

# ESIGNATURES AND THEIR LEGALITY IN INDIA



## Introduction

E-Signatures are legally valid and acceptable in the court of law in India. India follows the hierarchical root of the trust model where e-Signatures or digital signatures issued by a Certifying Authority are considered legally valid. Specific use cases for e-Signatures are indicated in the Information Technology Act 2000 (IT Act). The IT Act (established in 2000) highlights that a handwritten signature isn't always needed for a contract to be considered genuine and that contracts can't be refused for simply being electronic. They will be termed legal if individuals have reached an agreement (either agreeing verbally, electronically, or by physically signing).

Under Section 65B of the Evidence Act (1872). e-Signature solutions can be used to give electronic records that are admissible as evidence to support contracts in court. This means that Indian law treats electronic signatures equivalent to physical signatures with fewer exceptions. Usage of e-Signature must satisfy certain conditions that will be discussed in this document while providing an overview of how eMudhra's Digital signature solution meets them.

## CONTENTS

1. Introduction
2. Validity and requirements of e-Signature
3. Usage of eSignatures along with Aadhaar/PAN
4. Use Cases not appropriate for e-Signatures
5. Summary
6. About us

## Validity and requirements of e-Signature

The Indian IT act recognizes the legal status of a hand-written signature as well as e-Signatures and favors the use of electronic signatures. Companies listed in India can choose the best-suited option amongst these. Electronic Signature Technology works on Public Key Infrastructure framework, which uses a Cryptographic Key Pair – Private and Public Key for secure access and transmission of information.

Concerning security and compliance, e-Signature solutions must follow the below mentioned mandates recognized by the Indian IT Act which are:

- E-Signatures are generated by the issuer for the client in a secure device using an asymmetric cryptosystem with a long term validity of 1/2/3 years. This needs to be stored as a certificate based digital ID on a USB token secured by a personal pin, which is to be applied when the signer digitally signs the document
- E-Signature solutions must combine eKYC, which is enabled by Aadhaar/PAN identity number using eSign

For eSignatures to be valid, they must satisfy the following requirements:

- Each e-Signature is and must be unique to the signatory. They must be linked to the authorized signatory and no other person. This is done through a certificate based digital-ID
- During the time of signature, the authorized signatory must have control to affix his signature on respective documents
- Any changes or alterations done to the document, including changes on the affixed signature must be detectable
- Audit trail must be present during the signing process
- Only the Controller of Certifying Authorities appointed under the IT Act can issue the signer certificates and e-Signature or digital signature certificates

For legal validity of the documents signed using e-Signature, all the above requirements are to be satisfied under legal presumption.

## Usage of eSignatures along with Aadhaar/PAN

eSign services in India were introduced for easy and secure signing of electronic documents under the directives of the Controller of Certifying Authorities. Secure enrollment in eSign services can be done using the Aadhaar/PAN enabled eKYC method. This preferred method for e-Signature provides an alternate to the certificate-based Digital ID. Since this system is integrated into the national identity system, signers need not produce multiple documents as proof of their identity before getting their Digital ID.

Keeping in line with the Digital India Initiative by the Government of India, e-Signature services can facilitate a PAN Card / Aadhaar Holder to digitally sign a document within seconds from anywhere and anytime. A Certifying Authority under the Ministry of IT, Government of India can issue legally valid e-Signatures. eMudhra's eSign service is an electronic signature service as per the second schedule of the IT Act.

eSign service enables Application Service Providers (ASP) to enable their users to electronically sign documents using Aadhaar number. This will be a valid legal signature, in accordance to the India IT Act and substitutes the need for a physical or wet signature. In this regard, eMudhra can partner with other application service providers to build eKYC (including Aadhaar based) experiences into their solutions.. For instance, eMudhra's eSign can be used by Banks, Financial Institutions, and various other agencies for routine service requests such as Deposits, Nominations, Salary Accounts, etc.

## Use Cases not appropriate for e-Signatures

There are some specific use cases that not supported for digital or electronic processes or that includes requirements wherein wet ink or handwritten signatures or formal notarization is required.

Here are some cases wherein the IT Act is not applicable:

- Handwritten - negotiable instrument, other than a cheque
- Handwritten - Power-of-Attorney
- Handwritten - Trust Deed
- Handwritten - Will or any other testamentary disposition
- Handwritten - Any contract for the sale or conveyance of immovable property or any interest in such property

## Summary

The Government of India's Digital India initiative focuses on digital infrastructure and aims to transform India into a paperless economy. In the past few years, the Government's initiative to promote digitized economy has resulted in the widespread acceptance of electronic records and electronically signed documents by government authorities. The introduction of eKYC using Aadhaar/PAN by various regulators supports the increasing acceptance of eSignatures.

For organizations implementing e-Signatures, it is recommended that only electronic signatures be recognized by the IT Act to avoid any risks, such as admissibility and enforceability of documents or contracts signed electronically before the authorities.

Application service providers such as eMudhra offer dedicated solutions designed to address the requirements discussed in this paper.

---

[1] An AES is an "advanced electronic signature", a type of electronic signature that meets the following requirements:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using means that are under the signatory's sole control;
- (d) it is linked to other electronic data in such a way that any alteration to the said data can be detected.

[2] A QES is a specific digital signature implementation that has met the particular specifications of a government, including using a secure signature creation device, and been certified as 'qualified' by either that government or a party contracted by that government.

### External Resources

<http://www.meity.gov.in/content/information-technology-act>  
<http://lawcommissionofindia.nic.in/1-50/report13.pdf>

## About us

As the world goes Digital, security is ever more crucial to protect identities, data, and enable trust in a digital society. eMudhra focuses on SECURE Digital Transformation to enable organizations to progress and evolve without sacrificing "Trust," which matters most in our society. With an end-to-end stack around trust services, PKI, Paperless transformation, and Digital Authentication, eMudhra is optimally placed to aid digital journeys where identity assertion is critical. eMudhra chairs the Asia PKI Consortium, is a board member of the Cloud Signature Consortium and a member of the CA Browser Forum. Having been in business for over 12 years and built a reach that spans more than 45 countries, eMudhra is deeply committed to bringing change and helping societies across not just go digital but go digital in a secure way.

## Disclaimer

This information is intended to help you understand the legal framework of electronic signatures. However, eMudhra cannot provide legal advice. The law of electronic signatures is constantly evolving. This guide is not intended as a legal advice and should not serve as a substitute for professional legal advice. You should consult an attorney regarding any specific legal concerns. eMudhra, and all associates including agents, officers, employees or affiliates, are not liable for any direct, indirect, incidental, special, exemplary or consequential damages.