Digital Signature

According to the Information Technology Act, 2000, digital signatures mean authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3. Further, the IT Act, 2000 deals with digital signatures under Sections 2, 3, and 15.

Section 2(1)(p)

According to Section 2(1)(p), digital signature means '*authentication of any electronic record using an electronic method or procedure in accordance with the provisions of Section 3*'.

Further, authentication is a process for confirming the identity of a person or proving the integrity of information. Authenticating messages involves determining the source of the message and verifying that is has not been altered or modified in transit.

Section 3

Section 3 of the Information technology Act, 2000 provides certain provisions for the authentication of electronic records. The provisions are:

- Subject to the provisions of this section, any subscriber can affix his digital signature and hence authenticate an electronic record.
- An asymmetric crypto system and hash function envelop and transform the initial electronic record into another record which affects the authentication of the record.
- Also, any person in possession of the public key can verify the electronic record.
- Further, every subscriber has a private key and a public key which are unique to him and constitute a functioning key pair.

Secure Digital Signature (Section 15)

Let's say that two parties agree to apply a certain security procedure. If it is possible to verify that a digital signature affixed was

1. Unique to the subscriber affixing it.
2. Capable of identifying the subscriber.

and

1. Created in a manner under the exclusive control of the subscriber.
2. Also, it is linked to the electronic record in such a manner that a change in the record invalidates the digital signature

then

It is a secure digital signature.

Features

The three important features of digital signature are:

1. **Authentication** – They authenticate the source of messages. Since the ownership of a digital certificate is bound to a specific user, the signature shows that the user sent it.
2. **Integrity** – Sometimes, the sender and receiver of a message need an assurance that the message was not altered during transmission. A digital certificate provides this feature.
3. **Non-Repudiation** – A sender cannot deny sending a message which has a digital signature.

Electronic Signature

An electronic signature is described as any electronic symbol, process or sound that is associated with a record or contract where there is intention to sign the document by the party involved. The major feature of an electronic signature is thus the intention to sign the document or the contract. The other notable aspect that makes an electronic signature different from a digital signature is that an electronic signature can be verbal, a simple click of the box or any electronically signed authorization.

Difference between Digital and Electronic Signatures

BASIS FOR COMPARISON	DIGITAL SIGNATURE	ELECTRONIC SIGNATURE
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.
Authentication mechanism	Certificate-based digital ID	Verifies signers identity through email, phone PIN, etc.
Used for	Securing a document.	Verifying a document.
Validation	Performed by trusted certificate authorities or trust service providers.	No specific validation process.
Security	Highly secure	Vulnerable to tampering