

Chapter- 26

Digital Signature

Digital Signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of the document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

For digital signature a person has to obtain the digital signature certificate from the certifying authorities.

The person in whose name digital signature certificate is issued is known as subscriber.

The main uses of affixing of “Digital Signature” are:

- 1. To authenticate the identity of sender**
- 2. To authenticate the document sent**
- 3. Non Repudiation**

This means if an entity has signed some document then the entity can't deny the responsibility and liability arising out of the document later on.

Authentication of Electronic Record

The IT Act has provided the legal recognition to digital signature based on asymmetric crypto system. This system consists of key pair:

1. Private Key

2. Public Key

26.4 PRIVATE KEY VS. PUBLIC KEY			
	<i>Basis</i>	<i>Private key</i>	<i>Public key</i>
1.	Nature	Private key is secret i.e., known only to the owner or subscriber.	Public key is non-secret and is widely distributed to the public.
2.	Function	Private key is used by the subscriber to create the digital signature.	Public key is used by the relying party to verify the digital signature.
3.	Listing	Private key is not listed in the Digital Signature Certificate.	Public key is listed in the Digital Signature Certificate.

Process of creation and verification of digital signature

1. Sender prepares the message

The first step is that sender prepares the message/ document to be sent and attaches digital signature to it.

Example: Message prepared in the form of email and digital signature also applied to it.

2. Application of hash value/ message digest

Once the digital signature applied to the message/ document then a hash value/ message digest is created (hash value can be a numeric value, example 110010 etc)

3. Encryption of the message

Now the message/ document is encrypted (locked) by using the private key of sender. Now as the message it encrypted so, changes can't be done in it during the transit from sender to receiver. And sender sends the message to the receiver over the electronic medium.

4. Receiver decrypts the message

Once the message reaches the receiver, then receiver decrypts (unlock) the message by using the public key shared by sender with him.

5. Same Hash value/ message digest should be generated (as step 2)

When public key is entered then the same hash value/ message digest (as it was in step 2 of this process, example: 110010) should be generated. Which proves that the message was not tempered during the transit. If in case different hash value is generated then that means during the transit someone made changes to it.

6. Verification of digital signature

There is two way verification, which is done by applying digital signature to a document/ message:

1. If same hash value generates then that means document/ message was not tempered/changed in transit.
2. And once the hash value matches then the identity of the sender can be confirmed by seeing his digital signature attached to the document/ message.

Electronic Signature (e-signature)

Electronic signature means authentication of any electronic record by the subscriber, by electronic means.

For example:

- OTP sent on registered mobile number,
- Doing signature on device shared by courier boy to deliver online orders
- Entering username and password to open gmail, fb, twitter etc.
- Digital signature

E-signature is a broader term and digital signature is a part of it.

The central government has the power to add or to omit or to make any changes relating to the procedure of any e-signature or electronic authentication technique.

Difference between Digital Signature and E-Signature

Digital Signature	E-Signature
Definition	Definition
Highly secured	More vulnerable to tempering
Certificate based digital ID	Verifies signers identity through passwords, OTP etc.
A digital signature is one of the types of e-signature	This is a broader concept. Includes OTP, passwords, digital signature etc.
It's acceptable globally because it comply with international standards for security	These are not regulated as digital signatures