**Digital Signature**

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

**Electronic Signature**

An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

**Digital Signature** was the term defined in the old I.T. Act, 2000. **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL),** electronic authentication and signature methods may be classified into the following categories −

* Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
* Those bases on the physical features of the user, i.e., biometrics.
* Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
* Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use −

* Digital Signature within a public key infrastructure (PKI)
* Biometric Device
* PINs
* Passwords
* Scanned handwritten signature
* Signature by Digital Pen
* Clickable “OK” or “I Accept” or “I Agree” click boxes

he new section 3A has  been introduced to define "Electronic Signatures" retaining the existing Section 3 which defines "Digital Signatures" and this section states as follows

***Section 3A:******Electronic Signature***

*(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication*

*(a) is considered reliable ; and*

*(b) may be specified in the Second Schedule*

*(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-*

*(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 of no other person;*

*(b) the signature creation data or the authentication data were, at the time of signing, under the 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; and*

*(e) it fulfills such other conditions which may be prescribed.*

*(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated*

*(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;*

*Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable*

*(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament*

At present no system of electronic signature has been defined in the second schedule and hence there is no change in the authentication mechanism under the Act. The present system of Digital Signatures will therefore continue for the time being and will be the only method of authentication of an electronic document.

In case the Government needs to introduce a new system, it has to notify through the Official Gazette the relevant procedure which is considered reliable. This would also require the notification to be placed before the Parliament.

Obviously the system should meet the minimum criteria of effectively establishing the authentication of a document to the person who authenticates it and also should ensure that if the document has been changed since it was signed, such alteration becomes noticeable.

If we go by the reliability of the Hash algorithms and the asymmetric cryptosytems used for the current digital signature system which are reviewed worldwide by mathematicians on a regular basis, any alternative system should also meet similar stringent standards.

In other words, if any technical solutions need to be considered as a concurrent  alternative to the present PKI based system, then the system has to be not only put to extensive tests within India but also in global circles.

Additionally, the system has to be licensed in a manner similar to the manner of licensing Certifying Authorities at present. We may therefore either see the current Certifying Authorities (CAs) themselves introducing new systems or exclusive "Electronic Signature Certifying Authorities" who may seek license from the Government and function along with the current "Digital Signature Certifying Authorities".

It is therefore considered that in the near future, the digital signature system will continue to be the sole system of authentication that would be recognized by Indian law.

The need for "Digital Signature system" to continue for the time being makes the following blunders a serious legal lacuna.

In Section 2(d) of the new Act, now there is a definition of "Affixing of an Electronic Signature" as follows:

*"Affixing****Electronic****Signature" with its grammatical variations and cognate  expressions means adoption of any methodology or procedure by a person for the  purpose of authenticating an electronic record by means of  Electronic Signature;*

There is however no corresponding definition of what is meant by "Affixing of a Digital Signature".

Fortunately the definition of "Digital signature" and "Digital Signature Certificate" remains under Section 2(p) and 2(q)  while the definition of "Electronic Signature" and Electronic Signature Certificate" has been added under Sections 2(ta) and 2(tb).

In Sections 2 (ta) and 2 (tb), the definition of "Electronic Signature" and "Electronic Signature Certificate" is given as "includes Digital Signature" or "Digital Signature Certificate". Obviously, this does not mean that the two are same but the system used in digital signature is considered "Reliable" as per Section 3 A of the new Act.

As a result, of the inclusion of digital signature in 2(ta) and 2 (tb), the regulations regarding Certifying Authorities mentioning "Electronic Signatures" will be applicable for  Digital Signatures. However regulations meant for "Digital Signatures" may not all be applicable to Electronic Signatures and their issuers.

Sections 37, 38 and 39 meant for suspension and revocation of Digital signatures will not automatically apply for Electronic signatures.

While Section 40 A specifically speaks of an intended amendment when Electronic Signature becomes a reality, similar new sections 37A,38A and 39A would also be required in such an event. Additionally many more sections where only "Digital Signature" has been mentioned need to be supported by additional sections for Electronic Signatures. In particular Section 21 which talks of licensing of Certifying Authorities itself need to be supported with a corresponding section for Electronic Signatures.

Therefore, as and when procedures for Electronic Signatures are introduced, several sections need to undergo changes. This will be another major amendment to the Act.

Some of these difficulties could have been avoided by replacing the word "Digital Signature" by the words "Digital Signature and Electronic Signature where relevant" in clause 2 of the IT Amendment Bill 2006. Now it appears perhaps that clubbing of the terms "Digital Signature" and "Electronic Signature" under Sections 2(ta) and 2 (tb)  itself was avoidable.

The law could have just made an enablement of an alternative to Digital Signatures and left other things to be added as and when any new system of Electronic signature comes for consideration. At this point of time we donot know what kind of systems can substitute or work along with Digital signatures and what kind of changes would be required in the law to accommodate them.

The legal confusions these create may also affect interpretations in Indian Evidence Act and we have interesting battles of interpretations that will confuse and confound Legal and Judicial officers in Courts. If  the final draft of the Bill had been debated in public space for some time rather than being hurriedly pushed through the Parliament, perhaps some of these confusions could have been avoided.