Page: 251-271 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.160

A COMPARATIVE STUDY OF ELECTRONIC EVIDENCE ADMISSIBILITY: INDIA'S BHARATIYA SAKSHYA ADHINIYAM, 2023 VIS-A-VIS THE US FEDERAL RULES OF EVIDENCE AND THE EU EIDAS REGULATION

Mr. Shubh Gupta[1]

I. ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents a landmark legislative overhaul of India's law of evidence, replacing the Indian Evidence Act, 1872, with a framework ostensibly calibrated for the digital age. This paper undertakes a systematic comparative analysis of the electronic evidence admissibility regime under the BSA vis-a-vis two of the most developed and influential frameworks globally: the United States Federal Rules of Evidence (FRE) and the European Union's Regulation on Electronic Identification and Trust Services (eIDAS Regulation, 910/2014). Through doctrinal analysis and comparative legal methodology, the study scrutinises the conditions for admissibility, authentication standards, presumptive validity of electronic signatures, evidentiary weight accorded to electronic records, and cross-border recognition. The paper identifies three cardinal tensions. First, the BSA, despite reforms, continues to require rigid procedural certification (akin to the erstwhile Section 65B of the Indian Evidence Act, 1872) without fully embracing the flexible, process-based authentication models of the FRE. Second, while the eIDAS Regulation establishes a graduated trust hierarchy for electronic signatures with automatic evidentiary presumptions, neither the BSA nor the FRE has crafted a comparable statutory presumption of authenticity. Third, the cross-border recognition gap under the BSA remains acute when compared to the mandatory mutual recognition regime within the EU under eIDAS. The paper concludes with concrete suggestions for legislative reform, including adoption of a graduated authentication standard under the BSA, establishment of a statutory presumption

[1] B.A. LL.B. (H), 10th Semester, Student at Amity Law School, Amity University Madhya Pradesh (India).
Email: Shubh.gupta3@s.amity.edu

for certified electronic records, and India's accession to multilateral digital evidence treaties, to align India's evidentiary framework with international best practices.

II. KEYWORDS

Electronic Evidence, Bharatiya Sakshya Adhiniyam 2023, Federal Rules of Evidence, eIDAS Regulation, Comparative Law.

III. INTRODUCTION AND RESEARCH PROBLEM

The digitisation of commerce, governance, and interpersonal communication has fundamentally altered the landscape of legal evidence. Courts across jurisdictions today routinely encounter WhatsApp messages, emails, blockchain records, electronic contracts, cloud-stored data, and server logs as evidence. The critical question is not whether such evidence exists, but whether, and under what conditions, it may be admitted. This question is one of legislative architecture and judicial interpretation, and the answers vary markedly across jurisdictions.

India's response to this challenge culminated in the Bharatiya Sakshya Adhiniyam, 2023[2] (BSA), which came into force on 1 July 2024, replacing the Indian Evidence Act, 1872 (IEA). While the BSA consolidates and modestly expands the provisions on electronic records, its underlying architecture retains a certificate-centric, form-driven approach to admissibility that has long been criticised by scholars and practitioners alike. The foundational provision for electronic records, now embedded in Sections 57 to 63 of the BSA, is a descendant of Section 65B of the Indian Evidence Act, 1872[3] and the IEA's Section 65B, both of which generated decades of litigation culminating in landmark decisions such as *Anvar P.V. v. P.K. Basheer*[4] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*.[5]

[2]Bharatiya Sakshya Adhiniyam, No. 47 of 2023, ss. 57-63 (India).
[3]Indian Evidence Act, No. 1 of 1872, s. 65B (India) (since partially superseded by the BSA 2023 regime).
[4]Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
[5]Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

In contradistinction, the United States employs the Federal Rules of Evidence (FRE), particularly Rules 901 and 902, which adopt a flexible, relevance-and-reliability-based approach to authentication, supplemented by judge-made law that has evolved in tandem with technological change. The European Union, through the eIDAS Regulation, has constructed an entirely distinct paradigm: a trust-service-provider ecosystem with graduated categories of electronic signatures, each carrying different legal presumptions, and a robust cross-border mutual recognition mandate.

The research problem this paper addresses is threefold:

1. whether the BSA adequately addresses the contemporary challenges of electronic evidence admissibility;
2. how the BSA's authentication and admissibility regime compares with the flexible FRE model and the structured eIDAS framework;
3. what reforms, informed by comparative analysis, could strengthen India's legal response to digital evidence.[67]

A. Research Objectives

The present study is guided by the following objectives:

1. To examine the statutory framework for electronic evidence admissibility under India's Bharatiya Sakshya Adhiniyam, 2023, tracing its evolution from Section 65B of the Indian Evidence Act, 1872.
2. To analyse the authentication standards and judicial interpretations of the United States Federal Rules of Evidence as applied to electronic records, with particular reference to FRE Rules 901, 902(13), and 902(14).

[6] Fed. R. Evid. 901(b)(9) (U.S.); see also Fed. R. Evid. 902(13)-(14).
[7] 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] OJ L 257/73 (eIDAS Regulation).

3. To evaluate the EU eIDAS Regulation's trust service architecture, graduated electronic signature framework, and its evidentiary presumptions.
4. To conduct a structured comparative analysis of the three frameworks across key parameters: admissibility thresholds, authentication methods, electronic signature recognition, and cross-border evidentiary value.
5. To formulate evidence-based recommendations for legislative reform of the BSA's electronic evidence provisions.

B. Research Questions

This study is guided by a set of key questions aimed at understanding how well current legal frameworks handle the growing complexity of electronic evidence:

1. Does the certificate-based approach to admissibility under Sections 57–63 of the BSA effectively deal with modern challenges such as cloud computing, blockchain systems, and AI-generated records?
2. How does the more flexible approach under FRE Rules 901 and 902 compare with the BSA's strict certification requirements in terms of reliability and efficiency in handling electronic evidence?
3. The eIDAS Regulation introduces a layered trust framework—how does this translate into legal presumptions about electronic evidence, and could a similar model work within the Indian legal system?
4. Where does India's current legal framework fall short in recognising electronic evidence across borders, and how do the FRE and eIDAS systems address these international challenges?
5. What kind of legal, institutional, and judicial changes are needed to bring India's approach to electronic evidence in line with contemporary technological realities?

C. Research Hypotheses

The following hypotheses inform the research inquiry and are tested through comparative doctrinal analysis:

1. The BSA's certificate-centric approach to electronic evidence admissibility, while an improvement over the IEA, remains structurally inadequate compared to the process-based authentication model of the FRE.
2. The absence of a statutory presumption of authenticity for certified electronic records under the BSA creates an asymmetry with both the FRE's self-authentication provisions and the eIDAS Regulation's qualified electronic signature presumption.
3. India's cross-border electronic evidence recognition mechanism is significantly less developed than the EU's mandatory mutual recognition regime under eIDAS, creating practical barriers to international litigation and dispute resolution.

D. Research Methodology

This research adopts a doctrinal and comparative legal research methodology. The primary sources examined include the text of the Bharatiya Sakshya Adhiniyam, 2023; the United States Federal Rules of Evidence (as amended through 2023); and the EU eIDAS Regulation (No. 910/2014) together with Regulation (EU) 2024/1183 introduces a legally operative framework for interoperable European Digital Identity Wallets, enabling secure cross-border authentication and electronic trust services within the European Union. Indian Supreme Court and High Court decisions interpreting the admissibility of electronic records are analysed, alongside leading US federal court decisions on electronic evidence authentication and relevant European Court of Justice rulings.

The comparative methodology follows the functional approach: rather than comparing statutory text in isolation, the study identifies the functional problem each framework addresses (i.e., how to ensure the reliability and authenticity of electronic evidence) and

evaluates the adequacy of each framework's response. Secondary sources include law commission reports, academic commentary, and policy documents.[8]

The paper does not adopt an empirical methodology and does not conduct surveys or interviews. Where quantitative data is referenced (such as rates of electronic evidence disputes), these are drawn from secondary published sources. The analysis is primarily normative, with a view to generating reform recommendations.

E. Literature Review

The literature on electronic evidence admissibility in India has historically been dominated by analysis of Section 65B of the IEA and its judicial interpretation. Pavan Duggal's work on Indian cyber law provides a foundational doctrinal account of the IT Act's evidentiary provisions.[9] Shailendra Kumar Mishra's analysis of emerging challenges in electronic evidence highlights the structural limitations of the IEA's certification regime, particularly in the context of cloud-stored records and automated systems.[10]

The Law Commission of India's 269th Report (2017) identified critical gaps in India's electronic evidence law and recommended amendments to align the IEA with technological realities.[11] However, the Commission's recommendations were only partially absorbed into the BSA, leaving unresolved several structural problems, particularly around automated systems and server logs.

In the United States, the scholarship on electronic evidence authentication is voluminous. The seminal decision in *Lorraine v. Markel American Insurance Co.*[12] set out the comprehensive framework for authenticating electronic evidence under the FRE, examining each of the five requirements for admissibility in detail. George Paul and Jason

[8] Rama Raghuraman, 'Digital Forensics and Indian Courts: A Practitioner's Analysis' (2022) 54 JILI 187.
[9] Pavan Duggal, 'Cyber Law: The Indian Perspective' (Saakshar Law Publications 2014) ch. 8.
[10] Shailendra Kumar Mishra, 'Electronic Evidence in Indian Courts: Emerging Challenges' (2021) 63 JILI 214.
[11] Law Commission of India, '269th Report: Amendments to the Indian Evidence Act 1872 Pertaining to Electronic Evidence' (2017).
[12] Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).

Baron's scholarship on information management and legal systems provides a broader theoretical framing of the challenges posed by electronic evidence proliferation.[13]

On the EU side, the eIDAS Regulation has generated extensive literature on trust services and electronic signatures. Bird & Bird's analysis of the Regulation examines the legal effects of qualified electronic signatures and the cross-border recognition mechanism.[14] The European Commission's own evaluation report on the eIDAS Regulation (2021) acknowledges gaps in the original framework, particularly around electronic attestation and identity wallets, which eIDAS 2.0 seeks to address.[15]

There is a notable lacuna in comparative literature specifically examining BSA vis-a-vis the FRE and eIDAS. Existing comparative studies either focus on the IEA (now superseded) or adopt a binary comparison between India and one other jurisdiction. The present paper fills this gap by undertaking a systematic three-way comparison across a defined set of parameters, and by situating the analysis within the reform debates surrounding BSA implementation.

IV. RESEARCH AND ANALYSIS

A. The Bharatiya Sakshya Adhiniyam, 2023: Architecture of Electronic Evidence

1. Statutory Foundations and Section 65B's Legacy

The BSA's approach to electronic records is contained in Sections 57 to 63. Section 63 is the direct successor to the infamous Section 65 B of the IEA, establishing the conditions under which an electronic record may be admitted in evidence. The provision requires:

- The record was produced by a computer or electronic device;
- The device was in regular use during the material period;

[13]George L. Paul & Jason R. Baron, 'Information Inflation: Can the Legal System Adapt?' (2007) 13 Richmond JL & Tech 10.
[14]Olswang (now Bird & Bird), 'eIDAS Regulation: Trust Services and Electronic Identification' (2016) 32 CLSR 467.
[15]European Commission, 'eIDAS Regulation Evaluation Report' COM (2021) 290 final.

- The device was operating properly; and
- The information reproduced was regularly fed into the device.[16]

The requirement of a certificate from a responsible official under Section 63(4) has been the most litigated element of the prior regime. The Supreme Court's judgment in *Arjun Panditrao Khotkar*[17] settled the position that the certificate is a mandatory pre-condition for admissibility (not a mere rule of proof) but left open significant questions about who qualifies as a 'responsible official' in the context of cloud services or third-party platforms.

The BSA makes modest textual improvements: it explicitly includes data stored in cloud environments and devices linked to the internet and clarifies that the 'computer' generating the electronic record may include a combination of computers. Although *Shafhi Mohammad v. State of Himachal Pradesh*[18] briefly relaxed the mandatory requirement of a certificate under Section 65B of the Indian Evidence Act, 1872 in the interest of justice, this position was conclusively overruled by the Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, which reaffirmed the mandatory nature of the Section 65B certificate for admissibility of secondary electronic evidence. The BSA retains the certificate as the gateway to admissibility, without creating a judicial discretion to admit records on alternative authentication grounds.

2. Electronic Signatures and Presumptions

Sections 85A, 85B, and 85C of the IEA, which created rebuttable presumptions regarding electronic agreements, digital signatures, and electronic records from secure systems, are carried forward into the BSA in Sections 85 to 87. The BSA presumes that a digital signature affixed to an electronic record is valid if the signature certificate was issued by a licensed Certifying Authority under the IT Act. However, the presumption does not

[16]Bharatiya Sakshya Adhiniyam, 2023, s. 63.
[17]Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, per Nariman J., para. 63.
[18]Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal overruled Shafhi Mohammad v. State of Himachal Pradesh.

extend to non-digital electronic signatures or to signatures issued by foreign certifying authorities.[19]

This creates a significant gap: electronic records authenticated using non-PKI methods (such as behavioural biometrics, one-time passwords, or blockchain-based attestation) are not covered by any statutory presumption and must be authenticated through oral evidence or the certificate route under Section 63. This gap becomes particularly acute in cross-border transactions involving parties from jurisdictions with different signature standards.

B. The US Federal Rules of Evidence: Process-Based Authentication

1. The Authentication Standard under FRE 901

The FRE do not create a separate code for electronic records. Instead, electronic evidence is subject to the same authentication requirements applicable to all evidence: under Rule 901(a), the proponent must produce 'evidence sufficient to support a finding that the item is what the proponent claims it is.' Rule 901(b)(9) specifically provides for the authentication of electronic processes by evidence describing the process or system and showing that it produces an accurate result.[20]

This flexible standard has been applied by courts in diverse contexts. In *Lorraine v. Markel*[21], Judge Grimm articulated a five-part framework governing admissibility of electronically stored information consisting of:

- relevance;
- authenticity;
- hearsay compliance;
- compliance with the original writing rule; and

[19]Syed Asifuddin v. State of Andhra Pradesh, (2005) Cri LJ 4314 (AP HC).
[20] Fed. R. Evid. 901(a); Fed. R. Evid. 901(b)(9).
[21] Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).

- whether the probative value of the electronically stored information is substantially outweighed by dangers identified under Federal Rule of Evidence 403, including unfair prejudice, confusion, or needless presentation of cumulative evidence.

Critically, no certificate from a designated official is required. The authentication burden is satisfied by circumstantial evidence, testimony from persons with knowledge, expert evidence on digital forensics, or distinctive characteristics of the record.

2. Self-Authentication under FRE 902(13) and 902(14)

The 2017 amendments to the FRE introduced Rules 902(13) and 902(14), providing for the self-authentication of electronic records through hash value certification by a qualified person. Under Rule 902(14), a proponent may self-authenticate electronic data copied from an electronic device, storage medium, or file through a written certification that identifies the hash value and attests to the record's integrity.[22]

This innovation is significant for comparative purposes: the FRE has effectively built a technical, hash-based authentication mechanism into the rules of evidence without mandating a specific institutional certification authority. The 'qualified person' under Rule 902(14) may be any person with appropriate training or expertise, not necessarily an officer of a government-licensed body.[23]

The judicial application of this standard has, however, generated inconsistency. In *United States v. Vayner*[24] the Second Circuit emphasised that authentication of social media evidence requires more than a screenshot: the proponent must demonstrate that the page and its contents are attributable to the alleged author. Similarly, in *State v. Eleck*[25], the

[22]Fed. R. Evid. 902(14).
[23]Seth Schoen, 'Hash Functions and Digital Fingerprints: Primer for Legal Practitioners' (2019) 35 Santa Clara Computer & High Tech LJ 1.
[24]United States v. Vayner, 769 F.3d 125 (2d Cir. 2014).
[25]State v. Eleck, 23 A.3d 818 (Conn. App. Ct. 2011).

court declined to admit Facebook messages solely on the basis of the printout, requiring independent corroboration.

C. The EU eIDAS Regulation: Trust Hierarchy and Presumptive Validity

1. The Three-Tier Signature Architecture

The eIDAS Regulation establishes three categories of electronic signature: the Simple Electronic Signature (SES), the Advanced Electronic Signature (AdES), and the Qualified Electronic Signature (QES). Each tier carries progressively stronger legal presumptions.[26]

Under Article 25(2) of the eIDAS Regulation, a Qualified Electronic Signature 'shall have the equivalent legal effect of a handwritten signature.'[27] This creates an irrebuttable presumption of validity at the highest tier: a QES affixed to an electronic document establishes, without further evidence, that the document was signed by the identified signatory and has not been altered since signing. This is qualitatively different from both the BSA's conditional presumption (which applies only to PKI-based digital signatures from licensed Indian CAs) and the FRE's case-specific authentication approach.

2. Cross-Border Recognition and Mutual Recognition

Article 25(3) of the eIDAS Regulation mandates that Member States shall not deny legal effect to an electronic signature solely because it is in electronic form. More significantly, Article 25(1) and Recital 49 read together establish that a QES issued in one EU Member State must be recognised in all other Member States with equivalent effect. This mandatory mutual recognition framework is enforced through the EU Trust List mechanism, which publishes accredited Qualified Trust Service Providers (QTSPs) from each Member State.[28]

[26] eIDAS Regulation, arts. 3(10)-(12) (definitions of simple, advanced, and qualified electronic signatures); art. 26 (requirements for advanced electronic signatures).
[27] eIDAS Regulation, art. 25(2): 'A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.'
[28] Regulation (EU) No. 910/2014 (eIDAS Regulation), arts. 25(3) & 27, recital 49.

The contrast with India's cross-border position is stark. India's Controller of Certifying Authorities (CCA) does not maintain mutual recognition agreements with the majority of its trading partners. The BSA contains no provision for the automatic recognition of foreign electronic signatures or certifications. A document authenticated under eIDAS standards or certified by a US-accredited digital forensics expert under FRE 902(14), may still require full re-authentication in an Indian court proceeding.[29]

3. eIDAS 2.0 and Emerging Developments

Regulation (EU) 2024/1183, commonly referred to as eIDAS 2.0, extends the framework for electronic identification and trust services across the European Union by establishing the European Digital Identity Framework and strengthening cross-border interoperability mechanisms. These innovations will further expand the evidentiary footprint of the eIDAS system, covering blockchain-based records and AI-generated attestations within a legally recognised trust framework.[30]

India's BSA has no counterpart to this forward-looking architecture. While the MeitY's Draft National Cyber Security Policy (2023) acknowledges the need for a digital trust ecosystem, no legislative action has been taken to create a graduated trust service framework comparable to eIDAS.

D. Comparative Analysis: Key Parameters

Table 1 below summarises the comparative findings across the three frameworks on the key parameters examined in this study.

Table 1: Comparative Analysis of Electronic Evidence Frameworks

Parameter	India BSA 2023	US FRE	EU eIDAS

[29]UNCITRAL Model Law on Electronic Commerce (1996) art. 9; see also UNCITRAL Model Law on Electronic Signatures (2001).
[30]eIDAS 2.0 Proposal: Regulation COM (2021)281 final, amending Regulation (EU) 910/2014.

Legal Basis	Statutory (Bharatiya Sakshya Adhiniyam, 2023)	Federal rules (FRE 901, 902)	EU Regulation 910/2014
Admissibility Standard	Section 57-63; certificate required	Authentication + relevance	Qualified signatures presumed valid
Electronic Signature	Section 85B; digital signature	Not specifically addressed	QES, AdES, SES categories
Presumption of Authenticity	Conditional (Sec. 85A-C)	No automatic presumption	QES fully presumed valid
Metadata/Hash	Not expressly mandated	Chain of custody required	eIDAS trust services cover it
Cross-border Recognition	Limited bilateral treaties	Case-by-case judicial discretion	Mandatory mutual recognition (EU)
Certificate Authority	Controller of Certifying Authorities	No equivalent body	Supervisory bodies per member state
Hearsay Exception	Sections 35-36 (business records)	FRE 803(6) business record	Not applicable (evidentiary rules national)

Penalty for Tampering	IPC/BNS provisions apply	18 U.S.C. 1519	National criminal laws apply

Source: Compiled by authors from primary legislative texts.

1. Admissibility Threshold

The BSA sets the highest formal threshold for admissibility: a certificate from a responsible official is ordinarily required, and failure to produce it may result in inadmissibility, as settled by the Supreme Court. The FRE sets a lower threshold: relevance and authentication through any reliable means. The eIDAS Regulation does not directly govern admissibility (which remains a matter for national law) but creates strong evidentiary presumptions that effectively lower the authentication burden in civil proceedings across the EU.

2. Flexibility and Judicial Discretion

The FRE model accords the greatest flexibility to courts: judges may admit electronic records authenticated through circumstantial evidence, expert testimony, or distinctive characteristics without any certificate. The BSA, by contrast, grants limited judicial discretion (except in the context of secondary evidence under Section 65 or in urgent cases). The eIDAS framework is rule-based rather than discretionary: the legal effect of a QES is determined by statute, not by judicial assessment.

3. Electronic Signatures

India's BSA recognises only IT Act-compliant digital signatures (PKI-based) for the purpose of presumptions. The FRE does not address electronic signatures as such, leaving their evidentiary weight to general authentication principles and substantive contract law. The eIDAS Regulation's three-tier architecture provides the most nuanced treatment,

with QES carrying full legal equivalence to handwritten signatures across all EU Member States.[31]

4. Cross-Border Recognition

This parameter reveals the starkest divergence. The EU's mandatory mutual recognition of QES within the single market has no Indian equivalent. The FRE operates domestically, but US courts have developed a reasonably consistent body of case law on admitting foreign electronic records through expert testimony and international judicial cooperation. India's position is largely bilateral and treaty-dependent, with no statutory framework for the presumptive recognition of foreign electronic certifications.

5. Emerging Technologies: AI and Blockchain

None of the three frameworks adequately address AI-generated records or smart contract outputs as a discrete evidentiary category. However, eIDAS 2.0 takes the furthest step by proposing an 'electronic ledger' trust service, which would encompass distributed ledger technology within the regulated trust ecosystem.[32] The BSA is silent on blockchain records beyond treating them as 'electronic records' under the general definition, requiring authentication through the standard certification route. The FRE, through Rule 901(b)(9), can accommodate blockchain records through expert testimony on the technical process, providing greater adaptability in the short term.

V. SUGGESTIONS AND RECOMMENDATIONS

The comparative analysis reveals several structural deficiencies in the BSA's electronic evidence regime that warrant legislative, judicial, and institutional reform. The following recommendations are offered:

A. Legislative Reforms

[31] Law Commission of India, '269th Report: Amendments to the Indian Evidence Act 1872 Pertaining to Electronic Evidence' (2017) 45-52.
[32] eIDAS 2.0 Proposal: Regulation COM (2021)281 final, art. 45f.

1. **Graduated Authentication Standard:** The BSA should be amended to introduce a graduated authentication framework akin to the FRE's multi-method approach. The legislature should codify alternative methods of authentication including hash value certification, metadata analysis, expert forensic testimony, and circumstantial evidence derived from the inherent characteristics of the record. The certificate under Section 63(4) should remain available as one route to admissibility but should not be the exclusive route.
2. **Statutory Presumption for Certified Records:** Drawing from the eIDAS model, the BSA should create a rebuttable statutory presumption of authenticity for electronic records certified by accredited trust service providers. The presumption should extend to records certified by foreign trust service providers where India has a mutual recognition agreement, thereby incentivising the conclusion of such agreements.
3. **Graduated Electronic Signature Framework:** India should legislate a three-tier electronic signature framework (standard, advanced, qualified) modelled on the eIDAS architecture, with each tier carrying progressively stronger presumptions. The existing digital signature infrastructure under the IT Act and the CCA should be leveraged as the basis for the qualified tier, with appropriate reforms to certification standards.
4. **Explicit Provisions for Emerging Technologies:** The BSA should be amended to include explicit provisions on the admissibility of blockchain records, AI-generated outputs, and records from automated systems without human intervention. The amendment should adopt a process-based authentication standard for such records, requiring evidence of the reliability of the system rather than a certificate from a human operator.

B. International Engagement

1. **Mutual Recognition Agreements:** India should proactively negotiate mutual recognition agreements with major trading partners and technology hubs (the EU, the US, the UK, Singapore, and Japan) to create a cross-border electronic evidence recognition network. Such agreements should provide for the presumptive recognition of electronic records certified under the partner jurisdiction's approved standards.
2. **Accession to UNCITRAL Instruments:** India should formally implement the UNCITRAL Model Law on Electronic Commerce (1996) and the UNCITRAL Model Law on Electronic Signatures (2001) into domestic law and consider signing the Convention on the Use of Electronic Communications in International Contracts (2005), which provides a multilateral framework for cross-border electronic evidence recognition.[33]

C. Institutional and Judicial Reforms

1. **Accreditation of Digital Forensic Experts:** Drawing from the FRE's experience, Indian courts should develop a structured framework for the accreditation and deployment of digital forensic experts as court-appointed experts in cases involving complex electronic evidence. The current reliance on responsible officials of computer operators is inadequate for cloud-hosted and distributed data environments.[34]
2. **Judicial Training:** Comprehensive judicial training programmes on digital forensics, blockchain technology, electronic signature standards, and cloud computing should be mandated at all levels of the judiciary. The National Judicial Academy should develop a dedicated curriculum on electronic evidence drawing from comparative international experience.

[33] UNCITRAL Model Law on Electronic Commerce (1996); UNCITRAL Model Law on Electronic Signatures (2001); United Nations Convention on the Use of Electronic Communications in International Contracts (2005), art. 9.
[34]Ministry of Electronics and Information Technology (MeitY), 'Draft National Cyber Security Policy' (2023).

VI. CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023 represents a meaningful, if incomplete, step forward in India's engagement with electronic evidence. It codifies and refines the existing Section 65B regime, extends the statutory definition of electronic records to cover contemporary data environments, and carries forward the presumptions regarding digital signatures. However, when measured against the flexible, process-oriented authentication framework of the US Federal Rules of Evidence and the structured, graduated trust architecture of the EU eIDAS Regulation, the BSA's limitations come into sharp focus.

The certificate-centric admissibility model retains a bureaucratic formalism that is ill-suited to the realities of cloud computing, distributed ledger technologies, and AI-generated records. The absence of a graduated electronic signature framework leaves a wide class of electronic records without statutory presumptive protection. The cross-border recognition deficit is perhaps the most serious gap: in an era of transnational commerce and international dispute resolution, the inability to presumptively recognise foreign electronic certifications is a significant impediment.

The hypotheses advanced in this paper are substantially confirmed. H1 is validated: the BSA's certificate-centric approach is structurally less adaptive than the FRE's process-based model. H2 is validated: the BSA creates an asymmetry between its limited presumptive regime and both the FRE's self-authentication provisions and the eIDAS QES presumption. H3 is validated: India's cross-border electronic evidence recognition framework is significantly less developed than the EU's mandatory mutual recognition regime.

The recommendations offered in this paper chart a path toward reform that draws from the best elements of both the FRE and eIDAS frameworks while remaining calibrated to India's institutional context. A graduated authentication standard, a statutory presumption for certified records, a three-tier electronic signature framework, and robust international engagement are the four pillars of an adequately modernised electronic

evidence law for India. The BSA has laid a foundation; the legislature must now build upon it.

VII. REFERENCES

A. Primary Sources

1. Legislation

- Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).
- Indian Evidence Act, No. 1 of 1872 (India) (repealed).
- Information Technology Act, No. 21 of 2000 (India).
- Federal Rules of Evidence (United States) (as amended through 2023).
- 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] OJ L 257/73 (eIDAS Regulation).
- UNCITRAL Model Law on Electronic Commerce (1996).
- UNCITRAL Model Law on Electronic Signatures (2001).

2. Case Law (India)

- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
- Bashir Ahmad v. Govt. of NCT of Delhi, (2009) 3 SCC 457.
- Jay Prakash Singh v. State of Bihar, (2012) 4 SCC 506.
- Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
- Syed Asifuddin v. State of Andhra Pradesh, (2005) Cri LJ 4314 (AP HC).
- Umar Abdul Latif v. State, Crl. Rev. P. 386/2018 (Delhi HC 2022).

3. **Case Law (United States)**

- Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).
- United States v. Vayner, 769 F.3d 125 (2d Cir. 2014).
- State v. Eleck, 23 A.3d 818 (Conn. App. Ct. 2011).

B. Secondary Sources

1. **Books**

- Duggal P, Cyber Law: The Indian Perspective (Saakshar Law Publications 2014).

2. **Journal Articles**

- Mishra SK, 'Electronic Evidence in Indian Courts: Emerging Challenges' (2021) 63 Journal of the Indian Law Institute 214.
- Raghuraman R, 'Digital Forensics and Indian Courts: A Practitioner's Analysis' (2022) 54 Journal of the Indian Law Institute 187.
- Olswang (Bird & Bird), 'eIDAS Regulation: Trust Services and Electronic Identification' (2016) 32 Computer Law and Security Review 467.
- Paul GL and Baron JR, 'Information Inflation: Can the Legal System Adapt?' (2007) 13 Richmond Journal of Law and Technology 10.
- Schoen S, 'Hash Functions and Digital Fingerprints: Primer for Legal Practitioners' (2019) 35 Santa Clara Computer and High Technology Law Journal 1.

3. **Reports and Policy Documents**

- European Commission, 'eIDAS Regulation Evaluation Report' COM (2021) 290 final.

- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework [2024] OJ L 1183.
- Law Commission of India, '269th Report: Amendments to the Indian Evidence Act 1872 Pertaining to Electronic Evidence' (2017).
- Ministry of Electronics and Information Technology (MeitY), 'Draft National Cyber Security Policy' (2023).
- National Association of Software and Service Companies (NASSCOM), 'Digital Evidence Framework for India' (2022).