Unit 1: Digital and Electronic Signature: Concept and Procedure

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of Public and Private key
- Digital and Electronic signature
- Legal provisions with regard to digital and electronic signature

1.2 INTRODUCTION

Digital signature and electronic signature are used interchangeably but they are not the same. Digital signature is a mere subset of e-signature. Digital signatures are based on asymmetry, or public key, cryptography and are capable of fulfilling the demand of burgeoning e-commerce by not only providing message authentication, integrity and non-repudiation function but also making it highly scalable. Digital Signatures are basically ***'enciphered data'*** created using cryptographic algorithms. It is not a digitalized image of a handwritten signature. Digital signatures are an actual transformation of an electronic message using public key cryptography. It requires a key pair (private key for encryption and public key for decryption) and a hash function (algorithm).[66]

On the other hand, an electronic signature includes all types of electronically approved methods. It could be a graphical stamp, a process or even pressing the 'Agree' button in the terms and conditions etc. It includes simple forms like pressing ***'place order'*** to complex forms like a biometric signature.

1.3 CONCEPT OF PUBLIC AND PRIVATE KEY

Before digitally signing an electronic communication, the sender has to create a public-private key pair. There are two keys used for digital signatures i.e., Private key and Public key.[67] The private key is kept confidential by the signer and used by him only to create the digital signature whereas the public key is more widely known and is used to verify the digital signature by the relying party.

1.4 IMPORTANT TERMS RELATED TO DIGITAL SIGNATURE

"Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature. (Section 2(1) (d) of IT Act, 2000)[68]

[66] The control implications of a public key infrastructure <https://repository.up.ac.za/dspace/bitstream/handle/2263/4067/Bouwer_Control(1999).pdf?sequence=1&isAllowed=y>

[67] Adams, C, [1999] "Understanding Public-key Infrastructure", Macmillan Technical Publishing

[68] Certifying Authorities - Digital Signature Certificates <http://www.digitalsignaturesale.com/certifying-authorities/>

"Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature. (Section 2(1) (f) of IT Act, 2000)

"Certifying Authority" means a person who has been granted a license to issue an electronic signature certificate under Section 24. (Section 2(1) (g) of the IT Act, 2000)

"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3. (Section 2(1) (p) of the IT Act, 2000)

"Electronic Signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature. (Section 2(1) (ta) of the IT Act, 2000)[69]

"Electronic Signature Certificate" means an Electronic Signature Certificate issued under Section 35 and includes Digital Signature Certificate. (Section 2(1) (tb) of the IT Act, 2000)

"Key Pair" is an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key. (Section 2(1) (x) of the IT Act, 2000)

"Private Key" means the key of a key pair used to create a digital signature. (Section 2(1) (zc) of the IT Act, 2000)

"Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate. (Section 2(1) (zd) of the IT Act, 2000)

1.5 CREATION AND VERIFICATION OF A DIGITAL SIGNATURE

A digital signature is a two-way process, involving two parties, the signer (creator of the digital signature) and the recipient (verifier of the signature). A digital signature is complete, if and only if, the recipient successfully verifies it.[70]

[69] ICAI members use electronic signature for signing audit <https://taxguru.in/chartered-accountant/icai-members-may-use-electronic-signature-signing-audit-reports.html>

- ***Creation of a digital signature***

- The signer demarcates what is to be signed. The delimited information to be signed is termed as the 'message'.
- A hash function[71] in the signer's software computes a hash result (digital fingerprint) unique to the message.
- The signer's software then transforms (encrypts) the hash result into a digital signature using the signer's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.
- The digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. Since a digital signature is unique to its message, it is useful if it maintains a reliable association with its message.

- ***Verification of a digital signature***

Recipient:

- Receives digital signature and the message
- Applies signer's public key on the digital signature
- Recovers the hash result of the original message by means of the same hash function used by the signer to create the digital signature
- Computes a new hash result of the original message by means of the same hash function used by the signer to create the digital signature
- Compares the hash results recovered[72]

If the hash result computed by the verifier is identical to that of the hash result extracted from the digital signature during the verification process, it indicates that the message remained unaltered and vice versa.

Verification is a two-prong process i.e.,

---

[70] American Bar Association Digital Signature Guidelines <https://horseproject.wiki/index.php/American_Bar_Association_Digital_Signature_Guidelines>

[71] A 'hash result' is used in both creating and verifying a digital signature. It is an algorithm which creates a digital representation or fingerprint in the form of a hash value or hash result of a standard length which is usually much smaller than the message

[72] Top Compelling Reasons Fedena Blog <https://fedena.com/blog/2019/06/top-compelling-reasons-why-your-school-website-must-have-an-ssl-certificate.html>

- to verify whether the signer's private key was used to digitally sign the message and
- to verify whether the newly computed hash result matches the original hash result which was recovered from the digital signature during the verification process.

1.6 DIGITAL SIGNATURE AND PUBLIC KEY INFRASTRUCTURE

The digital signature regime operates online without any human intervention. The Sender sends a digitally signed message and the recipient receives and verifies it. The requirement is that both the sender and the receiver must have the digital signature software at their respective ends. This paves way for the participation of a ***Trusted Third-party (TTP)*** to certify the subscriber's identity and their relationship to their public keys. The Trusted Third Party is referred to as a Certifying Authority (CA). The main function of the certifying authority is to verify and authenticate the identity of the subscriber i.e., a person in whose name the digital signature certificate is issued.[73]

A Digital Signature Certificate securely binds the identity of the subscriber. It contains the name of the subscriber, his public key information, name of the certifying authority who issued the certificate, its public key information and the validity of the certificate. These certificates are stored in an online publicly accessible repository maintained by the Controller of certifying authorities or in the repository maintained by the certifying authority. Every Certifying Authority must maintain a repository[74] for the certificates as per the Certification Practice Statement (CPS).

Under the Information Technology Act, 2000, *Section 35 to 40* lay down the procedure for issuance, rejection, suspension and revocation of digital signature certificates. They provide that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs.25,000. The fee shall be prescribed by the Central Government and different fees may be prescribed for different classes of applicants. Furthermore, no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

[73] Tarek A El-Mageed, Nariman A El-Salam, [2004] "Public Key Cryptosystems and its Applications in Digital Signature" The 2nd International Conference on Informatics and System INFOS2004, Cairo-Egypt

[74] A repository maintains an up-to-date list of all the valid digital signature certificates, and also a list of suspended or revoked certificates

Digital signatures fulfil all statutory requirements associated with the acceptance of handwritten signatures. The law does not recognize the digital signature in a stand-alone environment. It gives recognition to the whole system – the public key infrastructure including the standards, which create and verify digital signatures. Digital signature establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the signer of an electronic message and also confirms that the said signer approved the content of an electronic message.[75]

1.7 PROCESS OF PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure is about the management and regulation of key pairs by allocating duties between contracting parties (certifying authorities/subscribers) laying down the licensing and business norms for certifying authorities and establishing business processes to construct contractual relationships in a digitalized world. The process is as follows:-

- Subscriber applies to Certifying Authority for Digital Signature Certificate.
- The Certifying Authority verifies the identity of the subscriber and issues the digital signature certificate.
- The Certifying Authority forwards the digital signature certificate to the repository maintained by the controller.
- Subscriber digitally signs an electronic message with the private key to ensure sender authenticity, message integrity, and non-repudiation and sends it to the relying party.
- The relying party receives the message, verifies the digital signature with the subscriber's public key and goes to the repository to check the status and validity of the subscriber's certificate.
- Repository does the status check on the subscriber's certificate and reverts back to the relying party.

Under the IT Act, Sections 17 to 34 provide a system for regulation of certifying authorities, to exercise supervision over the activities of certifying authorities and also lay down principles and conditions regulating the certifying authorities.

[75] CH Magazine | VARIOUS AUTHORITIES UNDER THE IT ACT <https://www.chmag.in/articles/legalgyan/various-authorities-under-the-it-act/>

1.8 DIFFERENCE BETWEEN ELECTRONIC AND DIGITAL SIGNATURE

CRITERIA	ELECTRONIC SIGNATURE	DIGITAL SIGNATURE
Definition	**It is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can 'sign' an electronic record.**[76]	**It is a term for one technology-specific type of electronic signature.**
Technology	**They can take many forms and can be created by many different technologies. It permits a broad range of 'electronic signatures' to satisfy the requirements of a legal signature.**	**It involves the use of public-key cryptography (asymmetric cryptography) to 'sign' a message.**
Example	**A name typed at the end of an email message by the sender, PIN used in ATM cards to identify the sender to the recipient etc.**	**It is a block of data at the end of an electronic message that attests to the authenticity of the said message. Digital Signatures are a transformation of an electronic message using public-key cryptography.**

[76] Legal Recognition to Electronic records in India <https://scholarticles.wordpress.com/2015/08/27/legal-recognition-to-electronic-records-in-india/>

1.9 LEGAL PROVISIONS RELATED TO DIGITAL AND ELECTRONIC SIGNATURE

The Information Technology Act, 2000 provides a legal framework to authenticate electronic records. The Act facilitates and safeguards electronic transactions in the electronic medium. It is based on UNCITRAL's Model Law on E-commerce, which adopts 'functional equivalent approach' advocating a shift from a paper-based environment to computer-based.[77]

- ***Section 3*** gives legal recognition to electronic records and digital signatures. ***Section 3A*** was inserted by the IT (Amendment) Act, 2008 which in turn allowed electronic signatures to be used for authentication of e-records. Section 3 provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The authentication of the electronic record shall be effected by the use of the asymmetric cryptosystem and hash function which envelops and transform the initial electronic record into another electronic record.
- ***Section 5*** provides for legal recognition of electronic signature. It states, where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.
- ***Section 6*** deals with the use of Electronic Records and Electronic Signature in the context of Government and its agencies.
- ***Section 14*** deals with secure electronic records. It states that, where any security procedure has been applied to an electronic record at a specific point of time, such record shall be deemed to be a secure electronic record from such point of time to the time of verification.
- ***Section 15*** provides for situations when an Electronic Signature can be considered as secure.

[77] Digital Signature | Ministry of Electronics <https://meity.gov.in/content/digital-signature>

- ***Section 16*** provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability, and cost of alternative procedures, the volume of similar transactions entered into by other parties etc.

1.10 ADOPTION OF SECURITY PROCEDURES AND THE IT ACT, 2000

The main purpose of the IT Act, 2000 is to secure electronic records ***(Section 14)*** and secure electronic records ***(Section 15)*** by applying appropriate security procedures.

Section 14 advocates application of any security procedure to make the electronic record secure. A secured electronic record shall be deemed to be a secured electronic record from the time the said security procedure is applied to the time of its verification. It is important to note that the onus of securing an electronic record rests with the creator of the said record. The presumption is that an electronic record is a secured one from the specific point of time when any security procedure has been applied to it to the time of its verification at the recipient's end, till the recipient proves it otherwise.

Section 15 lays down the security features for a subscriber-specific electronic signature, which includes digital signature as well. It provides for 2 specific features:-

- Signature creation data under the exclusive control of signatory or linked to the signatory (the authenticator) and to no other person and
- Storage and affixation of signature creation data as per prescribed processes.[78]

Section 16 of the act enunciates about security procedure. It is proactive in nature as it gives liberty to the Central Government to adopt and assimilate any technology for providing a regime of secure electronic record and electronic signature. This section puts an onus on the Central

[78] Afrianto, Irawan & Heryandi, Andri & Finandhita, Alif & Atin, Sufa. (2019). E-Document Autentification With Digital Signature For Smart City : Reference Model

Government to prescribe the security procedure is having regard to commercial circumstances, nature of transaction and other related factors as it may consider appropriate before adopting such security procedures and practices.[79] The lawmakers have made the Act flexible in terms of technology adoption and assimilation, which would further influence both e-commerce and e-governance transactions. The digital payments ecosystem in India has already been revolutionized without even taking cognizance of *Sections 14-16 of the Act.* There are Rules and Regulations pertaining to and for the purpose of regulating the functioning of Certifying Authorities. It lays down procedure and standards (rule 3-8) for securing electronic records and digital signatures. Under ***Rule 3 of the Information Technology (Security Procedure) Rules, 2004*** an electronic record shall be deemed to be a secure electronic record for the purpose of the act if it has been authenticated by means of a secure electronic signature.[80]

1.11 LET'S SUM UP

In this chapter, we have studied the concept of public and private key along with the important terms with respect to digital signature. We also saw how a digital signature is created and verified and the difference between digital and electronic signature. Finally, we have ended our discussion with legal provisions pertaining to digital and electronic signature and adoption of security procedures with respect to it.

1.12 FURTHER READING

- https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf
- http://www.ijhssnet.com/journals/Vol_6_No_12_December_2016/7.pdf
- http://www.ijarcs.info/index.php/Ijarcs/article/viewFile/2484/2472

[79] Stamp, M [2011] "Information Security: Principles and Practice" Second Edition, John Wiley and Sons
[80] Banerjee, Arindam (2016) The Impact of Electronic Signatures on Internal Control Systems

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is a digital signature?

Digital signatures are based on asymmetry, or public key, cryptography and are basically *'enciphered data'* created using cryptographic algorithms, and are actual transformations of electronic messages using public-key cryptography.

2. What are the differences between an electronic signature and digital signature?

Electronic signature is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can 'sign' an electronic record while a digital signature is a term for one technology-specific type of electronic signature while, digital signatures involve the use of public-key cryptography (asymmetric cryptography) to 'sign' a message.

3. Mention some legal provisions related to the digital and electronic signature?

Some of the legal provisions related to the digital and electronic signature are as follows:

- Section 3 of the Information Technology Act, 2000 which gives legal recognition to electronic records and digital signatures
- Section 5 of the Information Technology Act, 2000 which provides for legal recognition of electronic signature.
- Section 6 of the Information Technology Act, 2000 which deals with the use of Electronic Records and Electronic Signature in the context of Government and its agencies.
- Section 16 of the Information Technology Act, 2000 which provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures.

4. What is public key infrastructure?

Public Key Infrastructure is about the management and regulation of key pairs by allocating duties between contracting parties (certifying authorities/subscribers) laying down the licensing and business norms for certifying authorities and establishing business processes to construct contractual relationships in a digitalized world.

5. How is a digital signature verified?

The verification of a digital signature involves the following steps:

i. Verifying whether the signer's private key was used to digitally sign the message; and
ii. Verifying whether the newly computed hash result matches the original hash result which was recovered from the digital signature during the verification process.

1.14 ACTIVITY

Describe the legal provisions pertaining to digital and electronic signature along with the security procedures in I.T. Act, 2000. (800 words)