Adobe Sign

Electronic signatures in India.

Legal considerations and recommendations for best practices—A Trilegal white paper.

Introduction.

Indian law has recognised electronic signatures, or e-signatures, under the Information Technology Act, 2000 (IT Act) for over 16 years. With its increased emphasis on improving the ease of doing business; streamlining the storage of records; and improving the safety, security, and cost-effectiveness of records, the Government of India has promoted the use of digital technologies by Indian citizens and corporations. As a result, there has been a recent increase in the use of e-signatures, with more and more services using them. This, in part, is due to the government's focus on enabling electronic transactions using Aadhaar, the unique identification number issued by the Indian government to all Indian residents.

Indian law treats electronic signatures as equivalent to physical signatures, subject to a few exceptions, and generally allows documents to be signed using e-signatures. However, the e-signature must satisfy a number of conditions, and certain checks must be done before it can be relied upon. This white paper provides an overview of the law in India relating to e-signatures and briefly describes how Adobe Sign, an e-sign solution from Adobe, meets those conditions.

Requirements for validity.

The IT Act broadly provides for the enforcement of electronic signatures and recognises two types as having the same legal status as handwritten signatures. This lets companies choose the method best suited to their unique requirements. The methods specifically recognised under the IT Act are:

- Electronic signatures that combine an Aadhaar identity number with an electronic Know-Your-Customer (eKYC) method (such as a one-time passcode). This method is known as the eSign Online Electronic Signature Service.
- Digital signatures that are generated by an "asymmetric crypto-system and hash function." In this scenario, a signer is typically issued a long-term (1- to 2-year) certificate-based digital ID stored on a USB token that is used—along with a personal PIN—to sign a document.

Adobe Sign, an Adobe Document Cloud solution, supports both methods.

CONTENTS

For the two types of e-signatures to be valid, they must satisfy these additional conditions:

- E-signatures must be unique to the signatory (they must be uniquely linked to the person signing the document and no other person). This condition is met with a certificate-based digital ID.
- At the time of signing, the signatory must have control over the data used to generate the e-signature (for example, by directly affixing the e-signature to the document).
- Any alteration to the affixed e-signature, or the document to which the signature is affixed, must be detectable (for example, by encrypting the document with a tamper-evident seal).
- There should be an audit trail of steps taken during the signing process.
- Signer certificates must be issued by a Certifying Authority recognised by the Controller of Certifying Authorities appointed under the IT Act. Only a Certifying Authority licensed by the Controller of Certifying Authorities can issue e-signature or digital signature certificates. View a list of licensed Certifying Authorities.

If all these conditions are satisfied, then there is a legal presumption in favour of the validity of any document signed using an electronic signature.

The IT Act is currently the main source of law governing the validity of e-signatures in India. At this stage, there is no case law dealing specifically with disputes in relation to the application of e-signatures.

E-signatures with Aadhaar eKYC.

The Controller of Certifying Authorities introduced the eSign Online Electronic Signature Service for easy, effective, and secure signing of electronic documents by authenticating the signer using Aadhaar eKYC services. Signatures generated using an Aadhaar-enabled eKYC method are emerging as the preferred method for e-signatures recognised under the IT Act. It replaces the need to get a certificate-based digital ID through a printed paper application form with an ink signature. And because it is already tied to the national identity system, signers do not need to produce multiple documents before getting their digital ID.

Aadhaar eKYC is a paperless process in which the identity of the subscriber is verified through the Aadhaar authentication process of the Unique Identification Authority of India, using either biometrics or a one-time passcode (OTP). The eSign Online Electronic Signature Service works with specific accredited service providers that provide certificates and authentication services that comply with government guidelines.

Application service providers, like Adobe, are allowed to work with the accredited service providers to build Aadhaar eKYC experiences into their solutions. For instance, the Aadhaar implementation available for use with Adobe Sign is enabled by a partnership with one of the accredited providers, C-DAC.

Government use of e-signatures.

Government authorities such as the Ministry of Corporate Affairs, Department of Revenue, and Ministry of Finance accept electronic records authenticated using e-signatures.

The Reserve Bank of India (RBI) recently allowed small finance banks and payment banks to rely on electronic authentication for confirmation of the terms and conditions of the banking relationship. It also allowed a one-time-passcode based eKYC process for onboarding customers by all regulated entities. In addition, the Department of Telecommunications recently issued detailed guidelines allowing telecom service providers to use the Aadhaar eKYC process to issue new mobile connections as an alternative to the existing proof of identity and proof of address document-based process.

The government increasingly relies on the Aadhaar-based eKYC process as a mode of delivering services and proving identity. These examples indicate the shift towards use of e-signatures.

Where e-signatures cannot be used.

The following documents cannot be electronically signed and must be executed using traditional "wet" signatures to be legally enforceable:

- Negotiable instruments such as a promissory note or a bill of exchange other than a check
- Powers of attorney
- Trust deeds
- Wills and any other testamentary disposition
- Real estate contracts such as leases or sales agreements

Other considerations when signing electronically.

Requirement to stamp.

In India, certain documents must be stamped before or at the time of execution. Currently, no laws in India prescribe a method for stamping electronic documents.

Some states such as Maharashtra, Karnataka, and Delhi specifically extend the requirement for stamping to electronic records. When stamps are accepted electronically, solutions like Adobe Sign can be tailored to meet those requirements.

Companies should always confirm with their internal legal team whether a document needs to be stamped before signing and executing the document electronically. If a document is signed and executed electronically and is required to be stamped, then the company should ensure that a physical copy of the document is prepared and stamped.

If a document is not properly stamped, then in some circumstances, financial penalties may be imposed. Some states penalise the deliberate non-stamping of documents with imprisonment and/or a fine (although these provisions are rarely enforced).

Validity of other forms of electronic signing.

Documents signed using an electronic means other than an e-signature as prescribed under the IT Act are not necessarily invalid. For example, a contract that is executed using email as the first authentication method or that adds a second factor of authentication, such as a password or phone PIN, may be valid under Indian law, provided it satisfies the requirements of the IT Act.

However, documents that are executed using one of these methods are not treated the same as documents signed with wet signatures. For example, if the validity of an electronic contract is disputed, the party claiming validity of the contract must be able to demonstrate that the essentials of a valid contract are fulfilled and that the parties in fact did execute the contract using a non-tamperable method.

Despite this additional requirement, however, the use of email and other common methods of authentication of contracts is still widespread within the technology and e-commerce sector.

If email or another form of authentication is used to sign a document electronically, then the following industry best practices should be implemented to help satisfy the requirements of the IT Act:

- Include a mechanism for verifying the identity of the party who signed the document (for example, by sending a verification request to a unique email address, or sending an OTP to the signing party's mobile phone).
- Obtain the signing party's consent to do business electronically.
- Be able to demonstrate clearly that the signing party intended to sign the document electronically by the particular method used.
- Track the process securely, and keep an audit trail that logs each step.
- Secure the final document with a tamper-evident seal.

All of these industry best practices are incorporated into Adobe Sign.

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 a digitised economy has resulted in widespread acceptance of electronic records and electronically signed documents by government authorities. The introduction and adoption of Aadhaar eKYC by various sectoral regulators support the increasing acceptance of e-signatures.

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

Application service providers, like Adobe, offer dedicated solutions designed to address the requirements discussed in this paper.

Trilegal
September 2017

Resources.

Learn more about how Adobe Sign addresses legal electronic signatures in India.

DISCLAIMER: This information is general in nature and not legal advice. It cannot be relied on as legal advice. If legal advice is required, you should consult a lawyer.