INFORMATION TECHNOLOGY ACT, 2000

(PART - 2)

Subject	**:**	**Business Economics**
Course	**:**	**B.A., 2nd Semester, Undergraduate**
Paper No.	**:**	**203**
& Title	**:**	**Leagal Aspects of Business**
Unit No.	**:**	**5 (Five)**
& Title	**:**	**Information Technology Act, 2000**
Practical No.	**:**	**2 (Two)**
& Title	**:**	**Information Technology Act, 2000 (Part - 2)**

Credits

Subject Co-ordinator:

Dr. V. Chari
Prof. School of Commerce,
Gujarat University,
Ahmedabad.

Subject Expert

N.C. Raghavi Chakravarthy
Junior Research Fellow
S.D. School of Commerce
Gujrat Universty,Ahmedabad.

Technical Assistants

Smita Bhatt
Archna Patel

Video Editor

Jaydeep Gadhvi

Multimedia

Gaurang Sondarva

Camera

Mukesh Soni

Technician

Mukesh Soni

Prod. Asst. & Editing Concept

Mukesh Soni

General Asst.

Jagdish Jadeja

Helper

Ambalal Thakor

Graphic Artist & Animator

Dilip Dave

Jaydeep Gadhvi

Producer

Dinesh Goswami

Academic Script

Hello friends. In the previous session of the information technology act, we covered the background of the act, the cases where the provisions of the act are applicable as well as the cases where the provisions of the information technology act are not applicable. We also covered the various definitions of the electronic media as given in the act. We also discussed as to when information would be recognized as electronic records. Lastly, we also saw when digital signatures are legally recognized. In today's session, we will cover as to how the digital signatures are used in electronic governance and the various provisions for the regulations of the certifying authority.

In actual business transactions, the provisions which relate to the authentication of digital signatures and electronic governance play an important role.

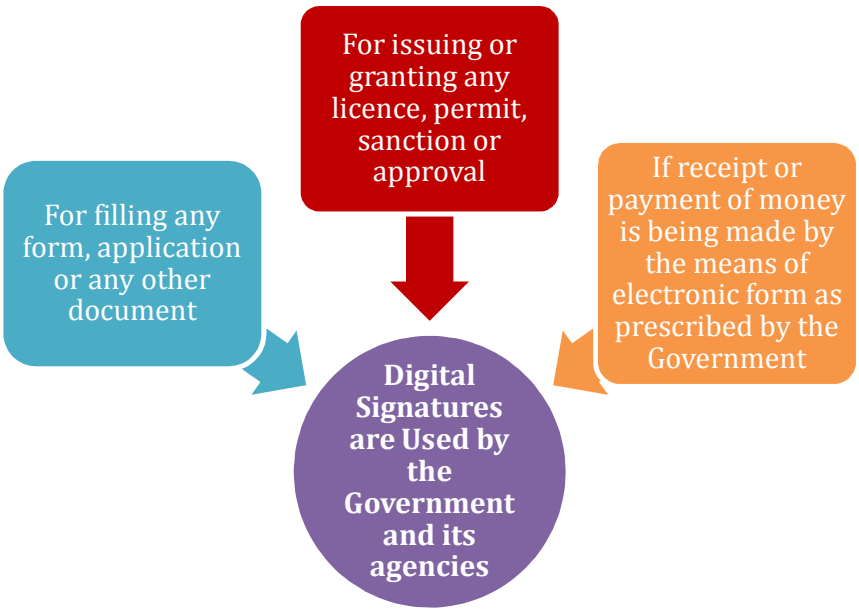
Use of Digital Signatures in Electronic Governance

Use of Electronic records and digital signatures by the government and its agencies

The Government and its agencies use the electronic record and digital signatures in the below circumstances:

1. For filling any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate government.

2. For issuing or granting any licence, permit, sanction or approval
3. If the receipt or payment of money is being made by the means of electronic form which is prescribed the appropriate government.



It is important that the manner and format of such electronic record has to be filed, created or issued as well as the manner or method of payment of any fee or charges that have to be made are prescribed by the appropriate government.

Retention of Electronic Records

The electronic records have to be retained when:

1. If any law explicitly prescribes the retention of the records.
2. If the information contained in such records should remain accessible for subsequent reference.
3. The electronic record accurately represents the original document which was originally generated, sent or received.
4. The details will help in identification of the origin, destination, date and time of dispatch or receipt of such an electronic record. The information generated for the purpose of sending or receiving an electronic record shall not be retained.

Publication date for the rule, regulation etc. published in the Electronic Gazette

The publication date for any rule, regulation, order, bye-law, notification or any other matter would be the date on it was published for the first time either in the Official Gazette or the Electronic Gazette.

It should be taken into note that the above provisions do not give a right to any person to insist that any Ministry, Department of the Central Government or the State Government or any other body established

and controlled by them to accept, issue, create, retain and preserve any document in electronic form or effect any monetary transaction in electronic form.

Powers of Central Government to frame rules in respect of digital signatures

The Central Government can frame rules and prescribe for the purpose of :

1. The type of digital signature
2. The manner and format of affixing such a signature
3. The procedure to identify the person affixing such a signature.
4. Control of the process and procedure for maintaining integrity, security and confidentiality of the electronic records of payments
5. Any other matters which give legal effect to the digital signatures.

For a digital document to be accepted legally, such a document needs to be certified by a certifying authority.

B. Regulation of certifying authorities

The certifying authorities are the ones who issue digital documents which enable the verification of the digital identity of any entity in order access information or services and also allow them to sign the documents digitally. Controllers are appointed in order to regulate the activities of the certifying authorities. Let us now discuss the various

provisions in the act for the regulation of the certifying authority.

Appointment of Controller and other officers:

The appointment of the controller and officers is undertaken by the Central Government by notification in the Official Gazette. It can also appoint any number of Deputy Controllers and Assistant Controllers as it deems fit.
The controller would undertake the functions that are prescribed to him under the act or any other additional function assigned to him by the Central Government. The Deputy and the Assistant Controllers would undertake the activities that are assigned to them by the Controller. The conditions for appointment, the experience, and the required qualification would be decided by the Central Government. The head office and the branch offices would be established by the Central Government wherever they deem fit.

Functions of the controller:

The functions of the Controller includes

1. Supervising the activities of the Certifying Authorities
2. Certifying public keys of the Certifying Authorities
3. Formulating standards that have to be followed by the Certifying Authorities

4. Deciding what qualification should the employees of Certifying Authorities should have
5. Specify the conditions which the Certifying Authority need to follow while undertaking their business.
6. Laying down criteria as to which information can be used by the certifying authority for the purpose of advertisement.
7. Deciding the form and content of the digital signature certificate and the key.
8. Instructing as to how the accounts of the certifying authority needs to be maintained.
9. Deciding as to who can be appointed as auditors and the remuneration that can be paid to them.
10. Helping in the establishment of any electronic system by a certifying authority either solely or jointly with other certifying authority and assuming the responsibility of regulating any such system that is in existence.
11. Laying down standards as to how the certifying authorities need to deal with the subscribers.
12. Intervening whenever there is a conflict between the certifying authority and the subscribers.
13. Deciding the duties that a certifying authority needs to perform.

14. Maintain a record of disclosures that are made by the Certifying authority. These records should be accessible to the public.

Grant of recognition to a foreign certifying authority:

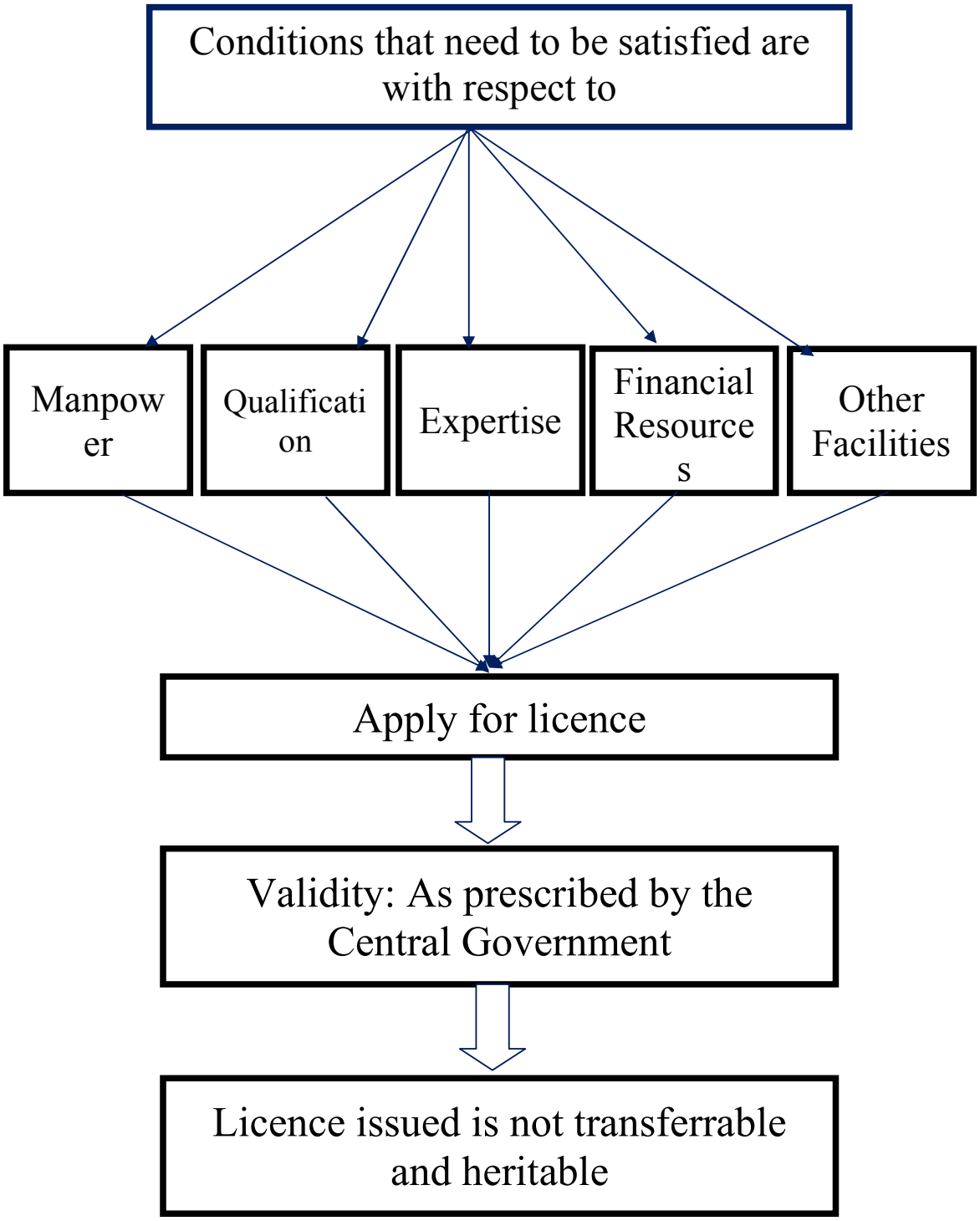
A foreign certifying authority can be granted recognition under this act. The Controller can grant recognition to the foreign certifying authority with prior approval of the Central Government. The recognition is granted by issuing a notification in the Official Gazette. If such a foreign authority has violated any condition of the act, then such a recognition which was granted to them can be revoked by issuing a notification in the Official Gazette.

Controller as a repository of Digital Signature Certificates

The controller has a record of all the Digital Signature Certificates issued by it. Further it also ensures that the hardware, software and the procedures are secured from any type of intrusion. It also ensures that all the standards that are prescribed by the central government are followed so that the secrecy and the security of the digital signatures are maintained. It also has a computerized database of all the public keys which is accessible by the general public. So essentially, a Controller acts a repository of the digital signatures

Criteria for applying for a digital licence

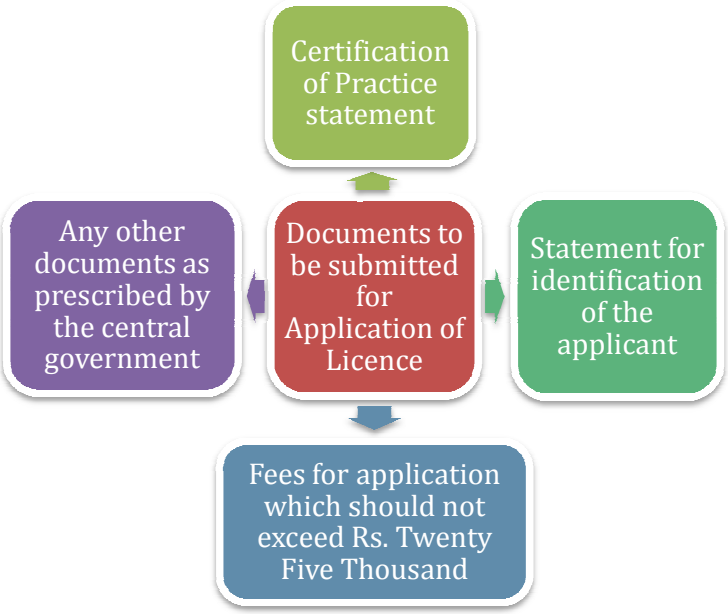
Any person who satisfies the conditions with respect to manpower, qualification, expertise, financial resources and other facilities as prescribed by the Central Government can apply for getting a licence to issue digital Certificates. Such a licence which is granted shall be valid for a period as prescribed by the Central Government and would not be transferrable or heritable.


Conditions that need to be satisfied are with respect to
Manpow er
Qualificati on
Expertise
Financial Resource s
Other Facilities
Apply for licence
Validity: As prescribed by the Central Government
Licence issued is not transferrable and heritable

Procedure for application for issue of a licence

The application for issue of a licence shall be in the manner as prescribed by the central government. It shall be accompanied by

1. A certification of practice statement
2. Statement for identification of the applicant
3. Fees for application which should not exceed Rupees Twenty Five Thousand as prescribed by the central government.
4. Any other documents as prescribed by the central government.

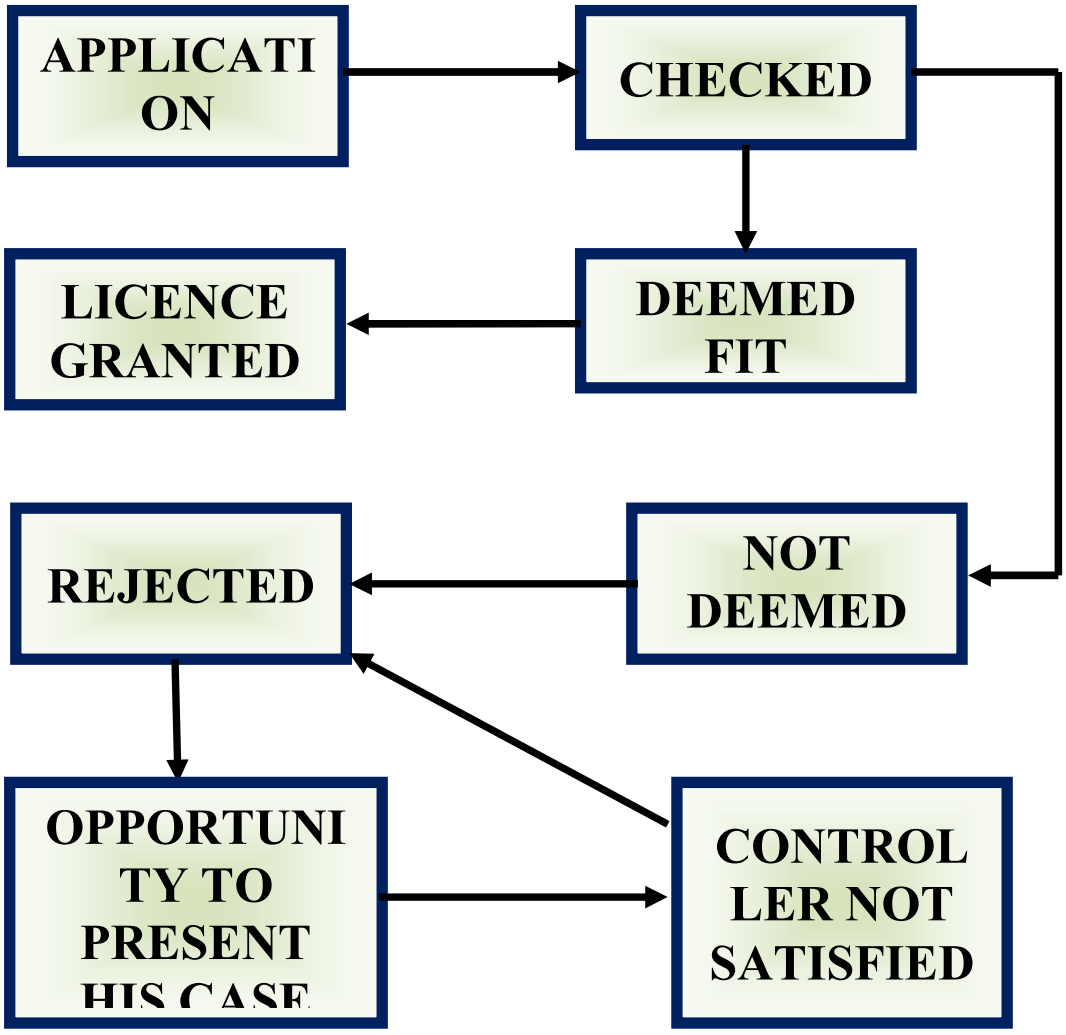


Procedure to renew a licence :

In order to renew a licence which has expired, an application accompanied by fees not exceeding twenty five thousand as prescribed by the central government need to be made forty five days prior to the expiry of the licence.

Procedure for granting a licence :

The application which is received is checked and if it is deemed fit, then such an applicant shall be granted the licence. In case if an application is rejected then such an applicant is given a reasonable opportunity to present his case. Even after this if the controller is not satisfied then the application would be rejected.

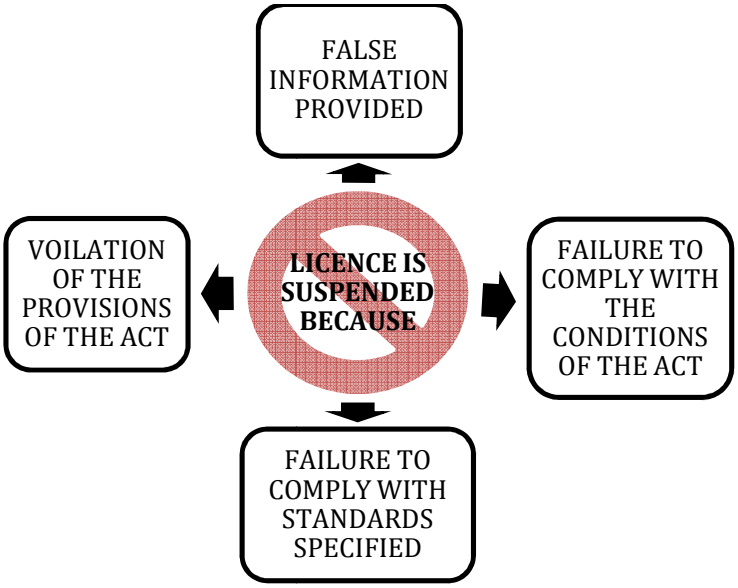


Circumstances when the licence issued is suspended

The controller may suspend the licence of the certifying authority in the following cases

1. If after inquiry it is found that the details provided in the application for issue or renewal of the licence are incorrect or false
2. If the certifying authority fails to comply with any terms and conditions of the act

3. If the certifying authority fails to comply with any standards that are specified.
4. Has violated any provisions of the act.



In case of revocation of the license, then such a revocation cannot be effected till the certifying authority has been given a reasonable opportunity to present his case. Till the certifying authority presents their case, the licence of such an authority would remain suspended for a period not exceeding a period of ten days. During that period, such an authority shall not issue any Digital Signature Certificate. When the licence that has been issued is suspended or revoked, the controller has to publish a notice on the database maintained by him or any other such databases

which are in existence. Such a notice should be accessible round the clock.

Delegation of powers by a controller

A controller can delegate his powers to the deputy controller or the assistant controller. Such a delegation of powers has to be made in written form which authorizes them to exercise any powers that have been delegated to them.

Procedure for investigation of a contravention

The investigation of the contravention shall be undertaken by the controller himself or any other officer authorized by him for this purpose. The controller or the officer authorized by him to undertake investigation shall have access to any computer system, apparatus, data or any other material connected with the system to undertake the investigation for the purpose of determining an act of contravention undertaken. The controller or any other officer authorized by him can order or demand technical or other assistance from the person in charge of operation of such a system or apparatus if he considers it essential.

Procedures that the certifying authorities need to follow

Every certifying authority needs to

1. Make use of hardware, software and procedures that are secure from intrusions and misuse.
2. Maintain reliability in their services which is required for the performance of their functions that they have to undertake.
3. Ensure that secrecy and privacy of the digital signatures is maintained.
4. Adhere to any other standards that are specified by the regulators

Moreover they should ensure that every person employed by them or engaged in their activities fulfill the criteria of employment laid under the act.

The certifying authority shall display the licence issued to them at a noticeable place in the premises where they carry out their business.

Surrender of licence by the certifying authority

The licence which has been issued has to be surrendered when the licence of the certifying authority has been suspended or revoked. In case if the certifying authority fails to surrender the licence then the person in whose name

the licence has been issued will be guilty of an offence and can be punished in the following manner :

1. Imprisonment of maximum six months
2. A fine of Ten Thousand Rupees
3. Or both of the above.

Disclosures that have to be made by the certifying authority

The certifying authority shall disclose the below matters in the form as prescribed by the regulators:

1. The digital signature certificate which includes the public key as well as the private key used by them to digitally sign another digital signature certificate.
2. Any certification practice statement
3. Revocation or suspension of its certifying authority certificate
4. Any other fact that materially and adversely affects reliability of a digital signature certificate issued by it or its own ability to perform its services.
5. In case of happening of any event or situation which adversely affects the integrity of its computer system or its ability to grant a digital signature certificate then the certifying authority shall undertake the following activities:

a. Exercise reasonable efforts to notify the people who are likely to be affected by that occurrence.

b. Undertake the procedures to deal with such events or situations as specified in its certification practice statement

SUMMARY

Friends, today's session was divided into two parts. In the first part we saw the provisions related to the use of digital signatures and E-Governance. We saw the various instances when the government and its agencies use the electronic records and digital signatures. We also covered the cases where the electronic records have to be retained. In the last part of the first section, we saw the powers of the central government to frame rules in respect of digital signatures. In the second part of today's session, we saw the provisions related to the regulation of the certifying authorities. In that we covered the provisions for appointment of the controllers and the functions that they have to perform. We also covered as to how a certifying authority is granted recognition. Then we saw as to how one can apply for digital licence as well as the procedure for its renewal. Then we covered the instances when the licence of a certifying authority is suspended. We also saw the procedure that the controller has to follow for undertaking an investigation if

there is any act of contravention. Lastly we saw the various disclosures that the certifying authorities need to make.
I hope that you understood the various provisions of the Information Technology Act, 2000. Thank you for joining with us.