DIGITAL SIGNATURE

- ---

- Ms. Aakriti saini
- Ms. Minny Narang

JOURNEY OF SIGNATURES UNDER THE IT ACT SO FAR

Signatures authorised under IT act are equivalent of handwritten signatures. Journey of signatures can be divided into three phases :

Phase I: Digital signatures (year 2000 onwards)

Phase II: Electronic signatures (year 2000 onwards)

Phase III: E-sign online signature service or E- hastakshar (sept 2016 onwards)

PHASE 1 : DIGITAL SIGNATURES

Authentication of electronic records (Sec. 3)

1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation-For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input .

CREATION OF DIGITAL SIGNATURES (RULE 4)

The sender prepares the message to be sent on the computer including his name

The sender applies hash function on the message to encrypt it using addressee's public key which gives hash result also known as message digest

The sender encrypts the message digest with his own private key. The outcome of this encryption is accepted as digital signature.

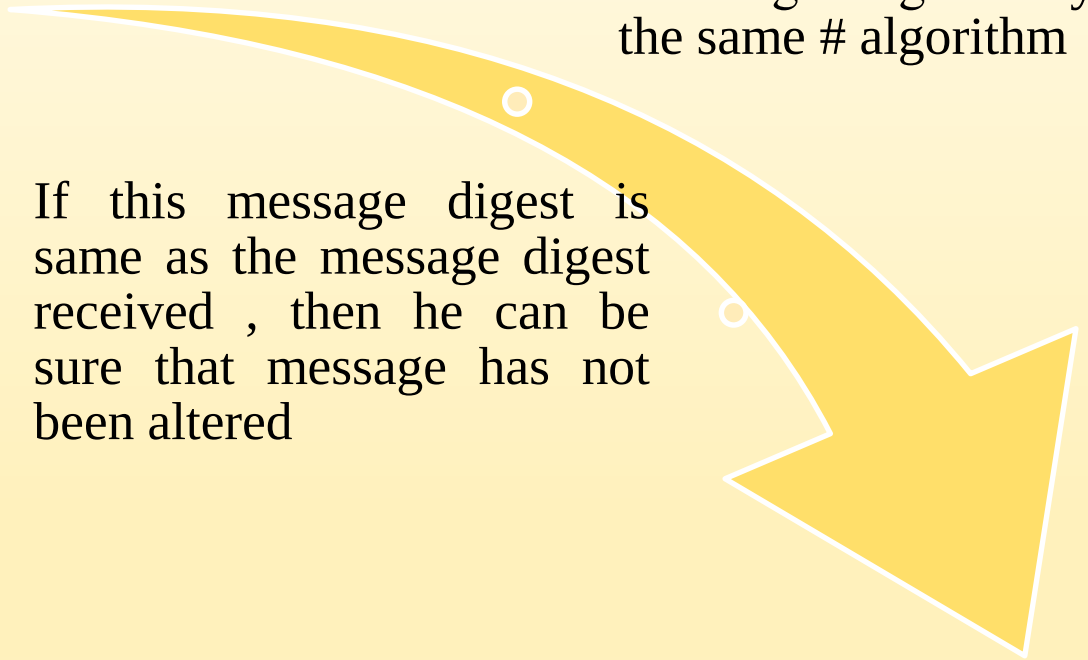
The sender attaches his digital signature to the message and sends it electronically to recipient

VERIFICATION OF DIGITAL SIGNATURES (RULE 5)

The receiver uses sender's public key to verify sender's Digital signature

The recipient also creates "message digest" by using the same # algorithm

If this message digest is same as the message digest received , then he can be sure that message has not been altered



The recipient can read the message by decrypting it with his "private key "

DIFFERENCES

BASIS	ENCRYPTION	DECRYPTION
Message	By public key of addressee	By private key of addressee
Digital signature	By private key of the sender	By public key of the sender
BASIS	**PRIVATE KEY**	**PUBLIC KEY**
Function	It is used to create Digital signatures	It is used to verify Digital signatures
Nature	Private key is confidential	It is widely known
listing	It is not listed in the digital signature certificate issued by CA	It is listed in the digital signature certificate issued by CA

PHASE 2 : ELECTRONIC SIGNATURES

- 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 technique which--

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

- 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.

- 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

- W.e.f 28th January, 2015 e – authentication using Aadhar e- KYC services was allowed by its insertion in the second schedule. It was further amended in 2019 in the light of supreme court judgment to allow for e – authentication technique using e- KYC services other than Aadhar e -KYC

PHASE 3 : E-sign online signature service or E-hastakshar (sept 2016 onwards)

- E-sign or E-hastakshar service was launched by the GOI on 3rd September, 2016.it also uses asymmetric crypto system. It enables instant signing of documents by the citizen of India in a legally acceptable form.
- **Elements of E- hastakshar system**

1. **ASP :** Application service provider which includes government agencies, banks, FI , educational institutions.
2. **ESP**: e- sign service provider. Presently CAs authorised under IT act by CCA (Controller of certifying authority). The ESP facilitates creation of the signature for the documents. Ann agreement needs to be executed between ASP and ESP.
3. E- KYC service provider or Aadhar e- KYC services.
4. User of E-sign (or applicant)

ELEMENTS IN E-HASTAKSHAR SYSTEM

DIFFERENCES

BASIS	DIGITAL SIGNATURE	ELECTRONIC SIGNATURE
Scope	A digital signature is an electronic signature . They are the subset of electronic signature.	It is broader in scope
Genesis	It uses asymmetric crypto system.	it uses electronic technique specified in the second schedule of the act.
Technology	It is technology specific . It is based on cryptography codes	It is technology neutral. It uses different technologies like PIN used for ATM.
security	It is more secure	It is less secure in comparison to digital signatures

BASIS	DIGITAL SIGNATURE	E- SIGN/ E- HASTAKSHAR
When introduced	Introduced by IT act since its inception.	Inserted in 2015 and launched in sept 2016
Validity	Valid for a particular period may be a year or two	One time use only
Elements in the mechanism	CCA, CA and subscriber or end user.	ASP, ESP, E- KYC service provider or Aadhar e- KYC services and end user.
Certifying authorities offering these services	Safescrypt, IDRBT, (n) code solutions, e Mudhra, capricorn	(n) code solutions, e Mudhra, CDAC, capricorn , NSDL e-gov
Hardware involved and its safe custody	Crypto token is given to the end user by CA and the user has to keep it safe during its validity period	No hardware is given by CA. based on authentication received from e-KYC service, the key pairs are used only once and the private key is deleted after one time use.