REGULATION OF CERTIFYING AUTHORITIES

(…continued)

Minny Narang

Aakriti Saini

CERTIFYING AUTHORITY

A) Definition

- According to Section 2(1)(g) of the Act, Certifying Authority is, "a person who has been granted a licence to issue an electronic signature certificate under Section 24."
- Certifying Authorities issue digital signature certificates to the applicant after duly verifying their identity and other details.
- There are 12 licenced certifying authorities in India including Safescrypt, E-Mudhra, (n) Code Solutions, IDRBT, NSDL, CDAC, Capricorn, Vsign, India Air Force, CSC, RISL, and Indian Army CA (IRCA). Safescrypt Ltd. is the first certifying authority in India.

B) Duties of Certifying Authority

1. **Certifying Authority to follow certain procedures (Section 30)-** Every Certifying Authority shall-
   - make use of hardware, software and procedures that are secure from intrusion and misuse;
   - provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

- 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;
- 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.

2. Ensuring compliance of the Act (Section 31)- Every certifying authority must ensure that every person employed or otherwise engaged by it complies with the provisions of this Act, rules, regulations and orders made there under.

3. Display of licence (Section 32)- Every certifying authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

4. Surrender of licence (Section 33)- Every such certifying authority whose licence has been suspended or revoked shall surrender the licence to the Controller.

5. Make certain disclosures (Section 34)-

(i) Every certifying authority shall disclose in the manner specified by regulations-

- its electronic signature certificate;
- any certification practice statement relevant thereto;
- notice of the revocation or suspension of its Certifying Authority certificate, if any; and
- any other fact that materially and adversely affects either the reliability of a electronic signature certificate, or the Authority's ability to perform its services.

(ii)Notice of adverse effects to affected persons- The certifying authority must disclose to the affected persons about any event which may materially and adversely affect the integrity of its computer system or the conditions subject to which an electronic signature certificate was granted.

PROCEDURE RELATING TO ISSUE OF ELECTRONIC SIGNATURE CERTIFICATE (SECTION 35-39)

1. Issue of Electronic Signature Certificate

a) Making of application- Any person may make an application to the Certifying Authority in the prescribed form and accompanied by

- such fee not exceeding Rs. 25000 as may be prescribed by Central Government,and
- a certification practice statement (CPS) or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

b) Grant of certificate- On receipt of an application, the Certifying Authority may after consideration of the certification practice statement and after making such enquiries, grant the electronic signature certificate.

According to Section 36, a certifying authority has to make a declaration while issuing DSC that it has complied with the provisions of this Act and has also fulfilled other obligations to protect the security of public and private keys of the subscribers.

The subscriber is required to convey his acceptance of the digital signature certificate and its conditions, after which the digital signature shall be considered valid.

A digital signature certificate is generally granted for 1 or 2 years, after which it can be renewed.

c) Rejection of application- The certifying authority may reject the application for reasons to be recorded in writing. However, no application shall be rejected unless the applicant has been given a reasonable opportunity of making his representation.

2. **Suspension of Digital Signature Certificate (Section 37)**– The Certifying Authority which has issued a Digital Signature Certificate may suspend such certificate in the following circumstances:

   a) on receipt of a request from the subscriber or any person duly authorized by him;

   b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

   However, such suspension shall not be for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard in the matter. Further, the Certifying Authority shall communicate the suspension of a Digital Signature Certificate to the subscriber.

3. Revocation of Digital Signature Certificate (Section 38)- A Certifying Authority may revoke a Digital Signature Certificate issued by it in the following instances:

(i) on the request of subscriber or of any person duly authorized by him; or

(ii) upon the death of the subscriber; or

(iii) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company

(iv) suo-moto by the certifying authority 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.

A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter. Further, on revocation the Certifying Authority shall communicate the same to the subscriber.

4.Notice of suspension or revocation (Section 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.

DUTIES OF SUBSCRIBERS

- **Definition of Subscriber**

  Section 2(1)(zg) defines subscriber as a person in whose name the electronic signature certificate is issued.

- **Duties of Subscriber**

  Section 40 to 42 of the IT Act prescribes the following duties of subscribers who have obtained electronic signature certificate from a certifying authority:

1. **Generating key pair (Section 40)-** Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the digital signature certificate has been accepted by a subscriber, the subscriber shall generate the key pair by applying the security procedure.

2. Duties of subscriber of Electronic Signature Certificate (Section 40A)- Inserted vide ITAA, this section provides that in respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.

3. Acceptance of Digital Signature Certificate (Section 41)-

(i) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate-

a) to one or more persons;

b) in a repository; or

c) otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(ii) Acceptance of Digital Signature Certificate amounts to certification by the subscriber certifies to all who rely on the information contained therein that–

a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

4. Control of private key (Section 42)- Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and

- Every subscriber shall take all steps to prevent its disclosure.
- If the private key has been compromised then the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified.
- The subscriber shall continue to be liable till he has informed the Certifying Authority that the private key has been compromised.