Regulation of Certifying Authorities

Subject: Commerce

Lesson: Regulation of Certifying Authorities

Course Developer: Nidhi Dhawan

College /Department: Zakir Husan College, University of Delhi

Regulation of Certifying Authorities

Table of Contents

Rationale

Internet is an infrastructure that links hundreds and thousands of networks to one another, that is linking businesses, educational institutions, government agencies and individuals together. In this electronic environment, trust is central to the growth of e-commerce and e-governance; and the future of online transactions and contracts depends upon the trust that the transacting parties place in the security of transmission and the data or content of communication. (http://cca.gov.in)

Figure: Rationale

The working of the computer, computer network and computer system is more process based than personalized, therefore, it is necessary to have an identification strategy, that is, a system of identity authentication is required to ascertain the integrity, confidentiality and authentication of communication channels and processes.

Before starting electronic communications, one must check the following baisc requiremnets viz:

- **Authenticity-** it means that the authenticity of the sender of the message must be determined by the recipient.
- **Message integrity-** It determines, whether the message that has been received is modified, altered or is incomplete.
- **Non-repudiation-** It means the sender cannot deny sending the message.
- **Privacy-**The message must be secure from an unauthorized person.

Electronic environmnet uses digital signature to idetify and prove transactions. A system is required for identity authentication, that has to be in the form of one or more trusted third parties which will not only authenticate that a digital signature belongs to a specific signer, but also dispense the public keys.

The following are the trusted parties enumerated below:

The *"Certifying Authority"*. Issues Digital Signature Certificates by authenticating the subscribers identity.

Digital signatures can be issued by Certifying authority only after obtaining a licence from the *"Controller of Certifying Authorities"* or 'root' certifying authority of India (RCAI).

Regulation of Certifying Authorities

Verification of the digital signatures of issuing certifying authority can also be done through its listed public key in the repository of the controller of certifying authority.

Digital certificates can be issued, published and revoked by certifying authority.

A *Public Key Infrastructure (PKI)* is developed having a set of Certifying Authorities subordinate to the superior Certifying Authorities (controller of certifying authorities)

PKI (Public Key Infrastructure)

Public key infrastructure (PKI) provides for encryption (public key) and digital signature for verifying and authenticating user identities.

The main task of PKI is to secure electronic transactions by making use of various softwares and encryption techniques by combining it with digital signature on network structure, thus providing a secured and trustworthy elctronic environment. PKI must include the items such as public key certificates,updation of public and private keys, a back up of keys and their recoveries, a digital signature certificate repository etc.

PKI involves the following:

According to the Act, PKI icludes the Subscriber (A certificate is used to check the identity of the subscriber); Certifying Authority (Certificate issuer)
Relying party(a party who is relying on the certificate)

From the above, it is clear that double role is to be performed by the certifying authority. (a) It has to issue Digital Certificate to the subscriber and (b) identify and authenticate the subscriber's information on the said certificate for the benefit of the relying party.

Controller Of Certifying Authorities (CCA)

Appointment of Controller and other officers (section 17)

Functions of Controller (section 18)

Recognition of foreign Certifying

Authorities (section 19)

Controller to act as repository (section 20)

License to Certifying Authorities to issue Digital Signature Certificates (Section21)

Regulation of Certifying Authorities

Figure: CCA

Certifying Authority to act as such for the grant of license

- Application for license (section 22)
- Renewal, grant or rejection of license (section 23, section24)
- Suspension for license and its notice (section 25, section 26)
- Powers of CCA (sec27 to 29)

All sections given above are discussed below.
Regulator of the Digital signature infrastructure in India is the Controller of Certifying Authorities (CCA): called the Controller, it primarily acts as an administrative authority rather than quasi- judicial body.

The various provisions relating to this Authority under the IT Act, 2000 are as follows

Section 17 of the Act deals with the Appointment of Controller and other officers

The Central Government appointed the Controller of Certifying Authority on Nov.1, 2000. The office of he Controller of Certifying Authority has three main functional departments (a) Technology (b) Finance and Legal(c) Investigation. Each department has Deputy and Assistant controller, who works under the superintendence and control of the controller of certifying authority.

(1) "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 and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act, subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such, as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller."

Therefore, Section 17 has the following basic ingredients:

Central Government appoints the controller of certifying authority and other officers, who will discharge the duties assigned to them under the Act. It also prescribes the qualifications and terms and conditions of the controller and all other personnel working therein along with the description of the the places at which their Head office and branch office will be located.

Functions of Controller of Certifying Authority

Section 18 of the Act enumerates fourteen functions of the controller. The Controller may perform "all or any" of these functions. Some of the important functions are exercising supervision, certifying public keys and laying down the standards to be maintained by the Certifying Authorities. For the complete lit of the functions of the controller, please refer to the text of the ACT which can be accessed on the following site; http://india.gov.in/outerwin.php?id=http://www.mit.gov.in/content/view-it-act-2000.

Figure: Functions

Section 19 of the Act deals with the Recognition of Foreign Certifying Authorities

According to the section 19 of the Act, the Controller can recognize any foreign authority with the previous approval of central Government. An ACT will recognise all the digital signature certificates issued by such an authority.

Revocation of such a recognition can be done by a Controller by giving notification in writing in the Official Gazette, if any of the condition or restriction, on the basis of which the certificate was issued, was contravened by the authority.

Figure: Foreign Certifying Authorities

Illustration
Trustline Company is recognized as a foreign Certifying Authority, by the Controller of certifying authority, under the Act. Trustline did certain activities, which were not according to the provisions of the Act, on the basis of which, it was working as a certifying authority. Can his recognition be revoked? Controller of certifying authority can revoke the recognition of TrustLine Company as a foreign certifying authority, if it is satisfied that any of the conditions or restrictions has been contravened by the company.

Controller to act as repository

According to section 20 of the Act, all the Digital Signature Certificates will be under control of the controller, i.e., He would be the repository of all the certificates. A controller has all the rights concerning the security and secrecy of all the certificates by making use of any hardware and software that secures them from all the type of hacking and intrusion. Database of all the public keys are maintained by him so that whenever required it can be made avaiable to any member of the public.

A National Repository of Digital Certificates(NRDC) is maintained by the Controller of Certifying Authority containing all the certificates issued by all the certifying authorities from all over the country in which case, public keys are certified by the Controller by using its own private keys enabling the user that a partiicular certificate is issued by a licensed certifying authority.

License to Certifying Authorities to issue Digital Signature Certificates

According to Section 21 of the Act, a license to issue a digital signature certificate can be issued to any person provided he applies for it in a prescribed manner and fulfills all obligations with regard to qualifications, expertise etc. The validity of the license will be as per the terms and conditions and period as prescribed by the ACT. Also, the license is not transferable.

Regulation of Certifying Authorities

Who can apply for grant of license to act as a Certifying Authority (CA)? (http://cca.gov.in)

The following persons can apply to the Controller for grant of license:

- An individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession;
- A company having - Paid up capital of not less than five crores of rupees; and net worth of not less than fifty crores of rupees
- A firm having - Capital subscribed by all partners of not less than five crores of rupees; and net worth of not less than fifty crores of rupees
- Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments

The following parameters related to the grant of license to the subscriber are discussed below:

(A) Application of license
(B) Renewal of license
(C) Suspension of license

(A) Application for license

According to section 22 of the Act, in order to act as a certifying authority, one has to apply in a prescribed format of the Central Government by accompanying the important documents such as certification practice statement, identity document, required fees etc. for the submission of the application.

Figure: License

Illustration
ABC Company, having a paid-up capital of three crores of rupees and a net worth of less than 40 crores of rupees, has applied for the grant of license. Can the license be issued to the ABC Company? The conditions of applying for the grant of license are not met by the company. License cannot be issued.

(B) Renewal of License

According to section 23 of the Act, a renewal of licence application can be made by certfying authority by accompanyig fees as laid in the ACT. A license will be made within forty five days from the date of expiry of the license.

Illustration
PeterX Company, a certifying authority, made an application for the renewal of license in 55 days, after the expiry of the validity of the license. Can the license be renewed? No. Application has to be made by the PeterX Company within forty five days before the date of expiry of the period of validity of the license.

Procedure for grant or rejection of license

According to section 24 of the Act, it is in the hands of the Controller to grant the license or to reject the renewal of license application, in case, if it is not applied in a prescribed manner and not fullfilling all the obligations as mentioned in the ACT. An applicant must have given a reasonable time and opportunity for explaining any default made by him in such a case before the rejection of any such application.

(C) Suspension of license

According to section 25 of the Act, a license can be revoked by a Controller on the basis of the following grounds:

- False information in the application
- Conditions and Standards not met fully
- Contravention of any provision of the ACT

A license cannot be suspended for a period of not more than 10 days and giving a party a reasonable chance to be heard before revoking any such license. If license is revoked on sufficient grounds, then during such a period of suspension, no issue of digital signature certificates can be made by the certifying authority.

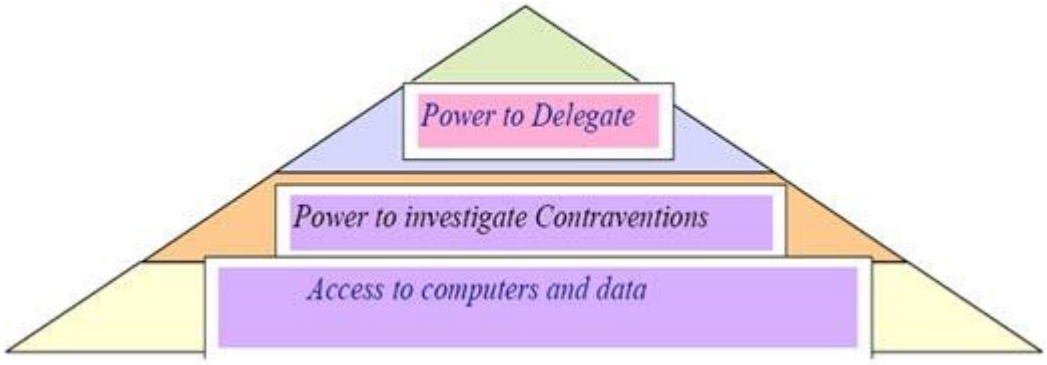
Illustration
Controller of Certifying Authority has revoked the license of Mohan on the basis of failing to comply with the standards specified under the Act without giving the reasonable opportunity of being heard to him. Can the license be revoked? The license will not be suspended for a period exceeding ten days, unless the reasonable opportunity of showing the cause against the proposed revocation is given to him.

Notice of suspension or revocation of license (Sec.26)

According to section 26 of the Act, a notice of suspension or revocation of license is to be made by the controller in all the repositories maintained by him and that is available and can be checked by anyone on a website.

Powers of CCA

According to the Act, following powers have been conferred on the controller of certifying authority. These powers are enumerated as below:



Power to delegate

According to section 27 of the Act, the controller can delegate any of his powers, and may authorize the Deputy and Assistant controller or any officer to exercise the same.

Power to investigate contraventions

According to section 28 of the Act, investigations can be made by the controller or any officer authorised for any contraventions of the provisions of the ACT.

Access to computers and data

According to section 29 of the Act, the controller may have access to any computer resources, computer system of any person to acquire any information, during the course of exercising his duties helpful in further investigations.

Procedure to be followed by CA

Functions and powers of CA

- Certifying Authority to issue Digital Signature Certificate (DSC)
- Representations to be checked while issuing DSC
- Suspension of DSC
- Revocation of DSC

Figure: CA

List of CA Certificates

Certifying Authorities are professional agencies, individuals, or corporate bodies, which possess the technical skills to issue Digital Signature Certificates to those who want to send secure e-records and digital signatures. In India, National Information Center (NIC) and Tata Consultancy Services (TCS) are among the leading certifying authorities.

The IT Act, 2000 has laid down the following Rules as the responsibilities of certifying authority.

Certifying Authorities to follow certain procedures

Section 30 of the Act states that certain procedure need to be followed by the certifying authorities in order to perform its task such as use of necessary hardware and softwares, use of security procedures and laid out standards.

Display of license

According to section 32, every Certifying Authority will display its license at a conspicuous place of the premises in which it carries on its business.

Surrender of license

According to section 33 of the Act, the certifying authority shall surrender the revoked license to the controller immediately, in case of default, he shall be impriisoned for a period upto six months or a fine upto ten thousand ruppes or both.

Illustration
Trust point Services Company is a certifying authority issuing the digital signature certificate, even after the suspension of the license. Is this act allowed under the Act? A person, in whose favor a license is issued, will be imprisoned upto six months or a fine up to ten thousand rupees or both.

Disclosure

Section 34 deals with the disclosure that are expected from the certifying authority. "Every certifying authority will disclose the following factors enumerated below:

- Its Digital Signature Certificate, which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
- Any certification practice statement relevant thereto;
- Notice of the revocation or suspension of its Certifying Authority certificate, if any;
- Any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services".

Functions and power of certifying Authority

According to the ACT, "the following are the functions of certifying authority:
To issue the Digital Signature Certificate (section 35)
To check the representations while issuing digital signature certificate (Section36)
To suspend the digital signature certificate (Section 37)
To revoke the digital signature certificate (Section 38)"

Figure: Functions and power

These functions are discussed as under:

(a) Certifying Authority to issue Digital Signature Certificate

According to section 35, "following steps are required to be followed by the certifying authority to issue digital signature certificate.

- Any person can make an application to the Certifying Authority, for the issue of Digital 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 Central Government to be paid to the certifying authority. Provided that while prescribing fees under sub-section (2), different fees may be prescribed for different classes of applicants.

- 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 under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application".

"No Digital Signature Certificate shall be granted, unless the Certifying Authority is satisfied that-

- The applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
- The applicant holds a private key, which is capable of creating a digital signature;
- 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 applicant".

No application can be rejected unless an applicant has ben heard on that matter and given a reasonable opportunity.

Illustration
Mohan was not granted the Digital Signature Certificate by the Certifying Authority, as he was not holding the private key corresponding to the public key to be listed in the digital signature certificate. His private key was lost. The Certifying Authority can reject the application on this ground, after giving the applicant a reasonable opportunity of showing cause against the proposed rejection.

(b) Representations to be checked while issuing Digital Signature Certificate
According to section 36 of the Act,"a Certifying Authority is required to certify the following, while issuing a digital signature certificate-

1. The Subscriber has complied with the provisions, rules and regulations mad e under the Act;
2. The Digital Signature Certificate has been published and is available to the persons relying on it and accepted by the subscriber;
3. The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
4. The subscriber's public key and private key constitute a functioning key pair;
5. The information contained in the Digital Signature Certificate is accurate; and
6. He 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)".

Illustration
ABC Company, a Certifying Authority, issued a Digital Signature Certificate to Raja. ABC Company must certify that Raja has accepted the digital signature certificate, and holds the private key corresponding to the public key listed in the digital signature certificate.

(c) Suspension of Digital Signature Certificate

According to section 37 of the Act, "the digital signature certificate may be suspended by the certifying authority on two parameters:

- Request fom the subscriber
- Certifying authorities opinion

A reasonable opportunity must be given to the subscriber and the suspension will not be for a period not more than fifteen days in such a case ".

Illustration
Trustline Company, a Certifying Authority suspended the Digital Signature Certificate issued to Mohan in public interest without giving him the opportunity of being heard. Can Trustline Company suspend the Digital signature Certificate this way? Mohan must be given an opportunity of being heard in this matter before the suspension of the digital signature certificate.

(d) Revocation of Digital Signature Certificate

According to section 38 of the Act, "a digital signature certificate may be revoked by the certifying authority on the basis of request made by the subscriber or any person duly authorized to do so or upon the death of the subscriber or upon the dissolution of the firm or winding up of the company, where the subscriber is a firm or a company."

Figure: Revocation

Grounds for the revocation of digital signature certificate by the certifying authority would be the false representation of the facts or cocealment of facts; requirements for the isuue of digital signature certificates not obliged with; security system is affected and relaibility is questioned; the subsciber becomes insolvent and in case of a company, it is wind up.

Illustration
A Certifying Authority has revoked the Digital Signature Certificate of the puja on the ground that the certification practice statement was not accompanied in the application for the issue of the license. A certifying authority can revoke her license in such a case. The same fact must be communicated to her and published in the repository specified in the DSC.

Notice of suspension or revocation

According to section 39 of the Act, "if a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority will 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 asre specified, the Certifying Authority will publish notices of such suspension or revocation, as the case may be in all such repositories.
It is mandatory for the certifying authority to publish a notice of suspension or revocation of digital signature certificates in its repository to maintain the integrity of digital signature certificates and to create the atmosphere of mutual trust between the certifying authority, subscriber and the relying party.
Also, it is mandatory for the certifying authority to make this information relating to the suspension or revocation of digital signature certificates available to the controller for inclusion of the same in the National Repository".

List of Certifying Authority Certificates mtnlTrust Line Public Primary Certification Authority (www.cca.gov.in)

"The following is the list of Certifying Authority Certificates mtnlTrust Line Public Primary Certification Authority

- Safescrypt Time Stamping Authority
- Safescrypt India-RCAI Class
- Tata Consultancy Services Certifying Authority
- NIC Certifying Authority "[6]

Summary

Introduction
It is necessary to have an identification strategy to ascertain the integrity, confidentiality and authentication of communication channels and processes.

For this, system is required in the form of one or more trusted third parties which will not only authenticate that a digital signature belongs to a specific signer but also dispense the public keys.

Trusted Third Party

- Certifying Authority
- Controller of Certifying Authority

Public Key Infrastructure

- It identifies the user by using encryption techniques
- It involves-Subscriber, Certifying authority, Relying Party

Controller of Certifying Authority(CCA)
"Appointment of CCA by Central Government by notification in the Official Gazette. Performs various functions:

- It may with the previous approval of the Central Government recognize any foreign certifying authority;
- Acts as repository of all Digital Signature Certificates; and
- Issues the Digitals Signature Certificate to an applicant for becoming a certifying authority.
- Renewal of license in the format prescribed by the Central Government shall be made not less than forty five days before the expiry of the validity of the license.
- Suspension of license by controller if CA fail to comply with the terms and conditions, subject to which license was granted.
- The Controller shall publish notice of suspension or revocation, as the case may be, in the database maintained by him."

Powers of CCA

- Power to delegate.
- Power to investigate contraventions.
- Access to computers and data.

Certifying Authority
"A certifying authority

- Possess the technical skills to issue Digital Signature Certificate to those who want to secure e-records and digital signatures.
- Observe such other standards as may be specified by regulations.
- Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carries on its business.
- Every Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller".

Functions and power of Certifying Authority

- Issue the Digital Signature Certificate(DSC)
- Check the representations while issuing DSC
- Suspend the DSC

- Revoke the DSC

List of CA Certificates

- mtnlTrustLine Public Primary
- Safescrypt Time Stamping Authority
- Safescrypt India-RCAI Class 3 CA
- Tata Consultancy Services Certifying Authority
- NIC Certifying Authority

References

References to Sections in this chapter are to Information Technology Act, 2000.

Aggarwal. S.K and Singhal.K (2006) *Business & Corporate Law,* Galgotia Publications, New Delhi, India Chapter 28

Kuchhal M.C. (2007) *Business Law*, Vikas Publishing House Pvt. Ltd. Delhi, India, Chapter 31.

Sharma Vakul (2007) *Information Technology Law* and Practice law and emerging technology cyber law and E-commerce, Universal Publishing Company, Delhi, India (Chapter1-9)

Goyal. B.K. (2005) *Business Law,* R.Chand & Co, New Delhi, India, Chapter 35

Sources:

http://www.cca.gov.in
www.google.com
http://www.legalserviceindia.com
http://www.thehindubusinessline.com/mentor/2004/01/19/stories/2004011900171000.htm
http://mapit.gov.in
(www.mcmcse.com)
www200.state.il.us

Refer to bare ACT for the sections and the related site-
http://india.gov.in/outerwin.php?id=http://www.mit.gov.in/content/view-it-act-2000.