

Dr. Durgavati

Institute Of Law , Jiwaji University , Gwalior (M.P.)

Email- durgaadvocate1982@gmail.com

Subject - Cyber Law (IT ACT)

Date - 01.04.2020

DIGITAL SIGNATURE AND ELECTRONIC

SIGNATURE

Meaning of the word ‘ Signature’-

The word ‘Signature’ as a person name written in a distinctive way as a form of identification in authorizing a cheque or document or concluding a letter. The purpose of the signature is to authenticate the message as originating from the purported signer.

The amendment act 2008 in order to maintaining continuity with the regime of digital signature has introduced the concept of “electronic signature”(sec-3). Examples of electronic signatures may include Biometric signatures, Passwords, PINs, Encryption applications etc.

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 physical features of the user, i.e., biometrics.
- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.

- 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

LEGAL ASPECTS OF DIGITAL SIGNATURES

- The digital signature is that which makes a document a legal one
- It is a representation of assuring that the document meets all legal and is authentic in its framework.
- The actual digital signature provides the following-
 - ✓ Evidence
 - ✓ Ceremony
 - ✓ Approval
 - ✓ Efficiency

ADVANTAGES OF DIGITAL SIGNATURE

- Authentication, identification of the person that signs.
- Integrity of data, every change will be detected.
- Non repudiation, because the author cannot be denied of his work(he created and sent).
- Imposter prevention, elimination of possibility of committing fraud by an imposter.

DISADVANTAGES OF DIGITAL SIGNATURE

- The disadvantages of using digital signatures involve the primary avenue for any business money.
- Though the use of digital signatures is very powerful way to secure and authenticate a message or document, its advantage are hampered by lost or theft of keys and the use of vulnerable storage facilities.
- A number of digital signature standard exist which are incompatible with each other and there is a strong need of a standard through which these different methods(keys) can interact.

ELECTRONIC SIGNATURES- SEC 3A

Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule.

Any electronic signature or electronic authentication technique will be considered reliable if-

- Is considered reliable
- May be specified in the second schedule.

- 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;
- 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;
- any alteration to the electronic signature made after affixing such signature is detectable;
- any alteration to the information made after its authentication by electronic signature is detectable.
- It fulfils such other conditions which may be prescribed.

DIFFERENCE BETWEEN DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

1. Basic-

Digital signature, can be visualised as an electronic "fingerprint", that is encrypted and identifies the person's identity who actually signed it.

Electronic signature, could be any symbol, image, process attached to the message or document signifies the signer's identity and act an consent on it.

2. Authentication Mechanism-

Digital signature, Certificate-based digital ID.

Electronic signature, Verifies signers identity through email, phone PIN, etc.

3. Used for-

Digital signature, Securing a document.

Electronic signature, Verifying a document.

4. Validation-

Digital signature , Performed by trusted certificate authorities or trust service providers.

Electronic signature, No specific validation process.

5. Security

Digital signature, Highly secure.

Electronic signature, Vulnerable to tampering