

LEGAL REVIEW OF DIGITAL SIGNATURE EVIDENCE UNDER THE INDONESIAN ELECTRONIC INFORMATION AND TRANSACTIONS ACT

Eka Aulia Putri^{1*}, Marilang¹, Fadli Andi Natsif¹, Istiqamah¹, St. Nurjannah¹

¹Universitas Islam Negeri Alauddin Makassar, Indonesia

*Correspondent Email: ekaauliaputri2603@gmail.com

Abstract

The main problem in this study is how the requirements for digital signatures can be recognized as valid evidence, and how the legal strength of digital signature evidence is reviewed from Law Number 19 of 2016 concerning information and electronic transactions. This type of research is library research with a juridical-normative approach. Sources of data are directly related to the topic of the problem such as laws and regulations, books, journals, to other written works related to the problem. The results of this research obtained by the author are the digital signature requirements so that they can be recognized as valid evidence, in article 11 of the ITE Law which stipulates that. The legal strength of proof inherent in digital signatures in terms of civil evidence has the legal power of evidence at the same level as private certificates, therefore the legal strength of evidence inherent in signatures on electronic letters is only formal and material proof.

Keywords: Proof; Digital Signature; Elecetronic Transactions

Abstrak

Pokok permasalahan dalam penelitian ini adalah bagaimana persyaratan digital signature sehingga dapat diakui sebagai alat bukti yang sah, dan bagaimana kekuatan hukum pembuktian perdata digital signature ditinjau dari UU Nomor 19 tahun 2016 tentang informasi dan transaksi elektronik. Jenis penelitian ini adalah penelitian kepustakaan dengan pendekatan yuridis-normatif. Sumber data yakni berkaitan langsung dengan topik permasalahan seperti peraturan perundang-undangan, buku-buku, jurnal, hingga karya tulis lainnya yang berkaitan dengan permasalahan. Hasil dari penelitian ini yang diperoleh oleh penulis adalah syarat digital signature sehingga dapat diakui sebagai alat bukti yang sah, tercantum pada pasal 11 UU ITE yang mengatur bahwa tanda tangan elektronik memiliki kekuatan dan akibat hukum yang sah selama memenuhi persyaratan. Kekuatan hukum pembuktian yang melekat dalam digital signature ditinjau dari pembuktian perdata memiliki kekuatan hukum bukti setingkat dengan akta dibawah tangan oleh karena itu kekuatan hukum bukti yang melekat dalam tanda tangan pada surat elektronik hanya kekuatan pembuktian formil dan pembuktian materil.

Kata Kunci : Pembuktian; Digital signature; Transaksi Elektoronik

DOI: 10.24252/aldev.v8i1.36827

This is an open-access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.





INTRODUCTION

Developments in social patterns have a significant impact on economic, social, and cultural aspects, primarily driven by the influence of information technology. The most visible transformation is in the economic sector, where a shift from conventional or manual systems to a digital economy utilizing electronic tools is evident. In the current era of globalization, the most prominent characteristic of the economy is its rapid pace, which compels humanity to enter an era of free-market competition (Banjarnahor et al., 2022).

The use of electronic systems in the business world is widespread today because they offer convenience, speed, and efficiency. E-commerce activities are no longer simple; they are no longer restricted by a country's territorial boundaries and are easily accessible anytime and anywhere. However, losses can occur for both transaction participants and third parties who have never engaged in a transaction. Such losses inevitably lead to conflicts that may reach the court process. In civil cases, evidence serves as the benchmark to assist judges in considering the truth of the events presented. Proving is the act of convincing a judge of the truth of the arguments put forward regarding a dispute, demonstrating that evidence is only necessary within a dispute or case before a judge or court (Subekti, 2002).

The use of information technology based on electronic means in electronic transactions is believed to have a positive impact on business actors, especially regarding the speed and ease of conducting global transactions without time and space limitations. In connection with this, the need for information confidentiality and the preservation of information authenticity has increased. Consequently, the Government of the Republic of Indonesia enacted Law Number 11 of 2008 concerning Information and Electronic Transactions (subsequently amended by Law Number 19 of 2016).

The use of digital signatures is addressed in Article 1, Number 12 of Law Number 19 of 2016, which states that an electronic signature consists of electronic information used as a verification or authentication tool (UU ITE, 2016). Based on Article 1, Number 1, electronic information is a set of electronic data including writing, sound, images, and other digital symbols that have been processed to have meaning.

In cases involving digital signatures, many individuals abuse the technology by creating electronic signatures without the consent of the owner, such as forgeries on a Notarial Deed Minute. This occurs despite regulations stating, based on Article 26 Paragraph (1), that the use of any private data through electronic media must be done with the consent of the person concerned. Any person whose rights are violated may file a lawsuit for damages incurred under this law.

Evidence is a stage that plays a crucial role for judges in delivering a verdict. The evidentiary process in a trial is the center of the judicial examination. It is central because the arguments of the parties are tested to find or apply the law in a specific case. The purpose of evidence is to establish the legal relationship between the litigating parties and to provide certainty to the judge. The evidentiary legal system in Indonesia is a closed and limited system where parties are not free to submit any type of evidence outside of what is strictly determined by law (Risal, 2018).

Currently, legal and information technology experts in Indonesia have formulated Law No. 19 of 2016 (ITE Law), which is expected to assist in gaining recognition and legal force for electronic signatures. This law is expected to bring a revolution to the law of evidence in Indonesia, resolving legal confusion regarding electronic writing and assisting in the resolution of civil disputes (Ahmaturrahman, 2005). As digital technology becomes more sophisticated, conventional evidence such as physical deeds is evolving

into electronic deeds to meet the demands of the modern e-commerce era.

METHOD

The type of research used in this study is library research with a normative juridical approach. The data sources for this research consist of primary, secondary, and tertiary data, collected through library research methods. The data analysis technique employed is qualitative analysis, which is applied systematically based on its quality to achieve the research objectives.

RESULT AND DISCUSSION

1. *Requirements That Must Be Fulfilled for a Digital Signature to be Recognized as Valid Legal Evidence*

An electronic signature is not a signature affixed to paper in the traditional sense, nor is it merely a conventional signature converted using a scanner; rather, it is obtained by first creating a message digest or hash, which serves as a mathematical summary of a document transmitted through cyberspace (Partodihardjo, 2009). There is a distinction between an electronic signature and a digital signature; the former is a legal term regulated under Indonesian legislation, while the latter refers to the specific method of electronic signing that utilizes asymmetric cryptography and public key infrastructure (Cahyadi, 2020). Principally, electronic signatures provide a guarantee of message integrity, ensuring that the sender is the authorized party responsible for the content, which differs from handwritten signatures that primarily function as an acknowledgment of a document's contents. It acts as a data item associated with a digital message encoding intended to provide certainty regarding data authenticity and to ensure the data has not been modified (Partodihardjo, 2009).

According to Article 11, Paragraph (1) of Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Information and Electronic Transactions, an electronic signature is considered valid if it meets specific requirements: the signature creation data must be linked only to the signer, the data must be under the signer's sole control at the time of signing, and any subsequent changes to the signature or the electronic information itself must be detectable. Furthermore, there must be a specific method to identify the signer and to demonstrate that the signer has given consent to the associated electronic information. This article provides explicit recognition that despite being a digital code, an electronic signature holds the same legal standing as a manual signature, possessing evidentiary power and legal consequences. These requirements represent the minimum standards, allowing for the broad development of various technical methods or processes for electronic signing.

Efa Laela Fakhriah categorizes several types of electronic evidence, starting with photos and recordings used to test authenticity through specific technology, and printouts from facsimile machines which are considered written evidence provided they match the original or are accompanied by a statement of conformity if the original is lost. Microfilm is also recognized as valid civil evidence provided its authenticity is guaranteed and traceable through registration or official reports. Additionally, emails created and communicated via computer networks and video teleconferencing—used when a witness cannot be physically present in court but their testimony is vital—serve as valid forms of evidence. Finally, electronic signatures attached to information serve as the identity and status of a legal subject, where authenticity is guaranteed through a hash function comparison to ensure the values match (Fakhriah, 2017).

Digital signatures offer superior security compared to traditional signatures because recipients can verify both the sender's identity and whether the message was altered after being signed. This guarantee of authenticity and integrity is achieved by encrypting the document using a private key (Sitompul, 2001). The ITE Law anticipates technological advancements by stipulating in Articles 5 through 12 that electronic information and its printouts are valid legal evidence, representing an expansion of the evidence types recognized under Indonesian procedural law. The primary benefits of a digital signature include authenticity, integrity, non-repudiation, and confidentiality. Each digital signature is unique to the specific document it signs because it is derived from the document's own data, meaning any change to the document will result in a completely different digital signature (Wahana Komputer, 2003).

2. *The Legal Strength of Digital Signature Evidence in Civil Law Reviewed Under Law Number 19 of 2016 concerning Information and Electronic Transactions*

The development of evidentiary law in Indonesia, particularly concerning the use of electronic evidence and electronic signatures, was officially introduced through the enactment of Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE Law). Previously, electronic evidence was only utilized as circumstantial evidence (*bukti petunjuk*) in criminal cases or as presumptive evidence (*bukti persangkaan*) in civil cases. However, with the issuance of this Law, electronic evidence—comprising electronic signatures, electronic documents, and their printouts—is explicitly recognized as valid legal evidence in court, provided it meets specific statutory requirements (Prodjohamidjojo & Bahri, 2018).

In traditional civil procedural law, electronic evidence and signatures were not initially recognized, even within electronic commerce or e-government transactions that are entirely paperless. Consequently, judicial interpretation is required to define the meaning and validity of such evidence. The view that an electronic signature cannot serve as written evidence is no longer absolute; it is increasingly seen as irrelevant in the technological age to view written evidence solely through the lens of 1848 standards.

This understanding is supported by the expectation that judges must be brave enough to make legal breakthroughs. As the primary authority in deciding cases, a judge can issue a verdict (*vonnis van de rechter*) that may not be directly based on existing written or unwritten legal regulations. In such instances, a judge must create their own regulation (*eigen regeling*). This action is justified under Article 10 Paragraph (1) of Law No. 48 of 2009 concerning Judicial Power, which stipulates that a judge may not refuse to examine, try, or decide a case on the grounds that the law is non-existent, unclear, or incomplete (the *ius curia novit* principle). If a judge's decision containing such *eigen regeling* is deemed appropriate and consistently applied by other judges, it becomes a source of law through jurisprudence (*rechtspraak*) (Sengkey, 2018).

With the ITE Law now serving as positive law, electronic deeds are considered equal to conventional deeds, and electronic signatures possess the same evidentiary strength as manuscript signatures. This is regulated under Law No. 11 of 2008 in conjunction with Law No. 19 of 2016. According to Article 11 of the ITE Law, an electronic signature carries valid legal force and consequences as long as it fulfills the following requirements: the signature creation data is linked solely to the signer; the data is under the exclusive control of the signer during the signing process; any subsequent changes to the signature or the associated electronic information are detectable; there is a specific method to identify the signer; and there is a method to demonstrate the signer's consent to the information (UU ITE, 2016).



This article provides explicit recognition that despite being a digital code, an electronic signature holds the same standing as a manual signature regarding evidentiary strength and legal consequences. These requirements represent the minimum standards, allowing for the broad development of technical methods or electronic signing processes. Regarding the evidentiary aspect, Article 5 Paragraph (1) of the ITE Law states that electronic information and/or its printouts constitute valid legal evidence. This ensures that electronic documents are binding and recognized to provide legal certainty for electronic systems and transactions.

In conclusion, the enactment of Law Number 19 of 2016 fulfills the principles of sound legislation. Regarding the evidentiary strength of electronic signatures as stated in Article 11, they are recognized as valid evidence with full legal force and consequences. This is because electronic deeds are now legally equated with conventional deeds, just as electronic signatures are equated with manuscript signatures.

CONCLUSION

The requirements that must be fulfilled for a digital signature to be recognized as valid legal evidence are found in Article 11 Paragraph 1 of the ITE Law, which explains that an Electronic Signature is considered valid if it meets the following criteria: the electronic signature creation data is linked only to the signer, the electronic signature creation data at the time of the electronic signing process is only under the control of the signer, any changes to the electronic signature that occur after the time of signing can be detected, any changes to the Electronic Information associated with the electronic signature after the time of signing can be detected, there is a specific method used to identify who the signer is, and there is a specific method to show that the signer has given consent to the associated electronic information.

The legal strength of digital signature civil evidence reviewed from Law Number 19 of 2016 concerning the amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions is, much like the evidentiary strength of a manual signature found in an authentic deed which is complete and perfect, in accordance with Article 11 which provides explicit recognition that although it is only a code, an Electronic Signature has the same standing as manual signatures in general which have legal force and legal consequences. The requirements as referred to in this article are the minimum requirements that must be met in every electronic signature. This provision opens the widest opportunity for anyone to develop methods, techniques, or processes for making electronic signatures, as for Article 11, it is as follows: the electronic signature creation data is linked only to the signer, the electronic signature creation data at the time of the electronic signing process is only under the control of the signer, any changes to the electronic signature that occur after the time of signing can be detected, any changes to the Electronic Information associated with the electronic signature after the time of signing can be detected, there is a specific method used to identify who the signer is, and there is a specific method to show that the signer has given consent to the associated electronic information.

REFERENCES

- Ahmaturrahman. *Hukum Acara Perdata Di Indonesia*. Palembang: Universitas Hukum, Universitas Sriwijaya, 2005.
- Banjarnahor, Daulat Nathanael, et al. *Aspek Hukum Bisnis*. Bandung: Widina Bhakti Persada Bandung, 2022.
- Cahyadi, Thalys Noor. "Aspek Hukum Pemanfaatan Digital Signature Dalam Meningkatkan Efisiensi, Akses Dan Kualitas Fintech Syariah." Jakarta: PT Gramedia Pustaka Utama, 2020.
- Fakhriah, Efa Laela. *Bukti Elektronik dalam Pembuktian Perdata*. Bandung: Refika Aditama, 2017.
- Indonesia. *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Indonesia. *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Partodihardjo, Soemarno. *Tanya Jawab Sekitar Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: PT Gramedia Pustaka Utama, 2009.
- Risal, M. Chaerul. "Penerapan Beban Pembuktian Terbalik dalam Upaya Penanggulangan Tindak Pidana Korupsi." *Jurisprudentie: Jurnal Ilmu Hukum* 5, no. 1 (Juni 2018): 76-90.
- Sengkey, Friandy J. "Perspektif Hukum Pidana Terhadap Tindak Pidana Intimidasi Melalui Media Sosial (Cyber Bullying)." *Lex Crimen* 7, no. 8 (2018): 120-128.
- Sitompul, Asril. *Hukum Internet: Pengenalan Mengenai Masalah Hukum di Cyber Space*. Bandung: Citra Aditya, 2001.
- Subekti. *Kitab Undang-Undang Hukum Perdata*. Jakarta: Pradnya Paramita, 2002.
- Syaiful Bahri. *Dinamika Hukum Pembuktian Dalam Capaian Keadilan*. Depok: Rajawali Pers, 2018. (Mencantumkan pemikiran Martiman Prodjohamidjojo).
- Wahana Komputer. *Memahami Model Enskripsi dan Security Data*. Yogyakarta: Penerbit Andi, 2003.