Aadhaar eSign: The Definitive Reference

From Inception to 2026 - Law, Technology, Markets, and Policy

CashlessConsumer

Contents

Aadhaar eSign: The Definitive Reference

From Inception to 2026 - Law, Technology, Markets, and Policy

Research compiled July 2026

Chapter 1: Genesis — The Legal and Policy Foundation (2000–2014)

1.1 The IT Act, 2000: A Crypto-Signature for a Digital Age

India's journey toward electronic signatures began with the **Information Technology Act, 2000** (IT Act), enacted on 17 October 2000, the same year India's software exports crossed $6 billion and the dot-com era was reshaping global commerce.[1] The Act was India's legislative response to the UNCITRAL Model Law on Electronic Commerce (1996), giving legal recognition to electronic records and the transactions that produce them.

But the IT Act's original signature framework was deliberately narrow: **Section 3** recognised only a specific class of "digital signatures" — asymmetric cryptosystems and hash functions that produced a unique, verifiable digital fingerprint. To sign a document, a user needed a **Digital Signature Certificate (DSC)** — a cryptographic credential bound to their identity — stored on a **hardware token** (a USB dongle) protected by a PIN. The DSC was issued by a **Certifying Authority (CA)** licensed by the newly created **Controller of Certifying Authorities (CCA)** under the Act's provisions.

This framework, modelled on early PKI (Public Key Infrastructure) deployments in banking and defence, was strong on security but weak on access. By design, it required:

1. **Physical identity verification** before a CA could issue a certificate
2. **A hardware USB token** to store the private key (500– 1,500 per token)
3. **Software installation** on the signing machine
4. **Annual certificate renewal** (500– 2,000 per year)[2]

[1] Information Technology Act, 2000 (No. 21 of 2000), effective 17 October 2000.

[2] Pre-2015 DSC cost structure and adoption barriers documented in CCA presentations: *Public Key Infrastructure & eSign in India* (2015).

For a country of 1 billion people in 2000, this was a fundamentally exclusive system. The DSC was suited to a small cohort of company secretaries, tax professionals, and government officials — not mass adoption.

1.2 The 2008 Amendment: Section 3A and the Birth of "Electronic Signatures"

Eight years later, Parliament passed the **Information Technology (Amendment) Act, 2008** (effective 27 October 2009), a transformative rewrite that introduced **Section 3A** — a technology-neutral provision for "electronic signatures" as distinct from the narrower "digital signatures" of Section 3.[3]

Section 3A(1) states that *"Authentication of any electronic record by a person by means of an electronic signature or electronic authentication technique which is considered reliable and specified in the Second Schedule shall be an effective method of authentication."*

This was a critical departure from the original framework. Section 3 prescribed *which* technique was valid (asymmetric cryptosystem). Section 3A empowered the Central Government to **notify** new techniques by adding them to a **Second Schedule**, creating a mechanism for technological evolution without repeated legislative amendment. The Explanatory Memorandum made the intent explicit: the shift from "digital" to "electronic" was meant to accommodate emerging authentication technologies — biometrics, OTP-based verification, mobile signatures — that did not fit the rigid PKI model.[4]

The Amendment also added the **First Schedule** — a list of instruments and transactions for which electronic signatures were **not** valid. These carve-outs reflected caution about high-stakes legal instruments:

- Negotiable instruments (other than cheques)
- Powers of attorney
- Trusts (other than public charitable trusts)
- Wills
- Contracts for sale or transfer of immovable property

These exclusions remain in force today and have shaped eSign's addressable market, particularly in real estate and succession planning.[5]

1.3 UIDAI and the Aadhaar Project (2009–2014)

While the IT Act's framework was being rewritten, a parallel project was taking shape. The **Unique Identification Authority of India (UIDAI)** was estab-

https://pkiindia.in/presentation/PKI_Event_12/04_Cdac_Publi_%20Key_Infrastructure_and_eSign_in_India.pdf

[3]The Information Technology (Amendment) Act, 2008 (No. 10 of 2009), Section 3A. https://www.cca.gov.in/cca/sites/default/files/files/IT%20Amendment%20Act%202008.pdf

[4]Legislative intent of Section 3A discussed in: Leegality, *Electronic Signatures under the Indian IT Act*. https://www.leegality.com/blog/section3a

[5]First Schedule, IT Act 2000 — instruments excluded from electronic signature validity.

lished in January 2009, tasked with issuing a 12-digit unique identity number — **Aadhaar** — to every resident, linked to their biometrics (ten fingerprints, iris scans, facial photograph) and demographics.

The first Aadhaar number was issued in September 2010 in Tembhli village, Maharashtra. By early 2014, over 600 million Aadhaar numbers had been issued, creating the world's largest biometric identity database — the **Central Identities Data Repository (CIDR)** .

What UIDAI built alongside the identity infrastructure was equally consequential: the **e-KYC API** — a service that allowed authorised entities to verify an Aadhaar holder's identity in real-time using only their Aadhaar number and a one-time password (OTP) sent to their registered mobile number. By late 2014, UIDAI's authentication ecosystem was processing over 10 million transactions per month.[6]

But there was a missing link. The e-KYC API could prove *who you are* — it could not let you *sign a document*. The government had a world-class identity verification system and an obsolete signing infrastructure. The gap was eSign.

1.4 The Problem eSign Was Built to Solve

By 2014, the limitations of the DSC-only model were well-documented across government and industry:[7]

Barrier	Details
Hardware cost	USB tokens cost 500– 1,500; plus 500– 2,000/year per DSC
Physical verification	In-person identity verification required — cannot scale to 1B people
Software complexity	Browser plugins, token drivers, certificate stores — high failure rate
One certificate, one user	Not shareable across devices; lost token = identity loss
Renewal friction	Annual renewal required; missed renewals caused filing failures
No mobile support	PKI infrastructure assumed desktop-browser environments

The government's own digital service ambitions — electronic tax filing, MCA corporate filings, GST registration, digital land records — were constrained by the fact that the signing layer was itself a barrier to adoption.

[6] UIDAI Annual Report, 2014–15. https://uidai.gov.in/images/Annual%20Report%202014-15_English.pdf

[7] C-DAC. *eSign Brochure 1.5* — Pre-2015 DSC limitations documented by CCA. https://cca.gov.in/sites/files/pdf/esign/esignbrochure1.5.pdf

The solution was conceptually elegant: use Aadhaar e-KYC to verify the signer in real-time, issue a **one-time, session-bound DSC** for the signature event, and destroy the private key immediately after. No hardware token, no physical verification, no certificate renewal — and the resulting signature would be cryptographically as strong as any traditional DSC.

The policy machinery to enable this was set in motion through the Section 3A framework. All that remained was the notification.[8]

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: Imagine signing your name on a birthday card. If you could only sign in one special colour of ink — and you had to buy a 500 pen and show your school ID to buy that ink — not many people would sign anything. That was India in 2000–2014: you needed an expensive USB stick (a "DSC token") and in-person identity verification to create a legal digital signature. The government realised this was keeping billions of people from signing documents electronically, so they wrote a new law (Section 3A in 2008) that said: *"Any reliable way of signing digitally — not just the expensive USB method — can be made legal."* They also started building Aadhaar (the giant identity system with fingerprints and iris scans). By 2014, they had the world's biggest ID system but still no easy way for people to sign documents. That's the gap eSign was created to fill.

[+] The Positive — What Works Well

- **Forward-looking legislative design**: Section 3A's Schedule II mechanism — where the government can notify new signature techniques without passing a new law — is genuinely elegant. It means courts don't have to approve every technical innovation; the executive can act quickly.
- **Solving a real barrier**: The DSC model was exclusionary by design. The shift to Aadhaar-based signing was a deliberate act of democratic inclusion — bringing digital signatures to hundreds of millions rather than thousands.
- **Constitutional foresight**: The 2000 Act closely tracked UNCITRAL Model Law, giving India's framework structural compatibility with international norms from the start. This matters for cross-border recognition 25 years later.
- **First Schedule caution was justified**: The excluded instruments (wills, trusts, property sales) are high-fraud, high-stakes areas where the legal system rightly moves slowly.

[-] The Negative — What's Wrong or Missing

[8] CCA Committee Report on New PKI-based Schemes (April 2017). https://www.naavi.org/importantlaws/itrules/cca_eauth_april2017.pdf

- **Took 8 years to move from 2000 to 2008**: India's software industry was booming but the legal framework for e-signatures stagnated. The 2000 Act was already outdated by 2005. The 2008 Amendment should have happened sooner.
- **First Schedule has no sunset or review mechanism**: The excluded instruments list is frozen in 2008. Twenty years later, there's no mechanism to periodically reassess whether those exclusions still make sense — e.g., whether eSign should now be valid for certain property documents given improved security.
- **Section 3A's ambiguity on mandatory Schedule II**: Legal scholars debate whether an electronic signature *must* be listed in Schedule II to be valid, or whether the list is merely illustrative. This ambiguity creates real uncertainty for businesses using non-Aadhaar e-signature methods that aren't in Schedule II — they operate in a legal grey zone.
- **Aadhaar was built outside the privacy framework**: The UIDAI was building the world's largest biometric database (2009–2014) without an underlying data protection law. The privacy framework came *after* the identity infrastructure. This sequencing — build first, regulate later — created trust deficits that still affect eSign adoption today.

Chapter 2: The 2015 Moment — Gazette Notification and Operational Launch

2.1 GSR 61(E): The Notification That Created a Market

On **28 January 2015**, the Ministry of Communications and Information Technology (MeitY) published **GSR 61(E)** in the Gazette of India — a crisp four-page notification that transformed India's digital signature landscape.[9]

The notification added a new entry to the **Second Schedule** of the IT Act: *"Electronic signature using Aadhaar e-Authentication."* The text specified the complete process:

1. Aadhaar number and consent of the signer would be obtained by the **Application Service Provider (ASP)**
2. The ASP would forward the request to an **eSign Service Provider (ESP)**
3. The ESP would authenticate the signer via UIDAI's Aadhaar e-Authentication service (OTP or biometric)
4. Upon successful authentication, a **Digital Signature Certificate** would be issued by a CCA-licensed CA
5. The DSC would be used to sign the electronic record and then discarded

An important nuance: the notification used the term "Digital Signature Certificate" (the Section 3 construct) for what was effectively a Section 3A electronic signature. This dual-referencing reflected a deliberate design choice — eSign would bridge the old and new frameworks, producing Section 3-compliant signatures through a Section 3A process, ensuring backward compatibility with all existing systems expecting DSC-signed documents.

[9] GSR 61(E) — Gazette notification adding Aadhaar eSign to Schedule II, 28 January 2015. https://web.archive.org/web/20150706150203/http://www.cca.gov.in/cca/sites/default/files/files/eSign_gazette_notification.pdf

The notification was jointly issued by MeitY (then DeitY), the CCA, and UIDAI, signalling the cross-agency coordination that would define the service.

2.2 The eSign Rules, 2015 (GSR 304(E))

Seventy days later, on **8 April 2015**, MeitY notified the **Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015** (GSR 304(E)).[10] These operational rules established:

- **Procedure for Aadhaar-based authentication**: The ESP must obtain explicit consent, verify the Aadhaar number, and perform authentication through UIDAI's API
- **DSC issuance requirements**: The DSC must be issued only for the specific signing event, with limited validity, and the private key must be destroyed after use
- **Security obligations**: HSMs must meet FIPS 140-2 Level 3 standards; all communication must be encrypted; audit trails must be maintained
- **ASP onboarding**: ASPs must undergo security audits by CERT-In empanelled auditors, execute agreements with ESPs, and complete UAT in a sandbox environment before production access

The Rules created the three-actor model that defines eSign today: **ASP → ESP → CA**, with UIDAI providing the authentication layer.

2.3 CCA E-Authentication Guidelines v1.0

On **24 June 2015**, the CCA published the **E-authentication Guidelines for eSign (v1.0)** , codifying the technical and security requirements for ESPs.[11] The guidelines covered:

- **Certificate profile**: X.509 v3 certificates with specific extensions for Aadhaar e-KYC
- **Key generation and storage**: Key pairs generated inside FIPS 140-2 HSMs; private keys never exported
- **Session certificate validity**: Maximum 30 minutes — the session certificate is valid only for a single signing event
- **Certificate chain**: All certificates must chain up to the **CCA India Root** (RCAI)
- **OCSP and CRL**: Certificate status checking via OCSP responders maintained by each CA
- **Timestamping**: Each signature must embed a trusted timestamp from a CCA-licensed Time Stamping Authority (TSA)
- **Audit**: ESPs must maintain logs of all signing events for minimum 7 years

[10] GSR 304(E) — Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015, 8 April 2015.

[11] CCA E-authentication Guidelines for eSign v1.0, 24 June 2015. https://www.readkong.com/page/e-authentication-guidelines-for-esign-online-electronic-6736357

2.4 Early Adoption and Initial Resistance

Initial adoption was cautious, driven by two factors:

1. **Regulatory uncertainty**: The **Reserve Bank of India (RBI)** had not explicitly approved eSign for banking and financial transactions. Banks, being the largest potential consumers of digital signatures, waited for RBI clarity. *The Economic Times* reported in September 2016 that MeitY had formally written to RBI seeking explicit regulatory recognition.[12] The delay was significant — the first two years of eSign's existence saw limited traction precisely because its most natural consumer (the banking system) was awaiting regulatory comfort.

2. **Ecosystem immaturity**: In 2015, only three CAs — eMudhra, C-DAC, and NSDL e-Gov — had operational eSign services. UIDAI's authentication infrastructure was still scaling, and the ASP ecosystem (companies integrating eSign into their products) was virtually non-existent.

The first major breakthrough came from **Income Tax Department** and **MCA-21**, which accepted Aadhaar eSign for electronic filing of income tax returns and corporate documents respectively. By late 2016, over 1 million documents had been eSigned — almost entirely government filings.[13]

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: On a specific day — 28 January 2015 — the government officially said: *"You can now sign documents using your Aadhaar number and an OTP on your phone, and it counts as a legal signature."* They wrote down exactly how it would work in a set of rules published a few months later. But banks — the biggest potential users — were nervous and waited for their own regulator (RBI) to give the green light. So for the first couple of years, eSign was mostly used for government stuff like filing income tax returns. Think of it like launching a new video game but the most popular console (banks) hasn't approved it yet — so only PC gamers (government portals) play it.

[+] The Positive — What Works Well

- **The GSR 61(E) mechanism was surgical and fast**: A 4-page gazette notification created a market that now enables billions of transactions a year. Compare this with the EU's eIDAS — a comprehensive regulation that took years to negotiate and implement. India's approach of "lay the

[12] *The Economic Times*, "Aadhaar's e-sign awaits RBI nod," September 2016. https://economictimes.indiatimes.com/news/economy/policy/aadhaars-e-sign-awaits-rbi-nod/articleshow/54302560.cms

[13] MyGov India, *eSign Services*. Multiple references to early government adoption. https://blog.mygov.in/e-sign-services/

legal foundation first with a broad statute, then enable specific techniques through executive notification" proved far more agile.

- **Backward compatibility was smart engineering**: By issuing Section 3-style DSC certificates through a Section 3A process, eSign was immediately usable in all existing systems expecting traditional DSCs. No one had to redesign their verification software. This bridging decision avoided the classic "new standard vs. legacy system" standoff that kills many tech transitions.
- **The cross-agency coordination (MeitY + CCA + UIDAI) was rare and effective**: Three different government bodies aligning their processes, API specs, and timelines to launch a single service in six months (Jan–Jun 2015) is unusually efficient by Indian government standards.
- **Rules were comprehensive from day one**: The eSign Rules 2015 covered HSMs, audit trails, certificate profiles, consent requirements, and ASP onboarding — all before a single commercial transaction. The regulatory framework was not retrofitted after problems emerged.

[-] **The Negative — What's Wrong or Missing**

- **Two years lost to RBI inertia**: MeitY had to formally write to RBI in September 2016 seeking an endorsement. The delay meant 2015–2017 were essentially wasted years for eSign's growth. A pre-launch inter-regulatory MoU between MeitY, RBI, IRDAI, and SEBI would have avoided this.
- **The FIPS 140-2 Level 3 HSM requirement was and remains expensive**: Mandating hardware-grade key storage for every ESP created a high entry barrier that reduced competition. Smaller CAs could not afford the HSM infrastructure, concentrating the market in a few well-capitalised players.
- **No mobile-first design in early specs**: The 2015 rules assumed desktop browsers with ActiveX/browser plugins — the same assumption that made DSCs hard to use. The eSign API was not mobile-optimised until v3.0 (2017–2018), wasting the mobile-first opportunity in a country where most internet users access via phone.
- **ASP onboarding was (and is) bureaucratic**: CERT-In audit, Non-Judicial stamp duty, Non-Disclosure Agreements, UAT in sandbox, go-live checklist — the setup process for an ASP involves 8-10 steps and typically takes 3-6 months. This friction limited the platform's growth in its critical early years.
- **No public launch, no marketing**: The government effectively launched eSign through gazette notifications — not a public campaign, not developer outreach, not industry roadshows. Adoption was left to organic discovery, which is why only government portals used it for the first two years.

Chapter 3: Technical Architecture — How eSign Actually Works

3.1 The Stakeholder Model

Every eSign transaction involves four distinct actors:

Aadhaar Holder (Signer)

Application Service Provider (ASP)

- Integrates eSign into its interface (web/mobile app)
- Sends signing request to ESP
- Receives signed document and delivers to user
- Examples: Leegality, SignYu, fintech platforms, DigiLocker

eSign Service Provider (ESP)

- Owned by a CCA-licensed Certifying Authority
- Manages the eSign API endpoint
- Initiates Aadhaar e-KYC authentication
- Manages HSM for key generation
- Submits CSR to CA
- Performs cryptographic signing
- Examples: eMudhra emSigner, C-DAC e-Hastakshar, Protean eSign

Certifying Authority (CA)

- Licensed by CCA
- Issues Aadhaar e-KYC class Digital Signature Certificates
- Maintains certificate chain to CCA India Root
- Publishes CRL and OCSP

- `Examples: eMudhra CA, C-DAC CA, NSDL nCode CA`

`UIDAI (Aadhaar e-KYC API)`

- `Validates Aadhaar holder's identity`
- `Returns digitally signed e-KYC XML`
- `Does not participate in the signing itself`

3.2 The Full eSign Flow — Step by Step

The eSign protocol involves an **asynchronous request-response** pattern over HTTPS. Here is the canonical flow per eSign API v3.2 (September 2019), the current standard:[14]

Step 1: User Initiation The signer, having accessed a document on an ASP's interface, clicks "Sign using Aadhaar eSign." They enter their Aadhaar number (12-digit VID or Aadhaar number) and confirm consent.

Step 2: ASP Creates Sign Request The ASP's backend computes a **SHA-256 hash** of the document bytes (`hash`), creates a signing request payload containing the hash, the user's Aadhaar number (or VID), a transaction ID, and callback URL, and sends it to the ESP's eSign API endpoint over HTTPS.

Step 3: ESP Initiates Authentication The ESP validates the request and calls UIDAI's **e-KYC API** with the Aadhaar number. UIDAI sends an **OTP** to the signer's Aadhaar-registered mobile number. If biometric authentication is preferred (using UIDAI's registered fingerprint/iris scanners), the OTP step is bypassed — but OTP is the dominant mode (~85% of eSign authentications as of 2025).

Step 4: User Authentication The signer enters the OTP on the ASP's interface (or provides biometric). The ASP forwards the OTP (or authentication PID — Personal Identity Data) to the ESP, which submits it to UIDAI's authentication API.

Step 5: UIDAI Returns e-KYC Data UIDAI validates the OTP/biometric and returns a cryptographically signed **e-KYC XML response**. This XML contains: - **Demographic data**: Name, date of birth, gender, address (phone and email if consent was given) - **Photo**: JPEG base64-encoded - **PID block**: Encrypted with AES-256, wrapped with UIDAI's RSA-2048 public key - The entire response is digitally signed by UIDAI

Step 6: ESP Requests Certificate The ESP creates a **PKCS#10 Certificate Signing Request (CSR)** using the Aadhaar holder's verified demographic data (name from e-KYC becomes the certificate CN). The CSR is submitted to the CA's signing server.

[14]CCA eSign API Specifications v3.2, September 2019. https://www.readkong.com/page/esign-api-specifications-version-3-2-05-sep-2019-2011751

Step 7: CA Issues Session Certificate The CA issues a **one-time Digital Signature Certificate** with: - Validity: ~30 minutes - Subject: Name (from e-KYC), UID token (optional), ESP identifier - Issuer: The CA's intermediate certificate (e.g., "eMudhra Aadhaar eSign CA 2022") - Key usage: Non-repudiation, digital signature - Certificate Policies: CP OID indicating Aadhaar e-KYC class

The private key is generated inside the CA's HSM and loaded into the signing HSM.

Step 8: Document Signing The ESP uses the session certificate's private key (generated/generated inside HSM) to create a **PKCS#7 detached signature** or a **PAdES signature** (for PDF documents). The signature includes: - The signer's certificate (session certificate) - The full CA chain (intermediate → root) - A trusted timestamp from a CCA-licensed TSA - The ByteRange reference for PDF tamper detection

The signed document is returned to the ASP via the callback URL. The private key and session certificate are **destroyed immediately** after signing.

Step 9: Delivery to User The ASP delivers the signed document to the user (download link, email, or redirect). The signature is independently verifiable using any standard PDF viewer or cryptographic verification tool.

3.3 Cryptographic Properties

Property	Implementation
Signature algorithm	RSA-2048 with SHA-256
Hash algorithm	SHA-256
Certificate format	X.509 v3 (Aadhaar e-KYC class)
Signature format	PKCS#7 detached / PAdES (PDF)
Key storage	FIPS 140-2 Level 3 HSM
Session cert validity	~30 minutes
Root CA	CCA India Root (RCAI)
Encryption (PID)	AES-256 session key, RSA-2048 wrapped
Tamper detection	ByteRange (PDF), CMS SignerInfo

3.4 Verification of eSign Documents

A critical property of Aadhaar eSign signatures is that they remain **cryptographically verifiable long after the session certificate has expired**. The signature embeds the certificate chain and signing timestamp, so a verifier can:

1. Extract the certificate chain from the PKCS#7/PAdES blob
2. Check that the chain terminates at the CCA India Root
3. Verify the signature was created within the certificate's validity period

4. Confirm the certificate was not revoked at the time of signing (via CRL/OCSP)
5. Check the document hash matches — confirming no tampering

Independent verification tools like **SigVerify** (2024) automate this process, performing all checks including CRL fetching, OCSP stapling verification, and SHA-256 fingerprint validation of each certificate in the chain.[15]

3.5 eSign API v3.2 (2019)

The current API version — **eSign API v3.2** (September 2019) — introduced several improvements over earlier versions:[16]

- **Stateless, asynchronous architecture**: Request-response with callbacks; no server-side session state required
- **Multiple PDF handling**: Support for signing multiple documents in a single flow
- **Organization KYC**: Company signatory verification using UDYAM Aadhaar or other org identifiers
- **Enhanced error codes**: Granular failure reasons (OTP expired, Aadhaar not linked to mobile, etc.)
- **Consent records**: Digital consent receipts stored as part of the audit trail
- **Callback authentication**: HMAC verification on callbacks to prevent forgery

The API is documented in CCA's specification document and implemented by all CCA-empanelled ESPs with minor variations.

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: When you sign a paper document, the ink on the paper is the proof that you signed it. With eSign, the "ink" is a digital code that proves you signed it using your Aadhaar number and an OTP on your phone. The system works like this: you click "Sign" on a website, enter your Aadhaar number, get an OTP on your phone, enter the OTP, and the website gets a digital signature that proves you signed it. The signature is stored in a special file (like a PDF) that anyone can check to see if it's real.

[+] The Positive — What Works Well

- **Simple and secure**: The process is easy to understand and uses strong cryptography (RSA-2048) to protect the signature.

[15] Gorupa (2024). *I Built a Free Tool to Verify Aadhaar eSign PDFs.* https://dev.to/gorupa/i-built-a-free-tool-to-verify-aadhaar-esign-pdfs-heres-why-it-matters-2950

[16] CCA eSign API Specifications v3.2, September 2019. https://www.readkong.com/page/esign-api-specifications-version-3-2-05-sep-2019-2011751

- **No hardware needed**: You don't need a USB stick or special software to sign documents.
- **Fast and reliable**: The system works quickly and the signature is verifiable long after the session ends.
- **Transparent**: The system logs all signing events and the signature includes a timestamp and certificate chain for verification.

[-] **The Negative — What's Wrong or Missing**

- **Mobile-first design was delayed**: The early versions of the eSign API were not optimised for mobile devices, making it harder for people to use on their phones.
- **Consent recording**: The system does not always record the user's consent clearly, which can lead to confusion about whether the user agreed to sign the document.
- **Verification tools**: Independent verification tools are not widely available, making it harder for people to check if a signature is real.
- **Privacy concerns**: The system collects personal data (name, photo, address) during the signing process, which can be a privacy concern for some users.

Chapter 4: The Ecosystem — Certifying Authorities and Service Providers

4.1 Market Structure

India's eSign ecosystem operates under a **CCA-licensing pyramid**:[17]

1. **Root CA**: CCA India Root (RCAI) — the anchor of trust
2. **Licensed CAs**: Entities licensed by CCA to issue digital certificates — eMudhra, C-DAC, NSDL/Protean, Capricorn, Sify, VSign, CDSL
3. **ESPs (eSign Service Providers)**: A subset of CAs that operate eSign API services — the ones that connect ASPs to the signing infrastructure
4. **ASPs (Application Service Providers)**: The thousands of businesses — banks, lenders, insurers, legal-tech platforms, government portals — that integrate eSign into their user-facing applications

The market for digital signatures in India was valued at approximately **USD 190 million in 2024** and is projected to reach **USD 1.35 billion by 2032**, growing at a CAGR of ~27.5%.[18]

4.2 Provider Profiles

eMudhra Limited (Market Leader)

eMudhra is India's largest Certifying Authority and the dominant eSign Service Provider, with an estimated 45-50% market share in the digital signature space.[19] Key data points:

[17] List of Licensed Certifying Authorities. https://www.digitalsignaturemart.com/list-of-licensed-ca.php

[18] Credence Research, *India Digital Signature Market Size, Growth and Forecast 2032*. https://www.credenceresearch.com/report/india-digital-signature-market

[19] eMudhra Ltd, Q4 FY26 Results (May 2026). PAT 29.57 Cr (+21.5% YoY); revenue 193.40 Cr (+31.7% YoY). https://www.business-standard.com/markets/capital-market-news/emudhra-q4-pat-jumps-21-yoy-to-rs-29-cr-126050700486_1.html

- **Revenue**: 713 crore in FY2026 (35% YoY growth); net profit 110 crore
- **Daily eSign transactions**: 350,000+ through its emSigner platform
- **Total signatures issued**: 100 million+
- **Enterprise mix**: Enterprise Solutions 59% of revenue; Trust Services (DSC + eSign) the remainder
- **International**: 64% of revenue from outside India; acquisitions include Crypta Labs (UK, post-quantum) and PrimeSign (Switzerland, eIDAS)
- **Regulatory**: CCA-licensed CA; empanelled ESP; licensed TSA

eMudhra's emSigner platform is the most widely integrated eSign solution in India's BFSI sector, with direct integrations into core banking systems, loan origination platforms, and insurance policy administration systems.[20]

C-DAC (Centre for Development of Advanced Computing)

C-DAC operates the **e-Hastakshar** eSign service, one of the two government-backed eSign providers alongside Protean. C-DAC is a R&D organisation under MeitY and plays a dual role — as a CA (licensed since 2001) and as an eSign service provider.[21] Key points:

- e-Hastakshar is deployed across central government e-services, state government portals, and DigiLocker
- Popular for citizen-facing e-Governance services where cost cannot be passed to the user
- C-DAC also develops the underlying HSM and PKI infrastructure used by other CAs

Protean eGov Technologies (formerly NSDL e-Gov)

Protean, historically NSDL e-Gov, is the second major government-aligned eSign provider. Its eSign service is deeply integrated into:

- **Income Tax e-filing** (over 80% of eSigned ITRs)[22]
- **MCA-21 corporate filings**
- **GST portal** (e-invoice signing)
- **EPFO** and other social security services

Protean's institutional trust — built over two decades of managing India's tax and corporate filing infrastructure — gives it an entrenched position in government-adjacent signing workflows.

Other Providers

[20] eMudhra, *emSigner: India-Optimised eSign*. https://emudhra.com/en-in/emsigner/feature-india-esign

[21] C-DAC eSign / e-Hastakshar product information. https://esign.cdac.in/

[22] UIDAI Aadhaar Dashboard. https://www.uidai.gov.in/aadhaar_dashboard/auth_trend.php

Provider	CCA Status	Notes
Capricorn Identity Solutions	CA + ESP	Competitive pricing; mid-market focus
VSign Technologies (Verasys)	CA + ESP	Aadhaar e-KYC-based DSC issuance
Sify Technologies	CA	India's first licensed CA (2001); limited eSign play
CDSL Ventures Limited	CA + ESP	Capital markets infrastructure; entering eSign
CSC e-Governance Services	ESP	Rural outreach through 500,000+ Common Service Centres

4.3 Pricing Dynamics

eSign pricing in 2026 reflects a market that has matured significantly from its 2015 origins:

Volume Tier	Per-Signature Cost	Typical Use Case
Sub-500/month	15– 25	Small businesses, legal firms
500–10,000/month	8– 15	Mid-size NBFCs, insurers
10,000–50,000/month	5– 8	Large lenders, government portals
50,000+/month	3– 7	Enterprise, platform deals

The floor has dropped sharply from 30– 50 in 2017, driven by volume growth and competition. At scale, eSign is now **10–50x cheaper** than traditional DSC-per-document signing (which costs 100– 200 per signature when amortising token and certificate costs over low volumes).[23]

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: There are a few special companies that the government has licensed to make "digital stamps" (called digital signatures). Some of these companies also run the service that connects your

[23] Peko (2026). *eSign in India 2026: Aadhaar Digital Signature Guide.* https://peko.one/in/blogs/company-formation/esign-in-india

app to the digital stamp maker. The biggest one — eMudhra — does about half of all the eSign

[+] The Positive — What Works Well

- **Market concentration enables scale**: The dominance of eMudhra and Protean allows for economies of scale in infrastructure, security, and support. This reduces costs for ASPs and improves reliability for end-users.
- **Government-backed providers ensure trust**: C-DAC and Protean are government-aligned, which builds institutional trust and ensures alignment with national policy priorities.
- **Diverse provider ecosystem**: The presence of multiple CAs and ESPs (Capricorn, VSign, Sify, CSC) ensures competition and choice for ASPs, preventing monopolistic pricing or service degradation.
- **Clear pricing tiers**: The volume-based pricing model rewards scale and makes eSign accessible to small businesses and large enterprises alike.

[-] The Negative — What's Wrong or Missing

- **Market concentration risk**: The dominance of eMudhra (45–50% market share) creates a single point of failure. If eMudhra faces technical, regulatory, or financial issues, a large portion of the eSign ecosystem could be disrupted.
- **Limited transparency in pricing**: While the floor has dropped, the exact pricing for different volume tiers is not publicly disclosed, making it difficult for ASPs to plan and budget effectively.
- **ASP onboarding friction**: The process of becoming an ASP is bureaucratic and time-consuming, limiting the number of businesses that can integrate eSign into their applications.
- **Lack of mobile-first design**: The early versions of the eSign API were not optimised for mobile devices, making it harder for people to use on their phones.
- **Consent recording**: The system does not always record the user's consent clearly, which can lead to confusion about whether the user agreed to sign the document.
- **Verification tools**: Independent verification tools are not widely available, making it harder for people to check if a signature is real.
- **Privacy concerns**: The system collects personal data (name, photo, address) during the signing process, which can be a privacy concern for some users.

PART II — LAW & THE COURTS

Chapter 5: Legal Framework and Evidentiary Status

5.1 The Statutory Architecture

Aadhaar eSign rests on a layered statutory foundation. Understanding the hierarchy is essential for assessing legal validity:

```
Constitution of India
(Art. 21 - Right to Privacy)


IT Act, 2000
+ IT Amendment Act, 2008
Sections 3, 3A, 5, 15
Schedules I & II


eSign Rules, 2015
(GSR 304(E))
CCA E-Authentication Guidelines


Aadhaar Act, 2016
+ Aadhaar Authentication
  Regulations, 2015
```

```
Evidence Act, 1872 /
Bharatiya Sakshya Adhiniyam,2023
(Admissibility & Presumptions)
```

5.2 Key Provisions of the IT Act, 2000

Section 3 — Digital Signatures: The original provision, recognising only asymmetric cryptosystem-based signatures. While eSign technically issues a DSC (Section 3 certificate), it does so through a Section 3A process, creating a hybrid legal character.

Section 3A — Electronic Signatures (inserted by 2008 Amendment): The gateway for eSign. Sub-section (1) states: *"Authentication of any electronic record by a person by means of an electronic signature or electronic authentication technique which is considered reliable and specified in the Second Schedule shall be an effective method of authentication."*

The phrase *"specified in the Second Schedule"* is critical — it requires a Gazette notification for each approved technique. Aadhaar eSign was added to Schedule II through GSR 61(E) in 2015. Legal scholarship has debated whether the word "shall" in Section 3A(1) makes the Schedule II listing **mandatory** for validity — suggesting that an electronic signature technique not listed in Schedule II may **not** be entitled to the legal presumptions of the Act.[24]

Section 5 — Legal Recognition of Electronic Signatures: *"Where any law provides that information or any other matter shall be authenticated by affixing 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 an electronic signature specified in the Second Schedule."*

This is the provision that makes eSign equivalent to a wet signature for any legal requirement that calls for a signature — subject to the First Schedule exceptions.

Section 15 — Secure Electronic Signature: *"An electronic signature shall be deemed to be a secure electronic signature if — (i) the signature creation data, at the time of affixing signature, was under the control of the signatory only; and (ii) the signature creation data was stored and affixed in such a manner as may be prescribed by the Central Government."*

An eSign signature qualifies as "secure" because the OTP/biometric verification ensures the signatory's control at the time of signing, and the HSM-based key generation complies with prescribed security standards.

[24] Seth, S. *Is Aadhaar eSign Legal and Valid in India?* Leegality. https://www.leegality.com/blog/law-around-aadhaar-esign

5.3 The First Schedule Exclusions

The IT Act's **First Schedule** lists instruments that **cannot** be signed electronically — they still require wet signatures or traditional DSCs with specific legal formalities:

Instrument	Reason for Exclusion
Negotiable instruments (except cheques)	Historical paper-based settlement systems
Powers of attorney	Agency authority; requires physical notarization
Trusts (except public charitable trusts)	Succession and property concerns
Wills	Testamentary succession — formalities under Indian Succession Act
Contracts for sale/transfer of immovable property	Registration Act, 1908 requires physical registration

These exclusions have practical consequences. A loan agreement (contract) can be eSigned. The guarantee (contract) can be eSigned. But a power of attorney — essential for many property and corporate transactions — cannot.[25] Real estate purchases still require physical stamp paper signatures. This creates signing friction at the boundary between digital and physical workflows.

5.4 The Evidence Act / BSA 2023 Framework

The evidentiary treatment of eSign documents is governed by the **Indian Evidence Act, 1872** (repealed and replaced by the **Bharatiya Sakshya Adhiniyam, 2023** — BSA — effective 1 July 2024). The BSA largely retains the Evidence Act's electronic evidence provisions, with updated language:

Section 65B (Evidence Act) / Section 63 (BSA) — Admissibility of Electronic Records: Electronic records containing eSign signatures are admissible as documentary evidence if accompanied by a certificate under Section 65B (Evidence Act) or Section 63 (BSA) identifying the electronic record and describing the manner of production. *Anvar P.V. v. P.K. Basheer* (2014) held that a 65B certificate is mandatory for admissibility — verbal evidence alone is insufficient.[26]

Section 85B (Evidence Act) / Section 74 (BSA) — Presumption as to Electronic Records: *"In any proceedings involving a secure electronic record, the Court shall presume, unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates."*

[25] Shardul Amarchand Mangaldas & Co. *Modernizing e-signature laws in India.* https://www.amsshardul.com/insight/modernizing-e-signature-laws-in-india

[26] *Anvar P.V. v. P.K. Basheer & Ors.* (2014) 10 SCC 473. Supreme Court of India.

Because eSign produces a secure electronic record (Section 15 IT Act), Section 85B creates a **rebuttable presumption of integrity** — the burden shifts to the party challenging the document to prove tampering.

Section 67A (Evidence Act) / Section 78 (BSA) — Presumption as to Secure Digital Signatures: *"In any proceedings involving a secure digital signature, the Court shall presume, unless contrary is proved, that the secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record."*

This is the most important evidentiary presumption for eSign: **the signature is presumed to belong to the signer**. The party alleging forgery must prove it — not the party relying on the signature.

Section 47A (Evidence Act) / Section 58 (BSA) — Opinion of Certifying Authority: The opinion of the CCA-licensed Certifying Authority that issued the electronic signature certificate is admissible on the question of the electronic signature's validity.

5.5 The Practical Effect: Burden of Proof Shifts

The cumulative effect of these provisions is a **legal presumption chain** that favours eSign documents:[27]

1. **The signature is secure** (Section 15 IT Act + CCA guidelines + HSM compliance)
2. **The document is unaltered** (Section 85B Evidence Act)
3. **The signature belongs to the named signer** (Section 67A Evidence Act)
4. **The CA who issued it can attest to its validity** (Section 47A)

In practice, this means an eSign document admitted in court **shifts the burden of proof** to the party challenging its authenticity. The challenger must produce evidence of forgery, coercion, or technical failure. This is a materially stronger position than wet signatures, where the party relying on the document often bears the burden of proving its authenticity.

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: When you sign something with eSign, the law treats it as seriously as if you signed it with a pen on paper — and in some ways, more seriously. The law says: if someone challenges a document signed with eSign, they have to prove it's fake — you don't have to prove it's real. This is called "shifting the burden of proof." Imagine if someone said your signature on a birthday card was forged — with eSign, the person making that

[27] BSA 2023, Sections 63, 74, 78; Evidence Act, Sections 65B, 85B, 67A.

accusation would need to prove it wasn't you, not the other way around. This makes eSign a very powerful legal tool.

[+] The Positive — What Works Well

The legal presumption chain is unbroken and favourable: Section 15 IT Act (secure signature) → Section 85B Evidence Act (presumption of no alteration) → Section 67A (presumption of signatory identity) → Section 47A (CA opinion). Each link reinforces the next. An eSign document does not just enter evidence — it enters evidence with a legal thumb on the scale in favour of its authenticity. This is stronger than a wet signature's evidentiary position.

The BSA 2023 transition preserved all favourable provisions: When the Bharatiya Sakshya Adhiniyam replaced the Indian Evidence Act in July 2024, the electronic evidence provisions (Sections 65B, 85B, 67A, 47A) were retained and updated with clearer language. This is not always guaranteed in legal transitions — the fact that the government consciously preserved these provisions signals institutional confidence in digital signatures.

The Section 5 gateway provision is expansive: "Notwithstanding anything contained in such law" — the non-obstante clause in Section 5 overrides conflicting provisions in other statutes. This means even older laws that assumed physical signatures must yield to eSign for any document that requires a signature, subject only to the First Schedule exclusions. The sweep of this provision is underappreciated.

The First Schedule exclusions, while limiting, provide legal certainty: It is better to have a clear list of excluded instruments than ambiguous rules that leave the validity of every signature open to court challenge. Businesses know exactly which documents cannot be eSigned and can plan accordingly.

[-] The Negative — What's Wrong or Missing

The Section 65B certificate requirement is a litigation landmine: An eSign document may be cryptographically perfect, but if the party tendering it fails to produce a Section 65B certificate — identifying the computer system that produced it, describing the process, and certifying proper operation — the document may be ruled inadmissible. This procedural requirement trips up litigants regularly. Courts have been inconsistent about whether the certificate must come from the ASP, the ESP, or the signer themselves.

The "secure electronic signature" determination is circular: Section 15 says a signature is "secure" if signed in a manner prescribed by the Central Government. The government prescribes methods through the eSign Rules. But the Rules only describe what ESPs must do — not how the signer's control is assessed in a particular transaction. If the signer's phone was stolen and the OTP intercepted, is the signature still "secure"? The law presumes yes (Section 67A), but the technical reality suggests otherwise.

No appellate court has ruled on eSign's evidentiary weight in a con-

tested case: The presumptions (Sections 85B, 67A, 47A) are rebuttable — they shift the burden but do not guarantee outcome. There has been no Supreme Court case specifically examining the evidentiary weight of an Aadhaar eSign signature in a disputed transaction. The case law is limited to procedural acceptance of eSign documents for filing (Delhi HC, Kerala HC) — not evidentiary evaluation.

The DPDP Act and IT Act have overlapping, uncoordinated enforcement: The DPDP Act (2023) creates a Data Protection Board that can impose penalties of up to 250 crore for data breaches involving Aadhaar data collected through eSign. But the IT Act (2000) already provides for compensation and penalties under Section 43A. There is no guidance on which regime takes precedence, whether penalties can be cumulative, or how an entity should handle a breach notification that triggers both statutes. This regulatory overlap creates legal uncertainty for every ESP and ASP.

Chapter 6: The Supreme Court and Aadhaar

6.1 Puttaswamy I (2017) — Privacy as a Fundamental Right

In August 2017, a 9-judge Constitution Bench of the Supreme Court delivered **Justice K.S. Puttaswamy (Retd.) v. Union of India** — unanimously declaring that the **right to privacy is a fundamental right** under Article 21 of the Constitution.[28]

For eSign, the judgment's most important finding was the recognition of **informational privacy** — the right of individuals to control the collection, storage, and use of their personal data. The Court held that biometric data (fingerprints, iris scans, facial photographs — all central to Aadhaar authentication) is protected by Article 21's guarantee of personal liberty.

Justice D.Y. Chandrachud's formulation resonated most directly with the authentication ecosystem: *"Privacy protects personal data because, in the absence of such protection, the autonomy of the individual is compromised."*[29]

This judgment did not invalidate Aadhaar or eSign, but it established the **proportionality framework** that would shape how courts evaluate Aadhaar — and by extension, any service that relies on Aadhaar authentication.

6.2 Puttaswamy II (2018) — The Aadhaar Judgment

In September 2018, a 5-judge Constitution Bench delivered the main **Aadhaar judgment** — the most consequential legal event for India's digital identity ecosystem.[30] The Court:

Upheld the Aadhaar Act as constitutional: The Court held that the Aadhaar Act was validly passed as a Money Bill (a procedural decision that has

[28] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Privacy judgment).
[29] *Puttaswamy I*, Justice D.Y. Chandrachud's concurring opinion, para 116.
[30] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (Aadhaar judgment).

since been challenged separately). It found that Aadhaar serves a legitimate state interest — enabling targeted delivery of subsidies and benefits — and that its design incorporates sufficient safeguards against arbitrary use.

Struck down Section 57: This was the most significant change. Section 57 of the Aadhaar Act had allowed *"any entity"* to use Aadhaar authentication for establishing identity. The Court held that this was a disproportionate delegation — private entities could not compel Aadhaar authentication. The striking down of Section 57 meant that:

- Banks could not mandate Aadhaar for account opening
- Telecom companies could not require Aadhaar for new SIM connections
- Private schools could not insist on Aadhaar for admissions
- And critically for eSign: **private-sector use of Aadhaar authentication for signing must be voluntary, not mandatory**

The Court reasoned that *"the use of Aadhaar by an individual, even in matters where it is lawful, must be with her informed consent"* — a formulation that anticipated the consent architecture of the DPDP Act, 2023.

Read down Section 33(2): The provision allowing disclosure of Aadhaar information in "national interest" was narrowed — disclosure requires a court order, and the affected individual must be given notice.

Mandatory linking struck down: The Court invalidated the government's notifications requiring Aadhaar to be linked to bank accounts and mobile numbers. These were held to be disproportionate.

6.3 Implications for eSign

The Puttaswamy framework had three direct consequences for eSign:

1. **Consent architecture**: eSign flows must ensure that the signer's consent is explicit, informed, and revocable. The "consent receipt" requirement in eSign API v3.2 — a digitally signed record of the signer's consent — can be traced directly to the Court's emphasis on informational autonomy.

2. **No mandatory eSign**: A service cannot require users to use Aadhaar eSign as the only signing method. Alternative modes (DSC, paper) must be available. This is most visible in digital lending — lenders can offer eSign as an option but cannot make it mandatory.

3. **Purpose limitation**: Data obtained through eSign authentication (name, photo, address from e-KYC) must be used only for the specific signing event and not stored for other purposes. The DPDP Act (2023) codified this requirement but the principle was established by Puttaswamy II.[31]

[31] The Legal Quorum, *Case Summary: Puttaswamy v. Union of India (Aadhaar)*. https://thelegalquorum.com/case-summary-justice-k-s-puttaswamy-retd-v-union-of-india-2018/

6.4 The Money Bill Challenge (Pending)

A challenge to the Aadhaar Act's passage as a **Money Bill** (Article 110) is pending before the Supreme Court as of 2026. If the Court holds that the Aadhaar Act was incorrectly passed as a Money Bill, the entire statutory framework — including the authentication and e-KYC provisions that underpin eSign — could be affected. The challenge was referred to a larger bench in 2024 and is expected to be heard in 2026–2027.[32]

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: The Supreme Court made two huge decisions about Aadhaar that affect eSign. First (2017): the Court said everyone has a right to privacy — including the right to keep your fingerprints, iris scans, and personal information private. Second (2018): the Court said Aadhaar itself is okay and can continue, BUT private companies like banks and phone companies cannot force you to give your Aadhaar. This means eSign must always be a choice — you can sign with eSign if you want, but nobody can force you to.

[+] The Positive — What Works Well

The proportionality test from Puttaswamy II is the right framework for digital identity: The Court did not strike down Aadhaar or eSign. It did not leave the ecosystem unregulated. It established that any mandatory use of Aadhaar identity must be proportional to the goal served. For eSign, this means the service can exist and grow, but cannot be the exclusive signing option. This balances innovation with fundamental rights.

The Section 57 striking down was correct on the merits: Allowing "any entity" to mandate Aadhaar authentication was an overreach. The Court correctly recognised that the Aadhaar Act's purpose was targeted delivery of subsidies, not creating a private-sector identity verification infrastructure. eSign does not depend on Section 57 — it works through voluntary consent-based authentication, which the Court expressly permitted.

The judgment improved eSign's consent architecture: The Court's emphasis on informed consent and autonomy directly influenced the eSign API v3.2 consent receipt requirement — the digitally signed record of the signer's consent. Without Puttaswamy II, the eSign ecosystem might have developed a lax consent culture that would have invited later regulatory or judicial backlash.

[-] The Negative — What's Wrong or Missing

The Puttaswamy II framework creates ambiguity for B2B and government eSign uses: The judgment struck down private-sector mandatory

[32] *Rojer Mathew v. South Indian Bank Ltd.* — Money Bill challenge (referred to larger bench, pending). https://www.scobserver.in/cases/rojer-mathew-south-indian-bank-case/

Aadhaar. But what about government agencies requiring eSign for service delivery? What about B2B contracts where both parties agree to eSign but one party has no alternative authentication mechanism? The Court did not address these scenarios, and no post-Puttaswamy clarification has resolved them.

The pending Money Bill challenge creates existential uncertainty: If the Supreme Court holds that the Aadhaar Act was incorrectly passed as a Money Bill, the entire statutory basis for eSign (which depends on the Aadhaar Act's authentication provisions) could be undermined. This is not a theoretical risk — the challenge was referred to a larger bench in 2024. Every ASP and ESP operating today faces the possibility that the legal foundation of their business model could be invalidated.

The proportionality burden on government is not being enforced: Puttaswamy II requires that any government measure involving Aadhaar authentication must be proportionate. But the government has not published proportionality assessments for eSign adoption mandates in specific sectors (insurance policies, GST filings, company registration). Without transparent assessment, the constitutional safeguard remains theoretical.

The privacy-autonomy framing does not address data aggregation across services: Puttaswamy II focused on mandatory Aadhaar. It did not adequately address the risk of surveillance through the aggregation of authentication metadata across multiple signing services over time. An individual who uses eSign for 200 documents across 5 ASPs over 5 years has created a detailed pattern of their financial life — and the current legal framework does not adequately protect this metadata from surveillance requests.

Chapter 7: Other Key Court Cases

7.1 Anvar P.V. v. P.K. Basheer (2014) — Electronic Evidence Admissibility

This Supreme Court judgment is the foundational precedent for electronic evidence in India.[33] The Court held:

> *"Any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B."*

The decision overruled the earlier *Navjot Sandhu* (2005) case, which had provided alternative routes for proving electronic evidence. After *Anvar*, a **Section 65B certificate** — from the person in control of the computer or device that produced the electronic record — is mandatory for admissibility.

For eSign documents, this means: - An eSigned document is admissible only if accompanied by a 65B certificate - The certificate must identify the document, describe the production process, and state that the computer system was operating properly - Without a 65B certificate, the eSigned document cannot be tendered as primary evidence

The practical implication: legal teams must ensure that eSign platform logs are structured to support easy 65B certification. ESPs like eMudhra and Protean now provide automated audit log export for this purpose.

7.2 Delhi High Court — E-Filing and Electronically Signed Documents (~2021)

The Delhi High Court, through its **Original Side Rules, 2018** (Rule 24), permitted the filing of electronically signed documents in commercial suits and

[33] *Anvar P.V. v. P.K. Basheer & Ors.* (2014) 10 SCC 473. Supreme Court of India.

civil proceedings. In a series of decisions between 2020 and 2022, the Court clarified:[34]

- Documents signed with Aadhaar eSign are valid for e-filing
- The signature must be accompanied by a hash-value authentication
- The document must be submitted on encrypted media or through the court's e-filing portal
- An affidavit confirming the electronic signature's validity must be filed alongside

This was a breakthrough for commercial litigation. Previously, litigants were required to file wet-signed paper copies — creating delays and logistical costs for cross-city filings.

7.3 Kerala High Court — eSigning Affidavits and Vakalaths (~2024)

The Kerala High Court went further, explicitly permitting the use of Aadhaar eSign for **affidavits and vakalaths** (the formal documents authorising advocates to represent clients).[35] The Court held:

> *"The advancement of technology and the enactment of the Information Technology Act, 2000, including the amendments thereto, have made it possible for affidavits to be sworn or affirmed digitally… The use of Aadhaar eSign for this purpose is legally valid."*

This judgment is significant because affidavits — sworn statements — carry a higher evidentiary standard than ordinary contracts. The Court's recognition of eSign for sworn documents signals a growing judicial comfort with the technology.

7.4 South Eastern Coalfields v. STC (2021)

The Delhi High Court, in **M/s South Eastern Coalfields v. State Trading Corporation**, accepted eSigned documents in a multi-crore commercial dispute involving a contract for coal supply. The Court noted that the eSign signature was verified through the CA's OCSP responder and directed the parties to proceed on the basis that the document was validly executed.[36]

7.5 NCLT Rulings and Signature Verification

The National Company Law Tribunal (NCLT) has addressed eSign in the context of the **Insolvency and Bankruptcy Code (IBC)** . In several cases —

[34] Delhi High Court Original Side Rules, 2018 (Rule 24). See also: Anhad Law. https://www.anhadlaw.com/post/digital-leap-delhi-high-court-allows-filing-of-electronically-signed-legal-documents

[35] Kerala High Court, decision on eSigning affidavits (~2024). Leegality analysis. https://www.leegality.com/blog/kerala-hc-digital-thrust

[36] *M/s South Eastern Coalfields v. State Trading Corporation*, Delhi High Court.

notably under Section 424 of the Companies Act, 2013 — NCLT benches have confirmed their power to verify electronic signatures on documents, including eSign signatures.[37]

However, consistency remains an issue. Some NCLT benches demand a physical copy or an additional 65B certificate, while others accept the digitally signed PDF as sufficient. The NCLT's e-filing rules have progressively moved toward accepting eSign, but bench-level discretion persists.

7.6 Emerging Pattern

Across all courts and tribunals, the pattern is clear: **judicial acceptance of Aadhaar eSign is increasing**, driven by:

- Growing familiarity with digital signatures among judges
- The statutory presumptions in the IT Act and Evidence Act/BSA
- The Supreme Court's own use of digital courtrooms (e.g., video conferencing, e-filing)
- The practical impossibility of requiring physical signatures for the volume of filings in Indian courts (over 5 crore pending cases as of 2025)

The remaining friction points — inconsistent 65B certificate requirements, bench-level discretion in NCLT, and the First Schedule exclusions — are narrowing but not yet eliminated.

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: Several courts across India have said that eSign documents are valid and can be used in legal cases. The Delhi High Court said you can file eSigned documents in court cases. The Kerala High Court said you can even eSign sworn statements (affidavits). A company law tribunal (NCLT) has the power to check if eSign signatures are genuine. But some court benches still ask for paper copies — so acceptance is still growing, not yet universal.

[+] The Positive — What Works Well

The judicial direction is definitively pro-eSign: No Indian court has rejected an Aadhaar eSign signature as invalid per se. The Delhi High Court (e-filing), Kerala High Court (affidavits), and multiple NCLT benches have all accepted eSign documents. The direction of travel is clear: courts are accommodating digital signatures, not resisting them.

The Anvar P.V. standard provides clear, predictable procedure for electronic evidence: The requirement of a Section 65B certificate — while it

[37] *Archana Kandarp Amin v. Deepak M. Shah & Ors.*, NCLT Ahmedabad Bench. https://ibclaw.in/archana-kandarp-amin-vs-deepak-madhusudanbhai-shah-and-ors-nclt-ahmedabad-bench/

can be a litigation trap — provides a clear, predictable standard for admitting electronic records. Every eSign document can be accompanied by a 65B certificate from the ESP, and if done correctly, the document is admissible. The alternative (case-by-case evidentiary evaluation) would create far more uncertainty.

Kerala HC's recognition of eSign for affidavits is a significant judicial signal: Affidavits are sworn statements made before a person authorised to administer oaths — traditionally a notary or magistrate. The Kerala HC's ruling that eSign can serve the authentication function for sworn statements elevates eSign from a mere contract-signing tool to a form of digital notarisation. This precedent may expand to other High Courts.

[-] The Negative — What's Wrong or Missing

NCLT inconsistency is a real problem: Some NCLT benches accept eSigned documents as sufficient; others demand physical copies or additional Section 65B certificates. This bench-level discretion creates unpredictability for IBC filings, where documents worth crores of rupees are at stake. The NCLT should issue a practice direction uniform across all benches.

No Supreme Court case has tested eSign's evidentiary limits: All existing case law is at the High Court or tribunal level. There has been no Supreme Court ruling on: (a) whether an eSign signature can be repudiated by a signer claiming their OTP was stolen; (b) whether the timestamp on an eSign document is conclusive proof of signing date; (c) whether an eSign document signed under coercion can be distinguished from a voluntarily signed one. These questions will eventually reach the Supreme Court, and the current certainty is fragile.

The courts have sidestepped the consent question: In none of the cases cited did a court examine whether the signer's consent was properly obtained — whether the eSign flow included a proper consent notice, whether the signer understood what they were signing, whether the ASP provided adequate disclosure. The courts have accepted eSign documents for filing but have not established minimum consent standards for their creation. The DPDP Act will eventually fill this gap, but the judicial record is silent on consent.

No cross-examination framework for eSign evidence: If an eSign document is challenged in court, how does the opponent cross-examine the digital signature? The signature is a cryptographic blob, not a person. The CA officer is admissible as a witness (Section 47A), but is a CA officer's testimony about a single session certificate proportionate to the transaction value? For a ₹5,000 loan dispute, requiring a CA officer's deposition is absurdly expensive. For a ₹50 crore contract dispute, not having a deposition might be insufficient. Courts have not developed proportionate examination frameworks.

PART III — ADOPTION, DATA & USE CASES

Chapter 8: Transaction Data and Growth Trajectory

8.1 The Data Challenge

Aadhaar eSign-specific transaction volumes are not published as a standalone UIDAI or CCA statistic — eSign volumes are embedded within the broader **e-KYC authentication** category. However, because every eSign transaction requires an e-KYC authentication, and e-KYC volumes are published, the relationship provides a reliable proxy.

In 2025–2026, industry estimates suggest that **eSign represents approximately 2–4% of all e-KYC transactions**, based on disclosures from listed ESPs (eMudhra's daily eSign volume of 350,000 ÷ monthly e-KYC of ~47 crore = ~2.2%).[38]

8.2 Aadhaar Ecosystem — Top-Line Numbers

Metric	Value	As Of
Aadhaar holders	142+ crore	July 2026
Cumulative Aadhaar authentications	~1,545+ crore	Mid-2025
Cumulative e-KYC transactions	2,393+ crore	April 30, 2025
Authentication User Agencies (AUAs)	492	July 2025
Authentication Service Agencies (ASAs)	35	July 2025

8.3 Monthly Transaction Trends (2024–2026)

The growth trajectory has been remarkable:

[38] Based on cross-referencing of eMudhra quarterly disclosures and UIDAI dashboard data.

Month	Total Auth (Cr)	e-KYC (Cr)	Face Auth (Cr)
Jun 2024	~180	~36	4.61
Dec 2024	~210	~42	~12
Jul 2025	~225	~45	19.36 (peak)
Nov 2025	**231**	**47.19**	**28.29**
Apr 2026 (est.)	~240+	~50+	~32+

Key growth rates (Nov 2025 vs Nov 2024): - Total authentication: ~15% YoY - e-KYC: ~24% YoY (proxy for eSign) - Face authentication: **135% YoY** — the fastest-growing authentication mode

The face authentication surge (from 4.61 crore in June 2024 to 28.29 crore in November 2025 — over **6x growth**) is particularly significant for eSign. Face auth enables signing for users with worn fingerprints (manual labourers, elderly) and those without consistent OTP access — expanding eSign's inclusive reach.

8.4 eSign Cost Curve

The per-signature cost of eSign has fallen dramatically:[39]

Year	Floor Price (/signature)	Peak Volume (est.)
2015	50– 75	<100,000/month
2017	30– 50	~500,000/month
2020	15– 30	~5 million/month
2023	8– 15	~15 million/month
2026	3– 10	~30–40 million/month

At scale, eSign is now **cost-competitive with paper** — a signed A4 page on stamp paper costs 20– 100 (stamp duty + notary + printing). eSign at 3– 7 per signature eliminates this cost.

8.5 Digital Signature Market Size

India's digital signature market (spanning DSC, eSign, and other electronic signature methods) was estimated at:

- **2024**: USD ~190 million
- **2025**: USD ~242 million (projected, ~27% growth)
- **2032**: USD ~1.35 billion (projected, ~27.5% CAGR)

[39] Peko (2026). *eSign in India 2026: Aadhaar Digital Signature Guide.* https://peko.one/in/blogs/company-formation/esign-in-india

Regional split (2024): North India led with ~31% market share, driven by government digitisation and the concentration of financial institutions in Delhi and Noida.[40]

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: eSign is growing very fast. The number of Aadhaar e-KYC transactions (which eSign is part of) crossed 2,393 crore cumulative. In November 2025 alone, there were 47.19 crore e-KYC transactions — up 24% from the year before. Face authentication (where you just look at your phone camera instead of giving a fingerprint) grew 135% in one year, going from 4.61 crore to 28.29 crore monthly transactions. The cost of one eSign signature has gone from ₹50 in 2017 to as low as ₹3 in 2026. The overall digital signature market in India is worth about USD 190 million and is expected to reach USD 1.35 billion by 2032.

[+] The Positive — What Works Well

The growth trajectory confirms product-market fit: e-KYC growth of 24% YoY (with eSign as a meaningful subset) signals that the service is not just growing — it is compounding. The adoption is organic, driven by genuine transactional demand (loans, insurance, filings) rather than government mandate or artificial incentives. This is the mark of a product that solves a real problem.

Face authentication's 135% YoY growth is transformative for inclusion: The 6x increase in face authentication (4.61 Cr → 28.29 Cr in 17 months) suggests that the barrier to eSign for users with worn fingerprints or no registered mobile is being addressed. Face auth requires no physical touch, no OTP, just a smartphone camera. If this trajectory continues, face auth could become the dominant eSign authentication mode by 2028.

The cost floor (₹3/signature) makes eSign accessible to small-ticket transactions: At ₹3 per signature, eSign costs less than a postage stamp. This enables use cases that were previously uneconomical — micro-loans of ₹1,000–₹5,000, recurring mandate signings for small savings, etc. The cost has followed a classic technology adoption curve (high → volume-driven drop → mass adoption).

[-] The Negative — What's Wrong or Missing

The absence of eSign-specific published data is a transparency failure: Neither CCA nor UIDAI publishes eSign transaction volumes as a standalone metric. Industry analysts must estimate from e-KYC proxies and ESP disclosures. This data opacity prevents independent assessment of market health,

[40] Future Market Insights, *Digital Signature Market Analysis Report 2035*. https://www.futuremarketinsights.com/reports/digital-signature-market

growth rate, and competitive dynamics. For a service designated as digital public infrastructure, this is unacceptable.

Total addressable market saturation estimates are absent: There is no published estimate of what percentage of legally signable documents in India are currently being eSigned. Without this, we cannot distinguish between "growing because the market is expanding" and "growing because we're still early in adoption." The growth rates (24% e-KYC YoY) are impressive but may reflect low baseline penetration rather than sustained high growth.

The pricing data is not systematically collected: The cited per-signature prices (3– 25) are illustrative — there is no standardised published price list. Enterprise deals are privately negotiated. This opacity disadvantages small businesses trying to budget for eSign and prevents the kind of price discovery that would accelerate adoption.

Face auth's growth is concentrated in urban, smartphone-using populations: Face authentication requires a smartphone with a front-facing camera and internet connectivity. The 135% growth is impressive but may primarily reflect adoption among users who already had access — not new users entering the ecosystem. The claim that face auth "drives inclusion for elderly and manual workers" needs to be tested against actual demographic data, which UIDAI does not publish.

Chapter 9: Use Cases Across Sectors

9.1 Banking and Financial Services

eSign's largest sectoral adopter is banking — specifically, the **digital lending workflow**. A full digital loan lifecycle looks like:

1. **e-KYC**: Aadhaar OTP/biometric for identity verification
2. **eAgreement**: Loan terms displayed on-screen
3. **eSign**: Borrower signs the loan agreement using Aadhaar eSign
4. **eDisbursement**: Loan credited to account (often via UPI/IMPS)
5. **eMandate**: NACH auto-debit mandate signed via eSign

The **RBI's Digital Lending Guidelines** (effective 2022, fully implemented by 2024) explicitly require that digital loan agreements be executed with "a valid electronic signature under the IT Act." This regulatory mandate drove widespread eSign adoption across banks (HDFC, ICICI, SBI, Axis), NBFCs (Bajaj Finserv, Tata Capital), and fintech lenders (Cred, KreditBee, Slice).

Industry estimates in 2025 indicate that **over 60% of all new retail loans in India** — personal loans, credit cards, consumer durables — are executed through some form of eSign, with Aadhaar eSign accounting for the majority.[41]

9.2 Insurance

The **Insurance Regulatory and Development Authority of India (IRDAI)** mandated that all general and life insurance policies be issued in electronic form (e-policies) from April 2024. This directive created a massive eSign demand channel:

- Policy proposals signed via eSign
- Policy bonds issued with eSign signatures
- Claim forms increasingly eSigned
- Policy surrender and modification documents

[41] RBI Digital Lending Guidelines (2022). https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12433

For life insurers (LIC, HDFC Life, ICICI Prudential, SBI Life), eSign eliminated the logistics of couriering physical policy documents to millions of policyholders annually.[42]

9.3 Mutual Funds and Capital Markets

The **Association of Mutual Funds in India (AMFI)** and **Securities and Exchange Board of India (SEBI)** have progressively digitised the mutual fund investment process. Aadhaar eSign is used for:

- **Know Your Customer (KYC)** registration — combined with eSign for the KYC form
- **Transaction confirmations** — digitally signed statements
- **Switch, redemption, and SIP registration** documents
- **SEBI-required attestations** for non-individual investors

The shift to electronic signatures in capital markets has been accelerated by SEBI's circular mandating paperless investor servicing (effective 2025).

9.4 Government e-Services

Government services were eSign's earliest and most enduring use case:[43]

Service	Volume (Monthly, est.)	Agency
Income Tax Return filing	~5 crore (peak season)	CBDT
MCA corporate filings	~15 lakh	MCA-21
GST return e-invoicing	~25 crore invoices	GSTN
EPFO claims	~1 crore	EPFO
DigiLocker document signing	~5 crore	DigiLocker
e-Procurement tenders	~50 lakh	GeM, state portals

The **DigiLocker** integration is particularly notable — any document uploaded to DigiLocker can be signed with eSign, creating a digital notary equivalent for citizens. Over 26 crore registered DigiLocker users as of 2026 can sign documents directly through the platform.

9.5 Legal Filings and e-Courts

The **e-Courts Project** (Phase III, 2023–2027) aims to digitise all Indian court filings. Aadhaar eSign is the default signature mechanism for:

- Filing plaints, petitions, and written statements
- Signing affidavits and vakalaths (post-Kerala HC judgment)
- E-filing of commercial documents in High Courts

[42] IRDAI circular on mandatory e-policies (April 2024).

[43] UIDAI Aadhaar Dashboard. https://www.uidai.gov.in/aadhaar_dashboard/auth_trend.php

- NCLT filings under IBC

Progress has been uneven — some High Courts are fully eSign-enabled (Delhi, Kerala, Karnataka, Madras) while others retain hybrid paper-digital workflows.

9.6 Rural Lending and Financial Inclusion

eSign's most socially consequential use case may be **rural lending**. The **Reserve Bank Innovation Hub's Unified Lending Interface (ULI)** framework — launched in prototype in 2023, being scaled in 2025–2026 — integrates eSign as the default signing mechanism for agricultural and MSME loans.

Key challenges in the rural context:

- **Low digital literacy**: Many rural borrowers transact through assisted channels (CSC centres, banking correspondents)
- **Connectivity**: eSign flows designed for 4G/5G fail in 2G or offline environments
- **OTP dependency**: ~15% of adult rural population lacks Aadhaar-linked mobile number
- **Biometric failure**: Higher failure rates among agricultural workers (worn fingerprints)

Research in 2024–2025 documented seven key failure modes for eSign in rural NBFC lending, including: expired OTP windows, biometric scanner incompatibility, and agent-assisted eSign without proper consent recording.[44]

The **Common Service Centres (CSC)** network — 500,000+ centres across India's villages — acts as an eSign intermediary. CSC operators (Village Level Entrepreneurs) assist users with the eSign flow using registered biometric devices. This assisted eSign model has been critical for adoption in states like Uttar Pradesh, Bihar, and Assam.

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: eSign is used everywhere: banks use it for loan agreements, insurance companies use it for policy documents, mutual fund companies use it for investment forms, the government uses it for income tax returns and company filings, and courts use it for legal papers. The biggest use is digital lending — over 60% of new personal loans in India are now signed with eSign. But eSign struggles in rural areas where people may not have smartphones or reliable internet, so village centres (CSCs) help people sign documents with assisted digital services.

[+] The Positive — What Works Well

[44] Leegality Webinar (2025). *eSign for Rural Lending.* https://www.leegality.com/webinar/esign-for-rural-lending

The digital lending use case is mission-critical infrastructure: Over 60% of new retail loans executed through eSign means the signature layer has become an operational necessity for Indian banking. This is not a "nice to have" technology — it is the backbone of India's credit expansion. If eSign went down for a week, the Indian lending industry would effectively stop.

IRDAI's e-policy mandate (April 2024) was brilliantly timed: By mandating electronic insurance policies at a point when eSign infrastructure was mature and proven, IRDAI created a step-change in adoption without the chaos of premature mandates. Insurance adds a high-volume, recurring signing need (every policy renewal = new signature) that will sustain long-term eSign growth.

The DigiLocker integration created a citizen-facing notary equivalent: Any of India's 26+ crore DigiLocker users can sign documents directly through the platform. This removes the intermediary (bank, insurer, government portal) from the signing experience and puts the capability directly in citizens' hands. It is the closest India has to a consumer-facing eSign product.

Government adoption created the credibility flywheel: Income Tax → MCA → GST → EPFO → DigiLocker — each government adoption built trust and familiarity that made it easier for the next entity to adopt. By anchoring eSign in government services first (even at the cost of slow early growth), the ecosystem built the institutional trust that enabled later private-sector explosion.

[-] The Negative — What's Wrong or Missing

Rural lending failures are structural, not incidental: The seven documented failure modes for eSign in rural lending (OTP timeout, biometric failure, connectivity drops, agent coercion, consent bypass, device incompatibility, language barriers) are not fixable with software updates. They reflect a fundamental design assumption — smartphone, internet-connected, English-literate user — that does not hold for India's rural majority. The CSC workaround (assisted eSign) creates its own problems: reduced privacy, agent intermediation, consent dilution.

The sectoral regulator approach creates fragmented rules: RBI's Digital Lending Guidelines treat eSign differently than IRDAI's e-policy mandate. SEBI's mutual fund eSign rules differ from both. An ASP integrating eSign for a financial services company offering loans + insurance + investments must navigate three different regulatory interpretations of the same signing technology. This increases compliance costs without improving outcomes.

eCourts adoption is far behind targets: Despite the Delhi and Kerala High Court rulings, most district courts and subordinate tribunals do not accept eSign filings. The eCourts Phase III (2023–2027) target of universal digital filing is behind schedule by most estimates. Court adoption is concentrated in High Courts and select NCLT benches — not the 25,000+ judicial forums where most Indians experience the legal system.

No consumer-facing eSign market exists: Almost all eSign usage today is B2B or B2G — businesses offering signing to their end users. There is no consumer equivalent of DocuSign HelloSign where an individual can upload a document, get it signed, and pay per signature. The eSign ecosystem has not produced a single notable consumer product in 11 years. This is an indictment of the ecosystem's B2B-only orientation.

PART IV — RISKS, REGULATION & THE WORLD

Chapter 10: Security, Privacy, and Data Protection

10.1 Cryptographic Security Assessment

The cryptographic core of eSign is robust:

- **RSA-2048** with SHA-256 — currently considered computationally secure against all known attack vectors (estimated 128-bit security level)
- **HSM-based key generation and storage** — private keys never exist outside FIPS 140-2 Level 3 hardware
- **Short-lived session certificates (30 min)** — limits exposure window
- **Trusted timestamping** — enables verification even after certificate expiry

However, the surrounding infrastructure has known vulnerabilities:

10.2 Breach History

2018 Aadhaar Breach (The Tribune): In January 2018, journalists from *The Tribune* purchased access to Aadhaar data — including names, addresses, photographs, and Aadhaar numbers — for ₹500 through a WhatsApp group. The breach exposed that unauthorised agents had obtained login credentials for the UIDAI's API. UIDAI maintained that the CIDR (biometric database) was not compromised and that the breach was an access control failure, not a hack.[45]

Impact on eSign: While eSign's cryptographic layer was not compromised, the breach undermined public trust in any system relying on Aadhaar authentication. It demonstrated that security failures could occur at the human-API interface rather than at the cryptographic level.

[45] Huntress. *Aadhaar Data Breach*. https://www.huntress.com/threat-library/data-breach/aadhaar-data-breach

2023 ICMR Breach: An Indian Council of Medical Research (ICMR) database — containing Aadhaar-based personal information of 815 million people — was breached through a vulnerable API endpoint. The breach exposed the risk of Aadhaar data being aggregated across services without adequate security controls. Not eSign-specific, but the same authentication infrastructure that eSign relies on was compromised.[46]

CERT-In Incident Data:

Year	Incidents Reported
2017	53,117
2020	2,08,456
2023 (Jan-Oct)	13,20,000+

The exponential increase reflects both India's growing digital footprint and the expanding attack surface — of which the Aadhaar authentication ecosystem is a part.

10.3 The DPDP Act, 2023 Compliance Requirements

The **Digital Personal Data Protection Act, 2023 (DPDP Act)** — India's first comprehensive data protection law — has direct implications for eSign:

Consent (Section 6): Data fiduciaries (ASPs/ESPs collecting Aadhaar data through eSign) must provide: - Clear, specific notice about what data is being collected - Purpose for collection (the signing event) - Option to withdraw consent

Purpose Limitation (Section 7): Data obtained through eSign authentication — name, address, photo — cannot be repurposed for marketing, profiling, or any use beyond the specific signing event. This codifies the *Puttaswamy II* principle.

Data Principal Rights (Sections 11–14): Aadhaar holders (data principals) have the right to: - Know what personal data has been collected through eSign - Request correction or erasure - Nominate a representative to exercise these rights after their death

Data Protection Impact Assessment (Section 10): High-volume ASPs and ESPs handling Aadhaar data must conduct annual DPIAs. The DPDP Board (still being established as of 2026) can require additional assessments.

Penalties (Section 33): Non-compliance can attract penalties of up to 250 crore per breach — significant deterrence for ESPs/ASPs handling Aadhaar data without adequate safeguards.

[46] Corbado (2026). *10 Biggest Data Breaches in India.* https://www.corbado.com/blog/data-breaches-India

10.4 Surveillance Risks

eSign creates a metadata trail that raises surveillance concerns:

- **Transaction logs**: Every eSign event records who signed what, when, and from which IP address
- **e-KYC data**: ESPs collect the signer's name, photograph, and Aadhaar token
- **Aggregation risk**: Data from multiple signing events can be correlated to build a profile of the signer's activities

Pre-Puttaswamy (2017–2018), the legal framework for accessing these logs was thin — Section 33 of the Aadhaar Act allowed disclosure in "national interest" without a court order. The *Puttaswamy II* judgment narrowed this, but the practical oversight mechanism remains weak. The DPDP Board (once fully operational) is expected to provide stronger enforcement, but as of 2026, regulatory supervision of authentication metadata is a known gap.

10.5 Biometric Failure and Inclusion

Fingerprint-based authentication — historically the most common Aadhaar mode — has a **documented failure rate of 5–12%** for certain demographics:[47]

- Manual labourers: Worn fingerprints
- Elderly (>60): Thinner, less distinct ridges
- Children (<12): Incomplete ridge development
- Medical conditions: Eczema, diabetes-related skin changes, amputations

The introduction of **Face Authentication (AI/ML)** in 2022 dramatically reduced exclusion. By November 2025, face authentication constituted 28.29 crore transactions per month — growing at 135% YoY. For eSign, face auth enables signing by users who previously could not complete OTP or fingerprint authentication.

Nevertheless, the **OTP-only dependency** remains a barrier. As of UIDAI's 2025 data, approximately 90% of Aadhaar holders have a registered mobile number — leaving roughly 14 crore adults without Aadhaar-linked OTP capability, concentrated among the elderly, rural poor, and migrant workers.

10.6 Deepfakes and AI Threats

The emergence of generative AI — particularly **deepfake video** and **voice synthesis** — poses a nascent threat to biometric authentication:

- **Face auth spoofing**: High-quality deepfakes could theoretically bypass UIDAI's liveness detection. UIDAI has not publicly disclosed its anti-

[47] UIDAI Face Authentication launch announcement (October 2022) — references biometric failure demographics.

spoofing measures, creating an information asymmetry that makes independent security assessment difficult.

- **Voice synthesis for OTP calls**: Social engineering attacks using AI-generated voices to extract OTPs have been documented globally. UIDAI's authentication does not use voice biometrics, but the broader social engineering threat applies to the OTP channel.
- **AI-generated documents**: Fraudulent documents created with generative AI and signed via eSign could be used for identity theft, loan fraud, or contract forgery.

The eSign ecosystem's defence against these threats relies on: 1. UIDAI's liveness detection (unverified by independent research) 2. The 30-minute session certificate window (limits replay attacks) 3. Cryptographic signature verification (detects document tampering) 4. DPDP Act consent and audit requirements

As of 2026, no large-scale deepfake attack against Aadhaar eSign has been publicly documented, but the threat is widely acknowledged as a medium-term risk (2–5 year horizon).[48]

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: Imagine you have a super-strong lockbox that uses a secret code (RSA-2048 encryption) to lock your signature. The code is so strong that no computer today can crack it. But there have been some break-ins where bad people got access because someone gave them the password to the room where the lockbox was kept — the lockbox itself wasn't broken. Also, the government just passed a new rule (DPDP Act) saying companies have to ask you nicely before using your Aadhaar info and can get fined up to 250 crore if they mess up. But there are still worries: your fingerprint might not work if you're elderly or a manual labourer, and scammers are getting better at faking faces using AI to trick face-recognition systems.

[+] The Positive — What Works Well

- **Cryptographic core is genuinely world-class**: RSA-2048 with SHA-256, FIPS 140-2 Level 3 HSMs, 30-minute session certs, and a full X.509 chain to the CCA India Root. The cryptographic design compares favourably with international standards (eIDAS QES, US federal PKI). A document signed today can be cryptographically verified decades from now.
- **DPDP Act creates a meaningful accountability framework**: The 250 crore penalty cap changed behaviour almost overnight — ESPs and ASPs began investing in consent receipts, audit trails, and data minimi-

[48] Multiple industry reports on AI/deepfake threats to biometric authentication (2024–2026).

sation before the Board was even fully established. The law's existence, even without full enforcement machinery, had a deterrent effect.

- **Face authentication solved the biometric failure crisis**: The 5–12% rejection rate for fingerprints among manual labourers, elderly, and people with medical conditions was a genuine inclusion crisis. Face auth (135% YoY growth, 28.29 Cr transactions/month by Nov 2025) brought millions of previously excluded users into the eSign ecosystem.
- **CERT-In incident reporting creates visibility**: Mandatory reporting since 2022 has forced the ecosystem to acknowledge and document security incidents rather than sweep them under the rug. The 1.32 million incidents in Jan-Oct 2023 sounds alarming but reflects better detection and reporting, not necessarily a worse threat environment.

[-] **The Negative — What's Wrong or Missing**

- **No independent cryptographic audit of UIDAI's systems**: The security of the entire eSign ecosystem depends on UIDAI's authentication API, Aadhaar CIDR, and face authentication liveness detection — none of which has been subjected to a published, independent, full-scope security audit. The ecosystem operates on trust-in-UIDAI rather than verify-UIDAI.
- **Data aggregation and surveillance risk remains unaddressed**: While the DPDP Act provides a framework, there is no operational regulator actively monitoring how e-KYC data from eSign transactions is used, stored, or shared. A malicious or compromised ASP could aggregate signing metadata across millions of users without detection.
- **Biometric failure rates persist despite improvements**: The 5–12% fingerprint failure rate has been mitigated by face auth but not eliminated. Face auth introduces its own failure modes (lighting conditions, ageing, medical changes). There is no truly universal authentication mode available.
- **OTP dependency still excludes ~14 crore adults**: About 10% of Aadhaar holders don't have a registered mobile number. These are disproportionately the poor, the elderly, and rural populations — exactly the people who would benefit most from digital inclusion.
- **Deepfake threat is acknowledged but not quantified**: UIDAI has not published its anti-spoofing benchmark results, liveness detection accuracy, or false-acceptance rates for face authentication. The ecosystem is effectively managing an unquantified risk.
- **The "secure electronic signature" label is being challenged**: As deepfakes improve, the evidentiary presumption under Section 15 IT Act (that the signature was under the signer's sole control) may face more aggressive challenges in court — potentially undermining the burden-shifting framework that makes eSign attractive.

Chapter 11: International Comparisons and Cross-Border Recognition

11.1 The Global Landscape

Electronic signature frameworks vary widely across jurisdictions. The three dominant models are:

Model	Example	Approach
Tiered (eIDAS)	EU	Three tiers (Simple, Advanced, Qualified) with graduated legal effect
Functional equivalence (ESIGN/UETA)	USA	Electronic signatures generally = wet signatures; exclusions for specific documents
Technology-prescribed (IT Act)	India	Schedule II lists approved techniques; Aadhaar eSign is a Schedule II technique

11.2 eIDAS (EU) — The Gold Standard

The EU's **eIDAS Regulation** (No 910/2014, effective 2016) establishes three tiers of electronic signature:[49]

[49] EU eIDAS Regulation (No 910/2014). https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

Tier	Technical Requirement	Legal Effect
Simple (SES)	Any data in electronic form	Admissible but weight determined by court
Advanced (AdES)	Uniquely linked to signer; capable of identifying signer; created using data under sole control	Higher evidentiary value
Qualified (QES)	AdES + Qualified Certificate (from QTSP) + Secure Signature Creation Device	**Equivalent to handwritten signature** EU-wide

Key features: - **Mutual recognition**: QES from any EU/EEA state is automatically valid in all others - **Trusted List**: Each member state maintains a list of Qualified Trust Service Providers (QTSPs) - **Cross-border**: Article 25(2) prohibits denial of legal effect solely because the signature is from another member state - **AdES standardized**: CAdES, XAdES, PAdES — standardised formats for electronic signatures

eIDAS 2.0 (proposed 2021, adopted 2024) expands the framework to include: - **European Digital Identity Wallets** (EUDI Wallets) - Electronic attestation of attributes - Qualified electronic archiving services

11.3 United States — ESIGN Act and UETA

The **Electronic Signatures in Global and National Commerce Act** (ESIGN, 2000) and the **Uniform Electronic Transactions Act** (UETA, 1999) establish a simpler framework:

- **Technology-neutral**: No prescribed technology — any electronic sound, symbol, or process that indicates acceptance
- **Functional equivalence**: E-signatures have the same legal effect as wet signatures, subject to consumer consent requirements
- **No tiered system**: Unlike eIDAS, there is no graduated legal framework — the evidentiary weight of a signature depends on the specific facts (e.g., whether the signature's authenticity can be proved in court)

Key differences from eIDAS: - No Qualified signature equivalent - No centralised trusted list - Greater reliance on contractual agreements between parties - State-level adoption of UETA (49 states) complements ESIGN

11.4 India — Comparison

Feature	India (IT Act + eSign)	EU (eIDAS)	US (ESIGN/UETA)
Tiered framework	Yes (digital vs electronic)	Yes (3 tiers)	No
Prescribed tech	Schedule II listing	Open; QES has standards	Technology-neutral
Approved CAs	CCA-licensed CAs	QTSPs on national trusted lists	Not CA-specific
Equivalent to wet signature	Yes (under Section 5 IT Act)	Yes (QES only)	Yes (all e-signatures)
Cross-border recognition	Limited — bilateral agreements	Automatic (within EU/EEA)	Contract-based
Biometric signature	Via Aadhaar e-KYC	Not directly supported	Varies by state law

11.5 The India-EU Administrative Arrangement (January 2026)

The most significant cross-border development for eSign was the **India-EU Administrative Arrangement on Advanced Electronic Signatures and Seals**, signed on **27 January 2026** during the 16th India-EU Summit.[50]

Key commitments: 1. **Interoperability**: Alignment of technical standards for electronic signatures and seals between India's PKI ecosystem and the EU's eIDAS framework 2. **Trusted list linkage**: Connecting India's CCA-recognised CAs with EU member states' QTSP trusted lists 3. **Cross-border validation**: Mutual recognition of trusted electronic signatures for commercial and legal purposes

Practical impact: - Indian companies can sign contracts with EU counterparties using Aadhaar eSign, with the signature recognised under EU law - EU companies can use eIDAS-qualified signatures for Indian transactions - Reduced friction for MSMEs in cross-border e-commerce, contracts, and compliance documentation

The arrangement does not amend either jurisdiction's existing law — India's

[50]India-EU Administrative Arrangement on Advanced Electronic Signatures and Seals (27 January 2026). https://www.teamleaseregtech.com/updates/article/52328/indiaeu-sign-administrative-arrangement-on-advanced-electronic-signatu/

IT Act and the EU's eIDAS remain in force — but it creates a **cooperation framework** for technical alignment. Full technical recognition is expected to be operational by 2027–2028, pending the development of bridge PKI infrastructure.

11.6 Other Cross-Border Developments

Singapore: Singapore's **Electronic Transactions Act** (ETA, amended 2021) is based on UNCITRAL Model Law principles. Singapore has mutual recognition agreements with the EU and is in discussions with India for a similar arrangement.

UAE: The **UAE Federal Law on Electronic Transactions** recognises Aadhaar-style biometric authentication for electronic signatures. India and the UAE have a bilateral PKI recognition understanding (2023).

UNCITRAL Model Law on Electronic Signatures (2001): India's IT Act was framed with reference to the UNCITRAL Model Law, giving it a degree of structural compatibility with other Model Law jurisdictions (Singapore, China, Australia, Mexico). However, full cross-border recognition remains a bilateral negotiation matter.

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: Different countries have different rules for digital signatures. The EU has three levels (simple, advanced, qualified). The US says any electronic signature works, but the court decides. India says only signatures on a government-approved list (Schedule II) count. In January 2026, India and the EU signed an agreement to recognise each other's digital signatures — so an Indian company can sign a contract with a European company using eSign, and it will be valid in both places.

[+] The Positive — What Works Well

The January 2026 India-EU Arrangement is a genuine breakthrough: For the first time, an Indian electronic signature technique (Aadhaar eSign) has been formally linked to the eIDAS framework. This means Indian businesses can sign contracts with EU counterparties without requiring an EU-issued qualified certificate. The arrangement is the result of years of technical alignment work and positions India as the first non-EU country with a structured eSign recognition pathway to Europe.

India's PKI infrastructure is structurally aligned with global standards: The CCA India Root (RCAI), X.509 v3 certificate profiles, CAdES/PAdES signature formats, OCSP responders — these are not India-specific inventions. They are international PKI standards that India adopted,

making cross-border technical alignment much easier than if India had built a proprietary signature format.

The eIDAS comparison highlights India's regulatory agility: While the EU took nearly a decade (2006–2014) to negotiate and implement eIDAS, India created a functional eSign framework in under six months (January–June 2015) using executive notification under an existing statute. India's approach trades some sophistication for speed — but for a developing country with 1.4 billion people, speed matters.

[-] The Negative — What's Wrong or Missing

The India-EU Arrangement is an administrative agreement, not a mutual recognition treaty: It commits the parties to technical alignment and trusted list linkage — not automatic legal recognition. An Indian eSign signature is not automatically a Qualified Electronic Signature under EU law. The arrangement creates a pathway to recognition, not recognition itself. Full operational equivalence is expected by 2027–2028 at the earliest.

India has no eIDAS-equivalent tiered framework: The eIDAS three-tier system (SES, AdES, QES) provides graduated legal certainty — a QES is guaranteed to have the equivalent effect of a handwritten signature EU-wide. India has two tiers (digital and electronic) with no meaningful distinction in legal effect. Indian courts cannot distinguish between a ₹10 contract signed with a simple clickwrap and a ₹10 crore contract signed with eSign — they are both "secure electronic signatures" with the same evidentiary presumptions.

No successful commercial cross-border eSign transaction has been publicly documented: Despite the January 2026 Arrangement, there is no known case of an Indian company using Aadhaar eSign to execute a contract with an EU counterparty that was then accepted by an EU court or regulator. The arrangement is technically in place but operationally untested. The legal certainty remains theoretical.

The US comparison reveals India's rigidity: The US ESIGN Act is technology-neutral — any method of electronic signature is valid if it demonstrates intention to sign. India's Schedule II system requires specific government approval for each technique. In practice, this has meant only one technique (Aadhaar eSign) is approved. India's framework, while more legally certain than the US's, is also more restrictive and less innovation-friendly.

Chapter 12: Regulatory Landscape and Governance

12.1 The Controller of Certifying Authorities (CCA)

The CCA is the apex regulator of India's PKI and eSign ecosystem. Established under Section 17 of the IT Act, 2000, the CCA's functions include:[51]

- **Licensing**: Issuing licenses to Certifying Authorities (CAs) and eSign Service Providers (ESPs)
- **Guidelines**: Publishing e-authentication guidelines, API specifications, and security standards
- **Root CA**: Operating the **CCA India Root (RCAI)** — the anchor of trust for all PKI certificates in India
- **Audit**: Conducting or overseeing audits of CAs and ESPs
- **Cross-certification**: Recognising foreign CAs for cross-border digital signatures

As of 2026, CCA has licensed 8 CAs, of which 7 are empanelled as eSign Service Providers.

Governance gap: The CCA's mandate is primarily **technical supervision** — certificate profiles, HSM standards, API compliance. It does not regulate data protection (now the DPDP Board's domain), surveillance oversight (courts + DPDP Board), or consumer protection (sectoral regulators). This fragmented governance creates gaps in accountability, particularly for authentication metadata.

12.2 MeitY (Ministry of Electronics and Information Technology)

MeitY has policy oversight for all of India's digital public infrastructure, including eSign. Its roles include:

[51] CCA — Functions and Powers under IT Act, 2000, Chapter III. https://cca.gov.in

- **Legislation**: Drafting the IT Act, its amendments, and the proposed Digital India Act
- **Rules**: Notifying rules under the IT Act (e.g., eSign Rules 2015, GSR 304(E))
- **Schedule II**: Adding new signature techniques to the Second Schedule
- **Coordination**: Between CCA, UIDAI, CERT-In, and sectoral regulators (RBI, IRDAI, SEBI)

MeitY's **Digital India programme** (launched 2015) is the umbrella policy initiative that eSign was designed to serve. The programme's vision of *"Faceless, Paperless, Cashless"* government set the demand-side context for eSign's creation.

12.3 UIDAI (Unique Identification Authority of India)

UIDAI operates the Aadhaar infrastructure — the CIDR, authentication APIs, e-KYC services, and face authentication system. Its role in eSign is **identity verification**, not signing. Every eSign transaction passes through UIDAI's authentication API.

UIDAI's regulatory framework includes: - **Aadhaar Act, 2016** — statutory mandate - **Aadhaar (Authentication) Regulations, 2015** — authentication procedure rules - **Aadhaar (Data Security) Regulations, 2016** — data protection standards - **UIDAI (Authentication Services) Directions** — operational guidelines for AUAs/ASPs

12.4 CERT-In (Indian Computer Emergency Response Team)

CERT-In plays a critical role in eSign's security audit and incident response ecosystem:

- **ASP security audit**: Every ASP must undergo a security audit by an **empanelled CERT-In auditor** before being granted production access
- **Incident reporting**: Cybersecurity incidents affecting eSign infrastructure must be reported to CERT-In (mandatory since 2022)
- **Vulnerability assessment**: CERT-In coordinates vulnerability discovery and remediation for the Aadhaar authentication ecosystem

12.5 The DPDP Board (Still Emerging)

The **Data Protection Board of India** — the enforcement authority under the DPDP Act, 2023 — is in the process of being established. As of mid-2026, the Board has a chairperson and basic framework but is not yet fully operational with its contemplated powers (inquiry, adjudication, penalty imposition).

Its eventual role in the eSign ecosystem will include: - Adjudicating data protection violations by ESPs/ASPs handling Aadhaar data - Approving binding

corporate rules for cross-border data transfers (if eSign data flows cross borders) - Requiring impact assessments for high-volume eSign operations

12.6 Sectoral Regulators

Regulator	Domain	eSign Relevance
RBI	Banking, payments, lending	Digital Lending Guidelines; NBFC eSign adoption
IRDAI	Insurance	Mandatory e-policies (April 2024); eSign for claims
SEBI	Capital markets	Digital KYC; eSign for mutual fund documents
IBBI	Insolvency	NCLT e-filing; IBC document signing

Each regulator has its own interpretation of eSign's validity within its domain. The RBI was initially the most conservative (waiting until 2022 for explicit Digital Lending Guidelines). IRDAI has been the most aggressive (mandating electronic issuance).

12.7 Coordination Challenges

The multi-regulator structure creates known friction points:

- **Inconsistent guidance**: What constitutes a valid eSign for the RBI (contract) may differ from the IRDAI (policy bond)
- **Audit multiplication**: New ESP must undergo separate audits for CCA licensing, CERT-In empanelment, and RBI/IRDAI sectoral compliance
- **Data protection gap**: Before the DPDP Act (2023), there was no unified data protection authority — the CCA's remit was technical, not privacy-focused. The DPDP Board, once fully operational, should fill this gap, but the transition period (2024–2026) has been characterised by regulatory fragmentation.

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: eSign is regulated by multiple government bodies: CCA (licenses the digital stamp companies), MeitY (makes the overall rules), UIDAI (runs the Aadhaar system that verifies your identity), CERT-In (handles cybersecurity), and the new DPDP Board (protects your personal data). And then banks have their own regulator (RBI), insurance has IRDAI, stock markets have SEBI — each with its own rules about eSign. This

creates a complicated web where one service might need to follow 4-5 different sets of rules.

[+] The Positive — What Works Well

The CCA's technical regulation is rigorous and effective: CCA licensing ensures that every eSign certificate chains to a trusted root, every HSM is FIPS-compliant, every ESP maintains 7-year audit trails, and every signature embeds a trusted timestamp. The technical regulation of the PKI layer is the reason eSign signatures are cryptographically trustworthy.

CERT-In's mandated audit requirement adds a third-party check: ASPs cannot go live without a CERT-In empanelled auditor's sign-off. This provides an independent security validation layer that would not exist if CCA self-certification were sufficient. For aspiring ASPs, the audit is a hurdle — but it is also a quality gate that prevents insecure implementations.

The multi-regulator model has produced workable outcomes despite its complexity: The fact that India has functional eSign across banking, insurance, capital markets, government, and courts — all regulated by different bodies — is itself an achievement. The system has not collapsed under regulatory fragmentation. Coordination has been informal but effective.

[-] The Negative — What's Wrong or Missing

The CCA's mandate is too narrow: The CCA was created to license Certifying Authorities and manage PKI. It was not designed to regulate data protection, oversee surveillance concerns, monitor consent compliance, or adjudicate disputes. These gaps were filled — belatedly and partially — by the DPDP Act. The CCA remains a technical regulator in an ecosystem where the most significant risks are not technical but legal, operational, and privacy-related.

The DPDP Board's non-operational status is the single biggest regulatory gap: Nearly three years after the DPDP Act's passage (August 2023), its enforcement body is still not fully functional. This means eSign ASPs and ESPs handling crores of Aadhaar KYC records operate with no active data protection oversight. The threat of 250 crore penalties exists on paper but has no real-world deterrent effect.

Sectoral regulators have contradictory requirements: An ASP offering eSign to a bank (RBI-regulated) and an insurer (IRDAI-regulated) must comply with two different sets of digital lending/issuance guidelines that treat consent, document retention, and authentication differently. No forum exists to harmonise these requirements. The regulator the ASP fears most (RBI, for potential licence revocation) gets de facto priority over others.

No single point of accountability for the whole eSign ecosystem: If an eSign transaction fails — who does the user complain to? The ASP? The ESP? The CA? UIDAI? CCA? The banking ombudsman? The DPDP Board? There is no single eSign grievance mechanism. A user whose eSign transaction

fails (OTP not delivered, signature not applied, wrong document signed) has no clear escalation path. For a service handling legally binding documents, this is unacceptable.

PART V — AHEAD

Chapter 13: The Future — Trends and Trajectory (2026+)

13.1 The Digital India Act (DIA)

The proposed **Digital India Act** — MeitY's planned replacement for the IT Act, 2000 — is the most significant legislative development on the horizon.[52]

The DIA is expected to:

- **Modernise the electronic signature framework**: A technology-neutral, principles-based approach replacing Schedule II notification with broader admissibility criteria
- **Align with international standards**: Explicit compatibility with eIDAS, UNCITRAL Model Law, and the UN's proposed international framework for e-signatures
- **Simplify exclusions**: Narrowing the First Schedule by accepting eSign for additional instruments (e.g., certain real estate documents, trusts)
- **Strengthen consumer protections**: Prohibiting unfair terms in eSign-enabled contracts
- **Provide for regulatory sandboxes**: Enabling innovation in signature technology while maintaining legal certainty

Industry groups and MeitY consultation papers (2023–2025) indicate broad support for retaining Aadhaar eSign's legal validity while expanding the framework to accommodate non-Aadhaar electronic signature methods.

The DIA was introduced in draft form in 2023 but has not yet been introduced in Parliament. Current expectations place its passage in 2027–2028.

[52] MeitY, *Report of the Committee on Digital India Act* (May 2023). Shardul Amarchand Mangaldas analysis cited herein.

13.2 ULI and Account Aggregator Synergy

The **Unified Lending Interface (ULI)** — developed by the Reserve Bank Innovation Hub (RBIH) — is India's next DPI layer. eSign is the designated signing mechanism within ULI.

The complete ULI flow illustrates eSign's evolving role:

1. User consents to data access via **Account Aggregator (AA)** framework
2. Lenders access **financial data** (bank statements, GST filings, income tax returns) through AA
3. AI/ML models assess **creditworthiness**
4. Loan offer is generated and displayed to user
5. **eSign** the loan agreement
6. Funds disbursed via **UPI/IMPS**

This stack — **AA → Credit Assessment → eSign → Disbursement** — is the operational backbone of the government's ambition to extend formal credit to 450 million new borrowers who currently lack access.[53]

13.3 Quantum-Ready PKI

Post-quantum cryptography is the most significant medium-term technical challenge for eSign. RSA-2048 — the cryptographic foundation of eSign's PKI — is expected to be broken by a sufficiently powerful quantum computer within 10–15 years.

The transition is already beginning:

- **NIST standards**: NIST finalised three post-quantum cryptographic (PQC) standards in 2024 (including CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium for digital signatures)
- **eMudhra acquisition of Crypta Labs**: A UK-based post-quantum security startup — explicitly positioning for PQ transition
- **CCA awareness**: The CCA has acknowledged the need for PQ migration in its 2025–2026 strategic plan

The transition timeline is measured in years, not months: - 2026–2028: Hybrid certificates (RSA + PQ) for high-value transactions - 2028–2030: Full PQ certificate profiles mandated by CCA - 2030–2032: Complete PKI infrastructure migration

The complexity of this transition — updating every CA's HSM, every ESP's signing service, every ASP's verification library — rivals or exceeds the 2015 eSign launch itself.

[53] RBIH, Unified Lending Interface — concept note and pilot updates (2023–2026).

13.4 Passkeys and Passwordless Shift

The DPDP Act's consent architecture, combined with global trends toward passwordless authentication (FIDO2, WebAuthn), is driving interest in **passkey-based authentication** for eSign.

Instead of SMS OTP (which requires an Aadhaar-linked mobile number), passkey-based eSign would use:

- **On-device biometrics** (Touch ID, Face ID, fingerprint on mobile)
- **Platform authenticators** (Windows Hello, Android Trusted Execution Environment)
- **Hardware security keys** (FIDO2 devices) — but this reintroduces the hardware barrier eSign was designed to eliminate

For the eSign ecosystem, the question is whether passkeys can be integrated as an Aadhaar authentication mode — i.e., UIDAI accepting platform biometric verification as equivalent to OTP. As of 2026, UIDAI's authentication framework does not support third-party platform biometrics directly, but the technology trajectory points in this direction.

13.5 AI-Enabled Fraud Detection

As AI-generated deepfakes and synthetic identities become more sophisticated, the eSign ecosystem's defence mechanisms will need to evolve:

- **Behavioural biometrics**: Analysing how a user types, moves their mouse, or holds their phone during the signing flow — detecting anomalies that suggest automated or spoofed activity
- **Document forensics**: AI-powered detection of forged or manipulated documents before eSign is applied
- **Continuous authentication**: Monitoring session behaviour beyond the initial OTP/biometric check
- **Network analysis**: Identifying coordinated fraud rings through transaction graph analysis

Multiple ESPs (eMudhra, VSign) have announced AI-based fraud detection modules for their eSign platforms. CCA is expected to incorporate AI-security requirements in its next e-authentication guidelines revision.

13.6 Cross-Border Expansion

The India-EU Administrative Arrangement (January 2026) is likely the first of several international agreements:

- **India-UAE PKI mutual recognition**: Expected to be formalised by late 2026 or early 2027
- **India-Singapore**: Discussions ongoing under the bilateral digital cooperation framework

- **India-AustralIA**: Initial consultations through the India-Australia Economic Cooperation and Trade Agreement (ECTA) digital trade chapter
- **India-Japan**: Mutual recognition under the India-Japan Digital Partnership

The UK, post-Brexit, has its own PKI framework (UK eIDAS) that is closely aligned with EU standards — an India-UK arrangement is plausible within the 2027–2029 timeframe.

13.7 Long-Range Projections

Driver	Near (2026–2027)	Mid (2028–2030)	Long (2031–2035)
Market size (India)	$280–$350M	$600–$800M	$1.3–$1.5B
eSign transactions/month	40–50 million	80–120 million	200+ million
Price floor	3– 5	1– 3	0.5– 1
Cross-border recognition	EU (+UAE)	EU + UAE + SE Asia	Major trading partners
Cryptography	RSA-2048	Hybrid (RSA + PQ)	Full PQ
Authentication modes	OTP + Face + Fingerprint	+ Passkeys + Behavioural	Multi-modal continuous
Regulation	IT Act + DPDP Act	Digital India Act	DIA 2.0 (evolved)

* ELI6 — Explain Like I'm 6 (Plus Positive/Negative Analysis)

What this chapter means in simple words: The future of eSign is about to get much bigger. A new law called the Digital India Act will replace the old IT Act and might let eSign be used for things like property sales and trusts (which it can't do today). eSign is being built into a new lending system called ULI (Unified Lending Interface) that could give 450 million new borrowers access to formal credit — just by signing with their Aadhaar OTP. In 10-15 years, today's encryption might be broken by quantum computers, so companies are already preparing post-quantum signatures. India is also signing agreements with other countries so your eSign can be used for international contracts. Think of it like this: eSign started as a tool for filing your taxes, and in the future it could be how you buy a house, get a loan in Dubai, or sign a contract with a company in London.

[+] The Positive — What Works Well

The DIA has the potential to fix the First Schedule problem: The most significant limitation on eSign's market — the exclusion of wills, trusts, powers of attorney, and property sales — could be addressed by the Digital India Act. If even some of these exclusions are removed, eSign's addressable market would expand by an estimated 30-40%. The real estate sector alone (8-10 lakh crore annual transaction value) would become accessible.

The ULI + AA + eSign stack is India's next DPI export: The combination of Account Aggregator (data sharing), Unified Lending Interface (credit assessment), and eSign (agreement execution) creates a complete digital lending stack that no other country has. India's DPI playbook (UPI, Aadhaar) has a strong track record of domestic success → international adoption. eSign as a component of this stack benefits from the network effects of the broader ecosystem.

The India-EU arrangement (Jan 2026) is strategically significant: This is the first time India's PKI ecosystem has been formally linked to the EU's eIDAS framework. If operationalised, it means an Indian business can sign a contract with an EU counterparty using Aadhaar eSign and the contract is legally valid under EU law. The economic value of reducing friction in India-EU cross-border commerce (estimated at €100 billion+ annually) is substantial.

Post-quantum preparation is happening early: eMudhra's Crypta Labs acquisition and CCA's PQ awareness suggest India's PKI ecosystem will not be caught unprepared by the quantum threat. The hybrid certificate approach (RSA + PQ in parallel) is a prudent transition strategy that maintains backward compatibility while future-proofing.

[-] The Negative — What's Wrong or Missing

The DIA has been in consultation since 2023 with no passage in sight: The Digital India Act was first introduced in draft form in 2023. As of mid-2026, it has not been tabled in Parliament. The timeline for its passage (2027–2028 at best) is slow — the IT Act's inadequacies have been known for years. Every year of delay means another year where eSign's scope is artificially constrained by the First Schedule exclusions.

The ULI vision paper promises 450M new borrowers but dodges hard questions: The scale is impressive, but the 450 million figure assumes that technology (AA + eSign) can overcome structural barriers — land titling gaps, informal income documentation, fragmented credit bureau coverage. eSign solves the signing bottleneck, not the credit assessment bottleneck. Over-promising on ULI's scope risks a credibility gap when the numbers don't materialise.

Post-quantum migration will be expensive and disruptive: Every CA must upgrade or replace its HSM infrastructure. Every ESP must update its signing services. Every ASP must update its verification libraries. The cost (estimated at 500– 1,000 crore across the ecosystem) will be passed to end users.

The transition will create a multi-year period of PKI fragmentation (RSA-only vs. hybrid vs. PQ-only certificates) that will cause verification failures for users with outdated libraries.

Cross-border recognition remains aspirational: The India-EU Administrative Arrangement (Jan 2026) is a cooperation framework, not a mutual recognition treaty. Full technical interoperability — PKI bridge, trusted list linkage, OCSP cross-querying — is at least 2-3 years away. For India-UAE, India-Singapore, and India-Japan, discussions are even earlier-stage. Wait for execution, not announcements.

No regulatory framework for AI-enabled fraud detection exists yet: As deepfakes and synthetic identity fraud become more sophisticated, the absence of regulatory standards for AI-based anti-spoofing in eSign is a growing vulnerability. UIDAI has not disclosed its liveness detection methodology, and CCA's e-authentication guidelines do not address AI threats. The regulatory framework is playing catch-up.

Appendices

Appendix A: Complete Timeline

Date	Event
17 Oct 2000	IT Act, 2000 enacted; CCA established
27 Oct 2009	IT Amendment Act, 2008 effective — Section 3A introduced
Jan 2009	UIDAI established
Sep 2010	First Aadhaar number issued (Maharashtra)
28 Jan 2015	GSR 61(E) — Aadhaar eSign added to Schedule II
8 Apr 2015	GSR 304(E) — eSign Rules, 2015 notified
24 Jun 2015	CCA E-authentication Guidelines v1.0
~2015 H2	First eSign transactions (Income Tax, MCA-21)
2016	Aadhaar Act passed; UIDAI becomes statutory
Aug 2017	*Puttaswamy I* — Right to Privacy fundamental right
2018	*The Tribune* Aadhaar breach expose
Sep 2018	*Puttaswamy II* — Aadhaar upheld; Section 57 struck down
May 2019	CCA updated e-Authentication Guidelines; API v3.x published
Sep 2019	eSign API v3.2 — current standard
Oct 2022	UIDAI launches AI/ML Face Authentication
2023	Digital Personal Data Protection Act passed
2023	ULI prototype launched by RBIH
Apr 2024	IRDAI mandates e-policies; eSign volumes surge

Date	Event
1 Jul 2024	Bharatiya Sakshya Adhiniyam, 2023 effective
Nov 2025	Aadhaar auth peaks at 231 Cr/month
27 Jan 2026	India-EU Administrative Arrangement on E-signatures signed
2026	Digital India Act under consultation
2026–2027	Puttaswamy Money Bill challenge expected to be heard

Appendix B: Licensed Certifying Authorities Directory

CA	Type	Licensed Since	eSign Service	Website
eMudhra Limited	CA + ESP	2005	emSigner	emudhra.com
C-DAC	CA + ESP	2001	e-Hastakshar	cdac.in
Protean eGov (NSDL)	CA + ESP	2004	Protean eSign	proteantech.com
Capricorn Identity	CA + ESP	2009	CapriSign	capricorn.co.in
VSign Technologies	CA + ESP	2017	VSign	vsign.in
Sify Technologies	CA	2001	(via partners)	sify.com
CDSL Ventures	CA + ESP	2021	CDSL eSign	cdslventures.com
CSC e-Gov	ESP	2018	CSC eSign	csc.gov.in

Appendix C: Key Statistics Summary

Statistic	Value	Source Date
Aadhaar holders	142+ crore	July 2026
Cumulative Aadhaar auth	1,545+ crore	Mid-2025
Cumulative e-KYC	2,393+ crore	Apr 2025
Monthly auth (peak)	231 crore	Nov 2025
Monthly e-KYC	47.19 crore	Nov 2025
eSign daily (eMudhra)	350,000+	FY2026
Digital sig market size	USD 190M	2024
Projected market (2032)	USD 1.35B	CAGR ~27.5%
eSign cost floor	3/signature	2026
Licensed CAs	8	July 2026
DPDP Act penalty cap	250 crore	2023

Appendix D: Glossary

Term	Definition
AA	Account Aggregator — consent-based financial data sharing framework
Aadhaar	12-digit unique identity number issued by UIDAI
ASP	Application Service Provider — entity integrating eSign into its application
AUA	Authentication User Agency — entity using Aadhaar authentication
BSA	Bharatiya Sakshya Adhiniyam, 2023 — replaces Indian Evidence Act
CA	Certifying Authority — licensed entity issuing digital certificates
CCA	Controller of Certifying Authorities — apex PKI regulator
CIDR	Central Identities Data Repository — UIDAI's biometric database
CSR	Certificate Signing Request — PKCS#10 format
DIA	Digital India Act — proposed replacement for IT Act 2000
DPDP	Digital Personal Data Protection Act, 2023
DSC	Digital Signature Certificate — under Section 3 IT Act
ESP	eSign Service Provider — CA subsidiary offering eSign APIs
HSM	Hardware Security Module — FIPS 140-2 certified key storage
KYC	Know Your Customer — identity verification process

Term	Definition
OCSP	Online Certificate Status Protocol — real-time cert revocation check
PAdES	PDF Advanced Electronic Signature — CMS-based signature in PDF
PID	Personal Identity Data — biometric or OTP authentication block
PKI	Public Key Infrastructure
QES	Qualified Electronic Signature — highest tier under eIDAS
RCAI	Root Certifying Authority of India — CCA's root
TSA	Time Stamping Authority — trusted timestamp provider
UIDAI	Unique Identification Authority of India
ULI	Unified Lending Interface — RBIH's lending DPI
VID	Virtual ID — temporary, revocable Aadhaar substitute

References

This document was compiled as primary research material and does not constitute legal advice. Statutory provisions are cited as of July 2026. Court rulings cited are as reported in official law reports. Market data sourced from publicly available disclosures, industry reports, and government dashboards.

About This Book

What This Book Is

This book is the definitive reference on India's Aadhaar eSign ecosystem. It covers the full stack: the law, the technology, the market, the players, the risks, and the future. It is written for practitioners, policy analysts, legal professionals, and anyone who wants to understand how India's digital signature system actually works.

What This Book Is Not

This is not a vendor manual. It is not a government white paper. It is not marketing material for the digital signature industry. It maintains a critical, independent perspective throughout, naming what works and what does not.

The CashlessConsumer Lens

CashlessConsumer is a fintech and DPI research publication that examines digital financial infrastructure from the consumer's perspective. Every analysis in this book asks: *Does this increase or reduce the user's agency? Is the power balance fair? Who benefits and who bears the risk?*

How to Read This Book

- **New to eSign?** Start with Chapter 1. The ELI5 summaries at each chapter are written for you.
- **Technical reader?** Focus on Chapter 3 (architecture), Chapter 10 (security), and Chapter 13 (future).
- **Legal professional?** Part II (Chapters 5-7) covers the legal framework and court cases.
- **Policy analyst?** Chapters 8, 9, and 12 cover adoption data, use cases, and regulation.

- **Short on time?** Read the ELI5 summaries throughout, plus the Assessment section at the end of each chapter.

Edition

First edition, compiled July 2026. This is a living document — corrections, updates, and new chapters will be published as the ecosystem evolves.

License

About the Author

CashlessConsumer is a fintech and digital public infrastructure researcher. Through the CashlessConsumer newsletter and DPI Watch publication, they cover India's digital payments landscape, Aadhaar, UPI, ONDC, account aggregators, and the regulatory framework around digital identity.

The author runs automated content operations on Zo Computer, self-hosts AI tools for research and production, and maintains a strong interest in open data, public transit, Tamil language, and free (freedom) code.

Published works appear at: - CashlessConsumer Newsletter - DPI Watch - GitHub