

No. 1(6)/2001 – CCA
Office of Controller of Certifying Authorities
Ministry of Information Technology
Government of India
'Electronics Niketan'
6, CGO Complex, New Delhi – 110 003

July 9, 2001

Circular No. 1/2001

**GUIDELINES FOR SUBMISSION OF APPLICATION FOR LICENCE TO
OPERATE AS A CERTIFYING AUTHORITY UNDER THE IT ACT, 2000**

An application can be made for obtaining a licence to operate as a Certifying Authority (CA) under Section 21 of the IT Act, 2000. Requirements, as stipulated in Sub-section 21(2) of the Act, need to be fulfilled by the applicant for issue of a licence to operate as a CA.

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.

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.

Alongwith the application in the format given in Schedule I, 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. In addition to the documents listed in Rule 10, the following documents, among others, may also be furnished.

- (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 40% of its capital)

- THIS OF 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. 5 crores in accordance with Rule 10(ii)(h) of the IT Act.
 - (vi) Crossed cheque or bank draft for Rs. 25,000/- (for fresh application) or Rs. 5,000/- (for renewal) in favour of the Pay & Accounts Officer, MIT, 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.
 - (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.
 - (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 triplicate. These should be in the form of three identical sets numbered 1,2 and 3.*

(K N GUPTA)
Controller of Certifying Authorities
ANNEXURE I
with No. 1(6)/2001 – CCA

dated July 9, 2001

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) In addition to four classes of certificates given below, the Certifying Authority may issue more classes of Public Key Certificates, but these must be explicitly defined including the purpose for which each class is used and the verification methods underlying the issuance of the certificate. The suggested four classes are the following :-

Class 0 Certificate: This certificate shall be issued only for demonstration/test purposes.

Class 1 Certificate: Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.

Class 2 Certificate: These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.

Class 3 Certificate: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals *only on their personal (physical) appearance* before the Certifying Authorities.

(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 (eg. 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.
