Eduvest – Journal of Universal Studies
Volume 4, Number 3, March, 2024
p- ISSN 2775-3735- e-ISSN 2775-3727

THE VALIDITY OF ELECTRONIC SIGNATURES IN ELECTRONIC TRANSACTIONS FROM THE PERSPECTIVE OF REGULATION NUMBER 71 OF 2019

Rudolf Hitler Satriawan Sitorus[1], George Frans Wanma[2]
[1,2,] STIE Mah-Eisa Manokwari, Indonesia
Email: rudolfsitorus1987@gmail.com,
georgefranswanma@stihcaritaspapua.ac.id

ABSTRACT

The development of information and communication technology (ICT) has driven the rapid growth of electronic transactions. The use of electronic signatures (TTE) is also a practical solution in electronic transactions. This research aims to determine the validity of TTE in electronic transactions based on PP No. 71 of 2019. This research uses normative legal research methods with a juridical-normative approach. Research data was obtained from literature studies of statutory regulations, books, scientific journals and other secondary legal sources. Data were analyzed qualitatively using interpretation and description methods. The research results show that based on Government Regulation (PP) no. 71 of 2019 concerning Implementation of Electronic Systems and Transactions, electronic signatures are recognized as a valid form of signature in electronic transactions. Electronic Signatures used in Electronic Transactions can be generated through various signing procedures. Electronic Signatures have legal force and legal consequences as long as they meet the requirements. So it can be concluded that electronic signatures have validity and legal force that is recognized in electronic transactions.

KEYWORDS *Validity, Electronic Signature, Electronic Transaction*

INTRODUCTION

The development of information and communication technology (ICT) has been a major driver in the rapid growth of electronic transactions. Innovations and advancements in technologies such as the internet, mobile devices, and digital payment systems enable people to conduct electronic transactions more easily, quickly, and efficiently (Saputra et al., 2023). Features like e-commerce, mobile banking, e-

How to cite: Rudolf Hitler Satriawan Sitorus, George Frans Wanma. (2024). The Validity of Electronic Signatures in Electronic Transactions from The Perspective of Regulation Number 71 of 2019. *Journal Eduvest*. 4,(3), 871-879
E-ISSN: 2775-3727
Published by: https://greenpublisher.id/

wallets, and payment gateways have facilitated online transactions between individuals, companies, and financial institutions without the need for physical presence. However, despite the enormous potential to realize fully digital services, there are still significant barriers hindering the complete transition to a digital environment, notably the difficulty in abandoning the use of physical documents.

In electronic transactions, payments are made digitally, yet this payment system still relies on physical documents to link online merchants with banks (Raharjo, 2021). Dependency on such physical documents constitutes a major obstacle in the transformation process towards fully digital financial services. One solution to address this is through the use of electronic signatures (ES). In the current digital era, digital documents are signed using ES that have been certified. Certified Electronic Signatures are digital verification and authentication methods using Electronic Certificates issued by Electronic Certificate Providers (PSrE) in Indonesia, officially recognized by the Ministry of Communication and Informatics (Diskominfo, 2022). However, amidst the increasingly widespread adoption of electronic transactions, questions regarding the validity of electronic signatures in a legal context have become a significant concern.

Policies regarding the provision of electronic systems and transactions have been regulated in Government Regulation Number 82 of 2012 which was later revoked considering the rapid development of information technology to promote digital economic growth and the enforcement of state sovereignty over electronic information in the territory of the Unitary State of the Republic of Indonesia, necessitating comprehensive regulation on the utilization of information technology and electronic transactions and Government Regulation Number 82 of 2012 concerning the Provision of Electronic Systems and Transactions is no longer in line with the development of legal needs in society, thus requiring replacement. Therefore, it was replaced with Law Number 71 of 2019 Concerning the Provision of Electronic Systems and Transactions.

Previous research by (Rozaqoh, 2022) examined the legality of digital signatures in e-commerce transactions according to positive law and Islamic law, the results showed that in positive law, the legality of digital signatures in e-commerce transactions is valid according to the law as stipulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 Electronic Transactions (ITE) and Government Regulation Number 71 of 2019 concerning the Provision of Electronic Systems and Transactions (PSTE). Meanwhile, in Islamic law, the legality of digital signatures in e-commerce transactions is valid if the contract used is clear with mutual consent and accountable, considering Islamic principles and benefits.

Another study by (Pasiwi, 2021) examined the validity of electronic signatures in electronic policies and their probative value from the perspective of evidentiary law, the results showed that electronic signatures on electronic policies are legally valid as long as they have been verified by a certificate authority and can be used as evidence in the proof process if there are issues in court. As a form of agreement, e-policies are regulated in the Commercial Code. However, it can be clearly seen that based on Article 255 of the Commercial Code, insurance must be done in writing with a deed, called a policy. Thus, e-policies can be interpreted as not meeting the requirements of a valid agreement, specifically the fourth requirement which

is a valid cause, because e-policies contradict the Commercial Code equivalent to the Law. Therefore, such insurance agreements can be interpreted as not meeting the objective requirements of an agreement that could render the agreement legally void.

The novelty of this research lies in its object of study, which is based on the perspective of Government Regulation No. 71 of 2019. The theoretical implications of this research are that understanding the concept of electronic signature validity in the context of law and information technology becomes more important. This research can also contribute to the development of legal theories concerning the recognition and validity of electronic documents in business and legal transactions. This research aims to determine the validity of ES in electronic transactions based on Government Regulation No. 71 of 2019.

RESEARCH METHOD

This research employs a normative legal research method with a juridical-normative approach. The normative legal research method is a scientific research procedure to discover truths based on scholarly logic from its normative side. The normative side in this research extends beyond just legal regulations but encompasses broader aspects, including the internal aspects of positive law such as the scope of legal conception, legal principles, and legal norms (Efendi et al., 2016). After the data is collected, qualitative analysis is conducted using interpretative and descriptive methods. This analytical process involves thorough reading and understanding of the collected data, followed by interpretation of the meanings and contexts of the information contained within the data. The results of this analysis are then elaborated in detail and organized into a logical and structured narrative form, thereby providing a better understanding of the researched topic.

RESULT AND DISCUSSION

The development of technology towards digitalization continues to experience rapid growth. In this era, human lifestyle has undergone an inseparable transformation due to the use of various electronic devices (Nikijuluw et al., 2020). The digital era brings positive impacts with significant changes in various aspects of life. One positive change that can be utilized well by society is the advancement in organizing electronic systems and transactions. Regulations related to the provision of electronic systems and transactions are governed by Government Regulation Number 71 of 2019 concerning the Provision of Electronic Systems and Transactions (hereinafter referred to as PP PSTE), which is a revision of the previous regulation, namely Government Regulation Number 82 of 2012 concerning the Provision of Electronic Systems and Transactions.

The transformation in society begins with the shift from conventional paper-based transactions to the adoption of electronic systems. Society believes that the role of information is crucial in contributing to economic, social, and cultural development. People now have the ability to share information about various things, including product or service sales information through information systems, which can attract buyers to choose certain products or services offered (Tandian &

Ramadhani, 2022). According to PP PSTE, an electronic system refers to a series of electronic devices and procedures aimed at preparing, collecting, processing, analyzing, storing, displaying, announcing, transmitting, and/or disseminating Electronic Information. The presence of such electronic systems is expected to facilitate transaction processes and contract-making.

Articles within PP PSTE state that electronic transactions change the order of society's life, so it cannot be avoided that legal actions such as contracts or agreements will shift to electronic forms, including the use of electronic signatures as a form of personal identification. According to the definition in the Indonesian Dictionary, a signature is a name written in a distinctive manner by one's own hand. Another definition states that a signature is a means of identity for verifying and legalizing information (Arifin & Naf'an, 2017). Meanwhile, according to (Slamet & Paliling, 2019), generally, a signature is interpreted as a writing used to authenticate or declare something according to the individual's wishes, with a composition of letters and curves resembling a script.

In fact, a signature has two basic legal functions, firstly as an identity mark of the signatory, and secondly as a sign of the signatory's consent to the obligations stated in the deed. Referring to these two legal functions, a definition can be given that a signature is an identity that serves as a sign of agreement to the obligations imposed on us (Slamet & Paliling, 2019). Signatures have important characteristics as described by (Jilan, 2023), including:

1. Signature is authentic evidence. Signature is considered as valid and reliable evidence related to a person's personal identity.
2. Signature cannot be forgotten. Signature is a unique mark that is difficult to forget or be replaced by others.
3. Signature cannot be transferred for reuse. Signature is unique to each individual and cannot be transferred for other purposes or reused without permission.
4. Signed documents are valid and cannot be altered. The signature on documents indicates the authenticity and genuineness of the documents. Signed documents are considered valid and cannot be altered without valid consent.
5. Signature cannot be repudiated. The owner of the signature cannot deny or reject that the signature belongs to them. This confirms the responsibility and authenticity of the signature made.

The important characteristics of manual signatures are not different from electronic signatures. An electronic signature, also known as a digital signature, is an electronic version that serves a similar function to a manual signature. Electronic signatures serve as evidence of the identification of the parties involved, fulfill formal requirements, and serve as a sign of agreement in an electronic transaction, optimizing the intentions of the parties in agreements that occur through electronic platforms (Mayasari, 2022). The PP PSTE provides a definition of an electronic signature as a signature consisting of Embedded Electronic Information, associated with, or related to other Electronic Information, and used as a means of verification and authentication.

Verification and authentication processes are necessary steps to prove that a document has been validated. A validated document indicates that it has been checked, read, scrutinized, and approved by the signatories. Therefore, the signatory bears responsibility for the document and is prepared to be held accountable when their responsibility is requested. Validation marks, commonly known as signatures, are indicators that the document has undergone appropriate validation processes (Pamungkas, 2023).

Electronic signatures replace traditional signatures on physical documents by utilizing digital technology. In the PP PSTE, devices for creating electronic signatures are described as software or hardware configured and used to create electronic signatures. According to (Hudzaifah, 2015), the operation of an electronic signature involves cryptographic techniques and public key cryptography, which utilizes two keys. The first key is used to create the electronic signature, while the second key is used to verify the electronic signature or return the message to its original form. This approach is known as an asymmetric cryptosystem. The use of electronic signatures requires two processes, from the signatory and from the recipient. These processes can be explained in detail as follows:

1. The formation of an electronic signature using a hash value generated from the document and a private key. To ensure the security of the hash value, it should be highly unlikely for the same electronic signature to be produced from two different documents and private keys.
2. Verification of the electronic signature is the process of checking the signature by referencing the original document and the provided public key, thereby determining whether the electronic signature was created for the same document using the private key corresponding to the public key.

Therefore, there is a significant difference between electronic signatures and ordinary signatures lies in their respective functions. Ordinary signatures serve as authentication for the contents of signed documents, while electronic signatures have the ability to ensure the authenticity of the electronic signature maker by using the concept of message integrity. Only the party with access rights, in this case, the message sender, can access the electronic signature (Kusuma et al., 2021).

An electronic signature is not a digital image of a handwritten or typed signature. Instead, it involves cryptographic hash functions that create an electronic signature requiring identity proof, ensuring the electronic signature cannot be forged or used by parties other than the signature owner (Yuniati & Sidiq, 2020). Despite the differences, the purpose of using electronic signatures remains the same as handwritten signatures. Electronic signatures can be used for similar purposes, such as acknowledging receipt of letters, giving consent, or for important information security purposes.

According to (Dermawan, 2021), although the use of electronic signatures is growing, there are still challenges in its implementation. Misconceptions exist in society about the understanding of electronic signatures, with the misconception that electronic signatures are scanned images of handwritten signatures. Additionally, security issues regarding electronic signatures are also a concern, especially regarding the risk of personal data theft. This concern arises because the signing process involves third parties or electronic system providers, which can be

exploited by irresponsible parties. Furthermore, there is still doubt or uncertainty about whether electronic signatures can be considered valid in the eyes of the law.

The PP PSTE is a legal regulation that governs the legality of electronic signatures and serves as the legal basis in Indonesia. Through this regulation, signatures are recognized as authentication and verification tools in electronic transactions. Additionally, electronic signatures are allowed to indicate the signatory's approval of electronically signed documents. This means that electronic signatures have legal force and consequences equivalent to wet or physical signatures (Dahlia & Susetio, 2023). Article 59 of the PP PSTE paragraph (1) states that electronic signatures used in electronic transactions can be produced through various signature procedures. Furthermore, paragraph (3) explains that electronic signatures will be legally valid and have legal consequences if they meet the specified requirements. These requirements include:

1. Data related to the creation of electronic signatures is only related to the signatory.
2. Data related to the creation of electronic signatures during the electronic signature process is only under the control of the signatory.
3. Any changes to the electronic signature occurring after the signing time can be known.
4. Any changes to electronic information related to the electronic signature after the signing time can be known.
5. There are specific methods used to identify the signatory.
6. There are specific methods to show that the signatory has given consent to the related electronic information.

This means that if an electronic signature meets all the requirements specified in the PP PSTE Article 59 provisions, then the signature is considered legally valid and will have legal consequences. Furthermore, Article 60 paragraph (2) of the PP PSTE categorizes electronic signatures into two types: certified electronic signatures and uncertified electronic signatures. A certified electronic signature is a signature that has been enhanced with an electronic certificate, while an uncertified electronic signature does not have this enhancement. If an electronic signature is uncertified, its security aspect is vulnerable and easily forged. In contrast, a certified electronic signature has been reinforced with an electronic certificate, so any changes or modifications can easily be detected by the system (Dermawan, 2021).

Article 62, paragraph (5) explains that an electronic signature on electronic information must be made using at least electronic signature creation data and include the signing time. This means that the two minimum requirements for an electronic signature on electronic information are, first, using electronic signature creation data. This electronic signature creation data can include unique information related to the identity or authority of the electronic signature maker. Second, the electronic signature must include the signing time, which is information about when the electronic signature was created. Fulfilling these requirements aims to make electronic signatures more secure, trustworthy, and easily identifiable. It also provides a stronger basis for the validity of signatures in electronic transactions.

An electronic signature is an approval given by a valid signature holder to an electronic document, and if there is misuse by another party, the burden of proving

the misuse of the electronic signature is placed on the electronic system provider, as stated in Article 52 of the PP PSTE (Fitri & Karo, 2020). Therefore, electronic signatures are recognized to have secure benefits in protecting users of electronic signature services. Furthermore, the advantages of electronic signatures over manual signatures lie in their ability to maintain the authenticity of documents. Documents signed electronically tend to be more secure from the risk of invalidity due to changes in handwriting or signature metadata. This security includes protection against modifications that unauthorized parties may make to the document. Consequently, this can facilitate the proof process compared to manual signatures, which require detailed examination in forensic laboratories to prove their authenticity (Saraswati et al., 2023).

According to (Lapian, 2024), there are reasons why the implementation of electronic signatures is starting, as follows: First, time-saving, where documents are signed and sent from anywhere. Second, cost-saving, where it can eliminate budget allocation for administrative purposes such as purchasing stationery, expedition costs, and document storage costs. As long as someone has a smartphone or computer connected to the internet, document signing and sending can be done anywhere without additional costs. Third, environmentally friendly, reducing paper and fuel usage in daily life by eliminating the printing and courier delivery processes.

Research results show that electronic signatures have legal validity and will have legal consequences if they meet all the requirements stated in Government Regulation (PP) Number 71 of 2019 concerning the Organization of Electronic Systems and Transactions Article 59. Electronic signatures are recognized to bring security benefits to users of their services, as well as being efficient and time-saving. The existence of electronic signature technology provides the possibility to reduce paper usage because the entire process can be done digitally, from signing to sending. The printing and delivery processes can be eliminated, reducing fuel and paper usage in daily activities. Thus, electronic signatures not only provide efficiency in electronic transactions but also make a positive contribution to environmental preservation.

CONCLUSION

Government Regulation (PP) Number 71 of 2019 concerning the Organization of Electronic Systems and Transactions asserts that electronic signatures are recognized as a valid form of signature in the context of electronic transactions. Electronic signatures used in electronic transactions can be generated through various signing procedures. It is important to note that electronic signatures will have legal validity and consequences if they meet the established requirements. Therefore, it can be concluded that electronic signatures have legitimacy and legal authority recognized in the context of electronic transactions.

REFERENCES

Arifin, J., & Naf'an, M. Z. (2017). Verifikasi Tanda Tangan Asli Atau Palsu Berdasarkan Sifat Keacakan (Entropi). *Jurnal Infotel*, *9*(1), 130–135.

Dahlia, M., & Susetio, W. (2023). Tinjauan Yuridis Penggunaan Tanda Tangan Digital Dalam Perjanjian Jual Beli. *Jurnal Multidisiplin Indonesia*, *2*(8), 2277–2289.

Dermawan, R. (2021). Pemanfaatan Tanda Tangan Digital Tersertifikasi Di Era Pandemi. *Jurnal Hukum Lex Generalis*, *2*(8), 762–781.

Efendi, J., Ibrahim, J., & Rijadi, P. (2016). *Metode Penelitian Hukum: Normatif Dan Empiris*.

Fitri, A., & Karo, R. P. P. K. (2020). Kebijakan Tanda Tangan Elektronik Di Indonesia: Tantangan Dan Manfaat Perspektif Keadilan Bermartabat Di Masa Pandemi Covid-19. *Prosiding Seminar Hukum Dan Publikasi Nasional (Serumpun)*, *1*(2), 75–91.

Hudzaifah, H. (2015). Keabsahan Tanda Tangan Elektronik Dalam Pembuktian Hukum Acara Perdata Indonesia. *Katalogis*, *3*(5).

Jilan, A. (2023). *Pelaksanaan Penggunaan Tanda Tangan Elektronik Di Era Pandemi Covid-19 Dalam Penyelenggaraan Sistem Dan Transaksi Elektronik*.

Kusuma, M. W., Dantes, K. F., & Sudiatmaka, K. (2021). Tinjauanyuridiskekuatanhukumterhadappenggunaantandatangan Elektronik Dalam Perjanjian Fidusia Berdasarkan Undang-Undangnomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11tahun2008 Tentanginformasi Dantransaksielektronik. *Jurnal Komunitas Yustisia*, *4*(2), 481–492.

Lapian, R. (2024). Pengaturan Penggunaan Tanda Tangan Elektronik Menurut Uu No. 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Lex Privatum*, *13*(1).

Mayasari, Y. (2022). Kedudukan Hukum Tanda Tangan Elektronik. *Jurnal Teknologi Dan Informasi*, *4*(1), 13–23.

Nikijuluw, G. M. E., Rorong, A. J., & Londa, V. (2020). Perilaku Masyarakat Di Era Digital (Studi Di Desa Watutumou Iii Kecamata Kalawat Kabupaten Minahasa Utara). *Jurnal Administrasi Publik*, *6*(92).

Pamungkas, P. D. A. (2023). Mengenal Tanda Tangan Elektronik Sebagai Bukti Validasi Dokumen Di Era Internet Of Things (Iot). *Tarfomedia*, *4*(1), 30–39.

Pasiwi, D. A. G. (2021). Keabsahan Tanda Tangan Elektronik Dalam Polis Elektronik Serta Kekuatan Pembuktianya Dalam Perspektif Hukum Pembuktian. *Juris And Society: Jurnal Ilmiah Sosial Dan Humaniora*, *1*(1), 131–142.

Raharjo, B. (2021). Fintech Teknologi Finansial Perbankan Digital. *Penerbit Yayasan Prima Agus Teknik*, 1–299.

Rozaqoh, A. (2022). *Legalitas Tanda Tangan Digital Dalam Transaksi E-Commerce Menurut Hukum Positif Dan Hukum Islam*. Iain Kediri.

Saputra, A. M. A., Kharisma, L. P. I., Rizal, A. A., Burhan, M. I., & Purnawati, N. W. (2023). *Teknologi Informasi: Peranan Ti Dalam Berbagai Bidang*. Pt. Sonpedia Publishing Indonesia.

Saraswati, A. I., Syabana, A. E., Siringoringo, G. R. M., & Farenia, N. M. (2023). Keberlakuan Tanda Tangan Elektronik Pada Dokumen Negara. *Unes Law Review*, *6*(1), 2066–2075.

Slamet, T. S., & Paliling, M. M. (2019). Kekuatan Hukum Transaksi Dan Tanda Tangan Elektronik Dalam Perjanjian. *Paulus Law Journal*, *1*(1).

Yuniati, T., & Sidiq, M. F. (2020). Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital Sebagai Alternatif Pengesahan Dokumen Di Masa Pandemi. *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 1058–1069.