GOLDEN RATIO OF LAW AND SOCIAL POLICY REVIEW
VOLUME 4, ISSUE. 2 (2025)
Website: https://goldenratio.id/index.php/grlspr

GOLDEN RATIO
ISSN [Online]: 2808-2923

LAW & SOCIAL POLICY | RESEARCH ARTICLE

Legal Analysis of Electronic Signatures Under Indonesia's Law No. 11 of 2008 on Electronic Information and Transactions

A. Khaerunnisa Malkab[1], La Ode Husen[2], Asriati[3]

[1,2,3] Department of Law, Faculty of Law, Universitas Muslim Indonesia, Makassar, Indonesia.
Email: akhaerunnisamalkab@gmail.com[1], laode.husen@umi.ac.id[2], asriati.asriati@umi.ac.id[3]

ARTICLE HISTORY

Received: May 16, 2025
Revised: June 22, 2025
Accepted: June 30, 2025

DOI
https://doi.org/10.52970/grlspr.v4i2.1879

ABSTRACT
This research aims to: (1) identify and analyze the legal provisions regarding the validity of electronic signatures within the Indonesian civil law system; and (2) examine and analyze the legal framework governing the verification of electronic signatures as evidence in civil cases according to the prevailing laws and regulations in Indonesia. This study employs a normative juridical research method, using primary data derived from statutory regulations and legal literature. The data were analyzed qualitatively and descriptively by examining the conformity of legal implementation with the principles of evidence in civil procedural law. The research findings indicate that: (1) electronic signatures have legitimate and legally recognized status as long as they meet the requirements stipulated in Article 11 of Law Number 11 of 2008 on Electronic Information and Transactions; and (2) the verification of the validity of electronic signatures follows the general procedures of evidence examination. The study recommends that: (1) there should be increased legal awareness regarding the validity and security of electronic signatures in digital transactions. Intensive public dissemination can help the community understand that legally valid electronic signatures possess the same legal force as conventional signatures, thereby enhancing efficiency and trust in technology-based economic activities; and (2) it is important to strengthen digital legal literacy and capacity through continuous training on electronic evidence and cybersecurity. With a comprehensive understanding, law enforcement officials can assess the validity of electronic signatures objectively and consistently in accordance with the principles of justice and legal certainty.

Keywords: Electronic Signature, Law No. 11 of 2008 on Electronic Information and Transactions, Validity, Verification.

I. Introduction

The rapid advancement of information technology has profoundly transformed human interaction and legal practices worldwide. Digitalization has not only revolutionized economic and administrative systems but has also challenged traditional legal frameworks to adapt to the realities of the digital age. One of the most significant transformations in this context is the emergence of the electronic signature, which functions as a digital authentication mechanism replacing the traditional handwritten signature in legal documents and electronic transactions (Fauzi, Rifai, & Shebubakar, 2024). Globally, electronic signatures have become an essential element of modern legal systems. Countries such as the United States, Singapore, and

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

Estonia have developed comprehensive regulations recognizing the legal validity of digital signatures in both electronic transactions and evidentiary processes (Slamet & Paliling, n.d.). In Indonesia, similar progress has been initiated through the enactment of Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), later amended by Law No. 19 of 2016. These laws represent major milestones in acknowledging the legal force of electronic documents and signatures as valid evidence within Indonesia's legal system.

However, despite the existence of these progressive legal instruments, the practical implementation of electronic signatures in Indonesia remains problematic. From a normative standpoint, the Indonesian Civil Code (KUHPerdata) continues to serve as the primary legal reference for civil matters, particularly in evidentiary procedures. Article 1868 of the Civil Code stipulates that an authentic deed must be executed in a physical form and signed directly by the parties involved and the competent official. This provision poses a significant challenge when applied to digital evidence, as electronic signatures are non-physical and rely on digital verification mechanisms operated by third-party certification authorities (Fitcanisa & Azheri, 2023). This incongruity between the Civil Code and the ITE Law has given rise to a duality of legal norms that undermines legal certainty in electronic transactions. Although Article 11 of the ITE Law explicitly grants electronic signatures equal legal force to traditional ones—provided they meet specific requirements—judicial practice often demonstrates inconsistency. Courts have repeatedly rejected documents signed electronically because they fail to meet the formal requirements of authenticity under the Civil Code (Usman, 2020). Such inconsistency reveals a persistent gap between modern digital legislation and its application in civil adjudication.

Compounding this issue is the low level of legal and digital literacy among the general public and law enforcement officials. Many individuals and business actors are unaware that a legally valid electronic signature must be created through a certified authentication system and issued by a recognized Electronic Certification Provider (Penyelenggara Sertifikasi Elektronik, PSrE). Without certification, such digital signatures lack evidentiary strength in court proceedings (Ilham et al., 2022). Consequently, numerous civil disputes involving digital contracts have been dismissed due to the absence of certified electronic signatures (Maryam Hanum, n.d.). This situation not only weakens the trust in digital legal instruments but also exposes users to legal uncertainty in online commercial activities. In Indonesia's growing e-commerce sector, major platforms such as Tokopedia and Shopee primarily rely on click-wrap agreements, which do not incorporate legally recognized electronic signatures. Although these mechanisms are commercially functional, they pose evidentiary challenges in court as they do not qualify as authentic deeds under civil law (Putri & Budiana, 2018).

Another layer of complexity lies in the role of notaries as public officials authorized to create authentic deeds. Many notaries remain reluctant to use electronic signatures in drafting notarial acts, citing doubts about their admissibility as valid evidence in court. This hesitation reflects the absence of clear procedural guidelines and consistent judicial interpretation concerning the legal weight of electronic signatures in official deeds (Fitcanisa & Azheri, 2023). Ironically, notaries—who act as guardians of legal authenticity—should ideally be at the forefront of adopting and legitimizing digital innovations in documentation. The challenges described above highlight Indonesia's ongoing transition toward a digital legal ecosystem. The tension between conventional legal frameworks and the imperatives of digital transformation has produced considerable legal uncertainty (Fauzi et al., 2024). Between 2021 and 2023, several civil cases in Jakarta and Surabaya involving digital contracts were dismissed due to the use of uncertified electronic signatures, underscoring the gap between regulatory ideals and practical enforcement.

Comparatively, other countries have taken more decisive steps to integrate technology into their civil law systems. Estonia, for instance, has successfully established a nationwide digital identity infrastructure, enabling all citizens to execute legally binding electronic signatures recognized by government institutions and courts (Slamet & Paliling, n.d.). Singapore's Electronic Transactions Act (ETA) offers another model, providing a strong legal foundation for electronic transactions and evidentiary procedures. These examples demonstrate the importance of harmonizing legal and technological frameworks to ensure the enforceability of digital evidence. From a regulatory perspective, Indonesia's legal framework is conceptually progressive. The ITE Law and its derivative regulations clearly define the elements, validity requirements, and mechanisms

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

for electronic signatures in legal and administrative contexts (Amelia Intan Saraswati et al., 2023). Nevertheless, the mere existence of legislation is insufficient without effective inter-regulatory synchronization and capacity building among law enforcement officers. Therefore, a comprehensive assessment of the implementation of Article 11 of the ITE Law is essential to determine its practical impact on civil evidence and judicial consistency.

This research seeks to address these gaps by analyzing the legal framework governing the validity of electronic signatures within Indonesia's civil law system and examining the procedural standards for their verification as evidence in civil proceedings. Through a normative and analytical legal approach, the study aims to identify areas of disharmony between statutory law and judicial practice, while proposing reforms to strengthen legal certainty in digital transactions. Theoretically, this study contributes to the enrichment of modern civil law scholarship, particularly in the domain of evidentiary law and cyber law. Practically, it provides guidance for judges, notaries, legal practitioners, and business actors regarding the use and authentication of electronic signatures in digital legal documents. Ultimately, this research aspires to support the development of a responsive, modern, and equitable civil justice system that aligns with the ongoing transformation toward digital governance and legal modernization in Indonesia.

II. Literature Review and Hypothesis Development

2.1. Theory of Evidentiary Strength

In civil proceedings, the evidentiary phase plays a decisive role in shaping judicial outcomes. After a lawsuit is registered and parties are duly summoned, the court process follows several stages—mediation (as regulated by Supreme Court Regulation No. 1 of 2016), pleadings, reply–rejoinder, and finally the stage of proof, which serves as the core mechanism for verifying legal claims. The purpose of the evidentiary process is to determine whether a claim is supported by a sufficient legal foundation to be granted or must be dismissed (E. & Isworo, 2022). Under Indonesian law, legitimate forms of evidence are listed exhaustively in Article 164 HIR/284 RBg and Article 1866 of the Civil Code, namely: documentary evidence, witness testimony, presumptions, confession, and oath. Each has its own evidentiary power and hierarchy in influencing judicial reasoning. In essence, evidence is the medium that demonstrates the truth of a legal fact and forms the basis for determining the existence of rights and legal relationships between parties (Eka Wahyuni, Rahman, & Risma, 2022).

From a theoretical standpoint, scholars such as Sudikno Mertokusumo distinguish between authentic deeds and private deeds. An authentic deed, drawn up by a competent public official, carries full evidentiary force. Conversely, a private deed's validity depends on acknowledgment by the parties. Within this framework, an electronic signature (TTE) is generally equivalent to a private deed, but may acquire authentic evidentiary value when it is issued and verified by an Accredited Electronic Certification Provider (PSrE), ensuring identity verification, data integrity, and non-repudiation (Fauzi, Rifai, & Shebubakar, 2024; Fitriani Irianti, Rahman, & Sahban, 2024). The assessment of evidentiary strength combines formal proof theory, emphasizing documentary form and procedural compliance, and material proof theory, which focuses on the substantive truth contained in the evidence. In the digital era, formal validity is reflected through electronic certificates, digital audit trails, and PSrE verification, while material validity depends on data integrity, metadata accuracy, and authentication of signers (Ilham et al., 2022). Such interpretation aligns with Articles 11–12 of the ITE Law, which outline the essential elements for electronic signatures to possess legal validity.

a. This framework is grounded on fundamental legal principles:
b. Legality Principle, requiring compliance with the ITE Law, the Civil Code, and relevant regulations.
c. Justice Principle, ensuring equal protection between electronic and physical documents.
d. Utility Principle, mandating the law to adapt to technological progress for societal benefit.
e. Proportionality Principle, balancing security requirements with accessibility for users.

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

Hence, the theory of evidentiary strength provides the analytical lens to assess the legal validity and probative power of electronic signatures within Indonesia's civil procedure (Lapian, 2024).

2.2. Law Enforcement Theory

Law enforcement refers to the process of realizing legal norms as tangible standards of conduct in social relations. In a broad sense, all legal subjects participate in upholding the law when they act according to legal norms; in a narrower sense, law enforcement is conducted by authorized institutions—courts, police, and prosecutors—to ensure rule compliance, even through coercive means when necessary (Nonet & Selznick, 2019). According to Phillip Nonet and Philip Selznick, a responsive legal system must enforce laws fairly, consistently, and adaptively to social changes. Lawrence M. Friedman further conceptualizes law enforcement as depending on three components: legal structure (institutions), legal substance (norms), and legal culture (values and public perception). Effective enforcement requires harmony among all three (Fauzi et al., 2024). Similarly, Soerjono Soekanto views law enforcement as translating legal ideals into reality through competent institutions.

Within the framework of electronic signature regulation, the substance of the law—the ITE Law and its amendments—exists, but the structure (institutional readiness and procedural mechanisms) and legal culture (public and judicial acceptance) remain underdeveloped. This mismatch explains why, despite the formal recognition of electronic signatures under Article 11 of the ITE Law, courts and administrative bodies often still require "wet signatures" for validation (Eka Wahyuni et al., 2022). This illustrates the gap between legal substance and legal culture that hinders effective law enforcement. In this context, the law enforcement theory becomes a tool to analyze how judges and legal officials interpret, verify, and apply digital evidence. The consistent enforcement of electronic signatures depends on technological literacy among law enforcers, standardized procedures for electronic verification, and updated judicial training.

2.3. Legal Compliance Theory

Legal compliance concerns the extent to which individuals or institutions consciously adhere to legal norms. Tom Tyler (1990) argues that obedience to the law is not merely driven by fear of sanctions but by perceived legitimacy, fairness, and trust in the legal system. Soerjono Soekanto distinguishes between instrumental compliance (based on fear of punishment) and normative compliance (based on belief in the law's justice and authority). In the context of electronic signatures, legal compliance is reflected in whether individuals, businesses, and government agencies implement certified digital signatures as required by the ITE Law and Government Regulation No. 71 of 2019. Despite clear provisions, resistance persists—many institutions still demand handwritten signatures or additional notarial verification (Devi Chintya Dewi et al., 2024). Such noncompliance indicates deficiencies in digital legal literacy, insufficient government socialization, and conservative legal culture (Ellya Rosana, n.d.). Legal compliance theory thus helps explain the behavioral dimension of why legal norms are not yet internalized despite their formal existence.

2.4. Theory of Legal Effectiveness

Soerjono Soekanto defines the effectiveness of law as the degree to which legal norms are observed and operational in society. Law is effective when it influences behavior consistently with legislative intent. Its effectiveness is determined by three interrelated elements: structure, substance, and legal culture (A. S. Utama, 2019). Applying this framework to electronic signatures, effectiveness depends on the clarity of regulations (ITE Law, PP 71/2019, Permenkominfo 11/2022), institutional capacity (availability of PSrE, verification systems), and public acceptance. Although electronic signatures have formal legal standing, effectiveness remains limited by inadequate infrastructure, technical understanding, and lingering judicial skepticism (Fauzi et al., 2024). The theory of legal effectiveness provides evaluative criteria for identifying

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

implementation barriers and suggests that achieving full effectiveness requires parallel improvements in legal institutions, public education, and technological adaptation.

2.5. Signature

Article 1(3) of Law No. 1 of 2020 on Stamp Duty defines a signature as a mark in the form of a name or initials used as a symbol of identity, including electronic signatures as regulated by the ITE Law. In linguistic terms, the Indonesian Dictionary (KBBI) defines a signature as a person's distinctive handwritten name. Tan Thong Kie (2007) views a signature as an expression of the signer's intent that the written statement beneath it be legally regarded as their own declaration. In legal and administrative practice, a signature functions not only as a personal identifier but also as authentication and consent, linking an individual's identity with their legal responsibility. Therefore, a valid signature—whether handwritten or electronic—is central to verifying the authenticity and enforceability of legal documents.

Article 1(12) of the ITE Law defines an electronic signature as electronic information attached to or associated with other electronic information used as a means of verification and authentication. Unlike traditional signatures, digital signatures use cryptographic algorithms that ensure the authenticity, integrity, and security of data (Pangaribuan et al., 2023). The legal basis of electronic signatures in Indonesia is primarily found in Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016, particularly Article 11. Additional frameworks include Government Regulation No. 71 of 2019 and Ministerial Regulation No. 11 of 2022, which classify electronic signatures into certified and non-certified categories and designate PSrE as the official certifying authority (Lapian, 2024). Electronic signatures serve three main legal functions: authentication (identity verification), integrity (ensuring the document remains unaltered), and non-repudiation (preventing denial of authorship). The technology promotes efficiency, security, and trust in electronic transactions across public and private sectors. The cryptographic process guarantees that even a minor alteration invalidates the signature, thereby ensuring evidentiary reliability (Devi Chintya Dewi et al., 2024).

Under Article 11(1) of the ITE Law, an electronic signature has full legal force if it fulfills six criteria: (a) exclusive linkage to the signer, (b) control over signing data, (c) detectability of alterations, (d) traceability of document changes, (e) identification of the signer, and (f) proof of consent. Verification typically involves PDF digital certificates validated through software such as Adobe Acrobat or PSrE platforms. Cryptographic hash functions ensure document integrity and authenticity by generating a unique digital fingerprint that immediately detects tampering (Pangaribuan et al., 2023). This mechanism offers superior reliability compared to manual signatures, which often require forensic examination. Consequently, electronic signatures strengthen evidentiary processes by offering automated, traceable verification standards.

2.6. Procedure for Examining the Validity of Electronic Signatures in Court

Under procedural law, the admissible forms of evidence in civil cases are enumerated in Articles 164 HIR, 284 RBg, and 1866 BW, while in criminal proceedings, Article 184 of the Criminal Procedure Code (KUHAP) governs the same. According to Article 5(1) and 16(1) of the ITE Law, electronic information and documents are recognized as valid evidence provided they are generated through secure electronic systems and meet the prescribed technical and legal standards. Electronic documents have evidentiary value equivalent to private deeds, provided that their authenticity is not disputed. When a dispute arises, the party contesting authenticity bears the burden of proof. Judges then evaluate based on both formal compliance (existence of digital certificates, timestamps, PSrE validation) and material integrity (unchanged content, traceable audit trail) (Ni Putu Riyani Kartika Sari & Dewi, 2020).

a. Practical assessment of an electronic signature's validity in court usually involves:
b. Certificate verification (authenticity, issuer, validity period, revocation status);

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

c. Identity correlation between signer and certificate holder;
d. Document integrity check (hash value and timestamp consistency);
e. Compliance with ITE and PSrE standards; and
f. Expert testimony in digital forensics when necessary (Fauzi et al., 2024; Fitriani Irianti et al., 2024).

This framework provides judges with objective guidelines to consistently determine the authenticity and evidentiary strength of electronic signatures in civil litigation.

III. Research Method

3.1. Research Type

This study adopts a normative legal research design—also called doctrinal or library research—which focuses on positive legal norms (both written and unwritten) as a coherent system of rules. Law is examined primarily as *das sollen* (what the law ought to be), rather than *das sein* (law in action). Accordingly, the analysis centers on statutes, jurisprudence, legal doctrines, and scholarly opinions, aiming to identify principles, norms, and their systematic relations (Soekanto, 2007; Soekanto & Mamudji, 2019; Marzuki, 2017; Ibrahim, 2021).

Within the normative design, the study employs several complementary approaches:

a. Statute approach: interpretation and systematization of the ITE Law, its amendment, and implementing regulations.
b. Conceptual/doctrinal approach: synthesis of concepts such as legal validity, evidentiary strength, authentication, integrity, and non-repudiation in electronic signatures.
c. Case/law approach (where available): reading of relevant court decisions to understand judicial construction of electronic signatures as civil evidence.
d. Analytical and comparative lens: where appropriate, horizontal comparisons across equivalent norms to detect congruence or conflict (Marzuki, 2017; Ibrahim, 2021).

3.2. Types and Sources of Legal Materials

The research uses three layers of legal materials:

a. Primary legal materials

Binding sources comprising the 1945 Constitution, laws and regulations (statutes, government regulations, presidential regulations, regional regulations), and other authoritative instruments (ministerial regulations/decisions). Where available, jurisprudence (court decisions) and treaties/private law contracts are also included. Core primary sources for this topic are:

1) Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) as amended by Law No. 19 of 2016;
2) Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions; and
3) Relevant ministerial regulations on electronic certification (PSrE).

b. Secondary legal materials

Scholarly interpretations that explain, critique, or systematize primary norms: monographs, journal articles, proceedings, and policy papers in the field of civil procedure, evidence, and cyber law (Salle, 2020; Qamar et al., 2017; Achmad Ali, 2012; Wiraguna, 2024; Ibrahim, 2021; Marzuki, 2017).

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

c. Tertiary legal materials

Auxiliary sources that clarify terms and assist retrieval—legal dictionaries, encyclopedias, and terminology guides—are used to ensure definitional precision and terminological consistency. Inclusion criteria are relevant to: (i) the validity of electronic signatures; (ii) evidentiary law in civil procedure; and (iii) interpretation of the ITE Law and its implementing regulations. Exclusion criteria remove non-legal technical sources unless they directly inform legal concepts (e.g., cryptographic integrity as it relates to legal validity).

3.3. Techniques for Collecting Legal Materials

Consistent with doctrinal design, materials are collected through library research (Soekanto & Mamudji, 2019; Salle, 2020):

a. Document retrieval: systematic searching of statutes, implementing regulations, and authoritative guidance; collection of court decisions where accessible.
b. Scholarly literature review: extraction from books, peer-reviewed journals, reputable proceedings, and institutional reports.
c. Authoritative databases and repositories: legislation portals and academic repositories (e.g., national legal information portals/JDIH, ministerial regulation repositories, university libraries, reputable journal databases).

To improve traceability and rigor, the study applies:

a. Search strings combining key terms (e.g., *electronic signature*, *validity*, *civil evidence*, *PSrE*, *non-repudiation*, *authentication*);
b. Source mapping (matrixing primary/secondary/tertiary materials to research questions); and
c. Documentation protocols (bibliographic management in APA 7th).

3.4. Analysis of Legal Materials

Analysis is qualitative and normative-analytical, emphasizing legal reasoning and interpretive methods rather than statistics (Marzuki, 2017; Ibrahim, 2021):

a. Interpretation and systematization
   1) Grammatical, systematic, and teleological interpretation of statutory provisions, especially Article 11 of the ITE Law and provisions in PP 71/2019, to ascertain the legal construction of electronic signatures (validity criteria, evidentiary consequences).
   2) Vertical synchronization (hierarchical coherence among the Constitution, laws, and regulations) and horizontal synchronization (consistency across norms at the same level) to detect harmony or conflict (Ibrahim, 2021).
b. Doctrinal synthesis
   1) Integration of scholarly doctrines on evidentiary strength (authentic vs private deeds), authentication, integrity, and non-repudiation to frame how electronic signatures fit into civil evidence theory (Achmad Ali, 2012; Qamar et al., 2017).
c. Prescriptive reasoning
   1) Beyond description, the analysis is prescriptive, formulating legal solutions/recommendations (e.g., verification standards in court, handling of disputes over authenticity, alignment of procedural guidance with PSrE practice) derived from the normative findings (Marzuki, 2017).

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

Where judicial decisions are examined, case synthesis is performed to identify patterns of judicial reasoning and their congruence with statutory standards. Where doctrinal debates arise, argumentative weighing (balancing principles of legality, justice, utility, and proportionality) is applied to propose coherent resolutions.

3.5. Operational Definitions

To avoid ambiguity, the study adopts the following operational definitions:

a. Law – A system of social rules prescribing human behavior, articulated through experience and observation, and formalized in binding norms (cf. Soekanto, 2007; Soekanto & Mamudji, 2019).
b. Legal validity – The status of a rule/act as binding and effective within Indonesia's legal order, typically evidenced by codification in written instruments (laws, regulations, circulars) and conformity with hierarchical and procedural requirements.
c. Signature – A person's distinctive mark (name/initials) affixed to a document as identification, authentication, and consent, functioning to attribute responsibility for its contents.
d. Electronic signature – Under ITE Law, electronic information attached to/associated with other electronic information used for verification and authentication; in practice, commonly implemented through digital signatures employing cryptography.
e. Legal force (kekuatan hukum) – The binding capacity of a norm or decision to create legal consequences and be enforceable against subjects of law.
f. Civil proof (pembuktian perdata) – The presentation of legally admissible evidence by litigants to persuade the judge regarding facts in dispute, thereby providing a foundation for judgment (Achmad Ali, 2012).
g. Legal compliance – Societal commitment and fidelity to prevailing legal norms as the "rules of the game," manifested in actual obedience based on legitimacy and/or sanction (Soekanto, 2007).
h. Legal effectiveness – The extent to which legal norms operate in practice (*law in action*) rather than merely on the books, reflecting influence on behavior and institutional practice (Soekanto & Mamudji, 2019).
i. Proof (pembuktian) – The body of rules on means of proof (admissible evidence and its use) aimed at attaining judicially acceptable truth through decisions or orders (Achmad Ali, 2012).

IV. Results and Discussion

4.1. Legal Regulation on the Validity of Electronic Signatures in Indonesia's Civil Law System

The legal validity of electronic signatures (ES) in Indonesia's civil law derives from Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was later amended by Law No. 19 of 2016 and the Second Amendment, Law No. 1 of 2024. These instruments affirm that electronic signatures have the same legal force as handwritten signatures, provided that authentication and data integrity requirements are met. Article 1, paragraph (12) of the ITE Law defines an electronic signature as electronic information attached to or associated with other electronic information used as a means of verification and authentication. Article 11 further specifies six validity requirements: (a) the signature must be uniquely linked to the signer; (b) the signer must retain control of signing data at the time of signing; (c) any alteration to the signature or associated information must be detectable; (d) there must be a method to identify the signer; and (e) a method to show that the signer has consented to the related information. These provisions embody the principle of functional equivalence, which ensures that electronic and manual signatures produce identical legal consequences (Lapian, 2024).

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

Further detail is provided by Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, which distinguishes between certified and non-certified electronic signatures. Certified electronic signatures, issued by a licensed Electronic Certification Provider (PSrE), carry higher evidentiary value because they guarantee signer identity, authenticity, and non-repudiation. This regulation closes interpretive gaps and positions electronic signatures firmly within both civil and administrative frameworks (Indonesia, 2019). Judicial recognition is reflected in Supreme Court Regulation (PERMA) No. 1 of 2019 on electronic court administration, later strengthened by PERMA No. 7 of 2022. These judicial instruments affirm that electronic documents and signatures are admissible as written evidence, provided their authenticity can be verified and is free from manipulation. From the perspective of civil law, this represents a paradigm shift from a paper-based evidentiary model to a digital-based one (Haklainul Dunggio, 2025). Although formally valid, the practical application of electronic signatures is still uneven. Institutions such as the National Land Agency (BPN) and the State Assets and Auction Service Office (KPKNL) have adopted electronic signing systems, but usage across the judiciary and among the public remains limited. This indicates that while the legal framework is complete, its implementation is partial. Nevertheless, courts have recognized electronic signatures as valid instruments of proof equivalent to handwritten ones, marking significant progress in the modernization of Indonesia's legal system (Hasan, Rizqy, & Putra, 2025).

4.2. Legal Provisions Governing the Examination of Electronic Signatures as Evidence in Civil Proceedings

Electronic signatures constitute a legitimate means of evidence under Articles 5 and 6 of the ITE Law, provided that the information they contain can be accessed, displayed, and verified for integrity. These provisions position electronic documents as legal equivalents to written ones (Indonesia, 2008). The process of examining the authenticity of electronic signatures in civil cases generally involves three aspects:

a. Integrity verification – ensuring that no alteration occurred after signing.
b. Authentication – confirming the signer's identity and control of signing data.
c. Non-repudiation – guaranteeing that the signer cannot deny having signed the document.

Courts evaluate electronic evidence by reviewing certification data, validity periods, and revocation status, often relying on the PSrE verification framework. If manipulation or forgery is suspected, judges may call digital forensic experts. Empirical data from the Makassar District Court show that judges consistently accept electronic signatures as legitimate evidence, provided legal and technical requirements are satisfied (Haklainul Dunggio, 2025). The functional equivalence principle, as adopted from the UNCITRAL Model Law on Electronic Commerce (1996), ensures that electronic and physical evidence are treated with equal evidentiary value. The Indonesian judiciary's approach mirrors this principle, recognizing that authenticity, not physical form, determines the strength of evidence (Rahardjo, 2021). Thus, the admissibility of electronic signatures in court aligns with both national legal doctrine and international standards. Although technical verification is rarely performed directly by judges, the legal assessment focuses on compliance with statutory provisions, ensuring authenticity and integrity.

4.3. Relevance of Theoretical Frameworks to Research Findings

a. Evidentiary Strength Theory

The findings confirm that electronic signatures possess the same evidentiary power as handwritten signatures, consistent with Article 11 of the ITE Law and PERMA No. 1 of 2019. Judges assess electronic signatures not merely by form but by their ability to provide material truth and judicial conviction. This shift reflects a modern evidentiary paradigm where substantive reliability outweighs physical formality (Rahardjo, 2021).

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

b. Law Enforcement Theory

According to Friedman's (1975) model, effective law enforcement depends on the harmony between structure, substance, and legal culture. In the case of electronic signatures, the structure (regulations and institutions) and substance (legal norms) are well established. However, the legal culture—including public trust and digital competence among legal actors—remains the weakest component (Soekanto, 2005; Setiawan, Nugraha, & Srihandayani, 2022). Thus, improving judicial training and public digital literacy is crucial to effective implementation.

c. Legal Compliance Theory

Compliance with electronic signature regulations depends on societal perception of legitimacy and fairness. The study shows that while legal professionals generally accept electronic signatures, segments of the public still doubt their reliability. Such skepticism often stems from the perception that manual signatures are "more real." This reveals a gap between normative recognition and sociological acceptance (Ahmad, Hasan, & Umar, 2023). Strengthening compliance requires continuous public education and transparent certification procedures (Friedman, 1975).

d. d. Legal Effectiveness Theory

Following Soekanto's (2005) framework, the effectiveness of a law is measured by its ability to function in society. Although Indonesia's statutory framework for electronic signatures is robust, implementation is hindered by technological and human-resource constraints. Adoption remains sectoral—apparent in BPN and KPKNL—but uneven across other institutions. Achieving full legal effectiveness demands integration between normative clarity, institutional capacity, and technological readiness (Utami et al., 2024).

The results demonstrate that Indonesia's judiciary has successfully integrated electronic signatures into civil procedure, confirming their legal and evidentiary validity. Judges now consider digital documents equivalent to physical ones, signaling modernization within legal practice. However, obstacles remain: infrastructural disparities, uneven institutional adoption, and limited public trust. These findings emphasize the need for continuous harmonization between law, technology, and culture to ensure the long-term success of electronic legal transformation.

V. Conclusion

The results of this research affirm that electronic signatures (ES) have attained a solid and legitimate position within Indonesia's civil law system, signifying a paradigm shift in how legal validity and evidentiary authenticity are conceptualized in the digital age. The formal recognition of electronic signatures through Law No. 11 of 2008 on Electronic Information and Transactions, reinforced by its amendments in Law No. 19 of 2016 and Law No. 1 of 2024, and further operationalized by Government Regulation No. 71 of 2019 and the Supreme Court Regulations (PERMA No. 1 of 2019 jo. PERMA No. 7 of 2022), illustrates that the Indonesian legal framework has transitioned from a rigidly formalistic model toward one that embraces technological adaptability. This transformation reflects a critical theoretical development: the embodiment of the principle of functional equivalence, in which digital acts are granted the same legal consequences as physical ones. Theoretically, this finding contributes to the evolution of legal thought concerning the nature of authenticity, consent, and proof within an increasingly dematerialized context of legal relations. The law is no longer confined to tangible instruments but is expanding toward a logic of digital objectivity, where cryptographic mechanisms, system integrity, and secure identification substitute the sensory and manual indicators once deemed essential to validity. The empirical confirmation that courts—particularly the Makassar District Court—now recognize the evidentiary power of electronic signatures underlines the gradual operationalization of the theoretical principle that legality lies not in the medium, but in the method of verification. In this respect, Indonesia's legal system demonstrates an adaptive capacity that aligns with

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

international standards, particularly the UNCITRAL Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures (2001). Theoretically, the study strengthens the notion that the evolution of digital law must not only focus on norm creation but also on epistemic legitimacy—how actors internalize, interpret, and operationalize technological norms within the socio-legal environment. Hence, the recognition of electronic signatures in Indonesia can be regarded as both a legal and epistemological reform: it reshapes the boundaries of proof, trust, and consent within civil law traditions that historically relied on physical evidence and ocular certainty.

From a managerial and policy-oriented perspective, the research underscores that the transition from formal legitimacy to practical effectiveness remains an ongoing challenge within Indonesia's legal and administrative apparatus. The study reveals that while the legal infrastructure supporting electronic signatures is complete and coherent, its implementation across institutions remains uneven, largely due to disparities in technological infrastructure, human resource competencies, and digital literacy among both public officials and society. This inconsistency produces a duality within Indonesia's legal practice—a coexistence of digital legitimacy and analog reliance. Therefore, the managerial implication of this research is the urgent need for a strategic institutional roadmap to unify the procedural adoption of electronic signatures across all state entities, ensuring that regulatory harmonization is accompanied by operational readiness. Government agencies such as the National Land Agency (BPN) and the State Asset and Auction Service Office (KPKNL) exemplify successful cases of digital integration; however, their models must be expanded horizontally to judicial institutions and other administrative bodies. The judiciary, in particular, stands as a crucial manager of legal transformation. It must strengthen its technical verification capabilities, including the capacity to evaluate cryptographic authenticity and electronic certification processes, not merely through external experts but through internal institutional expertise. This necessitates ongoing training programs, certification of judicial officers in electronic evidence examination, and integration of PSrE (Electronic Certification Provider) verification systems into court information infrastructures. From a governance standpoint, the managerial implication extends further toward the creation of cross-sectoral synergy between the Ministry of Communication and Informatics, the Financial and Business Sectors, and the Judiciary. These entities should collectively establish clear and interoperable standards for authentication, storage, and verification, ensuring that the legal process remains technologically consistent across domains. In this sense, the study's findings provide a managerial blueprint for fostering institutional resilience and trust in digital legal operations. When electronic processes are managed with transparency, uniformity, and robust technological safeguards, the legitimacy of digital governance itself becomes a function of managerial discipline as much as of normative authority.

Beyond administrative and procedural implications, this study holds profound significance for the theoretical development of legal sociology and digital compliance culture. Drawing from Friedman's triadic framework of law—structure, substance, and legal culture—the research demonstrates that Indonesia has successfully developed structural and substantive elements but continues to face challenges at the cultural level. Legal transformation requires more than regulatory innovation; it demands the cultivation of social belief systems that regard technology as a legitimate mediator of justice. The theoretical implication here is the redefinition of legal consciousness in the digital age, wherein public confidence in legal mechanisms depends not only on formal rules but also on perceptions of technological security, fairness, and accessibility. Building such consciousness necessitates a sustained process of social learning and habituation, wherein digital trust becomes an intrinsic part of the rule-of-law culture. From a managerial viewpoint, this insight translates into the necessity of public education and continuous legal socialization regarding electronic signatures. Policymakers and educators must embed digital law literacy within national curricula, professional training, and public campaigns, highlighting the equivalence and safety of electronic transactions. This will narrow the gap between normative recognition and sociological acceptance, enhancing compliance through knowledge rather than coercion. In the long term, as the legal ecosystem matures and digital literacy becomes normalized, Indonesia's civil justice system will evolve toward a technologically synchronized model of adjudication, characterized by transparency, efficiency, and accessibility. Thus, the study concludes that the

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

integration of electronic signatures in Indonesia is not merely a regulatory reform but a comprehensive transformation encompassing epistemic, structural, and cultural dimensions of law. Theoretically, it broadens the understanding of legitimacy in a digital society, and managerially, it offers a concrete roadmap for strengthening institutional capability, social trust, and systemic efficiency in the governance of digital legal processes.

References

Achmad, A. (2012). *Asas-asas hukum pembuktian perdata.* Jakarta: Kencana Prenada Media.

Ahmad, S., Hasan, A., & Umar, M. (2023). Kepatuhan terhadap hukum (sebuah perspektif filsafat hukum). *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory, 1*(4), 930–944.

Amelia Intan Saraswati, A., et al. (2023). Keberlakuan tanda tangan elektronik pada dokumen negara. *UNES Review, 6*(1). https://doi.org/10.31933/unesrev.v6i1

Devi Chintya Dewi, D., et al. (2024). Electronic signatures as a legal solution for contracts in Indonesia's digital era. *LETTERLIJK: Jurnal Hukum Perdata.* https://doi.org/10.25134/jise.v1i2.xx

E., & Isworo, A. S. (2022). Evidence instruments in judicial process: Ensuring justice and legal certainty (pp. 210–225).

Eka Wahyuni, E., Rahman, S., & Risma, A. (2022). Validity of digital signatures in civil law and the ITE Law. *Journal of Lex Generalis (JLS), 3*(5).

Ellya Rosana. (n.d.). Legal compliance is a manifestation of legal awareness in society.

Faulina, J., Barkatullah, A. H., & Gozali, D. S. (2022). Article 16, paragraph (1) letter f, article 54. *Prosiding Universitas PGRI Madiun, 1*(2).

Fauzi, I., Rifai, A., & Shebubakar, A. N. (2024). Potensi masalah hukum dalam tanda tangan elektronik dalam pembuktian hukum acara perdata Indonesia. *Jurnal Bedah Hukum, 8*(1), 124–144. https://doi.org/10.36596/jbh.v8i1.1047

Fauzi, I., Rifai, A., & Shebubakar, A. N. (2024). Potential legal issues in electronic signatures under Indonesia's civil procedure law. *Jurnal Bedah Hukum, 8*(1), 124–144. https://doi.org/10.36596/jbh.v8i1.1047

Fitcanisa, J. D., & Azheri, B. (2023). Keabsahan tanda tangan elektronik pada akta notaris. *Sibatik Journal, 2*(5), 1449–1458. https://doi.org/10.54443/sibatik.v2i5.809

Fitriani Irianti, F., Rahman, S., & Sahban. (2024). The legal evidentiary power of digital signatures in government contracts. *Journal of Lex Philosophy (JLP), 5*(2).

Friedman, L. M. (1975). *The legal system: A social science perspective.* New York: Russell Sage Foundation.

Haklainul Dunggio. (2025). *Interview: Judge of Makassar District Court.*

Hasan, L. K., Rizqy, M., & Putra, S. (2025). Electronic contracts and e-signatures in Indonesia: Legal framework and challenges in the digital revolution. *Helium Journal of Health, Education, Law, Information, and Humanities, 2*(1), 178–185.

Hudzaifah, H. (n.d.). Keabsahan tanda tangan elektronik dalam pembuktian hukum acara perdata Indonesia.

Ibrahim, J. (2021). *Teori dan metodologi penelitian hukum normatif.* Malang: Bayu Media.

Ilham, D. H., et al. (2022). Keabsahan tanda tangan elektronik pada perjanjian jual beli barang dari perspektif hukum perdata. *Journal Petitum, 10*(2), 161–173. https://uit.e-journal.id/JPetitum

Indonesia. (2008). *Law No. 11 of 2008 on Electronic Information and Transactions.*

Indonesia. (2016). *Law No. 19 of 2016 (Amendment to the ITE Law).*

Indonesia. (2019). *Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions.*

Indonesia. (2024). *Law No. 1 of 2024 (Second Amendment to the ITE Law).*

Lapian, R. (2024). Regulation of electronic signatures under Law No. 19 of 2016 on information and electronic transactions. *Lex Privatum, 13*(1), 45–60.

Law No. 1 of 2020 on Stamp Duty.

Law No. 11 of 2008 on Electronic Information and Transactions (as amended by Law No. 19 of 2016).

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.

ISSN [Online]: 2808-2923

Law No. 1 of 2024 on the Amendment to the Electronic Information and Transactions Law.

Marzuki, M. (2017). *Penelitian hukum* (Rev. ed., Vol. 13). Jakarta: Kencana.

Maryam Hanum, S. (n.d.). *Penggunaan teknologi dengan sarana video konferensi dalam pembuatan akta.* Program Studi Magister Kenotariatan, Universitas Sumatera Utara.

Ministerial Regulation No. 11 of 2022.

Ni Putu Riyani Kartika Sari, N. P. R. K., & Ni Luh Putu Geney Sri Kusuma Dewi, N. L. P. G. S. K. D. (2020). The existence of *Positief Wettelijk Bewijstheorie* in civil evidence. *Journal Akses, 12.*

Nonet, P., & Selznick, P. (2019). *Responsive law* (Indonesian translation).

Pangaribuan, L. J., et al. (2023). Document authentication strategies using digital signatures with the Schnorr algorithm. *KLIK: Kajian Ilmiah Informatika dan Komputer, 3*(4), 384–392.

Putri, W. S., & Budiana, N. (2018). Keabsahan kontrak elektronik dalam transaksi e-commerce ditinjau dari hukum perikatan. *Jurnal Akuntansi dan Hukum, 1*(2), 2620–3715.

Qamar, N., Syarif, M., Busthami, D. S., Hidjaz, M. K., Aswari, A., Djanggih, H., & Rezah, F. S. (2017). *Metode penelitian hukum (Legal research methods).* Makassar: CV Social Politic Genius (SIGn).

Rahardjo, S. (2021). *Hukum dan masyarakat digital: Pendekatan normatif terhadap transaksi elektronik.* Jakarta: Kompas.

Salle. (2020). *Metode penelitian hukum.* Makassar: CV Nas Media Pustaka.

Setiawan, P. J., Nugraha, X., & Srihandayani, L. (2022). Konsep penegakan hukum yang sistematis dalam perselisihan pra-yudisial di Indonesia. *Jurnal Hukum Ius Quia Iustum, 29*(1), 68–92.

Slamet, T. S., & Paliling, M. M. (n.d.). Kekuatan hukum transaksi dan tanda tangan elektronik dalam perjanjian.

Soekanto, S. (2005). *Faktor-faktor yang mempengaruhi penegakan hukum.* Jakarta: Rajawali Pers.

Soekanto, S. (2007). *Penelitian hukum normatif: Suatu tinjauan singkat.* Jakarta: RajaGrafindo Persada.

Soekanto, S., & Mamudji. (2019). *Penelitian hukum normatif: Suatu tinjauan singkat.* Jakarta: Rajawali Pers.

Supreme Court Regulation No. 1 of 2016 on Mediation Procedure.

Supreme Court Regulation No. 1 of 2019 on Electronic Case Administration and e-Litigation (as amended by PERMA No. 7 of 2022).

Tan Thong Kie. (2007). *Studi notariat: Beberapa mata pelajaran dan serba-serbi praktek notaris* (Vol. 1).

Tanti Kirana Utami, T. K., et al. (2024). Pengaruh teori perundang-undangan terhadap dinamika norma hukum dalam sistem hukum Indonesia. *Jurnal Hukum Ius Publicum, 5*(2), 265–293.

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

Utama, A. S. (2019). Public trust toward law enforcement in Indonesia (pp. 306–313).

Wiraguna, S. A. (2024). Normative and empirical methods in legal research: An exploratory study in Indonesia. *Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum, 3*(3).

2025. The Author(s). This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license.