Adobe Sign

Electronic signatures in India.

Legal considerations and recommended best practices—an Adobe/Trilegal white paper.

Introduction to electronic signatures.

Indian law has recognised electronic signatures, or e-signatures, under the Information Technology Act, 2000 (IT Act) for over 18 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.

The IT Act treats electronic signatures recognized under it as equivalent to physical signatures, subject to a few exceptions. It also generally allows documents to be signed using any form of e-signatures. However, an 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 in relation to e-signatures and briefly describes how Adobe Sign, an electronic signature solution from Adobe, simplifies electronic signatures and allows you to sign documents securely.

Requirements for validity.

The IT Act broadly provides for the enforcement of electronic signatures and recognises two types of electronic signature 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 USB token, which is used—along with a personal PIN—to sign a document.

For the two types of e-signatures to be valid under Indian law, they must satisfy these additional conditions (Reliability 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 audit trail of steps taken during the signing process.
- Signer certificates must be issued by a Certifying Authority (CA) recognised by the Controller of Certifying Authorities appointed under the IT Act. Only a CA licensed by the Controller of Certifying Authorities can issue e-signature or digital signature certificates. View a list of licensed Certifying Authorities.

If each of the Reliability Conditions is satisfied, then there is a legal presumption in favour of the validity of any document signed using an electronic signature.

Please note that Adobe has engaged eMudhra, which is a CA, to issue certificates that meet the requirements of the IT Act. Hence, a document signed using Adobe Sign which uses eMudhra-issued certificates carries the presumption of validity.

TRILEGAL

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 invalid. Section 10A of the IT Act states that contracts that are otherwise validly concluded will not be rendered invalid merely because they were made in electronic form. In the case of *Tamil Nadu Organic Private Ltd & Others v. State Bank of India*,* the Madras High Court observed that "contractual liabilities could arise by way of electronic means and that such contracts could be enforced through law." The High Court further stated that Section 10A of the IT Act enables the use of electronic records and electronic means for the conclusion of agreements, contracts, and other purposes.

A contract 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. The Supreme Court in the case of *Trimex International Fze Limited, Dubai v. Vedanta Aluminium Limited*† held that unconditional offer and acceptance through emails constituted a valid contract under the Indian Contract Act, 1872 (Contract Act). The Apex Court ruled that once the contract is concluded orally or in writing, the mere fact that a formal contract is yet to be prepared and initialled by the parties would not affect either the acceptance of the contract so entered into or implementation thereof, even if the formal contract has never been initialled.

This follows the principles enumerated under the Contract Act, which recognizes even oral and unwritten contracts, provided that principles relating to contract formation such as offer, acceptance, lawful consideration, and capacity of the parties are satisfied. Multiple judgments by Indian courts have held that the formation of a contract can be inferred based on the conduct of parties and that they need not be in writing.‡ This means that a party cannot successfully argue that a contract was never formed when he/she has acted upon the contract. For instance, an employee cannot dispute the existence of an electronic contract, if she acted upon it by coming to the workplace and performing her duties or drawing salaries or benefits under the employment contract.

The documents that are executed using such other methods are not treated the same as documents signed with wet signatures. Therefore, 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 technology that followed the Reliability Conditions.

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.

However, customers can use Adobe Sign in combination with certificates issued by eMudhra, which is a CA. For these use cases, there will be presumption of validity in favour of documents signed using Adobe Sign in combination with eMudhra-issued certificates. In addition, using Adobe Sign, the customer can implement features and functionality that achieve industry best practices including a mechanism for determining the identity of the signatories, audit trails, and providing encryption to ensure that the final document is tamper-proof.

Adobe Sign allows the user to electronically sign an electronic document using certificates and store such document in the cloud or email a signed document to a unique email address. In the case of a contract, the recipient signing party can countersign the document as required. However, the signing party cannot make any other modifications to the document unless so requested by the document sender. Once the signer completes the fields, Adobe Sign enables the contract to be emailed back to the sender, which can be downloaded as a tamper-proof PDF.

* *Tamil Nadu Organic Private Ltd & Others v. State Bank of India,* AIR 2014 Mad 103.

† *Trimex International Fze Limited, Dubai v. Vedanta Aluminium Limited,* (2010) 3 SCC 1.

‡. *Haji Mohammed Ishaq v. Mohamed Iqbal,* AIR 1978 SC 798.

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 digital signatures. In the case of e-filing with the Ministry of Corporate Affairs, income tax and GST (goods and service tax) filings, digital signatures are the preferred mode of execution.

The Reserve Bank of India (RBI) has allowed small finance banks and payment banks to rely on electronic authentication for confirmation of the terms and conditions of the banking relationship. The RBI also allowed a One Time Pin (OTP) based eKYC process for onboarding customers by all regulated entities, subject to certain conditions.

These examples indicate the shift towards the use of e-signatures.

Where electronic signatures cannot be used.

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

- Negotiable instruments such as a promissory note or a bill of exchange other than a cheque
- Powers of attorney
- Trust deeds
- Wills and any other testamentary disposition
- Real estate contracts such as leases or sale 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 law in India prescribes 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 deliberate non-stamping of documents with imprisonment and/or fine (although these provisions are rarely enforced).

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

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 a widespread acceptance of electronic records and electronically signed documents by government authorities.

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 electronic signature based dedicated solutions designed to address the requirements discussed in this paper.

Trilegal
January 2020