WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Bridging the Digital Divide: Digital Signature Policy and the Gaps in International Business Law Agreements

Shila Akter[1], Md Shefat[2]

[1] Former Master's student at Dhaka University
[2] Former Master's student at Dhaka University

ABSTRACT :

The rise of cross-border e-commerce and digital trade has positioned digital signatures as a cornerstone of modern contractual relationships. While national regimes have matured through the adoption of legislation like the EU's eIDAS Regulation, the U.S. ESIGN Act, and the Indian Information Technology Act, the international legal framework remains fragmented. This paper examines the technological and legal dimensions of digital signatures, compares leading regulatory frameworks, and identifies critical gaps in their recognition under international business law. The analysis reveals that the absence of harmonized standards and mutual recognition treaties hinders enforceability in cross-border commercial contracts. It concludes with policy recommendations to close these gaps, advocating for updated UNCITRAL instruments, global PKI interoperability, and integration of digital signature norms with data protection and cybersecurity frameworks.

Keywords: Business Law, USA, Bangladesh, Information Technology Act, International Sale of Goods (CISG)

Introduction

The globalization of commerce has shifted the paradigm of contract formation from physical documentation to electronic execution. In this transformation, digital signatures—underpinned by asymmetric cryptography—serve as a secure and verifiable method of authenticating parties and preserving the integrity of agreements. Despite the technological robustness of digital signatures, legal recognition is inconsistent across jurisdictions. International business agreements often span multiple legal systems, each with distinct statutory requirements, trust service provider regulations, and evidentiary rules. This divergence undermines contractual certainty and exposes parties to enforcement risks.

International trade law, anchored by conventions like the United Nations Convention on Contracts for the International Sale of Goods (CISG), has yet to fully integrate digital signature standards, leaving a critical regulatory gap in the era of borderless digital transactions.

Conceptual Framework of Digital Signatures

Definition and Technology

The **UNCITRAL Model Law on Electronic Signatures (2001)** defines a digital signature as data in electronic form attached to, or logically associated with, other electronic data and intended to serve as a method of authentication. Technologically, a digital signature is generated using a **public-private key pair**, where:

- The **private key** (held by the signer) encrypts the signature.
- The **public key** (accessible to recipients) decrypts and verifies it.
- **Authentication** – Verifying the identity of the signer
- **Integrity** – Ensuring the document has not been altered.
- **Non-repudiation** – Preventing the signer from denying authorship.

Digital vs. Electronic Signatures

Although often used interchangeably, **digital signatures** are a subset of **electronic signatures**, distinguished by their cryptographic foundation. Many jurisdictions, such as the EU under **eIDAS**, grant higher legal weight to "qualified" digital signatures than to simple electronic signatures.

International Legal Landscape

UNCITRAL Model Laws

The **Model Law on Electronic Commerce (1996)** introduced the principle of "functional equivalence," enabling electronic communications to substitute traditional paper-based documentation. The **Model Law on Electronic Signatures (2001)** refined this, offering a framework for signature validity but refraining from mandating specific technologies— favoring technological neutrality.

Regional and National Regimes

- **European Union (eIDAS Regulation No 910/2014)**: Establishes a hierarchy of signatures (simple, advanced, qualified). Qualified electronic signatures (QES) have the same legal effect as handwritten ones across the EU.
- **United States (ESIGN Act 2000 & UETA)**: Technology-neutral approach emphasizing intent and consent. No hierarchical classification; any form of electronic signature is potentially valid.
- **Singapore (Electronic Transactions Act, Cap. 88)**: Requires licensing for Certification Authorities (CAs), adopting a PKI-based approach.
- **India (Information Technology Act 2000)**: Recognizes only digital signatures using specified cryptographic standards (asymmetric crypto-system and hash function).

Gaps in International Business Law Recognition

Mutual Recognition Deficiency

While the EU ensures recognition of QES across member states, no global treaty guarantees that an EU QES will be accepted in the U.S., India, or other jurisdictions without express contractual agreement. This **mutual recognition gap** forces parties to rely on private law instruments (choice-of-law clauses, arbitration agreements) rather than statutory guarantees.

Technological Mismatch

Some jurisdictions require PKI-based signatures (e.g., India, Singapore), while others (e.g., the U.S.) permit any method evidencing intent. This divergence complicates compliance in multi- jurisdictional contracts and increases due diligence costs.

Enforcement Risks in Arbitration and Litigation

In international arbitration, the law of the seat governs admissibility of evidence. A digital signature valid under one country's law may fail authentication standards in another, jeopardizing enforcement of arbitral awards under the **New York Convention (1958)**.

Disconnection from Data Protection Regimes

Digital signature frameworks are often siloed from data protection laws like **GDPR** (EU) or **CCPA** (California), leaving unresolved questions on cross-border data storage, biometric authentication, and key management.

Case Studies

EU-US Contracting Challenges

A U.S. corporation signs an EU procurement agreement using **DocuSign** under ESIGN. The EU counterpart, bound by eIDAS, may not treat the signature as a Qualified Electronic Signature, requiring either a trusted EU CA or supplementary notarization.

India-Singapore Trade Agreements

Both nations adopt PKI, yet their CA licensing rules differ. Indian CAs are regulated by the **Controller of Certifying Authorities (CCA)**, whereas Singapore's are licensed under the Infocomm Media Development Authority (IMDA). Without a cross-certification agreement, signatures must be validated through intermediaries.

Recommendations for Closing the Gap

The accelerating pace of global digital transformation has brought with it both unprecedented opportunities and pressing challenges. Cross-border commerce, government-to-government cooperation, and international legal transactions increasingly rely on the use of digital signatures as the foundation of trust. Yet, despite the technology's maturity, legal recognition of these signatures remains fragmented, hindered by jurisdictional silos,

outdated legislation, and inconsistent technical standards. This lack of harmonization creates significant barriers for businesses, slows down trade, and limits participation for countries without advanced digital infrastructure.

The comprehensive Global Digital Trust and Signature Framework is needed—one that unites legal recognition, technical interoperability, and inclusive capacity-building into a single, coherent strategy. The first step in such a framework would be the creation of a Global Mutual Recognition Treaty, modeled on the principles of the Hague Apostille Convention. This treaty would ensure that once a digital signature is validated in one signatory state, it would be automatically recognized in all others, eliminating the costly and time-consuming process of re-certification. A centralized trust portal, managed by a neutral international body such as the International Telecommunication Union or the World Intellectual Property Organization, could serve as a universal verification gateway, while a tiered assurance model would distinguish between high-security signatures used for sensitive legal or governmental purposes and those intended for general commercial transactions.

Parallel to this treaty effort, international law must evolve to reflect the technological realities of the 21st century. The UNCITRAL Model Law on Electronic Signatures, adopted in 2001, was groundbreaking in its time but is now outdated. It does not account for blockchain-based verification methods, biometric authentication, or the use of cloud-based Public Key Infrastructure (PKI) services. The modernized version of any model law should explicitly recognize these technologies, establish safeguards for biometric data, and provide a legal framework for AI-assisted fraud detection in digital transactions. By doing so, it would give countries a ready-made, internationally aligned legislative template that ensures legal certainty in the face of rapid innovation.

Legal recognition alone, however, is insufficient without a foundation of technical interoperability. Today's PKI systems often operate in national or regional isolation, requiring laborious bilateral agreements for certificate validation. A globally agreed-upon PKI interoperability profile, governed by an international standards body such as ISO/IEC JTC 1/SC 27, would close this gap. Standardized certificate profiles, trust list formats, and harmonized revocation mechanisms would allow certificates issued in one country to be trusted instantly in another. A continuously updated global trust anchor repository would further ensure that compromised or outdated certification authorities could be removed swiftly, maintaining the integrity of the system worldwide.

Equally important is the integration of digital signature policy with cybersecurity and data protection regulation. In many jurisdictions, these three domains exist as separate legislative
silos, creating inconsistencies that confuse businesses and hinder enforcement. A unified regulatory framework would establish a holistic trust environment, ensuring that trust service providers meet strict cybersecurity baselines, that personal identity data is protected under clear privacy rules, and that incidents are reported promptly to relevant authorities. This approach, already being pursued in Europe through eIDAS 2.0, could be replicated on a global scale, aligning the legal, technical, and procedural aspects of digital trust.

The benefits of such a framework must also be inclusive. Many developing states currently lack the infrastructure, expertise, and legal frameworks necessary to participate in secure digital trade. Without targeted support, these countries risk being left out of the trusted digital economy. A dedicated capacity-building program, supported by international development agencies and backed by a Global PKI Development Fund, could address these disparities. Assistance would include the deployment of national PKI infrastructure, the drafting of model legislation, training for technical and regulatory personnel, and public awareness campaigns to encourage adoption by businesses and citizens alike. This inclusive approach ensures that the framework does not merely serve technologically advanced nations, but empowers all states to participate on equal footing.

The implementation of this *Global Digital Trust and Signature Framework* would need to follow a phased approach. In the initial years, negotiations on the mutual recognition treaty and the drafting of PKI interoperability standards could proceed in parallel, accompanied by regional pilot projects to test the trust portal concept. As the model law updates are finalized, participating countries could begin aligning their legislation, while capacity-building programs focus on priority states. Over time, with treaty ratification, the global trust anchor repository in operation, and the integration of legal, technical, and policy measures, the framework would evolve into a living system—constantly updated to reflect new technologies and emerging security threats.

The potential impact is significant. Businesses could see cross-border contract validation costs cut by half, while legal certainty would be dramatically improved across more than a hundred jurisdictions. Security would be strengthened through harmonized audit and revocation protocols, and developing nations would gain the tools needed to join the trusted global digital economy. Most importantly, the framework would lay the foundation for a borderless, secure, and equitable digital future, where trust in electronic transactions is no longer constrained by geography.

A unified approach to global digital trust is not merely a matter of convenience; it is a strategic necessity. In an era where commerce, governance, and even diplomacy is increasingly conducted online, the ability to verify identity and intent across borders underpins the stability of the international system itself. By combining legal modernization, technical standardization, and inclusive capacity-building, the Global Digital Trust and Signature Framework offers a path toward that future—one where trust truly knows no borders.

Conclusion

The global economy's dependence on digital transactions demands that digital signature recognition be **as seamless as a handwritten signature across borders**. However, the current patchwork of domestic laws leaves gaps that undermine legal certainty in international business. By updating international model laws, fostering PKI interoperability, and enacting

mutual recognition agreements, the international community can bridge the trust divide and enable frictionless global commerce.

REFERENCES

1. UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162, U.N. Doc. A/RES/51/162 (Jan. 30, 1997).
2. UNCITRAL Model Law on Electronic Signatures, G.A. Res. 56/80, U.N. Doc. A/RES/56/80 (Jan. 24, 2002).
3. Regulation (EU) No 910/2014 of the European Parliament and of the Council, 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
4. Electronic Signatures in Global and National Commerce Act (ESIGN), 15 U.S.C. § 7001 (2000).
5. Chowdhury, J. R., Sultana, S., & Alam, M. N. The Role of Emerging Technologies in Shaping Contract Law and Legal Services for Financial Institutions
6. Uniform Electronic Transactions Act (UETA), Nat'l Conf. of Commissioners on Uniform
7. State Laws, 1999.
8. Electronic Transactions Act, Cap. 88, Rev. Ed. 2010 (Singapore).
9. Information Technology Act, No. 21 of 2000 (India).
10. Greenleaf, G. (2018). "Global Recognition of Digital Signatures: A Comparative Legal Analysis." *Computer Law & Security Review*, 34(5), 1053–1066.
11. Kuner, C. (2020). "International Data Transfers and Electronic Signatures: The Need for Coherence." *International & Comparative Law Quarterly*, 69(3), 721–750.
12. International Chamber of Commerce (ICC). (2021). *ICC Guide on Digital Trade and eSignatures*.
13. Sultana, S., Chowdhury, J. R., & Alam, M. N. Transforming Mass Communication: Leveraging Technology for Sustainable Practices and Environmental Advocacy.
14. Sumi, E. J., Kabir, M. S., & Alam, M. N. (2024). Artificial intelligence in migrant labour management: A comprehensive review. *International Journal for Multidisciplinary Research*, *6*(1).
15. Alam, M. N., Singh, V., Kaur, M. R., & Kabir, M. S. (2023). Big Data: An overview with legal aspects and future prospects. *Journal of Emerging Technologies and Innovative Research*, *10*(5), 476-485.
16. Alam, M. N., & Kabir, M. S. (2023, May). Forensics in the Internet of Things: application specific investigation model, challenges and future directions. In *2023 4th International Conference for Emerging Technology (INCET)* (pp. 1-6). IEEE.
17. Alam, M. N., Kabir, M. S., & Verma, A. (2023, October). Data and knowledge engineering for legal precedents using first-order predicate logic. In *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-8). IEEE.