ENFORCEABILITY OF ELECTRONIC DOCUMENTS: AUTHENTICATION AND APPLICABILITY OF ELECTRONIC SIGNATURE

M Sanjana, School of Law (Christ Deemed to Be University)

ABSTRACT

The central aim of this paper is to examine the enforceability, and authentication of electronic documents and signatures in India, with particular reference to the Information Technology Act, 2000. The research addresses challenges like judicial ambiguities and procedural difficulties stemming from differing evidentiary standards for electronic and digital signatures. The study clarifies the distinction, noting that electronic signatures are a broad legal category, while digital signatures are a more secure, cryptography-based subset. The methodology involves a close examination of statutory definitions, procedural hurdles, and a comparative study of the Indian system with international models like the EU's eIDAS Regulation and the US's ESIGN Act. This comparative approach highlights the contrast between technology-, neutral and technology-specific legal frameworks. The paper's findings reveal that while India's legal structure provides a foundation for digital transactions, it has failed to keep pace with rapidly evolving technologies. The heavy reliance on Public Key Infrastructure (PKI) for digital signatures has created legal uncertainty regarding the recognition of newer authentication techniques, such as biometrics and, blockchain-based mechanisms. These gaps in the law pose significant risks of fraud and disputes, which can undermine trust in the entire digital ecosystem. The paper concludes by recommending crucial reforms to the IT Act. It advocates for technology-neutral reforms and a specific legal framework for recognizing blockchain-based signatures. These changes are deemed critical for aiming digital trust and supporting secure, modern digital commerce in India.

Keywords: Electronic Signature, Digital Signature, Authentication, Enforcement of Document, Information Technology Act, 2002, Bharatiya Sakshya Adhiniyama, 2023.

1. INTRODUCTION

The increasing shift from paper to digital transactions has made the enforceability of electronic documents and authentication of electronic signatures a critical legal and commercial issue. This transaction highlights the need to understand how various legal systems, including India's Information Technology Act, 2000, handle different methods of electronic authentication and their specific requirements for evidence.[1]

The core of this issue lies in maintaining trust and integrity in digital transactions. As legal experts have observed, the move from traditional handwritten signatures to digital and electronic ones has created both theoretical and practical challenges for legal frameworks worldwide. In India, the legal framework, primarily based on the Information Technology Act, 2000, makes a crucial distinction between electronic and digital signatures. Each is governed by specific rules under laws like Indian Evidence Act and Bhartiya Sakshya Adhiniyama.[2]

Digital signatures are highly regarded in Indian law for their strong cryptographic security and legal presumptions of validity. They offer a different method of authentication. In contrast, electronic signatures are a broader category that includes various methods like biometrics and Aadhar-based systems. These methods have different levels of reliability and legal acceptance.[3]

The enforceability of an electronic document is directly linked to its authentication-the process of ensuring that a digital record is genuine and meets legal standards for reliability and admissibility. This concept is a key concern for Indian courts, which must evaluate both the authenticity and legal validity of electronic evidence. This presents procedural challenges that are similar to those faced by courts in other jurisdictions like European Union and the United States, where laws aim to balance technological innovation with security.[4]

With the rise of new technologies like Blockchain and artificial intelligence, India's legal system is facing new questions whether current methods of document authentication are sufficient. There is a growing need for legislative updates to address potential gaps and support continued digital trade. This research will explore these challenges, examining the legal enforceability of electronic documents and the evolving application of electronic signatures,

[1] Jane K. Winn, The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce, 37 Idaho L. Rev. 353, 353-425 (2001).
[2] Id.
[3] Amelia H. Boss, The Future Of Electronic Commerce: Article 2B, ECON, And UCITA, 16 J. MARSHALL J. COMPUTER & INFO. L. 263 (1998).
[4] Warwick Ford & Michael S. Baum, Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Prentice Hall Ptr (2001).

all while considering the impact of new technologies on the Indian legal system and its global role. [5]

This paper has a foundational shift of background from the paper-based to digital transactions, situating its analysis within the context of legal and commercial transformation in India as well as globally. This topic is especially relevant in the digital age where the enforceability of electronic documents and the authenticity of electronic signatures present both technological and legal challenges. The study seeks to understand in depth how legal systems-most notably India's are actively responding to the need for trust and integrity in digitally facilitated transactions, recognizing that traditional doctrines often fall short for addressing new realities shaped by technology.

This paper is needed because the accelerating reliance on electronic transactions exposes individuals and businesses to risks of fraud, tampering, and disputes if this legal frameworks for authentication and validation are lacking. While the Indian legal system recognises both electronic and digital signatures, each carries its own set of evidentiary standards and legal consequences, occasionally leading to ambiguities in judicial interpretations and procedural complexities for courts in establishing the credibility of electronic evidence. The evolving distinction-and overlap between these forms of signatures underscores the importance of clarifying the statutory requirements and ensuring the legal regimes remains clear, effective, and fair. Further, continuous developments in blockchain, AI, and other emerging technologies compel Indian law to re-examine and adapt its frameworks, so as digital trust, maintain security, and maintains sustainable digital trade within and across borders.[6]

Even though the Information Technology Act, 2000 formally recognize both of the signatures, the statement of problem lies in the ambiguities persist due to the differing evidentiary standards attached to each. These inconsistencies lead to complications in judicial interpretation and present procedural hurdles in providing the authenticity of digital evidence in court. Moreover, technological advancements such as blockchain and artificial intelligence are progressing faster than existing legal frameworks can accommodate, threatening to create vulnerabilities and legal mechanisms for authentication, the increasing reliance on electronic transactions expose users to higher risk and frauds, tampering and disputes. This paper is

[5] Benjamin Wright, The Law of Electronic Commerce: EDI, E-mail, and Internet: Technology, Proof, and Liability, 12 J. HIGH TECH. L. 45 (1996).
[6] A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Or. L. Rev. 49, 49-115 (1996).

worked for the major problem questioning; How does Indian law, as defined by the Information Technology Act, 2000, differentiate between Electronic Signatures and Digital Signatures, and what are the specific legal and evidentiary requirements for each? What are the legal requirements for an Electronic Document to be enforced and accepted as valid evidence in Indian courts? This includes a focus on the Procedural rules under the Indian Evidence Act and Bharatiya Sakshya Adhiniyama, 1982? How do Indian laws on Electronic Signatures and documents compare with legal frameworks in other countries, such as the European Union (eIDAS Regulation) or the United States (ESIGN Act), particularly concerning the legal weight and technology-specific requirements? How do new technologies like Blockchain and Artificial Intelligence impact the existing legal framework for electronic documents and signatures in India, and what legislative reforms are necessary to address the challenges and opportunities they present? The Bharatiya Sakshya Adhiniyam, 2023 has significantly enhanced and expanded the framework for presumptions regarding electronic records and digital signatures. BSA not only retains the concept of presumptions but strengthens them with more detailed provisions. BSA has expanded, refined, and modernized these presumptions with seven dedicated sections (Sections 81, 85, 86, 87, 90, 93) covering electronic evidence.[7]

The present study addresses this problem by closely analysing statutory definitions and requirements, examining procedural challenges, and evaluating whether current frameworks adequately handle the threats and opportunities posed by emerging technology. By clarifying legal standards and proposing targeted reforms, this paper aims to strengthen digital trust, close interpretative gaps, and support reliable, sustainable digital commerce in India and internationally. Under the concept of electronic signatures, how these applications online such as, Docusign, Adobe, SignNow, PandaDoc, Zoho, etc., support this concept of authenticity and enforceability is also challenged and its integration with Aadhar is also analyzed.

2. LEGAL FOUNDATIONS OF ELECTRONIC AND DIGITAL SIGNATURES IN INDIA

The regulation of electronic and digital signatures in India is mainly governed by the Information Technology Act, 2000 (IT Act), which establishes the legal basis for e-commerce and electronic transactions. This landmark legislation gave electronic records and signatures the same legal validity as traditional handwritten ones, adopting a technology-neutral stance

[7] Lorna Brazell, Electronic Signatures and Identities: Law and Regulation, Sweet & Maxwell (3rd ed. 2018).

by recognizing various forms of electronic signatures, while also prescribing a more secure variant known as the digital signature.[8]

Under the IT Act, an electronic signature is defined as the authentication of an electronic record by a subscriber using methods listed in the Second Schedule, and this includes digital signatures. This definition allows flexibility, as everything from typed names to advanced biometric methods may qualify as valid signatures.[9]

A digital signature, however, is a specialized and more reliable form of electronic signature. It is based on asymmetric cryptography and hash functions, where a pair of public and private keys ensures data security, integrity, and non-repudiation. Only licensed certifying authority (CAs), under the supervision of the Controller of Certifying Authorities (CCA), can issue such signatures in the form of a Digital Signature Certificate (DSC), which authenticates the user [10]

2.1. Defining and differentiating Electronic and Digital Signatures

In India, the Information Technology Act, 2000 draws a clear line between electronic signatures and digital signatures, a distinction essential for understanding their legal recognition and evidentiary weight. An electronic signature is a broad category covering multiple methods of verifying electronic records, such as biometrics, OPTs, or Adhar based authentication. Its primary role is to confirm its authenticity of its digital record and ensure it meets the legal thresholds of legal reliability and admissibility in judicial proceedings. The ability to confirm the signer's identity while detecting any tampering after execution. While electronic signature serves as effective authentication tool, their legal strength is tied to how well they satisfy of reliability. Under BSA, The Court shall presume that every electronic record purporting to be an agreement containing the electronic or digital signature of the parties was so concluded by affixing the electronic or digital signature of the parties. There is a clear differentiation done for digital and electronic.[11]

A digital signature, by contrast, is a specialized form of electronic signature that employs cryptographic techniques for stronger authentication. Created using asymmetric cryptosystems and hash functions, it typically operates within a Public Key Infrastructure (PKI). Indian law

[8] Information Technology Act 2000, No. 21, Acts of Parliament, 2000 (India).
[9] The Indian Evidence Act, 1872, No. 1 of 1872, India Code (1872).
[10] Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, Handbook of Applied Cryptography, CRC PRESS (1996).
[11] Whitfield Diffie & Martin E. Hellman, New Directions in Cryptography, 22 Ieee Trans. On Info. Theory 644 (1976).

accords high evidentiary value to digital signatures because of their robust security features and legal presumption of their validity. Amendments made by the information technology act, 2008 introduced the broader term "Electronic Signature" in some provisions while continuing to retain "Digital Signature" in other, causing some interpretive ambiguity. Nonetheless, the main difference lies in their technical design: digital signatures from a secure subset of electronic signatures. While electronic signatures range in reliability and applicability, digital signatures deliver a stringer, presumed-valid form of authentication. Courts, when examining electronic evidence, also carefully distinguish between authenticity (the inherent truth of a record) and authentication (the process of establishing that truth). [12]

Aspect	**Electronic Signature**	**Digital Signature**
Legal Provisions	Defined under Section 3A, IT Act, 2000 as any reliable electronic authentication method.	Defined under Section 3, IT Act, 2000 using asymmetric Cryptography and has functions.
Scope	Broad term- includes various authentication techniques.	Specific, secure sub-type of electronic signature.
Technology Used	Methods can include Aadhar e-sign, OPTs, Biometrics, click-to-sign, or typed names.	Based on Public Key Infrastructure (PKI) with a private-public key pair.
Security Level	Security varies depending on the method used; reliability depends on compliance with IT Act standards.	Very high security-ensures data integrity, authenticity, and non-repudiation through encryption.
Authentication Mechanism	Linker signer to document by simpler methods like OPTs or biometric verification.	Cryptographically binds signer to the document using digital certificates.
Proof and Evidentiary Value	Courts evaluate based on reliability of methods and potential for tampering. No automatic presumption of validity.	Legally presumed valid and genuine under the IT Act
Examples	Aadhar e-Sign (OTP-based), OPT validations, biometric scans, "I Agree" clickwrap actions.	Digital Signature Certificate (DSCs) such as Class 2 and Class 3, used for e-filing (IT

[12] Luciana Duranti & Kenneth Thibodeau, The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES, 35 ARCHIVAL SCI. 13 (2006).

		returns, MCA), e-tendering, e-bidding.

These terms are identified in IT Act and sometimes the meaning is interchanged, which has led to confusion. Studying these terms helps understand their precise legal scope. The enforceability of agreements signed electronically hinges on whether the signature meets the criteria of reliability under Section 3A or the stricter standards of Section 3. This distinction carries significant real-world consequences. [13]

This objective of differentiation is justified because it allows a focused yet comprehensive examination of the Indian legal framework at the intersection of law, technology, and evidence. By asking not just "what" the difference are but also "how" the law enforces and evaluates them, it encourages research for a better understanding. [14]

In a nutshell, an electronic signature is a big umbrella term, many formats are present along with flexibility. It is good for everyday contract and authentication, user agreements and Aadhar OTP. On the other hand, digital signatures are specialized, PKI, certificate based and all time secure for high-value transactions, tax filing, e-governance, corporate filings. [15]

2.2. Electronic Records/Documents: Admissibility and Procedural Standards

Be it Digital or Electronic, apart from this, such a procedure is executed on a document or on a record, the major problem arises whether the admissibility of such a document is possible, and if so, what are the procedural standards. In India, the admissibility of electronic records as evidence is governed primarily by the Indian Evidence Act, 1872, particularly section 65B, which is being replaced by section 63 of the Bharatiya Sakshya Adhiniyama, 2023. The legal framework also incorporates standards under the information technology act, 2000.[16]

The section 65B states that electronic records as documents and sets out procedural requirements for their admissibility in court. It mandates the production of a certificate issued by a responsible official certifying the authenticity of the electronic record. However, section 63 of the latest Act, introduces updated conditions and procedural standards for admissibility,

[13] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
[14] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, 2014 O.J. (L 257) 73.
[15] Lilian Edwards, Law, Policy and the Internet, Hart Publishing (2019).
[16] Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 et seq. (2000).

including certification of electronic records by a responsible party. New certificate types providing technical authentication, including hash values and device specifications. [17]

It is to be noted that, the electronic records must meet relevance, authenticity, non-tampering, and reliability criteria. A certificate of authenticity accompanying electronic records is mandatory where electronic evidence is tendered as a secondary evidence. The certificate should affirm the device's proper operation, regular use in lawful activities, and integrity of the data. Courts weigh factors such as the method of identity authentication, audit trails, and whether relevant security measures prevent tampering or not. [18]

Any electronic records, including emails, digital document, and computer outputs, are legally treated as documents if procedural standards are met. Admissibility requires proof of the integrity and authenticity of the electronic evidence through prescribed certification. Recent legislative updates emphasize stricter and clearer procedural standards to ensure accurate authentication. The legal regime is complemented by rules designed to protect data integrity, confidentiality, and non-repudiation.[19]

Indian law uses the tiered approach to the evidentiary weight of electronic signatures. While all electronic signatures that meet the IT Act's requirements are considered valid, secure digital signatures are given a higher standing. Secure digital signatures are considered "secure", the court presumes the document has not been altered and that the signature was affixed by the person who intended to sign it. This creates a strong legal presumption of authentication. Non -secure signatures, is not considered "secure", the party asserting its validity must prove that the signature belongs to the person claimed.

Exclusions and Inadmissible documents are also observed, to be executed electronically, requiring a physically or 'wet ink' signature.[20]

- Wills and testamentary documents.
- Trust deeds.
- Powers of attorney.

[17] Patricia Brumfield Fry, A Preliminary Analysis of Federal and State Electronic Commerce Laws, 37 Hous. L. Rev. 967 (2000).
[18] Thomas J. Smedinghoff, The Legal Risks of Accepting or Relying on Electronic Records and Signatures, 16 J. Marshall J. Computer & Info. L. 75 (1997).
[19] Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press (2018)
[20] Emma Ganne, Can Blockchain Revolutionize International Trade? World Trade Organization (2018).

- Documents related to real estate that require registration under Registration Act, 1908. [21]
- Negotiable instruments like promissory notes and bills of exchange.[22]
- Court documents and affidavits requiring attestation or notarization.

For any electronic document to be considered legally reliable and valid, it must meet these criteria:[23]

- The electronic signature must be uniquely linked to the person using it, and their identity should be verifiable through a trusted source.
- The person must have exclusive control over the signature key or the means of creating the signature
- Any changed made to the document after it has been signed must be detectable[24]
- The signature process must comply with the procedures and standards prescribed by regulatory bodies like the Controller of Certifying Authorities 9CCA0.[25]
- For a digital signature, it must be issues by a certifying authority (CA) licensed under the IT Act.

Judicial Perspective

In India, currently judicial pronouncements primarily address electronic signatures collectively with digital signatures and electronic records without separately distinguishing electronically affixed signatures. The law and courts recognize electronic signatures widely, but specific case law solely on non-digital electronic signatures remains under-reported. Hence, use of electronic signatures is well supported legally in India, even though landmark case laws naming electronic signatures distinctly are not commonly available in India's jurisprudence yet.[26]

In the case of *Anvar P V v. Basheer & Ors.,*[27] Spoke about the admissibility of electronic records and electronic signatures under the Indian Evidence Act, 1872, specifically the compliance requirements with section 65B. the court held that the section 65B of the Evidence Act constitutes a complete code in itself for the admissibility of electronic evidence and shall not

[21] Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305 (2017).
[22] · Dr. Shashirekha Malagi, Laws Governing Digital Signatures in India: An Overview, 12 Int'l J. Hum. & Soc. Sci. Invention 22, 22-28 (2023).
[23] Khush Bhachawat, Electronic Contracts in India: Challenges and Complexities, 4 Int'l J.L. Mgmt. & Human. 3502 (2021).
[24] Pavan Duggal, Cyberlaw: The Indian Perspective, Saakshar Law Publications (2016).
[25] Trimix International FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 SCC 1 (India).
[26] Arjun Panditrao v. Kailash Kushanrao, (2020) 7 SCC 135 (India).
[27] Anvar P V vs. Basheer & Ors., (2014) 10 SCC 473

be affected by other provisions of the Evidence Act. All the electronic signatures must comply with Section 65B requirements for court admissibility. The authentication process must meet the strict certification standards. No alternative methods of proving electronic signatures can substitute the Section 65B. it can be pointed that there is limited judicial discretion and cost and time implications such as certification process may increase transaction costs and processing time, potentially undermining the efficiency benefits of electronic signatures.

On the other case, *Trimix International FZE Ltd. V. Vedanta Aluminium Ltd.,*[28] this represents judicial courage in embracing digital transformation while maintaining contract law fundamentals. However, it highlights the need for complementary developments in digital authentication, cybersecurity frameworks, a clearer evidentiary standard for electronic communications. The central question being, whether a contract could be validly formed through electronic communications and whether such electronic contracts, including their arbitration clauses, were legally enforceable under Indian Law. There was an authentication gap, security vulnerabilities were limited, inconsistency with later precedents are sharply restrictive.[29]

3. INTERNATIONAL PERSPECTIVE AND TECHNOLOGICAL TRASFORMATIONS IN ELECTRONIC TRANSACTIONS

The global transition from traditional paper-based transactions to digital formats has created pressing concerns around the legal validity of electronic documents and digital signature verification across different jurisdictions. This transformation underscores the importance of examining how various legal frameworks-including those in India, the United States, and the European Union-address electronic authentication methods an establish their evidentiary standards.[30]

As technology continues to evolve, legal systems worldwide are reassessing their regulatory approaches to maintain the reliability and security of cross-border electronic transactions. Yet this digital evolution brings substantial obstacles, especially concerning the sustained preservation and verification of electronically signed documentation over time. The fundamental challenge stems from the varied regulatory philosophies adopted by different

[28] Trimix International FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 SCC 1 (India).
[29] Duranti, K., & Stanfield, A. (2021). "Authenticating electronic evidence". In S. Mason & D. Seng (Eds.), "Electronic evidence and Electronic Signatures" (CMB- Combined Volume, 5, University of London Press. (pp.236-278).
[30] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, India Code (2023).

nations-the European Union tends to implement technology-specific regulations, whereas the United States generally embraces a more flexible, technology-agnostic framework. While electronic signature technology has reached considerable sophistication, its uneven legal recognition and practical implementation across jurisdictions continues to highlight the critical need for building confidence and predictability in digital commerce environments.[31]

3.1. Comparative Perspectives on Legal Recognition of E-Signatures

European Union (EU)

The EU has implemented a technology-specific regulatory framework that centers predominantly on Public -Key Cryptography as the foundation for electronic signature validation. This approach was formalized through a comprehensive directive establishing a community-wide electronic signature framework, which was officially enacted on December 13, 1999. Despite this standardized technological foundation, the practical application of advanced electronic signatures faces significant complexities in terms f legal acceptance. Even when sophisticated cryptographic signatures are employed, achieving full legal recognition remains challenging across various transaction types and jurisdiction within the EU.

The directive's effectiveness is further constrained by varying national requirements across European member states. In numerous countries within the union, certain categories of transactions demand authentication methods that exceed the security level of traditional handwritten signatures. This creates a regulatory gap where the EU's technology-specific approach may not adequately address the heightened security and verification standards required for high-value or legally sensitive transactions. Consequently, while the European Union has established a unified technological standard through its focus on public-key cryptography, the practical implementation reveals inconsistencies in legal recognition and applicability. These limitations highlight the ongoing challenges of harmonizing digital signature regulations across diverse national legal systems, even within a coordinated regulatory framework like the EU directive system.

The European Union has developed an extensive regulatory structure goverming electronic signatures, entered around the SIRAS Regulation (Regulation (EU) No 910/2014). This comprehensive framework guarantees that electronic signatures maintain legal validity,

[31] Dr. John Varghese, Electronic and Digital Records under Bharatiya Sakshya Adhiniyama: Part V, Authentication of Electronic Records, KERALA JUDICIAL ACADEMY (2023).

security, and universal acceptance throughout all member nations, while establishing specific protocols and standards for implementation

Regulatory Frameworks of EU:

The cornerstone legislation in the KIDAS Regulation (EU No 910/2014), which took effect on July 1, 2016, creating unified standards for electronic identification and digital trust services within electronic commerce. This regulation superseded earlier legislative frameworks and provided clear legal definitions for electronic signatures, establishing their judicial equivalence to traditional handwritten signatures across every EU member state. [32]

EU digital identity wallet system, designed to enable citizens to securely manage their digital credentials and execute document signing processes using the most advanced security protocols available.[33]

This evolving regulatory landscape demonstrates the EU's commitment to maintaining technological leadership in digital authentication while ensuring consistent legal recognition across diverse national jurisdictions. The framework continues to adapt to emerging technologies and security requirements in the digital transaction environment.

eIDAS Classification System:

There are three distinct categories of electronic signature:

- Simple Electronic Signature (SES): Entry-level format offering basic security features with limited protection measures.
- Advanced Electronic Signature (AdES): Intermediate level providing strengthened security through cryptographic safeguards and signer verification capabilities.
- Qualified Electronic Signature (QES): Premium security tier that holds full legal equivalence to handwritten signatures, requiring certified Qualified Trust Service Providers.

These framework mandates specific standards for:

Authorized Qualified Trust Service Providers (TSPs) responsible for issuing QES certificates. Document authenticity verification through cryptographic hash algorithms. Certified

[32] Anil K. Jain, Ruud Bolle & Sharath Pankanti, Biometrics: Personal Identification in Networked Society, Springer (1999).
[33] D. Maltoni et al., Handbook of Fingerprint Recognition, SpringeR (2nd ed. 2009).

timestamping services to verify signing dates and maintain comprehensive audit records. Identity verification protocols ensuring signer authentication and preventing signature denial

Implementation Process:

- Determine Signature Level: Evaluate transaction sensitivity-apply SES for routine/low-value processes, reserve AdES or QES for critical legal/commercial documentation.[34]
- Select Certified Provider: For QES requirements, choose an approved TSP from the official EU Trust List.
- Complete Identity Confirmation: Implement robust verification procedures for AdES and QES, including government identification, biometric data, or digital certificates.
- Execute Digital Signing: Utilize eIDAS-compliant software or platforms meeting regulatory standards.
- Apply Timestamp Verification: Include certified timestamps from qualified authorities as signing evidence.[35]
- Maintain Secure Records: Store executed documents with comprehensive, verifiable audit documentation.
- Ensure International Recognition: Deploy eIDAS-compliant signatures for guaranteed legal acceptance across all EU jurisdictions.

Signature Type	Security Level	Legal Effect	Requirements
SES	Basic	Admissible, not always decisive	Minimal
AdES	Enhanced (Crypto)	Stronger, signatory identification	Cryptographic + Identification
QES	Highest (Qualified)	Legally equivalent to handwritten	Qualified TSP + Identification

EU Digital Identity Wallet- by November, 2026, will provide secure digital identity management and QES capability via smartphone apps will be implemented.

[34] Fiona Smith, Electronic Contracts: Ensuring Mutual Assent in a Digital Age, 56 CASE W. RES. L. REV. 47 (2005).
[35] Joshua A.T. Fairfield, Smart Contracts, Bitcoin Bots, and Consumer Protection, 71 WASH. & LEE L. REV. ONLINE 35 (2014).

United States (US)

The United States has adopted a flexible, technology-agnostic strategy for electronic signature regulation. The "Electronic Signature in Global and National Commerce Act" (E-Sign), passed in 2000, aimed to establish consistent legal standards for digital transactions nationwide.[36]

The E-Sign Act maintains technology neutrality by emphasizing the functional parity between electronic and conventional signatures rather than mandating specific technological methods. This approach allows for greater innovation and adaptability as new technologies emerge, without requiring legislative updates for each technological advancement. [37]

The legislation provides an expansive definition of electronic signatures, encompassing any sound, symbol, or process that is linked to a document and intentionally used or accepted by an individual as their signature. This broad interpretation includes various forms of electronic authentication, from simple typed names and scanned signatures to sophisticated cryptographic methods and biometric identifiers.

Unlike the European Union's more prescriptive framework, the U.S. system prioritizes functional outcomes over technical specifications. This philosophy reflects American preferences for market-driven solutions and minimal regulatory interference in technological development. The E-Sign Act's technology-neutral stance has facilitated widespread adoption of diverse electronic signature solutions across different industries and transaction types, while maintaining legal validity and enforceability in courts nationwide. [38]

The United States maintains a comprehensive legal structure for electronic signatures, built upon two fundamental legislative acts: the Electronic Signatures in Global and National Commerce Act (ESIGN Act, 2000) and the Uniform Electronic Transactions Act (UETA, 1999). These statutes establish the legal validity and enforceability of electronic signatures across most commercial and consumer transactions throughout the nation. [39]

Legislative Framework of US

ESIGN Act (2000): Provides electronic signatures with equivalent legal standing to traditional handwritten signatures in federal, interstate, and international commerce contexts. The act

[36] Ian Lloyd, Information Technology Law, Oxford University Press (8th ed. 2017).
[37] James B. Rule, Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience, Oxford University Press (2007).
[38] Jonathan Clough, Principles of Cybercrime, Cambridge University Press (2nd ed. 2015).
[39] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, Praeger (2010).

explicitly prevents the rejection of signature validity or enforceability solely based on its electronic format.[40]

UETA (1999): Implemented by 49 states and multiple territories, creating uniform legal recognition for electronic documents and signatures within state jurisdictions and domestic commercial activities.

New York operates under the Electronic Signatures and Records Act (ESRA), which serves an analogous purpose by establishing state-specific regulations for electronic signature implementation. These legislative frameworks mandate particular criteria including: demonstrable intent to execute signatures, explicit consent for electronic record usage, dependable signer identification methods, proper maintenance of executed documents, and appropriate security measures.

This multi-tiered approach ensures comprehensive coverage across different jurisdictional levels while maintaining consistency in electronic signature recognition and enforcement nationwide. [41]

Implementation Process

1. Obtain Electronic Consent: All parties must agree to utilize electronic signatures and records for the transaction, typically through formal disclosure agreements

2. Choose Signature Technology: Select the most suitable electronic signature format-basic, advanced, or digital based on legal exposure and authentication requirements.

3. Verify Signer Identity: Implement authentication protocols such as password verification, multi-factor authentication, digital certificates, or biometric confirmation to establish signer identity.

4. Document Signing Intent: Ensure the signing process clearly establishes the signer's deliberate intention to execute the document (through actions like clicking "I agree" or electronic signing on devices).

5. Protect Document Integrity: Apply tamper-detection mechanisms and preserve signed documents in accessible formats for future reference and auditing purposes.

[40] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press (3rd ed. 2011).
[41] NIST Special Publication 800-63B: Digital Identity Guidelines, Nat'l Inst. Of Standards & Tech. (2017).

6. Maintain Documentation: Store electronically signed document records in compliant systems throughout the mandated legal retention periods.

Law	**Coverage**	**Main Requirements**	**Key Exclusions**
ESIGN	Federal/Interstate/International	Consent, Intent, Authentication, Retention	Wills, certain Family Documents
UETA	State/Domestic Transactions	Consent, Intent, Authentication, Retention	Local Exclusions
ESRA	New York State-specific	Similar to UETA/ESIGN	Testamentary, Fiduciary documentation

India

India's regulatory structure, established under the Information Technology Act of 2000, provides official legal recognition for both electronic and digital signature formats, although certain regulatory uncertainties continue to erase interpretive challenges. The legislation criticists a close differentiation between basic electronic signatures and secure digital signatures, with the latter carrying significantly stronger legal presumptions regarding document authenticity and validity. This dual-tier approach reflects India's attempt to balance accessibility with security requirements in digital transactions. Simple electronic signatures offer broader applicability for routine transactions, while secure digital signatures provide enhanced legal protection through stronger authentication mechanisms and cryptographic safeguards. However, the framework's implementation has encountered practical difficulties due to ambiguous language with the statutory provisions. These uncertainties have occasionally resulted in confusion among legal practitioners, businesses, and technology providers regarding the specific requirements and applications of different signature types. The distinction between electronic and digital signatures, while conceptually clear sometimes creates operational challenges in determining which standard applies to particular transaction

categories. [42]

Despite these interpretive issues. India's Information Technology Act represents a significant step toward establishing comprehensive digital transaction governance. The legislation's recognition of varying signature security levels acknowledges the diverse needs of different commercial and legal contexts while providing a foundation for secure electronic commerce development within the Indian market. [43]

Legal Framework:

Information Technology Act, 2000 (IT Act): The principal legislation governing electronic signatures, digital signatures, and electronic records in India. [44]

- Section 3: Defines the process of affixing digital signatures using asymmetric cryptosystems and hash functions. [45]
- Section 5: Grants legal recognition to digital signatures for signing electronic documents.[46]
- Section 10A: Affirms the validity of electronic contracts formed through electronic means, including digital signatures.[47]
- Sections 35-39: Regulate Certifying Authorities (CAs), including licensing and Standards for issuing digital signature certificates. [48]

3.2. Types of Electronic Signatures in India

Simple Electronic Signatures: Scanned images, typed names, or ticks, which do not carry statutory presumptions of validity.[49]

Advanced/Qualified Electronic Signatures (AES/QES): Use Public Key Infrastructure (PKI) and are issued by licensed Certifying Authorities. Aadhaar eSign falls under this category and offers stronger legal standing.

Legal Presumptions: Digitally signed electronic documents using CA-issued certificates are

[42] Ramesh Cheripelli & Swathi Ch, Evading Signatures Validation in Digitally Signed Pdf, 8 Eng'g & Sci. Int'l J. 82 (2021).
[43] Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons (2000).
[44] Syed Asifuddin v. State of Andhra Pradesh, (2005) 10 SCC 247 (India).
[45] Jagjit Singh v. State of Haryana, (2006) 11 SCC 1 (India).
[46] Vikram Singh v. Union of India, (2015) 9 SCC 502 (India).
[47] Ministry of Electronics and Information Technology, Cyber Security Framework and Guidelines, Gov't Of India (2020).
[48] Reserve Bank of India, Master Direction on Digital Payment Security Controls, RBI/2021-22/67 (2021).
[49] E-Commerce and Development Report 2021, United Nations Conference On Trade And Dev. (2021).

presumed valid and equivalent to handwritten signatures in Indian courts.

Regulatory Oversight: The Controller of Certifying Authorities (CCA) governs standards, interoperability, and licensing of CAs.

Steps for Implementation

1. Parties must agree to use electronic signatures for the transaction or document.
2. Decide between simple, advanced (digital), or Aadhaar-based eSign, based on risk and statutory requirements.
3. Use mechanisms such as Aadhaar e-KYC, PAN e KYC, or Digital Certificate-based authentication issued by licensed Certifying Authorities.
4. Sign electronically via compliant platform/software using the selected method.
5. The signed document should be protected from alteration, with any changes being detectable, and records should provide an audit trail of signing events.
6. Maintain electronic records securely as required for statutory periods, ensuring traceability.
7. Documents signed with valid digital signatures are generally accepted by courts and government authorities for contracts, filings, and business transactions.

Law	Requirements	Legal Status	Key use cases
IT Act, Section 3, 5	Asymmetric Crypto, CA Certification	Equivalent to handwritten	Business, Government, Personal
Aadhaar e-sig	Aadhar e-KYC Authentication	Presumed Valid	Banking, Filings, Government
Evidence Act, Section 65B	Presumptions for Secure Records	Legislative Support	Court, Enforcement
BSA, Section 86	Secure Electronic Records/Signatures	Presumed Valid - Integrity & Authenticity Presumed	Court, Enforcement, Digital Transactions
BSA, Section 63	Certificate (Part A + Part B), Hash Value, Expert Certification	Legislative Support - Enhanced Requirements	Court Admissibility, Electronic Evidence

BSA, Section 85	Electronic/Digital Signature on Agreements	Presumed Validly Concluded	E-commerce, Digital Contracts
BSA, Section 87	Electronic Signature Certificate	Certificate Information Presumed Correct	DSC Validation, Court Proceedings
BSA, Section 90	Electronic Messages (Email)	Content Presumed Accurate, Sender Not Presumed	Email Evidence, Digital Communications
BSA, Section 93	Electronic Records 5+ Years Old	Presumed Authentic if Proper Custody	Historical Records, Legacy Documents

3.3. Technological Innovations and the Case for Legal Reform

a) Blockchain Technology: Revolutionizing Document Security[50]

Blockchain technology represents a paradigm shift in electronic document management, offering decentralized, immutable, and transparent solutions for digital transactions. Blockchain can provide a decentralized and tamper-proof ledger for electronic transactions, reducing risks of fraud and unauthorized alterations. The technology's distributed ledger system creates an unchangeable record of transactions, making it virtually impossible to alter or forge electronic documents without detection.[51]

The implications for electronic signatures are particularly significant. Blockchain-based signatures can provide:

- Immutable Time-Stamping: Every signature transaction receives a permanent timestamp that cannot be altered retroactively
- Enhanced Non-Repudiation: The distributed nature of blockchain makes it extremely difficult for parties to deny their signature actions
- Reduced Intermediary Dependence: Eliminates the need for traditional Certificate Authorities in some implementations

[50] Rodney D. Ryder, Guide to Cyber Laws, Lexisnexis (5th ed. 2018).
[51] Nandan Kamath, Law Relating to Computers, Internet and E-Commerce, Universal Law Publishing (4th ed. 2019).

- Cross-Border Compatibility: Potential for global signature recognition without complex international agreements.

b) Artificial Intelligence: Transformation Authentication Process

Al technologies are increasingly used for identity verification, fraud detection, and intelligent document processing *Anvar PV vs P.K. Hasbsst & Oza* [52] on 18 September, 2014. The integration of Al in electronic signature systems introduces sophisticated capabilities that can significantly enhance security and reliability:

Behavioural Biometrics: Al can analyse, signing patterns, keystroke dynamics, and mouse movements to verify signer identity

Fraud Detection: Machine learning algorithms can identify suspicious activities during the signing process

Document Integrity Analysis: Al can detect subtle alterations or manipulations in electronic documents

Identity Verification: Facial recognition and voice authentication powered by Al provide additional security layers

Automated Compliance Checking: Al can ensure signature processes comply with regulatory requirements

Intelligent Document Processing: Natural language processing can extract and verify key contract terms automatically

Risk Assessment: Predictive analytics can evaluate transaction risks in real-time

3.4. Critical Gaps in India's Legal Framework

Existing Legal Frameworks were designed for earlier technologies like digital signatures based on Public Key Infrastructure (PKI). The technological specificity creates several challenges:

Technological Obsolescence

The Act's definition of digital signatures is narrowly focused on asymmetric cryptography. Emerging authentication methods like biometrics, blockchain signatures, and Al-powered verification fall into legal grey areas. These laws do not fully encompass newer methods such

[52] Anvar P V vs. Basheer & Ors., (2014) 10 SCC 473

as Aadhaar-based signatures, biometrics, or blockchain signatures, leading to uncertainties and potential litigation risks.[53]

Evidentiary Challenges

Section 65B of the Evidence Act, as interpreted in *Anvar P.V. vs P.K. Basheer*,[54] may not adequately address blockchain-based evidence. Al-generated authentication reports lack clear legal status. Smart contracts and automated signature processes raise questions about human intent and capacity. While this case was decided under the regime of Section 65B of the Evidence Act, its core principle those electronic records are inadmissible without a mandatory certificate is preserved and even strengthened under Section 63 of the Bharatiya Sakshya Adhiniyam (BSA). The BSA effectively codifies the Anvar ruling by clarifying that the certificate is a "condition precedent" for admissibility, but it updates the process by allowing for two signatures (one by the owner/custodian and one by an expert) to handle increasingly complex data. In the context of your specific challenges, Section 63 of the BSA can be seen as a direct replacement for Section 65B, but it remains a "procedural bottleneck" for blockchain: because a blockchain has no single "person in charge" as envisioned by the Anvar logic or the BSA text, the requirement for a certificate remains the primary evidentiary hurdle for decentralized tech.

Cross-Border Recognition

International transactions using new technologies face recognition challenges. Lack of harmonized standards with global frameworks. Potential conflicts with foreign electronic signature laws

Comprehensive Legislative Reform Requirements

Legal Reform is necessary to provide clear definitions and standards for emerging electronic signature technologies. The scope of required reforms extends across multiple dimensions: Broader technology-neutral definitions, including technical standards integration. There can be training programs for judicial officers on emerging technologies, expert witness frameworks for technical testimony.

[53] Praveen Dalal, Cyber Law, Cyber Crime and Cyber Security: Global and Indian Perspectives, Legalservice India (2016).
[54] Anvar P V vs. Basheer & Ors., (2014) 10 SCC 473

Cross borders harmonization rules supporting interoperability and mutual recognition of electronic signatures. Innovation regulatory balance having risk-based regulation, privacy and security safeguards.

- **Specific Recommendations for India**
- In the span of 1-2 years an amendment to IT Act, 2000 to include technology-neutral electronic signature definitions, guidelines for blockchain-based signature recognition.
- Between 3-2 years, comprehensive revision of Evidence Act provisions for electronic evidence. Establishment of regulatory sandboxes for testing new signature technologies.
- Between 5-10 years, complete overhaul of electronic transaction legal framework, integration with global digital identity initiatives.
- The integration of blockchain and AI technologies into electronic signature systems represents both an unprecedented opportunity to enhance security and efficiency, and a significant challenge to existing legal frameworks. India's response to these challenges through comprehensive legislative reform will determine its position in the global digital economy and its ability to provide secure, reliable electronic transaction systems for businesses and citizens alike.

4. CONCLUSION

The research reveals that India's current legal regime for electronic documents and signatures, focused on the Information Technology Act, 2000, is struggling to adapt to swiftly advancing technologies such as blockchain and artificial intelligence. Although the Act establishes a foundation for digital dealings, its dependence on a narrowly defined, PKI-based digital signature mechanism creates significant legal ambiguity for modern authentication tools, including Aadhaar-driven systems and biometric methods. This absence of explicit legal recognition for newer technologies exposes the digital ecosystem to potential fraud, disputes, and diminished trust. Existing procedures-particularly the stringent requirements of Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. Section 63 now requires dual certification (Part A + Part B), mandatory expert opinion, and hash value submission, also present difficulties in admitting blockchain-derived evidence or Al-generated reports. Additionally, the lack of alignment with global standards complicates cross-border digital transactions involving emerging technologies.

To remedy these challenges, the paper recommends a phased program of reforms aimed at bolstering digital trust and fostering sustainable electronic commerce in India. In the near term

(1-2 years), amendments to the IT Act should introduce technology-neutral definitions for electronic signatures, establishing clear criteria for validating contemporary signature methods, including those based on blockchain. Over the medium term (3-5 years), The Bharatiya Sakshya Adhiniyam, 2023 has already updated the rules for electronic evidence through Section 63, but further amendments are needed to explicitly address blockchain-derived evidence and AI-generated reports, together with the creation of regulatory sandboxes to pilot and evaluate innovative signature technologies. Finally, in the long, term (5-10 years), a wholesale transformation of the legal framework is advised, emphasizing integration with global digital identity programs and harmonization of international rules for mutual recognition of electronic signatures. These measures are essential for equipping India's legal system to manage secure, trusted electronic transactions in the evolving digital global landscape.