RCAI CPS

Version 4.0

25 February 2019

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	RCAI CPS
Status	Release
Version	4.0
Last update	25 Feb 2019
Document Owner	Controller of Certifying Authorities, India

DEFINITIONS

The following definitions are to be used while reading this CPS. Unless otherwise specified, CPS means CPS of RCAI. Words and expressions used herein and not defined but defined in the Information Technology Act, 2000 and subsequent amendments, hereafter referred to as the ACT shall have the meaning respectively assigned to them in the Act.

The following terms bear the meanings assigned to them hereunder and such definitions are applicable to both the singular and plural forms of such terms:

"Act" means Information Technology IT Act, 2000

"ITAct" Information Technology IT Act,2000, its amendments, Rules thereunder, Regulations and Guidelines Issued by CCA

"Auditor" means any accredited computer security professional or agency recognized and engaged by CCA for conducting audit of operation of CA;

"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;

"RCAI Infrastructure" The architecture, organization, techniques, practices, and procedures that are collectively support the implementation and operation of the RCAI. It includes a set of policies, processes, server platforms, software and work stations, used for the purpose of administering Digital Signature Certificates and keys.

"**Certification Practice Statement or CPS**" means a statement issued by a RCAI to specify the practices that the RCAI employs in issuing Digital Signature Certificates;

"Certificate"— means a Digital Signature Certificate.

"Certificate Issuance"—The actions performed by a CA in creating a Digital Signature Certificate and notifying the Digital Signature Certificate applicant (anticipated to become a subscriber) listed in the Digital Signature Certificate of its contents.

"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

Certificate Revocation List (CRL)—A periodically (or exigently) issued list, digitally signed by Licenced CA or RCAI , of identified Digital Signature Certificates that have been suspended or revoked prior to their expiration dates.

“Controller” or “CCA” means the Controller of Certifying Authorities appointed as per Section 17 subsection (1) of the Act.

"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 IT Act;

Digital Signature Certificate—Means a Digital Signature Certificate issued under sub-section (4) of section 35 of the Information Technology Act, 2000.

“Private Key" means the key of a key pair used to create a digital signature;

"Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

"RCAI"— means "Root Certifying Authority of India"

"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.

"Subscriber Agreement"—The agreement executed between a subscriber and CA for the provision of designated public certification services in accordance with this Certification Practice Statement

"Trusted Person"—means any person who has:-

i. Direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or Rules in respect of a RCAI or Licenced CA, or
ii. Duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of RCAI or Licenced CA's computing facilities.

Table of 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.

India PKI is a hierarchical PKI with the trust chain starting from the Root Certifying Authority of India (RCAI). RCAI is operated by the Office of Controller of Certifying Authorities, Government of India. Below RCAI there are Certifying Authorities (CAs) licensed by CCA to issue Digital Signature Certificates under the provisions of ITAct. These are also called Licensed CAs.

1.1 Overview of CPS

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:

- Generate self signed Root certificate

- 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 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 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 3647- 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 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 Root Certifying Authority of India (RCAI)

In the context of the CPS, the RCAI is responsible for:

1. Developing and administering India PKI CP.
2. compliance analysis and approval of the licensed CAs CPS;
3. Laying down guidelines for Identity Verification , Interoperability of DSCs and Private Key storage
4. Ensuring continued conformance of Licensed CAs with the CPS by examining compliance audit results.
5. The following self signed certificates are maintained by RCAI to issue CA certificate

Sl No	RCAI Common Name	Certified by	Valid upto
1	CCA India 2014	CCA India 2014	2024
2	CCA India 2015 SPL	CCA India 2015 SPL	2025

6. RCAI maintains CRL of CAs

1.3.1.2 CA

The CA is licensed by CCA as per Information Technology Act. The primary function of CA is to issue end entity certificates.

CA certificates are certified by Root Certifying Authority of India (RCAI). In India PKI hierarchy, Root certificate is the trust anchor for CA certificates.

CA optionally create Sub-CAs to issue Digital Signature Certificates. CA issue Digital Signature Certificates to end entities directly. CA also suspends or revokes the Digital Signature Certificates. The CA maintains the Certificate Revocation List (CRL) CA for the revoked and suspended Digital Signature Certificates in its repository. CRL is signed by issuing CA.

1.3.2 PKI Services

Certificate Services: RCAI accepts certificate signing requests from authorized representative of Licensed CAs. RCAI maintains separate special purpose Root for issuing SSL and code signing certificates. Issue Public Key certificates to the licensed CAs. RCAI Publish the certificates in the repository

CRL Services: RCAI accepts the revocation request from the authorized representative of Licensed CAs and also publish CRL in the repository

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificate usage is governed by the IT Act of 2000 and Interoperability Guidelines published by CCA.

1.4.2 Prohibited Certificate Uses

Certificate usage is governed by the IT Act of 2000 and Interoperability Guidelines published by CCA.

1.5 Policy Administration

1.5.1 Organization administering the document

This CPS is administered by CCA and is revised with the approval of CCA.

1.5.2 Contact Person

Questions/Queries regarding this CPS may be directed to the CCA at info@cca.gov.in

Controller
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

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

The determination of suitability of a CPS will be based on an independent auditor's results and recommendations.

1.5.4 CPS Approval Procedures

The CCA approve CPS of the RCAI and auditor's assessment will also be taken into account.

1.5.5 Waivers

There shall be no waivers to this CPS.

2 Publication & PKI Repository Responsibilities

2.1 PKI Repositories

RCAI maintains Hypertext Transfer Protocol (HTTP) based repositories that contain the following information:

1. RCAI certificates
   Self signed Certificates
2. CA Certificates
   Issued to Licensed CAs
3. Certificate Revocation List (CRL)
   Issued by the RCAI

2.1.1 Repository Obligations

RCAI maintains a repository and is available at cca.gov.in

2.2 Publication of Certificate Information

2.2.1 Publication of CA Information

See Section 2.1.

2.2.2 Interoperability

See Section 2.1.

2.3 Publication of Certificate Information

RCAI Certificates and CRLs are published as specified in this CPS in Section **0.**

2.4 Access Controls on PKI Repositories

The PKI Repository information which is not intended for public dissemination or modification is protected.

3 Identification & Authentication

The requirements for identification and authentication are specified under Information Technology Act, Rules and Guidelines issued there under. Before issuing a Certificate, the RCAI ensure that all Subject information in the Certificate conforms to the requirements that have been verified in accordance with the procedures prescribed in this CPS.

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 - Schedule I, supported by such documents and information as required by CCA.

3.1 Naming

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 [CCA-IOG].

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 Anonymity of Subscribers

RCAI does not issue subscriber certificates with anonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

The naming convention used by CCA to identify certificate holders uniquely is specified in the Interoperability Guidelines for Digital Signature Certificates [CCA-IOG].

3.1.5 Uniqueness of Names

Name uniqueness for interoperability or trustworthiness is enforced in association with serial number. The CCA ensures 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.

3.1.6 Recognition, Authentication & Role of Trademarks

No stipulation.

3.1.7 Name Claim Dispute Resolution Procedure

RCAI resolves any name collisions (in association with serial number) brought to its attention that may affect interoperability or trustworthiness. 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.

3.2 Initial Identity Validation

3.2.1 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 140-2 level 3 or higher level device. An independent verification may be performed as a part of the auditing process.

3.2.2 Authentication of Organization user Identity

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, and the rules, regulations and guidelines and upon receipt of independent audit report as required under 31 of IT CA Rules, the CCA will commence the process of issuance of Licence.

3.2.3 Authentication of Individual Identity

The documents mentioned in 3.2.2 ensure the authentication of individual identity

3.2.4 Non-verified Subscriber Information

RCAI does not include non-verified Information provided by Licensed CA in certificates.

3.2.5 Validation of Authority

The CA application form is accepted only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity. The

documents required by CA to establish the applicant's affiliation to organisation is as specified under CCA-CALIC

3.2.6 Criteria for Interoperation

Certificates are issued in accordance with [CCA-IOG] in order to ensure interoperability.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

The Licence to operate as CA is given for a period of 5 years. During the tenure of Licence, CA certificates are issued without further identification and authentication. The Authorized Signatory of the Licensed CA can send request for re-key requests.

3.3.2 Identification and Authentication for Re-key after Revocation

If a certificate has been revoked, the Authorized Signatory of the Licensed CA can request for re-key requests. For Licenced CAs, no identification and authentication is carried out for re-key after revocation.

3.4 Identification and Authentication for Revocation Request

During the tenure of Licence, the revocation request can be submitted by authorized person of CA. For processing a revocation request, the CCA will revoke the certificate, after terms and conditions specified under ACT , record the reason for the revocation and maintain relevant documentation . The CRL will be in the repository.

4 Certificate Life-Cycle Operational Requirements

Communication between RACI and CA are implemented with requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the content being managed.

Physical documents are packaged and transported in a tamper-evident manner by a certified mail carrier to meet integrity and confidentiality requirements.

Based on the content of communication, all, or none of the security services are enforced.

4.1 Certificate requests

Licenced CAs physically submit the certificate signing requests to RCAI in a media with a covering letter from authorised signatory of CA.

4.1.1 Submission of Certificate Application

The application for licence to operate as CA is submitted by the authorised signatory of the organisation.

4.1.2 Enrollment Process and Responsibilities

Once grant of license to the CA is approved by CCA, CA submit request for public key certification. The Licensed CAs must:

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

4.2 Certificate Application Processing

CA verifies the information to be included in the certificate based on the personal interaction, certified supporting documents, and other procedures specified CCA-CALIC and IT Act.

4.2.1 Performing Identification and Authentication Functions

See Section 0 and subsections thereof.

4.2.2 Approval or Rejection of Certificate Applications

Certificate request submitted to the CCA for processing could result in either approval or denial.

4.3 Certificate Issuance

The public key certificate is issued to CA 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 certificate request generated at CA should send to CCA by trusted personals of CA along with an authorization letter from authorised CA representative.
- The CCA establishes the uniqueness of the DN submitted by the applicant.
- The certificate request is used by the CCA to generate the certificate.
- CCA confirm that prior to certify Public keys of CAs under a special purpose trust chain where the corresponding private key of CA is used for issuance SSL and code signing certificates, CA systems are operated in offline mode.
- The acceptance of certificate to be provided by CA prior to publish on the web site of CCA
- All certificates issued are published in the Repository and are accessible through the web site of the CCA.

4.3.1 CA Actions during Certificate Issuance

See section 4.3.

4.3.2 Notification to Subscriber of Certificate Issuance

See section 4.3.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

See section 4.3.

4.4.2 Publication of the Certificate by the CCA

See section 4.3.

4.4.3 Notification of Certificate Issuance by the CCA to Other Entities

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 on its website to enable verification by relying parties.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Not Applicable

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are required to use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, for time remaining in validity and other information as the old one, but a new, extended validity period and a new serial number. Certificates are renewed only if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the CA name and attributes are unchanged.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the CA name and attributes are unchanged. Request for renewal of certificates are not accepted by CCA at present due to the constraint.

4.6.2 Who may Request Renewal

Request for renewal of certificates are not accepted by CCA at present.

4.6.3 Processing Certificate Renewal Requests

Request for renewal of certificates are not accepted by CCA at present.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period. At present CCA does not offer certificate Re-Key option to subscribers.

4.7.1 Circumstance for Certificate Re-key

Request for renewal of certificates are not accepted by CCA at present.

4.7.2 Who may Request Certification of a New Public Key

CA authorised representative can request for certification of new public key.

4.7.3 Processing Certificate Re-keying Requests

Request for re-key of certificates are not accepted by CCA at present.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

No Stipulation

4.9 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,

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

4.9.1 Circumstance for Revocation of a Certificate

The CCA may revoke CA certificate if the CCA has revoked or suspend the Licence issued to CA. The revocation or suspension of Licence may be based on the 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 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.

4.9.2 Who Can Request Revocation of a Certificate

Revocation request from the following parties can be accepted:

- An Authorized signatory of the Licensed CA

CCA can also order revocation certificates issued to Licensed CAs.

4.9.3 Procedure for Revocation Request

When a revocation is requested by any entity external to the CA, 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.

4.9.4 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.

4.9.5 Time within which CCA must Process the Revocation Request

CCA make best efforts to process revocation request within one working day after a valid revocation request is received.

4.9.6 Revocation Checking Requirements for Relying Parties

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.

4.9.7 CRL Issuance Frequency

Even if no changes to the certificates have been made, CRLs will be published once in every 30 days,

4.9.8 Maximum Latency for CRLs

RCAI issue CRLs at least once every 7 days, and the nextUpdate time in the CRL may be no later than 30 days after next update

4.9.9 Online Revocation Checking Availability

CCA made available on-line certificate status checking at http://ocvs.gov.in.

The on-line revocation/status checking provided by CCA meets the requirements for CRL issuance stated in 4.9.7.

4.9.10 Online Revocation Checking Requirements

No stipulation beyond Section 7.3.

4.9.11 Other Forms of Revocation Advertisements Available

Other than implementation of CRLs and on-line revocation status, no other forms of on-line revocation status will be provided by RCAI

4.9.11.1 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

None beyond those stipulated in Section 4.9.7.

4.9.13 Circumstances for Suspension

No stipulation.

4.9.14 Who can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

RCAI supports Online Certificate Status Protocol (OCSP) for obtaining the revocation status of CA certificates.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

Relying Parties are bound to their obligations and the stipulations of this CPS irrespective of the availability of the online certificate status service.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances CA signature key will be escrowed by a third-party.

5 Facility Management & Operational Controls

5.1 Physical Controls

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

By-pass or deactivation

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

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.

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

DVR (Digital Video Recorder) system

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

5.1.1 Site Location & Construction

The system components and operation of CA are contained within a physically protected environment to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information. The technical and physical infrastructure of the Root Facility (RF), established for the operation of the RCAI is fully secured in accordance with the requirements laid down under the IT Act. The RCAI operations are being conducted from New Delhi

CA's primary site consists of four physical security tiers comprising of:

Tier 1: The common area in the vicinity of the RCAI operations set-up where in physical access check is performed. This is the area where common facilities are incorporated.
Tier 2: This is the first level where RCAI operations commence. This is manned by physical security personnel and also enforces physical proximity access control restricting entries only to RCAI authorized personnel.
Tier 3: Enables two factor authentications (biometrics and physical proximity). The CA operations are carried out in this area.
Tier 4: This is where the core RCAI operations are housed. Servers are installed in this area.

Certificate issuance and revocation is done in this area which houses the Certificate Manager server. The Key Ceremony is also done here. The HSM module is housed in this area.

5.1.2 Physical Access

5.1.2.1 RCAI Physical Access

RCAI has implemented mechanism to protect equipments from unauthorized access.

The physical security requirements laid down for the RCAI equipment are:

1. No unauthorized access to the hardware is permitted
2. All removable media and paper containing sensitive plain-text information is stored in secure containers
3. All entry/exits are monitored either manually or electronically.
4. access logs are maintained and inspected periodically
5. Multiple layers of increasing security are provided in areas such as perimeter, building, and RCAI facility
6. Two person physical access controls are required to both the cryptographic module and computer system for RCAI operations.

5.1.3 Power and Air Conditioning

RCAI secure facilities are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power and also these secure facilities are equipped with air conditioning systems to control temperature and relative humidity.

PKI Repositories are provided with uninterrupted power sufficient for a minimum of 24 hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water Exposures

RCAI locations are reasonably protected against floods and other damaging exposure to water.

5.1.5 Fire Prevention & Protection

RCAI facility is equipped to prevent and extinguish fires. Appropriate procedures have also been implemented to minimize the damage due to smoke and fire exposure. These measures also meet all applicable fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information are stored within RCAI facilities and also in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access only authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic exposure).

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. Cryptographic devices are physically destroyed or zeroed in accordance with the manufacturer's guidance prior to disposal. Other waste is disposed of in accordance with the RCAI's normal waste disposal requirements.

5.1.8 Off-Site backup

Full system backups of the RCAI Systems sufficient to recover from system failure, are created on a periodic schedule, and incrementally backup copies are stored at an offsite location. Backups are performed and stored off-site not less than once every 6 months. The data is properly secured based on the classification of data, which is defined by the RCAI in the security policy.

5.2 Procedural Controls

5.2.1 Trusted Roles

RCAI ensures that

1. The person filling the role is trustworthy and properly trained.
2. The functions are distributed among more than one person, so that any malicious activity would require collusion.

RCAI operations are carried out by four roles which are listed below:

1. RCAI Administrator – authorized to install, configure, and maintain the RCAI; establish and maintain user accounts; configure profiles and audit parameters; and generate keys runnel for section system communication.
2. RCAI Officer – authorized to verify and approve certificates or certificate revocations.
3. Audit Administrator – authorized to view and maintain audit logs.
4. System Administrator – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.1.1 RCAI Administrator

The RCAI administrator is responsible for:

1. Installation, configuration, and maintenance of the RCAI;
2. Establishing and maintaining RCAI system accounts;
3. Configuring certificate profiles or templates and audit parameters, and;
4. Generating and backing up RCAI keys.

Administrators shall not issue certificates to subscribers.

5.2.1.2 RCAI Officer

The RCAI officer is responsible for issuing certificates, that is:

1. Registering CAs and requesting the issuance of certificates;
2. Verifying the CA details and accuracy of information included in certificates;
3. Approving and executing the issuance of certificates, and;
4. Requesting, approving and executing the revocation of certificates.

5.2.1.3 Audit Administrator

The Audit Administrator is responsible for:

1. Reviewing, maintaining, and archiving audit logs;
2. Performing or overseeing internal compliance audits to ensure that the RCAI is operating in accordance with its CPS;

5.2.1.4 System Administrator

The System Administrator is responsible for the routine operation of the RCAI equipment and operations such as system backups and recovery or changing recording media.

5.2.2 Number of Persons Required per Task

Separate individuals are identified for each trusted role to ensure the integrity of the RCAI operations. Two or more persons are required to perform the CA Certificates issuance and CRL generation:

1. RCAI key generation;
2. RCAI signing key activation; and
3. RCAI private key backup.

In addition, sensitive RCAI operations like operations of the cryptographic units and certificate manager requires the m-out-of-n control to handle the operations of

these sensitive functions. Also split control is implemented to ensure segregations between physical and logical access to systems. Personnel having secret shares do not have physical access and vice-versa. All roles are assigned to multiple persons in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

All personnel seeking to become trusted persons are in the payroll of RCAI. Thorough background checks are carried out prior to engaging such personnel for RCAI Operations. The Certifying Authority follow the procedures approved in Government for the background check and there are documented for audit purpose.

RCAI ensures that personnel have achieved trusted status and approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities
- Issued electronic credentials to access and perform specific functions on RCAI's IT systems.

5.2.4 Roles Requiring Separation of Duties

Role separation is enforced either by the RCAI equipment, or procedurally, or by both means. Individuals may assume more than one role, except:

1. Individuals who assume an RCAI Officer role will not assume RCAI Administrator or Audit Administrator role;

2. Individuals who assume an Audit Administrator role will not assume any other role on the RCAI ; and

3. Under no circumstances any of the four roles will perform its own compliance audit function.

No individual will be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles shall be selected on the basis of trustworthiness, and integrity, and shall be subject to background investigation. Personnel will be appointed to trusted roles on the basis of:

1. Having successfully completed an appropriate training program;
2. Having demonstrated the ability to perform their duties;

3. Being trustworthy;
4. Having no other duties that would interfere or conflict with their duties for the trusted role;
5. Having not been previously relieved of duties for reasons of negligence or non-performance of duties;
6. Having not been denied a security clearance, or had a security clearance revoked for cause;
7. Having not been convicted of an offense; and
8. Being appointed in writing by an appointing authority.

5.3.2 Background Check Procedures

All persons filling trusted roles shall have completed a favorable background investigation. The scope of the background check shall include the following areas covering the past five years:

1. Employment;
2. Education (Regardless of the date of award, the highest educational degree shall be verified);
3. Place of residence (3 years);
4. Law Enforcement; and
5. References

The results of these checks will not be released except as required in Sections 9.3 and 9.4

5.3.3 Training Requirements

RCAI ensures that all personnel performing duties with respect to the operation of a Certifying Authority receive comprehensive training. Training will be conducted in the following areas:

1. RCAI security principles and mechanisms
2. All PKI software versions in use on the CA system
3. All PKI duties they are expected to perform
4. Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Training (awareness) is conducted to make the trusted personnel aware of any significant change to the operations, and the executions of such plan are documented. Such changes are RCAI software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Periodic security awareness and any new technology changes training is provided on an ongoing basis, based on the newer versions or releases of the products.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

RCAI will take appropriate administrative and disciplinary actions against personnel who violate this policy. Action taken and will be documented.

5.3.7 Documentation Supplied To Personnel

All the relevant documents relating to RCAI operation required for trusted personnel to perform their duties such as Certificate Policy, the applicable CPS, user Manuals, Administrator Manual, policies or contracts etc are made available to RCAI personnel. RCAI maintains the documents identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

Audit log files are generated for all events relating to the security of the RCAIs. The security audit logs either automatically collected or if not possible, a logbook, paper form, or other physical mechanism are used. All security audits logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2.

5.4.1 Types of Events Recorded

All security auditing capabilities of the RCAI operating system and the RCAI applications required by this CPS are enabled. Each audit record shall include the following (either recorded automatically or manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. Success or failure where appropriate, and
4. The identity of the entity and/or operator that caused the event.

The following events shall be audited:

Auditable Event	RCAI
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	
LOCAL DATA ENTRY	
All security-relevant data that is entered in the system	
DATA EXPORT AND OUTPUT	
All successful and unsuccessful requests for confidential and security-relevant information	
KEY GENERATION	
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	
PRIVATE KEY LOAD AND STORAGE	
The loading of Component private keys	
All access to certificate subject Private Keys retained within the CA for key recovery purposes	
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	
All changes to the trusted Component Public Keys, including additions and deletions	
PRIVATE AND SECRET KEY EXPORT	
The export of private and secret keys (keys used for a single session or message are excluded)	
CERTIFICATE REGISTRATION	
All certificate requests	
CERTIFICATE REVOCATION	
All certificate revocation requests	
CERTIFICATE STATUS CHANGE APPROVAL	

Auditable Event	RCAI
The approval or rejection of a certificate status change request	
CONFIGURATION	
Any security-relevant changes to the configuration of the Component	
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	
CERTIFICATE STATUS PROVIDERMANAGEMENT	
All changes to the CSP profile (e.g. OCSP profile)	
REVOCATION PROFILE MANAGEMENT	
All changes to the revocation profile	
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	
All changes to the certificate revocation list profile	
MISCELLANEOUS	
Appointment of an individual to 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	
System Startup	
Logon attempts to PKI Application	
Receipt of hardware / software	
Attempts to set passwords	
Attempts to modify passwords	
Back up of the internal CA database	
Restoration from back up of the internal CA database	
File manipulation (e.g., creation, renaming, moving)	
Posting of any material to a PKI Repository	
Access to the internal CA database	
All certificate compromise notification requests	

Auditable Event	RCAI
Loading tokens with certificates	
Shipment of Tokens	
Zeroizing Tokens	
Re-key of the Component	
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	
Receipt of improper messages	
Misrouted messages	
Network attacks (suspected or confirmed)	
Equipment failure	
Electrical power outages	
Uninterruptible Power Supply (UPS) failure	
Obvious and significant network service or access failures	
Violations of Certificate Policy	
Violations of Certification Practice Statement	
Resetting Operating System clock	

5.4.2 Frequency of Processing Audit Logs

Audit logs are examined for key security and operational events immediately after each RCAI operation. In addition, RCAI reviews its audit logs as required in the event of any suspicious or unusual activity based on irregularities and incidents within RCAI systems.

The processing of audit logs includes a review of the audit logs and recording of significant events in an audit log summary. It includes a verification that the log has not been tampered with, a brief inspection of all log entries, and a detailed investigation of any irregularities in the logs. Actions taken based on audit log reviews are recorded.

5.4.3 Retention Period for Audit Logs

See Section 2.

5.4.4 Protection of Audit Logs

System configuration and procedures are implemented together to ensure that:

1. Only authorized people have read access to the logs;
2. Only authorized people may archive audit logs; and,
3. Audit logs are not modified.

After back-up and archived, the audit logs are allowed by the system to be over-written.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be archived as per Section 5.5.1.

5.4.6 Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application and operating system level. Manually generated audit data is recorded by RCAI personnel.

Audit processes are invoked at system startup, and cease only at system shutdown. In the case of failure of audit collection system, RCAI operations are suspended until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

This CPS imposes no requirement to provide notice (that an event was audited) to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit log are recorded, in part, to monitor system vulnerabilities. The logs are reviewed, and appropriate actions are taken following an examination of these monitored events.

5.5 Records Archival

5.5.1 Types of Records Archived

RCAI retains an archive of information and actions that are material to each certificate application and to the creation, Issuance, revocation, expiration, and renewal of each certificate issued by the RCAI. These records include all relevant evidence regarding:

Data To Be Archived
Certification Practice Statement
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration
Certificate requests
Revocation requests
Subscriber identity authentication data as per Section 0
Documentation of receipt and acceptance of certificates
Documentation of receipt of Tokens
All certificates issued or published
All CRLs and CRLs issued and/or published
All Audit Logs
All Audit Log Summaries
Other data or applications to verify archive contents
Compliance audit reports

5.5.2 Retention Period for Archive

Records associated with certificates are archived for a period of 7 years from the date of expiry of the certificate.

5.5.3 Protection of Archive

RCAI protects its archived records so that only authorized persons can access the archived data. RCAI protects the archive against unauthorized viewing, modification, deletion, or other tampering, by storage within a trustworthy system. The media holding the archive data and the systems required to process the archive data are maintained to ensure that the archive data can be accessed for the time period

5.5.4 Archive Backup Procedures

RCAI creates back-up copies of archives compiled as and when the archives are created. Backup copies of the archive and copies of paper-based records are maintained in an off-site disaster recovery/ warehouse facility.

5.5.5 Requirements for Time-Stamping of Records

Archived records are time stamped such that order of events can be determined.

Certificates, CRLs, other revocation databases and usage entries contain time and date information provided by System time, which is synchronized with Indian Standard Time(IST)

5.5.6 Archive Collection System (internal or external)

The archive collection system is internal to the RCAI

5.5.7 Procedures to Obtain & Verify Archive Information

Only RCAI trusted personnel are permitted to access the archived data. Additionally, the archive information may be made available to the CCA upon request.

5.6 Key Changeover

RCAI keys are changed periodically as stipulated by the ITAct and the key changes are processed as per key generation specified in this CPS. RCAI private key is used to sign CRLs . RCAI Keys are retained and protected till the validity period of certificate.

The following table provides the life times for certificates and associated private keys.

Key	**2048 Bit Keys**	
	Private Key	Certificate
Root CA	10 years	10 years
CA	10 years	10 years

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If a RCAI detects a compromise or suspected compromise, it will perform an investigation in order to determine the nature and the degree of damage. If the RCAI key is suspected of compromise, the procedures outlined in Section 5.7.3

shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the RCAI needs to be rebuilt, only some certificates need to be revoked, and/or the RCAI key needs to be declared compromised.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

RCAI have a Disaster Recovery center as per the guidelines of ITAct. The disaster recovery site is update with the latest available backup data.

If RCAI equipment is damaged or rendered inoperative, but the signature keys are not destroyed, RCAI makes all efforts to establish the operation as quickly as possible, giving priority to the ability to generate CRL or make use of Disaster Recovery facility for CRL generation.

If both primary and Disaster recovery sites cannot be used to establish revocation capability in a reasonable time-frame, the RCAI systems will be treated as compromised.

5.7.3 Private Key Compromise Procedures

If RCAI signature keys are compromised or lost,

CCA shall be notified at the earliest feasible time so that RCAI can revoke the CA certificate;

1. It will be published on the website of CCA, notify in the news papers .
2. All the CA certificates issued by RCAI will be revoked.
3. A new CA key pair shall be generated by RCAI in accordance with procedures set forth in this applicable CPS;
4. New CA certificate request will be obtained in accordance with the procedure and certify the requests
5. The RCAI will also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby RCAI installation including DR are physically damaged and all copies of the RCAI Signing Key are destroyed as a result, RCAI will l follow steps 1 through 4 in Section 5.7.3 above.

5.8 RCAI Termination

In the event of termination, RCAI will revoke all CA certificates issued.

RCAI will archive all audit logs and other records prior to termination.

RCAI will destroy all its private keys upon termination.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The following table provides the requirements for key pair generation for the various entities.

Entity	FIPS 140-1/2 Level	Hardware or Software	Generated in Entity Module
RCAI	3	Hardware	Yes
OCSP Responder	3	Hardware	Yes

For RCAI key pair generation, multiparty controls are used as specified in Section 5.2.2. RCAI creates a verifiable audit trail for key pair generation as per the security requirements Procedures which are followed and the same will be documented. The process is validated by an Auditor.

6.1.2 Private Key Delivery to Subscriber

No stipulation

6.1.3 Public Key Delivery to Certificate Issuer

CA generates PKCS#10 requests containing their public key and send it to the RCAI. The requests are physically handed over to RCAI in a media with covering letter of authorized signatory.

6.1.4 CA Public Key Delivery to Relying Parties

RCAI makes its Public Keys available to relying parties in repository available at cca.gov.in/

6.1.5 Key Sizes

The key length and hash algorithms used by RCAI and CA are given below

Cryptographic Function	***Cryptographic Algorithm***
Signature	2048-bit RSA or ECDSA with -p256 curve parameter
Hashing	SHA-256

6.1.6 Public Key Parameters Generation and Quality Checking

RSA and ECC keys are generated in accordance with FIPS 186-2.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Key usages are covered in certificate profiles defined in CCA-IOG.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2 Level 3, Security Requirements for Cryptographic Modules.

The table in Section 6.1.1 summarizes the minimum requirements for cryptographic modules; higher levels may be used.

6.2.2 Private Key Multi-Person Control

Use of a RCAI private signing key requires action by at least two persons.

6.2.3 Private Key Escrow

RCAI creates backup of its signature keys. These are stored in encrypted form and under the sole custody of RCAI

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

RCAI private signature keys are backed up under the same multi-person control as the original signature key. Numbers of backup copies are limited to three and securely stored under the same multi-person control as the operational key.

6.2.4.2 Backup of Subscriber Private Signature Key

The RCAI is never in possession of CA or subscriber's private signing keys.

6.2.5 Private Key Archival

At the end of the validity period, RCAI private key will be destroyed and will not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

RCAI key pairs are generated and secured by hardware cryptographic modules. RCAI ensures that The RCAI private keys are backed up in secure manner and transferred in an encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

RCAI stores Private Keys in hardware cryptographic module and keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 Level 3 rating of the cryptographic module.

6.2.8 Method of Activating Private Key

The RCAI officers must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, Personal Identification Numbers (PINs).

6.2.9 Methods of Deactivating Private Key

Cryptographic module that has been activated is never left unattended or otherwise available to unauthorized access. After use, cryptographic modules are deactivated. After deactivation, the use of the cryptographic modules based RCAI key pair requires the presence of the trusted roles with the activation data in order to reactivate said RCAI key pair.

6.2.10 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.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects Of Key Management

6.3.1 Public Key Archival

All public keys of the CCA will be archived

6.3.2 Certificate Operational Periods/Key Usage Periods

See Section 5.6

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

When they are not used, activation data are always stored in a safe for which access is controlled by holders in limited roles.

6.4.2 Activation Data Protection

The activation data used to unlock private keys is protected from disclosure.

After a predetermined number of failed login attempts, a facility to lock the account temporarily has been provided.

The activation data written on paper is stored securely in a safe.

6.4.3 Other Aspects of Activation Data

RCAI changes the activation data whenever the HSM is re-keyed. RCAI keep sufficient number of cryptographic module to avoid sending HSM for maintenance.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

RCAI is operated in a complete Offline environment. The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards.

1. Require authenticated logins for trusted roles
2. Provide Discretionary Access Control
3. Provide a security audit capability
4. Require a trusted path for identification and authentication
5. Provide self-protection for the operating system

RCAI computer systems are configured with minimum required accounts and network services.

RCAI has implemented a combination of physical and logical security controls to ensure that the RCAI administration is not carried without less than two person control.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the RCAI are as follows:

1. Hardware and software are purchased in such a way so as to reduce the likelihood that any particular component was tampered with.

2. All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location

3. The hardware and software are dedicated to performing the PKI activities. There are no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation.

4. Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required performing the PKI operations is obtained from sources authorized by local policy.

5. RCAI hardware and software are scanned for malicious code on first use and all media to be brought in thereafter.

6.6.2 Security Management Controls

The configuration of the RCAI system as well as any modification and upgrade is documented and controlled. There is a mechanism for detecting unauthorized modification to the RCAI software or configuration. The RCAI software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

6.7 Network Security Controls

CA employs appropriate security measures to ensure that they are guarded against physical and network based intrusion attacks. The systems will be turned on only

when RCAI operation is required and ensured that not connected to any external network

6.8 Time Stamping

All RCAI components are regularly synchronized with a time service such as Indian Standard Time Service. Time derived from the time service is used for establishing the time of:

- Initial validity time of a RCAI & CA Certificate
- Revocation of a CA Certificate
- Posting of CRL updates
- OCSP

Asserted times is accurate to within three minutes. Electronic or manual procedures are used to maintain system time.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificate profiles are detailed in the CCA-IOG

7.2 CRL Profile

The CRL profiles are listed below.

7.2.1 Full and Complete CRL

A RCAI makes a full and complete CRL available to the OCSP Responders as specified below. This CRL is published on the repository.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Per the requirements in [CCA-IOG]
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in Generalized Time)
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CRL Entry Extension	**Value**
Reason Code	c=no; optional

7.2.2 Distribution Point Based Partitioned CRL

RCAI issues only full and complete CRL signed by RCAI

7.3 OCSP Profile

OCSP requests and responses are in accordance with RFC 2560 as listed below.

7.3.1 OCSP Request Format

Requests sent to Issuer RCAI OCSP Responders(http://ocvs.gov.in) are not required to be signed. The following table lists the fields that are expected by the OCSP Responder.

Field	Value
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

7.3.2 OCSP Response Format

See RFC2560 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status[1], thisUpdate, nextUpdate[2],
Responder Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Applicable certificates issued to the OCSP Responder
Response Extension	**Value**
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	**Value**
None	None

[1] If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

[2] The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessments

Annual compliance audit by empanelled Auditor is carried out of RCAI infrastructure apart from half yearly internal audit

8.2 Identity and Qualifications of Assessor

CCA empanel auditors based on the competence in the field of compliance audits, qualifications and thorough familiarity with requirements of the ITAct, CP and CPS. The auditors perform such compliance audits as per the terms of empanelment and also under the guidance of CCA

8.3 Assessor's Relationship to Assessed Entity

The auditor is independent from the entity being audited. CCA determines whether an auditor meets this requirement.

8.4 Topics Covered by Assessment

RCAI has a compliance audit mechanism in place to ensure that the requirements of this CPS are enforced.

8.5 Actions Taken as a Result of Deficiency

CCA may determine that a RCAI is not complying with its obligations set forth in this CPS or the applicable CP. When such a determination is made, CCA take appropriate action on the deficiencies pointed out by the audit so as to secure the operations of RCAI repository and website

8.6 Communication of Results

On completion of audit by an empanelled auditor, Auditor submit an Audit Report, including identification of corrective measures taken or being taken by RCAI, to CCA . The report identifies the version of the CPS used for the assessment.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance and Renewal 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, rules, regulations, and guidelines from time to time.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation Status Information Access Fees

RCAI does not levy any fees for accessing the suspension and revocation list of certificates

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

The refund policy and other payments terms are governed as per the terms in CA licensing procedures mentioned in the ITAct

9.2 Financial Responsibility

RCAI is owned and operated by Government of India .

9.2.1 Insurance Coverage

No Stipulation

9.2.2 Other Assets

No Stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

RCAI offers no protection to CAs and end entities that extends beyond the protections provided in this CPS

9.3 Confidentiality of Business Information

RCAI maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential, or by its nature reasonably is understood to be confidential, and treat such information with the same degree of care and security as the RCAI treats its own most confidential information.

9.4 Privacy of Personal Information

RCAI stores, process, and disclose personally identifiable information in accordance with the provisions of IT Act 2000 & Rules made thereunder..

9.5 Intellectual Property Rights

RCAI will not knowingly violate any intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

RCAI claims all Intellectual Property Rights in and to the Certificates and revocation information that they issue. However, permission to reproduce and distribute Certificates and revocation information on a nonexclusive royalty-free, world-wide basis, may be granted provided that the recipient agrees to distribute them at no cost.

9.5.2 Property Rights in the CPS

This CPS is based on the proforma CPS published by CCA and as amended from time-to-time. All Intellectual Property Rights in this CPS pertaining to RCAI are owned by the CCA.

9.5.3 Property Rights in Names

RCAI may claim all rights, if any, in any trademark, service mark, or trade name of its services under the law for the time being in force.

9.5.4 Property Rights in Keys

RCAI may claim property rights to the keys used (e.g., RCAI key pair, OCSP Responder key pair etc.) under the law for the time being in force

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

9.6.1.1 RCAI

RCAI warrants

1. Operate as an offline Root CA.

2. Operate in accordance with this CPS.
3. Accept certificate signing requests from authorized representative of Licensed CAs
4. Maintain separate special purpose Root for issuing SSL and code signing certificates.
5. Issue Public Key certificates to the licensed CAs.
6. Publish the certificates in the repository.
7. Accept the revocation request from the authorized representative of Licensed CAs.
8. Immediately publish the CRL after revocation of Licensed CA.

9.6.1.2 Licensed CA

Licensed CA represents and warrants in accordance with provisions of IT Act, 2000 & Rules made thereunder that;

1. signing private key is protected and that no unauthorized person shall ever has access to that private key;
2. Each Subscriber has been required to represent and warrant that all information supplied by the Subscriber in connection with, and/or contained in the Certificate is true.
3. Only verified information appears in the certificate

9.6.2 Subscriber

No stipulation

9.6.3 Relying Party

Parties who rely upon the certificates issued under a policy defined in this document shall:

1. Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
2. Check each certificate for validity, using procedures described in RFC 5280, prior to reliance;

9.6.4 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, RCAI disclaims all warranties other than any express warranties contained in such agreements or set forth in this CPS.

9.8 Limitations of Liabilities

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 RCAI 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 RCAI 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.

9.9 Indemnities

No Stipulation

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon approval by CCA. Amendments to this CPS become effective upon ratification by approval by CCA and publication by RCAI at cca.gov.in. There is no specified term for this CPS.

9.10.2 Termination

While this CPS may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by CCA.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, RCAI is nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. The sections 5.5 and 9.0 of this CPS shall survive the termination or expiration of this CPS.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, CCA uses commercially reasonable methods to communicate, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

RCAI will review this CPS at least once every year. Additional reviews may be enacted at any time at the discretion of the CCA.

RCAI will use reasonable efforts to notify CAs and relying parties of changes.

9.12.2 Notification Mechanism and Period

Errors and anticipated changes to this CPS resulting from reviews will be published online at cca.gov.in.

This CPS and any subsequent changes is made publicly available within seven days of approval.

9.12.3 Circumstances under Which OID Must be Changed

CCA determines the requirement for changing the Certificate Policy OIDs.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among Licensed CAs and Customers

Unless the provision for dispute resolution under the ITAct is invoked, any dispute based on the contents of this CPS, between CA and one of its customers who has availed specific services will be resolved according to provisions in the applicable agreement between the parties.

Any dispute based on the contents of this CPS, between/among CAs shall be resolved by CCA.

9.13.2 Alternate Dispute Resolution Provisions

No stipulations.

9.14 Governing Law

The laws of India and more particularly the Information Technology Act, 2000, The Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001, and the guidelines issued and clarifications made from time to time by the Controller of Certifying Authorities, Ministry of Electronics and Information Technology shall govern the construction, validity, enforceability and performance of actions per this CPS.

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CPS or any of its rights or duties under this CPS, without the prior written consent of CCA. Further, the Office of CCA in its discretion may assign and delegate this CPS to any party of its choice.

9.16.3 Severability

If any provision of this CPS is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4 Waiver of Rights

No waiver of any breach or default or any failure to exercise any right hereunder is construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CPS are for convenience only and cannot be used in interpreting this CPS.

9.16.5 Force Majeure

RCAI is not liable for any failure or delay in its performance under this CPS due to causes that are beyond their reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.

9.17 Other Provisions

No stipulation.

10 Bibliography

The following documents were used in part to develop this CPS:

FIPS 140-2	Security Requirements for Cryptographic Modules, 1994-01 http://csrc.nist.gov/cryptval/
FIPS 186-2	Digital Signature Standard, 2000-01-27 http://csrs.nist.gov/fips/fips186.pdf
ITACT 2000	The Information Technoligy Act, 2000, Government of India, June 9, 2000.
RFC 3647	Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu. November 2003.
CCA-IOG	Interoperability Guidelines for DSC ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CP	X.509 Certificate Policy for India PKI ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-IVG	Identity Verification Guidelines,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-TSG	Time Stamping Services Guidelines for CAs,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-OCSP	OCSP Service Guidelines for CAs,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-SSL	Guidelines For Issuance Of SSL Certificates, http://www.cca.gov.in/cca/?q=guidelines.html
CCA-OID	OID Hierarchy for India PKI(OID) ,http://www.cca.gov.in/cca/?q=guidelines.html
CA-ESIGNAUTH	e-authentication guidelines ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-ESIGNAPI	eSign API Specifications,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CASITESP	CA SITE SPECIFICATION,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CRYPTO	Security Requirements for Crypto Devices ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CALIC	CA Licensing Guidelines ,http://www.cca.gov.in/cca/?q=guidelines.html

11 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CA	Certifying Authority
CCA	Controller of Certifying Authorities
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Status Provider
DN	Distinguished Name
DNS	Domain Name Service
FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
HR	Human Resources
HTTP	Hypertext Transfer Protocol
IAO	Information Assurance Officer
ID	Identifier
IETF	Internet Engineering Task Force
IT	Information Technology
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RCAI	Root Certifying Authority Of India
SHA-2	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply