# X.509 Certificate Policy for India PKI

Version 1.4

May 2015

Controller of Certifying Authorities

Department of Information Technology

Ministry of Communications and Information Technology

## Document Control

| | |
|---|---|
| Document Name | X 509 Certificate Policy for India PKI |
| Status | Release |
| Version | 1.4 |
| Last update | 05 May 2015 |
| Document Owner | Controller of Certifying Authorities, India |

# Table of Contents

# 1 Introduction

This Certificate Policy (CP) defines certificate policies to facilitate interoperability among subscribers and relying parties for e-commerce and e-governance in India. The CP and Certifying Authorities (CAs) are governed by the Controller of Certifying Authorities (CCA). Secure e-commerce and e-governance in India is governed by the Information Technology (IT) Act 2000. In support of the IT Act of 2000, the Government of India has developed and implemented the India Public Key Infrastructure (India PKI).

The 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 IT Act. CAs can be private sector companies, Government departments, public sector companies, or Non-Government Organizations (NGOs). These are also called Licensed CAs

The certificate policies apply to all components of the India PKI, if applicable. Examples of India PKI components include but are not limited to RCAI, CAs, Registration Authorities (RAs), and repositories.

Any use of or reference to this CP outside the purview of the India PKI is completely at the using party's risk. A CA that is not a member of the India PKI shall not assert the object identifiers (OIDs) listed in Section 1.2 of this CP in any certificates the CA issues.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework. Organization Hierarchy

## 1.1 Overview

### 1.1.1 Certificate Policy (CP)

Certificates contain one or more registered certificate policy OID, which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OIDs also publishes the CP, for examination by Relying Parties.

### 1.1.2 Relationship between CP and CPS

This CP states what assurance can be placed in a certificate issued under this policy. A Certification Practice Statement (CPS) for PKI component(s) states how the PKI component(s) meet the assurance requirements.

## 1.2 Document Identification

There are three levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an OID that can be asserted in certificates issued by the India PKI if the certificate issuance meets the requirements for that assurance level. The OIDs are registered under the CCA arc as follows:

| | |
|---|---|
| id-India PKI | ::= {2.16.356.100} |
| id-cp | ::= (id-India PKI 2} |
| id-class0 | ::= {id-cp 0} |
| id-class1 | ::= {id-cp 1} |
| id-class2 | ::= {id-cp 2} |
| id-class3 | ::= {id-cp 3} |
| Id-Aadhaar-eKyc | ::= {id-cp 4} |
| Id-OTP | ::= (Id-Aadhaar-eKyc 1} |
| Id-biometric | ::= (Id-Aadhaar-eKyc 2} |

Unless otherwise stated, a requirement stated in this CP applies to all assurance levels. The assurance levels asserted above are hierarchical with Class 3 being the highest level of assurance.

**OID for document signer certificates and key generation witness**

| | |
|---|---|
| id-India PKI | ::= {2.16.356.100} |
| id-cu (certificate usage) | ::= {id- India PKI 10} |
| id-document signer | ::= {id-cu 1} |
| id-key generation witness | ::= {id-cu 2} |

## 1.3 PKI Participants

### 1.3.1 PKI Authorities

1.3.1.1 Controller of Certifying Authorities (CCA)

The CCA is responsible for:

1. Drafting and approval of the India PKI CP;.
2. Commissioning compliance analysis and approval of the licensed CAs CPS;
3. Accepting and processing applications from Entities desiring to become Licensed CA; and
4. Ensuring continued conformance of Licensed CAs with this CP by examining compliance audit results.

#### 1.3.1.2 Root Certifying Authority of India (RCAI)

A Root CA is a trust anchor for subscribers of a PKI domain when the subscribers act as relying party. The Root Certifying Authority of India (RCAI) shall be controlled by and operated under the direction of CCA.

SSL and code signing certificates shall be issued from the special purpose trust chain created specifically for that purpose. The special purpose trust chain shall be operated in offline mode at Root CA and CA level.

#### 1.3.1.3 Intermediate CA

An Intermediate CA is one that Licensed by CCA as per Information Technology Act. The Intermediate CA is not a Root CA and its primary function is to issue certificates to sub-CAs. In case Intermediate CAs wish to issue end entity certificates then no Sub-CAs can be used in its operations. Intermediate CAs can only issue end entity certificates whenever required to facilitate in-house CA operations.

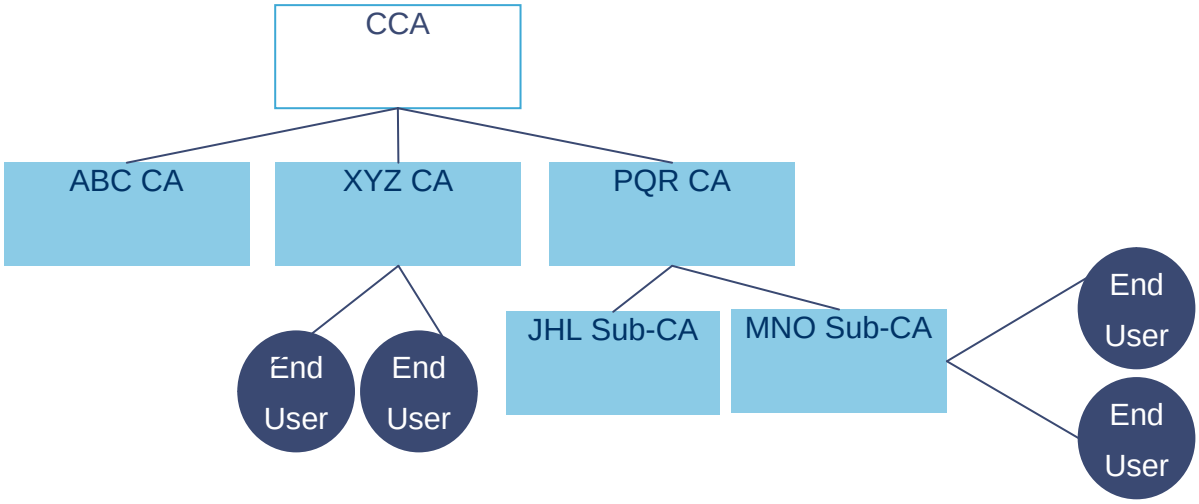
A CA with sub-CA must necessarily issue end entity certificates only through its sub-CA. A CA should have an offline certificate issuance system for issuance of SSL and Code signing certificates under special purpose trust chain

#### 1.3.1.4 Sub-CA

A Certifying Authority can create sub-CAs to meet the business branding requirement. These sub-CAs, which will be part of the same legal entity as the CA, will issue certificates to the end entities or subscribers. A sub-CA shall not issue certificates to other CAs or sub-CAs.

The sub-CA model will be based on the following principles:

- The CAs MUST NOT have more than ONE level of sub-CA
- The sub-CA MUST use a sub-CA certificate issued by the CA for issuing end entity certificates
- The sub-CA must necessarily use the CAs infrastructure for issuing certificate
- The sub-CAs operations shall be subject to same audit procedures as the CA
- The certificate policies of the sub-CA must be same as or sub-set of the CA's certificate policies




1.3.1.5 Certificate Status Provider (CSP)

A CSP is an authority that provides status of certificates or certification paths. CSP can be operated in conjunction with the CAs or independent of the CAs. Examples of CSP are:

1. Online Certificate Status Protocol (OCSP) Responders that provide revocation status of certificates.

2. Standard Based Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services.

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide certificate validation services shall adhere to the same security requirements as repositories.

### 1.3.2 Registration Authority (RA)

An RA is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificate. An RA interacts with the CA to enter and approve the subscriber certificate request information.

### 1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

### 1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, or to identify the creator of a message,. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

### 1.3.5 Applicability

The following are general guidelines. Additional guidelines are available in IT Act of India 2000 and specific guidelines from CCA.

| Assurance Level | Assurance | Applicability |
|---|---|---|
| Class 0 | This certificate shall be issued only for demonstration / test purposes. | This is to be used only for demonstration / test purposes. |
| Class 1 | Class 1 certificates shall be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases. | This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. |
| Class 2 | These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases. | This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial |
| Class 3 | This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities. | This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. |
| Aadhaar-eKyc - OTP | Aadhaar OTP class of certificates shall be issued for individuals use based on OTP authentication of subscriber through Aadhaar eKyc. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as | This level is relevant to environments where OTP based Aadhaar-eKyc authentication is acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time usage at this |

| | | |
|---|---|---|
| | Aadhaar holder | assurance level. |
| Aadhaar-eKyc - biometric | Aadhaar biometric class of certificates shall be issued based on biometric authentication of subscriber through Aadhaar eKyc service. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder. | This level is relevant to environments where biometric based Aadhaar-eKyc authentication is acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time usage at this assurance level |

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Uses

Certificate usage shall be governed by the IT Act of 2000 and Interoperability Guidelines from CCA.

### 1.4.2 Prohibited Certificate Uses

Certificate usage shall be governed by the IT Act of 2000 and Interoperability Guidelines from CCA.

## 1.5 Policy Administration

### 1.5.1 Organization administering the document

The CCA is responsible for all aspects of this CP.

### 1.5.2 Contact Person

Questions regarding this CP shall be directed to the CCA at info@cca.gov.in

### 1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

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

### 1.5.4 CPS Approval Procedures

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

### 1.5.5 Waivers

There shall be no waivers to this CP.

# 2 Publication & PKI Repository Responsibilities

## 2.1 PKI Repositories

Licensed CAs shall operate Hypertext Transfer Protocol (HTTP) or LDAP based repositories that provide the following information:

1. CA Certificates
   Issued to their sub-CAs

2. Certificate Revocation List (CRL)
   a) Issued by the Licensed CA
   b) Issued by their sub-CAs

3. Digital Signature Certificates issued by Licensed CA/sub-CA

### 2.1.1 Repository Obligations

Repository shall have high availability.

## 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

Certificates and certificate status information shall be published as specified in this CP in Section **4.**

## 2.4 Access Controls on PKI Repositories

Any PKI Repository information not intended for public dissemination or modification shall be protected.

# 3 Identification & Authentication

## 3.1 Naming

### 3.1.1 Types of Names

The CAs shall generate and sign certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields. Subject Alternative Name may also be used, if marked non-critical. Further requirements for name forms are specified in [CCA-PROF].

### 3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

All DNs and associated directory information tree shall accurately reflect organizational structures.

When DNs are used, it is preferable that the common name represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

### 3.1.3 Anonymity or Pseudonymity of Subscribers

CA and subscriber certificates shall not contain anonymous or pseudonymous identities.

### 3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be in accordance with applicable Standards.

### 3.1.5 Uniqueness of Names

Name uniqueness of Root CA, licensed CA and SubCA shall be enforced.

### 3.1.6 Recognition, Authentication & Role of Trademarks

No stipulation.

### 3.1.7 Name Claim Dispute Resolution Procedure

The CCA shall resolve any name collisions (other than subscribers) brought to its attention that may affect interoperability or trustworthiness.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the issuing CA. The CA shall then validate the signature using the party's public key. The CCA may allow other mechanisms that are at least as secure as those cited here.

### 3.2.2 Authentication of Organization user Identity

Requests for certificates in the name of an organizational user shall include the user name, organization name, address, and documentation of the existence of the organization. The CA or an RA shall verify the information relating to the authenticity of the requesting representative

### 3.2.3 Authentication of Individual Identity

A CA shall ensure that the applicant's identity information is verified. The CA or an RA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the applicable CPS. The process documentation and authentication requirements shall include the following:

1. The identity of the person performing the identity verification;
2. A signed declaration by that person that he or she verified the identity of the applicant;
3. The applicant shall present one photo ID. The applicant shall also present a document as a proof of residential address.
4. Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant;
5. The date and time of the verification; and
6. A declaration of identity signed by the applicant using a handwritten signature or equivalent per Indian Laws.

For Class 3 certificates, identity shall be established by in-person proofing before the RA, to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the RA and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement.

3.2.3.1 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the component shall have a

human sponsor. The PKI sponsor shall be responsible for providing the following registration information:

1. Equipment identification (e.g., serial number) or service name (e.g., Domain Name Service (DNS) name)
2. Equipment public keys
3. Contact information to enable the CA or RA to communicate with the sponsor when required

### 3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

### 3.2.5 Validation of Authority

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

### 3.2.6 Criteria for Interoperation

Certificates shall be issued in accordance with [CCA-PROF] 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 CAs and subscribers shall identify themselves through use of their current Signing Key or by using the initial identity-proofing process as described above.

Identity shall be established through the initial identity-proofing process for each assurance level per the table below:

| Assurance Level | Initial Identity Proofing |
|---|---|
| Class 1 | Every 3 Years |
| Class 2 | Every 3 Years |
| Class 3 | Every 3 Years |

When current Signing Key is used for identification and authentication purposes, the life of the new certificate shall not exceed beyond the initial identity-proofing times specified in the table above.

### 3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than during a renewal action, the subject (i.e., a CA or an end entity) is required to go through the initial registration process described in Section 3.2 to obtain a new certificate.

## 3.4 Identification and Authentication for Revocation Request

Revocation requests shall be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated public key, regardless of whether or not the private key has been compromised.

In the case of loss of key, RA/CA can suspend/revoke the certificate on verifying the subscriber's identity. In the case where subscriber is not in a position to communicate (death, unconscious state, mental disorder), on receiving such information RA or CA can suspend the certificate and after verification the certificate can be revoked.

# 4 Certificate Life-Cycle Operational Requirements

Communication among the CA, RA, and subscriber shall have requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the assurance level of the certificate being managed. For example, packages secured and transported in a tamper-evident manner by a certified mail carrier meet the integrity and confidentiality requirements for Class 3 assurance level. When cryptography is used, the mechanism shall be at least as strong as the certificates being managed. For example, web site secured using Class 2 Secure Socket Layer (SSL) certificate and set up with appropriate algorithms and key sizes satisfies the integrity and confidentiality requirements for Class 2 certificate management.

The content of communication shall dictate if some, all, or none of the security services are required.

## 4.1 Certificate requests

Requests by a Licensed CA for CA certificate shall be submitted to the CCA using a procedure issued by Office of CCA. The CCA shall make the procedure available to all entities. The application shall be accompanied by a CPS written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647].

The CCA shall evaluate the application in accordance with the provisions under the IT Act , and make a determination regarding whether or not to issue the requested certificate(s), depending on the results of audit of the CPS per section 1.5 and subsections thereof. Upon issuance, each certificate issued by the RCAI shall be manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is published or delivered to the Subject CA.

### 4.1.1 Submission of Certificate Application

For CA certificate requests to the RCAI, an authorized representative of the Licensed CA shall submit the request to the CCA.

For end entity certificates, the Licensed CA CPS shall describe the submission process.

### 4.1.2 Enrollment Process and Responsibilities

Applicants for public key certificates shall be responsible for providing accurate information in their applications for certification.

## 4.2 Certificate Application Processing

It is the responsibility of the CA to verify that the information in certificate applications is accurate. Applicable CPS shall specify procedures to verify information in certificate applications.

### 4.2.1 Performing Identification and Authentication Functions

See Section 3.2.3 and subsections thereof.

### 4.2.2 Approval or Rejection of Certificate Applications

A CA may approve or reject a certificate application.

## 4.3 Certificate Issuance

Upon receiving a request for a certificate, the CA shall respond in accordance with the requirements set forth in applicable CPS.

If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought. .

### 4.3.1 CA Actions during Certificate Issuance

A CA shall verify the source of a certificate request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, a CA shall post the certificate as set forth in the CA's CPS.

### 4.3.2 Notification to Subscriber of Certificate Issuance

A CA shall notify a subject (End Entity Subscriber) of certificate issuance.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct Constituting Certificate Acceptance

The subject must confirm acceptance of the certificate upon notification of issuance by the CA.

### 4.4.2 Publication of the Certificate by the CA

See Section 2.1.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

## 4.5 Key Pair and Certificate Usage

### 4.5.1 Subscriber Private Key and Certificate Usage

Subscribers and CAs shall protect their private keys from access by any other party.

Subscribers and CAs shall use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them.

### 4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall 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, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. 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 compromised, and the Subscriber 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 Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirement listed in Section 3.3.1 shall also be met.

### 4.6.2 Who may Request Renewal

A Subject may request the renewal of its certificate.

A PKI Sponsor may request renewal of component certificate.

A CA may request renewal of its subscriber certificates, e.g., when the CA re-keys.

### 4.6.3 Processing Certificate Renewal Requests

A certificate renewal shall be achieved using one of the following processes:

1. Initial registration process as described in Section 3.2; or
2. Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.

### 4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

### 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

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and reestablishes its identity. 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.

### 4.7.1 Circumstance for Certificate Re-key

A CA may issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled to a certificate.

### 4.7.2 Who may Request Certification of a New Public Key

A Subject may request the re-key of its certificate.

A PKI Sponsor may request may request re-key of component certificate.

### 4.7.3 Processing Certificate Re-keying Requests

A certificate re-key shall be achieved using one of the following processes:

1. Initial registration process as described in Section 3.2; or
2. Identification & Authentication for Re-key as described in Section 3.3.

### 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 and Suspension

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

### 4.9.1 Circumstance for Revocation of a Certificate

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

1. Identifying information or affiliation components of any names in the certificate become invalid;
2. The Subject can be shown to have violated the stipulations of its agreement with the CA;
3. The private key is suspected of compromise; or
4. The Subject or other authorized party (as defined in the applicable CPS) asks for the subscriber's certificate to be revoked.
5. Key Lost
6. Subscriber is not in a position to use certificate(Death – copy of Death certificate made available to the issuing CA)

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire. A revoked certificate shall appear on at least one CRL.

### 4.9.2 Who Can Request Revocation of a Certificate

A certificate subject, human supervisor of a human subject (for organizational user), Human Resources (HR) person for the human subject (for organizational user), PKI Sponsor for component, or issuing CA, may request revocation of a certificate.

For CA certificates, authorized individuals representing the Licensed CA may request revocation of certificates.

### 4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed by the subject).

Upon receipt of a revocation request, a CA shall authenticate the request and then revoke the certificate.

### 4.9.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

### 4.9.5 Time within which CA must Process the Revocation Request

A CA shall make best efforts to process revocation request so that it is posted in the next CRL unless a revocation request is received and approved within two hours of next CRL generation.

### 4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

### 4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. A CA shall ensure that superseded certificate status information is removed from the PKI Repository upon posting of the latest certificate status information.

CRLs shall be published not later than the next scheduled update.

At least once every 7 days for Root with minimum validity period of 30 days; At Least Once every 24 hours for all others with minimum validity of 7 days.

In addition, if a certificate is revoked for the reason of CA compromise or key compromise, the issuing CA shall issue and post a CRL immediately.

### 4.9.8 Maximum Latency for CRLs

CRLs shall be published immediately after generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL. CAs must issue CRLs at least once every 24 hours, and the nextUpdate time in the CRL may be no later than 7 days after issuance time (i.e., the thisUpdate time).

### 4.9.9 Online Revocation Checking Availability

In addition to CRLs, CAs and Relying Party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

If on-line revocation/status checking is supported by a CA, the latency of certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed 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

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

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. (check section numbering)

### 4.9.13 Circumstances for Suspension

Suspension shall be permitted in the event that a user's token is temporarily unavailable to them.

### 4.9.14 Who can Request Suspension

A human subscriber, human supervisor of a human subscriber (organizational user), Human Resources (HR) person for the human subscriber (organizational user), issuing CA, may request suspension of a certificate.

### 4.9.15 Procedure for Suspension Request

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed).

The reason code CRL entry extension shall be populated with "certificate Hold". The Hold Instruction Code CRL entry extension shall be absent.

### 4.9.16 Limits on Suspension Period

A certificate may only be suspended for up to 15 days. If the subscriber has not removed their certificate from hold (suspension) within that period, the certificate shall be revoked for the reason of "Key Compromise".

In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity shall be authenticated in person using initial identity proofing process described in Section 3.2.3.

## 4.10 Certificate Status Services

CAs are not required to support online certificate status services such as SCVP.

### 4.10.1 Operational Characteristics

No stipulation.

### 4.10.2 Service Availability

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

### 4.10.3 Optional Features

No stipulation.

## 4.11 End of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

## 4.12 Key Escrow and Recovery

### 4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances shall a CA or end entity signature key be escrowed by a third-party.

# 5 Facility Management & Operational Controls

## 5.1 Physical Controls

Physical security controls shall be in accordance with the Information Technology (IT) Act of 2000, India and guidelines from CCA.

### 5.1.1 Site Location & Construction

The location and construction of the facility housing CA and CSP equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA and CSP equipment and records.

### 5.1.2 Physical Access

5.1.2.1 CA Physical Access

CA and CSP equipment shall always be protected from unauthorized access. The physical security requirements pertaining to CA and CSP equipment are:

1. Ensure no unauthorized access to the hardware is permitted
2. Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
3. Be manually or electronically monitored for unauthorized intrusion at all times
4. Ensure an access log is maintained and inspected periodically
5. Provide at least three layers of increasing security such as perimeter, building, and CA room
6. Require two person physical access control to both the cryptographic module and computer system for CAs issuing Class 1, Class 2 and Class 3 certificates.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA and CSP equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

1. The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”);
2. For off-line CAs, all equipment other than the PKI Repository is shut down);

3. Any security containers are properly secured;
4. Physical security systems (e.g., door locks, vent covers) are functioning properly; and
5. The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

### 5.1.3 Power and Air Conditioning

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support continuity of operations.

### 5.1.4 Water Exposures

No stipulation.

### 5.1.5 Fire Prevention & Protection

No stipulation.

### 5.1.6 Media Storage

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

### 5.1.7 Waste Disposal

Sensitive waste material shall be disposed off in a secure fashion.

### 5.1.8 Off-Site backup

Full system backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups shall be performed and stored off-site not less than once every 7 days. At least one full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are drawn in terms of four roles listed below:

1. CA Administrator – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. CA Officer – authorized to request or 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 CA Administrator

The administrator shall be responsible for:

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

Administrators shall not issue certificates to subscribers.

#### 5.2.1.2 CA Officer

The CA officer shall be responsible for issuing certificates, that is:

1. Registering new subscribers and requesting the issuance of certificates;
2. Verifying the identity of subscribers 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 shall be responsible for:

1. Reviewing, maintaining, and archiving audit logs;

2. Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

5.2.1.4 System Administrator

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

5.2.1.5 Registration Authority

An RA's responsibilities are:

1. Verifying identity, pursuant to section 3.2;
2. Entering Subscriber information, and verifying correctness;
3. Securely communicating requests to and responses from the CA;

The RA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.6 CSP Roles

A CSP shall have at least the following roles.

The CSP administrator shall be responsible for:

1. Installation, configuration, and maintenance of the CSP;
2. Establishing and maintaining CSP system accounts;
3. Configuring CSP application and audit parameters, and;
4. Generating and backing up CSP keys.

The CSP Audit Administrator shall be responsible for:

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

The system administrator shall be responsible for the routine operation of the CSP equipment and operations such as system backups and recovery or changing recording media.

5.2.1.7 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components that are named as public key certificate subjects. The PKI Sponsor works with the RAs to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.1, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

### 5.2.2 Number of Persons Required per Task

Two or more persons shall be required to perform the following tasks for CAs that issue Class 1, Class 2 or Class 3 certificates:

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

All roles are recommended to have multiple persons in order to support continuity of operations.

### 5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

### 5.2.4 Roles Requiring Separation of Duties

5.2.4.1 Class 1, Class 2 and Class 3

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, except:

1. Individuals who assume an Officer role may not assume an CA Administrator or Audit Administrator role;
2. Individuals who assume an Audit Administrator shall not assume any other role on the CA; and
3. Under no circumstances shall any of the four roles perform its own compliance auditor function.

No individual shall be assigned more than one identity.

## 5.3 Personnel Controls

### 5.3.1 Qualifications, Experience, and Clearance Requirements

A group of individuals responsible and accountable for the operation of each CA and CSP shall be identified. The trusted roles of these individuals per Section 5.2.1 shall be identified.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation. Personnel appointed to trusted roles (including CA trusted roles, and RA role) shall:

1. Have successfully completed an appropriate training program;
2. Have demonstrated the ability to perform their duties;
3. Be trustworthy;
4. Have no other duties that would interfere or conflict with their duties for the trusted role;

5. Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
6. Have not been denied a security clearance, or had a security clearance revoked for cause;
7. Have not been convicted of a felony offense; and
8. Be appointed in writing by an approving authority.

### 5.3.2 Background Check Procedures

All persons filling trusted roles (including CA trusted roles, CSP trusted roles, and RA role), 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 shall not be released except as required in Sections 9.3 and 9.4

Background check procedures shall be described in the CPS. The background shall be refreshed every three years.

### 5.3.3 Training Requirements

All personnel performing duties with respect to the operation of a CA, CSP or a RA shall receive comprehensive training. Training shall be conducted in the following areas:

1. CA/CSP/RA 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

Individuals responsible for trusted roles shall be aware of changes in the CA, CSP, or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, and relocation of equipment.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulation.

### 5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions shall be taken against personnel who violate this policy.

### 5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to CA, CSP, or RA operations shall meet applicable requirements set forth in this CP (e.g., all requirements of Section 5.3).

### 5.3.8 Documentation Supplied To Personnel

The CA and CSP shall make available to its personnel this certificate policy, the applicable CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

## 5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs, CSPs, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be 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 CA, CSP, and RA operating system and the CA, CSP, and RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, 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 | CA | CSP | RA |
|---|---|---|---|
| **SECURITY AUDIT** | | | |
| Any changes to the Audit parameters, e.g., audit frequency, type of event audited | X | X | X |
| Any attempt to delete or modify the Audit logs | X | X | X |
| **IDENTITY-PROOFING** | | | |
| Successful and unsuccessful attempts to assume a role | X | X | X |
| The value of *maximum number of authentication attempts* is changed | X | X | X |
| The number of unsuccessful authentication attempts exceeds the maximum *authentication attempts* during user login | X | X | X |
| An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts | X | X | X |
| An Administrator changes the type of authenticator, e.g., from a password to a biometric | X | X | X |
| **LOCAL DATA ENTRY** | | | |
| All security-relevant data that is entered in the system | X | X | X |
| **REMOTE DATA ENTRY** | | | |
| All security-relevant messages that are received by the system | X | X | X |
| **DATA EXPORT AND OUTPUT** | | | |
| All successful and unsuccessful requests for confidential and security-relevant information | X | X | X |
| **KEY GENERATION** | | | |
| Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys) | X | X | X |
| **PRIVATE KEY LOAD AND STORAGE** | | | |
| The loading of Component private keys | X | X | X |
| All access to certificate subject Private Keys retained within the CA for key recovery purposes | X | N/A | N/A |
| **TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE** | | | |
| All changes to the trusted Component Public Keys, including additions and deletions | X | X | X |
| **PRIVATE AND SECRET KEY EXPORT** | | | |
| The export of private and secret keys (keys used for a single session or message are excluded) | X | X | X |
| **CERTIFICATE REGISTRATION** | | | |
| All certificate requests | X | N/A | X |

| Auditable Event | CA | CSP | RA |
|---|---|---|---|
| **CERTIFICATE REVOCATION** | | | |
| All certificate revocation requests | X | N/A | X |
| **CERTIFICATE STATUS CHANGE APPROVAL** | | | |
| The approval or rejection of a certificate status change request | X | N/A | N/A |
| **CONFIGURATION** | | | |
| Any security-relevant changes to the configuration of the Component | X | X | X |
| **ACCOUNT ADMINISTRATION** | | | |
| Roles and users are added or deleted | X | - | - |
| The access control privileges of a user account or a role are modified | X | - | - |
| **CERTIFICATE PROFILE MANAGEMENT** | | | |
| All changes to the certificate profile | X | N/A | N/A |
| **CERTIFICATE STATUS PROVIDERMANAGEMENT** | | | |
| All changes to the CSP profile (e.g. OCSP profile) | N/A | X | N/A |
| **REVOCATION PROFILE MANAGEMENT** | | | |
| All changes to the revocation profile | X | N/A | N/A |
| **CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT** | | | |
| All changes to the certificate revocation list profile | X | N/A | N/A |
| **MISCELLANEOUS** | | | |
| Appointment of an individual to a Trusted Role | X | X | X |
| Designation of personnel for multiparty control | X | - | N/A |
| Installation of the Operating System | X | X | X |
| Installation of the PKI Application | X | X | X |
| Installation of hardware cryptographic modules | X | X | X |
| Removal of hardware cryptographic modules | X | X | X |
| Destruction of cryptographic modules | X | X | X |
| System Startup | X | X | X |
| Logon attempts to PKI Application | X | X | X |
| Receipt of hardware / software | X | X | X |
| Attempts to set passwords | X | X | X |
| Attempts to modify passwords | X | X | X |
| Back up of the internal CA database | X | - | - |

| Auditable Event | CA | CSP | RA |
|---|---|---|---|
| Restoration from back up of the internal CA database | X | - | - |
| File manipulation (e.g., creation, renaming, moving) | X | - | - |
| Posting of any material to a PKI Repository | X | - | - |
| Access to the internal CA database | X | X | - |
| All certificate compromise notification requests | X | N/A | X |
| Loading tokens with certificates | X | N/A | X |
| Shipment of Tokens | X | N/A | X |
| Zeroizing Tokens | X | N/A | X |
| Re-key of the Component | X | X | X |
| **CONFIGURATION CHANGES** | | | |
| Hardware | X | X | - |
| Software | X | X | X |
| Operating System | X | X | X |
| Patches | X | X | - |
| Security Profiles | X | X | X |
| **PHYSICAL ACCESS / SITE SECURITY** | | | |
| Personnel Access to room housing Component | X | - | - |
| Access to the Component | X | X | - |
| Known or suspected violations of physical security | X | X | X |
| **ANOMALIES** | | | |
| Software error conditions | X | X | X |
| Software check integrity failures | X | X | X |
| Receipt of improper messages | X | X | X |
| Misrouted messages | X | X | X |
| Network attacks (suspected or confirmed) | X | X | X |
| Equipment failure | X | - | - |
| Electrical power outages | X | - | - |
| Uninterruptible Power Supply (UPS) failure | X | - | - |
| Obvious and significant network service or access failures | X | - | - |
| Violations of Certificate Policy | X | X | X |
| Violations of Certification Practice Statement | X | X | X |
| Resetting Operating System clock | X | X | X |

### 5.4.2 Frequency of Processing Audit Logs

Audit logs shall be reviewed at least once every 30 days. Statistically significant sample of security audit data generated by the CA, CSP, or RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. The Audit Administrator shall explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

### 5.4.3 Retention Period for Audit Logs

See Section 5.5.1.

### 5.4.4 Protection of Audit Logs

System configuration and procedures shall be 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.

It is acceptable for the system to over-write audit logs after they have been backed up and archived.

### 5.4.5 Audit Log Backup Procedures

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

### 5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the CA, CSP, or RA. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the CA shall determine whether to suspend CA operation until the problem is remedied.

### 5.4.7 Notification to Event-Causing Subject

This CP 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

No stipulation beyond Section 5.4.2.

## 5.5 Records Archival

### 5.5.1 Types of Records Archived

CA, CSP, and RA archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any certificate (including those revoked or expired) issued by the CA.

| Data To Be Archived | CA | CSP | RA |
|---|---|---|---|
| Certification Practice Statement | X | X | X |
| Contractual obligations | X | X | X |
| System and equipment configuration | X | X | - |
| Modifications and updates to system or configuration | X | X | - |
| Certificate requests | X | - | - |
| Revocation requests | X | - | - |
| Subscriber identity authentication data as per Section 3.2.3 | X | N/A | X |
| Documentation of receipt and acceptance of certificates | X | N/A | X |
| Documentation of receipt of Tokens | X | N/A | X |
| All certificates issued or published | X | N/A | N/A |
| Record of Component CA Re-key | X | X | X |
| All CRLs and CRLs issued and/or published | X | N/A | N/A |
| All Audit Logs | X | X | X |
| All Audit Log Summaries | X | X | X |
| Other data or applications to verify archive contents | X | X | X |
| Compliance audit reports | X | X | X |

### 5.5.2 Retention Period for Archive

The minimum retention periods for archive data are listed below for the various assurance levels.

| Assurance Level | Archive Retention Period |
|---|---|
| Class 1 | 7 Years |
| Class 2 | 7 Years |
| Class 3 | 7 Years |

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive

site. Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

### 5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA and CSP, the authorized individuals are Audit Administrators. For the RA, authorized individuals are someone other than the RA (e.g., Information Assurance Officer or IAO). The contents of the archive shall not be released except as determined by the CCA, the Licensed CA, or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CSP, or RA) with physical and procedural security controls equivalent or better than those for component.

### 5.5.4 Archive Backup Procedures

No Stipulation.

### 5.5.5 Requirements for Time-Stamping of Records

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

### 5.5.6 Archive Collection System (internal or external)

No stipulation.

### 5.5.7 Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, and transmit archive information shall be published in the applicable CPS.

## 5.6 Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs, then the old key shall be retained and protected.

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

| Key | 2048 Bit Keys | |
|---|---|---|
| | Private Key | Certificate |
| RCAI | 10 years | 10 years |
| Intermediate CA | 10 years | 10 years |
| Sub-CA | 10 years | 10 years |
| Time Stamp Authority | 3 years | 3 years |
| Code Signer | 3 years | 3 years |
| OCSP Responder | 3 years | 3 years |
| Human Subscriber Signature | 3 years | 3 years |
| Human Subscriber Encryption | Always | 3 years |
| SSL | 3 years | 3 years |
| Device | 3 years | 3 years |

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

If a CA or CSP detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA or CSP 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 CA or CSP needs to be rebuilt, only some certificates need to be revoked, and/or the CA or CSP key needs to be declared compromised.

The CCA shall be notified if any of the following cases occur:

1. Suspected or detected compromise of a licensed CA system;
2. Physical or electronic attempts to penetrate a licensed CA system;
3. Denial of service attacks on a licensed CA system; or
4. Any incident preventing the licensed CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL. A CA shall reestablish capability to issue CRL as quickly as possible.

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

If a CA or CSP equipment is damaged or rendered inoperative, but the signature keys are not destroyed, the operation shall be reestablished as quickly as possible, giving priority to the ability to generate CRL.

If a CA cannot establish revocation capability in a reasonable time-frame, the CA shall determine whether to request revocation of its certificate(s). If the CA is RCAI, the CA shall determine whether to notify all subscribers to delete the RCAI trust anchor.

### 5.7.3 Private Key Compromise Procedures

If a CA signature keys are compromised, lost, or suspected to be compromised:

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

1. A CA key pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
2. New CA certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
3. If the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e., not expired or revoked), the CA may re-issue (i.e., renew) those certificates with the not After date in the certificate as in original certificates; and
4. If the CA is the RCAI, it shall provide the Subscribers the new trust anchor using secure means.

The CA shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

If a CSP key is compromised, all certificates issued to the CSP shall be revoked, if applicable. The CSP will generate a new key pair and request new certificate(s), if applicable.

### 5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its certificates be revoked. The CA shall follow steps 1 through 5 in Section 5.7.3 above.

## 5.8 CA, CSP, and RA Termination

In the event of termination of a CA, CSP or RA, the entity shall request all certificates issued to it be revoked.

A CA, CSP, shall archive all audit logs and other records prior to termination.

A CA, CSP, shall destroy all its private keys upon termination.

CA, CSP, archive records shall be transferred an appropriate authority.

# 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 |
| Intermediate CA | 3 | Hardware | Yes |
| Sub-CA | 3 | Hardware | Yes |
| Time Stamp Authority | 3 | Hardware | Yes |
| Code Signing | 2 | Hardware | Yes |
| OCSP Responder | 3 | Hardware | Yes |
| RA | 2 | Hardware | Yes |
| Human Subscriber Signature | 1 for Class 1<br>2 for Class 2 & 3 | Software for Class 1<br>Hardware for Class 2 & 3 | Yes |
| Human Subscriber Encryption | 1 for Class 1<br>2 for Class 2 & 3 | Software for Class 1<br>Hardware for Class 2 & 3 | No Requirement |
| SSL | 2 for Class 3 | Software for Class 2<br>Hardware for Class 3 | Yes |
| Device/System | 2 for Class 3 | Software for Class 2<br>Hardware for Class 3 | Yes |
| Document Signer | 2 for Class 3 | Software for Class 2<br>Hardware for Class 3 | Yes |

Multiparty control shall be used CA key pair generation, as specified in Section 5.2.2.

For CAs that issue Class1, Class 2 or Class 3 certificates, CA key pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. The process shall be validated by an Auditor.

### 6.1.2 Private Key Delivery to Subscriber

The CA shall generate their own key pair and therefore do not need private key delivery. A subscriber shall generate the key pairs and there is no need to deliver private keys.

### 6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber, the public key and the Subscriber's identity shall be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it shall be at least as strong as the CA keys used to sign the certificate.

### 6.1.4 CA Public Key Delivery to Relying Parties

The public key of a trust anchor shall be provided to the subscribers acting as relying parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of trust anchor include but are not limited to:

1. The CA loading a trust anchor onto tokens delivered to subscribers via secure mechanisms;

2. Secure distribution of a trust anchor through secure out-of-band mechanisms;

3. Comparison of certificate hash (fingerprint) against trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); or

4. Loading trust anchor from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded and the trust anchor is not in the certification chain for the Web site certificate.

### 6.1.5 Key Sizes

If the CCA determines that the security of a particular algorithm may be compromised, it may require the CAs to revoke the affected certificates.

All CAs, Time Stamp Authority, OCSP Responder, RA, and Code Signing certificates shall be 2048 bit RSA.

All subscriber (human, SSL, and device) certificates and Transport Layer Security (TLS) protocols shall use the following algorithm suites.

| ***Cryptographic Function*** | ***Cryptographic Algorithm*** |
|---|---|
| Signature | From January 1, 2011, CAs must issue 2048-bit RSA SubCA and end-entity certificates. |
| Hashing | SHA-1 for certificates issued before 1/1/2012<br>SHA-256 for certificates issued on or after 1/1/2012 |

### 6.1.6 Public Key Parameters Generation and Quality Checking

RSA keys shall be 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-PROF].

## 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, Security Requirements for Cryptographic Modules. The CCA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the CCA. Cryptographic modules shall be validated to the FIPS 140-2 level identified in this section, or validated, certified, or verified to requirements published by the CCA. Additionally, the CCA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

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 CA private signing key shall require action by at least two persons.

### 6.2.3 Private Key Escrow

Under no circumstances shall the signature keys be escrowed by a third party.

The end entity private keys used solely for decryption shall be escrowed prior to the generation of the corresponding certificates. NICs CPS have a statement to this effect.

### 6.2.4 Private Key Backup

#### 6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as the original signature key. Number of backup copies shall be limited, shall be continuously accounted for, and shall be securely stored under the same multi-person control as the operational key.

#### 6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys in software may be backed up or copied, but must be held in the Subscriber's control.
Subscriber private signature keys in hardware may not be backed up or copied.

#### 6.2.4.3 CSP Private Key Backup

If backed up, the CSP private signature keys shall be backed up under the same single or multi-person control as the signature key is invoked. Number of backup

copies shall be limited, shall be continuously accounted for, and shall be securely stored under the same controls as the operational key.

### 6.2.5 Private Key Archival

Subscriber private signature keys shall not be archived by the CA.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

CA and CSP private keys shall be generated by and remain in a cryptographic module. The CA and CSP private keys may be backed up in secure manner

### 6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 rating of the cryptographic module.

### 6.2.8 Method of Activating Private Key

The user 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) or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

### 6.2.9 Methods of Deactivating Private Key

The cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS.

### 6.2.10 Method of Destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware is required in the case of Root CA

### 6.2.11 Cryptographic Module Rating

See Section 6.2.1.

## 6.3 Other Aspects Of Key Management

### 6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

### 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, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys. Activation data may be user selected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

### 6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure.

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

### 6.4.3 Other Aspects of Activation Data

CAs, CSPs, shall change the activation data whenever the token is re-keyed or returned from maintenance.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, CSP and shall include the following functionality:

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

The computer system shall be configured with minimum of the required accounts and network services.

For CAs a combination of physical and logical security controls shall ensure that the CA administration is carried out under 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 CA and CSP are as follows:

1. Hardware and software procured shall be purchased in a fashion 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 shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.

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

5. CA, CSP, hardware and software shall be scanned for malicious code on first use and periodically thereafter.

### 6.6.2 Security Management Controls

The configuration of the CA and CSP system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA and CSP software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA system. The CA and CSP software, when first loaded, shall be 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

No stipulation.

## 6.7 Network Security Controls

CAs, CSPs, shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. Unused network ports and services shall be turned off. For CAs, protocols that

provide network security attack vector(s) shall not be permitted through the boundary control devices.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

## 6.8 Time Stamping

All CA and CSP components shall regularly synchronize with a time service such as Indian Standard Time Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates
- OCSP or other CSP responses

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.1.

# 7 Certificate, CRL and OCSP Profiles

## 7.1 Certificate Profile

Certificate profiles are detailed in the CCA's Digital Signature Interoperability Guidelines document.

## 7.2 CRL Profile

The CRL profiles are listed below.

### 7.2.1 Full and Complete CRL

A CA shall make a full and complete CRL available to the OCSP Responders as specified below. This CRL may also be provided to the relying parties.

| Field | Value |
|---|---|
| Version | V2 (1) |
| Issuer Signature Algorithm | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption {1 2 840 113549 1 1 11} |
| Issuer Distinguished Name | Per the requirements in [CCA-PROF] |
| 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 | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or 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

A CA may make distribution based partitioned CRL available to the relying parties in lieu of or in addition to the full and complete CRL. The distribution point based partition CRL shall adhere to the following profile. Note that the CRL may not be an indirect CRL, may not partitioned based on reason codes, and may not assert a distribution point that is a name Relative to CRL Issuer.

| Field | Value |
|---|---|
| Version | V2 (1) |
| Issuer Signature Algorithm | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} |
| Issuer Distinguished Name | Per the requirements in [CCA-PROF] |
| 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 | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or 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) |
| Issuing Distribution Point | c=yes; distribution point field must contain a full name (i.e., distribution point field may not contain nameRelativetoCRLIssuer; the following fields must all be absent: onlySomeReasons, indirectCRL, and onlyContainsAttributeCerts |
| **CRL Entry Extension** | **Value** |
| Reason Code | c=no |

## 7.3 OCSP Profile

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

### 7.3.1 OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC2560 for detailed syntax. 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 | sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or 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

All CAs, RAs(on a sample basis) and CSPs shall be subject to a periodic compliance audit at least once per year.

## 8.2 Identity and Qualifications of Assessor

The auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with requirements of the applicable CP. The compliance auditor must perform such compliance audits as a primary responsibility. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

## 8.3 Assessor's Relationship to Assessed Entity

The auditor shall be a firm, which is independent from the entity being audited. The office of CCA shall determine whether an auditor meets this requirement.

## 8.4 Topics Covered by Assessment

CAs shall have a compliance audit mechanism in place to ensure that the requirements of this CP and applicable CPS are being implemented and enforced.

## 8.5 Actions Taken as a Result of Deficiency

The Office of CCA may determine that a CA is not complying with its obligations set forth in this CP or the applicable CPS. When such a determination is made, the office of CCA may suspend operation of a noncompliant CA, or may revoke the CA certificate, or may direct that other corrective actions be taken which allow interoperation to continue.

When the auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, or the applicable CPS, the auditor shall take the following actions:

1. The auditor shall note the discrepancy;
2. The auditor shall notify the audited CA; and
3. The auditor shall notify the office of CCA.

## 8.6 Communication of Results

An Audit Report, including identification of corrective measures taken or being taken by the CA, shall be provided to the office of CCA (in case of grant of licence and its renewal) and the audited CA (in case of annual audit). The report shall identify the versions of the CP and CPS used in the assessment.

# 9 Other Business and Legal Matters

## 9.1 Fees

### 9.1.1 Certificate Issuance and Renewal Fees

Licensed CAs may set any reasonable certificate issuance and renewal fees.

### 9.1.2 Certificate Access Fees

Licensed CAs may not charge for access to any certificates.

### 9.1.3 Revocation Status Information Access Fees

Licensed CAs may not charge for access to any revocation status information.

### 9.1.4 Fees for Other Services

Licensed CAs may set any reasonable fees for any other services such as access to archive records or key recovery.

### 9.1.5 Refund Policy

Licensed CAs may, but are not required to, have a documented refund process.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

Licensed CAs shall also maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to PKI Participants described in Section 1.3 of this CP

### 9.2.2 Other Assets

Licensed CAs shall also maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to PKI Participants described in Section 1.3 of this CP.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

Licensed CAs may, but are not required, to offer protection to end entities that extends beyond the protections provided in this CP. Any such protection shall be offered at commercially reasonable rates.

## 9.3 Confidentiality of Business Information

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

## 9.4 Privacy of Personal Information

Licensed CAs may store, process, and disclose personally identifiable information in accordance with the privacy policy of that licensed CA.

## 9.5 Intellectual Property Rights

Licensed CAs shall not knowingly violate any intellectual property rights held by others.

### 9.5.1 Property Rights in Certificates and Revocation Information

Licensed CAs may claim all Intellectual Property Rights in and to the Certificates and revocation information that they issue. However, they must grant permission to reproduce and distribute Certificates and revocation information on a nonexclusive royalty-free basis, provided that the recipient agrees to distributed them at no cost.

### 9.5.2 Property Rights in the CPS

All Intellectual Property Rights in this CP are owned by the Office of CCA. All Intellectual Property Rights in any CPS of a licensed CA may be claimed by that CA.

### 9.5.3 Property Rights in Names

The Certificate Applicant may claim all rights, if any, in any trademark, service mark, or trade name of the Certificate Applicant contained in any Application.

### 9.5.4 Property Rights in Keys

Licensed CAs may claim property rights to the keys they use (e.g., CA key pair, OCSP Responder key pair, time stamp authority key pair, etc.)

Subject to any agreements between a licensed CA and its customers, ownership of and property rights in key pairs corresponding to Certificates of Subscribers shall be specified in the applicable CPS.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

9.6.1.1 Licensed CA

Licensed CAs represent and warrant that:

1. Their CA signing private key is protected and that no unauthorized person has ever had access to that private key;

2. All representations made by the licensed CA in any applicable agreements are true and accurate, to the best knowledge of the applicable CA; and

3. 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.

4. Only verified information appears in the certificate

### 9.6.2 Subscriber

A Subscriber shall be required to sign a document (e.g., a subscriber agreement) containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

In signing the document described above, each Subscriber shall agree to the following:

1. Subscriber shall accurately represent itself in all communications with the PKI authorities.
2. The data contained in any certificates issued to Subscriber is accurate.
3. The Subscriber shall protect its private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures
4. The Subscriber lawfully holds the private key corresponding to public key identified in the Subscriber's certificate.
5. The Subscriber will abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.
6. Subscriber shall promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.

### 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;
3. Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with

application upgrades will often invalidate digital signatures and shall be avoided.

### 9.6.4 Representations and Warranties of Other Participants

No stipulation.

## 9.7 Disclaimers of Warranties

To the extent permitted by applicable law and any other related agreements, licensed CAs may disclaim all warranties (other than any express warranties contained in such agreements or set forth in the licensed CA's CPS).

## 9.8 Limitations of Liabilities

Licensed CAs may limit liabilities as long as they meet the liability requirements stated in [ITACT 2000].

## 9.9 Indemnities

Licensed CAs includes indemnification clauses as long as the clauses are consistent with [ITACT 2000].

## 9.10 Term and Termination

### 9.10.1 Term

The CP becomes effective upon ratification by the Office of CCA. Amendments to this CP become effective upon ratification by the Office of CCA and publication at

http://www.cca.gov.in/resource/CP.pdf

There is no specified term for this CP.

### 9.10.2 Termination

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

### 9.10.3 Effect of Termination and Survival

Upon termination of this CP, licensed CAs are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. The following sections of this CP shall survive the termination or expiration of this CP: 5.5 and 9.0.

## 9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, licensed CAs shall use 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

The Office of CCA shall review this at least once every year. Additional reviews may be enacted at any time at the discretion of the Office of CCA.

If the Office of CCA wishes to recommend amendments or corrections to this CP, such modifications shall be circulated to the licensed CAs. Comments from the licensed CAs shall be collected and adjudicated by the Office of CCA.

Office of CCA shall use commercially reasonable efforts to immediately notify licensed CAs of changes.

### 9.12.2 Notification Mechanism and Period

Errors, and anticipated changes to this CP resulting from reviews are published online at http://www.cca.gov.in/resource/CP_Updates.pdf. The most up to date copy of the CP can be found at http://www.cca.gov.in/resource/CP.pdf.

This CP and any subsequent changes shall be made publicly available within seven days of approval.

### 9.12.3 Circumstances under Which OID Must be Changed

Certificate Policy OIDs shall be changed if the Office of CCA determines that a change in the CP reduces the level of assurance provided.

## 9.13 Dispute Resolution Provisions

### 9.13.1 Disputes among Licensed CAs and Customers

Provisions for resolving disputes between a licensed CA and its Customers shall be set forth in the applicable agreements between the parties.

Dispute resolution procedures shall be consistent with [ITACT 2000].

### 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 Information Technology shall govern the construction, validity, enforceability and performance of actions per this CP.

## 9.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local and foreign laws, 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 CP or any of its rights or duties under this CP, without the prior written consent of the other party (such consent not to be unreasonably withheld), except that Office of CCA may assign and delegate this CP to any party of its choosing.

### 9.16.3 Severability

If any provision of this CP 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 shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

### 9.16.5 Force Majeure

Licensed CAs shall not be liable for any failure or delay in its performance under this CP 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 Differences among Various Assurance Levels

The following table summarizes differences among the various assurance levels described in this CP.

| Section | Area | Class 1 | Class 2 | Class 3 |
|---|---|---|---|---|
| 1.2 | Policy OID | Class Specific OID | Class Specific OID | Class Specific OID |
| 3.2.3 | Identity Proofing | One photo ID, address proof and no in person presence | One photo ID, address proof and no in person presence | One photo ID, address proof and in person presence |
| 3.3.1 | Identity Re Proofing | Every 3 Years | Every 3 Years | Every 3 Years |
| 5.1.2.1 | Two Person Physical Control on CA | Required | Required | Required |
| 5.2.2 | Two Person Control on CA Private Key | Required | Required | Required |
| 5.2.4 | Role Separation | Required | Required | Required |
| 5.5.1 | Archive Retention Period | 7 Years | 7 Years | 7 Years |
| 6.1.1 | CA Cryptographic Module FIPS 140-2 Level | 3 | 3 | 3 |
| 6.1.1 | End Entity Cryptographic Module FIPS 140-2 Level | 1 | 2 | 2 |
| 6.1.1 | Key Generation Ceremony | Required | Required | Required |
| 6.5.1 | Two Person Logical Control on CA | Required | Required | Required |

# 11 Bibliography

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


| | |
|---|---|
| CCA-PROF | Digital Signature Interoperability Guidelines, Controller of Certifying Authorities, India, Version: Release 1.1, August 14, 2009. |
| 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. |

# 12 Acronyms and Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CA | Certification 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 |
| KRP | Key Recovery Policy |
| KRPS | Key Recovery Practices Statement |
| 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) |
| SCVP | Simple Certificate Validation Protocol |
| SHA-1 | Secure Hash Algorithm, Version 1 |
| SSL | Secure Sockets Layer |
| TDES | Triple Data Encryption Standard |
| TLS | Transport Layer Security |
| UPS | Uninterrupted Power Supply |

Controller of Certifying Authorities

Department of Information Technology

Ministry of Communications and Information Technology

# X.509 Certificate Policy for India PKI - Change History

## 1. Authentication of Individual Identity

| | |
|---|---|
| Date | 14-03-2011 |
| Contents | 3.2 Initial Identity Validation |
| section | 3.2.3 Authentication of Individual Identity |
| Page no | 08 |

| Version 1.0 | Version 1.1 |
|---|---|
| 3. The applicant shall present one State or National Government-issued photo ID. For Class 2 or Class 3 certificates, the applicant shall present an additional photo or non-photo ID or form (e.g., credit card, income tax return, electricity bill, etc.) as the evidence of identity. | 3. The applicant shall present one photo ID. The applicant shall also present a document as a proof of residential address. |
| 4. Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant; | 4. Removed since no such procedure has been specified. |
| 6. A declaration of identity signed by the applicant using a handwritten signature or equivalent per Indian Laws and performed in the presence of the person performing the identity authentication. | 6. A declaration of identity signed by the applicant using a handwritten signature or equivalent per Indian Laws |

## 2. Certificate Issuance

| | |
|---|---|
| Date | 14-03-2011 |
| Contents | 4.3 Certificate Issuance |
| Page no | 12 |

| Version 1.0 | Version 1.1 |
|---|---|
| Upon receiving a request for a certificate, the CA shall respond in accordance with the requirements set forth in applicable CPS.<br><br>If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought. Specifically, the databases shall be protected using physical security controls, personnel security controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP. | Upon receiving a request for a certificate, the CA shall respond in accordance with the requirements set forth in applicable CPS.<br><br>If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought. |

## 3. Maximum Latency for CRLs

| | |
|---|---|
| Date | 14-03-2011 |
| Contents | 4.9 Certificate Revocation and Suspension |
| section | 4.9.8 Maximum Latency for CRLs |
| Page no | 15 |

| Version 1.0 | Version 1.1 |
|---|---|

| | |
|---|---|
| this update + 4 hours ≤ next Update ≤ this update + 72 hours | CRLs shall be published immediately after generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL. CAs must issue CRLs at least once every 24 hours, and the nextUpdate time in the CRL may be no later than 7 days after issuance time (i.e., the thisUpdate time). |

## 4. Registration Authority

| | |
|---|---|
| Date | 14-03-2011 |
| Contents | 5.2 Procedural Controls |
| section | 5.2.1.5 Registration Authority |
| Page no | 22 |

| Version 1.0 | Version 1.1 |
|---|---|
| An RA's responsibilities are:<br>1. Verifying identity, pursuant to section 3.2;<br>2. Entering Subscriber information, and verifying correctness;<br>3. Securely communicating requests to and responses from the CA;<br>4. Receiving and distributing Subscriber certificates. | An RA's responsibilities are:<br>1. Verifying identity, pursuant to section 3.2;<br>2. Entering Subscriber information, and verifying correctness;<br>3. Securely communicating requests to and responses from the CA; |

## 5. Class 1- Assurance Level , Applicability and Related Modification

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Applicability |
| Section | 1.3.5 Applicability |
| Version | 1.2 |
| Page no | 4 |

**Version 1.1**

| Assurance Level | Applicability |
|---|---|
| Class 1 | This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious. |
| Class 2 | This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. |
| Class 3 | This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. |

**Version 1.2**

| Assurance Level | Assurance | Applicability |
|---|---|---|
| Class 0 | This certificate shall be issued only for demonstration / test purposes. | This is to be used only for demonstration / test purposes. |
| Class 1 | Class 1 certificates shall be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases. | This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. |
| Class 2 | These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases. | This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial |

| | | |
|---|---|---|
| Class 3 | This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities. | This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. |

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Physical Access |
| Section | 5.1.2 Physical Access |
| Version | 2.5 |
| Page no | 19 |

| Version 1.1 | Version 1.2 |
|---|---|
| 6. Require two person physical access control to both the cryptographic module and computer system for CAs issuing Class 2 and Class 3 certificates | 6. Require two person physical access control to both the cryptographic module and computer system for CAs issuing Class1, Class 2 and Class 3 certificates. |

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Number of Persons Required per Task |
| Section | 5.2.2 Number of Persons Required per Task |
| Version | 1.2 |
| Page no | 22 |

| Version 1.1 | Version 1.2 |
|---|---|
| Two or more persons shall be required to perform the following tasks for CAs that issue Class 2 or Class 3 certificates: | Two or more persons shall be required to perform the following tasks for CAs that issue Class1 or Class 2 or Class 3 certificates |

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Roles Requiring Separation of Duties |
| Section | 5.2.4 Roles Requiring Separation of Duties |
| Version | 1.2 |
| Page no | 23 |

| Version 1.1 | Version 1.2 |
|---|---|
| 5.2.4.1 Class1 There is no role separation requirement | Removed |
| 5.2.4.2 Class 2 and Class 3 | 5.2.4.1 Class1, Class 2 and Class 3 |

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Key Pair Generation |
| Section | 6.1.1 Key Pair Generation |
| Version | 1.2 |
| Page no | 34 |

| Version 1.1 | Version 1.2 |
|---|---|
| For CAs that issue Class 2 or Class 3 | For CAs that issue Class 1 or Class 2 or |

| | |
|---|---|
| certificates, CA key pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. | Class 3 certificates, CA key pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. |

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Differences among Various Assurance Levels |
| Section | 10.Differences among Various Assurance Levels |
| Version | 1.2 |
| Page no | 51 |

Version 1.1

| Section | Area | Class 1 | Class 2 | Class 3 |
|---|---|---|---|---|
| 3.2.3 | Identity Proofing | One valid email ID and no in person presence | One photo ID, address proof and no in person presence | One photo ID, address proof and in person presence |

Version 1.2

| Section | Area | Class 1 | Class 2 | Class 3 |
|---|---|---|---|---|
| 3.2.3 | Identity Proofing | One photo ID, address proof and no in person presence | One photo ID, address proof and no in person presence | One photo ID, address proof and in person presence |

## 6. Validity of Certificates and related Modification

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Identification and Authentication for Routine Re-key |
| Section | 3.3.1 Identification and Authentication for Routine Re-key |
| Version | 1.2 |
| Page no | 9 |

Version 1.1

| Assurance Level | Initial Identity Proofing |
|---|---|
| Class 1 | Every 2 Years |
| Class 2 | Every 2 Years |
| Class 3 | Every 2 Years |

Version 1.2

| Assurance Level | Initial Identity Proofing |
|---|---|
| Class 1 | Every 3 Years |
| Class 2 | Every 3 Years |
| Class 3 | Every 3 Years |

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Key Changeover |
| Section | 5.6 Key Changeover |
| Version | 1.2 |
| Page no | 32 |

Version 1.1

| Key | 2048 Bit Keys | |
|---|---|---|
| | Private Key | Certificate |
| RCAI | 5 years | 5 Years |
| Intermediate CA | 5 Years | 5 Years |
| Sub-CA | 5 Years | 5 Years |
| Time Stamp Authority | 2 Years | 2 Years |
| Code Signer | 2 years | 2 years |
| OCSP Responder | 2 Years | 2 Years |
| Human Subscriber Signature | 2 Years | 2 Years |
| Human Subscriber Encryption | Always | 2 Years |
| SSL | 2 Years | 2 Years |
| Device | 2 Years | 2 Years |

Version 1.2

| Key | 2048 Bit Keys | |
|---|---|---|
| | Private Key | Certificate |
| RCAI | 10 years | 10 years |
| Intermediate CA | 10 years | 10 years |
| Sub-CA | 10 years | 10 years |
| Time Stamp Authority | 3 years | 3 years |
| Code Signer | 3 years | 3 years |
| OCSP Responder | 3 years | 3 years |
| Human Subscriber Signature | 3 years | 3 years |
| Human Subscriber Encryption | Always | 3 years |
| SSL | 3 years | 3 years |
| Device | 3 years | 3 years |

| | |
|---|---|
| Date | 17-02-2014 |
| Contents | Differences among Various Assurance |

| | |
|---|---|
| | Levels |
| Section | 10.Differences among Various Assurance Levels |
| Version | 1.2 |
| Page no | 51 |

Version 1.1

| Section | Area | Class 1 | Class 2 | Class 3 |
|---|---|---|---|---|
| 3.3.1 | Identity Re Proofing | Every 2 Years | Every 2 Years | Every 2 Years |

Version 1.1

| **Section** | **Area** | **Class 1** | **Class 2** | **Class 3** |
|---|---|---|---|---|
| 3.3.1 | Identity Re Proofing | Every 3 Years | Every 3 Years | Every 3 Years |

## 7. OID for Class 0 Certificates.

| | |
|---|---|
| Date | 06-05-2014 |
| Contents | OID for Class 0 certificates issued for demonstration / test purposes. |
| Section | 1.2 Document Identification |
| Version | 1.2 |
| Page no | 11 |

Version 1.2

| | |
|---|---|
| id-India PKI | ::= {2.16.356.100} |
| id-cp | ::= (id-India PKI  2} |
| id-class1 | ::= {id-cp 1} |
| id-class2 | ::= {id-cp 2} |
| id-class3 | ::= {id-cp 3} |

Version 1.3

| | |
|---|---|
| id-India PKI | ::= {2.16.356.100} |
| id-cp | ::= (id-India PKI  2} |
| id-class0 | ::= {id-cp 0} |
| id-class1 | ::= {id-cp 1} |
| id-class2 | ::= {id-cp 2} |
| id-class3 | ::= {id-cp 3} |

## 8. OID for Document Signer Certificates

| | |
|---|---|
| Date | 08-09-2014 |
| Contents | OID for Document Signer Certificates |
| Section | 1.2 Document Identification |
| Version | 1.2 |
| Page no | 11 |

Version 1.3

| | |
|---|---|
| id-India PKI | ::= {2.16.356.100} |
| id-cu (Certificate Usage) | ::= {id- India PKI 10} |
| id-document signer | ::= {id-cu 1} |

| 9. Key Pair Generation medium for Document Signer Certificates | |
|---|---|
| Date | 08-09-2014 |
| Contents | 6.1 Key Pair Generation and Installation |
| Section | 6.1.1 Key Pair Generation |
| Version | 1.2 |
| Page no | 43 |

### Version 1.3

| Entity | FIPS 140-1/2 Level | Hardware or Software | Generated in Entity Module |
|---|---|---|---|
| RCAI | 3 | Hardware | Yes |
| Intermediate CA | 3 | Hardware | Yes |
| Sub-CA | 3 | Hardware | Yes |
| Time Stamp Authority | 3 | Hardware | Yes |
| Code Signing | 2 | Hardware | Yes |
| OCSP Responder | 3 | Hardware | Yes |
| RA | 2 | Hardware | Yes |
| Code Signing | 2 | Hardware | Yes |
| Human Subscriber Signature | 1 for Class 1<br>2 for Class 2 & 3 | Software for Class 1<br>Hardware for Class 2 & 3 | Yes |
| Human Subscriber Encryption | 1 for Class 1<br>2 for Class 2 & 3 | Software for Class 1<br>Hardware for Class 2 & 3 | No Requirement |
| SSL | 2 for Class 3 | Software for Class 2<br>Hardware for Class 3 | Yes |
| Device/System | 2 for Class 3 | Software for Class 2<br>Hardware for Class 3 | Yes |
| Document Signer | 2 for Class 3 | Software for Class 2<br>Hardware for Class 3 | Yes |

| 10. Aadhaar-eKyc Class and OID | |
|---|---|
| Date | 17-04-2015 |
| Contents | Applicability |
| Section | 1.3.5 |
| Version | 1.4 |
| Page no | 5 |

### Version 1.4

| Assurance Level | Assurance | Applicability |
|---|---|---|
| Aadhaar-eKyc - | Aadhaar OTP class of certificates shall be issued for individuals use based on OTP authentication of subscriber through | This level is relevant to environments where OTP based Aadhaar-eKyc authentication is acceptable method for credential |

| | | |
|---|---|---|
| OTP | Aadhaar eKyc. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder | verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time usage at this assurance level. |
| Aadhaar-eKyc - biometric | Aadhaar biometric class of certificates shall be issued based on biometric authentication of subscriber through Aadhaar eKyc service. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder. | This level is relevant to environments where biometric based Aadhaar-eKyc authentication is acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time usage at this assurance level |

| | |
|---|---|
| Date | 17-04-2015 |
| Contents | Document Identification |
| Section | 1.2 |
| Version | 1.4 |
| Page no | 2 |

| | |
|---|---|
| Id-Aadhaar-eKyc | ::= {id-cp 4} |
| Id-OTP | ::= (Id-Aadhaar-eKyc 1} |
| Id-biometric | ::= (Id-Aadhaar-eKyc 2} |

Document Identification

| | |
|---|---|
| id-India PKI | ::= {2.16.356.100} |
| id-cu (certificate usage) | ::= {id- India PKI 10} |
| id-key generation witness | ::= {id-cu 2} |

| **11. Special Purpose trust Chain for SSL and Code Sigining** | |
|---|---|
| Date | 05-05-2015 |
| Contents | 1.3 PKI Participants |
| Section | 1.3.1.2, 1.3.1.3 |
| Version | 1.4 |
| Page no | 3 |

**Version 1.4**

| | |
|---|---|
| 1.3.1.2<br>Root Certifying Authority of India (RCAI) | SSL and code signing certificates shall be issued from the special purpose trust chain created specifically for that purpose. The special purpose trust chain shall be operated in offline mode at Root CA and CA level. |
| 1.3.1.3<br>Intermediate CA | A CA should have an offline certificate issuance system for issuance of SSL and Code signing certificates under special purpose trust chain |