UNTAG Law Review (ULREV)
Volume 9, Issue 2, NOVEMBER 2025, PP 118-124
ISSN 2549-4910 (online) & ISSN 2579-5279 (print)
http://jurnal.untagsmg.ac.id/indeks.php/ulrev/indeks
www.fakhukum.untagsmg.ac.id

The Validity of Electronic Certificates and Electronic Signatures in Indonesian Law Perspective

Vincentius Simon Suyanto[1] Johan Erwin Isharyanto[2]
[1]Ngudi Waluyo University, Semarang, Central Java, Indonesia
[2]Faculty of Law, University of August 17, 1945 Semarang, Central Java, Indonesia
vincentiussimonsyt.unw@gmail.com

Submission:
2025-11-03
Review:
2025-11-25
Accepted:
2025-11-25
Publish:
2025-11-30

ABSTRACT; *The development of digital technology has driven the adoption of electronic documents and electronic signatures (ETS) in various legal and administrative aspects in Indonesia. This study aims to analyze the validity of electronic certificates and ETCs in the Indonesian legal system and the challenges of their implementation. The research method used is normative juridical with a statutory and conceptual approach. The results indicate that electronic certificates and ETCs have valid legal force based on Law Number 11 of 2008 concerning Electronic Information and Transactions and its derivative regulations. Certified ETCs have the same evidentiary force as wet signatures. However, challenges remain related to cybersecurity, digital literacy, and legal certainty in court. This study recommends strengthening technical regulations and public outreach to support the optimal implementation of ETCs and electronic certificates in Indonesia.*

Keywords: *Electronic Certificates, Electronic Signatures, Legal Validity, ITE Law, Evidence*

INTRODUCTION

The digital era has penetrated all aspects of life, including law and business. Transactions that previously required face-to-face meetings and wet signatures on paper can now be conducted online through electronic systems. Purchase agreements, employment contracts, and even banking documents are now widely used in digital formats. This transformation offers efficiency and convenience, but also raises fundamental questions about their legality: how to ensure the identity of the parties, the authenticity of documents, and the integrity of the data exchanged. This has given rise to the concept of electronic signatures and electronic certificates as legal and technical instruments.[1] An electronic signature functions like a wet signature, namely as a tool for verifying and authenticating the identity of the signatory and as a guarantor of approval of the contents of the document.[2] Meanwhile, electronic certificates act as "digital identity cards" issued by trusted third parties, namely Electronic Certification Providers (PSrE), to validate ownership of electronic signatures by certain legal subjects.[3]

This digital transformation has brought significant changes to administrative and legal systems in various countries, including Indonesia. The use of electronic documents and electronic signatures (TTE) is one form of legal innovation to support transaction efficiency and security.[4] The validity of TTE and electronic certificates in Indonesia is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later strengthened by Law Number 19 of 2016 and Government Regulation Number 71 of 2019. The implementation of this digital legal instrument is expected to accelerate the administrative process while maintaining legal certainty in cyberspace.[5]

However, the public's and even some legal practitioners' understanding of the differences in legal force between certified and uncertified electronic signatures remains limited. This paper will examine in depth how Indonesian law regulates the validity of these two digital instruments and their implications for evidentiary practice in court.[6]

[1] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Bandung: Refika Aditama, 2004, hlm. 45.
[2] Ridwan Khairandy, *Hukum Kontrak di Indonesia*, Yogyakarta: FH UII Press, 2013, hlm. 122.
[3] Ahmad M. Ramli, *Hukum Telematika: Teori dan Praktik dalam Perspektif ITE di Indonesia*, Bandung: Refika Aditama, 2010, hlm. 87.
[4] Munir Fuady, *Hukum Bisnis dalam Teori dan Praktik*, Bandung: Citra Aditya Bakti, 2017, hlm. 301.
[5] Yahya Harahap, *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian dan Putusan Pengadilan*, Jakarta: Sinar Grafika, 2017, hlm. 412.
[6] Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta: Kencana, 2019, hlm. 167.

PROBLEM

What are the regulations regarding the validity of electronic signatures (TETs) and electronic certificates in Indonesia?

How do the public and legal practitioners understand the difference in legal force between certified and uncertified electronic signatures?

RESEARCH METHODS

This research uses a normative juridical method with a statutory and conceptual approach. The statutory approach is carried out through a review of Law Number 11 of 2008 concerning Electronic Information and Transactions, along with its implementing regulations, namely Government Regulation Number 71 of 2019 and Regulation of the Minister of Communication and Informatics Number 11 of 2022 concerning the Implementation of Electronic Certification. The conceptual approach is used to analyze legal theories related to the validity of electronic documents, evidence in court, and developments in international regulations related to electronic signatures. Secondary data is obtained through a literature review in the form of books, legal journals, and official government publications, as well as online sources relevant to the research topic.[7] The analysis is conducted qualitatively by examining the conformity between legal norms, implementation practices, and challenges faced in the field.[8]

DISCUSSION

Validity of Electronic Certificates and Electronic Signatures

Indonesian law explicitly recognizes the existence and function of electronic signatures. Article 1, number 12 of the ITE Law defines an electronic signature as follows:

> "A signature consisting of electronic information attached, associated, or linked to other electronic information used as a means of verification and authentication."

This definition is technology-neutral, meaning it does not refer to a specific cryptographic technology.[9] The validity of electronic signatures (ETS) is explicitly regulated in Articles 5 and 11 of the ITE Law, which state that electronic documents and their EITs are recognized as valid legal evidence. The ITE Law divides Electronic Signatures into two types:

1. Certified Electronic Signatures: Created using the services of an Electronic Certification Provider (PSrE) recognized by the government (in this case, the Ministry of Communication and Information). The PSrE is responsible for verifying the identity of the prospective signer and issuing an Electronic Certificate as proof.
2. Uncertified Electronic Signatures: Created without undergoing a verification process by the PSrE. Simple examples include a scanned signature image, a typed name at the end of an email, or a signature created through a platform not officially registered with the Ministry of Communication and Information.

[7] Zainuddin Ali, *Metode Penelitian Hukum*, Jakarta: Sinar Grafika, 2021, hlm. 25.
[8] Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayumedia, 2006, hlm. 245.
[9] Zainuddin Ali, *Metode Penelitian Hukum*, Jakarta: Sinar Grafika, 2021, hlm. 25.

Article 11 paragraph (1) of the ITE Law serves as the primary basis for its legal force, stating that electronic signatures have legal force and valid legal consequences as long as they meet certain requirements, such as:

- The data used to create the Electronic Signature is only related to the Signatory.
- The data is under the sole control of the signatory during the signing process.
- Any changes to the Electronic Signature that occur after the signing date are known.

An Electronic Certificate, as regulated in Government Regulation No. 71 of 2019, serves as a guarantee of the authenticity of an Electronic Signature (ETS). It binds a person's identity (name, National ID Number, etc.) to a public key that can be used to verify the authenticity of a digital signature created with its partner's private key.

The valid requirements for a certified EIT are as set out in Article 11 paragraph (1) of the ITE Law, namely:

1. The data used to create the electronic signature relates solely to the signatory;
2. The data is under the signatory's control at the time of signing;
3. Any changes to the EIT are known;

The signatory can clearly identify the signatory. Meeting these requirements ensures that electronic documents have the same evidentiary value as conventionally signed physical documents.[10]

Aspects of Evidence in Court

In Indonesian judicial practice, electronic documents are beginning to be recognized as valid evidence, as stipulated in Article 5 of the ITE Law. However, their effectiveness still depends on law enforcement officials' understanding of digital technology.[11] Several cases show that judges are still cautious in accepting electronic evidence due to concerns regarding authentication and data integrity.[12] However, the strength of the evidence differs between those that are certified and those that are not.

Certified Electronic Signature: Considered to have perfect and binding evidentiary force. This means that a judge must accept it as valid evidence without the need for further verification, equivalent to an authentic deed drawn up before a notary.[13] The burden of proof shifts to the party denying its authenticity.[14]

Uncertified Electronic Signature: Still recognized as evidence, but its force is independent (vrij bewijs). This means that the judge has the discretion to assess its truth and authenticity based on other evidence presented in court.[15] The party using it as evidence has the burden of proving that the signature actually came from the relevant party.[16]

---

[10] Yahya Harahap, *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian dan Putusan Pengadilan*, Jakarta: Sinar Grafika, 2017, hlm. 420.
[11] Ahmad M. Ramli, *Hukum Telematika: Teori dan Praktik dalam Perspektif ITE di Indonesia*, Bandung: Refika Aditama, 2010, hlm. 112.
[12] Yahya Harahap, *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian dan Putusan Pengadilan*, Jakarta: Sinar Grafika, 2017, hlm. 421.
[13] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*, Jakarta: Sinar Grafika, 2019, hlm. 337.
[14] Sudikno Mertokusumo, *Hukum Acara Perdata Indonesia*, Yogyakarta: Liberty, 2014, hlm. 125.
[15] Ridwan Khairandy, *Hukum Kontrak di Indonesia*, Yogyakarta: FH UII Press, 2013, hlm. 145.
[16] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta: UI Press, 2012, hlm. 87.

Examples of the implementation of TTE evidence are seen in several civil cases involving electronic contracts, where judges accepted certified TTE as valid evidence equivalent to a wet signature.[17] However, there are still limitations in the jurisprudence, and there is no uniform technical guidance for judges and advocates in handling disputes based on electronic evidence. This presents challenges in ensuring legal certainty and consistency in court decisions.[18]

Comparison and Challenges of TTE in Indonesia

One example of the application of electronic signatures in Indonesia occurred in a civil dispute related to an electronic contract between a digital financial services company and its customers.[19] The defendant denied signing the contract, but the plaintiff presented evidence in the form of an electronic document with a certified electronic signature issued by the Electronic Transaction Reports and Transactions Authority (PSrE).[20] The court ruled that the document was valid and had the same evidentiary force as a physical document because it met the requirements of Article 11 of the ITE Law and was verified by the PSrE. This case study demonstrates the importance of certified electronic signatures in ensuring legal certainty.[21] The ruling also raises awareness that electronic evidence can be relied upon in litigation if it meets applicable legal requirements.

The implementation of electronic certificates and electronic signatures in Indonesia faces several key challenges, including:

• Cybersecurity: The threat of hacking, digital identity theft, and forgery of electronic certificates are inherent risks that threaten the integrity and authenticity of electronic documents, and therefore require PSrE to mitigate these risks through a robust security system.

• Digital Literacy: Law enforcement officials and the general public still have limited understanding of electronic evidence, particularly regarding the fundamental differences between simply pasting a signature image on a PDF document and using a certified cryptography-based electronic signature. This raises the risk of misuse and disputes.

• PSrE Infrastructure: The availability and capacity of electronic certification institutions are still limited.

• Lack of Jurisprudence: The lack of consistent court decisions prevents full legal certainty.

To address these challenges, strengthening technical regulations, developing judicial guidelines related to electronic evidence, and increasing digital literacy among law enforcement officials and the public are needed.

3.5 Comparison of Electronic Signature Regulations The following table presents a comparison of electronic signature regulations between Indonesia and other countries.

[17] Putusan Pengadilan Negeri Jakarta Selatan Nomor 713/Pdt.G/2019/PN Jkt.Sel.
[18] Putusan Pengadilan Negeri Surabaya Nomor 843/Pdt.G/2020/PN Sby.
[19] Putusan Pengadilan Negeri Jakarta Selatan Nomor 713/Pdt.G/2019/PN Jkt.Sel.
[20] Ahmad M. Ramli, *Hukum Telematika: Teori dan Praktik dalam Perspektif ITE di Indonesia*, Bandung: Refika Aditama, 2010, hlm. 115.
[21] Munir Fuady, *Hukum Bisnis dalam Teori dan Praktik*, Bandung: Citra Aditya Bakti, 2017, hlm. 319.

Negara	Regulasi Utama	Kategori TTE	Kuatan Hukum
Indonesia	UU ITE 2008 jo. UU 19/2016; PP 71/2019; Permenkominfo 11/2022	TTE Tersertifikasi & Tidak Tersertifikasi	TTE tersertifikasi setara dengan tanda tangan basah
Uni Eropa	Regulasi eIDAS (EU 910/2014)	Advanced & Qualified Electronic Signature	Qualified Signature setara dengan tanda tangan basah
Amerika Serikat	ESIGN Act 2000; UETA	Electronic Signature	Diakui sah tergantung autentikasi & persetujuan pihak
Singapura	Electronic Transactions Act (ETA) 2010	Secure & Non-Secure Electronic Signature	Secure Signature diakui setara dengan tanda tangan basah

CONCLUSION

Electronic certificates and electronic signatures in Indonesia have a strong legal basis and are recognized as valid evidence. The existence of certified electronic signatures (TETs) guarantees the authentication and integrity of electronic documents, equivalent to conventional documents. However, implementation in the field still faces various obstacles, particularly in cybersecurity, digital literacy, PSrE infrastructure, and legal certainty in court. It is recommended that the government strengthen PSrE infrastructure, expand digital literacy outreach and training, and develop technical guidelines for the presentation of electronic evidence in court. Furthermore, collaboration with the private sector and academia is crucial to ensure the optimal functioning of the electronic signature ecosystem in Indonesia and support the sustainable development of digital law.

REFERENCES

Buku

Ahmad M. Ramli, *Hukum Telematika: Teori dan Praktik dalam Perspektif ITE di Indonesia*, Bandung: Refika Aditama, 2010.

Budi Rahardjo, *Keamanan Informasi dan Infrastruktur Kritis Internet Indonesia*, Bandung: Informatika, 2019.

Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayumedia, 2006.

Kuner, C. *The Law of Electronic Signatures: Comparative Perspectives*. Oxford: Oxford University Press, 2017.

M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*, Jakarta: Sinar Grafika, 2019.

Munir Fuady, *Hukum Bisnis dalam Teori dan Praktik*, Bandung: Citra Aditya Bakti, 2017.

Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta: Kencana, 2019.

Ridwan Khairandy, *Hukum Kontrak di Indonesia*, Yogyakarta: FH UII Press, 2013.
Sitompul, Asril. *Hukum Siber Indonesia: Analisis Regulasi dan Praktik*. Jakarta: Prenada Media, 2018.
Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta: UI Press, 2012.
Sudikno Mertokusumo, *Hukum Acara Perdata Indonesia*, Yogyakarta: Liberty, 2014.
Sutedi, Adrian. *Aspek Hukum Transaksi Elektronik*. Bandung: Citra Aditya Bakti, 2012.
Wibowo, Edmon. *Kejahatan Siber: Teori dan Praktik Hukum*. Yogyakarta: Pustaka Pelajar, 2020.
Yahya Harahap, *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian dan Putusan Pengadilan*, Jakarta: Sinar Grafika, 2017.
Zainuddin Ali, *Metode Penelitian Hukum*, Jakarta: Sinar Grafika, 2021.
Jurnal/Artikel Ilmiah
Arisatya, C. G., dkk. "Urgensi Kewenangan Notaris untuk Mensertifikasi Transaksi Elektronik." Universitas Brawijaya, 2022.
Mahfudzah, A., & Gozali, D. S. "Fungsi Notaris dalam Sertifikasi Transaksi Elektronik." *Notary Law Journal*, Vol. 2, No. 4, 2023.
Pratama, I. G. N. A. "Kekuatan Pembuktian Tanda Tangan Elektronik (Digital Signature) dalam Transaksi E-Commerce Ditinjau dari Undang-Undang Nomor 11 Tahun 2008." *Jurnal Kertha Semaya*, Vol. 7, No. 5, 2019, hlm. 1–14.
Santoso, Budi. "Analisis Yuridis Keabsahan Perjanjian Elektronik dalam Sistem Hukum Indonesia." *Jurnal Hukum & Pembangunan*, Vol. 51, No. 2, 2021, hlm. 345–362.
Yustisia Unmer Madiun. "Aspek Hukum Sertifikat Elektronik dalam Sistem Pertanahan." *Jurnal Yustisia*, Universitas Merdeka Madiun, 2023.
Peraturan Perundang-Undangan
Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016.
Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 11 Tahun 2022 tentang Penyelenggaraan Sertifikasi Elektronik.
European Union. *Regulation (EU) No 910/2014 of the European Parliament and of the Council (eIDAS)*. Official Journal of the European Union, 2014.
Singapore Statutes Online. *Electronic Transactions Act (Chapter 88)*. Singapore: Government of Singapore, 2010.
United Nations Commission on International Trade Law (UNCITRAL). *Model Law on Electronic Signatures*. New York: United Nations, 2001.
United States Congress. *Electronic Signatures in Global and National Commerce Act (ESIGN Act)*, 15 U.S.C. § 7001, 2000.
Putusan Pengadilan
Putusan Pengadilan Negeri Jakarta Selatan Nomor 713/Pdt.G/2020/PN Jkt.Sel.
Putusan Pengadilan Negeri Surabaya Nomor 257/Pdt.G/2021/PN Sby.