RCAI CPS

Version 2.0

September 2011

Controller of Certifying Authorities

Department of Information Technology

Ministry of Communications and Information Technology

Document Control

Document Name	RCAI CPS
Status	Release
Version	2.0
Last update	19 September 2011
Document Owner	Controller of Certifying Authorities, India

Signature ----------

Contents

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, technical standards have been framed in Rules and Regulations under the Act. 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. The IT Act aims at promoting the growth of E-Commerce and E-Governance through the use of Electronic Signatures including Public Key Cryptography based digital signatures.

CCA licenses Certifying Authorities (CAs) and exercise supervision over their activities. It is required to certify the public keys of the CAs, 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.

The Certification Practice Statement (CPS) of the Controller of Certifying Authorities states how the PKI component(s) meet the assurance requirements defined in the Certificate Policy(CP) and also 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.

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.

Root Certificate: CCA's self signed certificate which is at the root of the India PKI hierarchy.

Root Key: CCA's key pair is the Root Key.

RCAI: The CA hosting CCA's Root Key and certifies the public keys of all licensed 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.

Certificate Policy (CP): states what assurance can be placed in a certificate issued under this policy. Certificates contain one or more registered certificate policy identifier, which may be used by a Relying Party to decide whether a certificate can be trusted for a particular purpose. CP addresses all aspects associated with the generation, production, distribution accounting, compromise recovery and administration of public key certificates.

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

Controller of Certifying Authorities (CCA): means the Office of the Controller.

Cyber Appellate Tribunal: means the Cyber 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 Repository services.

The RCAI is responsible for:

- Issue of X.509 Public Key Certificate containing the public key of the Licensed CA
- Generating CRLs

The Repository is responsible for:

- Publishing Public Key Certificates and CRLs issued by the RCAI

The CCA issues Licenses 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 Licenses 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.

This CPS is based on the RFC 2527- Internet X.509 PKI Certificate Policy and Certificate Practice Framework. 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 repository. This CPS is referred to as the “RCAI CPS”. All documents issued by the CCA including the CPS can be downloaded from http://cca.gov.in

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 RCAI. RCAI has assigned following OID to this document.

id-India PKI	::= {2.16.356.100}
id-cp	::= {id-India PKI 2}
id-cps	::= {id-RCAI CPS 3}

1.3. Community and Applicability

The India PKI community comprises the CCA, RCAI, Licensed CAs & their subscribers and relying parties. 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.

1.4. Contact Details

1.4.1. Specification administration organization

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

Office of Controller of Certifying Authorities,
Electronics Niketan, 6 CGO Complex,
Lodhi Road, New Delhi- 110 003,
E-Mail: info@cca.gov.in
URL: http://cca.gov.in

1.4.2. Contact Person

Deputy Controller (Technology),
Office of Controller of Certifying Authorities,
Electronics Niketan, 6 CGO Complex, Lodhi Road,
New Delhi- 110 003,
E-Mail: info@cca.gov.in
URL: http://cca.gov.in

2. General Provisions

2.1. Obligations

2.1.1. RCAI obligations

RCAI shall

- Operate as an offline Root CA.
- Operate in accordance with this CPS.
- Accept certificate signing requests from authorized representative of Licensed CAs
- Issue Public Key certificates to the licensed CAs.
- Publish the certificates in the repository.

- Accept the revocation request from the authorized representative of Licenced CAs.
- Immediately publish the CRL after revocation of Licenced CA.
- Issue and publication of routine CRLs.
- Preserve audit logs and certificate issuance process.

2.1.2. The Repository obligation

The repository shall publish

- Public key certificates of licensed CAs
- Certificate Revocation Lists

The availability of the information is through the website, http://cca.gov.in

2.1.3. Licensed CA Obligations

The Licenced CA must:

- protect their private key in a secure manner.
- have CPS approved by CCA
- perform the CA operation as per their India PKI CP, CPS and DSC Interoperability guidelines
- update the CPS when the India PKI CP policy change or in accordance with the CCA guidelines
- publish a name and contact information of the party responsible for this Licenced CA
- maintain a web site and publish the Licence, Sub CA certificates, subscriber certificates and CRLs.
- should revoke all the certificates to subscribers and publish the CRL immediately in the case of compromise of their signing key and this may be reported to RCAI immediately.

2.1.4. Relying Party Obligations

Before relying on a certificate under India PKI hierarchy, Relying parties are obligated to:

- read and comply with the provisions of this CPS.
- verify the purpose of a certificate, its validity period, key usage, class of certificate and path to trust anchor.
- ascertain from the applicable CCA CRL(available on http://cca.gov.in) that the certificate has not been revoked.
- be bound by the liability described in the CPS up on reliance on a certificate.

2.2. Liability

The Government of India disclaims any liability that may arise from use of any certificate issued by the RCAI, 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 RCAI.

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 RCAI 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 governing law is 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 decide appeals filed by individuals aggrieved by the order of 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 endeavor 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 fees

Certificates are issued to CAs as part of the licence granted to them to operate under the IT Act. Within the validity period of the licence, Certificates are issued free of cost to the CA

The fee for issuance of licence shall be twenty five thousand rupees or such other amount as may be prescribed under the IT Act, 2000 rules, regulations, and guidelines from time to time.

2.5.2. Certificate Access Fee

CCA does not levy any fee for accessing certificates through CCAs web site.

2.5.3. Revocation or status information access fees

CCA does not levy any fees for 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.

- Self-signed certificates of RCAI
- Certificates issued to all Licensed CAs
- CPS of RCAI and CAs
- CRLS issued by RCAI

2.6.2. Frequency of publication

Certificates will be published in the repository immediately after issuance and it will be available to public through website http://cca.gov.in .

CRLs will be published in the repository immediately after revocation or once in every 30 days in the case of no revocation

2.7. Audit

The RCAI is audited annually by one of the empanelled auditors maintained by Office of CCA. Compliance audit results are communicated to CCA.

2.7.1. Actions taken as a result of deficiency

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

2.8. Confidentiality

The CCA collects information about the CAs as part of the Licence application. These data are processed in a way that ensures protection of their private information. The information published in the website, their digital signature certificate, and in the CRL are not confidential

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:

- Software and hardware developed by CCA
- Certification Practice Statement of CCA
- Common name of Root Certificates
- 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 Interoperability Guidelines for Digital Signature Certificates (available at cca.gov.in)

3.1.2. Need for names to be meaningful

The Subject name contained in a 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 Interoperability Guidelines for Digital Signature Certificates (available at cca.gov.in)

3.1.4. Uniqueness of names

The CCA shall ensure that the set of names is unambiguous. The name shall conform to X.500 standards and Interoperability Guidelines for Digital Signature Certificates (*available at cca.gov.in*) 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 may 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. Revocation Request

Licensed CAs shall designate an authority, who can request the revocation of its certificate(s). The Controller of Certifying Authorities can also decide to revoke a CA certificate.

4. Operational Requirements

4.1. Licence Application

An application for a licence 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).

On successful completion of evaluation of the application for grant of Licence with respect to the provisions of the IT Act, 2000 and the rules, regulations and guidelines and upon receipt of independent audit report as required under Rule 31, the CCA will commence the process of issuance of Licence.

4.2. Certificate Issuance

Once grant of license to the CA is approved by CCA, the public key certificate is issued after checking the following criteria,

- 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 DN submitted by the applicant.
- The certificate request is used by the CCA to generate the certificate.
- All certificates issued are published in the Repository and are accessible through the web site of the CCA.

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 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.

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

4.4.1. Circumstances for revocation

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;
- 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 licencee does not meet material obligations of its agreements with CCA, those of any applicable CP, 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 the 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 revocation

Revocation request from the following parties can be accepted:

- An Authorized signatory of the Licenced CA

CCA can also order revocation certificates issued to Licenced CAs.

4.4.3. Procedure for revocation request

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

- a certificate revocation request delivered to CCA by an appropriately authorized person.

In processing a revocation request, the CCA will:

- Revoke the certificate, record the reason for the revocation and maintain relevant documentation.
- Publish the CRL on the repository.

4.4.4. 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.

4.4.5. 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.

4.4.6. 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.

4.4.7. Revocation/status checking availability

The CCA shall provide CA certificate status checking through publication of the CRL on the web site

4.4.8. Special requirements regarding key compromise

In case of key compromise the concerned CA shall intimate the CCA immediately for revocation of the CA certificate.

4.5. Security Audit Procedures

4.5.1. Types of event recorded

The minimum audit records of RCAI to be kept include:

SECURITY AUDIT

- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs

IDENTITY-PROOFING

- Successful and unsuccessful attempts to assume a role
- The value of maximum number of authentication attempts is changed
- The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from a password to a biometric

ROOT KEY GENERATION

- Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)

ROOT CA CREATION

- All CA creation parameters including trusted roles

LICENCED CA CERTIFICATE SIGINING

- All certificate PKCS#10 requests signing

CERTIFICATE REVOCATION

- All certificate revocation requests

ACCOUNT ADMINISTRATION

- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified

CERTIFICATE PROFILE MANAGEMENT

- All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT

- All changes to the revocation profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile

MISCELLANEOUS

- Creation of a Trusted Role
- Designation of personnel for multiparty control
- Installation of the Operating System
- Installation of the PKI Application
- Installation of hardware cryptographic modules
- Removal of hardware cryptographic modules
- Destruction of cryptographic modules
- Logon attempts to PKI Application
- Receipt of hardware / software
- Attempts to set passwords
- Attempts to modify passwords
- Restoration from back up of the internal CA database
- Posting of any material to a PKI Repository
- Access to the internal CA database
- All certificate compromise notification requests
- Zeroizing Tokens

CONFIGURATION CHANGES

- Hardware
- Software

- Operating System
- Patches
- Security Profiles

PHYSICAL ACCESS / SITE SECURITY

- Personnel Access to room housing Component
- Access to the Component
- Known or suspected violations of physical security

ANOMALIES

- Software error conditions
- Software check integrity failures
- Equipment failure
- Electrical power outages
- Uninterruptible Power Supply (UPS) failure

4.5.2. Frequency of processing log

The RCAI's audit logs are regularly reviewed by the trusted personnel of Office of CCA 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. Actions 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 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.

4.6. Records Archival

4.6.1. Types of event recorded

Audit information as detailed in §4.5.1 are recorded.

4.6.2. Retention period for archive

All RCAI records concerning the operation of its certification services are archived and are retained for a period of 7 years.

4.6.3. Protection of archive

Archived information is stored in a restricted access facility.

4.6.4. Archive backup procedures

A second copy of all information retained or backed up by CCA shall be stored at the disaster recovery site shall have adequate protection from environmental threats such as temperature, humidity and magnetism.

4.6.5. Requirements for correct source of time

The time source GPS clock for the RCAI ensures that all electronic automated RCAI records are associated with the time and date of their occurrence.

The clock of the computer system shall be synchronized with the GPS clock to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

The 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 staffs are allowed to handle archive.

4.6.7. Procedures to obtain and verify archive information

The integrity of the backups is verified immediately after backup Information stored off-site is also periodically verified for data integrity.

4.7. RCAI Key changeover

On key changeover, a new public key will be made available via the web

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, software and/or data.

4.8.2. Entity key is compromised

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

4.8.3. 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 repository will be re-established on an independent disaster recovery site.

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 CAs 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 archives will be retained in the manner and for the time indicated in 4.6.
- Provide access to 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 RCAI, and the Repository is fully secured in accordance with the requirements laid down under the IT Act.

5.1. Physical Security Controls

5.1.1. Site Location and Construction

The RCAI operations are being conducted from New Delhi

5.1.2. Physical access

Physical access to RCAI for performing operations is controlled and restricted to the authorized individuals only. The RF is provided with physical security round the clock.

5.1.2.1. By-pass or deactivation

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

5.1.2.2. 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.

5.1.2.3. Sensing and preventive measures for RF.

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

The security guard in the RF and the Chief Security Officer (CSO) take the suitable escalation procedures.

5.1.2.4. DVR (Digital Video Recorder) system

The RF is constantly monitored using a CCTV system to detect any unusual activities. Round-the-clock Digital video Recording is also carried out

5.1.3. Power Supply and Air Conditioning

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

5.1.4. Water exposures

The RF is equipped to detect potential water related threats.

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

Storage media are protected from environment threats such as temperature, humidity and magnetic field.

5.1.7. Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Other waste is disposed off in accordance with the normal waste disposal requirements.

5.1.8. 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 RCAI.

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. CA Administrator
d. Auditor

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

Contractors are allowed access to the Root Facility only under the supervision and presence of at least two trusted persons.

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 defined Security procedures 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 minimum FIPS 140-1 level 3 certified.

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's self-signed certificate, along with this CPS and other documentation such as the IT Act, Rules and Regulations, Certificate Policy (CP) are available on CCA's website http://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 as well as the hash algorithm used by the CCA for signing are as per the Interoperability Guidelines.

6.1.6. Public Key Parameters Checking

Not Applicable

6.1.7. Parameter Quality Checking

Not Applicable

6.1.8. 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 minimum FIPS 140-1 level 3.

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

Use of the private key for signing will require multi-person (minimum two) authorisations

6.2.3. Private Key Backup

RCAI Private Key is backed up multi person control and kept in a secure manner.

6.2.4. Method of Destroying Private Key

Private signature keys will be deleted or zeroised when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Prior to disposal, the Hardware cryptographic modules will be physically destroyed.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

All public keys of the CCA will be archived.

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 and CP

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Not Applicable

6.6.2. Security management controls

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

- Security Officer
- System Administrator
- CA Administrator

6.7. Network Security Controls

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

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

CCA issues certificates in conformance with Interoperability Guidelines

7.2. CRL Profile / Certificate Suspension and Revocation List Profile

The CCA issues CRLs in conformance with Interoperability Guidelines

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.

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/