Digital Signature Certificate

Sections 35 to 39

Certifying authority to issue Digital Signature Certificate. –

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

(2) 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:

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:

Provided that 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:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

42. Control of private key. –

(1) 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 take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation:- For removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the certifying Authority that the private key has been compromised.

41. Acceptance of Digital Signature Certificate. –

(1) A subscriber shall deemed to have accepted a Digital Signature Certificate is the publishes or authorizes the publication of a Digital Signature Certificate- to one or more person;

in a repository; or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

By accepting a Digital Signature Certificate the subscriber certifies to all who reasonable rely on the information contained in the Digital Signature Certificate that—

the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to h old the same;

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;

all information in the Digital Signature Certificate that is writing the knowledge of the subscriber is true.

36. Representations upon issuance Digital Signature Certificate. –

A Certifying Authority while issuing a Digital Signature Certificate shall certify that- it has complied with the provisions of this Act and the rules and regulations made thereunder;

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

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

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

the information contained in the Digital Signature Certificate is accurate; and

it has no knowledge of any6 material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations in clauses (a) to (d).

37. Suspension of Digital Signature Certificate. –

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate.- on receipt of a request to that effect from-

the subscriber listed in the Digital signature Certificate; or

any person duly authorized to act on behalf of that subscriber;

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.'

38. Revocation of Digital Signature Certificate. –

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

where the subscriber or any other person authorized by him makes a request to that effect; 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.

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 material fact represent in the Digital Signature Certificate is false or had been concealed;

a requirement for issuance of the Digital Signature Certificate was not satisfied;

the Certifying Authority's private key of security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

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.

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

39. Notice of suspension or revocation. –

(1) 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.

40. Generating key pair.-

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, the subscriber shall generate the key pair by applying the security procedure.