

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ELECTRONIC SIGNATURES AND DIGITAL AUTHENTICATION UNDER THE INFORMATION TECHNOLOGY ACT, 2000: A COMPREHENSIVE LEGAL ANALYSIS

AUTHORED BY - YADUNANDAN M.D. & ADHAM BASHEER

ABSTRACT

The exponential growth of digital commerce and e-governance in India necessitated a robust legal framework governing electronic authentication. The Information Technology Act, 2000 (hereinafter “IT Act”), enacted to give effect to the UNCITRAL Model Law on Electronic Commerce (1996), established a comprehensive scheme for electronic signatures, digital certificates, and associated liability structures.¹ This assignment undertakes an exhaustive examination of the legal architecture governing electronic signatures in India encompassing the roles of Certifying Authorities, the procedural requirements for grant and revocation of certificates, subscriber obligations, the technical foundations of key pair generation, and the penal consequences for violations. The analysis draws upon statutory text, subordinate legislation including the Information Technology (Certifying Authorities) Rules, 2000,² judicial pronouncements, and leading academic scholarship in the field. The study concludes that while the IT Act provides a reasonably sound foundational framework, significant gaps persist in enforcement, cross-border recognition, and the accommodation of emerging technologies.

I. INTRODUCTION

1.1 Background and Context

The transition from paper-based commerce to digital transactions represents one of the most transformative developments in legal history. Signatures — as instruments of authentication, consent, and legal binding — have existed since antiquity. The seal of a Roman magistrate, the wax impression of a medieval lord, the ink signature of a Victorian merchant: each served the

¹ Information Technology Act, 2000, No. 21 of 2000, preamble (India) [hereinafter IT Act]; see U.N. Comm’n on Int’l Trade L., Model Law on Electronic Commerce with Guide to Enactment 1996, G.A. Res. 51/162 (Jan. 30, 1997).

² Information Technology (Certifying Authorities) Rules, 2000 (India) [hereinafter CA Rules].

same fundamental purpose of attributing a document to an identifiable source and signifying the author's assent to its contents. The advent of digital communication, however, rendered these traditional mechanisms inadequate.

Electronic communication is, by its very nature, susceptible to interception, impersonation, and alteration. A document transmitted over the internet carries no inherent indication of its author's identity, nor any guarantee that it has not been modified in transit. This technical vulnerability posed a fundamental challenge to the recognition of electronic transactions as legally valid. The solution devised by cryptographers — public key infrastructure (PKI) and digital signatures — offered a mathematically robust mechanism for authenticating electronic documents, but its legal recognition required legislative intervention.

India's response to this challenge was the Information Technology Act, 2000, which received the assent of the President on 9 June 2000 and came into force on 17 October 2000.³ The Act was significantly amended by the Information Technology (Amendment) Act, 2008 (effective 27 October 2009), which broadened the concept of "digital signature" to the wider category of "electronic signature," thereby accommodating evolving technologies beyond asymmetric cryptography.⁴

1.2 Objectives and Scope

This assignment pursues the following objectives:

- To analyse the conceptual distinction between electronic signatures and digital signatures and their respective legal status under Indian law;
- To examine the institutional architecture established by the IT Act for the issuance, management, and revocation of digital signature certificates;
- To assess the duties imposed upon subscribers and the consequences of their breach;
- To evaluate the technical framework governing key pair generation and its legal implications;
- To critically examine the penalties and adjudicatory mechanisms prescribed under the IT Act; and
- To identify lacunae and recommend reforms in light of contemporary technological and jurisprudential developments.

³ Gazette of India, Extraordinary, pt. II, § 1, No. 27 (June 9, 2000) (publishing the Act upon Presidential assent); IT Act § 1(3) (Act to come into force on the date appointed by the Central Government by notification).

⁴ Information Technology (Amendment) Act, 2008, No. 10 of 2009 (India) (in force Oct. 27, 2009); IT Act §§ 2(1)(p), 2(1)(ta), 3, 3A.

II. CONCEPTUAL FRAMEWORK: ELECTRONIC SIGNATURE AND DIGITAL SIGNATURE DISTINGUISHED

2.1 The Pre-Amendment Position: Digital Signatures

As originally enacted, the IT Act, 2000 employed only the concept of “digital signature,” defined under Section 2(1)(p) as authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3.⁵ Section 3 in its original form restricted recognised authentication to asymmetric cryptosystems using a public-private key pair and a hash function, which enveloped and transformed the initial electronic record into another electronic record.⁶

This restrictive approach, while technically sound at the time, reflected the technological limitations of the late 1990s and failed to anticipate the rapid diversification of authentication mechanisms that followed.

2.2 The 2008 Amendment: Introduction of Electronic Signatures

The Information Technology (Amendment) Act, 2008 fundamentally restructured the authentication framework. Section 3A was inserted to provide for “electronic signatures,” defined in Section 2(1)(ta) as authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule, and including a digital signature.⁷ Alongside digital signatures under Section 3, the Second Schedule recognises e-authentication using Aadhaar or other e-KYC services, introduced in 2015 and widened in 2019 to cover “other” e-KYC services.⁸

This amendment brought Indian law into closer conformity with the UNCITRAL Model Law on Electronic Signatures (2001), which adopts a technology-neutral approach to the recognition of electronic authentication mechanisms.⁹ Commentators have observed that the amendment was necessitated by the recognition that the future of electronic authentication would not be monopolised by any single technology, and that the law needed sufficient flexibility to

⁵ IT Act § 2(1)(p).

⁶ IT Act § 3.

⁷ IT Act §§ 2(1)(ta), 3A; Information Technology (Amendment) Act, 2008, No. 10 of 2009 (India). Section 3A(2) requires that an electronic signature or authentication technique be considered reliable, which it is if, among other things, the signature creation data is linked to the signatory alone and under the signatory’s control at the time of signing, and any alteration to the signature or the signed record after affixation is detectable. *Id.* § 3A(2).

⁸ Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015, G.S.R. 61(E) (Jan. 27, 2015) (India) (inserting e-authentication using Aadhaar e-KYC services into the Second Schedule); Notification S.O. 1119(E), Gazette of India, Extraordinary, pt. II, § 3(ii), No. 985 (Mar. 5, 2019) (inserting “or other” before e-KYC services); IT Act sched. II.

⁹ U.N. Comm’n on Int’l Trade L., Model Law on Electronic Signatures with Guide to Enactment 2001, G.A. Res. 56/80 (Dec. 12, 2001).

accommodate innovations yet unanticipated.¹⁰

2.3 Legal Equivalence with Handwritten Signatures

Section 5 of the IT Act provides that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.¹¹

This provision establishes the cornerstone of electronic signature law in India: the functional equivalence of electronic signatures with handwritten signatures. Electronic records were admitted in evidence under Sections 65A and 65B of the Indian Evidence Act, 1872, subject to the certification requirement of Section 65B(4).¹² With effect from 1 July 2024, the Evidence Act has been repealed and replaced by the Bharatiya Sakshya Adhiniyam, 2023, under which Section 61 gives electronic records the same legal effect as other records and Section 63 (the successor to Section 65B) governs their admissibility, with a certificate under Section 63(4).¹³ The Supreme Court of India, in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India), authoritatively settled that the certificate under Section 65B(4) is a condition precedent to the admissibility of electronic evidence, following *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India), and overruling *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).¹⁴ The decision underscores the significance of proper electronic authentication in legal proceedings, and its reasoning continues to inform the reading of Section 63(4) of the Bharatiya Sakshya Adhiniyam, which now also requires the certificate to disclose the hash value of the record.¹⁵

¹⁰ See generally S.V. Joga Rao, *Law of Cyber Crimes and Information Technology Laws* (Wadhwa & Co. 2004).

¹¹ IT Act § 5. Certain instruments, such as negotiable instruments (other than cheques), powers of attorney, trusts, and wills, are excluded from the Act. *Id.* § 1(4) & sched. I.

¹² Indian Evidence Act, No. 1 of 1872, §§ 65A, 65B (India) (repealed).

¹³ Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, §§ 61, 63 (India) (in force July 1, 2024).

¹⁴ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India); *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India); *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).

¹⁵ Bharatiya Sakshya Adhiniyam, 2023, § 63(4); see also *id.* § 39(2) (treating the opinion of an Examiner of Electronic Evidence notified under IT Act § 79A as expert opinion).

III. ISSUING AUTHORITIES AND CERTIFYING AUTHORITIES

3.1 Statutory Framework

The IT Act establishes a hierarchical structure of authorities responsible for the governance and oversight of digital signature certificates. This structure comprises: (a) the Controller of Certifying Authorities (CCA); (b) Certifying Authorities (CAs); and (c) Sub-Certifying Authorities recognised under the relevant CA's certification practice statement.¹⁶

3.2 The Controller of Certifying Authorities

Section 17 of the IT Act provides for the appointment of a Controller of Certifying Authorities by the Central Government.¹⁷ The Controller is the apex regulatory authority in the PKI hierarchy and exercises extensive supervisory and quasi-judicial functions.

Functions of the Controller (Section 18):

The Controller's functions under Section 18 include:¹⁸

- Exercising supervision over the activities of Certifying Authorities;
- Certifying public keys of Certifying Authorities;
- Laying down standards to be maintained by Certifying Authorities;
- Specifying qualifications and experience required of employees of Certifying Authorities;
- Specifying the conditions under which Certifying Authorities shall conduct their business;
- Specifying the form and content of a digital signature certificate;
- Specifying the form and manner in which accounts shall be maintained by Certifying Authorities;
- Specifying the terms and conditions subject to which auditors may be appointed;
- Facilitating the establishment of any electronic system by a Certifying Authority;
- Specifying the manner in which Certifying Authorities shall conduct their dealings with subscribers;
- Resolving any conflict of interests between Certifying Authorities and subscribers;
- Laying down duties of subscribers; and
- Maintaining a database containing the disclosure record of every Certifying Authority accessible to the public.

¹⁶ IT Act §§ 17–18 (Controller), 21–24 (licensing of Certifying Authorities); CA Rules.

¹⁷ IT Act § 17.

¹⁸ IT Act § 18.

Under Section 19, the Controller may, with the prior approval of the Central Government and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of the IT Act.¹⁹

3.3 Certifying Authorities: Licensing Requirements

Section 21 of the IT Act provides that any person may apply to the Controller for a licence to issue electronic signature certificates, and Section 22 prescribes the form and contents of the application; the grant or rejection of the application is governed by Section 24.²⁰ The licensing regime is elaborated in the Information Technology (Certifying Authorities) Rules, 2000.

Grant and Conditions of Licence (Sections 21 to 24):

Upon receipt of an application, the Controller may grant or reject it under Section 24, and a licence is valid for the period prescribed and is renewable under Section 23.²¹ Conditions attached to the licence, drawn from the Act, the CA Rules and the Controller's guidelines, include obligations to: (a) make available an online repository; (b) issue certificates only after verifying the identity of the subscriber; (c) ensure revocation of certificates within specified timeframes; (d) submit to periodic audits; and (e) comply with all standards and guidelines issued by the Controller.²²

As of the Controller's published list, the licensed CAs in India include Safescrypt, IDRBT, Code Solutions, e-Mudhra, C-DAC, Capricorn, Protean, Vsign (Verasys), CSC, and CDSL Ventures, among others.²³

IV. GRANT OF DIGITAL SIGNATURE CERTIFICATES

4.1 The Application Process

Section 35 of the IT Act governs the application for digital signature certificates. Any person may make an application to the Certifying Authority for the issue of a digital signature certificate in the prescribed form.²⁴ The application must be accompanied by: (a) a certification practice statement or statement containing such particulars as may be prescribed; (b) the prescribed fee not exceeding twenty-five thousand rupees; and (c) any other document required

¹⁹ IT Act § 19.

²⁰ IT Act §§ 21, 22, 24; *see also id.* § 23 (renewal of licence).

²¹ IT Act §§ 21(3), 23, 24.

²² IT Act §§ 30–31, 34–35; CA Rules rr. 19–20.

²³ Controller of Certifying Authorities, Licensed CAs, https://cca.gov.in/licensed_ca.html (last visited Oct. 14, 2026).

²⁴ IT Act § 35(1).

by the CA for verification of identity.²⁵

4.2 Identity Verification and Classes of Certificates

The cornerstone of the certificate issuance process is identity verification. The CA Rules and the Controller's guidelines prescribe procedures for identity verification that differ depending on the class of certificate:²⁶

Class 1 Certificates: Issued based on user-provided information (name, email address) verified against a database. These certificates confirm only that the email address is unique to the subscriber and are appropriate for low-security applications.

Class 2 Certificates: The identity of the subscriber is verified against a trusted database such as a government-issued identity document. These were widely used for income tax e-filings and company registry filings.

Class 3 Certificates: Require in-person verification before a Registration Authority or the CA itself. These are the highest-assurance certificates required for high-value applications such as e-tendering, e-procurement, and court e-filings.

With the increasing integration of Aadhaar-based authentication, the verification process has been considerably streamlined. e-Mudhra and other CAs now offer paperless certificate issuance based on Aadhaar OTP or biometric verification, significantly reducing time and cost while maintaining identity assurance levels.²⁷

4.3 Issuance of Certificates

Under Section 35(4), the Certifying Authority may, after considering the certification practice statement and making such enquiries as it deems fit, grant the certificate or, for reasons recorded in writing, reject the application; no certificate may be granted unless the CA is satisfied that the applicant holds the private key corresponding to the public key to be listed in the certificate and that the public key can be used to verify a digital signature created by that private key, and no application may be rejected without giving the applicant a reasonable opportunity of showing cause.²⁸

In practice, upon issuance the CA publishes the certificate in its publicly accessible repository,

²⁵ IT Act § 35(2)–(3).

²⁶ See Controller of Certifying Authorities, Guidelines, <https://cca.gov.in/guidelines.html> (last visited Oct. 14, 2026); CA Rules.

²⁷ IT Act sched. II (e-authentication technique using Aadhaar or other e-KYC services; issuance of a Digital Signature Certificate based on e-authentication); Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015, G.S.R. 61(E) (Jan. 27, 2015) (India).

²⁸ IT Act § 35(4) & provisos.

notifies the subscriber, and ensures that the certificate accurately reflects the information contained in the application.²⁹

V. REVOCATION AND WITHDRAWAL OF ELECTRONIC SIGNATURES

5.1 Distinction Between Suspension and Revocation

The IT Act and the CA Rules draw a distinction between two mechanisms for invalidating a certificate: suspension (temporary) and revocation (permanent). This distinction has significant practical consequences for the rights of subscribers and the obligations of relying parties.³⁰

5.2 Suspension of Digital Signature Certificates (Section 37)

Under Section 37, the Certifying Authority that issued a certificate may suspend it: (a) on receipt of a request from the subscriber listed in the certificate or any person duly authorised to act on the subscriber's behalf; or (b) if it is of the opinion that the certificate should be suspended in the public interest.³¹

A certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard, and on suspension the CA must communicate the suspension to the subscriber.³²

5.3 Revocation of Digital Signature Certificates (Section 38)

Section 38 provides two pathways for revocation:

Revocation on Request, Death or Dissolution (Section 38(1)): A Certifying Authority may revoke a digital signature certificate where the subscriber or any person authorised by the subscriber requests revocation, upon the death of the subscriber, or upon the dissolution of the firm or winding up of the company where the subscriber is a firm or company.³³

CA-Initiated Revocation (Section 38(2)): Subject to the hearing requirement in Section 38(3), a Certifying Authority may revoke a certificate at any time if it is of the opinion that: (a) a material fact represented in the certificate is false or has been concealed; (b) a requirement for issuance of the certificate was not satisfied; (c) the CA's private key or security system was compromised in a manner materially affecting the certificate's reliability; or (d) the subscriber

²⁹ See IT Act §§ 34, 36; CA Rules.

³⁰ IT Act §§ 37–39.

³¹ IT Act § 37(1).

³² IT Act § 37(2)–(3).

³³ IT Act § 38(1).

has been declared insolvent or dead, or, where the subscriber is a firm or company, has been dissolved, wound up or otherwise ceased to exist.³⁴

5.4 Procedure, Notice, and Effective Date

Section 38(3) imposes a hearing requirement: a certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter, and Section 38(4) requires the Certifying Authority to communicate any revocation to the subscriber.³⁵ Section 39 further requires the CA to publish a notice of suspension or revocation in the repository specified in the certificate.³⁶ These procedural safeguards ensure that subscribers and relying parties are not left unaware of the status of a certificate, which could otherwise cause significant commercial harm.

Once revoked, the certificate details are published in the Certificate Revocation List (CRL), a publicly accessible registry of invalidated certificates. Relying parties are expected to check the CRL or use the Online Certificate Status Protocol (OCSP) before relying on a certificate.³⁷ The Act does not specify an effective date of revocation in the notice, and the position in respect of transactions concluded before the publication of the notice is therefore a matter of the general law and of the CA's Certification Practice Statement. Section 73 is instructive in this regard, since it permits the publication of a revoked or suspended certificate for the purpose of verifying a digital signature created prior to the suspension or revocation, which presupposes that earlier signatures are not retrospectively invalidated.³⁸

VI. GENERATING KEY PAIRS

7.1 Legal Significance of Key Generation

The generation of the cryptographic key pair is the foundational technical act upon which the entire digital signature system rests. The legal framework recognises that the manner of key generation directly affects the security of the resulting signatures — a weakly generated key pair compromises every document subsequently signed with the private key.³⁹

³⁴ IT Act § 38(2).

³⁵ IT Act § 38(3)–(4).

³⁶ IT Act § 39.

³⁷ See IT Act § 39; CA Rules.

³⁸ IT Act § 73(1) (proviso).

³⁹ IT Act §§ 16, 40.

7.2 Technical Process of Key Generation

Key pair generation involves:

- (a) **Selection of Algorithm:** The CA Rules and the Controller's standards prescribe approved cryptographic algorithms. Currently, RSA (Rivest-Shamir-Adleman) with a minimum key length of 2048 bits and ECDSA (Elliptic Curve Digital Signature Algorithm) with approved curves are recognised.⁴⁰
- (b) **Random Number Generation:** The security of any cryptographic key is fundamentally dependent upon the randomness of the seed used in its generation. Predictable or low-entropy random number generators represent a critical vulnerability. Hardware Security Modules (HSMs) are typically used by CAs to ensure high-quality randomness.
- (c) **Key Storage:** The private key must be stored in a secure cryptographic device (such as a USB token or smart card) that prevents extraction of the key material. The Controller's guidelines require that Class 3 certificates be issued only on hardware cryptographic tokens certified to FIPS 140-2 Level 2 or equivalent standards.

VIII. ACCEPTANCE OF DIGITAL SIGNATURE CERTIFICATES

8.1 The Concept of Acceptance

The acceptance of a digital signature certificate is a legally significant act that triggers the subscriber's representations and liabilities under the IT Act. As noted in the discussion of Section 41, acceptance occurs when the subscriber publishes or authorises the publication of the certificate to any person or in any repository, or otherwise demonstrates approval of it.⁴¹

The concept of acceptance in digital signature law reflects a general principle of certification practice: the CA issues the certificate, but the subscriber's voluntary assumption of the rights and obligations associated with it by publishing or using the certificate completes the legal relationship.

8.2 Representations Made upon Acceptance

By accepting a digital signature certificate, the subscriber represents to all who reasonably rely on it that: (a) the subscriber holds, and is entitled to hold, the private key corresponding to the public key listed in the certificate; (b) all representations made by the subscriber to the CA in

⁴⁰ CA Rules r. 6 & scheds.; Controller of Certifying Authorities, Guidelines, <https://cca.gov.in/guidelines.html> (last visited Oct. 14, 2026).

⁴¹ IT Act § 41(1).

obtaining the certificate, and all material relevant to the information contained in the certificate, are true; and (c) all information in the certificate that is within the subscriber's knowledge is true.⁴² The subscriber is also expected to use the certificate in accordance with its stated purpose and the limitations imposed by the CA's Certification Practice Statement.

8.3 Relying Parties and Good Faith

A critical aspect of the acceptance mechanism is its effect upon relying parties. The IT Act creates a system where a relying party who checks a certificate and finds it to be valid (not revoked or suspended, issued by a licensed CA, and not expired) is entitled to rely upon the representations in the certificate without independent verification.⁴³

8.4 Practical Implications of Acceptance

In practice, certificate acceptance occurs when the subscriber uses the certificate for the first time — filing a tax return, signing a contract, or submitting a bid in an e-procurement system. The law treats this first use as the manifestation of acceptance, since Section 41(1) deems acceptance on any demonstration of approval.⁴⁴

The implications are significant: from the moment of acceptance, the subscriber is presumed to have full knowledge of the certificate's contents, including any limitations on its use specified in the certificate or the CA's CPS. A subscriber who uses a certificate for purposes beyond those authorised in the CPS may find that the CA's liability limitations are enforceable against them.

X. PENALTIES AND ADJUDICATION

10.1 Overview of the Penal Framework

The IT Act establishes a comprehensive scheme of penalties for violations related to electronic signatures and digital certificates. These penalties may be classified as: (a) civil penalties and compensation adjudicated by the Adjudicating Officer; and (b) criminal penalties enforced by police and prosecuted before criminal courts.⁴⁵

⁴² IT Act § 41(2).

⁴³ IT Act §§ 36, 41(2).

⁴⁴ IT Act § 41(1).

⁴⁵ IT Act chs. IX, XI.

10.2 Certificate-Specific Offences

Section 71 — Misrepresentation to Controller or CA:

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or electronic signature certificate shall be punished with imprisonment for a term which may extend to two years, or with a fine which may extend to one lakh rupees, or with both.⁴⁶

Section 73 — Penalty for Publishing Electronic Signature Certificate False in Certain Particulars:

No person shall publish an electronic signature certificate, or otherwise make it available to any other person, with the knowledge that the Certifying Authority listed in the certificate has not issued it, that the subscriber listed in the certificate has not accepted it, or that the certificate has been revoked or suspended, unless the publication is for the purpose of verifying a signature created prior to such suspension or revocation. Contravention is punishable with imprisonment for a term which may extend to two years, or with a fine which may extend to one lakh rupees, or with both.⁴⁷

Section 74 — Publication for Fraudulent Purpose:

Any person who knowingly creates, publishes, or otherwise makes available an electronic signature certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with a fine which may extend to one lakh rupees, or with both.⁴⁸

The distinction between Sections 73 and 74 is significant: Section 73 targets the publication of a certificate with knowledge that it was not issued by the listed CA, was not accepted by the listed subscriber, or has been revoked or suspended, while Section 74 addresses the creation or publication of a certificate for a fraudulent or unlawful purpose. Both may be invoked where a person creates a false certificate and then publishes it for a fraudulent purpose.

Section 72 — Breach of Confidentiality and Privacy:

Any person who, in pursuance of any of the powers conferred under the Act, rules or regulations, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and discloses it to any other person is liable under Section 72. As originally enacted and as amended in 2008, this attracted imprisonment up to two years or a fine up to one lakh rupees, or both;

⁴⁶ IT Act § 71.

⁴⁷ IT Act § 73.

⁴⁸ IT Act § 74.

the Jan Vishwas (Amendment of Provisions) Act, 2023 has since recast the consequence as a monetary penalty of up to twenty-five lakh rupees.⁴⁹

Section 68 — Failure to Comply with Orders of Controller:

The Controller may, by order, direct a Certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, if necessary to ensure compliance with the Act, rules or regulations.⁵⁰ Following the 2008 amendment, intentional or knowing non-compliance was punishable with imprisonment up to two years or a fine up to one lakh rupees, or both; the Jan Vishwas Act, 2023 has replaced this with a penalty which may extend to twenty-five lakh rupees.⁵¹

10.3 General Cyber Offences Relevant to Electronic Signatures

Section 43 — Penalty and Compensation for Damage to Computer Systems:

Any person who, without permission of the owner or person in charge, accesses or secures access to a computer, computer system, or computer network and downloads or copies any data, computer database, or information, or introduces any computer virus, or damages or denies access, shall be liable to pay damages by way of compensation to the person so affected.⁵² This provision applies to a person who unauthorisedly accesses a subscriber's computer system to steal their private key.

Section 66C — Identity Theft:

Whoever, fraudulently or dishonestly, makes use of the electronic signature, password, or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine which may extend to one lakh rupees.⁵³ This provision is of direct relevance to electronic signature fraud.

Section 66D — Cheating by Personation Using Computer Resource:

Whoever, by means of any communication device or computer resource, cheats by personating, shall be punished with imprisonment for a term which may extend to three years, and shall also be liable to fine which may extend to one lakh rupees.⁵⁴ This provision, read with Section 66C,

⁴⁹ IT Act § 72; Jan Vishwas (Amendment of Provisions) Act, 2023, No. 18 of 2023 (India) (amending IT Act provisions with effect from Nov. 30, 2023).

⁵⁰ IT Act § 68(1).

⁵¹ IT Act § 68(2); Jan Vishwas (Amendment of Provisions) Act, 2023, No. 18 of 2023 (India).

⁵² IT Act § 43. The original statutory ceiling of one crore rupees on such compensation was removed by the 2008 amendment, with pecuniary jurisdiction now governed by § 46(1A). *See* Information Technology (Amendment) Act, 2008, No. 10 of 2009 (India).

⁵³ IT Act § 66C.

⁵⁴ IT Act § 66D.

provides a comprehensive criminal framework for electronic signature fraud. General offences of forgery and cheating under the Bharatiya Nyaya Sanhita, 2023 (which replaced the Indian Penal Code, 1860) may also apply to forged electronic records.⁵⁵

10.4 The Adjudication Mechanism

Appointment of Adjudicating Officers (Section 46):

For the purpose of adjudging whether any person has committed a contravention of the provisions of the IT Act, the Central Government shall appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a state government to be an Adjudicating Officer, possessing such experience in the field of information technology and legal or judicial experience as may be prescribed.⁵⁶

Powers of Adjudicating Officers:

The Adjudicating Officer exercises jurisdiction over claims for injury or damage not exceeding five crore rupees, with claims above that figure vesting in the competent court.⁵⁷ The Adjudicating Officer, after giving a reasonable opportunity of representation, may impose such penalty or award such compensation as is provided under the relevant section, and has the powers of a civil court, including those of summoning and enforcing the attendance of persons and examining them on oath.⁵⁸

Factors Considered in Adjudication (Section 47):

While adjudging the quantum of compensation, the Adjudicating Officer shall have due regard to: (a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default; (b) the amount of loss caused to any person as a result of the default; and (c) the repetitive nature of the default.⁵⁹

10.5 The Appellate Tribunal (Formerly the Cyber Appellate Tribunal)

Establishment and Composition (Section 48):

The IT Act originally provided for a Cyber Appellate Tribunal (CAT) to exercise appellate jurisdiction over orders of the Adjudicating Officer. By Part XIV of Chapter VI of the Finance Act, 2017, the CAT was merged into the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which has since been the Appellate Tribunal for the purposes of the IT Act, with

⁵⁵ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India) (in force July 1, 2024).

⁵⁶ IT Act § 46(1), (3).

⁵⁷ IT Act § 46(1A).

⁵⁸ IT Act § 46(2), (5).

⁵⁹ IT Act § 47.

effect from 26 May 2017.⁶⁰

Jurisdiction (Section 57):

Any person aggrieved by an order made by the Controller or an Adjudicating Officer may prefer an appeal to the Appellate Tribunal.⁶¹ The Tribunal has powers analogous to those of a civil court and may confirm, modify, or set aside the order appealed against, with a further appeal lying to the High Court on a question of fact or law.⁶²

Practical Limitations:

The CAT faced significant operational challenges before the merger: vacancies in the office of Chairperson led to extended periods of non-functionality, and a substantial number of cases (102, according to the Law Commission) were pending at the time of merger.⁶³ This institutional weakness has been identified by commentators as a fundamental gap in the implementation of the Act's penalisation framework.⁶⁴ Whether the merger with TDSAT has resolved those difficulties remains a matter for empirical study.

10.6 Compounding of Offences (Section 77A)

The IT (Amendment) Act, 2008 introduced Section 77A, permitting a court of competent jurisdiction to compound offences under the Act, other than offences for which the punishment is life imprisonment or imprisonment for a term exceeding three years. The Section bars compounding where the accused is, by reason of previous conviction, liable to enhanced punishment or to a punishment of a different kind, or where the offence affects the socio-economic conditions of the country or has been committed against a child below eighteen years or a woman, providing an expeditious resolution mechanism.⁶⁵

XII. CONCLUSION

The Information Technology Act, 2000 established a strong foundation for electronic signatures in India through certifying authorities, certificate procedures, subscriber duties, and civil and criminal penalties. Digital signatures now support government services, finance, courts, and commerce. However, enforcement limits, weak penalties for serious fraud, past

⁶⁰ Finance Act, 2017, No. 7 of 2017, § 169 (India) (substituting “Appellate Tribunal” for “Cyber Appellate Tribunal” throughout the IT Act and amending § 48(1)); IT Act § 48(1).

⁶¹ IT Act § 57(1).

⁶² IT Act §§ 58, 62.

⁶³ Law Comm’n of India, Report No. 272, Assessment of Statutory Frameworks of Tribunals in India, annex. I (2017).

⁶⁴ See generally Gupta & Agarwal, *supra* note 30.

⁶⁵ IT Act § 77A(1)–(2) (applying Code of Criminal Procedure, 1973, §§ 265B, 265C); see also *id.* § 77B (offences punishable with imprisonment of three years to be bailable).

tribunal vacancies and delays, emerging technologies, and unresolved cross-border recognition remain challenges. Reform should strengthen penalties, build law enforcement and adjudicatory capacity, pursue mutual recognition agreements, clarify blockchain signatures' legal status, and apply the Digital Personal Data Protection Act, 2023 to Certifying Authorities' handling of personal information. These measures are essential to maintaining public confidence in India's digital economy.

XIII. BIBLIOGRAPHY

Statutes and Legislation

- Information Technology Act, 2000, No. 21 of 2000 (India), as amended by the Information Technology (Amendment) Act, 2008, No. 10 of 2009 (India), and subsequently by the Finance Act, 2017, No. 7 of 2017 (India), and the Jan Vishwas (Amendment of Provisions) Act, 2023, No. 18 of 2023 (India).
- Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023 (India) (§§ 39, 61, 63).
- Indian Evidence Act, No. 1 of 1872 (India) (§§ 65A, 65B) (repealed with effect from July 1, 2024).
- Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India); Indian Penal Code, No. 45 of 1860 (India) (repealed).
- Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
- Information Technology (Certifying Authorities) Rules, 2000 (India).
- Information Technology (Certification Practice Statement) Guidelines, 2001 (India).
- Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015, G.S.R. 61(E) (Jan. 27, 2015) (India).
- Notification S.O. 1119(E), Gazette of India, Extraordinary, pt. II, § 3(ii), No. 985 (Mar. 5, 2019) (amending the Second Schedule to the IT Act).

International Instruments

- U.N. Comm'n on Int'l Trade L., Model Law on Electronic Commerce with Guide to Enactment 1996, G.A. Res. 51/162 (Jan. 30, 1997).
- U.N. Comm'n on Int'l Trade L., Model Law on Electronic Signatures with Guide to Enactment 2001, G.A. Res. 56/80 (Dec. 12, 2001).
- 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 (eIDAS Regulation), 2014 O.J. (L 257) 73.

Case Law

- *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).
- *K.S. Puttaswamy (Privacy-9J.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
- *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 S.C.C. 1 (India).
- *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).

Books

- Verma, S.K. & Raman Mittal (eds.), *Legal Dimensions of Cyber Space* (Indian Law Institute 2004).
- Joga Rao, S.V., *Law of Cyber Crimes and Information Technology Laws* (Wadhwa & Co. 2004).
- Ryder, Rodney D., *Guide to Cyber Laws (Information Technology Act, 2000, E-Commerce, Data Protection & the Internet)* (Wadhwa & Co. 2007).
- Gupta & Agarwal, *Information Technology: Law and Practice* (Universal Law Publishing Co. 2010).
- Godbole, Nina & Sunita Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives* (Wiley India 2011).
- Handl, Günther, Joachim Zekoll & Peer Zumbansen (eds.), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (Martinus Nijhoff Publishers 2012).
- Kamath, Nandan, *Law Relating to Computers, Internet and E-Commerce* (Universal Law Publishing Co., latest ed.).

Reports and Official Publications

- Law Comm'n of India, Report No. 272, *Assessment of Statutory Frameworks of Tribunals in India* (2017).
- Ministry of Electronics and Information Technology, *Annual Report on Certifying Authorities* (Gov't of India 2023–24).
- Reserve Bank of India, *Report of the Working Group on Digital Lending* (RBI 2021).
- U.N. Comm'n on Int'l Trade L., *Explanatory Note on the UNCITRAL Model Law on Electronic Commerce* (U.N. 1996).
- Controller of Certifying Authorities, *Interoperability Guidelines for Digital Signature Certificates* (CCA, Gov't of India 2015).

- Controller of Certifying Authorities, *Licensed CAs*, https://cca.gov.in/licensed_ca.html (last visited Oct. 14, 2026).

