Dr. Durgavati

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

Email- durgaadvocate1982@gmail.com

Subject - cyber law ,(I T Act)

Unit-II (secure e record & secure digital signature)

Class – B.A.LL.B. X SEM

Date - 07.04.2020

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

SECTION 14 - SECURE ELECTRONIC RECORD

Section 14 – Secure Electronic Record-

Where any security procedure has been applied to an electronic record at a specific point of time then such record shall be deemed to be a secure electronic record from such point of time then to the time of verification.

As per rule 3 of the Information Technology (security procedure) rules, 2004, " An electronic record shall be deemed to be a secure electronic record for the purposes of the act, if it has been authenticated by means of a secure digital signature."

SECTION 15 SECURE ELECTRONIC SIGNATURE

(SUBSTITUTED VIDE ITAA 2008)

SECURED ELECTRONIC SIGNATURE –

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 subscribe .

Regarding Digital Signature rule of the Information Technology (security procedure) rules , 2004 provides that- **secure digital signature**

SECURITY PROCEDURE

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including –

- The nature of the transaction.
- The level of sophistication of the parties with reference to their technological capacity.
- The volume of similar transactions engaged in by other parties.
- The availability of alternatives offered to but rejected by any party.
- The cost of alternative procedures, and
- The procedures in general use for similar types of transactions or communications.

SECURE DIGITAL SIGNATURE

Section 15. Secure digital signature.-

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was –

A. unique to the subscriber affixing it;

B. capable of identifying such subscriber;

C. created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which related in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

SECURE DIGITAL SIGNATURE

- Digital signatures are the most advanced and secure type of electronic signature. You can use them to comply with the most demanding legal and regulatory requirements because they provide the highest levels of assurance about each signer's identity and the authenticity of the documents they sign.

- Digital signatures use a certificate-based digital ID issued by an accredited Certificate Authority (CA) or Trust Service Provider (TSP) so when you digitally sign a document, your identity is uniquely linked to you, the signature is bound to the document with encryption, and everything can be verified using underlying technology known as Public Key Infrastructure (PKI).

SECURE DIGITAL SIGNATURE

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a Digital Signature, at the time it was affixed, was –

- Unique to the subscriber affixing it.
- Capable of identifying such subscriber.
- Created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated then such digital signature shall be deemed to be a secure digital signature.

SECURE DIGITAL SIGNATURE

- Your digital ID is trusted.- Compliant, certificate-based digital IDs come from accredited providers. You need to prove your identity before you can get one.
- It all gets encrypted -Your digital signature and the document you sign are encrypted together and bound with a tamper-evident seal.
- It’s unique to you -Every time you sign a document, you use your own unique digital certificate and PIN to validate your credentials and prove you’re who you say you are.
- It’s easy to validate - Both the signed document and your digital signature can be re-validated by a CA or TSP for up to 10 years after the signing event.

What is the difference between digital signatures and electronic signatures

- Electronic signatures, or e-signatures, refer broadly to any electronic process that indicates acceptance of an agreement or a record. The term digital signature is frequently used to refer to one specific type of electronic signature.
- Typical electronic signature solution use common electronic authentication methods to verify signer identity, such as email, corporate IDs, or a phone PIN. Multifactor authentication is used when increased security is needed. The best e-signature solutions demonstrate proof of signing using a secure process that includes an audit trail along with the final document.

- Digital signatures use a specific type of electronic signature. They use a certificate-based digital ID to authenticate signer identity and demonstrate proof of signing by binding each signature to the document with encryption — validation is done through trusted Certificate Authorities (CAs) or Trust Service Providers (TSPs).

- Signature types are linked with signature laws and regulatory requirements. Learn how they're used to help create legally binding electronic signaure processes.

SECTION 16 –POWER OF THE CENTRAL GOVERNMENT TO PRESCRIBE SECURITY PROCEDURES AND PRACTICES (AMENDED VIDE ITAA 2008)

- The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices.

  Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

  section 16 of the Information Technology act, 2000 (21 of 2000) the central government made the " Information Technology (security procedure)rules,2004, of which reffered above (rule 3 and 4)

Thank you