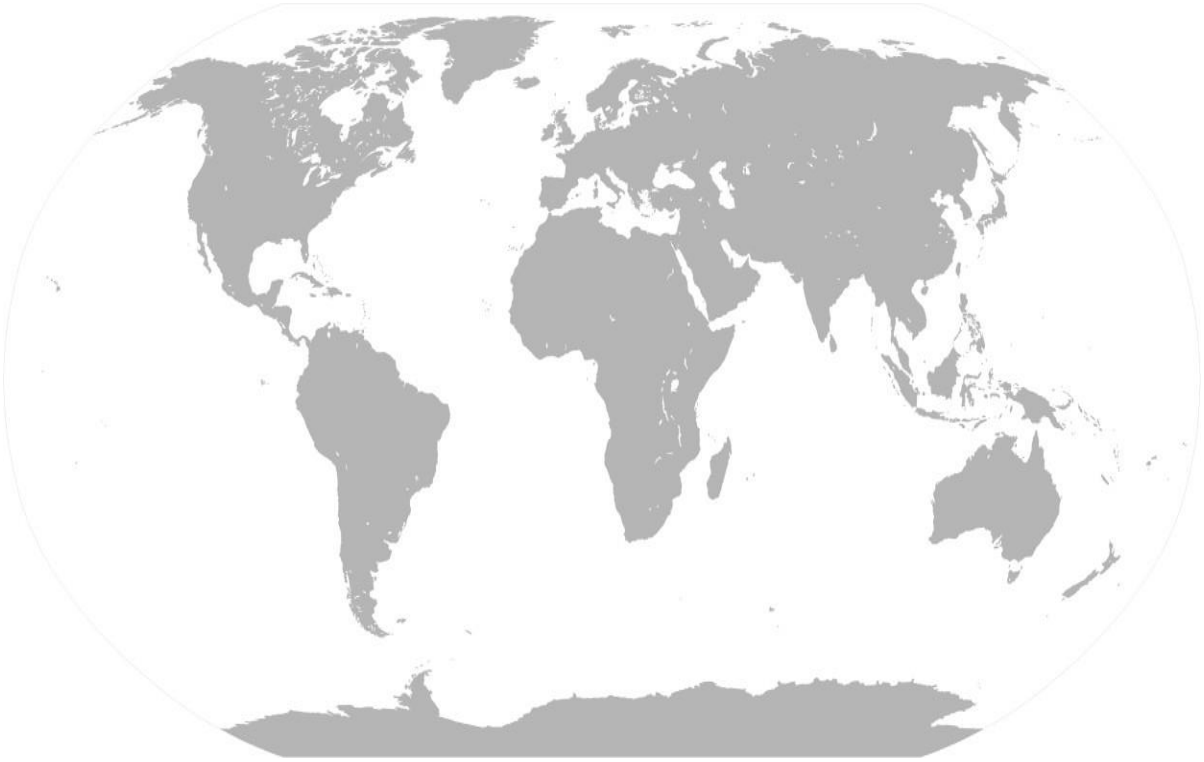
Amicus
Transcending Frontiers



ELECTRONIC SIGNATURE – LEGALLY POSITIVE?

APRIL 22, 2020

E-mail: info@amicusservices.in
Website: www.amicusservices.in

ELECTRONIC SIGNATURE – LEGALLY POSITIVE?

COVID-19 has forced all of us to be innovative with the way we work and made us realize the importance of doing things digitally. The basic legal framework with respect to electronic signature (e-sign) and electronic records has been there for quite some time in India, but there has been a reluctance by both private entities as well as authorities to make regular use of it. The current situation can therefore, be seen as a blessing in disguise as it is now forcing authorities, courts and corporate entities to seriously consider the digital way of doing things. In this article, we explore the existing laws on electronic signature for signing of contracts and the way forward.

A. Essential Elements of a Contract

To understand the validity and enforceability of the electronic signing of contracts, it is first important to understand the essential elements of a contract. As per The Indian Contract Act,1872 ("**Contract Act**") all agreements are contract if[1]:

1. they are made by free consent;
2. by parties competent to contract;
3. for a lawful consideration and with a lawful object and
4. not expressly declared to be void.

Contracts are only required to be in writing if any law specifically provides for it. Further the communication of offer or acceptance or revocation is deemed to be made by the action or omission of the communicating party[2]. Hence, for an agreement to be a contract it is not required that it is executed through wet signature and can be oral or even electronically signed as long as the intention of the parties to enter into contract can be proved.

B. Electronic Signature under the Information Technology Act, 2000

The Information Technology Act, 2000 ("**IT Act**") is the primary Act which deals with electronic records, electronic signatures, grants legal recognition to electronic transactions and highlights other ancillary legal definitions vis-à-vis the concerned spectrum of the Act. In terms of sections 3 and 3A of the IT Act any subscriber may authenticate an electronic record[3] by affixing his electronic signature. Section 2(ta) of the

[1] Section 10 of the Contract Act- All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void.
Nothing herein contained shall affect any law in force in India and not hereby expressly repealed, by which any contract is required to be made in writing or in the presence of witnesses, or any law relating to registration of documents.

[2] Section 3 of the Contract Act- The communication of proposals, the acceptance of proposals, and the revocation of proposals and acceptances, respectively, are deemed to be made by any act or omission of the party proposing, accepting or revoking, by which he intends to communicate such proposal, acceptance or revocation, or which has the effect of communicating it.

[3] Section 2(t) of the IT Act- "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche

Act defines an electronic signature to mean authentication of any electronic record by a subscriber by means of the electronic technique by:

1. **Digital Signature -** A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. It is based on two keys public and private. The user retains control of the private key; it can only be used with the issued password. The public key is disseminated with the encrypted information. One key locks or encrypts the plain text, and the other unlocks or decrypts the cipher text but neither key can perform both functions. In case a document is changed after the affixation of the digital signature, the digital signature is invalidated. A digital signature certificate (DSC) is issued by the certifying authority[4]and contains information about the user's name, pin code, country, email address, date of issuance of certificate and name of the certifying authority.

2. **Any electronic technique specified in the Second Schedule (of the IT Act) –** The Central Government is permitted to add reliable ways of electronic signature/electronic technique to the second schedule of the IT Act. Currently, e-authentication technique using Aadhaar or other e-KYC services are allowed. As until now, the certifying authorities are providing electronic-signing based on Aadhaar e-KYC. Any person having Aadhaar number can use this technique. Every time a transaction request is made, KYC authentication takes place in real-time through Aadhaar e-KYC and by using one time password/biometric of such user. A Digital Signature Certificate is thereafter issued for one-time use for digitally signing the document. The user can also use offline KYC (XML) to open an eKYC Account. Thereafter on following the procedure laid down by the Certifying Authority digital signature certificate will be issued to the user.

Since Aadhaar based e-signing is backed by the IT Act and undertaken voluntarily by the subscriber it is assumed to be outside the purview of Supreme Court judgment that restricted the usage of Aadhaar e-KYC authentication by private entities[5]. Unfortunately, there has been no clarity on this aspect from any authority and it continues to be a matter of concern for the entities which use such electronic signature extensively. On 5th March 2019, the Ministry of Electronics and Information Technology amended the Second Schedule to the IT Act and inserted the word "Other" after Aadhaar e-KYC to include e-authentication technique using other e-KYC services. Therefore, Electronic Signature can be generated using e-Authentication techniques which may or may not be linked to Aadhaar.

C. Enforceability of Electronic Signatures based Contracts

1. The definition of the electronic signature under the IT Act does not include any other type of signing i.e. click wrap or virtual signature, so the question that has to be answered is whether these electronic signatures are enforceable in courts or not? Section 10A of the IT Act comes to the rescue as it provides that, where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances as the case may be, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the

[4] As per 2(g) of the IT Act "Certifying Authority" means a person who has been granted a licence to issue an Electronic Signature Certificate under section 24;
[5] Justice K.S. Puttaswamy and Ors. vs. Union of India (UOI) and Ors. (26.09.2018 - SC) : MANU/SC/1054/2018

ground that such electronic form or means was used for that purpose. The section thus clarifies that contracts that are executed using other type of electronic signature can be enforced through law. The said proposition was further expounded by the Madras High Court in the judgment of Tamil Nadu Organic Private Ltd v. State Bank of India6 wherein, relying upon Section 10A of the Act, it has observed that contractual liabilities could arise by way of electronic means.

2. An important piece of legislature in determining enforceability of any document is the Indian Evidence Act, 1872 ("**Evidence Act**") which has gone through multiple amendments to be aligned with the IT Act. Under the Evidence Act, courts are to presume that electronic record containing electronic signature[7] was concluded by affixing the electronic signature of the parties[8]. Similarly, in case of secure electronic signature[9] the burden of proof is on the person disputing it[10]. Hence, under the Evidence Act, secured electronic signature as defined under the IT Act are presumed to have been duly affixed.

3. The Evidence Act is silent on the presumption in case of other types of electronic signature however the burden of proof will likely be on the person relying upon it. There is not much jurisprudence in India on e-signing of documents but courts in the past have upheld the validity of electronic contracts based on the actions of the parties. In Trimex International FZE, Dubai v. Vedanta Aluminum Limited[11] wherein contract through email was held to be valid it was observed: "It is clear that in the absence of signed agreement between the parties, it would be possible to infer from various documents duly approved and signed by the parties in the form of exchange of e-mails, letter, telex, telegrams and other means of tele-communication." Therefore, it is important that reliable data with respect to affixation of the other types of electronic signature of the person is duly recorded and stored to enable a party to prove the affixation of such. Section 3A of the Act provides certain conditions pertaining to the reliability of electronic authentication and these can be taken as guiding principles for proving the validity and authenticity of other types of electronic signature. The conditions of reliability include:

a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory' or, as the case may be, the authenticator and to no other person;
b) the signature creation data or the authentication data were, at the time of signing, under the

---

[6] AIR 2014 Mad 103

[7] As per Section 3 of the Evidence Act the expression "electronic signature", "secure electronic signature" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.

[8] Section 85A of the Evidence Act- The Court shall presume that every electronic record purporting to be an agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties.

[9] As per section 15 of the IT Act - 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 exclusive control of signatory and no other person; and
(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.
Explanation.-- In case of digital signature, the "signature creation data" means the private key of the subscriber.

[10] Section 67A of the Evidence Act: Except in the case of a secure electronic signature, if the electronic signature of any subscriber is alleged to have been affixed to an electronic record the fact that such electronic signature is the electronic signature of the subscriber must be proved.

[11] (2010) 3 SCC 1

control of the signatory or, as the case may be, the authenticator and of no other person;

c) any alteration to the electronic signature made after affixing such signature is detectable;

d) any alteration to the information made after its authentication by electronic signature is detectable

D. Documents and transactions that cannot be authenticated by an electronic signature

The IT Act does not apply to the following documents and transactions:

1. A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
2. A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
3. A trust as defined in section 3 of the Indian Trust Act, 1882;
4. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called.
5. Any contract for the sale or conveyance of immovable property or any interest in such property.

E. Conclusion

Digital signature and electronic signature mentioned in Second Schedule of the IT Act including e-kyc based electronic signatures, are enforceable and under the Indian Evidence Act, 1872 there is a presumption that secured electronic signature are valid unless the contrary is proved. Any other type of electronic signature is also enforceable under the IT Act but the burden of proof will be on the person relying upon it. Therefore, for other types of electronic signature it must be ensured that the contract or the electronic signature cannot be modified post affixation of the electronic signature(s). Audit trail of the virtual signature like live photo and GPS coordinates of the signatory, time stamp, IP Address of the device should be recorded and securely stored. These kind of data should also be collected for documents executed by digital signature and e-KYC based electronic signature as under the Evidence Act certain presumptions are available only if it is shown that the signature creation data, at the time of affixing signature was secured i.e. was under the exclusive control of signatory and storage and affixation of e signature was in a manner as prescribed.

F. Way Forward

In the post COVID-19 era everyone will be looking at using electronic signatures for day to day operations and not just as an alternative to be used in exceptional cases. Unfortunately, the current legal framework on digital authentication is inadequate to deal with such a situation. The following steps may be taken by the government/governing authorities to achieve the desired objective:

1. Certain presumptions under the Evidence Act are only available to secured electronic signature[12] which puts a limited burden of proof on the person relying on the electronic signature to show that the data was under the control of the signatory. This is open to interpretation as how this is to

[12] ibid

be proved. In our view, digital signature and e-kyc based e signing are issued and used as per the procedure prescribed under the IT Act therefore the presumption under the Evidence Act should be without restriction in case of such electronic signatures and the burden of proof should be on the signatory.

2. The definition of "electronic signature" under the IT Act to be broadened to include other types of digital authentication subject to adherence to conditions of reliability as provided under the IT Act or such other conditions as may be required. Similarly, amendment must also be made to the Evidence Act to grant a presumption of validity to different types of digital authentication which can be made subject to compliance with certain conditions.

3. The definition of "electronic record" under the IT Act provides that it means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche[13]. The definition of "electronic record" should be amended to specifically include electronic contracts and agreements that are stored in computer or any other electronic device to clarify the validity of electronic contracts. Further the presumptions pertaining to electronic record and electronic signature should be aligned to ensure that there is no requirement to separately prove the validity of electronic record as well as the electronic signature affixed on it especially if the electronic record cannot be changed or tampered with post affixation of the signature.

4. In December, 2019 NSDL e-Governance Infrastructure Limited (NSDL e-Gov), a licensed Certifying Authority (CA) to provide e-Sign had issued a notice to various companies stating that it is discontinuing its Aadhaar e-sign services which notice was thereafter revoked within a day. As no reason was given for the discontinuation or revocation of discontinuation of e-signing this has created more uncertainty around the continuation of Aadhaar e-KYC based e-signing. It is, therefore, the need of the hour that clarification and confirmation on the continued use of Aadhaar based e-sign is issued to clear the ambiguity surrounding it.

- ***Joyeeta Banerjee (Associate Partner)***

[13] Ibid