UNIT 8 : THE INFORMATION TECHNOLOGY ACT-2000

UNIT STRUCTURE

8.1 Learning Objectives

8.2 Introduction

8.3 Brief History

8.4 Objectives of the Act

8.5 Definitions Under the Act

8.6 Provisions Relating to Digital Signature and Electronic

8.7 Electronic Records

8.8 Attribution, Acknowledgement and Dispatch of Electronic Records

8.9 Regulation of Certifying Authorities

8.10 Electronic Signature Certificates

8.11 The Cyber Appellate Tribunal

8.12 Offences and Penalties Under the Act

8.13 Let Us Sum Up

8.14 Answers To Check Your Progress

8.15 Model Questions

8.1 LEARNING OBJECTIVES

After going through this unit you will be able to:

- discuss about the objectives of IT Act
- discuss the various terms used in the Act
- know the Provisions relating to digital signature and electronic signature
- explain the Provisions relating to electronic records
- discuss the composition and powers of Cyber appellate tribunal
- discuss about Regulation of certifying authorities
- know about the Offences and penalties under the Act.

8.2 INTRODUCTION

In the 21st century Information Technology has become the lifeline of the human civilization. Keeping in view the growing use and importance of & Information Technology, Government of India decided to bring the area of Information Technology under the preview of law. Accordingly The Information Technology Act, 2000 was enacted. In this chapter we will discuss about The Information Technology Act, 2000. This Act give legal recognition to digital records and other activities carried out electronically. This has a great bearing over e-commerce and e-business.

After going through this unit you will have a broad idea about uses and applicability of The Information Technology Act, 2000.

8.3 BRIEF HISTORY

The use of computer, internet and Information Technology has changed the lifestyle of the people of 21st century. Today paper based communication is replaced by e-communication, paper based transaction is replaced by e-commerce and paper based governance by e- governance. Use of IT and computer bring some new word to use, such as cyber world, e-communication, e- business, e-commerce, e-banking, e-contract, e-tendering, e-certificate, e-library etc. Despite making the life easy and fast, use of IT by criminals as a weapons of offence has threaten the world. Accordingly a new branch of law emerged to tackle the problems of cyber-crime in the cyber space i.e. Cyber Law or Information Technology Act.

So far Business is concern, now a days most of the business transactions are done with the help of computer and information technology. Business activities carried out through electronic form are known as electronic commerce or e-commerce. It reduces the need for paper based transactions. The hurdle faced by e-commerce and e-governance is its legal recognition i.e. signature over the document. But, there are laws governing paper base records and documents which bears signature.

In the given situation, for the first time in the year 1996, The United Nations Commission on International Trade and Law (UNCITRAL) adopted

a model law on e-commerce. This was adopted by the General Assembly of the UN by passing a resolution in the year 1997, where India was also a signatory. Further the Government of India felt the need for a separate law and amendments in the existing laws giving legal recognition to digital signature and electronic records for facilitating e-commerce and e-governance. This gave birth to the Information Technology Bill, 1999. The Bill was passed in both the house of the parliament in May, 2000, and it receives assent of the President of India in August, 2000 and come to be known as Information Technology Act, 2000. The Act further amended in the year 2008 to suit the need of the hour.

The Act has a major impact on e-commerce and e-governance, therefore it is important to study various provisions of The Information Technology Act, 2000.

8.4 OBJECTIVES OF THE ACT

The Information Technology Act, 2000 was enacted with the following Objectives:

- To legalise transactions carried out electronically
- To give legal recognition to digital signatures
- To facilitate electronic filing of documents with government departments
- To facilitate electronic storage of data
- To facilitate and give legal recognition of electronic fund transfers between banks and financial institutions
- To amend the Indian Penal Code, the Indian Evidence Act, 1872; The Banker's Book Evidence Act, 1891 and Reserve Bank of India Act, 1934.

8.5 DEFINITIONS UNDER THE ACT

Before going to the provisions of the Act in detail, it will be better to know the meaning of some terms used in the Act. This will help us in understanding the provisions of the Act in a better way. In the following

section we will discuss some definition included in the sec.2 of the Act.

Appropriate Government

According to Sec 2 (1) (*e*) of the Act "appropriate Government" means as respects any matter,

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

Asymmetric Crypto System

According to Sec 2 (1) (*f*) "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.

Communication Device

According to Sec. 2 (1) (*ha*)"communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

Computer

According to Sec. 2 (1) (*i*) "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

Computer network

According to Sec. 2 (1) (*j*) "computer network" means the interconnection of one or more computers or computer systems or communication device through—

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the

interconnection is continuously maintained.

Computer resource

According to Sec. 2 (1) (*k*)"computer resource" means computer, computer system, computer network, data, computer database or software.

Computer system

According to Sec. 2 (1) (*l*) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

Cyber security

According to Sec. 2 (1) (*nb*) "cyber security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

Data

According to Sec. 2 (1) (*o*) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the Computer.

Digital signature

According to Sec. 2 (1) (*p*) "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.

Digital Signature Certificate

According to Sec. 2 (1) (*q*) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) Of section 35;

Electronic form

According to Sec. 2 (1) (*r*)"electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

Electronic Gazette

According to Sec. 2 (1) (*s*) "Electronic Gazette" means the official gazette published in the electronic form.

Electronic record

According to Sec. 2 (1) (*t*) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

Electronic signature

According to 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 and includes digital signature.

Function

According to Sec. 2 (1) (*u*) "function" in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.

Information

According to Sec. 2 (1) (*v*) "information" includes [data, message, text,] images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

Intermediary

According to Sec. 2 (1) (*v*) "intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

Key pair

According to Sec. 2 (1) (*x*) "key pair", in 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.

Electronic Governance

Electronic governance refers to the use of Information Technology in the functioning of government machinery. Use of Information Technology in the functioning of government can bring transparency and promptness. It involves electronic filing of documents with the government departments and agencies, creating a network of e-services and making services available through online. From 16th September, electronic filing using digital signature has been made compulsory for companies. This will allow companies to file any documents in the electronic form and make payments of fee by using Internet banking and credit/debit card.

Keeping in view, the importance of e-governance the Information Technology Act 2000, gives legal recognition to electronic records, digital signatures and electronic dealings with government officials and agencies. The Act laid down the following provisions to facilitate e-governance.



CHECK YOUR PROGRESS

Q 1: Define Digital signature under IT Act.

.....

.....

Q 2: Define Data under IT Act.

.....

.....

8.6 PROVISIONS RELATING TO DIGITAL SIGNATURE AND ELECTRONIC

In the earlier section of the unit we have discuss about various definitions that we help us in understanding the provisions of the Act. In this section we will discuss about provisions of the Act regarding digital

signature and electronic signature which is given in the Sec.3 of the Act.

8.6.1 Authentication of electronic records

According to Sec 3 of the Information Technology Act, any subscriber may authenticate an electronic record by affixing his digital signature. 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 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.

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

8.6.2 Electronic signature

The provisions related to Electronic Signature has been laid down in the Act under Sec 3A, which prescribes-

Not with standing 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.[Sec 3A(1)]

For the purpose of this section any electronic signature or electronic authentication technique shall be considered reliable if—

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.[Sec3A(2)].

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. [Sec3A(3)].

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; Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable. [Sec 3A(4)].

Every notification issued under sub-section (4) shall be laid before each House of Parliament [Sec3A(5)].

8.7 ELECTRONIC RECORDS

According to Sec. 2 (1) (*t*) “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. We have already

discussed about provisions relating to Authentication of electronic records. Now, we will discuss other provisions related to Electronic Records in the following paragraph.

8.7.1 Legal recognition of electronic records (Sec.4)

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.

8.7.2 Legal recognition of electronic signatures

According to Sec-5 of the Act, Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should 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 signatures affixed in such manner as may be prescribed by the Central Government.

Explanation— For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

8.7.3 Use of electronic records and electronic signatures in Government and its Agencies

According to Sec-5 of the Act, Where any law provides for 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;and the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner; and 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. The appropriate Government may, by rules, prescribe—

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a) stated above.

8.7.4 Retention of electronic records

Section 7 of the Act provides that Where 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. These provisions will not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

8.7.5 Power to make rules by Central Government in respect of electronic signature

Section 10 of the IT Act empowered the Central Government to make rules in respect of electronic signature prescribing:

(a) the type of electronic signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure, which facilitates identification of the person affixing the electronic signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to electronic signatures.

8.8 ATTRIBUTION, ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS

8.8.1 Attribution of electronic records

According to section 11 of the IT Act an electronic record shall be attributed to the originator, if it was sent by the originator himself; or by a person who had the authority to act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically.

8.8.2 Acknowledgment of Receipt of Electronic Records

Section 12 of the IT Act provides that where the originator

has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by any communication by the addressee, automated or otherwise; or any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received. [Sec-12(1)].

Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator [Sec-12(2)].

Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent[Sec-12(3)].

8.8.3 Time and place of dispatch and receipt of electronic record

According to Section 13 of the Act unless otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator [Sec-13(1)].

Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows:

(a) if the addressee has designated a computer resource for the

purpose of receiving electronic records— receipt occurs at the time when the electronic record enters the designated computer resource; or if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee [Sec-13(2)].

Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business[Sec-13(3)].

The provisions of sub section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3) [Sec-13(4)].

For the purposes of this section,

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) “usual place of residence”, in relation to a body corporate, means the place where it is registered.

8.8.4 Secure electronic record

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. **(Sec-14)**

8.8.5 Secure electronic signature

An electronic signature shall be deemed to be a secure electronic signature if the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and the signature creation data was stored and affixed in such exclusive manner as may be prescribed Explanation. In case of digital signature, the "signature creation data" means the private key of the subscriber. **(Sec-15)**

8.9 REGULATION OF CERTIFYING AUTHORITIES

8.9.1 Appointment of Controller and other officers

Under section 17 of the IT Act, the Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers Assistant Controllers, other officers and employees as it deems fit.

8.9.2 Functions of Controller

Under section 18 of the IT Act, the Controller may perform all or any of the following functions, namely:

(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 Authorities 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 material and Advertisements that may be distributed or used in respect of a Digital Signature Certificate and the Public Key;

(g) specifying the form and content of a Digital Signature Certificate and thekey;

(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 of disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

8.9.3 Recognition of foreign Certifying Authorities

Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any Foreign Certifying Authority as a Certifying Authority for the purposes of this Act. Where any Certifying Authority is recognized, the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition he may, for reasons to

be recorded in writing, by notification in the Official Gazette, revoke such recognition.(Sec-19)



CHECK YOUR PROGRESS

Q 3: What is secured electronic record under IT Act.?

.....

.....

Q 4: Mention two functions of the controller.

.....

.....

8.9.4 Licence to issue Electronic Signature Certificates

Subject to the provisions of this Act, any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.

No licence shall be issued under the Act, unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government.

A licence granted under this section shall be valid for such period as may be prescribed by the Central Government; not transferable or heritable and subject to such terms and conditions as may be specified by the regulations (Sec-21).

8.9.5 Application for Licence

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government and shall accompanied by:

(a) a certification practice statement;

(b) a statement including the procedures with respect to

identification of the applicant;

(c) payment of such fees, not exceeding twenty five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government. **(Sec-22)**

8.9.6 Renewal of Licence

An application for renewal of a licence shall be in such form and accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty five days before the date of expiry of the period of validity of the licence:

Provided that an application for the renewal of the licence made after the expiry of the licence may be entertained on payment of such late fee, not exceeding five hundred rupees, as may be prescribed. **(Sec-23)**

8.9.7 Suspension of Licence

The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain the procedures and standards specified in section 30;

(d) contravened any provisions of this Act, rule, regulation or order made thereunder.[Sec-25(1)]

However, no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause

against the proposed revocation.

The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him.

However, no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.[Sec-25(2)]

Further, No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.[Sec-25(3)]

8.9.8 Procedures to be followed by Certifying Authority

Every Certifying Authority shall

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse:

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the electronic signatures are assured; be the repository of all Electronic Signature Certificates issued under this Act or publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and observe such other standards as may be specified by regulations(Sec-30).

8.9.9 Surrender of licence

Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller. Where any Certifying

Authority fails to surrender a licence, the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both **(Sec-33)**.

8.10 ELECTRONIC SIGNATURE CERTIFICATES

8.10.1 Certifying Authority to issue Electronic Signature Certificate

Any person may make an application to the Certifying Authority for the issue of an Electronic Signature Certificate in such form as may be prescribed by the Central Government. Every such application shall be accompanied by such fee not exceeding twenty five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority. Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

On receipt of an application, the Certifying Authority may, after consideration of the certification practice statement or the other statement and after making such enquiries as it may deem fit, grant the Electronic Signature Certificate or for reasons to be recorded in writing, reject the application.

Provided that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection. (Sec-35)

8.10.2 Representations upon issuance of Digital Signature Certificate

Sec 36 of the I T Act provides that a Certifying Authority while issuing a Digital Signature Certificate shall certify that

(a) it has complied with the provisions of this Act and the rules and regulations made there under;

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(ca) the subscriber holds a private key which is capable of creating a digital signature

(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

8.10.3 Suspension of Digital Signature Certificate (Sec-37)

Section 37 of the IT Act provides that Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,

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

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorised 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 fifteen days unless the subscriber has been given an opportunity of being heard in the matter. On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.



CHECK YOUR PROGRESS

Q 5: When Digital Signature Certificate is suspended?

.....

.....

8.10.4 Revocation of Digital Signature Certificate

Section 38 of the IT Act discuss about revocation of Digital Signature Certificate.

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it

- (a) where the subscriber or any other person authorised 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.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a 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.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

8.10.5 Notice of suspension or revocation (Sec-39)

Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice. Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

8.11 THE CYBER APPELLATE TRIBUNAL

8.11.1 Establishment of Cyber Appellate Tribunal

The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal. The Central Government shall also specify the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Cyber Appellate Tribunal has been setup under the IT Act under the aegis of Controller of Certifying Authorities. Initially the Tribunal was known as the Cyber Regulations Appellate Tribunal, which started functioning from October 2006. The Cyber Regulations Appellate Tribunal is renamed as Cyber Appellate Tribunal after the amendment of the IT Act in the year 2008. **(Sec-48)**

5.11.2 Composition of Cyber Appellate Tribunal

(1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint.Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act, 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008.

(2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

(3) Subject to the provisions of this Act

  (a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercise by the Branches thereof;

  (b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two Members of such Tribunal as the Chairperson may deem fit;

  (c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify;

  (d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

(4) Not with standing anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a

Member of such Tribunal from one Bench to another Bench.

(5) If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit. **(Sec-49)**

8.11.3 Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court.

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of, and professional experience in, information technology, telecommunication, industry, management or consumer affairs. Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, as has held the post of Additional Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than one year or Joint Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than seven years.

(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been an member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that Service for a period of not less than five years. **(Sec-50)**

8.11.4 Term of office, conditions of service, etc., of Chairperson and Members

(1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty five years, whichever is earlier.

(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.

(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member. **(Sec-51)**

8.11.5 Appeal to Cyber Appellate Tribunal

Section 57 of the IT Act prescribes the procedures of making an apple to the Tribunal.

(1) Save as provided in sub-section (2) any person aggrieved by an order made by an adjudicating officer under this Act may prefer an appeal to a Cyber Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty five days from the date on which a copy of the order made by the controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed.

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1) the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

8.11.6 Procedure and powers of the Cyber Appellate Tribunal

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:

(a) summoning and enforcing the attendance of any person and examining him on oath;
(b) requiring the discovery and production of documents or other electronic records;
(c) receiving evidence on affidavits;
(d) issuing commissions for the examination of witnesses or documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it ex parte;
(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974). **(Sec-58)**

8.11.7 Civil court not to have jurisdiction

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act. **(Sec-61)**

8.11.8 Appeal to High court

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of

the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order. Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days. **(Sec-62)**

8.12 OFFENCES AND PENALTIES UNDER THE ACT

8.12.1 Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

For the purposes of this section, “computer source code” means the listing of programmes, computer Commands, design and layout and programme analysis of computer resource in any form. **(Sec-65)**

8.12.2 Computer related offences

If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation, For the purpose of this section,

(a) the word “dishonesty” shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860).

(b) the word “fraudulently” shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).(Ses-66)

8.12.3 Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,

(a) any information that is grossly offensive or has meaning character, or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail massage for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such massage,shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation, For the purposes of this section, terms “electronic mail” and “electronic mail message” means a message or information created to transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.[Sec-66(A)]

8.12.4 Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. [Sec-66(B)]

8.12.5 Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. [Sec-66(C)]

8.12.6 Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. [Sec-66(D)]

8.12.7 Punishment for violation of privacy

Whosoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. [Sec-66(E)]

Explanation, For the purposes of this section

(a) ”transmit” means to electronically send a visual image with the internet that it be viewed by a person or persons;

(b) ”capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) ”private area” means the naked or undergarment clad genitals, public area, buttocks or female breast;

(d) ”publishes” means reproduction in the printed or electronic form and making it available for public;

(e) ”under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public regardless of whether that person is in a public or private place.

8.12.8 Punishment for cyber terrorism

Whosoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disputes or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the state or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security

of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life. [Sec-66(F)]

8.12.9 Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees. [Sec-67]

8.12.10 Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment

of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees. [Sec-67(A)]

8.12.11 Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form

Whoever, (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship which one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online; or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five year and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees;

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form—

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is in the interest of science, literature, art or learning or other objects

of general concern; or

(ii) which is kept or used for bona fide heritage or religious purpose.

Explanation, For the purpose of this section, "children" means a person who has not completed the age of 18 years. [Sec-67(B)]

8.12.12 Indian Computer Emergency Response Team to serve as national agency for incident response

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1)with a Director General and such other officers and employees as may be prescribed .

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security-

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisors, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

(f) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.

(7) Any service provider intermediaries, data centers, body corporate or person who fails to provide the information called for the comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may be extend to one year with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1).]

8.12.13 Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. (Sec-71)

8.12.14 Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made the reunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or

other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.(Sec-72)

8.12.15 Punishment for disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.[Sec-72(A)]

8.12.16 Penalty for publishing Electronic Signature Certificate false in certain particulars

No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying an electronic signature created prior to such suspension or revocation.

Any person who contravenes this provisions shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.(Sec-73)

8.12.17 Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. (Sec-74)

8.12.18 Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation. *Provided* that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.(Sec-76)



8.13 LET US SUM UP

- The Information Technology Act, 2000 was enacted in year 2000 and it was further amended in Year 2008 by IT Amendment Act, 2008.
- The Act aims to provide the legal infrastructure for e-commerce in

India. The Act also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

- The IT Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Electronic Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Electronic Signature Certificates.
- The IT Act laid down various provisions for penalties, Compensation and adjudication for various offences.
- The IT Act laid down provisions for establishment of the Cyber Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.



8.14 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: According to Sec. 2 (1) (*p*) “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.

Ans to Q No 2: According to Sec. 2 (1) (*o*) “data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be

in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the Computer.

Ans to Q No 3: According to Sec 14 of the Act, Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Ans to Q No 4: (a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the certifying authorities;

Ans to Q No 5: a Digital Signature Certificate may suspend,

(a) on receipt of a request to that effect from the subscriber listed in the Digital Signature Certificate; or any person duly authorised 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 fifteen days unless the subscriber has been given an opportunity of being heard in the matter. On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.



8.15 MODEL QUESTIONS

Q 1: Explain briefly the objectives of the Information Technology Act 2000 as amended.

Q 2: What are the conditions subject to which electronic record may be authenticated by means of affixing electronic signature?

Q 3: Discuss theprovisions ofthe Information Technology Act 2000 as amended to facilitate E-governance

Q 4: What are the regulations relating to the appointment and powers of the certifying authorities underInformation Technology Act 2000 as amended?

Q 5: Explain the duties of a certifying authority under Information Technology Act 2000 as amended?

Q 6: Describe the composition and powers of Cyber appellate tribunal.

*** ***** ***