Root Certifying Authority of India
CPS

1. Introduction

The Information Technology Act, 2000 was enacted by the Indian Parliament in June, 2000. It was notified for implementation in October, 2000 with the issuance of Rules under the Act. The purpose of the Act is to promote the use of digital signatures for the growth of E-Commerce and E-Governance. It provides legal recognition to electronic records, and puts digital signatures at par with handwritten signatures. The Act defines the legal and administrative framework for the creation of Public Key Infrastructure (PKI) in the country to generate trust in electronic environment. To help establish PKI in the country and ensure interoperability among all Certifying Authorities, technical standards have been framed in Rules and Regulations under the Act. Electronic authentication of individuals, businesses and other entities, as also secure communication of messages over the Internet and any open networks are the aims of the PKI. The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act for purposes of the IT Act. The Office of the CCA came into existence on November 1, 2000. It aims at promoting the growth of E-Commerce and E-Governance through the wide use of digital signatures.

The CCA has to license Certifying Authorities (CAs) and exercise supervision over their activities. It is required to certify the public keys of the CAs, as also lay down the standards to be maintained by the CAs, and perform several other functions under section 18 of the Act to regulate the functioning of CAs in the country. It is also required to issue licences to CAs by signing/certifying their public keys, i.e. signing their Digital Signature Certificates more commonly known as Public Key Certificates (PKCs). The Certification Practice Statement (CPS) of the Controller of Certifying Authorities has been prepared to address the issues related to the licensing process and other relevant topics such as certificate policy, issuance and cancellation of licences, security control and operational policy & procedures and other matters relevant to obligations and responsibilities of the CCA and CAs in accordance with the IT Act, Rules and Regulations.

This CPS uses certain expressions. These are given below. Their definitions are as given in the IT Act, Rules and Regulations:

Applicant

Licensed Certifying Authority (CA)

means a person or organization who has been granted a Licence to issue Digital Signature Certificates under Section 24 of the IT Act, 2000.

Information Technology Act, 2000 (IT Act, 2000)

means the Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly

referred to as “electronic commerce” which involve the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

National Repository of Digital Certificates (NRDC)

means the repository of all Digital Signature Certificates issued under the IT Act, 2000.

Root Certifying Authority of India (RCAI)

is the Root CA operated by the CCA that certifies the public keys of all CAs in India.

Certification Practice Statement (CPS)

means the statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates, in accordance with the Guideline No. 1(6)/2001-CCA dated July 9, 2001.

Controller

means the Controller of Certifying Authorities appointed under sub-section (1) of section 17 of the IT Act, 2000.

Office of Controller of Certifying Authorities (CCA)

means the Office of the Controller appointed under section 17(1) of the IT Act, 2000.

Cyber Appellate Tribunal

means the Cyber Regulation Appellate Tribunal established under sub-section (1) of section 48 of IT Act, 2000.

Digital Signature

means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the IT Act, 2000.

Digital Signature Certificate (DSC)

means a Digital Signature Certificate issued under sub-section (4) of section 35 of the IT Act, 2000.

Licence

means a Licence granted to a Certifying Authority under section 24 of the IT Act, 2000.

1.1 Overview

This CPS provides information that describes the practices employed by the Controller of Certifying Authorities in operating the RCAI and NRDC services.

The RCAI is responsible for:

- Issue of Licence by means of an X.509 certificate
- Digitally signing the public key of the Licensed CA
- Generating CRLs for the licences issued

The NRDC is responsible for:

- Publishing digital signature certificates and CRLs issued by the RCAI
- Publishing digital signature certificates and CRLs of subscribers issued by all Licensed CAs

The CCA issues Licences to Certifying Authorities under section 24 of the IT Act, after duly processing their applications as provided for under the Act. This process includes examining the application and accompanying documents as provided for in sections 21 to 24 of the IT Act, and all the Rules and Regulations thereunder; approving the CPS; auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA. The CCA can suspend or revoke Licences in accordance with the provisions of sections 25 and 26 of the IT Act. The CCA also approves changes in the CPS, if any, of the CAs. CCA also receives the periodic audit reports from all the Licensed CAs, and proposes action as provided for under section 18 of the IT Act and Rule 31 of the Rules under the Act. The CCA operates the RCAI under section 18(b) and NRDC under section 20 of the IT Act.

The structure of this CPS is based on the Internet X.509 PKI Certificate Policy and Certificate Practice Framework (RFC 2529) circulated by the CCA as part of its Guidelines issued on 9 July, 2001 vide No. 1(6)/2001-CCA. This CPS covers the practices followed by the CCA for the procedures related to the Licence/certificate application, issuance, use, validation, suspension, revocation and their expiry, as well as the operational maintenance of the RCAI and NRDC. This CPS is referred to as the "Root Certifying Authority of India CPS". All documents issued by the CCA including the CPS can be downloaded from http://cca.gov.in/documents/.

This CPS is subject to a regular review process that strives to take into consideration developments in international PKI standardization initiatives, development in technology and information security, as well as other relevant issues.

1.2 Identification

This document is the Certification Practice Statement of the Root Certifying Authority of India. RCAI has assigned following OID to this document.

OID: 2.16.356.100.2

Joint – ISO – ITU-T Assigned Country Code : India	2.16.356
CCA	100
CPS	2

RCAI will also issue OIDs to licensed CAs. The CAs will then choose to assign OIDs for different purposes under this scheme.

1.3 Community and Applicability

The CCA PKI community comprises all the Licensed CAs and their subscribers. The Licenced CAs are issued certificates digitally signed by the RCAI of the CCA and hence specifically this CPS shall apply to all the Licensed CAs. At the apex level, the Department of Information Technology and the CCA are also members of this PKI community. CCA, through its RCAI and NRDC, is at the hub of trust in electronic environment.

1.3.1 Ministry of Communications and Information Technology

The Ministry of Communications and Information Technology is the ministry of the Government of India under whose administrative control the office of the CCA functions. This ministry is responsible for policy on E-Commerce and E-Governance, as also on the IT Act in particular and cyberlaws in general. It is also responsible for certain practices and procedures, and standards under the IT Act.

1.3.2 Controller of Certifying Authorities

The CCA regulates the CAs in the country under various sections of the IT Act. It discharges its responsibilities in the PKI regime in the country. Towards this end, it operates the RCAI and NRDC. The following acts are performed by the CCA:

- It follows procedures and norms laid down under the Act to issue a licence to a CA.
- It operates the RCAI to certify the public keys of CAs by digitally signing them thereby making available their licences in the electronic world for verification by any user.
- It operates the NRDC containing all the PKCs and CRLs issued by all the CAs in the country.
- It ensures that alternate mechanisms are put in place for a CA whose certificate/licence has been revoked by it.
- It maintains a Panel of Auditors.
- It arranges audit for first time CA Applicant.
- It receives periodic audit report from CAs.
- It provides date and time stamping for all the certificates issued by it.

- It maintains database of CAs.
- It receives disclosure record of all CAs.
- It assigns unique OIDs to all entities in the PKI regime in the country.
- It organizes other digital signature certification related practices.

The CCA has constituted the following forums as advisory groups to advise it on PKI matters:

1.3.2.1 CA Technology Forum

- Advisory forum of CA technology providers to advise the CCA on technology standards and other related issues of PKI
- Advising on inter-operability issues for a successful PKI in the country

1.3.2.2 CA's Council

- Discussions with the CAs operating in the country to resolve issues of concern to the CAs and users so as to ensure widespread use of digital signatures in the country.

1.3.2.3 DS User Forum

- Discussions with the digital signature users at large to study their problems and difficulties concerning PKI and other implementation issues.
- Formulate response for resolving them with CAs.

1.3.2.4 Legal Advisory Forum

- Advise the CCA on legal issues concerned with the implementation of the IT Act, and any other issues such as the modifications of the Act so as to improve the PKI framework for facilitating the growth of E-Commerce and E-Governance.

1.3.2.5 Auditor's Panel

- Discussions with the Auditor's Panel on a regular basis to maintain and augment audit standards to continuously improve the effectiveness of CAs.

1.3.3 RCAI

The CCA has established the RCAI under section 18(b) of the IT Act to digitally sign the public keys of CAs in the country. It operates RCAI as per the standards laid down under the Act. The requirements fulfilled by the RCAI include the following:

1. The licence issued to the CA is digitally signed by the CCA.
2. All public keys corresponding to the signing private keys of a CA are digitally signed by the CCA.
3. That these keys are signed by the CCA can be verified by a relying party through the CCA's website or CA's own website.

The RCAI is operated using SmartTrust software. The authorized CCA personnel access the Administrator WorkBench to initiate and perform Root CA functions. Where necessary, this CPS distinguishes the different users and roles accessing the SmartTrust software for Root CA functions. Where this distinction is not required, the term Root CA is used to refer to the total CA entity, including the software and its operations.

The RCAI root certificate is the highest level of certification in India. It is used to sign the public keys of the Licensed CAs in India. The RCAI root certificate is a self-signed certificate.

1.3.4 National Repository : NRDC

The CCA's repositories are as follows:

- National Repository of Digital Certificate: http://cca.gov.in/nrdc.htm
- Certificate Suspension and Revocation List : http://cca.gov.in/crl.htm

In accordance with Section 20 of the IT Act, all certificates and CRLs issued by all the licence CAs are contained in the NRDC. This also contains the certificates and CRLs issued by the CCA through its RCAI. Relying parties can verify the CA's public keys from the NRDC.

1.3.5 Licensed Certifying Authorities

A Certifying Authority (CA) can operate in the country after being duly licensed by the CCA as per provisions of the IT Act. It provides services to its subscribers and relying parties as per its CPS which is approved by the CCA as part of the licensing procedure. The licence of a CA can be suspended or revoked by the CCA as provided under section 25 of the IT Act. During the period of suspension, the said CA cannot operate as a CA.

A CA provides the following services:

- Identification and authentication
- Certificate issuance
- Certificate suspension and revocation
- Certificate renewal
- Notification of certificate-related information
- Display of all these on its website
- Time-stamping

In addition, the CA communicates to the CCA the following information as required under the IT Act:

- Any changes in its CPS
- Certificates issued by it to its subscribers
- CRLs issued by it
- Compromise of its private key under section 34 of IT Act
- Disclosure record under section 34 of the IT Act
- Periodic audit reports under Rule 31

1.3.6 End entities

The End entities of RCAI would be the Licensed CAs in India. However, the subscribers and relying parties who use the certificates issued by a CA need to be assured that the CA is licensed by the CCA. Relying Parties trust and use the certificates issued by a CA who has been licensed by the CCA. They should be able to verify the licence through an indicator to that effect in the PKCs issued by a CA. By viewing the PKC using any standard application, the relying party should be able to verify the CA Distinguished Name and its public key as appearing in the Certificate as having been certified by the CCA. The procedure is specified in 1.3.3.

1.3.7 Applicability

This CPS is applicable to all certificates issued by RCAI. The practices described in this CPS apply to the issuance and use of certificates and Certificate Revocation Lists (CRLs) for Licensed CAs within India.

1.4 Contact Details

1.4.1 Specification administration organization

The organization administering this CPS is the Controller of Certifying Authorities. Inquiries should be addressed as follows:

Office of Controller of Certifying Authorities,
Jawahar Lal Nehru Stadium, Lodi Road,
New Delhi- 110 003
E-Mail: dctech@cca.gov.in
Telephone: +91-11-4369525
URL: http://cca.gov.in

1.4.2 Contact Person

The Deputy Controller (Technology),
Office of Controller of Certifying Authorities,
Jawahar Lal Nehru Stadium, Lodi Road,
New Delhi- 110 003,
E-Mail: dctech@cca.gov.in
URL: http://cca.gov.in
Telephone: +91-11-4369525

2. General Provisions

2.1 CCA Obligations

2.1.1 CCA obligations

2.1.1.1 RCAI shall

- Operate as an offline Root.
- Issue Licence in the form of a certificate to the CAs.
- Revoke licence on a valid request and update CRL within a maximum of 6 hours of the revocation.
- Issue and publish digital signature certificates for all keys used by Licenced CA and CRLs
- Provide accurate Information
    - CA Licence information
    - Suspension or revocation of a CA Licence
    - Cancellation of a CA Licence
    - Transfer or merger of a CA
    - Suspension or revocation of a PKC
- Conduct signing operations only on working days. No signing operations will be carried out on Saturday, Sunday or public holidays.
- Shall neither send nor receive any encrypted communication.

2.1.1.2 The National Repository Obligations

- The NRDC shall Ensure operation of 7 days a week, 24 hours a day access to the NRDC. Planned exceptions to the 24x7x365 availability will be notified on CCA's web site. These are:

    - Monthly emergency power off tests
    - Yearly business continuity test

CCA provides access to the NRDC, enabling subscribers and the relying parties to search CA's and end-users certificates, suspension and revocation list of certificates through information and communication networks.

CCA also maintains a separate directory which gives information on the licensed CAs and the revocation list i.e. the Authority Revocation List (ARL). The mechanisms for NRDC access include:

- X.500 Directory Server System that is accessible through the Lightweight Directory Access Protocol (LDAPV3)
- Availability of the information through the website of the CCA – cca.gov.in.
- Access control mechanisms when needed to protect repository information as described in later sections

2.1.1.3 Measures on Vulnerability of Private Key

CCA revokes its self-signed certificate when CCA recognizes that its private key has been compromised. It then creates a new key pair for signing, issues its self-signed certificate, and issues signed certificates for all the CAs using its new signing private key. CCA notifies this to all the CAs so as to enable them to guarantee the safety and trustworthiness in the management under this CPS.

CCA, when informed of the compromise or vulnerability of the private key of a CA, revokes the certificate issued to the CA and immediately notifies this through its ARL so as to enable everybody to be aware of the event under this CPS.

2.1.2 Licensed CA Obligations

A CA that has been issued a Licence by the CCA under the IT Act, 2000, to act as a CA, shall comply with the terms and conditions of the Licence set forth in the Regulations. The Licensed CA shall ensure compliance with its approved CPS.

2.1.2.1 Providing and Notifying Accurate Information

A Licensed CA has to notify its subscribers and the relying parties about the information as given below which can affect the trustworthiness or validity of a certificate in order to enable anybody confirm whether it is as per the provisions of the IT Act:

- CA Licence
- CPS of the CA, including changes
- Certificate suspension and revocation practice of CA
- Cancellation of CA Licence
- Transfer or merger of CA with another entity
- Information on a subscribers certificate
- Certificate suspension and revocation practice of a subscriber
- Disclosure record as required under Section 34 of IT Act, 2000
- Other certification practice related information.

2.1.2.2 Protecting Private Key

The Licensed CA must create its own key pair in a secure way using a trustworthy Hardware Security Module as stipulated in Regulations. It will manage its private key securely in accordance with the procedures mandated under the Act, Rules and Regulations.

When creating a subscriber's key pair, on subscriber’s request, a CA must create it in a secure way using a trustworthy software or hardware and distribute the private key securely to the subscriber. Upon request by a subscriber, a CA shall make available software for generation of his key pair at subscriber’s end. (No trace of the private key would be available in Hardware or software of CA. The private key of the subscriber would not be known to the CA at any time).

2.1.2.3 Using a Certified Private Key

A CA shall use only those private keys in its operations, the public keys corresponding to which have been certified by the CCA.

2.1.2.4 Compromise of Private Key

As soon as a CA realizes that any of its private keys has been compromised, it shall immediately report the matter to the CCA, revoke the certificates issued with that key and update its CRL. It will suspend its self-signed certificate corresponding to that key pair. It shall securely generate another key pair, and get the public key certified by the CCA.

2.1.3 Subscriber Obligations

Subscribers who receive certificates from licensed CAs shall be required to comply with the requirements set forth in sections 40 to 42 of the IT Act, and the Rules thereunder.

2.1.4 Relying Party Obligations

This CPS does not specify what steps a relying party should take to determine whether to rely upon a certificate. The CCA, however, has mandated that the CAs shall make available their digital signature certificates that have been signed by the CCA for access by any relying party. They will also make available the tools necessary for performing the trust path creation, certificate mappings, for validation of their public keys with the help of public key of CCA by the relying parties. The CCA shall also enable PKCs of CAs that have been signed by it for access by any subscribers and relying parties.

In general, a Relying party has to understand the purpose of a certificate, its validity period, utilization range, use and trustworthiness prior to using the same. It has to ascertain from the CRLs that the certificate has not been revoked.

2.2 Liability

2.2.1 CA Liability

The Government of India disclaims any liability that may arise from use of any certificate issued by the CCA, or by the CCA's decision to revoke a certificate issued by it. In no event will the CCA or the Government of India be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the CCA.

The CCA, however, guarantees that the contents given below relevant to the Licence/certificate issued by it are correct.

- The contents in the issued certificate are correct.
- The certificate is issued under the IT Act.
- The matters about suspension and revocation of certificate are correct.

The CCA has no responsibility for any delays or damages due to force majeure such as warfare or a natural disaster or reasons beyond provisions of the IT Act, the rule and regulations.

2.3 Financial responsibility

The CCA disclaims all liability due to the use of any certificates issued by the CCA which certify public keys of CAs.

2.3.1 Indemnification by relying parties

No Stipulation

2.3.2 Fiduciary Relationships

The CCA is not the agent, fiduciary, trustee or any other representative of any of the Licensed CAs and must not be represented by the Licensed CAs in that form. Licensed CAs have no authority to bind the CCA, by contract or otherwise of any obligation or financial implication.

2.3.3 Administrative processes

No Stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The Certification Practice Statement, relationship between CCA and Licensed CA and any other parties will be interpreted in accordance with the IT Act, 2000 and the relevant rules and regulations.

2.4.2 Dispute Resolution procedures

The CCA is competent under the IT Act, clause 18(l), to resolve any dispute between CAs and subscribers. However, Cyber Appellate Tribunal, under the IT Act, is the competent court to mediate a dispute arising out of any order of the CCA.

The CCA can mediate between CAs and subscribers directly or through an arbitrator. For this purpose he can request any information or materials from both the parties which are in order as per their CPS, and the provisions of the IT Act. It will be the endeavour of the CCA to facilitate the resolution of conflicts between CAs and subscribers that may arise as a result of the use of certificates.

2.5 Fees

2.5.1 Certificate Issuance or renewal fees

Certificate Issuance

CCA charges a fee of twenty five thousand rupees for issuance of a Licence/certificate as per notified rules, regulations and guidelines. In case more than one public key is certified then the fees will be per PKC.

Certificate Renewal

An application for renewal of a Licence shall be—

(a) in such form as may be prescribed by the Central Government and available on web site of CCA and shall be made not less than forty-five days before the date of expiry of the period of validity of the Licence.

In case more than one public key is certified then the fees will be per PKC.

CCA charges a fee of five thousand rupees for renewal of a licence/certificate as per notified rules, regulations, and guidelines.

(b) accompanied by such fees, not exceeding five thousand rupees.

2.5.2 Certificate Access Fee

CCA makes no charge to the relying party reading and confirming certificate

2.5.3 Revocation or status information access fees

CCA makes no charge to the relying party accessing the suspension and revocation list of certificates.

2.5.4 Fees for other services such as policy information

CCA can charge for printed documents, CD-ROMs etc., if required under the provisions of the IT Act.

2.5.5 Refund policy

Not Applicable

2.6 Publication and Repository

2.6.1 Publication of information on services offered by CCA

The CCA publishes following information to the repository and/or on its website. The repository is referred to as NRDC

- Digital self-signed CCA certificate of RCAI
- Digital Certificates of all Licensed CAs and of all the public keys used by them
- Digital Certificates of all subscribers
- Practices being followed in issuing / renewing / revoking / suspending the digital certificates
- List of invalid digital certificates (commonly known as Certificate Revocation Lists [CRLs])

2.6.2 Frequency of publication

2.6.2.1 Issued Certificates

The RCAI shall publish all certificates in the NRDC within one working day of the completion of the issuance of the certificate.

2.6.2.2 Revoked Certificates

The RCAI shall add revoked certificates originally certified by CCA to the relevant CRL on a daily/weekly basis on the completion of the revocation process.

2.6.3 Access controls

All users will be able to read the information published in the NRDC. Access controls declining write, modify or any other capability other than read shall be defined and managed by the RCAI.

2.6.4 Repositories

The CCA shall maintain NRDC containing

- Digital signature certificates of Licensed CAs
- ARL's of licensed CAs.
- Digital signature certificates of end entities of Licensed CAs
- CRLs of end entities of licensed CAs.

2.7 Compliance audit

Audit logs of all transactions are maintained to provide an audit trail of all actions, transaction and processes. Audit logs are monitored by the CCA as per procedures detailed in the Operations Manual.

2.7.1 Frequency of entity compliance audit

The CCA shall conduct,

- half yearly audit of the Security Policy, physical security and planning of its operation;
- a quarterly audit of its repository.

2.7.2 Topics covered by audit

The CCA shall get its operations audited annually by an auditor and such audit shall include inter - alia,

- security policy and planning;
- physical security;
- technology evaluation;
- Certifying Authority's services administration;
- relevant Certification Practice Statement;
- compliance to relevant Certification Practice Statement;
- contracts/agreements;
- regulations prescribed by the CCA;
- Policy requirements of Certifying Authorities Rules, 2000.

2.7.3 Actions taken as a result of deficiency

The CCA shall immediately take appropriate action on the deficiencies pointed out by the audit so as to secure the operations of RCAI and NRDC.

2.8 Confidentiality

The CCA collects information about the CAs as part of the application. These data are processed in a way that ensures protection of their private information. All information other than what is published in their licence and digital signature certificate, and in CRL is kept in confidence.

2.8.1 Types of information to be kept confidential

The following information shall be confidential namely:

- CA licence application, whether approved or rejected;
- CA licence application information collected from the CA or elsewhere as part of the registration and verification process but not included in the Digital Signature Certificate information;

2.8.2 Types of information not considered confidential

Information included in public certificates and CRLs of Licensed CAs issued by the RCAI is not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

When a certificate is revoked/suspended, a reason code shall be included in the CRL entry for the action. This reason code is not considered confidential and may be shared with all other users and relying parties. However, no other details concerning the revocation are disclosed.

2.8.4 Release to law enforcement officials

Confidential Information shall only be released by the CCA to courts and law enforcement agencies in accordance with applicable legal requirements.

2.8.5 Release as part of civil discovery

No Stipulation

2.8.6 Disclosure upon owner's request

The information related to the CA's certificate would be disclosed by the CCA to a third party, only when required by the CA, with a signed request.

2.8.7 Other information release circumstances

No Stipulation

2.9 Intellectual Property Rights

No right or interest in any intellectual property rights are granted to any Licensed CA or any relying party. All rights in intellectual property are reserved . Any content copied from this document should include reference to this source.

Intellectual property rights on the items listed below belong to the CCA according to the Copyright Act and other related regulations:

- Software and hardware developed by CCA
- Certification Practice Statement of CCA
- Name of CCA
- Corporate Name
- Internet Domain Name
- Key pairs created by CCA

3. Identification and Authentication

3.1 Initial Registration

All CA applicants shall fill the 'Form for Application for grant of Licence to be a Certifying Authority' as described in Information Technology (Certifying Authority) Rules, 2000 - Schedule I, supported by such documents and information as required by CCA.

3.1.1 Types of names

Each CA Applicant must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subjectName field and in accordance with PKIX Part 1(RFC 2459). Each CA Applicant may use an alternative name via the SubjectAlternateName field, which must also be in accordance with PKIX Part 1. The DN must be in the form of a X.501 printable String and must not be blank. It should have the following structure :-

c=in, o=IndiaPKI, ou=<Licensed CA>

3.1.2 Need for names to be meaningful

The Subject name contained in a Licence CA certificate MUST be meaningful in the sense that the CCA is provided with proper evidence of the association existing between the name and the entity to which it belongs.

3.1.3 Rules for interpreting various name forms

The naming convention used by CCA to identify certificate holders uniquely is ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.4 Uniqueness of names

The CCA shall ensure that the set of names is unambiguous. The CCA shall reject a Licence application in the case where the name cannot sufficiently distinguish the Applicant from an existing Licensed CA's Distinguished Name. The name shall conform to X.500 standards for name uniqueness.

3.1.5 Name claim dispute resolution procedure

The CCA may, by reasonable endeavours, resolve disputes that may arise over the allocation of names and in its discretion may reject, change, re-issue or revoke certificates in relation to any Distinguished Name.

3.1.6 Recognition, authentication and role of trademarks

No Stipulation

3.1.7 Method to prove possession of private key

To establish that the applicants possess valid functioning key pairs, CCA would require applicants to submit a Certificate Signing Request (CSR) in accordance with the PKCS#10 standard. The signing key pair of the Licensed CA shall be stored in FIPS 140-1 level 3 or higher level device. An independent verification shall be performed as a part of the auditing process.

3.1.8 Authentication of organization identity

The documents mentioned in §4.1 ensure the authentication of organization identity.

3.1.9 Authentication of individual identity

The documents mentioned in §4.1 ensure the authentication of individual identity.

3.2 Routine Rekey

Not Applicable

3.3 Rekey after Revocation

Not Applicable.

3.4 Revocation Request

The authority to revoke the RCAI root certificate rests with the Controller of Certifying Authorities.

Licensed CAs shall designate an authority, who can request the revocation of its Licence. The Controller of Certifying Authorities also can authorize the revocation of a Licensed CA under section 25 of the IT Act, 2000.

4. Operational Requirements

4.1 Certificate Application

An application for a certificate is made by filling out the application form as given in Schedule I of the Rules of the IT Act. The form and relevant information can be obtained directly from the office of the CCA or downloaded from the web site of the CCA (cca.gov.in).

4.1.1 Certificate Application Submission

All applications are to be submitted, in triplicate, physically to the office of the CCA at the following address:

Office of the Controller of Certifying Authorities,
Gate No. 29, JawaharLal Nehru Stadium,
Lodhi Road, New Delhi- 110 003

As part of the application for grant of Licence, the date by which the applicant will be ready to start the audit will be indicated. The application will be deemed to have been received on this date for processing purposes.

4.1.2 Information required as part of an Application

Each application for issue of a licence to become a CA must be accompanied by documents and information as stipulated in the Guidelines for submission to operate as a CA. In addition to the documents listed in Rule 10, the following documents, among others, may also be furnished.

- Company Profile/Experience of Individuals
- For an individual, proof of capital of Rs. 5 crores or more in his business or profession
- For a company/firm,
  - proof of paid-up capital not less than Rs. 5 crores
  - proof of net worth not less than Rs. 50 crores
- Proof of Equity (Proof that equity share capital held in aggregate by NRIs, FIIs or foreign companies does not exceed 49% of its capital)
- An undertaking to submit Performance Bond or Banker's Guarantee valid for six years from a scheduled bank for an amount specified by the IT Act, Rules and Regulations.
- 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.
- Certified true copies of the company's incorporation, articles of association etc.
- Original business profile report with certification from Registrar of Companies.
- Audited accounts for the past 3 years (if applicable).

- The CA's Certification Practice Statement (CPS) as laid down in Annexure I to these Guidelines.
- Technical specifications of the CA system and CA security policies, standards and infrastructure available/proposed and locations of facilities.
- Information Technology and Security Policy proposed to be followed by the CA in its operations under Rule 19.
- Statement addressing the manner in which the CA shall comply with the requirements stipulated in the IT Act, Rules and Regulations.
- Organisational chart and details of all trusted personnel.
- 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.
- Date by which commencement of CA operations is proposed. Operations can only commence after due compliance with Rule 20.
- 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.

4.1.3 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 by the Auditor within 21 Days. Based on the audit report, the results of the financial evaluation, and on the applicant's meeting all technical, financial, infrastructural, legal and regulatory requirement, 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.

4.2 Certificate Issuance

4.2.1 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.

4.2.2 Paper Licence

Each Licence issued will be accompanied by a certificate digitally signed by the CCA. One of the public keys included for certification will be identified as the primary public key to be certified. The certificate issued by the CCA along with the Licence will contain this public key. The remaining public keys will also be certified through certificates digitally signed by the CCA.

4.2.3 Certificate Issuance

CCA issues the certificate after checking the following criteria, in the case of each of the above public keys.

- A certificate request is generated by the applicant in PKCS # 10 format and submitted to the CCA. The CCA establishes that the public key corresponds to a functioning key pair
- The CCA establishes the uniqueness of the public key being certified.
- The CCA establishes the uniqueness of the DN submitted by the applicant.
- The certificate request is used by the CCA to generate the certificate.
- The certificate is physically handed over to the applicant.
- All certificates issued are published in the National Repository and are accessible through the web site of the CCA.
- Validity period: All Licences are valid from the date & time of issue for a period of five years, and will not be, in any case, later than the expiry date of the CCA's Root certificate.

4.2.3 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)

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 it's application.
MMMM	**0000**	-	**in case of fresh licence**
	yyyy	-	year of renewal
ZZZ	**Reserved for future use**		

The digital signature certificate(s) issued by the CCA corresponding to the above licence and other public keys submitted by the CA contain the following information :

- Version
- Serial Number
- Signature Algorithm used by the CCA to sign the certificate
- Issuer (CCA's) DN
- Validity
- Subject information including CA's DN
- Public key of the CA
- Signature of CCA
- Extensions

4.2.4 Validity Period of a Certificate

The licence is valid for a period of five years from the date of its issue.

The licence is not transferable.

4.3 Certificate Acceptance

The certificate issued by the CCA to the CA applicant will be deemed to have been accepted on its receipt by the CA applicant.

4.4 Certificate Suspension and Revocation

The Controller of Certifying Authorities can order, or an Authorized Signatory of the Licensed CA can request, that a certificate be revoked when any of the information it contains is known or suspected to be inaccurate, or when the private key associated with the certificate is compromised or suspected to have been compromised, or in the interests of national security as per the provision under section 25 and 26 of the IT Act, 2000.

Suspension of certificates issued by CCA always precedes revocation but revocation shall follow only under the specific procedures described in this section. All suspension and revocation requests are required to be valid. Such validity shall be determined by their compliance or non-compliance with the procedures of this CPS, which include references to the authority of the person who may make a request.

The CCA may revoke a certificate when it considers revocation necessary or expedient.

4.4.1 Circumstances for Suspension & revocation

Licences can be revoked or suspended by the CCA under Rule 14. The CCA shall revoke a certificate if the CCA has reasons to believe that the CA :

- 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;
- failed to maintain the standards specified under clause *(b) of* sub-section (2) of section 20;
- contravened any provisions of the IT Act, Rule, Regulation or orders made thereunder,
- the private key corresponding to the public key in the certificate has been lost, disclosed without authorisation, stolen or compromised in any way.
- the security, trustworthiness or integrity of the CA's PKI is materially affected due to the CA's activities.
- the licence does not meet material obligations of its agreements with CCA, those of any applicable CPS, or this CPS;
- there has been an improper or faulty issuance of a certificate due to:
  - A material prerequisite to the issuance of the Certificate not being satisfied;
  - A material fact in the Certificate is known, or reasonably believed, to be false.
- the licencee is bankrupt, being wound-up or is making arrangements or compositions with its creditors;
- the CA does not possess sufficient financial resources to maintain its provision of certification services;
- any other material circumstance that requires investigation to ensure the security, integrity or trustworthiness of the CA's PKI.

An investigation into the need for suspension will take place by which the following is carried out:

- Validate the need for suspension and obtaining authorisation for the suspension

  - On completion of investigation into need for suspension, either certificate is suspended or reinstated with certificate status as valid.

- On suspension of a certificate.

  - The reason for the suspension is recorded.

  - A CRL (Certificate Revocation List) is immediately generated and published on the Root CA Directory and the NR.

  - The CA to which the certificate refers publishes in a prominent manner a suspension notice on its Web Site and its Certification Revocation List distribution point.

  - CA to which the certificate refers, notifies its End Users of the suspension.

  - A notice containing the Certificate details and the date and time of suspension is issued to the subscriber.

Pending completion of any inquiry ordered by the CCA, no CA whose certificate has been suspended will issue any certificates during this suspension. The suspension of certificates issued by the CCA Root may occur immediately if the suspension has been requested by the authorized signatory of the licensed CA or after an investigation has taken place.

4.4.2 Who can request suspension

The CCA shall action suspension request from an Authorized signatory of the Licensed CA. The CCA, on his own, can also initiate suspension of a certificate.

4.4.3 Procedure for suspension request

When a suspension or revocation is requested by an authorized signatory of a CA, the suspension or revocation request may be submitted through:

- a digitally signed suspension or request verifiable with the public key contained in the certificate to which the request refers to and performance of an off-line request
- a certificate suspension or request physically delivered to CCA by an appropriately authorized person

4.4.4 Limits on suspension period

Certificates issued by the RCAI of 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.

If on completion of the inquiry, any of the above is established beyond doubt then the certificate may be revoked by the CCA.

Revocation of the certificate of a CA can happen for a number of reasons.

- When a CA applies for a certificate revocation
- When the CCA recognizes that a certificate of a CA was issued in an illegal manner.
- When the CCA recognizes the dissolution of a CA
- When the CCA recognizes that a private key of a CA is lost, damaged, stolen or compromised

4..4.5 Who can request revocation

Revocation request from the following parties can be accepted :

- An Authorized signatory of the Licenced CA
- Controller of Certifying Authorities

4.4.6 Procedure for revocation request

When a revocation is requested by any entity external to the CCA, the revocation request may be submitted through:

- a digitally signed revocation request through the communication of compromise of private key by a CA to the CCA verifiable with the public key contained in the certificate to which the request refers to and performance of an off-line request in accordance with procedures designed by CCA for such purpose.
- a certificate suspension or revocation request physically delivered to CCA by an appropriately authorized person.

In processing a revocation request, the Root CA will:

- Revoke the certificate on the Root CA, record the reason for the revocation, and maintain relevant documentation.
- Generate immediately a CRL (Certificate Revocation List) from the Root CA
- Withdraw the certificate from the CCA Web site and place a prominent revocation notice on its place.
- Issue a notice containing the Certificate details and the date and time of revocation to the certificate subscriber.
- Notify the CA that its certificate has been revoked under the provisions of the IT Act.
- Publish the revocation on the National Repository.

4.4.7 Revocation request grace period

Revocation requests shall be processed within one working day of having a definitive decision by the CCA to revoke the certificate in accordance with CCA's operational procedures.

4.4.8 CRL issuance frequency

The CCA shall update the CRL within one working day after a valid revocation request is processed and at least every month, even if no changes to the CRL have been made.

4.4.9 CRL checking requirements

A relying party may check the CCA's CRL for determining the CA's certificate status before relying on any certificate issued by the CA.

4.4.10 On-line revocation/status checking availability

The CCA shall provide on-line certificate status checking through publication in NRDC.

4.4.11 Other forms of revocation advertisements available

On suspension and/or revocation of a certificate issued by the RCAI, the CCA will issue advertisement in at least two national newspapers and one vernacular newspaper in the region where the Licensed CA is established.

4.4.12 Checking requirements for other forms of revocation advertisements

No Stipulation

4.4.13 Special requirements regarding key compromise

The CCA is to be notified immediately by a CA in case of a key compromise.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

The minimum audit records of RCAI to be kept include:

(i) System start-up and shutdown;
(ii) RCAI's application start-up and shutdown;
(iii) Attempts to create, remove, set passwords or change the system privileges of the CA Master Officer, CA Officer, or CA Administrator;
(iv) Changes to keys of the RCAI or any of his other details;
(v) Changes to Digital Signature Certificate creation policies, e.g. validity period;
(vi) Login and logoff attempts;
(vii) Unauthorised attempts at network access to the RCAI's system;
(viii) Unauthorised attempts to access system files;
(ix) Generation of keys;
(x) Creation and revocation of Digital Signature Certificates;
(xi) Failed read-and-write operations on the Digital Signature Certificate or Certificate Revocation List (CRL) directory.

Records of the following application transactions shall be maintained:

(a) Registration;
(b) Certification;
(c) Publication;
(d) Suspension; and
(e) Revocation.

Records and log files shall be reviewed regularly for these activities.

To facilitate decision-making, all agreements and correspondence relating to services provided by RCAI are collected and consolidated at a single location.

- Certificate application records, including records relating to rejected applications;
- Certificate generation requests, whether or not Certificate generation was successful;
- Certificate issuance, suspension and revocation records, including CRLs;
- Audit records, including security-related events;

4.5.2 Frequency of processing log

The CCA's audit logs are regularly reviewed by its personnel and all significant events are detailed in an audit log summary. Such reviews verify that the log has not been tampered with, and then briefly inspect all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews are documented.

4.5.3 Retention period for audit log

The CCA retains its audit logs onsite for at least twelve months and subsequently retains them in the manner described in para 10 of the Information Technology Security Guidelines as given in Schedule-II of IT (CA) Rules, 2000.

4.5.4 Protection of audit log

The electronic audit log system includes mechanisms to protect the log files from unauthorized viewing, modification, and deletion.

Manual audit information will be protected from unauthorized viewing, modification and destruction.

4.5.5 Audit log backup procedures

CCA uses highly secure systems to maintain the integrity of its electronic audit logs over time and has established a series of security procedures regarding their storage, access and backup.

4.5.6 Audit collection system

The CCA audit collection system is a combination of automated and manual processes. The system is maintained through access control mechanisms and role separations with regard to the software and hardware and through confidential documented operational procedures known and followed by CCA personnel. The control measures of both the automated and the manual processes are audited in accordance with §2.7 of this CPS.

4.5.7 Notification to event-causing subject

Operations personnel notify the security administrator when a process or action causes a critical security event or discrepancy.

4.5.8 Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The RCAI ensures that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

A full risk assessment has been completed for the CCA Root CA operations and will be performed at a minimum annually.

4.6 Records Archival

4.6.1 Types of event recorded

All significant events are recorded including new officer creation, incident reports, daily events, changes to the environment or system, CCTV recording of CA operations.

All events concerning the operation of CCA Root CA certification services are recorded.

Transactions that meet exception criteria are completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

Adequate audit trails are captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) are analyzed. This information includes such information as who, what, when, where, and any special information such as:

(i) Success or failure of the event

(ii) Use of authentication keys, where applicable

Automated or manual procedures are used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:

(i) Significant computer system events (e.g. configuration updates, system crashes)

(ii) Security profile changes
(iii) Actions taken by computer operations, system administrators, systems programmers, and/or security administrators

Digital Signature Certificates stored and generated by the RCAI are recorded.

Audit information as detailed in §4.5 are recorded.

4.6.2 Retention period for archive

All CCA Root CA records concerning the operation of its certification services are archived and are retained for a period of ten(10) years.

Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation by a law enforcement agency, shall be retained as per provisions of the IT Act.

4.6.3 Protection of archive

All information pertaining to the CCA's operation, CA's application, verification, identification, authentication and CA's agreement to Terms and Conditions of the licence shall be stored within the country.

4.6.4 Archive backup procedures

A second copy of all information retained or backed up by CCA shall be stored at a location within the country duly protected either by physical security alone, or a combination of physical and cryptographic protection. The secondary site shall have adequate protection from environmental threats such as temperature, humidity and magnetism. Such a disaster recovery site is under planning.

4.6.5 Requirements for time-stamping of records

The time source GPS clock for the CCA Root CA is independently verified periodically and all electronic automated Root CA records are associated with the time and date of their occurrence.

The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

The real time clock of the computer or communications device is set to Indian Standard Time (IST). Further, there is a procedure in place that checks and corrects drift in the real time clock.

4.6.6 Archive collection system

Only authorized and authenticated staff are allowed to handle archive material.

4.6.7 Procedures to obtain and verify archive information

The CCA verifies the integrity of the backups once every six months. Information stored off-site is also periodically verified for data integrity. This is done atleast once every six months.

4.7 Key changeover

4.7.1 The lifetime of RCAI signing keys is set to five years. On key rollover, a new public key will be made available via the web and through the NRDC.

4.7.2 A Licensed CA may only apply to renew its key within three months prior to the expiration of its Licence, provided the previous certificate has not been revoked. Automated key changeover for Licensed CAs is not permitted.

4.8 Compromise and Disaster Recovery

4.8.1 Computing resources, software, and/or data are corrupted

The CCA has established business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data.

4.8.2 Entity public key is revoked

In the event of the RCAI private signature key being revoked, the CCA shall revoke and re-issue all certificates in use at that instant.

4.8.3 Entity key is compromised

In the event of the RCAI private signature key being revoked, the CCA shall revoke and re-issue all certificates in use at that instant.

4.8.4 Secure facility after a natural or other type of disaster

In the event of a natural or other type of disaster the operation of RCAI and NRDC will be re-established on an independent disaster recovery site, using the backup data taken on a daily basis from the primary CA site.

The recovery time for bringing up the secondary site is targeted to be better than 48 hours. The disaster recovery site is under planning.

4.9 CA Termination

In the event of change in government policies, and/or Acts, as a result of which if the CCA is terminated, the CCA shall:

- Provide no less than 6 months notice to all current Licensed CA of its intent to cease operations
- Ensure the secure preservation and maintenance of all relevant databases, archives, records and documents with an independent custodian and/or

designated government body. The CCA archives will be retained in the manner and for the time indicated in 4.6.

- Provide access to National Repository maintained by the CCA, for a maximum period of 12 months following cessation of services
- Revoke all valid certificates at the end of the notice period.
- Ensure availability and access to relevant CRLs for a period of 12 months following cessation of operations.

5. Physical, Procedural and Personnel Security Controls

The technical and physical infrastructure of the Root Facility (RF), established for the operation of the Root Certifying Authority of India (RCAI), and the National Repository of Digital Certificates (NRDC) is fully secured in accordance with the requirements laid down under the IT Act.

5.1 Physical controls

5.1.1 Site Location and Construction

The Root CA of India (RCAI) operations are being conducted from the Root Facility of CCA. The National Repository (NR) and its operations are conducted from Jawaharlal Nehru Stadium, New Delhi.

5.1.2 Physical access

Physical access to RF for performing RCAI operations is controlled and restricted to the authorized individuals only.

Entry to the working area (WA), anteroom (AR) and the SR are registered in the log register. Entry to the WA is done using an access control system. The log register and access control audit trail files are reviewed regularly.

5.1.2.1 The 6-tier security for RCAI

Six-tier security has been implemented at the RF.

- Tier 1 – The security of the building where the RF is located, forms the first level of security.
- Tier 2 – Entry to the WA is after entering details to a log register and proper physical verification by the security guard at the entrance. This is the second tier of Security.
- Tier 3 – Entry to the WA is through a proximity access control system. This forms the third tier of security.
- Tier 4 – Entry to SR is through AR. The entry to AR is restricted by twin doors and proximity access control system. This forms the fourth tier of security.
- Tier 5 – The entry to SR is restricted by twin doors and a combination of proximity and biometric access control system. This is the fifth-tier of security.
- Tier 6 – A fire resistant safe is placed inside the SR. This forms the sixth-tier of security.

5.1.2.2 By-pass or deactivation

The By-pass or deactivation of normal physical security arrangements are authorized and documented.

5.1.2.3 Trespass detection and alarm system

Access to the site is controlled through proximity cards. In addition, a biometric access system is used for access to the SR, of the authorized personnel.

Vibration sensors along with motion sensing and alert devices have been installed to ensure that no unauthorized personnel can gain access to the SR. In the case of a forceful entry, alert gets activated and is sounded at the designated place.

5.1.2.4 Sensing and preventive measures for RF.

The RF is monitored using appropriate equipment for surveillance based on various sensors. The sensors installed are:

a. Motion sensors
b. Vibration sensors
c. Smoke sensors

These sensors are connected to an alarm system. On security breach the alarm gets activated. The security guard in the RF and the Chief Security Officer (CSO) take the suitable escalation procedures.

5.1.2.5 DVR (Digital Video Recorder) system

The RF is constantly monitored using a CCTV system to detect any unusual activities.

5.1.2.6 HSM and smart card storage at the SR

The Hardware Security Module (HSM) is installed in one of the server in SR. The smart cards in the SR are protected by the tier-6 of security.

5.1.2.7 At RF, it is ensured that:

a. Access to RF is restricted to authorized personnel.
b. The RF is provided with physical security round the clock.

5.1.2.8 Emergency planning for RF

Following measures are in position to attend to any emergency situation at the RF:

a. Provisions have been made to provide access to the security guards in case of emergency.
b. Fire extinguishers are placed at RF to overcome fire hazards.

c. In case of any untoward incident or emergency the designated AC(Tech) will be informed by Security officer and guard.
d. Officers, staff and security guards are given adequate training and routine mock drills are conducted to ensure their readiness.

5.1.2.9 Power supply and air conditioning

a. Continuous power supply has been ensured by suitable deployment of UPS and DG set.
b. Emergency lights are also placed in RF.
c. The air conditioning system installed in the RF is equipped with temperature and humidity control.

5.1.2.10 Natural disaster protection

Necessary precautions have been taken to protect and prevent the impact of natural disasters such as flood, earthquake etc.

5.1.2.11 Water exposures

The RF is well protected from potential water related threats.

5.1.2.12 Fire prevention and protection

Fire alarm system has been installed to handle any emergent situation arising out of fire.

5.1.2.13 Media storage

Storage media are protected from environment threats such as temperature, humidity and magnetic field. Any media, which is to be transported to National Repository (NR), is done so in secured and tamper proof manner.

5.1.2.14 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. HSM and related devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal. Other waste is disposed off in accordance with the CCA's normal waste disposal requirements.

5.1.2.15 Off-site backup for SR

Routine backups of the system data, audit log data, and other sensitive information are performed and stored in a secure place at the CCA's office.

5.2 Procedural controls

5.2.1 Trusted roles

The following roles have been identified in connection with RCAI operations at SR:

a. Coordinator
b. System Administrator
c. System Operator
d. Auditor

- At least two persons are required to perform each critical and routine task in the RCAI operation.
- DC (T) authorizes all the activities of RCAI operation. For each session DC (T) designates an AC (T) as a coordinator. The AC (T) in turn assigns the roles to various officers
- All the officers designated to perform various roles have been issued proximity cards and granted access to specific locations. They are also issued electronic tokens for the session by the coordinator to perform specific functions.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The background, qualifications, and experience of the technical personnel are verified as per the rules and regulations.

5.3.2 Employees Verification/Investigation

CCA has followed appropriate government procedures for appropriate investigation of all personnel

5.3.3 Training Requirements

CCA has provided comprehensive training to all the technical personnel performing duties, in the following areas:

a. Relevant aspects of the IT Security Policy and Security Guidelines framed in IT (CA) Rules, 2000;
b. RCAI related software /hardware training
c. RCAI related duties they are expected to perform
d. Disaster recovery and continuity procedures.

5.3.4 Re-training frequency and requirements

Refresher training of technical personnel is conducted as and when required, and CCA reviews these requirements on a regular basis.

5.3.5 Sanctions for unauthorized actions

In the event of actual or suspected unauthorized actions by a person performing duties with respect to RCAI operation, access to RF is denied to him/her, with immediate effect. Further actions will be initiated as per government procedures/rules.

5.3.6 Contracting personnel requirements

No contractor is allowed access to RCAI system.

5.3.7 Documentation supplied to personnel

Officers/staff operating SR have been provided with comprehensive user manuals detailing the procedure of certificate creation, update, renewal, suspension, and revocation, and software functionality etc.

5.4 Compliance with Security Service Regulations

Office of CCA observes and adheres strictly to 'Security Service Regulations' for the security measures, which are not shown in the Certification Practice Statement.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair for the CCA is generated in a hardware security module (HSM) which is FIPS 140-1 level 4 certified. Licensed CAs generate their key pairs in a HSM certified to meet the requirements of FIPS 140-1 level 3 certified at minimum.

6.1.2 Private Key Delivery to Entity

Not applicable.

6.1.3 Public Key Delivery from CA (applicant) to CCA

CAs' Public keys are delivered to the CCA as a PKCS#10 certificate request. The signature on the PKCS#10 request is verified to confirm that the CA is in possession of the private key associated with each public key delivered. A certificate is then signed by the CCA and issued to the CA in the format as specified in 7.1.

6.1.4 Root CA Public Key Delivery to Users

The self-signed Certificate of the CCA is available to End-Users for Certificate validation purposes. The certificate hash (thumbprint) and the Root CA certificate are available on the web site of each licensed CA as well as CCA's Web site (cca.gov.in). Relying parties must confirm the validity of their copy of the CCA certificate using this thumbprint. The CCA Digital signature certificate, along with this CPS and other documentation such as the IT Act, Rules and Regulations are available on CD from the office of the CCA or on CCA's website cca.gov.in.

This certificate shall also be made available by each CA and sub-CA on its website to enable verification by relying parties.

6.1.5 Key Sizes

The modulus of the CCA Root CA and the keys of CCA are all 2048 bits in length and use the RSA algorithm. The hash algorithm used by the CCA for signing is SHA-1.

6.1.6 Public Key Parameters Checking

Not Applicable

6.1.7 Parameter Quality Checking

Not Applicable

6.1.8 Hardware/Software Key Generation

Keys are generated in a hardware security module that complies with FIPS 140-1 Level 4.

6.1.9 Key Usage Purposes

The key of the CCA will be used for:

- the issuance of certificates to the Certification Authorities that have been Licensed.
- Issuance of Certificate Revocation Lists

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

The cryptographic module used by the CCA is certified to FIPS 140-1 level 4.

6.2.2 Private Key (n out of m) Multi-person Control

The private key stored on the HSM does not leave the HSM for any purpose whatsoever. Whenever the private key on the HSM is to be used for signing, three levels (?) of authorizations (based on smart cards and PINs) will be invoked. The first will be at the 'Crypto-Officer' level specifically for activating the HSM. The second two will be at the 'Security Officer' level of the Certificate Issuing System (CIS). All three authorizations are required, thus establishing 3-out-of-3 control.

6.2.3 Private Key Backup

CCA's Private Key is backed up only for disaster recovery purposes. This backup is also done under the same multi person control as in the case of the original key.

During key generation, the HSM is configured to generate 3 sets of smart cards, containing backup keys. The first 2 sets are housed in the Strong Room containing the CIS and the backup system, while the 3rd set will be placed in the Disaster Recovery site.

6.2.4 Private Key Archival

The Root Private Key will not be archived.

6.2.5 Private Key Entry into Cryptographic Module

Private key for the CCA is generated in Hardware Security Modules as described in § 6.1 of this CPS. The HSM is sensitive to motion, tilting and temperature. To ensure that the private key does not get destroyed, it is ensured that the HSM is maintained within the limits set for the above three parameters.

6.2.6 Method of Activating Private Key

- CCA Private key activation requires entry and validation of a PIN/passphrase compliant with specified security parameters.

- CCA's private key for signing can only be activated by authorization at three levels of trusted persons.
- Two Security officers at the level of the CIS.
- One Crypto officer at the HSM level.
- All the above authorizations will be through smart cards and associated PINs.

6.2.7 Method of Deactivating Private Key

The CCA Private key is deactivated after each use by manually shutting down the system.

6.2.8 Method of Destroying Private Key

The CCA Private key in the HSM may be destroyed by returning the HSM to its factory initialized state. SmartCards and other cryptographic tokens used by the CCA will be physically destroyed prior to disposal.

The HSM can be destroyed through motion, tilting or temperature changes outside preset limits. Other than this, destroying the lithium battery on the HSM, will also destroy the private key from the HSM.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All public keys of the CCA will be archived.

6.3.2 Usage Periods for the Public and Private Key

The Root key pair of the CCA and certificate will expire after 15 years from the moment of their generation.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Not applicable

6.4.2 Activation Data Protection

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CCA has established and documented all computer security technical controls implemented for the Root CA as specified in IT Security Guidelines of IT (CA) Rules, 2000.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Not Appliable

6.6.2 Security management controls

Security management controls are enforced by rigid separation of operator roles.

- Security Officer
- Registration Officer
- System Administrator

6.7 Network Security Controls

The CCA's Root is maintained and operated off-line and is not networked with any external components.

The National Repository Service is maintained on-line and uses firewalls and other mechanisms for connections to untrusted networks including the Internet. These connections are further secured by using intrusion detection systems where applicable. The configuration and access control to these network security devices is strictly controlled and limited to authorized personnel only.

6.8 Cryptographic Module Engineering Controls

The cryptographic module used by the CCA is certified to FIPS 140-1 level 4.

7. Certificate, Certificate Suspension and Revocation List Profile

7.1 Certificate Profile

7.1.1 Version number(s)

CCA issues certificates in conformance with X.509 version 3 and RFC 2459.

7.1.2 Certificate Extensions

- Certificate Extension used are
  - Key Usage Marked **critical**
  - Basic Constraints with a pathLenConstraint of '0' marked **critical**
  - Policy Constraint marked **critical**
  - Alternate Identity marked **critical**

7.1.3 Algorithm object Identifiers

Certificates shall be signed using the RSA algorithm

7.1.4 Name Forms

CCA shall populate the name constraint field in the certificates with directory names.

7.1.5 Name Constraints

RCAI does not support anonymous names. Names must be meaningful and must be associated with the subscriber. Names are constrained to be unique Distinguished Names (DN)

7.1.6 Certificate policy object Identifier

All certificates issued in accordance with this Certification Practice statement shall reference the OID for this policy. The OID for this policy is detailed in section 1.3

7.1.7 Usage of Policy Object Identifier

The Policy Constraint is marked critical to ensure that all certificate holders and relying parties are aware of the requirement to conform with this CPS.

7.1.8 Policy qualifiers syntax and semantics

None in the present version.

7.1.9 Processing semantics for the critical certificate policy extension

None in the present version.

7.1.10 Certificate Format

An issued certificate shall contain:

- The identify of the Licensed CA
- Copy of the public key of the Licensed CA
- Unique distinguished name
- Validity period of no longer than five years from the date of issue
- Unique certificate serial number
- Digital signature of RCAI
- For future use

7.2 CRL Profile / Certificate Suspension and Revocation List Profile

7.2.1 Version number(s)

The CCA issues CRLs in conformance with X.509 Ver. 2 CRLs.

7.2.2 CRL and CRL entry extensions

None

8. Specification Administration

8.1 Specification change procedures

CCA will periodically review the CPS in light of policy and/or infrastructure technology change. The CPS will be revised if required.

The revision-related record of the Certification Practice Statement will be maintained and will include the following:

Latest Version of the Certification Practice Statement with version no.

- Revised contents with changes highlighted

Revision record of the Certification Practice Statement

- Previous versions of the Certification Practice Statement

8.2 Publication and notification policies

The revised Certification Practice Statement will be made available by the CCA to the user community through publication on CCA's website.

CCA also notifies the CAs about the revised Certification Practice Statement. The revised Certification Practice Statement is in force from the date and time of publication on CCA's website.

8.3 CPS approval procedures

8.3.1 Items that can change without notification

Editorial, typographical corrections or changes to the contact details shall be made to this Certification Practice Statement without notification.

8.3.2 Changes with notification

The CCA shall give a minimum of 45 days notice to the certificate holders of any substantial changes made to the certification practice statement.

Changes to items, which in the judgment of the CCA will not materially impact a substantial majority of certificate holders may be changed on a minimum 30 days notice. While changes required by law, or those in the judgment of the CCA required to be implemented for the benefit of certificate holders may be made with a reasonable notice period. Notice of all changes made under section 8.3.2 of this certification practice statement will be published on the website of the CCA at http://cca.gov.in/documents.