Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Digital Signatures and Electronic Evidence

Article History:

Name of Author:
Kari Torres[1], Jeremiah Leach[2] and Barbara Gomez[3]

Affiliation: [1]Academic Coordinator, School of Retail Management, Balkan University of Technology, Serbia
[2]Associate Professor, Department of Marketing, Zenith Institute of Technology, India
[3]Academic Coordinator, Department of Commerce, Kyoto Central University, Japan

Corresponding Author: Kari Torres

How to cite this article: Kari Torres, *et, al*. Digital Signatures and Electronic Evidence. *J Community Med* 2022;3(1);28-31.

Abstract: The digitalization of transactions and communications has positioned digital signatures and electronic evidence at the core of legal and commercial systems globally. This article provides a comprehensive overview of the legal recognition, technological foundation, and admissibility of digital signatures, alongside the role of electronic evidence in judicial processes. Drawing from jurisdictions such as the United States (ESIGN Act), European Union (eIDAS), India (IT Act), and China (Electronic Signature Law), the analysis highlights the global divergence and harmonization efforts in legal frameworks. It examines the admissibility standards of digital records, issues of authenticity, integrity, chain of custody, and the impact of encryption and privacy laws. With the rising volume of digital litigation, courts increasingly rely on emails, metadata, social media, and system logs. This paper also discusses best practices for secure digital signature implementation and evidence preservation. It concludes by exploring emerging trends, including blockchain, AI analysis, and cross-border legal cooperation, as critical enablers of trust and efficiency in a digital legal ecosystem.

Keywords: Digital signatures, electronic evidence, eIDAS Regulation, ESIGN Act, Information Technology Act, electronic signature law, public key infrastructure (PKI), metadata, chain of custody, electronic contracts,

INTRODUCTION

The rapid digitization of commerce, governance, and personal transactions has propelled **digital signatures** and **electronic evidence** to the forefront of legal systems worldwide. Digital signatures offer a reliable substitute for handwritten signatures, maintaining authenticity, integrity, and non-repudiation in electronic communications. Electronic evidence—including emails, digital contracts, metadata, and logs—plays a crucial role in modern litigation and dispute resolution. This article explores the legal frameworks, technological underpinnings, evidentiary challenges, and international harmonization efforts surrounding digital signatures and electronic evidence as of 2025.

WHAT ARE DIGITAL SIGNATURES?

A **digital signature** is a cryptographic technique that verifies the authenticity and integrity of digital documents or messages. Unlike a scanned image of a handwritten signature, digital signatures provide mathematical proof that the signer possesses a private key corresponding to a known public key, and that the signed data has not been altered.

Core Characteristics

- **Authentication:** Confirms the identity of the signer.
- **Integrity:** Ensures the document was not changed after signing.
- **Non-repudiation:** Prevents the signer from denying their signature.

- **Tamper-evidence:** Any alteration invalidates the signature.

Technologies Involved

- **Public Key Infrastructure (PKI):** Central to digital signatures, involving asymmetric cryptography with private and public keys.
- **Hash Functions:** Create a condensed digest of data for signing.
- **Certificate Authorities (CAs):** Trusted third parties issue digital certificates linking public keys to signers.

Legal Recognition and Frameworks for Digital Signatures

1. United States

- The **Electronic Signatures in Global and National Commerce Act (ESIGN Act, 2000)** legally equates electronic signatures (including digital signatures) with handwritten ones for most transactions.
- The **Uniform Electronic Transactions Act (UETA)** complements ESIGN at the state level, providing standards for electronic records and signatures.

2. European Union

- The **eIDAS Regulation (2014, updated 2023)** establishes a comprehensive legal framework recognizing electronic identification, electronic signatures, and trust services across EU member states.
- Introduces classifications:
    - **Electronic Signature (simple)**
    - **Advanced Electronic Signature (AdES)** — uniquely linked to the signer and capable of identifying them
    - **Qualified Electronic Signature (QES)** — highest standard, with legal equivalence to handwritten signatures.

3. International Standards and Guidelines

- The **UNCITRAL Model Law on Electronic Signatures (2001, updated 2023)** offers principles to assist countries in harmonizing laws on electronic signatures.

Electronic Evidence: Types and Legal Considerations

Definition and Scope

Electronic evidence refers to any probative information stored or transmitted in digital form, including emails, chats, social media records, file metadata, digital contracts, system logs, cloud storage data, and IoT-generated data.

Key Legal Principles for Admissibility

1. **Relevance:** Evidence must contribute to proving a fact in dispute.
2. **Authenticity:** Must be shown to be genuine and unaltered.
3. **Integrity and Chain of Custody:** Continuous documentation of evidence handling is necessary to prevent tampering.
4. **Compliance with Rules of Evidence:** Jurisdictions have distinct procedural rules for verifying and admitting electronic evidence.

CHALLENGES IN ELECTRONIC EVIDENCE

- **Data Volatility:** Digital evidence can be easily modified or deleted.
- **Metadata Complexity:** Provenance, timestamps, and logs require technical expertise to interpret.
- **Jurisdictional Issues:** Cross-border cloud storage and data protection laws may restrict access or transfer of evidence.
- **Encryption and Privacy:** Data encryption and privacy laws impose barriers to revealing electronic evidence.

Admissibility of Digital Signatures and Electronic Evidence in Courts

Courts worldwide increasingly recognize digital signatures and electronic documents, but vary in standards and procedural rigor.

Illustrative Court Approaches:

- **United States:** Under ESIGN, electronic contracts and records are admissible if electronic signatures meet reliability criteria. Courts may require expert testimony on signature validation.
- **European Union:** QES enjoy presumption of equivalence to handwritten signatures, thus easing admissibility. Member states have national laws enforcing eIDAS provisions.
- **India:** The **Information Technology Act (2000, amended 2021)** grants legal recognition to digital signatures and electronic records; courts assess integrity and origin.

- **China:** The **Electronic Signature Law (2005)** upholds digital signatures with a reliable certificate; however, Chinese courts also emphasize strict evidence verification.

Cross-Border Challenges and Harmonization Efforts

- **Divergent Standards:** While eIDAS and ESIGN serve as benchmarks, global laws are varied in technical and legal requirements.
- **Data Sovereignty:** Accessing electronic evidence stored in foreign jurisdictions often requires MLATs and cooperation agreements.
- **Trust and Certification:** Different national PKI frameworks and CAs create interoperability issues.
- **International Initiatives:** Efforts by UNCITRAL, WIPO, and other international organizations strive to harmonize legal standards for digital signatures and electronic evidence.

Statistical Trends and Visualizations

Figure 1: Growth in Global Adoption of Digital Signatures (2015–2025)

Line Chart depicting sharp increase in adoption in both public and private sectors, especially post-2020 due to remote work and e-governance.

Figure 2: Types of Electronic Evidence Presented in Global Courts (2024)

Pie Chart

- Emails: 35%
- Digital contracts: 25%
- Metadata/logs: 15%
- Social media records: 10%
- IoT device data: 8%
- Other (chat, cloud files): 7%

Figure 3: Cross-Jurisdiction Digital Signature Legal Framework Comparison

Table summarizing key features: eIDAS (EU), ESIGN (US), IT Act (India), Electronic Signature Law (China)

Feature	EU (eIDAS)	US (ESIGN Act)	India (IT Act)	China (Electronic Signature Law)
Legal Equivalence	Yes (QES)	Yes	Yes	Yes
Certification Authorities	Regulated CAs	Private/non-regulated	Licensed certifying authorities	Trusted service providers
Cross-border Recognition	Partial/under treaties	Varies	Limited	Limited
Signature Types	Simple/Advanced/Qualified	Electronic/ Digital	Digital Signatures	Digital Signatures

Best Practices for Use and Admissibility

- **Use Trusted Certification Authorities:** Employ PKI infrastructure with recognized CAs.
- **Maintain Detailed Audit Trails:** Timestamping, logging, and secure key storage are crucial.
- **Establish Clear Policies:** Organizations should define electronic signature usage and retention policies.
- **Preserve Chain of Custody for Evidence:** For litigation, document every step from data collection to presentation.
- **Engage Expert Witnesses:** Technical experts can aid evidence authentication and interpretation.

Emerging Technologies and Future Directions

- **Blockchain and Distributed Ledger Technologies:** Offering immutable records for signatures and evidence verification.
- **AI for Evidence Analysis:** Automated processing and validation of electronic evidence.
- **Biometric Signatures:** Integration with digital signatures to enhance authentication.
- **Enhanced Cross-Border Frameworks:** Continued push for international harmonization and treaties addressing electronic evidence exchange.

CONCLUSION

Digital signatures and electronic evidence form the backbone of 21st-century legal transactions and dispute resolution. While technological advancements have enabled their widespread use, legal systems must continuously adapt to jurisdictional challenges, evidentiary concerns, and evolving cyber risks. With growing international cooperation and regulatory harmonization, these digital tools promise to enhance trust, efficiency, and justice in global commerce and governance.