E-ISSN: 2622-7045 I P-ISSN: 2654-3605
UNES LAW REVIEW
https://review-unes.com uneslawreview@gmail.com +62 856-5804-3983
DOI: https://doi.org/10.31933/unesrev.v6i4
Received: 25 June 2024, **Revised:** 13 July 2024, **Publish:** 17 Juliy 2024

Validity of Digital Signature Evidence as Valid Evidence in Civil Procedure Law

Neilpon Yulinar Marquez[1], Hono Sejati[2], Mohamad Tohari[3]
[1] Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: yulinarmarquezneilpon@gmail.com
[2] Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: sejatihono@gmail.com
[3] Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: mohamadtohari.undaris@gmail.com

Corresponding Author: yulinarmarquezneilpon@gmail.com

Abstract: Indonesia is entering a globalization era that drives technological advancements and business activities towards greater efficiency, particularly in the form of e-commerce. The use of Digital Signatures in its development is starting to shift the dominance of conventional signatures in agreements typically made on paper. Based on civil procedural law systems, judges are bound by valid evidence, implying that judicial decisions are limited by the evidence regulated by the law (HIR/RGB). This study adopts a doctrinal approach, examining law based on legislative regulations and legal concepts, and utilizing various data sources such as primary, secondary, and tertiary legal documents. Data collection methods include legal literature, legislative regulations, scientific literature, and relevant internet information on the discussed topic. The research findings indicate that a digital signature is not a replica of a conventional signature scanned using a scanner, but rather utilizes cryptographic techniques. The principle of lex specialis derogat legi generali states that the use of digital signatures in Civil Procedural Law holds a legal equivalence to authentic deeds.

Keyword: Signature; Digital; Evidence.

INTRODUCTION

The influence of information technology has changed the landscape of people's lives in all aspects, such as economic, social, and cultural. The most obvious change is the transformation of the economy from a conventional and manual one to a digital system using electronic devices. The current era of globalization is characterized by extraordinary speed in all things, pushing humans into the era of free markets and free competition.[1] The influence of the internet on a global scale has created a major revolution in this world. The internet has changed the global economic landscape in a more digital direction, a phenomenon known as the digital economy. It is reflected in the increasing economic activity that uses the internet as a medium for communication, collaboration, and cooperation. The application of electronic

systems in business is now common because it provides convenience, speed, and efficiency. However, E-commerce has become more complex because it is no longer limited by national borders, so it can be accessed anywhere and at any time. In this context, losses can arise, both for parties involved in the transaction and other parties who are not directly involved. Such losses often trigger conflicts that are ultimately resolved through legal proceedings, to obtain a final and binding court decision.

In civil proceedings in court, evidence is the key to assisting the judge in assessing the truth of the events presented to him. Proof aims to convince the judge about the truth of the arguments or evidence presented in a legal dispute, showing that this evidentiary process is important in the context of a dispute before a judge or court. Evidence in civil proceedings, as regulated in Article 1866 of the Civil Code, includes Written evidence, witnesses, allegations, confessions, and oaths.[2] As digital technology advances rapidly, once effective evidence may no longer be relevant ten years ago. There are visible problems with written evidence, where distribution only consists of two forms, namely deeds, and non-deeds, both of which must be conventional. However, with today's increasingly sophisticated technological advances, letters or deeds no longer have to be in conventional form, but can be in electronic form. Indonesia is experiencing an era of globalization which is encouraging the development of technology and business activities towards higher efficiency, especially in e-commerce. In its development, the use of digital signatures has begun to replace conventional signatures which are usually used in paper agreements. The usage of digital signatures in electronic commerce aims to maintain the integrity and authenticity of data in electronic documents.

Law Number 11 of 2008 concerning Electronic Information and Transactions has regulated e-commerce activities or electronic transactions in Indonesia, which was later updated with Law Number 19 of 2016 concerning Electronic Information and Transactions. This regulation aims to protect the position of producers and consumers in online transactions, ensure security, and build trust between the two. This trust is built by giving legal recognition to written or electronic documents, as well as recognizing their validity and strength in the eyes of the law.[3] Article 1 number 12 in Law Number 19 of 2016 concerning Information and Electronic Transactions explains the validity of a Digital Signature, calling it an "Electronic Signature" which is a series of Electronic Information related to other electronic information, used as a verification and authentication tool. In addition, article 5 paragraphs (1) and (2) recognize electronic evidence as valid legal evidence and expand the scope of valid evidence by the procedural law in force in Indonesia. Article 5 paragraph (3) expressly states that Electronic Information and/or Electronic Documents are considered valid if the Electronic System is used by the provisions of this law. The concept of electronic signatures appears in electronic documents which are non-paperless. However, this is in line with legal principles which state that documents must be accessible, sent, and stored in paper form.[4]

There are still weaknesses in the court process in Indonesia regarding the use of electronic media as evidence in trading. According to the applicable procedural law system (HIR/RGB) in civil trials, judges are limited to valid evidence as determined by law. It means that judges can only make decisions based on evidence recognized by law.[5] Therefore, in this research, two questions will arise: 1) How can Digital Signature settings be used as a tool for valid evidence in Civil Procedure Law? 2) What is the legal strength of digital signatures as valid evidence in Civil Procedure Law?

METHOD

The author uses a doctrinal approach, namely legal research that is composed of research in the form of discovering the principles and basic philosophy (dogma or doctrine) of positive law, efforts to inventory positive law, as well as finding laws in concert that are

appropriate to be applied to resolve a particular legal case.[6] In this context, the doctrinal approach refers to analysis based on statutory provisions (black letter law) and legal concepts. In this approach, the author will carefully examine the applicable laws and relevant legal theories and their relevance to the problems discussed in this research. Data collected during research, which aims to answer legal questions, will be supported by literature references regarding legal theories that are relevant and relevant to this research. The research also requires tertiary legal sources, such as legal encyclopedias and legal dictionaries, including the legal dictionary Black's Law Dictionary.

RESULT AND DISCUSSION

Digital Signature Settings as Evidence

There is a distinction between electronic signatures and traditional signatures that are often written on paper or scanned with a scanner. Electronic signatures are acquired via a process that involves creating a message digest or hash, which is essentially a mathematical summary of the document sent digitally.[7] It's worth noting that electronic signatures and digital signatures are not the same thing. In Indonesian law, electronic signatures are defined as specific terms, whereas digital signatures are electronic signing methods that utilize asymmetric cryptographic techniques with public key infrastructure.[8] Electronic signatures are designed to guarantee message integrity, thereby certifying that the sender is a legitimate individual who takes responsibility for it. It differs from the traditional signature function, which is intended to provide approval for the contents of a message or document. Electronic signatures are data that are associated with digital message encryption, which is designed to ensure data authenticity and protect it from modification.[7]

The purpose of adding a signature to a document is to verify its authenticity. However, a Digital Signature functions differently from a traditional signature. It employs a distinct method to mark a document or data, which ensures that the sender is identified and the document's integrity remains unchanged during transmission. The Digital Signature relies on the message's content, requires a secret key, and utilizes cryptographic techniques. According to Article 11 paragraph (1) of Law Number 11 of 2008, in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions, an Electronic Signature is considered valid only if it meets certain conditions.

a. Electronic Signature creation data relates only to the Signer;
b. Electronic Signature creation data during the electronic signing process is only under the control of the Signer;
c. Any changes to the Electronic Signature after signing can be detected;
d. Any changes to the Electronic Information related to the Electronic Signature after signing can be detected;
e. There are methods used to identify Signatories;
f. There are methods used to demonstrate that the Signer has consented to the relevant Electronic Information.

The benefit of a Digital Signature is that a digital signature will secure electronic data sent over an open network, resulting in the following benefits: [5]

1. Authenticity;
2. Integrity;
3. Non-Repudiation;
4. Confidentiality.

Each Digital Signature has unique characteristics for each signed document, as it is generated from the document itself, and even small changes to the document will result in a different digital signature.[9] In the civil procedural law system, electronic signatures are not yet regulated as evidence, because Article 1866 of the Civil Code only recognizes five types

of evidence, namely written evidence, witness evidence, presumptive evidence, confessions, and oaths. However, with rapid technological advances in Indonesia, people's behavior in making agreements has changed from using conventional signatures to electronic signatures. Recognition of electronic signatures in Indonesia is made through two regulations, namely Law Number 11 of 2008 concerning Electronic Information and Transactions, which was later updated with Law Number 19 of 2016 concerning Electronic Information and Transactions, and Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions. Certified electronic signatures must meet certain requirements, including going through a system test process for issuing electronic certificates. Meanwhile, electronic signatures that are not certified are created without going through the services of an electronic certification provider. The implications of these two types of electronic signatures are related to the technical standards applied.[10]

Laws Number 11 of 2008 and Number 19 of 2016 in Indonesia govern the use of digital signatures. These laws define a digital signature as an "electronic signature," which means a signature consisting of electronic information that verifies and authenticates other electronic information. The laws also establish rules for using electronic evidence in legal proceedings. Article 5, paragraph (1) states that electronic information, electronic documents, and printouts are valid legal evidence. Article 5, paragraph (2) specifies that electronic information, electronic documents, and printed results are valid evidence extensions according to the procedural law in Indonesia. Additionally, article 5, paragraph (3) explicitly states that electronic information and/or electronic documents are considered valid only if the electronic system used complies with the provisions outlined in these laws.

The definition of an electronic signature containing information indicates that the creation of the signature involves unique data that refers specifically to the signer and can identify the signer, by the provisions in Article 61 (3) of Government Regulation Number 71 of 2019 concerning Electronic System Operators. The requirements that the data must fulfill include the following:

a. The security and confidentiality of the Electronic Signature Creation Data creation process must be guaranteed by the Electronic Signature Provider or Electronic Signature Service Supporter;
b. If cryptographic code is used, Electronic Signature Creation Data must not be easily guessed from Electronic Signature verification data through certain calculations, within a certain period, and with reasonable means;
c. Electronic Signature Creation Data must be stored in electronic media controlled by the Signer; And
d. Data related to the Signer must be stored in a place or data storage facility that uses a trustworthy system, owned by the Electronic Signature Provider or Signature Service Supporter.

In creating electronic signatures, the methods and techniques used are critical to ensure the accuracy and security of electronic information. The use of cryptographic techniques, including public key applications such as consent keys, data encryption, and digital signatures, are highly secure measures in this context.

Legal Strength of Digital Signature Evidence in Civil Procedure Law

The purpose of proof is to confirm the existence of a fact or establish a specific event, as stated in Article 163 of the HIR (283 RGB). Anyone making a claim or denying the rights of others must provide evidence of their right or event, indicating that proof encompasses both events and rights. The process of proof allows for the affirmation or rejection of arguments presented by parties involved in a case. In Indonesia's judicial system, Civil Law, such as HIR or KUHPerdata, regulates various processes in the judicial system. Proof in Civil

Procedural Law is classified in Article 1866 of the Civil Code or Article 164 of the HIR or RGB's Article 283, which includes five types of evidence: written, with witnesses, presumptions, confessions, and oaths. However, presenting electronic data, such as digital signatures, as evidence poses challenges in the judicial process in Indonesia.

Generally, the use of digital signatures in e-commerce transactions means that transactions do not require physical documents or even a signature. This lack of a physical signature may result in electronic data presented as evidence lacking valid probative force, according to Article 1866 of the Civil Code. The judge or opposing party will likely reject the use of digital signatures as evidence in the legal process.

a. Digital Signature Proof According to Law Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning Notary Positions;

   Before the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions, electronic documents only had the power of proof limited to private deeds. In this context, private deeds are made without the presence or intermediary of authorized public officials. The evidentiary power of this document depends on whether the parties acknowledge its existence or if there is no denial from one of the parties. If one party denies the document, the burden of proof will emerge by the party who denies it, and the judge will assess the rejection of the evidence.

   Electronic documents that have been signed with an electronic signature are substantially recognized in evidentiary law in Indonesia after being regulated in Article 5 paragraph (2) of Law Number 11 of 2008 concerning Electronic Information and Transactions. This article states that electronic information and/or electronic documents and their printouts are considered valid legal evidence, which is an extension of legal evidence by the procedural law in force in Indonesia. With the enactment of Law Number 11 of 2008 concerning Information and Electronic Transactions, by Article 18 together with Article 7 and Article 11, the evidentiary power of electronic documents that have been signed with a Digital Signature is considered to be equivalent to the evidentiary power of an authentic deed made by a public official.

   This regulation is contrary to Article 1 point 7 of Law Number 30 of 2004 concerning the Position of Notary, which changes the definition of "deed" as an authentic deed made by or before a Notary by the procedures stipulated in this law. Due to the conflict between these regulations, if one party files a lawsuit with an electronic document signed using an electronic signature as evidence, the judge in resolving the dispute in court is expected to find an innovative solution. As the highest authority in deciding a case, judges need to take creative steps in making decisions, regardless of the existence of written or unwritten legal rules.

b. Digital Signature Proof According to Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Information and Electronic Transactions;

   Electronic signatures that use asymmetric cryptography technology involve the use of two keys, namely the private key and the public key. To ensure that the electronic signature on an electronic document has evidentiary power in court, the step that needs to be taken is to register the electronic signature with the Certification Authority (CA). By doing this, the Certification Authority (CA) can act as an official entity, utilizing the infrastructure it has, especially in verifying signature times on electronic transactions. Digital signatures that have been certified by the Certification Authority (CA) provide a higher level of authentication for a document. Digital signatures are difficult to forge because they are closely linked to a unique combination of document and private key, as long as the process complies with the provisions stipulated in the applicable laws and regulations.

Often, there are differences between laws issued by state bodies, where one law can conflict with another rule. For example, Law Number 11 of 2008, which conflicts with Law Number 30 of 2004. In cases where legal rules conflict, the judge refers to the principle of lex specialis derogat legi generali, which means a more specific law overrides the law. Invite a more general one. In this context, Law Number 11 of 2008 overrides Law Number 30 of 2004. Thus, the evidentiary power of electronic documents signed with an electronic signature is considered equivalent to an authentic deed.

For an electronic signature to meet the minimum standard of proof, it must be supported by expert witnesses, such as the Certification Authority (CA) or Digital Forensic experts, who have an in-depth understanding and can guarantee that the electronic information related to the electronic signature complies with the requirements regulated in the Law. Apart from that, they must also be able to ensure that the electronic document remains intact since its creation without undergoing any changes when received by another party (integrity) and that the signature comes from the individual who claims to have created it (authenticity), and that the signature This cannot be denied by the maker (non-repudiation).

The legal system of evidence in the Netherlands is currently regulated in the Burgerlijke Rechtsvordering (Civil Procedure Book, abbreviated as RV) which was revised on 1 January 2002. This section, from Articles 149 to 207, regulates various aspects of evidence in civil cases, including how evidence is carried out (bewijslevering), assessment of evidence (bewijswaardering), strength of evidence (bewijskracht), burden of proof (bewijslast), offer of evidence (bewijsaanbod), and means of evidence (bewijsmiddel). Proving, or bewijslevering, refers to how the parties involved are required to present evidence to the judge during the trial. Meanwhile, the assessment of the evidence presented (bewijswaardering) is carried out by the judge, unless there is a statutory provision that states otherwise, as regulated in Article 152 paragraph (2) RV which states that "The assessment of the evidence is left to the judge's decision, unless the law -the law determines otherwise."[5]

All types of evidence can be used in the evidentiary process in court, but the assessment of the strength of the evidence presented is determined by the judge unless there are statutory provisions that stipulate otherwise. Evidence can have binding evidentiary power for the judge or more flexible evidentiary power, where the determination of the strength of the evidence is completely left to the judge, as previously stated in Article 152 paragraph (2) RV. Article 152 paragraph (1) Rv emphasizes that in principle, all types of evidence can be used in the evidentiary process in court unless there are statutory provisions that determine otherwise. It shows that the civil evidentiary legal system in the Netherlands adopts an open approach, which allows the use of evidence that is not specifically regulated in law.

CONCLUSION

Digital Signature, also known as Digital Signature, is a form of electronic signature that relies on cryptographic technology for security, where the information contained within identifies the owner. Apart from using cryptography, Digital Signature involves two different keys, namely a public key and a private key, to increase the level of security. Although Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions classifies uncertified electronic signatures as part of electronic signatures, Law Number 11 of 2008 concerning Electronic Information and Transactions explains that a signature must fulfill six conditions to have valid legal consequences. In general, the use of Digital Signature as evidence must guarantee four important things, namely authenticity, integrity, non-repudiation, and confidentiality. Once these four items are

fulfilled, the Digital Signature can be given electronic certification and used as evidence in the judicial process.

Law Number 11 of 2008 concerning Electronic Information and Transactions recognizes electronic information and electronic documents as valid evidence, as regulated in Article 5 paragraphs (1) and (2). This is considered an extension of valid evidence by the procedural law in force in Indonesia. However, if we compare it with Law Number 30 of 2004 concerning Notary Positions, valid evidence is an authentic deed and a private deed. In the process of making the deed, the Notary must be directly involved, witness and document each stage, and physically sign the deed with the parties involved. Electronic signatures are not considered valid in evidentiary law because they do not meet the requirements. However, the principle of lex specialis derogat lex generalis applies here, which means that specific laws will override general laws. In this context, Law Number 11 of 2008 has greater power than Law Number 30 of 2004. Therefore, the evidentiary power of an electronic document signed with an electronic signature is equivalent to an authentic deed.

.

REFERENCES

D. N. Banjarnahor *et al.*, *ASPEK HUKUM BISNIS*. Bandung: CV WIDINA MEDIA UTAMA, 2020.

R. Subekti and R. Tjitrosudibio, *Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek)*, Cet. 37. Jakarta: Pradnya Paramita, 2006.

B. Ardwiansyah, "KEABSAHAN PENGGUNAAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI MENURUT UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK," *Lex Privatum* , vol. 5, no. 7, 2017, Accessed: Apr. 25, 2024. [Online]. Available: https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/18232

D. S. Listyana, I. A. Wati, and Lisnawati, "Kekuatan Pembuktian Tanda Tangan Elektronik Sebagai Alat Bukti Yang Sah Dalam Perspektif Hukum Acara Di Indonesia Dan Belanda," *Verstek: Universitas Sebelas Maret*, vol. 2, no. 2, pp. 146–154, 2014.

E. L. Fakhriah, *Bukti Elektronik Dalam Sistem Pembuktian Perdata*. Jakarta: PT. Refika Aditama, 2017.

Suratman and P. Dillah, *Metode Penelitian Hukum*. Bandung: Alfabeta, 2013.

S. Partodihardjo, *Tanya Jawab Sekitar Undang-undang No. 11 Tahun 2008: Tentang Informasi dan Transaksi Elektronik*. Jakarta: Gramedia Pustaka Utama, 2009.

T. N. Cahyadi, "ASPEK HUKUM PEMANFAATAN DIGITAL SIGNATURE DALAM MENINGKATKAN EFISIENSI, AKSES DAN KUALITAS FINTECH SYARIAH," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, vol. 9, no. 2, p. 219, Aug. 2020, doi: 10.33331/rechtsvinding.v9i2.424.

Wahana Komputer, *Memahami Model Enkripsi dan Security Data*. Yogyakarta: Andi, 2003.

A. M. Andalan, "Kedudukan Tanda Tangan Elektronik dalam Transaksi Teknologi Finansial," *Jurist-Diction*, vol. 2, no. 6, p. 1931, Nov. 2019, doi: 10.20473/jd.v2i6.15921.