signature system where the data receiver can compare hash values (random values) (Soemarno Partodihardjo, 2008). Dr. Edmon mentioned in his book what is meant by hash function is a mathematical process to summarize or make the essence of a message electronically so that it becomes compressed into the form of a smaller message or document so that it can be communicated more efficiently in an electronic communication (Edmon Makarim, 2020).

The second is the integrity or integrity of the message or document communicated serves to ensure that the message, document or electronic data sent does not experience any changes from parties who do not have rights or no authority whatsoever. The third is Non-Repudiation or undeniable which serves to guarantee that the sender of the message or electronic document cannot deny the message or electronic document sent. The sender cannot also deny the content of the message or electronic document sent because it uses asymmetric involving the private key and public key. Finally, namely Confidentiality or confidentiality of messages communicated which serves to ensure the confidentiality of a message or electronic document sent, because it can be possible that only certain people know it meaning that not just anyone can know what the contents of the message or electronic document have been signed-in and included in the digital envelope.

However, in its application, electronic signatures certainly cannot be separated from obstacles. The obstacles that occur include there are still many doubts about the authenticity and security of officials to start trying to implement electronic signatures, the mindset or mindset that considers electronic signatures difficult to do, and the need for new cultural adjustments in society, especially for people who will often use electronic signatures such as government agencies, courts, business people in making agreements or cooperation contracts and others.

On the other hand, the application of electronic signatures is still limited to certain documents. Article 5 Paragraph 4 of the ITE Law states that signatures in electronic form do not apply to documents or letters that based on other laws must be made in written form. Signatures in electronic form also do not apply to documents that must be made in the form of notarial deeds or deeds made by the deed making officer. If previously discussed about the advantages and some parts of the barriers, then there are further disadvantages of electronic signatures which are also more or less the influence of hampering the application of this electronic signature. The weaknesses that are obstacles to the implementation of electronic signatures are:

1. Security is still questionable, electronic signatures are still vulnerable to cybersecurity attacks, such as forgery and eavesdropping. This may pose a risk of loss for users of electronic signatures.
2. Compatibility, electronic signatures use different technologies, so compatibility problems can occur between systems. This can make it difficult for users to use electronic signatures across multiple systems.

3. The cost is still expensive, the creation and use of electronic signatures still requires relatively expensive costs. This can be an obstacle for people who want to use electronic signatures.
4. Ignorance of the public, there are still many people who do not understand the concept of electronic signatures and their benefits. This can cause people to be reluctant to use electronic signatures.

CONCLUSION

Some conclusions obtained from the results of this study are based on the ITE Law that electronic signatures are signatures that include electronic information attached or interrelated with each other where the signature is used as a means of confirmation and guarantees the truth about the information. An electronic signature is not a signature affixed to paper as is usually a signature or convention a signature using a scanning machine, but an electronic signature is a tool used to ensure the purity of electronic evidence in the form of electronic documents or electronic information.

The legal basis for the use of Electronic Signatures is regulated in article 11 paragraphs (1) and (2) of the ITE Law and Articles 59-64 PP No. 71/2019, which has the same position as signatures in general, which can be used as approval for receipts or approvals regarding important information in an agreement, document, or transaction instrument. The creation of signatures in electronic form must meet the legal validity and legal consequences of signatures in electronic form by using electronic certificates made by Electronic Certification Provider (PSrE) services that have been licensed by the Government of the Republic of Indonesia and made using certified electronic signature making devices.

Electronic Signatures provide their own benefits for users, including (i) authenticity (ensured) or authenticity of a message that serves to show where electronic data comes from, (ii) integrity or integrity of messages or documents communicated serves to ensure that messages, documents and electronic data sent do not experience any changes at all from parties who do not have rights or no authority whatsoever, (iii) Non-Repudiation which serves to ensure that the sender of the message or electronic document cannot deny the message or electronic document sent. The sender cannot also deny the content of the message or electronic document sent because it uses asymmetry involving the private key and public key, and (iv), namely Confidentiality or confidentiality of the message communicated which serves to ensure the confidentiality of a message or electronic document sent, because it can be possible that only certain people know it meaning that not just anyone can know what the contents of the message or Electronic documents that have been signed-in and entered in a digital envelope. The implementation of Electronic Signatures in Indonesia is not easy, because even though it has been clearly stated its validity and legal protection in the ITE Law, however, there are still many doubts from various parties due to the lack of socialization both from the government and organizing institutions regarding the application of electronic signatures. On the other hand, there are constraints regarding the imposition of fees that must be paid by users to Electronic Certification Providers (PSrE) to issue electronic certificates for the implementation of electronic signatures, therefore the author hopes that the Government can be present through the Electronic Certification Center of the State Cyber and Encryption Agency (BSSN) by providing services at a cost that is affordable to the public, so that the implementation and use of electronic signatures can be run massively in Indonesia.

REFERENCES

Ahmad Redi. (2010). *Electronic Signature Dalam Mewujudkan Secure Electronic Transaction di Sektor Perbankan Indonesia* (Tesis). Magister Universitas Indonesia, Jakarta.

Edmon Makarim. (2015). Keautentikan Dokumen Publik Elektronik Dalam Administrasi Pemerintahan Dan Pelayanan Publik. *Jurnal Hukum dan Pembangunan Tahun ke-45 No. 4*.

Edmon Makarim. (2020). *Notaris dan Transaksi Elektronik; Kajian Hukum Tentang Cyber Notary atau Electronic Notary* (4 ed.). Depok: Rajawali Pers.

Efa Laela Fakhriah. (2017). *Bukti Elektronik Dalam Sistem Pembuktian Perdata* (1 ed.). Bandung: Refika Aditama.

Farida Dewi. (2012). *Tanggung Jawab Hukum Penyelenggara Tanda Tangan Digital Tersertifikasi yang Berinduk (Analisis Komparatif Terhadap Kasus Diginotar di Belanda)* (Tesis). Magister Universitas Indonesia, Jakarta.

Hilman Hadikusuma. (2013). *Metode Pembuatan Kertas Kerja atau Skripsi Ilmu Hukum*. Bandung: Mandar Maju.

Izzah, A. N. El, & Sugandha, W. (2021). Penggunaan Tanda Tangan Elektronik Dalam Penyelenggaraan E-Government Guna Mewujudkan Pelayanan Publik Yang Efisien. *Journal of Law, Society, and Islamic Civilization*, *9*(1), 1. https://doi.org/10.20961/jolsic.v9i1.52836

Julius Indra Dwipayono Singara. (2004). Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia. *Jurnal Legalitas*.

Muchsin. (2006). *Ikhtisar Ilmu Hukum*. Jakarta: Badan Penerbit Iblam.

Pengantar ilmu hukum. (2008). *Pengantar Ilmu Hukum*. Jakarta: Kencana prenada media.

Rifkie Primartha. (2011). Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES). *Jurnal Sistem Informasi (JIS) , 3*.

Satjipto Rahardjo. (1991). *Ilmu Hukum*. Bandung: Alumni.

Soedjono Dirjosisworo. (1983). *Pengantar Ilmu Hukum*. Jakarta: Raja Grafindo Persada.

Soemarno Partodihardjo. (2008). *Tanya Jawab Sekitar Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*. Jakarta: PT. Gramedia.

Soemarno Partodihardjo. (2009). *Tanya Jawab Sekitar Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: PT. Gramedia Pustaka Utama.

Stephen Mason. (2003). *Electronic Signatures in Law* (Vol. 4). London: LexisNexis Butterworths.

Sudikno Mertokusumo. (2003). *Mengenal Hukum Suatu Pengantar*. Yogyakarta: Liberty.

Sugeng. (2017). *Hukum Telematika Indonesia* (Vol. 1). Jakarta: Prenadamedia Group.

Sulaiman, Nur Arifudin, & Lily Triyana. (2020). Kekuatan Hukum Digital Signature Sebagai Alat Bukti Yang Sah Di Tinjau Dari Hukum Acara Perdata. *Risalah Hukum , 16*(2), 95–105.

Titi S. Slamet, & Marianne Masako Paliling. (2019). Kekuatan Hukum Transaksi dan Tanda Tangan Elektronik Dalam Perjanjian. *Paulus Law Journal*, *1*.

United Nations. (2002). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*. New York: United Nations Publication.