

# Digital Signatures & the Indian law

This document is an extract from the book *Ecommerce - Legal Issues* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws



[www.asianlaws.org](http://www.asianlaws.org)

### 3. Digital Signatures - legal issues

The technical concepts relating to digital signatures have been discussed in detail in the previous chapter. Let us take an overview of this concept using a simple illustration.



#### Illustration

Sanya uses a digital signature software (e.g. PGP) installed on her computer, to generate a public and private key pair. Simply put, these keys are very large numbers.

She then stores her private key very securely on her computer. She uploads her public key to the website of a licensed certifying authority (CA). She also courier a filled in application form and photocopies of her passport and Income Tax PAN card to the CA.

After following some verification procedures, the CA sends Sanya a hardware device by post. This device contains Sanya's digital signature certificate. The digital signature certificate contains Sanya's public key along with some information about her and the CA.

Sanya then has to accept her digital signature certificate.

All digital signature certificates are stored in the online repository maintained by the Controller of Certifying Authorities (e.g. at [www.cca.gov.in](http://www.cca.gov.in))

Each Certifying Authority stores digital signature certificates issued by it in an online repository.

In order to digitally sign an electronic record, Sanya uses her private key.

In order to verify the digital signature, any person can use Sanya's public key (which is contained in her digital signature certificate).

In case Sanya had originally generated her private key on a smart card or USB Crypto



Token then the subsequent signatures created by her would be **secure digital signatures**.

**Note:** The smart card / crypto token have a chip built into it, which has technology to enable the signing operation to happen in the device itself. The private key does not come out of the device in its original form.

In case Sanya had generated and stored her private key on a hard disk, floppy, CD, pen drive etc then subsequent signatures are not secure digital signatures.

### 3.1 Authenticating electronic records

#### According to section 3 of the IT Act

3. (1) *Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.*

(2) *The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.*

*Explanation—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—*

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;*
- (b) that two electronic records can produce the same hash result using the algorithm.*

(3) *Any person by the use of a public key of the subscriber can verify the electronic record.*

(4) *The private key and the public key are unique to the subscriber and constitute a functioning key pair.*

Let us examine some of the terms used in this section:

**Subscriber** is a person in whose name the Digital Signature Certificate is issued.

**Authenticate** means "to give legal validity to", "establish the genuineness of".

#### **Illustration**

Pooja has issued a certificate stating that Sameer has been employed in her company for 3 years. Pooja affixes her digital signature to this certificate. Pooja has authenticated the certificate.

**Electronic record** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.





**Affixing digital signature** means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

**Asymmetric crypto system** is a system of using mathematically related keys to create and verify digital signatures. The key pair consists of a **private key** and a **public key**. The private key pair is used in conjunction with a one-way hash function to create digital signatures. The public key is used to verify the digital signatures created by the corresponding private key.

A one-way **hash function** takes variable-length input – say, a message of any length – and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way – even by just one bit – an entirely different output value is produced.


In interpreting this provision, the term “digital signature” must not be compared to “signature” in the conventional sense. This is because although **a person usually has one conventional handwritten signature for all messages**, he will have a **different digital signature for every message** that he signs.

#### Illustration

Mr. Sen writes a message as under:

Dear Mr. Gupta,

I accept the terms and conditions discussed by us today.



Mr. S Sen

**Figure 1: Conventionally signed message**

Here, Mr. Sen’s signature is as marked in the above message. Every document he signs will bear this signature.

However, his digital signature for this message could be

```
iQA/AwUBO0BCsFPnhMicaZh0EQJllgCgt1qtfq
azO2ppYNdZN685h2QtYQsAoOgZ
eH3gqHf5Tisz1C7tzvHC09zx
=g/BR
```

**Figure 2: Digital Signature**

Although his digital signature for the message in Figure 1 is as shown in Figure

2, his digital signature for any and every other message will be different.

E.g. if he changes the word “today” in the message in Figure 1 to “yesterday”, his digital signature for the new message could be:

```
iQA/AwUBO0BDdlPnhMicaZh0EQIOBQCgiu0v  
AT47Q7VJsgQYWU69OtV+MMAoL772XDQB  
vzPYOKSWDS6wjuch01T  
=TSA
```

**Figure 3: New Digital Signature**

What the law implies here is that a person may authenticate an electronic record by means of a digital signature, which is unique to the message being digitally signed.

The public key and private key are basically two very large numbers that are mathematically related to each other. If a particular private key was used to “sign” a message, then only the corresponding public key will be able to verify the “signature”.

The law also lays down that the private key and public key are unique to each subscriber. This implies that no two subscribers should have the same public and private key pair. This is practically achieved by using very large numbers (hundreds of digits) as keys. The probability of two persons generating the same key pair is thus extremely remote.





## 3.2 Secure digital signature

A secure digital signature should satisfy the following conditions:

1. **It should be unique to the subscriber affixing it.** A digital signature is unique and is based upon the message that is signed and the private key of the signer.
2. **It should be capable of identifying such subscriber.** What this implies is that the digital signature should be verifiable by the public key of the signer and by no other public key.
3. **It should be created in a manner or using a means under the exclusive control of the subscriber.** This implies that the signer must use hardware and software that are completely free of any unauthorized external control.
4. **It should be linked to the electronic record to which it relates in such a manner that if the electronic record were altered, the digital signature would be invalidated.** All standard software programs used to create digital signatures contain this feature. Without this feature the whole purpose of creating digital signatures would be defeated.

According to notification G.S.R. 735 (E), notified by the Central Government on the 29<sup>th</sup> of October, 2004, a secure digital signature is one to which the following security procedure has been applied:

- (a) a **smart card**<sup>6</sup> or **hardware token**<sup>7</sup>, as the case may be, with **cryptographic module**<sup>8</sup> in it, is used to create the key pair;
- (b) the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;
- (c) the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;
- (d) the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;

---

<sup>6</sup> a device containing one or more integrated circuit chips.

<sup>7</sup> means a token which can be connected to any computer system using Universal Serial Bus (USB) port.

<sup>8</sup> This can be understood as the software, e.g., PGP, used to generate the key pair used for creating and verifying a digital signature.

- (e) the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;
- (f) the standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and
- (g) the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.







### 3.3 Digital Signature Certificates

Any person can make an application<sup>9</sup> to the Certifying Authority (CA) for the issue of a Digital Signature Certificate.

Each application is required to be accompanied by:

1. The prescribed fee (not exceeding twenty-five thousand rupees) to be paid to the CA.<sup>10</sup>
2. A certification practice statement or a statement containing specified particulars<sup>11</sup>.

On receipt of an application the Certifying Authority may grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application.

A Digital Signature Certificate cannot be granted unless the Certifying Authority is satisfied that:

1. The applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate,
2. The applicant holds a private key, which is capable of creating a digital signature,
3. 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.

The Certifying Authority cannot reject an application unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

#### **Representations upon issuance of Digital Signature Certificate**

While issuing a Digital Signature Certificate a Certifying Authority must certify that:

1. It has complied with the provisions of the IT Act and allied rules.
2. It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it.

---

<sup>9</sup> Schedule IV of the Information Technology (Certifying Authorities) Rules, 2000 prescribes the form for this.

<sup>10</sup> Different fees may be prescribed for different classes of applicants.

<sup>11</sup> As per Executive order dated 12th September 2002 issued by Ministry of Communications and Information Technology every application for the issue of a Digital Signature Certificate shall not be required to be accompanied by a certificate practice statement.

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.
6. It 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 (1) to (4) above.

### **Suspension of Digital Signature Certificate**

The Certifying Authority, which has issued a Digital Signature Certificate, may suspend such Digital Signature Certificate:

1. on a request from the subscriber listed in the Digital Signature Certificate,
2. on a request from any person duly authorized to act on behalf of that subscriber,
3. if it is of opinion that the Certificate should be suspended in public interest.

A Digital Signature Certificate cannot be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate the Certifying Authority shall communicate the same to the subscriber.

### **Revocation of Digital Signature Certificate**

A Certifying Authority can revoke a Certificate issued by it on the:

1. request of the subscriber, or
2. request of any person authorized by him, or
3. upon the death, dissolution or winding up of the subscriber.

A Certifying Authority may revoke a Digital Signature Certificate issued by it at any time, if it is of the opinion that:

1. a material fact represented in the Digital Signature Certificate is false or has been concealed,
2. a requirement for issuance of the Digital Signature Certificate was not satisfied,





3. the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability,
4. the subscriber has been declared insolvent or dead, has been dissolved, wound-up or otherwise ceased to exist.

A Digital Signature Certificate may 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 is required to communicate the same to the subscriber.

**Notice of suspension or revocation**

In case of suspension or revocation of a digital signature certificate, the Certifying Authority is required to publish a notice of such suspension or revocation in the repository specified in the Digital Signature Certificate for publication of such notice.

Where more than one repository has been specified, the Certifying Authority will publish notices of such suspension or revocation in all such repositories.

### 3.4 Duties of subscribers

#### **Generating key pair**

A subscriber must apply relevant security procedure while generating his key pair. The key pair consists of the private key and the public key.

The public key will be sent to the Certifying Authority for inclusion in the subscriber's Digital Signature Certificate.

#### **Acceptance of Digital Signature Certificate**

A subscriber is deemed to have accepted a Digital Signature Certificate if:

1. He publishes the certificate to others or to a repository.
2. He authorises the certificate's publication to others or to a repository.
3. Demonstrates his approval of the Digital Signature Certificate in any manner.

Upon accepting a Digital Signature Certificate the subscriber certifies that:

- ✓ He holds the private key corresponding to the public key listed in the Certificate and is entitled to hold the same,
- ✓ All representations made by him to the Certifying Authority and all material relevant to the information contained in the Certificate are true,
- ✓ All information in the Certificate is true to the best of his knowledge.

#### **Control of private key**

Every subscriber is required to:

1. Exercise reasonable care to retain control of his private key.
2. Take all steps to prevent its disclosure to an unauthorized person.

If this private key has been compromised, then, the subscriber is required to communicate the same without any delay to the Certifying Authority in the prescribed manner.

The subscriber is liable till he has informed the Certifying Authority that his private key has been compromised.





## **3.5 Regulation of Certifying Authorities**

The Information Technology Act empowers the Controller of Certifying Authorities to regulate licenced Certifying Authorities in India.

### **Appointment of Controller and other officers**

The Central Government is empowered to appoint:

1. A Controller of Certifying Authorities,
2. Deputy Controllers and
3. Assistant Controllers.

The Controller is required to discharge his functions subject to the general control and directions of the Central Government.

The Deputy Controllers and Assistant Controllers are required to function under the general superintendence and control of the Controller.

The Central Government is also empowered to prescribe the:

1. qualifications, experience & terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers,
2. places where the Head Office and Branch Office of the office of the Controller are to be located.

### **Functions of Controller**

The Controller is empowered to supervise the activities of the Certifying Authorities (CAs), certify their public keys, lay down the standards to be maintained by them and specify the qualifications and experience, which their employees should possess. The Controller is empowered to specify the following:

1. The conditions subject to which the CAs should conduct their business,
2. The contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key,
3. The form and content of a Digital Signature Certificate and the key,
4. The form and manner in which accounts are required to be maintained by the CAs,
5. The manner in which the CAs are to conduct their dealings with the subscribers, and

6. The terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.

The Controller is also empowered to:

1. facilitate the establishment of any electronic system by a CA (solely or jointly),
2. to regulate such systems,
3. resolve any conflict of interests between the CAs and the subscribers,
4. lay down the duties of the CAs and
5. maintain a database of disclosure records of every CA<sup>12</sup>.

### **Recognition of foreign certifying authorities**

The Controller is authorised to recognize any foreign Certifying Authority as a Certifying Authority for the purposes of the IT Act. However, such approval:

- ✓ requires the previous approval of the Central Government, and
- ✓ is required to be notified in the Official Gazette.

The Digital Signature Certificate issued by a recognized Certifying Authority will be valid for the purposes of the IT Act.

If the recognized foreign Certifying Authority contravenes any of the conditions and restrictions subject to which it was granted recognition, the Controller is empowered to revoke such recognition. The reasons for such revocation are required to be recorded in writing and the revocation is required to be notified in the Official Gazette.

### **Controller to act as repository**

The Controller is the repository of all Digital Signature Certificates issued under the IT Act. To ensure the secrecy and security of the digital signatures, the Controller is required to:

1. make use of hardware, software and procedures that are secure from intrusion and misuse,
2. observe standards prescribed by the Central Government.

The Controller is also required to maintain a computerized database of all public keys. This database should be maintained in such a manner that the public keys are available to any member of the public.

---

<sup>12</sup> This database may contain particulars accessible to the public





### **License to issue Digital Signature Certificates**

A Certifying Authority can make an application, to the Controller, for a license to issue Digital Signature Certificates in India. The person making such an application is required to fulfil the requirements prescribed by the Central Government<sup>13</sup>. Such a license will be:

1. valid for a prescribed period<sup>14</sup>,
2. will not be transferable or heritable and
3. will be subject to specified terms and conditions.

### **Application for license**

The application is required to be in prescribed form<sup>15</sup> and is to be accompanied by:

1. a certification practice statement,
2. a statement including the procedures with respect to identification of the applicant,
3. a prescribed fee,<sup>16</sup>
4. other prescribed documents.<sup>17</sup>

### **Renewal of license**

Section 23 provides that an application for renewal of a license must be:

1. in the prescribed form,
2. accompanied by the prescribed fees,<sup>18</sup>
3. made not less than 45 days before the expiry of the license.

---

<sup>13</sup> See the Information Technology (Certifying Authorities) Rules, 2000

<sup>14</sup> This period is 5 years as per Rule 13(1) of the Information Technology (Certifying Authorities) Rules, 2000

<sup>15</sup> The form is provided in Schedule I of the Information Technology (Certifying Authorities) Rules, 2000

<sup>16</sup> The maximum fees is Rs. 25,000 under Rule 11 of the Information Technology (Certifying Authorities) Rules, 2000

<sup>17</sup> See Rule 10 of the Information Technology (Certifying Authorities) Rules, 2000

<sup>18</sup> Rs. 5,000 as per Rule 11 of the Information Technology (Certifying Authorities) Rules, 2000

### **Procedure for grant or rejection of license**

The Controller is empowered to grant the license or reject the application after considering the documents accompanying the application and such other factors, as he deems fit. However, no application can be rejected unless the applicant has been given a reasonable opportunity of presenting his case.

### **Suspension of license**

The Controller may revoke the license of a Certifying Authority if he is satisfied (after due inquiry) that the Certifying Authority has:

1. made a false or incorrect statement in, or in relation to, the application for the issue or renewal of the license,
2. failed to comply with the terms and conditions subject to which the license was granted,
3. failed to maintain the specified standards,<sup>19</sup>
4. contravened any provisions of the IT Act or allied rules, regulations or orders.

However, no license can be revoked unless the Certifying Authority has been given a reasonable opportunity of **showing cause** against the proposed revocation.

The Controller may suspend the license of a Certifying Authority pending the completion of any inquiry ordered by him. However, no license can be suspended for a period exceeding ten days unless the Certifying Authority has been given a **reasonable opportunity** of showing cause against the proposed suspension.

The Certifying Authority whose license has been suspended **cannot issue** any Digital Signature Certificate during such suspension.

### **Notice of suspension or revocation of license**

Section 26 deals with the notice of suspension or revocation of license. Where the license of the Certifying Authority is suspended or revoked, the Controller is required to publish notice of such suspension or revocation in the database maintained by him.

In the event that one or more repositories are specified, the Controller is required to publish notices of such suspension (or revocation) in all such repositories. The database containing the notice of such suspension (or revocation) is to be made available through a web site accessible round the clock. The Controller may publicize the contents of the database in appropriate electronic or other media.

---

<sup>19</sup> These standards are prescribed under section 20(2)(b) of the IT Act.







### **Power to delegate**

The Controller is authorised to delegate any of his powers to the Deputy Controller, Assistant Controller or any officer.

### **Access to computers and data**

The IT Act contains provisions relating to access to computers and data in the event that the Controller (or any person authorized by him) has reasonable cause to suspect that any **contravention** of the provisions of the IT Act (or allied rules or regulations) has been committed.

In such cases, the Controller can have **access** to any computer system for obtaining any information or data contained in the computer system.

The Controller may order any person in charge of the computer system to provide him with the necessary reasonable **technical and other assistance**.

### **Certifying Authority to follow certain procedures**

Certifying Authorities are required to:

1. make use of hardware, software and procedures that are secure from intrusion and misuse,
2. provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions,
3. adhere to security procedures to ensure that the secrecy and privacy of the digital signature are assured, and
4. observe other specified standards.

### **Certifying Authority to ensure compliance with the Act, etc.**

**Every person** employed or engaged by a Certifying Authority should **comply with the provisions of the IT Act** (and allied rules) in the course of his employment or engagement.

### **Display of license**

Every Certifying Authority is required to **display its license** at a conspicuous place of the premises in which it carries on its business.

### **Surrender of license**

Every CA whose license is suspended or revoked is required to immediately surrender the license to the Controller. Failure to surrender a license is an offence punishable with **imprisonment** up to 6 months and / or **fine** up to Rs 10,000.

## **Disclosure**

Every Certifying Authority is required to disclose the following in the prescribed manner:

1. its Digital Signature Certificate which contains its public key corresponding to the private key used by it to digitally sign another Digital Signature Certificate,
2. certification practice statement,
3. notice of the revocation or suspension of its Certifying Authority certificate, if any,
4. any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which it has issued, or its ability to perform its services.
5. if any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority must:
  - use reasonable efforts to notify any person who is likely to be affected by that occurrence, or
  - act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.





### 3.6 Certifying Authority (Procedure Rules)

The Information Technology (Certifying Authorities) Rules, 2000 were published in the Official Gazette on 17 October 2000 and have come into force from that date.

**Rule 3** provides for the use of public key cryptography to authenticate information by means of digital signatures. **Rule 4** and **Rule 5** contain provisions relating to the creation and verification of digital signatures.

**Rule 6** lays down that the Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards. It also provides the most important standards that may be considered for different activities associated with the Certifying Authority's functions.

These are as under:

	The product	The standard
1	Public Key Infrastructure	PKIX
2	Digital signature certificates and Digital Signature revocation list	X.509. version 3 certificates as specified in ITU RFC 1422
3	Directory (DAP and LDAP)	X500 for publication of certificates and Certification Revocation Lists (CRLs)
4	Database Management Operations	Use of generic SQL
5	Public Key algorithm	DSA and RSA
6	Digital Hash Function	MD5 and SHA-1
7	RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit) PKCS#5 Password Based Encryption Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request PKCS#12 Portable format for storing/transporting a user's private keys and certificates
8	Distinguished name	X.520
9	Digital Encryption and Digital Signature	PKCS#7
10	Digital Signature Request Format	PKCS#10

**Rule 7** provides for the conformance of Digital signature certificates to the ITU X.509 version 3 standard. All digital signature certificates are required to contain the following information:

1. Serial number assigned by Certifying Authority to distinguish it from other certificates
2. Signature Algorithm Identifier, which identifies the algorithm used by Certifying Authority to sign the digital signature certificate,
3. Name of the Certifying Authority who issued the Digital signature certificate,
4. Validity period of the digital signature certificate,
5. Name of the subscriber whose public key the Certificate identifies,
6. Public key information of the subscriber.

**Rule 8** lays down detailed provisions relating to the licensing of certifying authorities. Indian citizens having a capital of five crores of rupees or more and companies having paid up capital of not less than five crores of rupees or net worth of at least rupees fifty crores, may apply for grant of a license to issue Digital signature certificates.

Companies in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of the capital, shall not be eligible for grant of license.

In case a newly formed company (whose main object is to act as Certifying Authority) applies for grant of license, the net worth referred to above will be the aggregate net worth of its majority shareholders holding at least 51% of paid equity capital, being Hindu Undivided Families, firms or companies. These majority shareholders shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company.

The majority shareholders are restricted from selling or transferring equity shares unless the company acquires or has its own net worth of not less than fifty crores of rupees. In other cases the prior approval of the Controller must be acquired for selling or transferring the shares.

A firm having capital subscribed by all partners of not less than five crores of rupees or net worth of not less than fifty crores of rupees may also apply for grant of a license to issue Digital signature certificates. Firms in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, will not be eligible for grant of license.





In the case of a firm that has been registered under the Indian Partnership Act during the preceding financial year or in the financial year during which it applies for grant of license and whose main object is to act as Certifying Authority, the net worth referred to above will be the aggregate net worth of all of its partners (not including non-resident Indians and foreign nationals).

These partners are restricted from selling and transferring capital held in the firm. They can do so if the firm has acquired or has its own net worth of not less than fifty crores of rupees. In other cases the prior approval of the Controller will be needed.

The Central Government or any State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments can also apply for grant of a license to issue Digital signature certificates.

Applicants are required to submit a performance bond or furnish a banker's guarantee from a scheduled bank in favour of the Controller for an amount of not less than rupees five crores. The performance bond or banker's guarantee will remain valid for a period of six years from the date of its submission.

Companies and firms having net worth of rupees 50 crore and above but not having paid up capital of Rs 5 crore or more are required to submit a performance bond or furnish a banker's guarantee for rupees ten crores.

This bond or guarantee may be invoked on suspension of the license, for payment of an offer of compensation made by the Controller, for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority or its employees, for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, or for any other default made by the Certifying Authority.

**Rule 9** provides that the infrastructure associated with all functions of generation, issue and management of digital signature certificates as well as maintenance of Directories containing information about the status, and validity of digital signature certificates will be installed at any location in India.

**Rule 10** provides that every application for a licensed Certifying Authority must be made to the Controller in the prescribed form. The documents and information required to be submitted along with the form include:

1. A Certification Practice Statement (CPS),
2. A statement including the procedures with respect to identification of the applicant,
3. A statement for the purpose and scope of anticipated Digital signature certificate technology, management, or operations to be outsourced,

4. Certified copies of the business registration documents
5. A description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;
6. An undertaking by the applicant that to the best of its knowledge and belief it can and will comply with the requirements of its Certification Practice Statement;
7. An undertaking that the Certifying Authority's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of digital signature certificates are audited by the auditors and approved by the Controller,
8. An undertaking to submit a performance bond or banker's guarantee within one month of the Controller indicating his approval for the grant of license.

**Rule 11** provides for a non-refundable fee of twenty-five thousand rupees to be paid along with the application for grant of license. For renewal of license a non-refundable fee of five thousand rupees is payable. The fee is not refundable in the event of suspension or revocation of the license.

Licensed Certifying Authorities are required to have arrangements for cross certification with other licensed Certifying Authorities within India. Such arrangements have to be submitted to the Controller before the commencement of operations.

**Rule 12** provides that any dispute arising as a result of an arrangement between the Certifying Authorities or between the Certifying Authority and the subscriber must be referred to the Controller for arbitration or resolution.

Provisions relating to licensing, location of facilities, submission of application, fee, cross certification and validity of license shall also apply in the case of an application for renewal of a license.

An application for renewal of license is required to be submitted not less than forty-five days before the date of expiry of the period of validity of license and may be submitted in the form of electronic record.

**Rule 13** lays down that the license issued to a certifying authority will be valid for a period of 5 years from the date of issue and that the license is not transferable.

**Rule 14** empowers the Controller to suspend the license in accordance with the provisions of section 25(2) of the Act.





**Rule 15** contains provisions relating to renewal of the licence of a certifying authority. A certifying authority is required to submit an application for the renewal of its licence at least 45 days prior to the expiry of the validity period of the licence.

**Rule 16** contains provisions relating to Issuance of Licence. The Controller may, within four weeks from the date of receipt of the application grant or renew the licence or reject the application. This period of 4 weeks may be extended to a maximum of eight weeks under special circumstances.

On approval of the application the applicant will be required to submit the performance bond or banker's guarantee within one month from the date of such approval and execute an agreement with the Controller binding himself to comply with the terms and conditions of the licence and the provisions of the Act and the allied rules.

**Rule 17** empowers the Controller to refuse to grant or renew a licence if-

1. The applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or
2. The applicant is in the course of being wound up or liquidated; or
3. A receiver and / or manager have been appointed by the court in respect of the applicant; or
4. The applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or
5. The Controller has invoked performance bond or banker's guarantee; or
6. A Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or
7. A Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or
8. The audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation; or
9. A Certifying Authority fails to comply with the directions of the Controller

**Rule 18** lays down that the Certification Practice Statement of the Certifying Authority will comply with and be governed by Indian laws.

**Rule 19** lays down the security guidelines for Certifying Authorities. Certifying Authorities have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labelling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

The Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are prescribed.

Certifying Authorities shall formulate their own Information Technology and Security Policy, for operation, complying with the guidelines, and submit them to the Controller before commencement of operation. Any change made by the Certifying Authority in the Information Technology and Security Policy is required to be submitted by it within two weeks to the Controller.

**Rule 20** provides that the licensed Certifying Authority will not commence commercial operation of generation and issue of digital signature certificates before -

1. confirming to the Controller the adoption of Certification Practice Statement,
2. generation of its key pair
3. audit of installation of facilities and infrastructure associated with all functions of generation, issue and management of digital signature certificate
4. submission of the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller

**Rule 21** contains provisions relating to the requirements prior to cessation as Certifying Authority. Before ceasing to act as a Certifying Authority, a Certifying Authority is required to give notice to the Controller of its intention to cease acting as a Certifying Authority. The notice has to be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of licence.

The Certifying Authority is also required to advertise his intention sixty days before the expiry of licence or ceasing to act as Certifying Authority in daily newspapers or newspapers specified by the Controller.

The Certifying Authority is also required to notify its intention to the subscriber and Cross Certifying Authority of each unrevoked or unexpired digital signature certificate issued by it.







The notice is required to be given sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital signature certificate, as the case may be. The notice is required to be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post.

The Certifying Authority is also required to revoke all Digital signature certificates that remain unrevoked or unexpired at the end of the ninety days notice period. Such revocation is required irrespective of whether or not the subscribers have requested revocation.

The Certifying Authority is required to make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital signature certificates.

The Certifying Authority is also required to make reasonable arrangements for preserving the records for a period of seven years and to pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital signature certificate) to subscribers for revoking the Digital signature certificates before the date of expiry.

After the date of expiry mentioned in the licence, the Certifying Authority is required to destroy the certificate–signing private key and confirm the date and time of destruction of the private key to the Controller.

**Rule 22** provides that the Controller has to maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority. This database is required to contain the following details:

1. The name of the person / Directors, nature of business, Income-tax Permanent Account Number, web address, if any, office and residential address, location of facilities associated with functions of generation of digital signature certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;
2. The public key(s), corresponding to the private key(s) used by the Certifying Authority and recognized foreign Certifying Authority to digitally sign Digital signature certificate;
3. Current and past versions of Certification Practice Statement of Certifying Authority;
4. Time stamps indicating the date and time of -
  - Grant of licence;

- Confirmation of adoption of Certification Practice Statement and its earlier versions by Certifying Authority;
- Commencement of commercial operations of generation and issue of Digital signature certificate by the Certifying Authority;
- Revocation or suspension of licence of Certifying Authority;
- Commencement of operation of Cross Certifying Authority;
- Issue of recognition of foreign Certifying Authority;
- Revocation or suspension of recognition of foreign Certifying Authority.

**Rule 23** says that the Digital signature certificate can be granted only after a Digital signature certificate application in the form provided by the Certifying Authority has been submitted by the subscriber to the Certifying Authority and the same has been approved by it. The application form is required to contain the prescribed particulars.

The rule further says that no interim Digital signature certificate can be issued and that the digital signature certificate must contain one or more repositories in which revocation or suspension of the Digital signature certificate will be listed, if the Digital signature certificate is suspended or revoked.

The subscriber identity verification method employed for issuance of Digital signature certificate is required to be specified in the Certification Practice Statement of the Certifying Authority.

The rule contemplates situations where a new Digital signature certificate is issued to a person on the basis of another valid Digital signature certificate held by that person.

If subsequently the older Digital signature certificate has been suspended or revoked, the Certifying Authority that issued the new Digital signature certificate is required to conduct investigations to determine whether it is necessary to suspend or revoke the new Digital signature certificate.

The Certifying Authority is required to provide a reasonable opportunity for the subscriber to verify the contents of the Digital signature certificate before it is accepted.

Once a subscriber accepts the issued Digital signature certificate, the Certifying Authority is required to publish a signed copy of the Digital signature certificate in a repository.





If the Digital signature certificate has been issued by the licensed Certifying Authority and accepted by the subscriber, and the Certifying Authority comes to know of any fact that affects the validity or reliability of such Digital signature certificate, it is required to notify the same to the subscriber immediately.

All Digital signature certificates are to be issued with a designated expiry date.

**Rule 24** contains provisions relating to the generation of Digital signature certificates. The process will entail:

1. receipt of an approved and verified Digital signature certificate request,
2. creating a new Digital signature certificate,
3. binding the key pair associated with the Digital signature certificate to a Digital signature certificate owner,
4. issuing the Digital signature certificate and the associated public key for operational use,
5. allotting a distinguished name associated with the Digital signature certificate owner, and
6. using a recognized and relevant policy as defined in the Certification Practice Statement.

**Rule 25** says that before the issue of the digital signature certificate, the Certifying Authority will be expected to:

1. Confirm that the user's name does not appear in its list of compromised users;
2. Comply with the procedure as defined in his Certification Practice Statement including verification of identification and/or employment;
3. Comply with all privacy requirements;
4. Obtain consent of the person requesting the Digital signature certificate, that the details of such Digital signature certificate can be published on a directory service.

**Rule 26** contains provisions relating to the life of a digital signature certificate. A Digital signature certificate has to be granted with a designated expiry date. It expires automatically upon reaching the designated expiry date at which time it must be archived.

It cannot be reused after expiry. The period for which a digital signature certificate has been issued cannot be extended, but a new Digital signature certificate may be issued after the expiry of such period.

**Rule 27** says that Certifying Authorities are required to archive the following for a minimum period of seven years:

1. Applications for issue of digital signature certificates,
2. Registration and verification documents of generated Digital signature certificates,
3. Digital signature certificates,
4. Notices of suspension,
5. Information of suspended digital signature certificates,
6. Information of revoked digital signature certificates,
7. Expired digital signature certificates

**Rule 28** lays down provisions relating to compromise of digital signature certificates. A digital signature certificate is deemed to be compromised when the integrity of the private key associated with it is in doubt or when the Digital signature certificate owner is in doubt, as to the use, or attempted use of his key pairs, or otherwise, for malicious or unlawful purposes.

Digital signature certificates that become compromised while in operational use are to be revoked in accordance with the procedure defined in the Certification Practice Statement. A digital signature certificate can remain in the compromised state for only such time as it takes to arrange for revocation.

**Rule 29** provides for revocation of digital signature certificates. A digital signature certificate may be revoked and become invalid for any trusted use, where –

1. There is a compromise of the digital signature certificate owner's private key;
2. There is a misuse of the digital signature certificate;
3. There is a misrepresentation or errors in the digital signature certificate;
4. The digital signature certificate is no longer required

Revoked digital signature certificates are to be added to the Certificate Revocation List.





**Rule 30** lays down the fees for issue of digital signature certificate. The Central Government can prescribe the fees that Certifying Authorities can charge for the issue of digital signature certificates.

The rule allows Certifying Authorities to levy fees for access to its X.500 directory for certificate downloading, certificate revocation and status information. Certifying Authorities are required to provide an up-to-date fee schedule to all their subscribers and users.

The rule allows publishing of the fee schedule on a nominated web site. No fee can be levied for access to Certification Practice Statement via Internet. Certifying Authorities can charge fees for providing printed copies of their Certification Practice Statements.

**Rule 31** says that Certifying Authorities must get their operations audited annually by an auditor. The audit must include the following:

1. Security policy and planning;
2. Physical security;
3. Technology evaluation;
4. Certifying Authority's services administration;
5. Relevant Certification Practice Statement;
6. Compliance to relevant Certification Practice Statement;
7. Contracts / agreements;
8. Regulations prescribed by the Controller;
9. Policy requirements of Certifying Authorities Rules, 2000
10. Certifying Authorities are also required to conduct half yearly audit
11. Security Policy, physical security and planning of their operations and quarterly audit of their repositories.

Certifying Authorities are required to submit copies of each audit report to the Controller within four weeks of the completion of such audit. In the event that an irregularity is found, the Certifying Authority is required to take immediate appropriate action to remove such an irregularity.

**Rule 32** provides that the auditor has to be independent of the Certifying Authority being audited and cannot be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Certifying Authority.

The auditor and the Certifying Authority are not to have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

**Rule 33** says that the following information must be kept confidential:

1. Digital signature certificate application, whether approved or rejected,
2. Digital signature certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the Digital signature certificate information,
3. Subscriber agreement

**Rule 34** lays down that the access to confidential information, by the operational staff of a Certifying Authority, is to be on a “need-to-know” and “need-to-use” basis. The rule further provides that paper based records, documentation and backup data containing all confidential information as prescribed in rule 33 must be maintained in secure and locked container or filing system, separately from all other records.

The rule further provides that the confidential information is not to be taken out of the country except in a case where a properly constitutional warrant or other legally enforceable document is produced to the Controller and he permits to do so.

**Schedule I** specifies the form for application for grant of licence to be a certifying authority.

**Schedule II** contains Information Technology Security Guidelines.

**Schedule III** contains security guidelines for Certifying Authorities.

**Schedule IV** specifies the form for application for issue of digital signature certificates.

**Schedule IV** contains a glossary of terms.

### **3.7 List of licenced CAs**

The licenced Certifying Authorities in India include:

1. Safescrypt
2. NIC
3. IDRBT
4. TCS
5. MTNL
6. Customs & Central Excise
7. (n)Code Solutions CA (GNFC)

The disclosure records of these Certifying Authorities can be obtained from the website of the Controller of Certifying Authorities at: [www.cca.gov.in](http://www.cca.gov.in)





[www.asianlaws.org](http://www.asianlaws.org)

**Head Office**

6th Floor, Pride Senate,  
Behind Indiabulls Mega Store,  
Senapati Bapat Road,  
Pune - 411016.  
India

**Contact Numbers**

+91-20-25667148  
+91-20-40033365  
+91-20-64000000  
+91-20-64006464

**Email:** [info@asianlaws.org](mailto:info@asianlaws.org)

**URL:** [www.asianlaws.org](http://www.asianlaws.org)