International Journal of Latest Research in Humanities and Social Science (IJLRHSS)
Volume 06 - Issue 01, 2023
www.ijlrhss.com || PP. 01-07

Legal Position of Electronic Signatures in Indonesia

Sudarini, Kadek Wiwik Indrayanti, Supriyadi
Master of Law Study Program
Postgraduate Program at Merdeka University, Malang, Indonesia
Terusan Dieng Number 62-64 Malang 65146

Abstract: An electronic signature is a signature made electronically that functions the same as an ordinary signature on an ordinary paper document. A signature is data which, if not falsified, can function to justify the actions of the person whose name is printed on a document he is signing. This study uses a normative juridical research method with a statutory approach. The issues raised are regarding the legal power of electronic signatures in Indonesia and legal protection for users of certified electronic signatures. The results of this study are that electronic signatures have legal force if they have used an electronic system that has been regulated in the laws and regulations that apply in Indonesia, including Law Number 19 of 2016 concerning Amendments to Law No.11 of the year 2008 concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions. A valid electronic signature can be used as legal evidence if the integrity of the information in it can be guaranteed and can be accounted for, accessible, and can be displayed so that it can explain a situation. And legal protection for users of verified electronic signatures is a guarantee of privacy and/or protection in terms of personal data where this is also regulated in laws and regulations that regulate electronic transactions, then the parties carry out electronic transaction activities are also required to pay attention to the principle of prudence, have good faith, transparency, accountability, and fairness. The last resort that can be taken if a dispute occurs is through a lawsuit in court and through other alternative dispute resolution mechanisms.

Keywords: signature, electronics, user

1. Background

In the current era of digitalization, information technology in society is increasingly sophisticated and this fact shows that the field of information technology and telecommunications is always developing and has the impact of increasing the variety of available communication facilities. The existence of globalization in the field of communication which is increasingly supported by the existence of the internet makes this world increasingly without boundaries. The Indonesian people themselves are currently in an era of reform in all areas of life which are adapted to the development of information technology (Titi. S, 2020). Indonesian people currently own and use information technology products and telecommunication services.

Electronic transactions that are currently developing do not require face-to-face meetings, signatures, and without regional boundaries. Transactions that occur can occur between cities, between islands, and even between countries using information technology facilities. When this information is damaged, the risks that must be borne by those who send, need or just view it because of the use of public networks, everyone can find out the electronic information, or if one of the parties does not carry out the achievements of the electronic transaction, this can detrimental to related parties (Mainstay, A.M, 2019).

E-Business is an activity of doing business on the internet, which not only purchases, sales and services but also customer service and collaboration with business partners, while Chaffey defines "e-Business is the transformation of key business processes through processes the use of internet technologies" . Meanwhile, according to the definition of e-commerce, is the use of the internet, websites, mobile applications and browsers that run on a mobile platform to conduct business transactions (Mayana, 2021). According to Harisno & Pujadi e-commerce is defined as all forms of trade/trade transactions of electronic goods or services and activities related to consumers, manufactures, service providers and intermediaries using computer networks Technically e-commerce is part of e-business, because e- Business is all transactions that occur in online business including direct sales to consumers (e-commerce), transactions with manufacturers and suppliers. In essence, e-business is an activity in establishing relationships with consumers and exchanging data within one company by utilizing the Internet network (Izzah, 2021).

The most fundamental difference between the two is the transaction, e-commerce is more oriented towards transactions involving the exchange of money, while e-business is oriented towards more abstract long-term business interests, for example, trust and service to consumers, work regulations, relations between business partners and handling other cases as well as all aspects of doing business including product design and marketing, supplier management and others (Sihombing, L.B, 2020).

The information society or what is known as the information society is currently present and is believed to be an important part of world society in the third millennium, this is marked by the use of information technology sophistication which is increasingly widespread in various activities in human life, not only in developing countries. -developed countries but also including in Indonesia. This phenomenon in turn has positioned information as a very important and profitable economic commodity and therefore laws are needed to regulate such information. Information technology used in electronic commerce has a positive impact, namely transactions can be carried out quickly and more easily and transactions can be carried out globally without any barriers and limitations of place and time, which have now become commonplace. Face to face agreements (meeting in person) are no longer needed for business people but meet face to face through electronic media so that it can be said, this electronic trade is a new economic driver in the field of technology, especially in Indonesia (Athaya, A, 2021).

Related to this, the need for confidentiality of information and guarantees for the authenticity of information has also increased. Establishing a system for authentication of computer-based information requires knowledge and ability to manage the security of computer use. But there is a view that says that combining these two things is not an easy job. This general view assesses that concepts in the legal world often have little correlation with existing concepts in the world of computer security. The concept of a digital signature, for example, which is known in the world of computer security, is the result of applying computer techniques to information. Meanwhile, analog signatures generally have a broader meaning, namely a sign made with the intention of legalizing the document being signed (Bayu Ardwiansyah, 2017).

Until today, the laws and regulations in Indonesia determine that there is only one way to give legal force and legal consequences to an agreement, namely by having a manuscript signature. However, in trading practice in particular, manuscript signatures have increasingly been displaced by the use of electronic signatures attached to agreements. In other words, electronic agreements raise debate about the recognition, legal force and legal consequences of an electronic signature when there is a legal dispute between its users both at the national and international levels. Information technology security is then provided by law. In a sense, the law does not act as an obstacle to technological development, but rather as a counterweight to technological developments by providing security guarantees for its users (Titi S. Slamet, 2020).

In technological developments known as digital signatures (digital signature). The electronic signature here is not a written or real signature. The intended digital signature is the transformation (change in form) of the message using an asymmetric cryptography system, a system that makes a message sent by the sender safely delivered to the recipient using the private key and public key so that, thus, a message recipient has a public key. from the sender of the message can test whether the transformation is carried out using a private key that is paired with the public key, as well as testing whether the message has been changed since the transformation was carried out on the message (Ariadi, I. W, 2016).

A digital signature is a signature created electronically that functions the same as a regular signature on a plain paper document. A signature is data that, if not falsified, can function to justify the actions of the person whose name is printed on a document he signed (Rosani, 2020). Document security guarantees provided by digital signatures are actually better than ordinary signatures. Recipients of electronic messages affixed with digital signatures can check whether the message really came from the correct sender and whether the message has been changed after being signed either intentionally or unintentionally. In the case of electronic payment systems, other evidence can be used besides electronic data. or digital in the form of a digital signature to be classified.

The digital signature included in an agreement can be made within a certain period of time. The digital signature is created using the private key, which is the key pair of the public key contained in the document. Digital signatures that are used with full awareness of the signing must be free from elements of pressure and coercion. Electronic certificates are used to support electronic signatures. The signing must ensure the correctness and integrity of all information related to the electronic certificate.

Generally, a digital signature will be included in the document and also stored with the document as well. Digital signatures can also be sent or stored as separate documents, as long as they can be associated with the document. Because digital signatures are unique to the document, such separation of digital signatures is unnecessary. According to the law, the process of forming and verifying digital signatures fulfills the most important elements. First, Signer Authentication. If the public key and private key pair are associated with a defined legal owner, then the digital signature will be able to link/associate the document with the signer.

A digital signature cannot be forged unless the signer loses control of his private key. Second, digital signature document authentication also identifies the signed document with a much higher degree of certainty and accuracy than a paper signature. Third, the assertion of creating a digital signature requires the use of the private key of the signer. This action can confirm that the signatory agrees and is responsible for the contents of the document. Fourth, the efficiency of the process of establishing and verifying digital signatures provides a

high degree of certainty that the existing signature is a valid and genuine signature of the owner of the private key. From the background described above, the legal issues that will be analyzed in this study are regarding the legal power of electronic signatures in Indonesia and legal protection for users of certified electronic signatures.

2. Method

This research is a juridical-normative law research. Data collection techniques in this study used literature and document or archive studies, namely by collecting data related to the research needs to be studied, in addition to various books and other supporting legal materials (Bahder, 2008). The analysis technique used was descriptive qualitative data, with a statutory and comparative approach (Peter, 2006).

3. Results and Discussion

3.1 Analysis of the Legal Power of Electronic Signatures in Indonesia

The electronic signature in Article 1 number 12 of Law Number 19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Electronic Information and Transactions is a signature consisting of electronic information that is attached, associated with and related to other information where it is it includes electronic contracts that are used as verification or authentication tools. In Article 5 paragraph (1) of Law No. 19 of 2016 it is also stated that information and/or electronic documents in the form of electronic contracts or printouts are valid evidence.

Edmon Makarim provides an understanding of electronic contracts as agreements or legal relations that are carried out electronically by integrating networks of computer-based information systems with communication systems (computer-based information systems) based on telecommunication networks and services (telecommunication-based), which in turn facilitated by the existence of a global internet computer (network of network). Rosa Agustina gave her opinion that what is meant by an electronic contract is any agreement created by means of electronic devices or information technology and contained in electronic documents or other electronic media.

Article 1 point 17 of Law no. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) states that electronic contracts are agreements between parties made through an electronic system and therefore to be valid must also meet the requirements for an agreement that can be proven, while the system electronics as stated in Article 1 point 5 of Law 19 of 2016, namely a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information (Ardwiansyah, B, 2017).

Electronic signatures are also regulated in Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (hereinafter referred to as PP PSTE). In article 59 paragraph (3) PP PSTE it is stated regarding the requirements for electronic signatures so that they have legal force and legal consequences, namely among others;

a) Electronic Signature Creation data is related only to the Signer;
b) Electronic Signature Creation data during the electronic signing process is only in the power of the Signer;
c) all changes to the Electronic Signature that occur after the time of signing can be known;
d) all changes to the Electronic Information related to the Electronic Signature after the time of signing can be known;
e) there is a certain method used to identify who the signatory is; and
f) there are certain ways to show that the signatory has given consent to the related Electronic Information (Usman, T, 2020).

In Article 60 paragraph (1) PP PSTE it is stated that electronic signatures serve as a means of authentication and verification of the identity of the signer and the integrity and authenticity of electronic information. Basically, electronic signatures are different from digital signatures, electronic signatures are legal terms as stipulated in Indonesian laws and regulations, while digital signatures are terms used to describe electronic signature methods using asymmetric cryptographic methods with key infrastructure. public. This is as stated in Article 60 paragraph 2 (two) that electronic signatures include; certified electronic signature and non-certified electronic signature (Saepulrohman, A, 2021).

Electronic documents that have been digitally signed are electronic documents that are produced through certain processes including the encryption process, using a private key, from plain text that has gone through a hashing process. The private key that is uniquely generated each individual has a mathematically related key pair called the public key which is then attached to the electronic certificate along with the electronic document

that has been encrypted. The nature of the key pair is an encryption result that is generated from one of the keys, which is decrypted using the key pair. The private key can open the encryption generated using the public key and vice versa. By using the public key attached to the electronic certificate, the system can check whether the public key of the individual listed in the electronic certificate can open encryption using the private key (Arianti, N. K. S, 2020). If the encryption can be opened, then the public key and private key are related to each other so that it can be concluded that only the information and identity contained in the electronic certificate is valid.

The definition of an electronic certificate in Article 1 number 20 PP PSTE is an electronic certificate that contains an electronic signature and identity that shows the legal subject status of the parties in an Electronic Transaction issued by an electronic certification provider. While the definition of an electronic certification provider listed in Article 1 number 21 PP PSTE is a legal entity that functions as a trusted party, which provides and audits Electronic Certificates. The party issuing the key pair along with the electronic certificate is referred to as the Electronic Certification Operator (PSeE) or Certficate Authority (CA). This is stated in Article 60 paragraph 3 (three) letter b that the electronic certificate is made by an electronic certification operator in Indonesia who is registered because the legal consequences of using a certified electronic signature or not will affect the strength of the evidentiary value.

As stated in Article 13 paragraph (3) of the ITE Law, electronic certification operators consist of; Indonesian electronic certification administrators and foreign electronic certification administrators. Electronic certification operators must be able to provide accurate, clear and certain information to each service user which includes; the method used to identify the signer, things that can be used to find out the electronic signature maker's personal data; and what can be used to demonstrate the enforceability and security of electronic signatures.

In terms of storing data for making electronic signatures, the implementation of Electronic Certification is mandatory; ensure that the use of electronic signature creation data is only under the power of the signatory, using certified electronic signature creation devices in the process of storing electronic signature creation data; and ensure that the mechanism used for the use of electronic signature creation data for electronic signatures implements a combination of at least 2 (two) authentication factors.

In Article 64 PP PSTE it has been ensured that the authentication factors that can be selected to be combined, authentication factors can be distinguished into 3 (three) types as stipulated in the elucidation of Article 64 paragraph 2 PP PSTE, namely;

a) Something that is owned individually (what you have), for example an ATM card or smart card
b) Something that is known individually (what you know) for example a PIN/Password or cryptographic key
c) Something that is characteristic of an individual (what you are) for example voice patterns, handwriting dynamics or fingerprints.

Based on the description above, what is meant by a digital signature is a certified electronic signature, digital signatures can only be done using an electronic certificate issued by an electronic certification provider that is recognized by the Ministry of Communication and Informatics, not a signature made by yourself using an application. then paste it in the document on the computer. So the position of an electronic signature, even though it is only in the form of a code, has the same strength as a manual signature in general and has legal consequences as long as it fulfills the requirements stipulated in article 59 of PP PSTE.

In Article 5 paragraph 2 (two) of the ITE Law it is stated that Electronic Information and/or Electronic Documents and/or their printouts are an extension of valid evidence in accordance with the procedural law in force in Indonesia by using an electronic system in accordance with the provisions stipulated in the Law. – Invite. Electronic Information and/or Electronic Documents are valid legal evidence but this does not apply to letters which according to the law must be made in written form and letters along with documents which according to the law must be made in the form of a notarial deed or a deed drawn up by an official. deed maker.

The elucidation of this paragraph emphasizes that documents which according to the law must be made in writing include, but are not limited to securities, securities, and letters used in the process of enforcing civil, criminal and state administrative procedural law. Even though an uncertified electronic signature also has legal validity and must still comply with the ITE Law, it is better to use a certified electronic signature because it has the highest evidentiary strength because it has been recognized by the Government and the Government has also provided an electronic document checking application if something happens and can be directly verified.

However, Article 6 of the ITE Law also states that in the event that there are other provisions as mentioned above, it is implied that information must be in written or original form, electronic information and/or electronic documents are considered valid as long as the information contained therein can be accessed. displayed, its integrity guaranteed, and can be accounted for so that it explains a situation. The Ministry of Communication and Informatics in this case has the authority to act as a Root CA, which only has one in

Indonesia, the Ministry of Communication and Informatics provides electronic signature certificates to Electronic Certification Operators (PSrE) and performs supervision.

PSrE consists of two types, namely government and non-government. The government PSrE is BSSN and BPPT, while the non-government ones are Privy ID, Vida, PERURI, Solusi Net and DTB. These institutions will provide electronic certification to users. In the event that something undesirable happens, if using a certified electronic signature, in accordance with Article 58 PTSE, PSrE Indonesia is obliged to bear the loss caused by their intention or negligence. Indonesia, it becomes the responsibility of the person, business entity or agency that suffers losses.

3.2 Analysis of Legal Protection for Certified Electronic Signature Users.

Electronic system users are everyone, state administrators, business entities and the public who utilize goods and services, facilities or information provided by PSRE as stipulated in Article 1 number 11 PP PSTE. Everyone can use this electronic signature after fulfilling certain requirements. Where users of electronic signatures can also be called consumers who are entitled to legal protection regulated in Law Number 8 of 1999 concerning Consumer Protection (hereinafter referred to as UUPK).

In Article 1 point 2 of the ITE Law, it is stated that electronic transactions are legal actions carried out through computers, computer networks, and/or other electronic media. The agreement that exists in an electronic transaction carried out by business actors and consumers creates a contract or legal relationship between the parties (Disemadi, H. S., 2021). If the consumer agrees with the terms or conditions put forward by the business actor, an agreement is made even though the sale and purchase agreement is signed with an electronic signature. Electronic contracts also apply as conventional contracts in general, the formation of agreements also goes through the offer and acceptance stages. There are two types of communication means in the bargaining process distinguished from the duration required, namely instantaneous communication and non-instant communication. In the bidding process which is carried out by means of electronic communication such as telex, fax and e-mail, the time difference is not as sharp as in the case of acceptance by letter or telegram. An electronic contract is formed by a means of communication that moves very quickly, so it is not easy to determine the time it occurred at the time of acceptance. In relation to the time of acceptance, the Principles of International Commercial Contracts (PICC) stipulates that the offer must be accepted according to the time specified (in the offer) or if no definite time is specified, then the acceptance must be given within a reasonable time according to with the condition and speed of the means of communication used by the party offering.

The concept of Digital Signature, which is known in the world of computer security, is the result of applying computer techniques to information. Whereas in the general world, a signature has a broader meaning, namely a sign made with the intention of legalizing the document being signed. In the real world, signatures are used to guarantee the authenticity and legality of a document. This signature is a sign that is uniquely owned by a person and is used to validate that that person agrees and acknowledges the contents of the document being signed (Budianto, A., 2021).

One of the implementations of electronic signatures by Privv ID must comply with the provisions contained in the ITE Law and PP PSTE, which are required regarding the fulfillment of electronic document security aspects, namely Authentication, Integrity, and Non-Repudiation. The signing process begins with registration on the electronic signature organizer platform. In this process, the user enters data including name, email address, cellphone number, and uploads a photo of the National Identity Card (KTP). After that, the electronic signature user waits to receive a registration confirmation email and verifies the validity of the identity document. This process is carried out in order to ensure that all data used in registration and electronic signatures are in the control of only electronic signature users. After that the user of the electronic signature uploads the document to be signed, then during the signing process there is an electronic certificate which can show that any changes to the electronic signature that occur after the time of signing will be known to the user.

In the electronic signature process, there is information regarding the time when the electronic signature was embedded and the validity period. In addition to information regarding changes to electronic signatures, users can also find out if there are changes to electronic information related to the electronic signature after the time of signing. The electronic signature organizer platform will display information regarding the validity of the signer's identity, the time of signing, and the condition of the original document being signed.

Article 26 paragraph (1) PP PSTE stipulates that electronic system operators are required to maintain confidentiality, integrity, authenticity, accessibility, availability and traceability of electronic information and/or electronic documents in accordance with statutory provisions. Electronic system operators are obliged to protect their users and the general public from losses caused by the electronic systems they operate. Here it is clear that the rights of certification providers on digital signatures must be protected, especially in terms of personal data protection. Article 1 number 29 PP PSTE explains that personal data is any data about a person, either identified and/or identifiable separately or combined with other information, either directly or indirectly through electronic

and/or non-electronic systems. In Article 29 PP PSTE, electronic system operators are required to provide information to electronic system users at least regarding:

a) Electronic System Operator Identity
b) Transacted object
c) Eligibility or security of Electronic Systems
d) Procedure for using the device
e) Contract terms
f) Procedure for reaching an agreement
g) Guarantee of privacy and/or protection of Personal Data
h) Complaint center telephone number.

Article 45 paragraph (1) PP PSTE explains that electronic transactions carried out by parties give legal consequences to the parties and continued in paragraph (2) the implementation of electronic transactions must pay attention to good faith, prudential principles, transparency, accountability and fairness.

The article explains that users of certified electronic signatures can be protected by obtaining guarantees of privacy and/or protection of personal data. Subsequent parties in electronic transaction activities must pay attention to good faith, have the principles of prudence, transparency, accountability and fairness. Users and administrators of electronic certification must carry out their respective roles properly.

Business actors in electronic transaction activities are required to protect personal data. Personal data is also regulated in Article 26 paragraph (1) of the ITE Law which explains "Unless otherwise stipulated by Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. Every person whose rights are violated as referred to above can file a lawsuit for losses incurred based on statutory regulations."

The last legal step to get legal protection can be done by taking the dispute resolution route. Dispute resolution can be carried out by Digital Signature users if there is a violation or loss committed by the electronic certification operator. Article 38 paragraph (1) of the ITE Law explains that everyone can file a lawsuit against the party operating the Electronic System and/or using Information Technology which causes losses. Furthermore, paragraph (2) explains that the public can file a lawsuit on a representative basis against the party operating the electronic system and/or using information technology which results in harm to society, in accordance with the provisions of the Laws and Regulations.

In addition to settling civil lawsuits, the parties can resolve disputes through arbitration, or other alternative dispute resolution institutions in accordance with the provisions of the Laws and Regulations as stipulated in Article 39 paragraph (1) and paragraph (2) of the ITE Law. Likewise with related third parties (Intermediaries) who contribute so that technically a trade transaction (E-Commerce) can be carried out electronically. Collaboration between the related parties in an electronic system for trade transactions must be built from a spirit of cooperation that is mutually beneficial and jointly responsible and/or accountable proportionally to the users of the system according to their respective functions and roles.

4. Conclusion

Electronic signatures in order to have legal force if you have used an electronic system that has been regulated in the applicable laws and regulations in Indonesia, including Law Number 19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Information and Transactions Electronics and Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions. A valid electronic signature can be used as legal evidence if the integrity of the information in it can be guaranteed and can be accounted for, accessible, and can be displayed so that it can explain a situation.

Legal protection for users of verified electronic signatures is a guarantee of privacy and/or protection in terms of personal data where this is also regulated in laws and regulations governing electronic transactions, then the parties in carrying out electronic transaction activities are also prosecuted to observe the principle of prudence, have good faith, transparency, accountability, and fairness. The last resort that can be taken if a dispute occurs is through a lawsuit in court and through other alternative dispute resolution mechanisms.

Bibliography

[1]. Bahder Johan Nasution, 2008. Metode Penelitian Ilmu Hukum, Bandung: Mandar Maju
[2]. Peter Mahmud Marzuki, 2006. Penelitian Hukum, Jakarta: Kencana Prenada Media
[3]. Titi S. Slamet, Marianne Masako Paliling. (2020). Kekuatan Hukum Transaksi Dan Tanda Tangan Elektronik Dalam Perjanjian. Paulus Law Journal, 1(1), 9–18. https://doi.org/10.51342/plj.v1i1.43
[4]. Andalan, A. M. (2019). Kedudukan Tanda Tangan Elektronikdalam Transaksi Teknologi Finansial. Jurist-Diction, 2(6), 1931. https://doi.org/10.20473/jd.v2i6.15921

[5]. Mayana, R. F., & Santika, T. (2021). Legalitas Tanda Tangan Elektronik: Posibilitas Dan Tantangan Notary Digitalization Di Indonesia. Acta Diurnal JurnalIlmu Hukum Kenotariatan, 4(2), 244–262. Retrieved from http://jurnal.fh.unpad.ac.id/index.php/acta/article/view/517
[6]. Izzah, A. N. E., & 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
[7]. Sihombing, L. B. (2020). Keabsahan Tanda Tangan Elektronik Dalam AktaN otaris. Jurnal Education and Development, 8, (No. 1), Hal. 134.
[8]. Athaya, A. (2021). Efisiensi Tanda Tangan Elektronikdalam Pelayanan Adminduk Daring di Disdukcapil Kabupaten Wonogiri. Journal of Law, Society, and Islamic Civilization, 9(1), 10. https://doi.org/10.20961/jolsic.v9i1.50885
[9]. Bayu Ardwiansyah. (2017). Keabsahan Penggunaan Tanda Tangan Elektronik Sebagai Alat Bukti Menurut Undang –Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Lex Privatum, V(7), 6–18.
[10]. Titi S. Slamet , Marianne Masako Paliling. (2020). Kekuatan Hukum Transaksi Dan Tanda Tangan Elektronik Dalam Perjanjian. Paulus Law Journal, 1(1), 9–18. https://doi.org/10.51342/plj.v1i1.43
[11]. Ariadi, I. W. (2016). Bentuk-Bentuk Digital Signature Yang Sah Dalam Transaksi Elektronik Di Indonesia. Jurnal Magister Hukum Udayana (Udayana Master Law Journal), 5(1), 175. https://doi.org/10.24843/jmhu.2016.v05.i01.p16
[12]. Rosani Zulkarnaen, N. J. (2020). Tinjauan Kekuatan Pembuktian Digital Signature Dalam Sengketa Perdata Ditinjau Dari Uu No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Jurnal Ilmiah METADATA, 1(3), 168–189. https://doi.org/10.47652/metadata.v1i3.12
[13]. Ardwiansyah, B. (2017). Keabsahan Penggunaan Tanda Tangan Elektronik Sebagai Alat Bukti Menurut Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Lex Privatum, 5(7), 84–90.
[14]. Usman, T. (2020). Keabsahan Tanda Tangan Elektronik Pada Perjanjian Jual Beli Barang Dari Perspektif Hukum Perdata. Indonesia Private Law Review, 1(2), 87–98. https://doi.org/10.25041/iplr.v1i2.2058
[15]. Saepulrohman, A., & Negara, T. P. (2021). Implementasi Algoritma Tanda Tangan Digital Berbasis Kriptografi Kurva Eliptik Diffie-Hellman. Komputasi: Jurnal IlmiahIlmu Komputer Dan Matematika, 18(1), 22–28. https://doi.org/10.33751/komputasi.v18i1.2569
[16]. Arianti, N. K. S., Budiartha, I. N. P., & Arini, D. G. D. (2020). Tanda Tangan Elektronikdalam Akta Pernyataan Keputusan Rapat Umum Pemegang Saham Perseroan Terbatas. Jurnal InterpretasiH ukum, 1(1), 148–153. https://doi.org/10.22225/juinhum.1.1.2202.148-153
[17]. Disemadi, H. S., & Prasetyo, D. (2021). Tanda Tangan Elektronikpada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia. Wajah Hukum, 5(1), 13. https://doi.org/10.33087/wjh.v5i1.300
[18]. Budianto, A., Pangesti, S., Pasaribu, D., & Faustina, S. (2021). Barcoding Digital Signature Authencity Sebagai Alat Bukti Perkara Pidana. Refleksi Hukum: Jurnal Ilmu Hukum, 5(2), 255–274. https://doi.org/10.24246/jrh.2021.v5.i2.p255-274