CA LICENSING GUIDELINES

Version 2.1

01 April 2024

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	CA LICENSING GUIDELINES
Status	Release
Version	2.1
Last update	01 April 2024
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.

The potential CA aspirants should consult & present the business plan, location of facilities, expertise etc to the Office of CCA before submitting the application & fee, construction of technical infrastructure etc. The CA Licence application shall be received only after the satisfactory clearance of the business plan.

Before submitting the application, the CA technical infrastructure of the applicant should be ready.

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

1. Check the completeness of the 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 in Annexure 1(detail in the CPS template published at cca.gov.in)
4. Audit of CA infrastructure (technical, physical and procedural) and CA software(CA & website) by the auditor empanelled by CCA
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 website of CCA

Application Form

An application form can be submitted for obtaining a license 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 in Schedule I of the Rules under the IT Act, 2000. A 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 license.

Eligibility Criteria

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

Note: In the case of renewal, The condition in the second proviso of 8(b) (ii)&second

proviso of 8(b) will not be applicable

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 the award of a 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 a 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, MeitY, 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 the 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) The organizational chart and details of all trusted personnel.

(xv) Date by which the applicant will be ready for the 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.

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

to process the application.

Note:

The application for a 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 also in line with CPS template published on the website of CCA

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 the physical site can be seen in the **CA site preparation Guidelines** published on the website.

Terms and conditions for Licence

A license 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 with respect to 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. The 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 the 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.

License 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:

YYYYXXXXDDMMYYNNNMMMMZZZ (24 characters)

With the following composition

YYYY	-	Year of issuance		
XXXX	-	Serial Number allotted to CA (based on the 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 a fresh license

yyyy - year of renewal

ZZZ - Reserved for future use

Circumstances for Suspension & revocation of License

Suspension of Licence

Licences can be suspended by the CCA under Section 25 of the 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 the 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 which validate the need for suspension and obtain authorisation for the suspension. On completion of an investigation into the need for suspension, either the License will be further suspended or reinstated as valid.

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

Revocation of Licence

The 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 on 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

1. **The CA will have its operations audited**
    - Annually by an Auditor empanelled by the CCA
    - Annually by a Cert-IN empanelled auditor
    - Half-yearly by an internal audit team

The overall scope of the audit will be as follows, however, the applicability of the scope may depend on a 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 with relevant Certification Practice Statement;
(vi)Contracts/agreements;
(vii) Regulations prescribed by the Controller;
(ix) Policy requirements of Certifying Authorities Rules, 2000.
(x) Adherence to the IT Act, 2000, the Rules and Regulations thereunder and Guidelines issued by the Controller from time to time.
(xi) Compliance of Verification method, Services, and DSCsto relevant Guidelines issued by the Controller based on the sample provided to Auditors
(xiii) The subject matter or specific cases as provided by the Controller
(xiv) Audit with respect to Web trust operating standards.
(xv) Security Evaluation Requirements as per Annexure VI
(xvi) CA Software, and website requirements as per Annexure V
(xvii) Financial Status Verification as per Annexure VIII

The audit report will be submitted to the Controller within 21 days after 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

2. **SSL CA**

Notwithstanding the requirements mentioned for a Licenced CA, if the CA setup is only for the purpose of issuance of SSL& code signing certificates, the CPS, CP, manpower, technical, physical, procedural, and audit requirements of the CA shall be in line with Webtrust/CAB Forum guidelines to enable enrollment in browser forum guidelines, however, organizational and financial requirements shall be as per the provisions under the IT Act.

Renewal of licence before expiry

The application for renewal of the Certifying Authority's licence shall be submitted 45 days before the expiry of the licence. The process for the renewal of the Licence will be similar to a 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 for shifting the site of CA Operations is in Annexure IV

****

ANNEXURE I

CERTIFICATION PRACTICE STATEMENT

The CPS framework given below is based on *RFC-2527: Internet X.509 Public KeyInfrastructure 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, and 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 section 1.2 Document Identification of X.509 Certificate Policy for India PKI. CAs will issue DSCs with assurance classes only in accordance with the 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 before 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 of 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, and 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 the 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.

ANNEXURE II

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 TerritoryPin :
   - 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 the case of foreign nationals, 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 _____

For Government Ministry/Department/Agency/Authority

28. Particulars of Organisation: *

Name of Organisation

Administrative Ministry/Department

Under State/Central Government

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 No.

Web page URL Address

Name of the Head of Organisation

Designation

E-mail Address

29. Bank Details

Bank Name *

Branch *

Bank Account No. *

Type of Bank Account *

30. Whether bank draft/pay order for licence fee enclosed * : Y / N ,
If Yes

Name of Bank

Draft/pay order No.

Date of Issue

Amount

31. Location of facility in India for generation of Digital Signature Certificate *

32. Public Key @

33. Whether undertaking for Bank Guarantee/Performance Bond attached * : Y / N
(Not applicable if the applicant is a Government Ministry/Department/Agency/ Authority)

34. Whether Certification Practice Statement is enclosed * : Y / N

35. Whether certified copies of business registration document are enclosed: Y / N (For Company/Firm/Body of Individuals/Association of Persons/Local Authority) If yes, the documents attached:

ii) .....

iii) .....

iv) .....

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. Columns No. 1 to 17 are to be filled up by individual applicants.
4. Columns No. 18 to 27 are to be filled up if the applicant is a Company/Firm/Body of Individuals/Association of Persons/Local Authority.
5. Column No. 28 is to be filled up if the 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 the applicant is a Government organisation

ANNEXURE III

Eligibility Criteria

IT(CA), Rule (8):.Licensing of Certifying Authorities.—(1) The following persons may apply for the 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 a 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 Indians, foreign nationals, Foreign Institutional Investor and foreign companies:

Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined based on 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 a 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).

ANNEXURE IV

Guidelines for shifting site of CA Operations

1. Any Certifying Authority which intends to shift the CA site of its operations, either Primary site or Disaster Recovery site, must inform the Office of CCA 45 days in advance (before the 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.

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 the 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 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 commence within 45 days of its closure at the old site.

Annexure V

Compliance Requirements for the Applicant Software System, CA Software and Website

1. Compliance Requirements for the Applicant system.

The applicant software provides external access to users. The compliance requirements for the software are below.

S.NO	Control	Compliance(Y/N)
The applicant interface software		
1.	The verification requirements shall be as per CCA-IVG. The applicant software should have strictly implemented the functions as mentioned in the Guidelines issued by CCA	
Audit Logs and Evidence requirements		
1.	The applicant software must generate audit logs for user actions, user failures, and modifications to the configuration	
2.	The audit logs shall be secured in the CA facility with physical and system access controls as required for CA operations.	
3.	The audit logs should be stored in the CA facility.	
4.	The audit logs are to be protected for data integrity preferably using Syslog servers	
5.	The applicant interface access shall be periodically reviewed.	
Session Time Out		
1.	In the eKYC account creation process, inactivity time limits shall be enforced. The activity time limits shall be as per the following 1. eSign-based Signature - Immediate 2. eKYC account Information submission - 20 minutes 3. OTP authentication - 5 minutes 4. DSC applicant Login - 20 Minutes 5. Exit upon inactivity - 5 minutes	

2. Compliance Requirements for the CA System

For the applicable requirements as specified under the Guidelines issued by CCA, the CA management software is expected to be certified as CC EAL4 or higher in consistent with the Certificate Issuing and Management Components Protection Profile, Version 1.5. (NIST) or

Protection Profile for Certification Authorities or both. The CAs are encouraged to obtain Common Criteria EAL4+ certification ASAP. In case the CA software does not have certification at present, as an interim measure, a security audit of the CA software shall be carried out as per "4. Security Evaluation Requirements for CA". The compliance report in this regard should be made available to the empanelled auditors. The broad areas to be covered but not limited to the security audit of CA software are below:

S.NO	Control	Compliance(Y/N)
1.	Security Policy	
2.	Roles (Administration Officers, Registration Officers, Authentication Officers)	
3.	Access Control and Authorization	
4.	Identification and Authentication	
5.	Remote Data Entry and Export	
6.	Key Management: Key Generation, Key Storage, Key Destruction, and Key Export	
7.	Cryptographic module requirements	
8.	Profile Management(Certificate, CRL, OCSP)	
9.	Certificate applicant data registration	
10.	Certificate Registration	
11.	Certificate Preparation	
12.	Certificate approval	
13.	Certificate Signing	
14.	Certificate Activation	
15.	Certificate storage & delivery	
16.	Certificate Publication	
17.	Certificate Revocation	
18.	Certificate Status Information Provision – OCSP, CRL	
19.	CA Policy Administration	
20.	Key Archiving and Recovery	
21.	PIN Management	
22.	Audit and Log Review	
23.	Batch Processing	
24.	Initial Boot Process	
25.	Threats(Authorised user threats, System related threats, Cryptography-related threats, External attacks)	

3. Compliance Requirements for the CA Website

CA shall have a dedicated website for the Licenced CA-related requirements. The website should meet the following requirements

S.NO	Control	Compliance(Y/N)
1.	CA website shall display current past versions of CPS	
2.	The repository of CA shall be made available to the public	
3.	CA website shall provide a direct interface to applicants. CA website shall make available the direct payment options to the DSC applicants.	
4.	CA website shall publish CRL and CA certificate details	
5.	A help desk for subscribers and application owners shall be provided and the details should be available on the website of CA	
6.	Contact details & email shall be published on the CA website	
7.	The website shall provide a Grievance & Redressal interface	
8.	The certificate fees shall be made available on the website	
9.	The list of empanelled token providers shall be published by CA on their website.	
10.	CA shall provide a certificate search option for a subscriber based on authentication	
11.	The website shall provide eKYC account-related information access as mentioned in the IVG	
12.	Provision for submitting the certificate revocation request by a subscriber shall be provided	
13.	The website should display the list of directors and the authorised representative details	
14.	Ensure that no confidential information is available publically through the CA website	
15.	Ensure high availability of the CA website at all levels	
16.	If outsourced, CA shall maintain all agreements related to development and hoisting.	
17.	Role-wise access control mechanism implemented for the access to the website for updation and administration	
18.	CA shall record the non-availability/hacking/other failure-related incidents and the same shall be made available to auditors.	

Annexure VI

Security Evaluation Requirements for CA

CA shall have an arrangement with Cert-In empanelled agencies for an annual comprehensive security evaluation and also in case of any significant change in any one or more components of IT infrastructure.

The overall scope of this security evaluation shall include System architecture, Design, Network, operating system and Software applications (internal & external). Software application audit includes all the software hosted by the organisation such as CA software, website, eSign Application, OCSP, Time Stamping, external eKYC interface (UID, Banking, PAN, GST etc), Mobile Apps, DLL, etc. The only exception is in case CA software and any of the software is already CC EAL 4+ certified. In case of any change, CA should analyse the impact due to change(s) and get a security evaluation concerning the applicable area where there is a significant impact due to the change.

The comprehensive security evaluation comprises the following -

1. **Architecture, Design, Network & Firewall Access Rules (FAR) Review**: Evaluation of existing network security architecture, Design, HLDs, LLDs, including topology/configuration, and security components/features, network segmentation inspection of single point of failure, high availability etc.
2. **Secure Configuration of OS, servers, Network equipment and Database:** Evaluation of security practices and their implementation, passwords, Patches, service packs, open ports, unused services, permission, authentication, additional security measures implemented, encryption etc. as per the best practices and security standards.
3. **Source Code Review**: Testing of the source code of a software application to identify vulnerabilities, security weaknesses, coding errors, and potential areas for improvement. The scope includes all software applications hosted and distributed by CA except CC EAL certified. In case of unavailability of source code, the self-signed certificate from OEM with the present status of vulnerability should be reviewed.
4. **Application Security Testing**: The active analysis of all the CA applications for any weakness(es), technical flaws, or vulnerabilities as per OWASP Application Security Verification Standard 4.0.3
5. **Vulnerability Assessment/PT**: The vulnerability assessment should cover the Network devices, OS, Applications etc. The vulnerability assessment and penetration testing should cover OWASP Top 10 and SANSTop 25 guidelines for all the applications.
6. **Functional Testing with reference to the Guidelines issued by CCA:** The checklist for the functional testing should be as per CCA-FT

7. **Mobile APP:** The mobile APP shall be tested in accordance with the OWASP- Mobile Application Security Verification Standard v2.1.0
8. **Digital Forensics Readiness Assessment:** The CA shall collect, preserve, protect (temper evident) and analyze digital evidence so that this evidence can be effectively used in any legal matters or court of law. The security audit team should include a forensic expert and should cover tamper-evident logs of devices, applications and operation systems.

The final audit report shall contain the status of every round of testing/audit and also the final status after the remedial action taken by CAs. These remedial actions shall be verified and accepted by the auditor. A maximum of 10 calendar days shall be permitted for remedial action. The auditor shall submit its report within 30 days of the initiation of the audit. Any subsequent closure of the audit observation shall be verified by the auditor before submitting it to the Office of CCA.

Annexure VII

Conditions for Appointment of Auditor

1. For annual audits, CAs shall not be allowed to engage the same auditor in consecutive years. However, there is no restriction in other types of audits related to pre-licence audit, Site shifting, enabling new eKYC mode, ESP empanelment, Infrastructure change(hardware, software, application, new DR site) etc
2. In the case of a special audit, CCA will decide the auditor.
3. Cert-in/STQC empanelled auditors shall carry out the annual security audit as per the scope mentioned in Annexure VI
4. The annual audit and security audit shall not be carried out by the same audit agencies.
5. In case the auditor firm is engaged in any manner in respect of the set-up of CA, then the same auditor shall not audit the CA for the next 3 years.
6. In the case of the CA internal audit by an empanelled auditor, the same auditor shall not be allowed to perform the annual audit of that CA in the same year.
7. The auditor should provide an undertaking for compliance with these conditions at the time of submitting the annual audit report.

Annexure VIII

Financial Status Verification

The financial status verification shall be carried out by the qualified resource of the empanelled auditor or the agency nominated by CCA

The scope includes the following

1. Validate the source of paid-up capital & net-worth
2. Assessment of Business Process and Financial Practices related to DSC issuance
3. Invoice and Tax Evasion
4. Advance payment resulting in financial liability.
5. Any loss to the subscriber which is attributable to the CA.
6. Overall Financial sustainability
7. Latest Audited Balance sheet

* * * * *