Unit 3: Regulation and Responsibilitie Certifying Authorities and Controller Certifying Authorities

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Role of Certifying Authorities and Controller of Certifying Authorities
- Regulation of Certifying Authorities and Controller of Certifying Authorities
- Powers of Controllers of Certifying Authorities

1.2 INTRODUCTION

As per the existing laws in our country, Digital Signature Certificates are issued by Certifying Authorities in accordance with the provisions of the Information Technology Act, 2000. Certifying Authorities, therefore, have a very significant role to serve in, which is in turn backed by statutory obligations and responsibilities. Before a Certifying Authority starts issuing Digital Signature Certificates, it is required to receive a license from the controller of certifying authorities. Certifying Authorities, in essence, play a twin role by issuing Digital Signature Certificates to subscribers in one hand and identifying with and authenticating such subscribers

on the other. Given that Certifying Authorities play a very crucial role in the process of generation of Digital Signature Certificates, it is also important to regulate the activities of such Certifying Authorities.

1.3 REGULATION OF CERTIFYING AUTHORITIES

The provisions of the Information Technology Act, 2000 acknowledge an authority superior to Certifying Authorities and refers to the same as the 'Controller of Certifying Authorities'. Chapter VI of the Information Technology Act, 2000 lay down provisions that elaborate upon means and ways for the Controller of Certifying Authorities to regulate Certifying Authorities. Guidelines that are to be followed by Certifying Authorities have also been laid down in ***the Information Technology (Certifying Authorities) Rules, 2000*** and ***the Information Technology (Certifying Authorities) Regulations, 2001.***[93]

As per the legal regulations and obligations of the Certifying Authorities, and the powers conferred to them in accordance with the law of the land, the nature of such entity should rather be an administrative authority than being a quasi-judicial body. Accordingly, ***Section 17 of The Information Technology Act, 2000*** lays down those requisites associated with the appointment of the Controller of Certifying authorities and other offices. By virtue thereof, the central government has the authority to appoint the Controller of Certifying Authority which in turn could have three functional departments such as (a) Technology, (b) Finance and Legal and (c) Investigation. Each department is to have a deputy controller and assistant controllers to oversee the smooth functioning of the entity.[94]

As a part of regulating the functions of the Certifying Authorities, the Controller of Certifying Authorities is required to perform certain functions as laid down under section 18 of the Information Technology Act, 2000, which inter alia include:

(i) Exercising supervision over the activities of the Certifying Authorities: As has been stipulated under Rule 31 of the Information Technology (Certifying Authority) Rules, 2000, the Certifying Authority shall be required to conduct half-yearly or quarterly

[93] Information Technology Act, 2000
[94] The Cyber Regulations Tribunal (Procedure) Rules, 2000

audits and submit such reports to the Controller of Certifying Authorities within four (4) weeks from the date of completion of such audit. The essence of this provision lies in the fact that as a Certifying Authority, as a licensee, is required to fulfil such conditions as are stipulated by the Controller of Certifying Authorities.

(ii) Certifying public keys of Certifying Authorities: The Root Certifying Authority of India (RCAI) has been established by the Controller of Certifying Authorities to certify public keys of the Certifying authorities in the country, as a result of which, the RCAI shall be *inter alia* responsible for digitally signing public keys of licensed Certifying Authorities; issuing licenses etc.

(iii) Laying down standards to be maintained by the Certifying Authorities: Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 lays down the standards that are to be considered for the functioning of Certifying Authorities.

(iv) Specifying the qualifications and experience which employees and Certifying Authorities should possess: This provision mandates that a system administrator be appointed to oversee that the protective security measure associated with the system are entirely functional and that a network administrator is appointed as an individual responsible for ensuring that the operations are executed properly.

(v) Specifying conditions subject to which the Certifying Authorities conduct their business.

(vi) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of an Electronic Signature Certificate and the public key.[95]

(vii) Specifying the form and content of an Electronic Signature Certificate and the key.

(viii) Specifying the form and manner in which accounts shall be maintained by Certifying Authorities: as per regulation 3 (vi) of the Information Technology (Certifying Authorities) Regulations, 2001, Certifying Authorities are required to comply with the financial mandates and parameters as issued under the Act during the period when the license will stay valid.

(ix) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them: This is to be complied with in sync with Rule 31 and

[95] Gupta, Apar, Commentary on Information Technology Act, 2000, LexisNexis ButterworthsWadhwa Nagpur Publication, Ed. 2, 2011

32 of the Information Technology (Certifying Authorities) Rules, 2000, which in turn lay down the terms of regulating audit and auditor's relationship with Certifying Authorities.

(x) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of systems: As per Rule 19(2) of the Information Technology (Certifying Authorities) Rules, 2000, security guidelines have been laid down to ensure that integrity, confidentiality and availability of data, services and systems of Certifying Authorities are maintained.

(xi) Specifying the manner in which the Certifying Authorities shall conduct dealings with the subscribers: As per regulation 3 of the Information Technology (Certifying Authorities) Rules, 2001, a Certifying Authority is required to use methods which the Controller of Certifying Authorities has approved for the purposes of verifying a subscriber's identity before issuing or renewing any public key.[96]

(xii) Resolving ant conflict of interests between the Certifying Authorities and subscribers: As per Rule 12 of the Information Technology (Certifying Authorities) Rules, 2000, disputes arising between Certifying authorities and subscribers shall be referred for resolution to the Controller of Certifying authorities through arbitration or any other mode of resolution.

(xiii) Laying down the duties of the Certifying Authorities.

(xiv) 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: Rule 22 of the Information Technology (Certifying Authorities) Rules, 2000 makes reference to the database of Certifying Authorities, thereby stating that the Controller shall be required to maintain a database for the disclosure record.

1.4 STATUTORY RESPONSIBILITIES OF CERTIFYING AUTHORITIES

The statutory responsibilities and obligations that Certifying Authorities are legally required to abide by have been laid down in the provisions of the Information Technology Act, 2000:

(a) ***Section 35*** – Certifying Authority to issue Electronic Signature Certificate: This provision addresses that any person who wants to acquire a Digital Signature Certificate

[96] Henery Chan, Raymond Lee, Thoram Dillon, Elizabeth Chang, E-Commerce; Fundamentals and Applications, Wiely India Pvt. Ltd (India), Reprint 2008

can file an application addressing the Certifying Authority requesting the issuance of the certificate in the prescribed manner, coupled with the payment of the requisite application fee which shall not exceed Rs. 25,000/- (Rupees Twenty-Five Thousand only). The provision further mandates for the application to be accompanied by a 'certification practice statement' or any other statement specifying the necessary particulars, in absence of the former. In approval of the application submitted, a Digital Signature Certificate may be issued by the Certifying Authority after making the necessary enquiries, or the application may be rejected with relevant reasons recorded in writing after providing the applicant with an opportunity of showing cause against such rejection of the application.[97]

(b) ***Section 36*** – Representations upon issuance of Digital Signature Certificate: The provision lists down the requisites that a Certifying Authority is legally required to ensure while issuing a Digital Signature Certificate. It is mandated as per the section that –

i. The provisions of the Act, as well as the rules and regulations associated with it, have been complied with while the issuance of the Digital Signature Certificate;
ii. The Digital Signature Certificate has been published or otherwise made available to the applicant and that the applicant has acknowledged the same;
iii. The applicant holds the private key and its corresponding public key as listed in the Digital Signature Certificate;
iv. The applicant holds the private key that creates a digital signature;
v. The public key as listed in the Digital Signature Certificate is capable of verifying the digital signature affixed by the private key that the applicant holds;
vi. The public key and the private key held by the applicant together form a valid and functioning key pair;
vii. The Digital Signature Certificate only contains information that is accurate;
viii. No material fact exists that is potentially capable of adversely affecting the reliability of the aforementioned conditions.[98]

[97] Sharma, Vakul, Information Technology and Practice, Universal Law Publication, 2008
[98] Indira Carr, India joins the cyber-race: Information Technology Act 2000, Int. TJs 2000, 6(4), 122-130, (2000)

(c) ***Section 37*** – Suspension of Digital Signature Certificate: this provision of the act endows upon the Certifying Authority issuing the Digital Signature Certificate the power to suspend such Digital Signature Certificate granted on certain grounds; such as, upon receipt of a request of such suspension of certificate from the person listed as the subscriber in the Digital Signature Certificate or any other person authorised to act on his or her behalf; or in the event the Certifying Authority believes that the suspension of such Digital Signature Certificate shall be in the interest of the public at large. Furthermore, the provision further lays down that unless the subscriber has been given an opportunity of being heard with respect to such suspension of the Digital Signature Certificate, the certificate shall not be suspended for any longer than fifteen days. It further imposes on the Certifying Authority the obligation of communicating to the subscriber all information associated with such suspension of the Digital Signature Certificate.

(d) ***Section 38*** – Revocation of Digital Signature Certificate: This provision addresses instances that could cause the Certifying Authority issuing a Digital Signature Certificate to revoke it. The circumstances in which the Certifying Authority could so revoke a Digital Signature Certificate granted by itself are –

(i) The subscriber of the Digital Signature Certificate making a request of revocation of the certificate granted;

(ii) A person duly authorised by the subscriber of the Digital Signature Certificate making a request of revocation of the certificate granted;

(iii) Upon death or insolvency of the subscriber of the Digital Signature Certificate;

(iv) In instances wherein the subscriber of the Digital Signature Certificate is a firm or a company, the respective dissolution and winding up thereof;

(v) In the event the Certifying Authority issuing the Digital Signature Certificate is of the opinion that incorrect and erroneous information has been represented as material facts in the Digital Signature Certificate;

(vi) In the event the Certifying Authority issuing the Digital Signature Certificate is of the opinion that a material requirement associated with the issuance of the Digital Signature Certificate remains unfulfilled;

(vii) In the event, the Certifying Authority issuing the Digital Signature Certificate is of the opinion that the security system and/or the private key held by the Certifying Authority had been compromised so as to affect the reliability of the Digital Signature Certificate.

The provision, however, emphasises on how the Digital Signature Certificate is not to be revoked without giving its subscriber a reasonable opportunity of being heard. It further imposes on the Certifying Authority the obligation of communicating to the subscriber all information associated with such revocation of the Digital Signature Certificate.[99]

1.5 STATUTORY POWERS OF CONTROLLERS OF CERTIFYING AUTHORITIES

The Information Technology Act, 2000 lays down provisions to address the powers of the Controller of Certifying Authorities in a manner such as follows:

(i) ***Section 27*** – Power to delegate – As per the Act, the Controller shall have the power to authorize the deputy controller of Certifying Authorities, or any other office, in writing, to exercise the powers of the Controller in the same capacity. This provision of the Act is to be ideally read with section 17 thereof, which in turn lays down the organizational structure of the Controller and its team along with the Deputy Controllers, Assistant Controllers and other officers and employees. Nevertheless, in spite of such delegation made by the Controller, the quasi-judicial powers held by the Controller to resolve disputes, if any, between the Certifying Authorities and the subscribers, shall necessarily be retained with the Controller.

(ii) ***Section 28*** – Power to investigate contraventions- Any contravention of the provisions of the Act and/or rules and/or regulations can be taken up for investigation by the Controller or any officer authorized by the Controller. In such event of an investigation, the powers conferred on Income Tax authorities under chapter XIII of the Income Tax Act, 1961, shall apply on the Controller or any other officer authorized by the Controller for the purposes of this provision, however, in accordance with the limitations as laid down under that Act. This power as grated vide this provision is solely investigative in nature. This provision further signifies

[99] Vakul Sharma, Information technology: Law and Practice, Universal Law Publication, Ed. 2, 2008

that the Controller or any other officer authorised by him/her, shall be deemed to have the power to impound and retain in custody documents or books of accounts produced through search or seizure for such period of time that it may deem fit.

(iii)***Section 29*** – Access to computers and data – This provision grants to the Controller or any other person authorized by it broad powers to search and have access to any computer system, apparatus, data connected to such system, etc. solely based upon the reasonable cause to believe that a contravention of the Act or its provisions has been committed.

1.6 CONCLUSION

The provisions of the Information Technology Act, 2000 address the necessity of ensuring that the integrity associated with the system of acquiring and implementing digital signatures is maintained through the delegation of responsibilities amongst various statutory bodies such as Certifying Authorities, Controller of Certifying Authorities, etc. In a world which is going through a dramatic transition that envisages a sea of technological changes which might take extensive sophistication to tackle, it is of utmost importance to ensure that there is due regulation at every stage of action, and that requisite measures have been taken to address any mishap and/or contravention of the ideal provisions laid down as guidelines. In an age where digital signatures are replacing manual signatures, and digital signature certificates are gaining prominence; and public at large are slowly and steadily acknowledging the convenience associated with such change, it is essential that the government ensures that there is enough regulation in place to address instances wherein a misuse or misinterpretation of such nascent and modern technology could take place.[100] It is for this purpose that the Certifying Authorities have been statutorily established, and the Controller of Certifying Authorities have been laid down. Furthermore, the law of the land also ensures that there are specific guidelines established to address the functioning of such authoritative bodies, establish their hierarchy, carve out their responsibilities and powers and in turn create inter-linking of laws for better implementation of such provisions. It is therefore extremely important to learn about the responsibilities, functions and modes of regulating Certifying Authorities as well as Controllers of Certifying Authorities.

[100] VivekSood, Cyber Law Simlpified, Fourth Ed., 2008, Tata McGraw-Hill Publishing Company Ltd

1.7 LET'S SUM UP

In this chapter, we have studied who is a certifying authority along with the regulations and statutory powers under the Information Technology Act, 2000. Finally, we have ended the discussion with the powers given to the certifying authorities.

1.8 FURTHER READING

- http://www.commonlii.org/sg/journals/SGJlIntCompLaw/2003/9.pdf
- Regulation of Certifying Authorities - The Informational Tech. Act, 2008, B.Com, EDUREV.IN (2019), https://edurev.in/studytube/Regulation-of-Certifying-Authorities-The-Informati/74d7d226-f41e-4dfa-97e8-4a9b6bf40993_p?courseId=-1 (last visited Nov 19, 2019).
- Ikram, N. & A., Mahboob,. (2002). Regulatory Issues with Certification Authorities.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Who is a Controller of Certifying Authorities?**

A. A Controller of Certifying Authorities is the entity that supervises the functioning of the Certifying Authorities.

2. **What are the functions of the Controller of Certifying Authorities?**

A. The functions of the Controller of Certifying Authorities inter alia include supervising the functions of the Certifying Authorities, certifying public keys for Certifying Authorities, laying down standards to be maintained and followed by Certifying Authorities etc.

3. **What are the statutory powers of Controller of Certifying Authorities under the existing laws?**

A. The statutory powers of Controller of Certifying Authorities under the existing laws include the power to delegate, the power to investigate contravention of provisions of the act, access to computer data, etc.

4. Which provisions of the Act address the statutory responsibilities of certifying authorities?

A. The provisions of the Act address the statutory responsibilities of certifying authorities are sections 35, section 36, section 37 and section 38.

5. What are the sources of laws, rules and regulations that address the functioning and regulation of Certifying Authorities and Controller of Certifying Authorities?

A. The sources of laws, rules and regulations that address the functioning and regulation of Certifying Authorities and Controller of Certifying Authorities are provisions of the Information Technology Act, 2000, Information Technology (Certifying Authorities) Rules, 2000 and the Information Technology (Certifying Authorities) Regulations, 2001.

1.10 ACTIVITY

Under the IT Act 2000, what are the implications for 'Certifying Authorities'? (800-1000 words)