CHAPTER 7

Unit IV

Digital Signature, Certifying Authorities and E-Governance

Syllabus Topic : Digital Signatures

7.1 Digital Signatures

Q.7.1.1 What is digital signature? What are the functions of digital signature? (Ref. Sec. 7.1) **(5 Marks)**

Q.7.1.2 Explain the cryptosystem and hash function. (Ref. Sec. 7.1) **(5 Marks)**

Q.7.1.3 Write short note on digital signature. (Ref. Sec. 7.1) **(5 Marks)**

- A digital signature is an electronic method for illustrating the authenticity of a digital message or record. A substantial digital signature gives the recipient motivation to trust that the message was made by a known sender and that it was not changed in transit.
- Digital signatures are regularly utilized for software conveyance, money related exchanges, and in different situations where it is imperative to recognize impersonation or altering.
- Following are the functions of digital signature :
  1. To authenticate the document.
  2. To identify the document.
  3. Securing the document from forgery.
  4. To make the contents of the document binding on person putting digital signature.
  5. Evidence for identification of document.
- Digital signatures are used in e-commerce and by e-governance for the purpose of authentication. Digital signature in IT Act, 2000 means authentication of electronic record. Section 3 of IT Act, 2000, describes authentication of electronic records as follows:

Authentication of electronic records

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 of electronic record

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 making it computationally infeasible.

(a) To derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) That two electronic records can produce the same hash result using the algorithm.

1. Any person by the use of a public key of the subscriber can verify the electronic record.
2. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

There are many digital signature system are available. Asymmetric crypto system and hash function are recognized by the IT Act for authentication of electronic records.

Asymmetric cryptosystem

- Asymmetric cryptosystem is also known as public key cryptography or ciphers. In this cryptosystem two keys are used named public key and private keys.
- Public key is used to encrypt the data and private key is used to decrypt the data. The keys are made up of large numbers and are paired together but these 2 keys are not identical.
- The private key is kept secret while the public key is chat with everyone. Private key is used to create the digital signature and public key is used to verify the digital signature as given in IT act 2000.
- It is important to secure the private key, to secure the private key store it in floppy or card or CD (Compact Disc) or pen drive. Do not store the private key on hard disk as it is not considered a safe practice.

Hash functions

- The hash functions are used to check the integrity of the data which is send across the internet. Hash function takes a message of any length as input, and gives fixed length output. The examples of hash algorithms are MD5 and SHA.
- Hash function is a mathematical function that maps the arbitrary size data to fixed length string. It is used to check the integrity of the data that data is not altered.
- To validate the integrity, a hash of information is created. When data is send at that time its hash is computed, at the receivers side when data is received then hash of received data is computed then both the hash values are compared if the hash value matches then there will be no change in data else data is changed.
- The process of creating the digital signature and verification is given in Rules 4 and 5 of IT Rules, 2000 as follows :

"Rule 4 : Creation of digital signature"

To sign an electronic record or any other item of information, the signer shall first apply the hash function in the signer's software; the hash function shall compute a hash result of standard length which is unique (for all practical purposes) to the electronic record; the signer's software transforming the hash result into a digital signature using signer's private key; the resulting digital signature shall be unique to both electronic record and private key used to create it; and the digital signature shall be attached to its electronic record and stored or transmitted with its electronic record.

" Rule 5 : Verification of digital signature"

The verification of a digital signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a digital signature and by using the public key and the new hash result, the verifier shall check :

(i) If the digital signature was created using the corresponding private key; and

(ii) If the newly computed hash result matches the original result which was transformed into digital signature during the signing process. The verification software will confirm the digital signature as verified if :

(a) The signer's private key was used to digitally sign the electronic record, which is

known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a digital signature created with the signer's private key; and

(b) The electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

Syllabus Topic : Digital Signature Certificate

7.2 Digital Signature Certificate

Q. 7.2.1 Explain digital signature certificate. (Ref. Sec. 7.2) **(5 Marks)**

- Digital signature certificates are the digital equivalent of physical signature. This certificate is used to prove the identity, to access data and internet services. Digital signature certificate ensures that there is no alteration in data and authenticates the electronic document.
- Digital certificates are issued by the certifying authorities who are having the license of issuing the digital signature.
- In IT Act, 2000, in chapter 7 digital signature certificate related information is given and in IT rules, 2000 digital signature certificates authorities' rules are given.
- The Digital signature certificate form is issued by the certificate authorities along with the fees up to 25000 rupees. There may be different fees for different classes.
- Certification of the practice statement should be submitted along with digital signature certificate form. Digital signature practice statement is defined in IT Act, 2000. It is necessary for the applicant to state in certificate of practice statement the practices he wants to employ in using digital signatures.
- When the digital signature authority receives the application they do the enquiry and if they satisfy then they issue the digital signature certificate.
- Applicant receives the digital signature certificate along with a key pair that private and public key. The applicant hold the private key for creating digital signature and the public key is used to verify the digital signature.
- Before issuing the digital signature certificate the certifying authority should check that (IT Act, 2000,Rule 25 of certify authorities rules).

1. The user name is should not appear as a compromised users in its list.

2. Comply with the procedure as defined in his certification practice statement including verification of identification and/or employment;
3. Comply with all privacy requirements;
4. Obtain consent of the person requesting the digital signature certificate, that the details of such digital signature certificate can be published on a directory service.

- The Subsection (1) of Section 41 of IT Act, 2000 mention that a subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a digital signature certificate.

(a) To one or more persons;

(b) In a repository, or otherwise demonstrates his approval of the digital signature certificate in any manner.

- The Subsection (2) of Section 41 of IT Act, 2000 mention that by accepting a digital signature certificate the subscriber certifies to all who reasonably rely on the information contained in the digital signature certificate that :

(a) The subscriber holds the private key corresponding to the public key listed in the digital signature certificate and is entitled to hold the same;

(b) All representations made by the subscriber to the certifying authority and all material relevant to the information contained in the digital signature certificate are true;

(c) All information in the digital signature certificate that is within the knowledge of the subscriber is true.

Suspension of digital signature certificate (The Subsection (1) of Section 37 of IT Act, 2000)

- The certifying authorities can suspend the digital signature certificate in one of the following situations :

(a) On receipt of a request to that effect from

(i) The subscriber listed in the digital signature certificate; or

(ii) Any person duly authorized to act on behalf of that subscriber,

(b) If it is of opinion that the digital signature certificate should be suspended in public interest.

- A digital signature certificate shall not be suspended for a period exceeding 15 days unless the subscriber has been given a chance of being heard in the matter.

- On suspension of a digital signature certificate, the certifying authority shall communicate the same to the subscriber.

☞ **Revocation of Digital Signature Certificate (The Subsection (1)(2)(3) of Section 38 of IT Act, 2000)**

- The certifying authority can revoke the digital certificate in following situations:
  (a) Where the subscriber or any other person authorized by him makes a request to that effect; or
  (b) Upon the death of the subscriber, or
  (c) Upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.
- Without prejudice to aforesaid certifying authority may revoke a digital signature certificate which has been issued by it at any time, if it is of opinion that
  (a) A material fact represented in the digital signature certificate is false or has been concealed;
  (b) A requirement for issuance of the digital signature certificate was not satisfied;
  (c) The certifying authority's private key or security system was compromised in a manner materially affecting the digital signature certificate's reliability;
  (d) The subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

Syllabus Topic : Certifying Authorities and Liability in the Event of Digital Signature Compromise

7.3. Certifying Authorities and Liability in the Event of Digital Signature Compromise

Q. 7.3.1 Explain certifying authorities and their liability in the event of digital signature compromise. (Ref. Sec. 7.3) **(5 Marks)**

- The role of certifying authority is very important in digital signature environment. certifying authority.
  1. Issues the digital signature certificates.
  2. Manage the functioning of digital signature.
  3. Provides evidence of proof in legal dispute.

- For the regulation purpose of the certifying authorities the central government has appointed a controller of certifying authorities.
- They may appoint deputy controllers and assistant controllers as per requirement. The deputy controllers and assistant controllers performs the functions given by controller of certifying authorities.
- The Central Government decides the head office and the branch office of the controller to be located.
- As given in Section 18 of IT Act, 2000, the functions of the controller of certifying authorities are as follows:

(a) Exercising supervision over the activities of the certifying authorities;

(b) Certifying public keys of the certifying authorities;

(c) Laying down the standards to be maintained by the certifying authorities;

(d) Specifying the qualifications and experience which employees of the certifying authority should possess;

(e) Specifying the conditions subject to which the certifying authorities shall conduct their business;

(f) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a [Electronic Signature] certificate and the public key;

(g) Specifying the form and content of a 27 [Electronic Signature] certificate and the key;

(h) Specifying the form and manner in which accounts shall be maintained by the certifying authorities;

(i) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) Facilitating the establishment of any electronic system by a certifying authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) Specifying the manner in which the certifying authorities shall conduct their dealings with the subscribers;

(l) Resolving any conflict of interests between the certifying authorities and the subscribers;

(m) Laying down the duties of the certifying authorities;

(n) Maintaining a database containing the disclosure record of every certifying authority containing such particulars as may be specified by regulations, which shall be accessible to public.

7.3.1 Recognition of Foreign Certifying Authorities

Q. 7.3.2 Explain recognition of foreign certifying authorities. (Ref. Sec.7.3.1) (5 Marks)

- As per Section 19 of IT Act, 2000, the controller of certifying authorities may, with the previous approval of the Central Government, and by notification in the official gazette, recognize any foreign certifying authority as a certifying authority. Certificate issued by certifying authority is valid under the Act.
- The controller can revoke the certificate of certifying authorities if he is satisfied that any certifying authority has contravened any of the conditions and restrictions subject to which it was granted recognition.
- For license certificate authorities have to pay 25000 and for renewal of the licence of license 5000 rupees is charged which is non-refundable.
- The license is valid for 5 years. When the application is done for renewal of license that application have to done not less than 45 days before the license expiry date.
- The controller has to grant or reject the application for license within 4 weeks from the date of the receipt of the application (Section 24).
- The controller can refuse the grant or renewal of certifying authority license if (Rule 17 of the certifying authorities rules, 2000):
  - (i) The applicant has not provided the controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or
  - (ii) The applicant is in the course of being wound up or liquidated; or
  - (iii) A receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or
  - (iv) The applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the act or these rules; or
  - (v) The controller has invoked performance bond or banker's guarantee; or
  - (vi) A certifying authority commits breach of, or fails to observe and comply with, the

procedures and practices as per the Certification Practice Statement; or

(vii) A certifying authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or

(viii) The audit report recommends that the certifying authority is not worthy of continuing Certifying Authority's operation; or

(ix) A certifying authority fails to comply with the directions of the controller.

7.3.2 Commencement of Operation by Licensed Certifying Authorities (Rule 20 of Certifying Authority's Rules, 2000)

Q. 7.3.3 Explain commencement of operation by licensed certifying authorities. (Ref. Sec. 7.3.2) (5 Marks)

The licensed certifying authority shall commence its commercial operation of generation and issue of digital signature only after :

(a) It has confirmed to the controller the adoption of Certification Practice Statement;

(b) It has generated its key pair, namely, private and corresponding public key, and submitted the public key to the controller;

(c) The installed facilities and infrastructure associated with all functions of generation, issue and management of digital signature certificate have been audited by the accredited auditor in accordance with the provisions of Rule 31; and

(d) It has submitted the arrangement for cross certification with other licensed certifying authorities within India to the controller.

Suspension of license

- After doing the inquiry if the controller is not satisfied then he can suspend the license. The license cannot be suspended up to 10 days until the reason is not given to the certifying authority.
- The controller of certifying authority has to publish the renewal and suspension of the license. If the certifying authority failed to surrender the license after renewal or suspension then punishment of imprisonment up to 6 months and 10,000 rupees fine is issued against the certifying authority.

Database of certifying authorities

- Rule 22 of certifying authorities rules states that The controller shall maintain a database of the disclosure record of every certifying authority, cross certifying authority and foreign certifying authority, containing inter alia the following details :

(a) The name of the person/names of the directors, nature of business, income tax permanent account number, web address, if any, office and residential address, location of facilities associated with functions of generation of digital signature certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;

(b) The public key(s), corresponding to the private key(s) used by the certifying authority and recognized foreign certifying authority to digitally sign digital signature certificate;

(c) Current and past versions of certification practice statement of certifying authority;

(d) Time stamps indicating the date and time.

☞ Confidential Information

- Rule 33 of certifying authorities rules states that the following information shall be confidential :

  (a) Digital Signature Certificate application, whether approved or rejected;

  (b) Digital Signature Certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the digital signature certificate information;

  (c) Subscriber agreement.

- Section 42 imposes some responsibility on subscriber of a digital signature. Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his digital signature certificate and take all steps to prevent its disclosure.

- If the private key of the subscriber gets compromised then the subscriber shall communicate the same without any delay to the certifying authority.

Syllabus Topic : E-Governance In India : A Warning to Babudom!

7.4 E-Governance In India : A Warning to Babudom!

Q.7.4.1 Explain E-governance in India. (Ref. Sec. 7.4) (5 Marks)

E-Governance legal mechanism is mentioned in chapter 3 of Information Technology Act, 2000. It explains the legal recognition of electronic records and signatures.

7.4.1 Legal Recognition of Electronic Records

The Section 4 of IT Act, 2000 mention the legal recognition of electronic records. It states that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is :

(a) Rendered or made available in an electronic form; and

(b) Accessible so as to be usable for a subsequent reference.

7.4.2 Legal Recognition of Electronic Signature

The Section 5 of IT Act, 2000 mention the legal recognition of electronic signature. It states that 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.

7.4.3 Use of Electronic Records and Electronic Signatures in Government and its Agencies

The Section 6 of IT Act, 2000 mention the use of electronic records and electronic signatures in government and its agencies. Where any law provides for :

(a) The filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate government in a particular manner;

(b) The issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;

(c) The receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate government.

7.4.4 Retention of Electronic Records

The Section 7 of IT Act, 2000 mention the retention of electronic records any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or

information are retained in the electronic form, if :

(a) The information contained therein remains accessible so as to be usable for a subsequent reference;

(b) The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) The details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

7.5 Exam Pack (Review Questions)

☛ Syllabus Topic : Digital Signatures

Q. 1 What is digital signature? What are the functions of digital signature? (Refer Section 7.1) **(5 Marks)**

Q. 2 Explain the cryptosystem and hash function.(Refer Section 7.1) **(5 Marks)**

Q. 3 Write short note on digital signature. (Refer Section 7.1) **(5 Marks)**

☛ Syllabus Topic : Digital Signature Certificate

Q. 4 Explain digital signature certificate. (Refer Section 7.2) **(5 Marks)**

☛ Syllabus Topic : Certifying Authorities and Liability in the Event of Digital Signature Compromise

Q. 5 Explain certifying authorities and their liability in the event of digital signature compromise. (Refer Section 7.3) **(5 Marks)**

Q. 6 Explain recognition of foreign certifying authorities. (Refer Section 7.3.1) **(5 Marks)**

Q. 7 Explain commencement of operation by licensed certifying authorities. (Refer Section 7.3.2) **(5 Marks)**

☛ Syllabus Topic : E-Governance in India : A Warning to Babudom!

Q. 8 Explain E-governance in India. (Refer Section 7.4) **(5 Marks)**

Chapter Ends...

□□□