INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

MEANING AND LEGAL FRAMEWORK OF ELECTRONIC SIGNATURE IN INDIA

AUTHORED BY - HARIKRISHNAN T P
LLM STUDENT GOVT LAW COLLEGE ERNAKULAM

Introduction

The rapid digitization of commerce necessitates a secure and legally recognized method for authenticating electronic records: the electronic signature. The robust functioning of this system hinges on a Public Key Infrastructure (PKI) overseen by statutory bodies, typically designated as Certifying Authorities (CAs) or Issuing Authorities. These CAs are the lynchpin, licensed to issue and manage the Digital Signature Certificate (DSC), which acts as the digital identity of the signatory. The technical foundation of the electronic signature involves generating key pairs—a cryptographic private key and its corresponding public key. The legal responsibility for safeguarding the system rests heavily on the individual user, termed the subscriber. The subscriber's primary and non- negotiable duties include the stringent control of the private key; its compromise is catastrophic to the signature's validity.

The legal framework meticulously governs the entire DSC lifecycle. It outlines the process for the initial grant of the certificate following due diligence, mandates formal acceptance of the digital signature certificate by the subscriber, and defines the critical procedures for revocation and withdrawal in cases of key compromise, change in material facts, or misuse. Furthermore, the statute clearly enumerates the other duties of subscribers, ensuring their continued compliance with security standards. Finally, to ensure the trustworthiness and enforceability of digital transactions, the framework includes rigorous penalties and adjudication provisions, allowing for the legal review and punishment of individuals or CAs who violate the stipulated security and procedural requirements, thereby maintaining high public confidence in digital commerce.

Electronic Signature

An electronic signature (or e-signature) is a broad term that refers to any electronic sound, symbol, or process that indicates a person's intent to agree to the content of a document or record.[1] essentially, it's the digital equivalent of a traditional "wet ink" signature. An electronic

ISSN: 2582-6433

signature (e-signature) is any mark, symbol, or process made on a digital document to show a person's approval, consent, or agreement—just like signing with a pen, but in electronic form.It can be typed, drawn, clicked, or created using secure digital tools.

Examples of E-Signatures:
Typing your name at the end of an email (e.g., "Regards, John").Clicking an "I Agree" button on a website while accepting terms. Drawing your signature on a touchscreen using a stylus or finger. Using scanned images of your handwritten signature on a PDF.Digital signature using cryptography (e.g., signing with Aadhaar e-sign in India).[1]

Intent to Sign: The core idea is that the signatory intends to be bound by the terms of the document, just as they would with a handwritten signature. Electronic Form: It exists entirely in a digital environment. This can be as simple as: Typing your name into a document or email.[3]Clicking an "I Agree" button on a website. Drawing your signature with a mouse or finger on a touchscreen device.[5]A scanned image of a handwritten signature.[6]

Logically Associated: The electronic signature is linked to the document it's signing, ensuring it applies to that specific content.[7]Legal Validity: In many jurisdictions worldwide (like the U.S. with the ESIGN Act and UETA, and the EU with eIDAS), electronic signatures are legally recognized and enforceable, often holding the same legal weight as handwritten signatures.

Electronic Signature vs. Digital Signature:

While often used interchangeably, it's important to note that digital signatures are a specific type of electronic signature that offers a higher level of security and assurance. Digital signatures use cryptographic techniques (like Public Key Infrastructure or PKI) and digital certificates issued by trusted third parties to: Verify Identity: Strongly authenticate the signer's identity. Ensure Integrity: Guarantee that the document has not been altered since it was signed. Provide Non-Repudiation: Make it difficult for the signer to later deny having signed the document. The term "electronic signature" itself isn't ancient, but the concept of using electronic means to show intent and authenticate a document has surprisingly deep roots.[2]

[1] *Information Technology Act, 2000*, Section 2(ta) — defines "electronic signature" as authentication of any electronic record by a subscriber by means of an electronic technique specified in the Second Schedule and includes digital signature.
[2] United Nations Commission on International Trade Law (UNCITRAL), *Model Law on Electronic Signatures*, 2001

ISSN: 2582-6433

Etymology

(Pre-Digital Era):Telegraphs (19th Century): One of the earliest examples of a legal precedent for "electronic" signatures dates back to the 1869 New Hampshire Supreme Court case, *Howley v. Whipple*. The court ruled that telegraphic messages could be legally binding, essentially recognizing that [3]a signature transmitted electronically (via a "copper wire a thousand miles long" using "electricity" as a "subtle fluid") had the same legal weight as a handwritten one. This highlights the foundational idea that the *method* of signing can be electronic, as long as the *intent* is clear.

Howley v. Whipple (1869)
Court: New Hampshire Supreme Court (USA) Facts: In this case, one party had entered into a contract using a telegram (which was considered "electronic" for that time).Issue: Could a telegram count as a "signed writing" for a contract? Decision: The court held YES – a telegram is a valid written communication, and the sender's name at the end serves as a signature. Importance: This was one of the first cases recognizing that an electronic medium (telegram) can count as a signed document.

Fax Machines (Late 19th - 20th Century): While the fax machine was invented in 1846, its widespread use in the late 20th century became a common way to send signed documents electronically. Although the original signature was "wet ink," the transmission of its image was electronic, and these faxed signatures were often accepted legally.

Emergence of the Term and Modern Legal Frameworks:

The specific term "electronic signature" as we understand it today became prominent with the rise of digital technology and the need for legal clarity in electronic transactions[4]. Cryptography means "secret writing." It is the science of protecting information so that only the right person can read or use it. In simple words: It hides your information using codes. Only someone with the right key can unlock (read) it. It ensures privacy (no one else can read), authenticity (it's really from you), and integrity (it wasn't changed).

1970s - 1980s: Cryptography and Digital Signatures: The theoretical foundations for what we

[3] *Howley v. Whipple*, 48 N.H. 487 (1869).
[4] Stallings, William. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2017.

ISSN: 2582-6433

now call "digital signatures" (a more secure type of electronic signature) emerged in the late 1970s with the work of cryptographers.

Relevance of Cryptography in E-Signature Evolution

1. From Simple to Secure – Early e-signatures (like telegrams in *Howley v. Whipple*) only proved intent, but not authenticity or integrity. Anyone could forge a name. Cryptography solved this problem.
2. Digital Signatures – In the 1990s, public key cryptography (asymmetric encryption) transformed e-signatures. A private key is used by the signer to create a unique digital signature. A public key allows others to verify its authenticity. This ensures the message hasn't been altered (integrity) and confirms who signed it (authenticity).
3. Legal Acceptance –Laws like the U.S. E-SIGN Act (2000) and India's IT Act, 2000 (Sections 3 & 5) explicitly require the use of secure digital signatures (cryptography-based).These signatures are tamper-evident, making them admissible in court.

1990s: Commercialization and Standardization: As the internet and personal computers became more common, the need for legally recognized electronic transactions grew.

Lotus Notes 1.0 (1989): This software was one of the first widely marketed products to offer digital signature capabilities.PDF Format (1999): The possibility of embedding digital signatures into PDF documents was introduced. Late 1990s - Early 2000s: Legal Acts: This is when the term "electronic signature" truly cemented its place in legal and commercial language.

Uniform Electronic Transactions Act (UETA) - USA (1999): This influential model law, adopted by many U.S. states, provided a broad definition for "electronic signature" as "an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."

Electronic Signatures in Global and National Commerce Act (ESIGN Act) - USA (2000): This federal law further solidified the legal validity of electronic signatures in the United States, giving them the same legal weight as traditional wet-ink signatures for most purposes. This act was crucial in driving widespread adoption. eSignature Directive (1999) and eIDAS Regulation (2016) - European Union: Similar legislative frameworks were established in Europe to provide legal certainty for electronic signatures across member states.

ISSN: 2582-6433

In essence, while the *idea* of an electronic signature can be traced back to early electronic communication methods, the *term* and its formal legal recognition gained widespread usage and definition with the advent of the internet and the need for secure and legally binding digital transactions in the late 20th and early 21st centuries.[5]Electronic signatures hold significant legal validity in India, primarily governed by the Information Technology Act, 2000 (IT Act), as amended by the Information Technology (Amendment) Act, 2008.[5]

Definition of Electronic Signature under Indian Acts

The core definition is found in Section 2(1)(ta) of the Information Technology Act, 2000 (as amended):[6]"Electronic Signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature."[6]

Key aspects of this definition:

Authentication of Electronic Record: The primary purpose of an electronic signature is to authenticate an electronic record (which itself is defined broadly in the IT Act to include data, records, images, or sound stored, received, or sent in electronic form).By a Subscriber: It refers to the person who holds the electronic signature or digital signature certificate. Electronic Technique specified in the Second Schedule: This makes the definition technology-neutral. While earlier, the IT Act largely focused on "digital signatures" (a specific cryptographic technique), the 2008 amendment broadened it to "electronic signature" to encompass other reliable electronic authentication techniques that the Central Government may specify in the Second Schedule.[3] This allows for evolving technologies like Aadhaar-based eSign, biometric signatures, etc. Includes Digital Signature: This is crucial. A digital signature (which uses asymmetric crypto systems and hash functions) is considered a subset of electronic signatures under Indian law.

Section 3A of the IT Act further specifies when an electronic signature is considered reliable:[7]

An electronic signature or electronic authentication technique shall be considered reliable if:

[5] U.S. Department of Commerce, *Electronic Signatures in Global and National Commerce Act (E-SIGN Act), 2000*, and European Parliament, *Regulation (EU) No 910/2014 (eIDAS Regulation), 2016.*
[6] Section 2(1)(ta) of the Information Technology Act, 2000 (as amended
[7] Section 3A, of the Information Technology Act, 2000

ISSN: 2582-6433

The signature creation data or authentication data are, within the context in which they are used, linked to the signatory or authenticator and to no other person.[4]The signature creation data or authentication data were, at the time of signing, under the control of the signatory or authenticator and of no other person.[56]Any alteration to the electronic signature made after affixing such signature is detectable.[78]Any alteration to the information made after its authentication by electronic signature is detec[9]table.[10]It fulfils such other conditions which may be prescribed.[11]

Section 5 of the IT Act grants legal recognition to electronic signatures, stating that where any law requires information or a document to be signed, that requirement is deemed to be satisfied if it is authenticated by an electronic signature as per the IT Act.[12]

Exceptions: It's important to note that certain documents are exempt from electronic signing and still require a physical (wet-ink) signature as per the First Schedule of the IT Act, such as:[8]

A negotiable instrument (other than a cheque)[13,] A Power of Attorney[14]A Trust DeedA, Will or any other testamentary disposition, Any contract for the sale or conveyance of immovable property or any interest in such property.[15]

Types of E-Signatures Recognized in India:

1. Digital Signatures (Section 3): These are the highly secure, certificate- based signatures relying on asymmetric cryptography and DSCs issued by Certifying Authorities. They offer strong authentication, integrity, and non-repudiation.[9]
2. Electronic Signatures (Section 3A): Introduced by the IT (Amendment) Act, 2008, this category broadens the scope to include other electronic authentication techniques. An electronic signature is considered reliable if:

The signature creation data is linked uniquely to the signatory.
The signature creation data was under the sole control of the signatory at the time of signing. Any alteration to the electronic signature after affixing it is detectable. Any alteration to the information after its authentication by electronic signature is detectable. It fulfills any other prescribed conditions. The Second Schedule to the IT Act specifies techniques for electronic signatures, most notably Aadhaar eSign (authentication using Aadhaar number and

[8] Information Technology Act, 2000, Section 5 read with First Schedule, Government of India.
[9] Information Technology Act, 2000, Section 3read with First Schedule, Government of India.

ISSN: 2582-6433

OTP/biometrics). This has significantly boosted the adoption of e-signatures for a wide range of transactions

Legal Validity and Enforceability:

- Section 4: Legal Recognition of Electronic Records: Grants legal validity to electronic records, making them equivalent to paper-based documents.[10]
- Section 5: Legal Recognition of Digital Signatures: States that where any law requires information to be authenticated by affixing the signature or to be signed, that requirement shall be deemed to have been satisfied if such information is authenticated by means of a digital signature affixed in such manner as may be prescribed by the Central Government.
- Section 10A: Validity of Contracts Formed Through Electronic Means: This crucial section clarifies that a contract cannot be denied enforceability solely on the ground that it was formed through electronic means. This provides explicit legal backing for e-contracts.
- Indian Evidence Act, 1872 (Amendments): Sections 65A and 65B deal with the admissibility of electronic records as evidence. Section 47A specifically states that the opinion of the Certifying Authority is a relevant fact when the court has to form an opinion as to the electronic signature of any person. Sections 85A, 85B, and 85C create presumptions in favour of electronic records and electronic signatures:

Section 85A: Presumes that electronic agreements containing electronic signatures are concluded between the parties. Section 85B: Presumes the integrity of secure electronic records and the validity of secure electronic signatures. Section 85C: Presumes the truth of facts stated in an Electronic Signature Certificate.[11]

Background of the Case: Narayana v. K.S. Krishna (2019) - Karnataka High Court

While specific detailed facts of the *Narayana v. K.S. Krishna* case regarding the digital signature on a promissory note are not widely published in easily accessible public domains (as it might be a lower court judgment or unreported, or details are confined to legal databases requiring subscription), the general nature of such a case would involve the following[12]

[10] Information Technology Act, 2000, Section 4 read with First Schedule, Government of India.
[11] Information Technology Act, 2000, Section 85 read with First Schedule, Government of India.
[12] *Narayana v. K.S. Krishna*, Karnataka High Court, 2019 – Case discussing enforceability of digitally signed promissory notes under the IT Act.

ISSN: 2582-6433

The Dispute: Typically, these cases arise when a lender (plaintiff) sues a borrower (defendant) for the recovery of money, presenting a promissory note as evidence of the debt. The Promissory Note: In this specific instance, the promissory note, which is usually a physical document, was claimed to have been digitally signed. This is the core unusual aspect that brought the IT Act into play. The Challenge: The defendant (borrower) would likely have challenged the validity or authenticity of the promissory note, specifically questioning whether a digitally signed promissory note has legal enforceability, especially given the traditional requirement for physical signatures and the exclusions in the IT Act. The Plaintiff's Argument: The plaintiff (lender) would have argued that the digital signature on the promissory note is valid under the IT Act, 2000, and therefore, the promissory note should be considered a legally enforceable document.[13]

Karnataka High Court's Stance and Reasoning (Inferred):

The Karnataka High Court *acknowledged the validity of a digital signature on a promissory note, subject to the conditions of the IT Act*. This acknowledgment, while appearing to contradict the First Schedule's exclusion, likely hinges on a nuanced interpretation or specific circumstances:

Focus on Evidentiary Value vs. Substantive Validity: The court might have distinguished between the *substantive legal validity* of a digitally signed promissory note as a fully enforceable negotiable instrument and its *evidentiary value* as proof of a debt or transaction. While it might not be a "negotiable instrument" in the strict sense for all purposes of the Negotiable Instruments Act, the digital signature could still serve as valid electronic evidence (under Section 65A/65B of the Evidence Act) of the underlying debt or agreement. The court might have accepted it as a valid *electronic record* proving the transaction, even if it didn't grant it the full status of a "negotiable instrument" for all purposes (e.g., easy transferability to third parties by endorsement, which relies on physical characteristics).[14]

Specific Context of the Digital Signature: The court might have looked at the context in which the digital signature was affixed. Was it part of a broader electronic contract where the promissory note was an ancillary document? If the digital signature was merely an authentication of an underlying *agreement to pay*, and not solely intended to create a *negotiable*

[13] ibid

[14] *Narayana v. K.S. Krishna*, Karnataka High Court, 2019 – Case discussing enforceability of digitally signed promissory notes under the IT Act.

ISSN: 2582-6433

instrument that could be freely negotiated, the court might have viewed it differently.

"Subject to the conditions of the IT Act": This phrase is key. It implies that the court was not blindly accepting it but was ensuring that the digital signature met all the rigorous technical and security requirements of the IT Act for reliability (e.g., Section 3 on authentication, Sections 14 and 15 on secure electronic records and digital signatures, and Section 40 regarding the secure generation of the key pair). If these conditions were met, the court might have seen it as sufficiently reliable proof of the signatory's intent, even if it didn't override the First Schedule's blanket exclusion for a negotiable instrument *per se*.

"Evolving Acceptance of Digital Documents": Your observation about "evolving acceptance" is crucial. Courts are often pragmatic. While the law might have specific exclusions, if a transaction is clearly proven and the digital signature provides a high degree of assurance of authenticity and integrity, a court might lean towards upholding the underlying intent of the parties, rather than allowing a technicality to defeat justice. This is especially true if the dispute is simply about recovering a debt between the original parties, and not about the negotiability of the instrument to third parties.

The *Narayana v. K.S. Krishna* case, if interpreted as allowing a digitally signed promissory note to be valid *as proof of debt* (even if not fully a "negotiable instrument" under the Act), highlights:[15] Judicial Pragmatism: Courts are willing to interpret the law to facilitate electronic transactions where the intent is clear and the technology is reliable. Emphasis on Reliability: The "subject to the conditions of the IT Act" clause signifies that the court will scrutinize the security and authenticity of the digital signature. Broader Acceptance of Electronic Evidence: It reinforces the growing trend of accepting electronic records and signatures as valid evidence in Indian courts, even in traditional areas of law.

Issuing authority

For an electronic signature depends on the type of electronic signature and the legal framework it operates under. In general, for digital signatures, which are a more secure and legally robust type of electronic signature, the issuing authority is a Certifying Authority (CA).

[15] ib

ISSN: 2582-6433

Controller of Certifying Authorities (CCA): This is the apex body in India that licenses and regulates Certifying Authorities (CAs). The CCA operates under the Information Technology Act, 2000 (IT Act). They don't issue digital signature certificates directly to end-users, but they license the CAs who do.

Licensed Certifying Authorities (CAs): These are the entities authorized by the CCA to issue Digital Signature Certificates (DSCs) to individuals and organizations. They verify the identity of the signer and then issue the DSC, which contains the signer's public key and is signed by the CA's private key.

Examples of licensed CAs in India include: eMudhra LimitedCentre for Development of Advanced Computing, (C-DAC)Capricorn Identity Services Pvt. Ltd. Protean, eGov Technologies Limited (previously NSDL e-Gov)Verasys Technologies Private Limited (Vsign CA), IDSign CA, And others listed on the CCA's website.[16]

Controller of Certifying Authorities (CCA):

Role: The CCA is the apex regulatory body established under Section 17 of the IT Act. Its main functions (as per Section 18) include:[17] Licensing and regulating Certifying Authorities (CAs): The CCA grants licenses to CAs to issue Digital Signature Certificates. Laying down standards: It specifies the standards that CAs must follow, including technical and operational guidelines.

Establishing the Root Certifying Authority of India (RCAI): The CCA operates the RCAI, which digitally signs the public keys of the CAs, forming the root of trust in the Indian Public Key Infrastructure (PKI).Supervision and auditing: The CCA monitors the activities of licensed CAs to ensure compliance with the IT Act and its rules. Issuance: The CCA *does not* directly issue DSCs to end-users. Instead, it issues licenses to CAs.

*Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal and Others (2020) 7 SCC 1*Relevance: As discussed previously, this Supreme Court case, while primarily on Section 65B of the Evidence Act for admissibility of electronic records, indirectly stresses the

[16] Information Technology Act, 2000, Sections 17–34; Controller of Certifying Authorities (CCA), Ministry of Electronics and Information Technology (MeitY), Government of India – Legal framework for digital signatures and licensed Certifying Authorities.
[17] ib

ISSN: 2582-6433

importance of the issuing authority. For an electronic record (which could include a digitally signed document) to be admissible, its authenticity and integrity must be verifiable.[18]

Certifying Authorities (CAs)

In the context of e-signatures, especially digital signatures (a more secure type of e-signature), a Certifying Authority (CA) is a trusted third-party entity that issues digital certificates. These certificates are crucial for verifying the identity of individuals or entities in electronic transactions and for ensuring the integrity and authenticity of digital signatures. The CA acts as an impartial guarantor, linking a public key to a specific individual or organization and vouching for their identity. In India, the Controller of Certifying Authorities (CCA) licenses and regulates the CAs, establishing a framework for their operations and maintaining the Root Certifying Authority of India (RCAI)

Role and Functions:

Identity Verification: CAs perform rigorous identity verification checks before issuing digital certificates. This can involve physical presence, document verification, and other due diligence processes. Issuance of Digital Certificates: They issue digital certificates that contain the public key of the subscriber, their distinguished name (a unique identifier), the CA's distinguished name, and the CA's digital signature. Maintenance of Repositories: CAs maintain repositories of issued and revoked certificates, making them accessible for verification by relying parties. Ensuring Trust: By acting as a trusted intermediary, CAs enable secure and verifiable electronic transactions, thereby fostering trust in the digital ecosystem.[19]

Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal (2020) 7 SCC 1: This Supreme Court case primarily dealt with the interpretation of Section 65B of the Indian Evidence Act, 1872, concerning the admissibility of electronic records as evidence. While not directly about CAs, the judgment emphasizes the necessity of compliance with statutory provisions for authentication of electronic records.

In effect, it reinforces the legal framework within which CAs operate and their importance in establishing the genuineness of electronic documents and signatures. The case highlighted the

[18] Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal and Others (2020) 7 SCC 1
[19] ibid

ISSN: 2582-6433

need for proper certificates under Section 65B (4) for electronic evidence, indirectly affirming the chain of trust established by CAs for digital signatures.[20]

Grants of E-signatures

"Grant of e-signature" broadly refers to the legal recognition and authorization for a person or entity to use an electronic signature. More specifically, in the context of advanced and qualified electronic signatures (like digital signatures), it involves the issuance of a digital signature certificate by a Certifying Authority (CA) to a subscriber. This certificate, once "granted," enables the subscriber to create legally valid and secure electronic signatures.[21]

Process of Grant: Application: An individual or organization applies to a licensed Certifying Authority for a digital signature certificate. Identity Verification: The CA verifies the applicant's identity using various methods, as mandated by regulations. Key Pair Generation: A unique cryptographic key pair (a public key and a private key) is generated. The private key remains under the sole control of the subscriber, while the public key is embedded in the digital certificate. Certificate Issuance: Upon successful verification, the CA digitally signs and issues the digital certificate, which contains the subscriber's public key and other identifying information. This act of issuance constitutes the "grant" of the e-signature (specifically, a digital signature capacity) to the subscriber.

Revocations of E-signatures

Revocation of an e-signature, specifically a digital signature, refers to the act of invalidating a digital signature certificate before its scheduled expiry date. This is a critical security measure to prevent the misuse of a certificate if its associated private key is compromised or if the information contained in the certificate becomes invalid.[22]

Grounds for Revocation (as per IT Act, 2000, Section 38):
A Certifying Authority may revoke a Digital Signature Certificate issued by it under various circumstances, including but not limited to: Compromise of Private Key: If the private key

[20] Information Technology Act, 2000, Section 21; Controller of Certifying Authorities (CCA), Ministry of Electronics and Information Technology (MeitY), Government of India – Role and regulation of Certifying Authorities in issuing Digital Signature Certificates.
[21] Information Technology Act, 2000, Sections 3, 5, and 35; Controller of Certifying Authorities (CCA), Ministry of Electronics and Information Technology (MeitY), Government of India – Guidelines on Grant and Issuance of Digital Signature Certificates.
[22] Section 38 of it act 2000

ISSN: 2582-6433

associated with the digital signature certificate is compromised, lost, or suspected of being accessed by an unauthorized person. False Information: If a material fact represented in the Digital Signature Certificate is found to be false or concealed. Non-compliance with Requirements: If the requirements for the issuance of the certificate were not adequately met. Change in Subscriber Details: If there is a change in the subscriber's details, such as name, organization, or contact information, that renders the existing certificate inaccurate. Subscriber's Request: The subscriber or their authorized representative formally requests the revocation. Demise of Subscriber: In the event of the subscriber's death. Dissolution of Entity: If the subscriber is a firm or company and undergoes dissolution or winding up.

Withdrawal of Electronic Signatures

"Withdrawal of electronic signatures" is not a commonly used or legally defined term in the same way "revocation" is for digital signature certificates. In practice, when one refers to withdrawing an e-signature, it typically refers to a repudiation or challenge to the validity or authenticity of a previously affixed electronic signature, or a request for the revocation of the underlying digital signature certificate. It implies a situation where the signatory (or someone on their behalf) no longer wishes for their signature to be legally binding or effective for a particular document or transaction.[23]

Revocation of Digital Signature Certificate (DSC): As discussed previously, this is the formal process by which a Certifying Authority (CA) invalidates a DSC before its expiry. If a DSC is revoked, any signatures made *after* the revocation date using that certificate will generally be considered invalid. This is the closest legal concept to "withdrawal" of the *capacity* to sign electronically.

Repudiation of Signature: A party might "withdraw" their e-signature in the sense that they *deny* having affixed it, or argue that it was affixed without their consent, or that the document was altered after they signed it. This typically leads to a legal dispute regarding the authenticity and integrity of the electronic record and signature.[24]

[23] Information Technology Act, 2000, Sections 17–19; Controller of Certifying Authorities (CCA), Ministry of Electronics and Information Technology (MeitY), Government of India – Guidelines on Revocation and Suspension of Digital Signature Certificates
[24] ibid

ISSN: 2582-6433

Duties of Subscribers

A "subscriber" in the context of e-signatures (specifically digital signatures) is the person in whose name a Digital Signature Certificate (DSC) is issued. They are the individual or entity who holds the private key corresponding to the public key listed in the DSC and uses it to create digital signatures. The IT Act, 2000, places specific responsibilities on subscribers to ensure the security and integrity of their digital signatures.

Key Duties of Subscribers (as per IT Act, 2000, particularly Sections 40, 41, and 42): Generating Key Pair (Section 40): Upon acceptance of a DSC, the subscriber is required to generate their key pair (private and public keys) using a secure system. This ensures that the private key remains unique and under their sole control.[25]

Acceptance of Digital Signature Certificate (Section 41): A subscriber is deemed to have accepted a DSC if they publish or authorize its publication (e.g., in a repository) or otherwise demonstrate their approval. By accepting, the subscriber certifies to relying parties that:[26] They hold the private key corresponding to the public key in the DSC. All representations made to the Certifying Authority (CA) for obtaining the certificate are true. All information in the DSC known to the subscriber is true.

Control of Private Key (Section 42): This is perhaps the most crucial duty. Every subscriber must exercise reasonable care to: Retain control of their private key.Take all steps to prevent its disclosure to unauthorized persons.

Notification of Compromise (Section 42(2)): If the private key is compromised, lost, stolen, or suspected of being accessed by an unauthorized person, the subscriber has a statutory duty to immediately communicate this to the Certifying Authority in the prescribed manner. Failure to do so can lead to liability.

Compliance with Certification Practice Statement (CPS): While not explicitly stated as a separate section in the Act for subscribers, indirectly, subscribers are expected to understand and adhere to the practices outlined in the CA's Certification Practice Statement (CPS), which

[25] Information Technology Act, 2000, Sections 40–42 – Duties and responsibilities of subscribers holding Digital Signature Certificates (DSCs) regarding security, usage, and integrity of digital signatures.
[26] ibid

ISSN: 2582-6433

details the policies and procedures governing the issuance, management, and revocation of digital certificates.[27]

Who is a "Subscriber"?

Under Section 2(1)(zg) of the IT Act, a subscriber is a person in whose name the Digital Signature Certificate (DSC) has been issued by a Certifying Authority (CA).When a subscriber misuses the DSC or fails to comply with obligations, the law imposes penalties.[28]

Key Penalties on Subscribers

1. Penalty for Publishing False Digital Signatures (Section 41)

If a subscriber knowingly publishes a DSC that is false or misleading, or has not been issued to them, or they don't have the authority to publish: Penalty: Imprisonment up to 2 years, or fine up to ₹1 lakh, or both.2. Penalty for Failure to Use Reasonable Security Practices (Section 42)If a subscriber fails to take reasonable care to retain control of their private key and it is compromised, causing wrongful loss or gain: Penalty: Imprisonment up to 2 years, or fine up to ₹1 lakh, or both.[29] Other Related Offences (Sections 66C & 72) Section 66C: Fraudulent or dishonest use of electronic signature → Imprisonment up to 3 years and fine up to ₹1 lakh. Section 72: Breach of confidentiality or privacy while using e-signatures → Imprisonment up to 2 years, or fine up to ₹1 lakh, or both.

CONCLUSION

The comprehensive framework surrounding the electronic signature successfully bridges the gap between digital convenience and legal enforceability. This system is fundamentally built upon the principles of the Public Key Infrastructure (PKI), where the technical core involves the secure generating of key pairs and the issuance of Digital Signature Certificates (DSCs).At the organizational level, this trust is managed by the Certifying Authorities (CAs) and Issuing Authorities, specialized entities licensed to vet identities and issue the DSC. The lifecycle is strictly defined, covering the initial grant of the signature and the mandatory formal acceptance of the digital signature certificate by the user, which confirms their commitment to its terms.

[27] Information Technology Act, 2000, Sections 40–42 – Duties and responsibilities of subscribers holding Digital Signature Certificates (DSCs) regarding security, usage, and integrity of digital signatures.
[28] Information Technology Act, 2000, Section 2(1)(zg) – Definition of "subscriber" in the context of Digital Signature Certificates and related obligations
[29] Information Technology Act, 2000, Sections 40–42 – Duties and responsibilities of subscribers holding Digital Signature Certificates (DSCs) regarding security, usage, and integrity of digital signatures.

ISSN: 2582-6433

Crucially, the integrity of the entire system rests heavily on the subscriber. Their primary duties revolve around maintaining the security and non-compromise of the signature, particularly the absolute control of the private key. To account for changes or breaches, the framework mandates clear procedures for the revocation and withdrawal of electronic signature status.

Ultimately, the legal weight of this system is reinforced through robust provisions for penalties and adjudication. These measures ensure accountability for all stakeholders—CAs and subscribers alike—who violate established protocols. By seamlessly integrating authorized oversight, cryptographic security, individual responsibility, and legal sanctions, the framework provides the necessary trust foundation for secure global digital commerce.