DIGITAL SIGNATURE

PHYSICAL SIGNATURES AND SIGNATURES UNDER THE IT ACT, 2000

Signatures authorized under the IT Act, 2000 are treated at par with physical or manual signatures. In other words, signatures authorized by the IT Act are equivalent of handwritten signatures.

The IT Act has provided the rules for the process of authentication through signature and also created trusted third party mechanism in the form of Certifying Authority (CA) via Controller of Certifying Authority (CCA) for issuing such signatures to end users.

JOURNEY OF SIGNATURES UNDER THE IT ACT SO FAR

Journey of Signatures under the IT Act so far can be divided into three phases:
Phase I: Digital Signatures (year 2000 onwards)
Phase II: Electronic Signatures (year 2008 onwards)
Phase III: E-sign online signature service or E-hastakshar (Sept. 2016 onwards)

The divison into various phases is done only for the sake of clarity. Otherwise digital signature certificate system under Phase I continues to exist along with E-sign online signature service Phase III.

PHASE I: DIGITAL SIGNATURES (YEAR 2000 ONWARDS)

The IT Act, 2000 introduced the concept of digital signatures under Sec. 2(1)(p) as authentication of any electronic record by a subscriber, i.e., a person in whose name the Digital Signature Certificate' (DSC) is issued,by means of an electronic method or procedure in accordance with the provisions of Sec. 3.

Authentication of Electronic Records (Sec. 3)

(i) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
(ii) 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:

"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 and Verification of Digital Signatures
Creation of Digital Signatures (Rule 4)
(a) The sender prepares the message to be sent including his name on a computer.
(b) The sender applies a 'hash function' on the message to encrypt it using addressee's public key which gives out a hash result. The 'hash result' is also called the 'message digest.
(c) The sender encrypts this 'message digest' further using his own 'private key'. The outcome of this encryption is accepted as the digital signature of the sender. In other words, the digital signature consists of this 'encrypted message digest'. **This signature is unique to the message and will be different for each new message.**
(d) The sender attaches his digital signature to the message.
(e) The sender sends the digital signature and the encrypted message to the recipient electronically.

Verification of Digital Signatures (Rule 5)
(a) The recipient uses the sender's 'public key' to verify the sender's digital signature. Verification proves that the message is authentic, unaltered and sent by the sender only.
(b) The recipient also creates a 'message digest' of the message, using the same secure hash algorithm. If this 'message digest' is the same as the 'message digest" received from the sender, the receiver can be sure that no alteration has been made in the original message. The recipient can read the message by decrypting it with his 'private key'.

Digital signature cannot be copied, tempered or altered. Digital signature will ensure that original content is intact and not changed. Digital signature provides proof of **signer's identity, data integrity and non-repudiation** (i.e., sent by the sender only) of signed document.

Encryption and Decryption

Basis	Encryption	Decryption
Message	By public key of addressee (which is in sender's hands)	By private key of addressee (which is in his own hands)
Digital Signature	By private key of the Sender (which is in his own hands)	By public key of sender (which is in addressee's hands)

Table: Distinction between Private Key and Public Key

Basis	Private Key	Public Key
1. Function	Private key is the key of the key pair used to create digital signatures [Sec. 2(1)(zc)].	Public key is the key of the pair used to verify digital signatures [Sec. 2(1)(zd)].
2. Nature	Private key is confidential, i.e., it is not shared by the subscriber with any other person	Public key is widely known
3. Listing	Private key is not listed in the digital signature certificate issued to the subscriber by a Certifying Authority.	Public key is listed in the digital signature certificate issued to the subscriber by a Certifying Authority

PHASE II: ELECTRONIC SIGNATURES (YEAR 2008 ONWARDS)

The IT Act, 2000 (vide Amendment Act, 2008) introduced the concept of Electronic Signatures by insertion of Sec. 2(1)(ta) and Sec. 3A. As per Sec. 2(1)(ta):
"Electronic Signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule of the Act and includes digital signature.
As per Sec. 3A, 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. With effect from 28th January, 2015, e authentication technique using Aadhar e-KYC (Know Your Customer) services was allowed to be used by its insertion in the Second Schedule. Second Schedule is further amended w.e.f. 1/3/2019 and has inserted e-authentication technique using e-KYC services other than Aadhar e-KYC also in the light of Supreme Court verdict. The term 'digital signature' and 'electronic signature' are not interchangeable terms. There are vast differences between the two.
Sec. 2(1)(p) of the Information Technology Act, 2000 gives the legal definition of the term Digital Signature whereas Sec. 2(1)(ta) of the Information Technology Act, 2000 gives the legal definition of the term Electronic Signature.

The term Digital Signature has been there in the Information Technology Act, 2000 since inception whereas the term Electronic Signature was inserted in the Information Technology Act, 2000 by the Information Technology (Amendment) Act, 2008.

Sec. 2(1)(p) of the Information Technology Act, 2000 defines the term "Digital Signature" as authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Sec. 3 whereas Sec. 2(1)(ta) (as inserted by IT Amendment Act. 2008) of the Information Technology Act, 2000 defines the term "Electronic Signature" to mean authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.
A digital signature is a "secure" electronic signature, but an electronic signature is not necessarily a digital signature.

Table: Difference between Digital Signature and Electronic Signature

Basis	Digital Signature	Electronic Signature
1.Scope	A digital signature is an electronic signature. Digital signatures are actually a sub-set of electronic signatures because they are also in electronic form.	The term electronic signature is broader than digital signatures.
2.Genesis	It uses asymmetric crypto system (key pair)	It uses electronic technique specified in the Second Schedule and includes digital signature.
3.Technology	It is technology-specific (public key cryptography). It is based on cryptography codes.	It is 'Technology neutral'. It may be created by different technologies e.g. secret code or PIN used with ATM, retinal scan etc.
4. Security	Due to the technology used, digital signature offers more security.	It is less secure as compared to digital signature when it adopts methods other than digital signature.

PHASE III: E-SIGN ONLINE SERVICE OR E-HASTAKSHAR (SEPT. 2016 ONWARDS)

The IT Act, 2000 in year 2015 introduced E-authentication technique by insertion in Schedule II. E-sign or E-hastakshar service was launched by the Government of India on 3rd Sept., 2016. It is to be noted that it also uses asymmetric crypto system only. E-sign service enables instant

signing of documents online by a citizen of India in a legally acceptable form. This service enables a person to electronically sign a form or document anytime and anywhere.

When the term 'Electronic Signatures' was inserted in the IT Act by Amendment in 2008 via adding Sec. 2(1)(ta) it was construed to be called digital signature when asymmetric crypto system is used and simply electronic signature when symmetric crypto system is used. Though the insertion of E-authentication technique through Schedule II uses the term E-sign (Electronic Signature) or E-hastakshar by using E-authentication technique using e-KYC services or Aadhar e-KYC services yet it uses asymmetric crypto system only.

Elements in E-hastakshar System

1. ASP, i.e., Application Service Provider. ASPS include government agencies, banks, financial institutions, educational institutions, etc.

2. ESP, i.e., e-Sign Service Provider. Presently Certifying Authority (CA) as authorized under the IT Act by Controller of Certifying Authority (CCA). Five agencies have been recognised so far for this purpose.The e-Sign Service Provider facilitates creation of signature of the user for the document which will be applied to the document on acceptance by the user. An 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)

Table : Examples where e-sign Online Service is Used

Digital Locker	Self attestation
Tax	Application for Tax ID, e-filing
Financial Sector	Application for account opening in banks and post office
Passport	Application for issuance, reissue
Educational	Application forms for course enrolment and exams
Transport Department	Application for driving licence renewal, vehicle registration

Source: cca.gov.in

It is Important to understand the difference between digital signature as explained in Phase I and E-sign or E-hastakshar Phase III. It again needs to be emphasied that both these systems (i.e.,

Phase I and Phase III) use asymmetric crypto technique yet there are significant differences between the two as outlined in following table.

Table: Difference between Digital Signature and E-sign or E-hastakshar

Basis	Digital Signature	E-sign/E-hastakshar
1. When introduced	Introduced by IT Act, 2000 since inception.	Inserted in 2015 and launched in Sept. 2016.
2. Validity	Valid for a particular period may be a year or two.	One time use only.
3. Elements in the Mechanism	CCA, CA and subscriber or end user	ASP,ESP (CA),e-KYC service provider or Aadhar e-KYC services and end user or signatory.
4. Certifying Authorities offering these services	Safescrypt, IDRBT, (n)Code Solutions, e Mudhra, Capricorn.	(n)Code Solutions, e Mudhra, CDAC, Capricorn, NSDL
5. Hardware involved and its safe custody	Crypto token is given to end user by CA and safe custody of it during its validity period is end user's obligation.	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.

DIGITAL SIGNATURE (END ENTITY RULES) 2015

Digital signature (end entity rules) 2015 provide for 'xml digital signature'. xml stands for Extensible Markup Language. 'xml digital signature' means the digital signature on xml electronic record. These rules provide for time stamp notation also that indicates the correct date and time of an action and identity of the person or device that sent or received electronic record.