

CA LICENSING GUIDELINES

Version 1.0

March 2017



Controller of Certifying Authorities
Ministry of Communications and Information Technology

Document Control

Document Name	CA LICENSING GUIDELINES
Status	Release
Version	1.0
Last update	20 Mar 2017
Document Owner	Controller of Certifying Authorities, India

Introduction

The CCA issues Licences to Certifying Authorities (CA) under section 24 of the IT Act, after duly processing their applications as provided for under the Act. A Certifying Authority can issue Digital Signature Certificates (DSC) only after being duly licensed by the CCA as per provisions of the IT Act. Before submitting the application, CA technical infrastructure of the applicant should be ready.

Overview of the process followed by the office of CCA on receiving application for grant of licence to operate as a CA under the IT Act

1. Check completeness of application and availability of all supporting documents
2. Ensure that Eligibility Criteria are met by the CA
3. Examine the Certification Practice Statement (CPS) submitted by the CA applicant as per the framework provided at Annexure 1
4. Appointment of empanelled Auditor by CCA for Audit of CA infrastructure (technical, physical and procedural)
5. Examination of Audit report submitted to CCA by the Auditor
6. Grant of "in-principle" approval by CCA if audit report found satisfactory
7. Submission of Bank Guarantee, Undertaking and Certificate Signing Request to CCA by CA applicant
8. Issuance of Public Key Certificate to the CA applicant by CCA
9. Issuance of Paper Licence to CA.
10. Publishing of CA details on the web-site of CCA

Application Form

An application form can be submitted for obtaining a licence to operate as a Certifying Authority (CA) as per section 21 of the IT Act, 2000.

The Form for application for grant of Licence to be a Certifying Authority to be submitted to the Controller, has been prescribed under Rule 10 of the IT Act and appears at Schedule I of the Rules under the IT Act, 2000. The copy of the same is also given in Annexure 2 of these guidelines. The same form is to be used for applying for renewal of licence.

Eligibility Criteria

The eligibility criteria for becoming a CA shall be as per rule 8 of IT (CA) Rules 2000. (Annexure III)

Supporting Documents

Along with the application in the format given in annexure 2, an applicant has to submit all the documents that are essential to substantiate the claim for award of licence to operate as a CA. It is the responsibility of the applicant to submit all documents required under the IT Act, Rules and Regulations.

- (i) Company Profile/Experience of Individuals

- (ii) For an individual, proof of capital of Rs. 5 crores or more in his business or profession
- (iii) For a company/firm,
 - (a) proof of paid-up capital not less than Rs. 5 crores
 - (b) proof of net worth not less than Rs. 50 crores
- (iv) Proof of Equity (Proof that equity share capital held in aggregate by NRIs, FIIs or foreign companies does not exceed 49% of its capital)
- (v) An undertaking to submit Performance Bond or Banker's Guarantee valid for six years from a scheduled bank for an amount not less than Rs. 50 lakhs in accordance with Rule 10(ii)(h) of the IT(CA) Rules.
- (vi) Crossed cheque or bank draft or through NEFT/RTGS(Bank Account Number 604820110000002, IFSC Code BKID0006048, Branch Bank of India, CGO Complex, 6 Electronic Niketan ,NewDelhi-110003) for Rs. 25,000/- (for fresh application) or Rs. 5,000/- (for renewal) in favour of the Pay & Accounts Officer, DIT, New Delhi. Both fees are non-refundable
- (vii) Certified true copies of the company's incorporation, articles of association etc.
- (viii) Original business profile report with certification from Registrar of Companies.
- (ix) Audited accounts for the past 3 years (if applicable).
- (x) The CA's Certification Practice Statement (CPS) as laid down in Annexure I to these Guidelines.
- (xi) Technical specifications of the CA system and CA security policies, standards and infrastructure available/proposed and locations of facilities.
- (xii) Information Technology and Security Policy proposed to be followed by the CA in its operations under rule 19 of IT(CA) rules.
- (xiii) Statement addressing the manner in which the CA shall comply with the requirements stipulated in the IT Act, Rules and Regulations.
- (xiv) Organisational chart and details of all trusted personnel.
- (xv) Date by which the applicant will be ready for audit to start. The application shall be deemed to have been received on this date for processing purposes.
- (xvi) Date by which commencement of CA operations is proposed. Operations can only commence after due compliance with Rule 20 of IT(CA) rules.
- (xvii) An undertaking by the applicant that they will make payment to the Auditor appointed by the CCA at the rate to be prescribed by the CCA.

The Controller reserves the right to call for any other information that may be required to process the application.

Note:

The application for licence to operate as a Certifying Authority, including all supporting documents, must be submitted in duplicate. These should be in the form of two identical sets numbered 1 and 2.

CPS

The CA Certification Practice Statement (CPS) should state how the PKI component(s) meet the assurance requirements. The CA's Certification Practice Statement (CPS) should be prepared as per the CPS framework laid down in Annexure I to these Guidelines

Cryptographic site preparation

Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are given in Schedule II and Schedule III respectively. The information on physical site can be seen in CA site preparation Guidelines published on the website.

Terms and conditions for Licence

A licence issued to a CA will be subject to terms and conditions under Section 21(3)(c). The detailed Terms and Conditions are available in Regulation 3 of the Regulations under the IT Act, 2000.

Processing of an Application

On receipt of an application, the application and supporting documents/information will be examined in the office of the CCA with regard to the financial parameters as well as in respect of the information supplied by the applicant in the CPS and other documents. The financial parameters will be examined by the office of the CCA for compliance with all relevant stipulations in the IT Act. The remaining information, on successful completion of desk evaluation of legal, regulatory, technical & infrastructural requirements in the office of the CCA, will be handed over for auditing to one of the Auditors empanelled for this purpose by the office of the CCA. Audit will be carried out by the Auditor within the ambit of the Terms & Conditions stipulated by the CCA. The applicant will be informed about the Auditor deputed to carry out the audit. The audit report has to be submitted to the CCA by the Auditor within 21 Days from the commencement of Audit. Based on the audit report, the results of the financial evaluation, and on the applicant's meeting all technical, financial, infrastructural, legal and regulatory requirements, the CCA will decide whether a Licence is to be issued to the applicant or not. Any shortcomings in conformance as indicated by the Auditor, will be notified to the applicant who will be expected to correct the same and report to the CCA. If the non-conformance is major, then a fresh audit evaluation may be scheduled at a mutually agreed time.

Licence Issuance

On successful completion of evaluation of the application for grant of Licence with respect to qualification, expertise, manpower, financial resources other infrastructural facilities and legal and regulatory requirements, the CCA will commence the process of issuance of Licence. Each Licence issued will be accompanied by a public key certificate digitally signed by the CCA. The licence is valid for a period of five years from the date of its issue and is not transferable

Information in Licence

The paper licence issued by the CCA includes the following :

- Licence serial no.
- Name of the CA
- Address
- Date of issue
- Valid until
- Public Key

The format for the Licence Serial no. is as follows:

YYYYXXXDDMMYYNNMMMMZZ (24 characters)

With the following composition

YYYY	-	Year of issuance
XXXX	-	Serial Number allotted to CA (serialized based on order of receipt of application)
DDMMYY	-	Valid until date (DD)/ month (MM)/ year (YY)
NNN	-	000 - Primary Licence 001, 002 etc. - Incremented for each key submitted by the CA for certification. This will be indicated by the CA in their application.

MMMM - **0000** - **in case of fresh licence**

ZZZ - **Reserved for future use** yyyy - year of renewal

Circumstances for Suspension & revocation of License

Suspension of Licence

Licences can be suspended by the CCA under Section 25 of IT Act. The CCA shall suspend a Licence if the CCA has reasons to believe that the CA has

- made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;
- failed to comply with the terms and conditions subject to which the licence was granted;
- contravened any provisions of the IT Act, Rule, Regulation or orders made thereunder,
- Failed to maintain the procedures and standards specified in section 30 of IT Act.

The licence granted to the persons referred to in clauses (a) to (c) of sub-rule (1) of rule 8 of IT(CA) rules shall also stand suspended when the performance bond in the form of banker's guarantee furnished by such persons is invoked under sub-rule (2) of that rule.

An investigation into the need for suspension will take place by which validate the need for suspension and obtaining authorisation for the suspension. On completion of investigation into need for suspension, either License will be further suspended or reinstated as valid.

Pending completion of any inquiry ordered by the CCA during this suspension, CA will issue not issue any certificates.

Revocation of Licence

Licence issued by the CCA can remain suspended for a maximum period of ten working days. Upon termination or prior to termination of suspension, CCA will determine whether it should be revoked or reinstated as valid. The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder. If on completion of the inquiry, any of the above is established beyond doubt then the Licence may be revoked by the CCA. An Authorized signatory of the Licensed CA can also request for revocation

Audit

The CA will have its operations audited

- Annually by an Auditor empanelled by the CCA
- Half-yearly by an internal audit team

The overall scope of the audit will be as follows, however the applicability of the scope may be depends on fresh Licence or renewal of Licence or yearly audit or services offered by CA.

- (i) Security policy and planning;
- (ii) Physical security;
- (iii) Technology evaluation;
- (iv) Certifying Authority's services administration;
- (v) Relevant Certification Practice Statement;
- (v) Compliance to relevant Certification Practice Statement;
- (vi) Contracts/agreements;
- (vii) Regulations prescribed by the Controller;
- (ix) Policy requirements of Certifying Authorities Rules, 2000.
- (x) Adherence to IT Act, 2000, the Rules and Regulations thereunder and Guidelines issued by Controller from time to time.
- (xi) Compliance of Verification method, Services and DSCs to relevant Guidelines issued by Controller based on the sample provided to Auditors
- (xiii) The subject matter or specific cases as provided by Controller
- (xiv) Audit in respect of Web trust operating standards.

The audit report will be submitted to the Controller within 21 days after of such audit and where irregularities are found, the Certifying Authority shall take immediate appropriate action to remove such irregularities.

In the case of the audit after the cessation of CA operation for a period of seven years, the availability and usability of records of DSC issuance , CRL generation and DSC application forms shall be mandatorily included in the audit apart from other requirements under IT Act

Renewal of licence before expiry

The application for renewal of Certifying Authority's licence shall be submitted before 45 days of expiry of licence. The process for the renewal of Licence will be similar to fresh licence in respect of audit and supporting documents.

The Controller may refuse to grant or renew a licence any of the provisions under IT(CA) Rules rule 17.

Re-location of CA Site

The guideline lines for shifting site of CA Operations is in the annexure IV

CERTIFICATION PRACTICE STATEMENT

The CPS framework given below is based on *RFC-2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. All the components listed in the framework must be specified in the CPS.

GENERAL PROVISIONS

This component specifies any applicable presumptions on a range of legal and general practice topics and shall contain,-

(a) Obligations

This sub-component shall contain the type of entity, the provisions relating to the entity's obligations to other entities and may include:

1. Certifying Authority (CA) obligations,
2. Subscriber obligations,
3. Relying party obligations,
4. Repository obligations

(b) Liability

This sub-component shall contain provisions regarding apportionment of liability for each type of entity such as, -

1. Warranties and limitations on warranties;
2. Kinds of damages covered (e.g., indirect, special, consequential, incidental, punitive, liquidated damages, negligence and fraud) and disclaimers;
3. Loss limitations (caps) per certificate or per transaction;
4. Other exclusions (e.g., Acts of God, other party responsibilities, etc).

(c) Financial Responsibility

This sub-component shall consist of provisions relating to financial responsibilities of the Certifying Authority and repository such as:

1. Indemnification of Certifying Authority by relying parties;
2. Fiduciary relationships (or lack thereof) between the various entities;
3. Administrative processes (e.g., accounting, audit, etc.).

(d) Interpretation and Enforcement

This sub-component will contain provisions relating to the interpretation and enforcement of the Certificate Policy and the Certification Practice Statement and shall address the following topics:

1. Governing laws;
2. Severability of provisions, survival, merger, and notice; and
3. Dispute resolution procedures.

(e) Fees

This sub-component shall consist of provisions relating to the fees charged by the Certifying Authorities and repositories such as:

1. Certificate issuance or renewal fees;
2. Certificate access fee;
3. Revocation or status information access fee;
4. Fees for other services such as policy information; and
5. Refund policy.

Note.-

- (i) In respect of issuance, renewal, access, revocation and status information the fee structure shall be based on the class of certificate.
- (ii) The different classes of certificates issued must be specified.
- (iii) The details of Classes are as given in the in the section 1.2 Document Identification of X.509 Certificate Policy for India PKI. CAs will issue DSCs with assurance classes only in accordance with X.509 Certificate Policy for India PKI.

(f) Publication and Repositories

This sub-component shall contain all applicable provisions regarding:

1. Certifying Authority's obligations to publish information regarding its practices, its certificates, and the current status of such certificates;
2. Frequency of publication;
3. Access control on published information objects including certificate policy definitions, Certificate Practice Statements, certificates, certificate status, and CRLs; and
4. Requirements pertaining to the use of repositories operated by Certifying Authorities or by other independent parties.

(g) Compliance Audit

This sub-component shall contain the following information:

1. Frequency of compliance audits for each entity;

2. Identity/qualifications of the auditor;
3. Auditor's relationship to the entity being audited;
4. List of topics covered under the compliance audit;
5. Actions taken as a result of a deficiency found during compliance audit;
6. Compliance audit results: with whom they are shared with (e.g. Certifying Authorities and/or end entities), who provides them, auditors and how they are audited and how the audits are communicated.

(h) Policy of Confidentiality

This sub-component will address the following:

1. Types of information that must be kept confidential by Certifying Authority;

2. Types of information that are not considered confidential;
3. Who is entitled to be informed of reasons for revocation and suspension of certificates
4. Policy on release of information to law enforcement officials;
5. Information that can be revealed as part of civil discovery;
6. Conditions upon which Certifying Authority may disclose upon owner's request; and
7. Any other circumstances under which confidential information may be disclosed.

(i) Intellectual Property Rights

This sub-component shall consist of ownership rights of certificates, practice/policy specifications, names, and keys.

IDENTIFICATION AND AUTHENTICATION

This component will describe the procedures used to authenticate a certificate applicant to a Certifying Authority prior to certificate issuance. It will also describe how parties requesting re-key or revocation are authenticated. It will contain naming practices, including recognition of name ownership and name dispute resolution.

This component will have the following sub-components:

- (a) Initial Registration;
- (b) Routine Re-key;
- (c) Re-key After Revocation; and
- (d) Revocation Request.

OPERATIONAL REQUIREMENTS

This component will specify requirements imposed upon issuing Certifying Authority or end entities with respect to various operational activities and will contain the following sub-components:

- (a) Certificate Application;
- (b) Certificate Issuance;
- (c) Certificate Acceptance;
- (d) Certificate Suspension and Revocation;

- (e) Security Audit Procedures;
- (f) Records Archival;
- (g) Key Changeover;
- (h) Compromise and Disaster Recovery; and

- (i) Certifying Authority Termination/Suspension.

PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

- (i) This component will describe the matters relating to non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing Certifying Authority to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.
- (ii) This component can also be used to define non-technical security controls on repository and end entities.
- (iii) These non-technical security controls are critical to trusting the certificates since lack of security may compromise Certifying Authority operations resulting, for example, in the creation of certificates or CRLs with erroneous information or the compromise of the Certifying Authority private key.

This component will consist the following three sub-components:

- (a) Physical Security Controls;
- (b) Procedural Controls; and
- (c) Personnel Security Controls.

TECHNICAL SECURITY CONTROLS

- (i) This component will be utilized to define the security measures taken by the issuing Certifying Authorities to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually held key shares). This component may also be used to impose constraints on repositories and end entities to protect their cryptographic keys and critical security parameters. Secure key management is critical and the component will ensure that all secret and private keys and activation data are protected and used only by authorized personnel.
- (ii) This component will also contain other technical security controls used by the issuing Certifying Authority to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, audit, and archival. Technical controls will include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.
- (iii) This component can also be used to define other technical security controls on repositories and end entities.

This component shall have the following sub-components:

- (a) Key Pair Generation and Installation;
- (b) Private Key Protection;
- (c) Other Aspects of Key Pair Management;
- (d) Activation Data;
- (e) Computer Security Controls;
- (f) Life-Cycle Security Controls;
- (g) Network Security Controls; and

- (h) Cryptographic Module Engineering Controls.

CERTIFICATE AND CRL PROFILES

This component will specify the certificate format and, if CRLs are used, the CRL format. Assuming use of the X.509 certificate and CRL formats, this includes information on profiles, versions, and extensions used.

This component will have two sub-components:

- (a) Certificate Profile; and
- (b) CRL Profile.

SPECIFICATION ADMINISTRATION

This component will contain the specifications as to how particular certificate policy definition or CPS will be maintained and shall contain the following sub-components:

- (a) Specification Change Procedures;
- (b) Publication and Notification Procedures; and
- (c) CPS Approval Procedures.

OUTLINE OF A SET OF PROVISIONS

This component will contain outlines for a set of provisions, intended to serve as a checklist or a standard template for use by certificate policy or CPS writers. Such an outline will facilitate:

- (a) Comparison of two certificate policies during cross-certification (for the purpose of equivalency mapping).
- (b) Comparison of a Certificate Practice Statement with a certificate policy definition to ensure that the CPS faithfully implements the policy.
- (c) Comparison of two Certificate Practice Statements.

Form for Application for grant of Licence to be a Certifying Authority

For Individual

1. Full Name *

Last Name/Surname

First Name

Middle Name

2. Have you ever been known by any other name? If Yes,

Last Name/Surname

First Name

Middle Name

3. Address

A. Residential Address *

Flat/Door/Block No

Name of Premises/Building/Village

Road/Street/Lane/Post Office

Area/Locality/Taluka/Sub-Division

Town/City/District

State/Union Territory

Pin

Telephone No

Fax

Mobile Phone No.

B. Office Address *

Name of Office

Flat/Door/Block No.

Name of Premises/Building/Village

Road/Street/Lane/Post Office

Area/Locality/Taluka/Sub-Division

Town/City/District

State/Union Territory

Pin :

Telephone No.

Fax

4. Address for Communication *

Tick ✓ as applicable A

or B

5. Father's Name *

Last Name/Surname

First Name

Middle Name

6. Sex * (For Individual Applicant only) Tick ✓ as applicable : Male/ Female

7. Date of Birth (dd/mm/yyyy) * _____/_____/_____

8. Nationality *

9. Credit Card Details

Credit Card Type

Credit Card No.

Issued By

10. E-mail Address

11. Web URL address

12. Passport Details #

Passport No.

Passport issuing authority

Passport expiry date (dd/mm/yyyy) _____/_____/_____

13. Voter's Identity Card No. #

14. Income Tax PAN No. #

15. ISP Details

ISP Name *

ISP's Website Address, if any

Your User Name at ISP, if any

16. Personal Web page URL address, if any

17. Capital in the business or profession * Rs .

(Attach documentary proof)

For Company/Firm/Body of Individuals/Association of Persons/Local Authority

18. Registration Number * _
19. Date of Incorporation/Agreement/Partnership * _____/_____/_____
20. Particulars of Business, if any: *
- Head Office
 - Name of Office
 - Flat/Door/Block No.
 - Name of Premises/Building/Village
 - Road/Street/Lane/Post Office
 - Area/Locality/Taluka/Sub-Division
 - Town/City/District Pin
 - State/Union Territory
 - Telephone No.
 - Fax
 - Web page URL address, if any
 - No. of Branches
 - Nature of Business
21. Income Tax PAN No. *
22. Turnover in the last financial year Rs .
23. Net worth * Rs .
(Attach documentary proof)
24. Paid up Capital * Rs .
(Attach documentary proof)
25. Insurance Details
- Insurance Policy No. *
 - Insurer Company *
26. Names, Addresses etc. of Partners/Members/Directors (For Information about more persons, please add separate sheet(s) in the format given in the next page) *
- No. of Partners/Members/Directors
- Details of Partners/Members/Directors
- A. Full Name
 - Last Name/Surname
 - First Name
 - Middle Name
 - B. Address
 - Flat/Door/Block No.
 - Name of Premises/Building/Village

Road/Street/Lane/Post Office

Area/Locality/Taluka/Sub-Division

Town/City/District

State/Union Territory Pin

Telephone No.

Fax No.

Mobile Phone No.

C. Nationality

In case of foreign national, Visa details

D Passport Details #

Passport No.

Passport issuing authority

Passport expiry date

E. Voter's Identity Card No. #

F. Income Tax Pan No. #

G. E-mail Address

H. Personal Web page URL, if any

27. Authorised Representative *

Name

Flat/Door/Block No.

Name of Premises/Building/Village

Road/Street/Lane/Post Office

Area/Locality/Taluka/Sub-Division

Town/City/District

Pin

State/Union Territory

Telephone No.

Fax

Nature of Business

36. Any other information

Date

Signature of the Applicant

- Instructions :
1. Columns marked with * are mandatory.
 2. For the columns marked with #, details for at least one is mandatory.
 3. Column No. 1 to 17 are to be filled up by individual applicant.
 4. Column No. 18 to 27 are to be filled up if applicant is a Company/Firm/Body of Individuals/Association of Persons/Local Authority.
 5. Column No. 28 is to be filled up if applicant is a Government organisation.
 6. Column Nos. 29,30,31 and 34 are to be filled by all applicants .
 7. Column No. 32 is applicable for application for renewal of licence
 8. Column No. 32 is applicable if applicant is a Government organisation

Eligibility Criteria

IT(CA), Rule (8): .Licensing of Certifying Authorities.—(1) The following persons may apply for grant of a licence to issue Digital Signature Certificates, namely:—

(a) an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession;

(b) a company having—

(i) paid-up capital of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees:

Provided that no company 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 its capital, shall be eligible for grant of licence:

Provided further that in a case where the company has been registered under the Companies Act, 1956 (1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least 51% of paid equity capital, being the Hindu Undivided Family, firm or company:

Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company:

Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity shares held in such company—

(i) unless such a company acquires or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Controller;

(c) a firm having—

(i) capital subscribed by all partners of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees:

Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of all of its partners:

Provided also that the partners referred to in the second proviso shall not include Non-resident Indian and foreign national:

Provided also that the partners of a firm referred to in the second proviso whose net worth has been determined on the basis of such partners, shall not sell or transfer its capital held in such firm—

- (i) unless such firm has acquired or has its own net worth of not less than fifty crores of rupees;
- (ii) without prior approval of the Controller;

(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation.—For the purpose of this rule,—

- (i) "company" shall have the meaning assigned to it in clause 17 of section 2 of the Income-tax Act, 1961 (43 of 1961);
- (ii) "firm", "partner" and "partnership" shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression "partner" shall also include any person who, being a minor has been admitted to the benefits of partnership;
- (iii) "foreign company" shall have the meaning assigned to it in clause (23A) of section 2 of the Income-tax Act, 1961 (43 of 1961);
- (iv) "net worth" shall have the meaning assigned to it in clause (ga) of sub-section (1) of section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986);
- (v) "Non-resident" shall have the meaning assigned to it as in clause 26 of section 2 of the Income-tax Act, 1961 (43 of 1961).

Guidelines for shifting site of CA Operations

1. Any Certifying Authority which intends to change the site of its operations, either Primary site or Disaster Recovery site, must inform the Office of CCA 45 days in advance (before proposed date of shifting). The location and address of the new site must be provided along with the layout plan of the facilities at the proposed site.
2. The selection of the new site by the Certifying Authority should be made keeping in view the requirements specified in the document 'CA Site Specification' published on the website of CCA. The physical infrastructure at the proposed site will have to be audited by an Auditor empanelled with the Office of CCA. The Auditor will be appointed by the Office of CCA.
3. In-principle approval for the shifting will be provided by the Office of CCA after receiving a satisfactory report on the audit of physical infrastructure at the proposed site, till which time operations at old site should continue.
4. After obtaining in-principle approval from the Office of CCA, shifting of technical infrastructure will be undertaken. The Certifying Authority must get the audit of the technical infrastructure at the new site done by an empanelled auditor. The auditor will be appointed by the Office of CCA . The audit report submitted by the Auditor will be examined by the Office of CCA and after ascertaining compliance, approval for starting operations at the new site will be given by the Office of CCA to the Certifying Authority.
5. The shifting and audit of the technical infrastructure at the new site should be completed in a time frame so as to ensure that the operations at the new site commences within 45 days of its closure at the old site.

* * * * *