IDRBT CA

CERTIFICATION PRACTICE STATEMENT

VERSION 4.2.4

DATE OF PUBLICATION: 04.07.2025

OID: 2.16.356.100.1.2.2

INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY

CERTIFYING AUTHORITY (IDRBT CA)

CASTLE HILLS, ROAD NO: 1,

MASAB TANK, HYDERABAD – 500 057

TELANGANA, INDIA

PHONE: +91 40 23294216/17/19/21/23

FAX: +91 40 23535157

EMAIL: cahelp@idrbt.ac.in

Deepak Kumar

Digitally signed by Deepak Kumar
Date: 2025.07.31 14:44:54 +05'30'

CERTIFICATION PRACTICE STATEMENT

Document Name	CPS of IDRBT CA
Release	Version 4.2.4
Status	Release
Issue Date	04.07.2025

Amendment Certificate RELEASE

Version No.	Description	Approved by	Approval date	CCA approved date
IDRBTCA/DOC/ CPS/4.0.0	New template of CPS	PAC	28.02.2019	11.04.2019
IDRBTCA/DOC/ CPS/4.0.1	1) Approval of Physical DSC Application 12 Annexure I 12.1 2) Application Verification and Communication 12 Annexure I 12.2 Class3 3) SSL Certificate 12 Annexure I 12.4	PAC	03.03.2020	17.07.2020
IDRBTCA/DOC/ CPS/4.0.2	1) Applicability to PKI Participants 1.3.6 Table modified 2) Identification and Authentication for Routine Re-key 3.3.1 Table modified 3) Authentication of Organization user identity 12.1 Added Physical Verification 4) Certificate Application Information verification and Communication 12.2 Table modified 5) Removed section for Class 2 and modified Class 3 Certificates 12.6 6) Application Form modified 13.1 7) Superior Authority Responsibilities modified 14.1	PAC	17.02.2021	31.03.2021
IDRBTCA/DOC/ CPS/4.0.3	1) Changes in ROOT Certificate 1.3.1.2 2) Certificate application information verification communication 12.2 3) Inclusion of Document Signer Certificate 12.5 4) Changes in application form 13.1	PAC	25.04.2022	
IDRBTCA/DOC/	1) Modification of CA 1.3.1.2	PAC		

CPS/4.1.3	2) Addition of Sub-CA 1.3.1.3 3) PKI Repositories 2.1 4) Key Change Over 5.6 5) Registration Authority (RA) 1.3.3			

ATTENTION

The use of IDRBT Certifying Authority's (IDRBT CA) Certification Services are subject to various Indian laws and jurisdiction of courts, tribunals, and authorities in India, which may include but are not limited to: The Information Technology Act, 2000 (IT Act) and Rules and Regulations framed there under, and the other Indian laws and any statutory modifications or re-enactment of the above.

Use of the Digital Certificates in an unauthorized manner or violation of the practices specified in IDRBT CA CPS shall be liable for punitive action and shall be proceeded against, both under the relevant civil and criminal laws, in addition to being subject to punishment under the Information Technology Act, 2000 and/or any other relevant law/s of the land. The duties of the subscribers to be followed are described in the Chapter VIII of the Information Technology Act, 2000.

IDRBT CA has the right to inquire about and assist in the trial of any individual who purportedly commits an offense affecting IDRBT CA's policies and practices. Such a person shall be liable to be punished under the rules and provisions of The Information Technology Act 2000.

IDRBT CA's Certification Services are not designed, purported, or certified for use or resale as control equipment in perilous circumstances or for uses requiring foolproof performance such as the operation of nuclear plants, weapons control systems, where breakdown may lead directly to death, personal injury or severe environmental damage.

DEFINITIONS

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

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

"Act" means Information Technology IT Act, 2000

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

"ASP" or "Application Service Provider" is an organization or an entity using Electronic Signature as part of their application to facilitate the user for requesting issuance and electronically signing the content through any empanelled ESP.

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

"CA" refers to IDRBT CA, a Certifying Authority, licensed by the Controller of Certifying Authorities (CCA), Govt. of India under provisions of ITAct, and includes CA Infrastructure issuing Digital Signature Certificates & also for providing Trust services such as TS, OCSP & CRL

"CA Infrastructure" The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of the CA. It includes a set of policies, processes, server platforms, software, and workstations, used to administer Digital Signature Certificates and keys.

"**CA Verification Officer**" means a trusted person involved in identity and address verification of DSC applicants and providing approval for issuance of DSC.

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

"Certificate"—A Digital Signature Certificate issued by CA.

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

“Certificate Policy”—The India PKI Certificate Policy laid down by CCA and followed by CA addresses all aspects associated with the CA’s generation, production, distribution, accounting, compromise recovery, and administration of Digital Signature Certificates.

Certificate Revocation List (CRL)—A periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital Signature Certificates that have been suspended or revoked before their expiration dates.

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

Crypto Token—A hardware cryptographic device used for generating and storing a user’s private key(s) and containing a public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

"Digital Signature" means authentication of any electronic record by a subscriber using an electronic method or procedure as per the provisions of section 3 of the IT Act;

“Digital Signature Certificate Applicant” or “DSC Applicant” —A person that requests the issuance of a Digital Signature Certificate by a Certifying Authority.

“Digital Signature Certificate Application” or “DSC Application” —A request from a Digital Signature Certificate applicant to a CA for the issuance of a Digital Signature Certificate

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

“ESP” or “eSign Service Provider” is a Trusted Third Party as per the definition in the Second Schedule of the Information Technology Act to provide eSign service. ESP is operated within CA Infrastructure & empanelled by CCA to provide Online Electronic Signature Service.

Organization—An entity with which a user is affiliated. An organization may also be a user.

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

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

“Registration Authority” or “RA” An entity associated with the Certifying Authority (CA) to support the subscriber on demand for the Digital Signature Certificate (DSC) enrollment process

“Relying Party” is a recipient who acts in reliance on a certificate and digital signature.

“Relying Party Agreement” Terms and conditions published by CA for the acceptance of the certificate issued or facilitated the digital signature creation.

"Subscriber Identity Verification method" means the method used for the verification of the information (submitted by the subscriber) that is required to be included in the Digital Signature Certificate issued to the subscriber following CPS. CA follows the Identity Verification Guidelines laid down by Controller.

Subscriber— A person in whose name the Digital Signature Certificate is issued by CA.

Time Stamping Service: A service provided by CA to its subscribers to indicate the correct date and time of an action, and the identity of the person or device that sent or received the time stamp.

Subscriber Agreement— the agreement executed between a subscriber and CA for the provision of designated public certification services following this Certification Practice Statement

Master Agreement— the agreement executed between RA and CA for the provision of designated public certification services following this Certification Practice Statement

Time Stamp—A notation that indicates (at least) the correct date and time of an action, and the identity of the person or device that sent or received the time stamp.

"Trusted Person" means any person who has: -

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

An Executive summary of CPS, the RIGHTS AND OBLIGATIONS

NOTE: This is only a summary of the IDRBT CA Certification Practice Statement (IDRBT CA CPS). It summarizes the most important rights, obligations, and liabilities.

1. IDRBT CA Certification services

IDRBT CA Certification Services are designed to support secure electronic transactions and other general security services for Digital Signatures and other Network Security Services. To accomplish this, IDRBT CA serves as a Trusted Third Party, licensed by the Controller of Certifying Authorities (CCA) for issuing, managing, renewing, and revoking Digital Certificates following published practice (IDRBT CA CPS).

At present IDRBT issues Digital Certificates mainly to Banks and Financial Institutions that are members of INdian Financial NETwork (INFINET) and other Institutions as per the policy in force. IDRBT CA is empanelled as eSign Service Provider (ESP) to enable paperless enrollment and also for public services managed by IDBRT

IDRBT CA currently offers 5 distinct classes of certificates. Each class of certificate provides specific functionality and security features. The Classes are:

- Class 1 Certificate
- Class 2 Certificate
- Class 3 Certificate
- eKYC – Single-Factor
- eKYC – Multi-Factor

2. Rights and Obligations

By applying for a certificate to be issued by IDRBT CA, the applicants accept and agree with IDRBT CA CPS and to all who reasonably rely on the information contained in the certificate that, at the time of acceptance and throughout the operational period of the certificates, until notified otherwise by the certificate owner, of the following points:

- All representations made by the certificate owner to IDRBT CA regarding the information contained in the certificate are true. All information contained in the certificate is true to the extent that the certificate owner had knowledge or notice of such information.

- Each digital certificate created corresponding to the public key listed in the certificate is the digital certificate of the certificate owner and the certificate has been accepted and is operational (not expired or revoked).
- No unauthorized person has ever had access to the certificate owner's private key.

By accepting a certificate, the certificate owner assumes a duty to retain control of the certificate owner's private key, to use a trustworthy system, and to take sound precautions to prevent its loss, disclosure, modification, or unauthorized use. The user must request to revoke his certificate when there has been a loss, theft, modification, unauthorized disclosure, or other compromises of the private key of the certificate with IDRBT CA.

This CPS assumes that the reader is familiar with basic PKI concepts, including:

- The use of digital signatures for authentication, integrity, and non-repudiation;
- The use of encryption for confidentiality;
- The principles of asymmetric encryptions, public key certificates and key pairs;
- The role of Certifying Authorities and Registration Authorities

3. Liability

Without limiting certificate owner’s obligations stated in the CPS, certificate owners are liable for any misrepresentation they make in certificates to third parties that, reasonably rely on the representations contained therein.

IDRBT CA does not warrant the accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of IDRBT CA.

For more information, visit IDRBT CA’s website at https://idrbtca.org.in/

Table of Contents

1 INTRODUCTION

Institute for Development and Research in Banking Technology - Certifying Authority (IDRBT-CA), represented by Institute for Development and Research in Banking Technology (IDRBT), is a Society registered (in 1996) under the Society Registration Act at the address - Castle hills, Road no. 1, Masab Tank, Hyderabad, Telangana-500057, India.

IDRBT CA Certification Services are designed to support secure electronic transactions and other general security services for Digital Signatures and other Network Security Services. To accomplish this, IDRBT CA serves as a Trusted Third Party, licensed by the Controller of Certifying Authorities (CCA) for issuing, managing, renewing, and revoking Digital Certificates as per CPS.

IDRBT issues Digital Certificates and provides e-Sign services to Banks, Financial Institutions, non-banking entities, their employees and customers.

The term "Certifying Authority" or CA as used in this CPS, refers to IDRBT CA as the entity that holds the CA license from the Controller of Certifying Authorities (CCA), Govt. of India.

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

1.1 Overview of CPS

India PKI 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). Certificates issued by CAs contain one or more registered Certificate Policy OID, which may be used by a Relying Party to decide whether a certificate can be trusted for a particular purpose.

The Certification Practice Statement (CPS) of IDRBT CA details the practices and operational procedures implemented to meet the assurance requirements. This CPS 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. Controller of Certifying Authority issues licenses to operate as Certifying Authority subject to a successful compliance audit of the CA as per the CPS. The CPS is also

(i) intended to apply to and is a legally binding document between the CA, the Subscribers, the applicants, the Relying Parties, employees, and contractors; and

(ii) intended to serve as notice to all parties within the context of the CA CPS

CPS refers to the various requirements specified under the following guidelines issued by CCA

(i) The identity Verification Guidelines [CCA-IVG]: For the identity verification for different types of certificates like the personal, organizational person, SSL, encryption, code signing, system certificate, etc.

(ii) Interoperability Guidelines for DSC[CCA-IOG]: For the certificate profile including content and format of the certificates, key usage, extended key usage, etc.

(iii) X.509 Certificate Policy for India PKI[CCA-CP]: Assurance Class, Certificate policy id, the validity of certificates, key size, algorithm, storage requirements, audit parameters, etc.

(iv) Guidelines for Issuance of SSL Certificates[CCA-SSL]: Additional requirements for the issuance of SSL certificates

(v) Security Requirements for Crypto Devices [CCA-CRYPTO]: The crypto device management & security requirements for holding subscribers' private key

(vi) CA Site Specification [CCA-CASITESP]: Requirements for the construction of the cryptographic site and security requirements

1.2 Identification

The contact details are mentioned in section 1.5.2 of this CPS.

The following are the levels of assurance defined in the Certificate Policy. Each level of assurance has an OID that can be asserted in certificates issued by CA if the certificate issuance meets the requirements for that assurance level. The OIDs registered under the CCA are as follows:

Assurance Level	OID
Class 1	2.16.356.100.2.1
Class 2	2.16.356.100.2.2
Class 3	2.16.356.100.2.3
eKYC – Single-Factor	2.16.356.100.2.4.1
eKYC – Multi-Factor	2.16.356.100.2.4.2

The OIDs allocated to CA and CPS are as given below

Serial No.	Product	OID
1	IDRBT CA	2.16.356.100.1.2
2	IDRBT CA CPS	2.16.356.100.1.2.2

OID for document signer certificates

Document Signer	2.16.356.100.10.1

1.3 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 Controller of Certifying Authorities (CCA)

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

1. Developing and administering India PKI CP.
2. Compliance analysis and approval of the licensed CAs CPS;
3. Laying down guidelines for Identity Verification, Interoperability of DSCs, and Private Key storage
4. Ensuring continued conformance of Licensed CAs with the CPS by examining compliance audit results.

1.3.1.2 CA

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

IDRBT CA certificates are certified by the Root Certifying Authority of India (RCAI). In India's PKI hierarchy, the Root certificate is the trust anchor for CA certificates. The following are the CA Certificates issued to CA.

Sl No	CA Certificates	Certified by
1	IDRBT CA 2022	CCA India 2022
2	IDRBT CA SPL 2022	CCA India 2022 SPL

CA created Sub-CAs to issue Digital Signature Certificates. CA certifies Sub-CA certificates and these Sub-CAs issue end entity certificates. Sub-CA suspends or revokes the end-entity Digital Signature Certificates. The CA maintains the Certificate Revocation List (CRL) CA for the revoked and suspended Digital Signature Certificates in its repository. CRL is signed by issuing CA.

1.3.1.3 Sub-CA

Sub-CAs are created and maintained in CA Physical infrastructure to meet business branding requirements. These Sub-CAs, which are part of the same legal entity as the CA, issue certificates to end entities or subscribers. The list of Sub-CAs is available at https://idrbtca.org.in.

1.3.2 PKI Services

(i) Certificate Services: Based on the assurance level requirements, CA issues various classes of Certificates. The category of certificates includes individual, organizational person, and special types of certificates. These special types of Certificates include System Certificates, Document Signers, Encryption, etc. The certificates are issued subjected to the verification requirements specified under CCA-IVG and annexure-1

(ii) CRL Services: CA makes available CRL at https://idrbtca.org.in for freely downloadable by Subscribers and Relying Parties

(iii) OCSP (Online Certificate Status Protocol) Validation Services: CA provides OCSP validation services to Relying Parties for certificate status verification in real-time. The OCSP service of the CA is operated as per CCA-OCSP

(iv) eSign - online Digital Signature Services: CA is empanelled as ESP to offer eSign online Digital Signature Service as per the CCA-eAUTH for facilitating digitally signed DSC application forms of subscribers. e-KYC class of certificates will be issued as stated under CCA-CP. ESP of CA also provide external eSign services Managed by CA

eSign-Online Digital Signature Services is based on online Aadhaar eKYC or eKYC by CA. For CA eKYC-based eSign service or issuance of DSC, applicants are required to create an eKYC account with CA. CA carries out the verification based on the following modes mentioned in CCA-IVG

1. Online Aadhaar eKYC,
2. Off-line Aadhaar eKYC,
3. PAN eKYC,
4. Organizational KYC

The DSCs are issued to applicants for document signing provided through the eSign Service of CA. The applicants are electronically authenticated to the eKYC services of CA or other specified eKYC services by CCA. CA provide a direct interface to the applicant for providing authentication information and also for accessing eKYC information retained in the CA eKYC database. CA issue short-validity Digital Signature Certificates of 30 minutes to eSign users directly. After the generation of

DSC and signature creation, ESP of CA ensures that the private keys are destroyed immediately. The subscriber's private key storage requirements are not applicable in this mode of DSC issuance.

CA does not suspend or revokes eKYC classes of Digital Signature Certificates. However, the CA maintains a null Certificate Revocation List (CRL) in its repository to satisfy the requirements of relying party applications. CRL is signed by issuing CA. Similarly, re-key and renewal do not apply to eKYC classes of Digital Signature Certificates

The identity and address of the DSC applicant are obtained based on the authentication of the DSC applicant to the eKYC service. To retain the eKYC of the applicant by CA, the process of the applicant's identity verification is followed as specified under CCA-IVG. In the case of external eKYC service, the response received from the eKYC provider will be accepted provided with eKYC provider provides an eKYC response directly to CA up on the authentication by the applicant. The list of approved eKYC providers is specified by CCA and listed in CCA-eAUTH.

ESP of CA facilitates DSC application form generation; key generation of DSC applicant based on the authentication provided by the DSC applicant and ensures that the applicant's identity information and public key are properly bound. Additionally, the CA records the process that was followed for the issuance of each certificate. The process documentation and authentication requirements are as specified in the CCA-eAUTH and CCA-IVG

Once the verification of the applicant is carried out and recorded in the CA eKYC database, the issuance of eKYC classes of DSC is implemented in an automated environment with the requirement of authentication of the applicant to the eKYC database. Issuance of eKYC classes and Class1-3 of DSCs are carried out from separate certificate issuance systems.

The users of the Application Service Provider (ASP) interface with ESP of CA for Signature and DSC issuance through the ASP gateway. ASPs are registered with the ESP of CA after a verification process. CA verifies the source of the request and authenticates users directly for each certificate request received from ASP before DSC issuance. . Certificates are electronically verified to ensure that all the fields and extensions are properly populated. The certificates are of one-time use and the issued certificates are achieved. The private keys of applicants are destroyed immediately after certificate generation and signature function. The signatures along with the certificate are delivered to the end entity subscribers.

In the case of issuance of eKYC classes of DSC to the users of eSign Service, the requirements specified above will override the requirements specified for Class 1-3 in the respective sections of this CPS

(v) Time Stamping Service: CA Provides Time Stamping Service in accordance with CCA-TSP.

1.3.3 Registration Authority (RA)

The RA provide necessary assistance to the applicants during the Digital Signature Certificate (DSC) enrollment process without representing or acting on behalf of the subscriber

1.3.4 Subscribers

A Subscriber is an entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate as per the certificate policy asserted in the certificate, and who does not itself issue certificates.

1.3.5 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.

1.3.6 Applicability

IDRBT CA issues the following classes of certificates. The Assurance level and Applicability as defined under India PKI CP is given below

Assurance Level	Assurance	Applicability
Class 1	Class 1 certificates shall be issued for bank officials. 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	Class 2 certificate issuance processes utilize various procedures to obtain probative evidence	This is appropriate for digital signatures

	of the identity of applicants. These validation procedures provide strong assurance of an applicant's identity.	and encryption where assurance level is medium.
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.
eKYC - Single Factor	eKYC -Single Factor class of certificates shall be issued based on Single Factor authentication of the subscriber to the applicable eKYC services. These certificates will confirm that the information in the Digital Signature certificate provided by the subscriber is the same as information retained in the eKYC databases pertaining to the subscriber	This level is relevant to environments where Single Factor authentication to eKYC service is an acceptable method for credential verification before issuance of DSC. Certificate holders' private keys are created on hardware and destroyed immediately after one-time usage at this assurance level.
eKYC - Multi-Factor	eKYC - Multi-Factor class of certificates shall be issued based on Multi-Factor authentication of the subscriber to the applicable eKYC services. These certificates will confirm that the information in the Digital Signature certificate provided by the subscriber same as the information retained in the eKYC databases of the subscriber.	This level is relevant to environments where Multi-Factor authentication to eKYC service is an acceptable method for credential verification before 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 is governed by the IT Act of 2000 and the Interoperability Guidelines published by CCA.

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization administering the document

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

1.5.2 Contact Person

Questions/Queries regarding this CPS may be directed to the CA at cahelp@idrbt.ac.in
CA can be contacted at the following address.:

The CA Administrator
IDRBT,
Castle Hills, Road No: 1, Masab Tank
Hyderabad – 500057
Telephone Number: +91-40-23294216/17/19/21/23
Fax number: +91-40- 23535157
e-mail: cahelp@idrbt.ac.in

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

The IDRBT CA Policy Approval Committee must sanction CPS intended for use within the IDRBT CA PKI. However, the final approval to the CPS will be made by the Controller of Certifying Authorities, Ministry of Electronics & Information Technology, Government of India.

IDRBT CA's policy authorities consist of:

- Policy Approval Committee
  IDRBT CA Policy Approval Committee has been established to maintain the integrity of the policy infrastructure in IDRBT CA (Ref# IDRBTCA/DOC/SPP: Security Policies and Procedures).
  The same committee periodically reviews the operational requirements of IDRBT CA Certification Services and revises the policies.

1.5.5 Waivers

There are no waivers to this CPS.

2 PUBLICATION & PKI REPOSITORY RESPONSIBILITIES

2.1 PKI Repositories

CA maintains Hypertext Transfer Protocol (HTTP) or LDAP-based repositories that contain the following information:

1. CA Certificates
   Issued to their sub-CAs
2. Certificate Revocation List (CRL)
   Issued by the Licensed CA
   Issued by their sub-CAs
3. Digital Signature Certificates issued by CA

2.1.1 Repository Obligations

CA maintains a repository and is available at https://idrbtca.org.in/

2.2 Publication of Certificate Information

2.2.1 Publication of CA Information

See Section 2.1.

2.2.2 Interoperability

See Section 2.1.

2.3 Publication of Certificate Information

CA Certificates and CRLs are published as specified in this CPS in Section 4.

2.4 Access Controls on PKI Repositories

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

3 IDENTIFICATION & AUTHENTICATION

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

3.1 Naming

3.1.1 Types of Names

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

3.1.2 Need for Names to be Meaningful

The certificates issued according to this CPS take care of the following

(i) Names used in the certificates identify the person or object to which they are assigned in a meaningful way.

(ii) The DNs and associated directory information trees reflect organizational structures.

(iii) The common name represents the subscriber in a way that is easily understandable by 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

3.1.3 Anonymity of Subscribers

CA does not issue subscriber certificates with anonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms will be according to applicable Standards.

3.1.5 Uniqueness of Names

Name uniqueness for interoperability or trustworthiness is enforced in association with serial numbers.

3.1.6 Recognition, Authentication & Role of Trademarks

No stipulation.

3.1.7 Name Claim Dispute Resolution Procedure

The CA resolves any name collisions (in association with the serial number or unique identifier) 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 DSC applicant named in a certificate generates its keys, the DSC applicant is required to prove possession of the private key, which corresponds to the public key in the certificate request. This will be performed by the DSC applicant using its private key to sign a value and provide that value to the issuing CA. The CA then validates the signature using the DSC applicant public key.

3.2.2 Authentication of Organization user Identity

Requests for certificates in the name of an organizational user are mandated to include the user name, organization name, address, and documentation providing the existence of the organization. CA verifies the information relating to the authenticity of the requesting representative as per the requirements mentioned under Annexure 1.

3.2.3 Authentication of Individual Identity

CA follows the process of the applicant's identity verification as specified under CCA-IVG. CA provides a software interface for key generation by DSC applicants and ensures that the applicant's identity information and public key are properly bound. Additionally, the CA records the process that was followed for the issuance of each certificate. Process information depends upon the certificate level of assurance and is addressed in the applicable CPS. The process documentation and authentication requirements include the following:

1. The identity of the person performing the identity verification;
2. A signed declaration by that person on the application is that he or she verified the identity of the applicant;
3. The applicant is required to present one photo ID and also an attested document as proof of residential address.
4. Unique identifying numbers from the Identifier (ID) of the verifier and 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.
7. Identity is established by in-person proofing before CA or an equivalent mechanism like online Video Verification. To confirm identities; the information provided by whom is verified to ensure legitimacy.

3.2.3.1 Authentication of Component Identities

Requests are accepted from the human sponsor in the case of computing and communications components (routers, firewalls, servers, etc.), which are named as the certificate subject. The human sponsor will 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 CA to communicate with the sponsor when required

3.2.4 Non-verified Subscriber Information

CA does not include non-verified Information provided by DSC applicants in certificates.

3.2.5 Validation of Authority

Certificates that contain explicit or implicit organizational affiliation are issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity. The procedure followed by CA to establish the applicant's affiliation to the organization is as specified under CCA-IVG.

3.2.6 Criteria for Interoperation

Certificates are issued in compliance with CCA-IOG to ensure interoperability.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

The subscribers have to undergo a fresh identity-proofing process for the period for which the certificate has been issued. The maximum time for which initial identity-proofing can be relied upon for issuance of a fresh certificate is as per the table below:

Assurance Level	Initial Identity Proofing
Class 1	2 Years
Class 3	2 Years

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

3.3.2 Identification and Authentication for Re-key after Revocation

If a certificate has been revoked, CA issue a fresh certificate to the subscriber-only after the initial registration process described in Section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests are authenticated in the following manner.

1. Electronic requests to revoke a certificate authenticated using that certificate's associated public key, regardless of whether or not the private key has been compromised.

2. In case the possession of the key is not with the subscriber, suspend/revoke the certificate after verifying the subscriber's identity.
3. In the case where the subscriber is not in a position to communicate (death, unconscious state, mental disorder), revoke the certificate after verification

The subscriber should request the IDRBT CA for the certificate revocation specifying the reason. Where sufficiently reliable authentication of the revocation list is not possible, the IDRBT CA accepts or reject the request on the best possible judgment basis. If IDRBT CA is in doubt and cannot receive further information on whether to revoke or not, priority will be given to the revocation. The certificate holder will be informed that the certificate has been revoked and the reasons for revocation will be presented. The IDRBT CA will log all actions taken during a revocation process.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Communication among the CA, RA, and the subscriber are implemented with 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.

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

When cryptography is used, CA implemented the mechanism, at least as strong as the certificates being managed, to secure web site using Secure Socket Layer (SSL) certificate and set it up with appropriate algorithms and key sizes to satisfy the integrity and confidentiality requirements for certificate management.

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

4.1 Certificate requests

The applicant intending to obtain DSC from CA needs to submit a DSC application form filled with identity details, address, photo, and signature with duly attested supporting documents to CA. On receipt of the request and information in the prescribed format, CA carries out the verification of documents and Video and Mobile number verification if applicable. The detailed requirements for each category of DSC applicants are specified under CCA-IVG.

A signed declaration by the person performing the identity verification is recorded on the DSC application form that he or she verified the identity of the applicant.

Upon the approval of the CA trusted person for the DSC application request, the DSC is issued to the DSC applicant. The DSCs are published on the repository of the CA, on acceptance by the subscriber.

4.1.1 Submission of Certificate Application

The DSC applicant is required to submit the duly filled DSC application form along with the supporting documents to CA. The application forms for various types of certificates are available on the CA website at https://idrbtca.org.in.

4.1.2 Enrollment Process and Responsibilities

For certificates, all end-user applicants undergo an enrollment process consisting of:

- Completing and submitting a certificate application form and providing the required information,
- Generating a key pair.
- Delivering his/ her, or its public key to CA
- Demonstrating to CA that the certificate applicant has possession of the private key corresponding to the public key delivered to CA.

- Manifesting assent to the relevant subscriber agreement.

4.2 Certificate Application Processing

CA verifies that information in certificate applications is accurate based on the supporting documents, telephonic interaction, Video Verification, and other procedures specified under CCA-IVG.

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

Certificate Applications submitted to the CA for processing could result in either approval or denial.

4.3 Certificate Issuance

After a certificate applicant submits a certificate application, the CA verifies or refutes the information in the certificate application. Upon successful verification based on all required authentication procedures for various classes of certificates, forward the certificate application for approval. The applicant's request for certificate issuance is reviewed by a trusted person which may result in approval or denial of the certificate.

The responses received from publically available databases, used to confirm Subscriber information, are protected from unauthorized modification.

4.3.1 CA Actions during Certificate Issuance

CA verifies the source of a certificate request before issuance. If the crypto medium has opted for key generation and storage, the details such as make, model, serial no, etc are also recorded. Certificates are checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, CA publishes the certificate in the repository.

4.3.2 Notification to Subscriber of Certificate Issuance

CA will notify the subject (End Entity Subscriber) of certificate issuance through email and internet links.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The DSC applicant must confirm acceptance of the certificate upon notification of issuance by the CA. Notification and link are sent to the subscriber for downloading the certificate. The content of the certificate will be displayed to the subscriber along with the download option. Downloading the certificate constitutes the subscriber's acceptance of the certificate.

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 are liable to protect their private keys from access by any other party. For individual Signature certificates, subscribers are required to generate key pairs in FIPS 140-2/3 level 2 crypto devices.

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

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, for the time remaining in validity and other information as the old one, but with a new, extended validity period and a new serial number. Certificates are renewed by CA only 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 Circumstances 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. Requests for renewal of certificates are not accepted by CA at present due to the constraint present in the CCA-IVG.

4.6.2 Who may Request Renewal

In a normal scenario,

A Subject may request the renewal of its certificate.

A PKI Sponsor may request renewal of the 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

In the normal scenario, a certificate renewal will be using one of the following processes:

1. The 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

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

4.7.1 Circumstances for Certificate Re-key

CA issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled to a certificate subject to the requirements set forth under CCA-IVG.

4.7.2 Who may Request Certification of a New Public Key

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

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

4.7.3 Processing Certificate Re-keying Requests

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

1. The 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

CA authenticates the request for revocation before revocation. Subscribers are required to submit paper-based revocation requests as specified under IT CA Rules. Electronic requests to revoke a certificate have to be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4.9.1 Circumstances for Revocation of a Certificate

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

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

Whenever any of the above circumstances occur, CA revokes the certificate and places it on the CRL. Revoked certificates are included on all new publications of the certificate status information until the certificates expire. CA ensures that the revoked certificate will 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 CA, may request revocation of a certificate.

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

4.9.3 Procedure for Revocation Request

CA identifies the certificate to be revoked as mentioned in the request for revocation, the reason for revocation, and verifies the authentication requirements (e.g., digitally or manually signed by the subject). CA may perform Telephonic verification and video verification to ensure the identity of the subscriber.

Upon receipt of a revocation request, CA authenticates the request and then revokes the certificate, and informs the subscriber about the revocation of the certificate by email.

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

CA make its 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 the next CRL generation.

4.9.6 Revocation Checking Requirements for Relying Parties

The 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 the 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

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

CA publishes CRLs no later than the next scheduled update.

CA issue CRLs at least once every 24 hours with a minimum validity of 7 days.

In addition, CA issues CRLs and posts the CRL immediately if a certificate is revoked for the reason of a key compromise.

4.9.8 Maximum Latency for CRLs

CA publishes CRLs immediately after generation. Furthermore, each CRL will be published no later than the time specified in the nextUpdate field of the previously issued CRL. CAs 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

CA supports online certificate status checking. Client software using online certificate status checking need not obtain or process CRLs.

The online revocation/status checking provided by CA meets or exceeds the requirements for CRL issuance stated in 4.9.7.

IDRBT CA provides an online Directory Server for verifying the status of Certificates issued within the IDRBT CA PKI. IDRBT CA may implement the Online Certificate Status Protocol (OCSP) in the future for the online status checking of the certificates.

4.9.10 Online Revocation Checking Requirements

No stipulation beyond Section 7.3.

4.9.11 Other Forms of Revocation Advertisements Available

Other than the implementation of CRLs and online revocation status, no other forms of online revocation status will be provided by CA.

4.9.11.1 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

None beyond those stipulated in Section 4.9.7.

4.9.13 Circumstances for Suspension

The suspension will be permitted if a user's token holding a private key is temporarily unavailable to them.

4.9.14 Who can Request a Suspension

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

4.9.15 Procedure for Suspension Request

The requester submitting a request to suspend a certificate should provide the information to 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 will be populated with "certificate Hold" by CA. The Hold Instruction Code CRL entry extension will 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 will be revoked for the reason of "Key Compromise".

To mitigate the threat of an unauthorized person removing the certificate from hold, the subscriber identity will be authenticated in person using the initial identity proofing process described in Section 3.2.3.

4.10 Certificate Status Services

IDRBT CA provides an online Directory Server for verifying the status of Certificates issued within the IDRBT CA PKI. IDRBT CA may implement the Online Certificate Status Protocol (OCSP) in the future for the online status checking of the certificates.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

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

5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS

5.1 Physical Controls

CA operation premises are actively monitored with redundant power and notification methods. Sensitive areas within the facility, such as power and network connection are also controlled within the protected facility.

The operation site has multiple tiers of security enforced through Photo ID badges, proximity cards, and biometric access devices. All visitors are escorted by trusted persons and every visitor signs the visitor's log.

The facility is continually staffed (24x7), either by trusted persons or by an on-site guard service during non-business hours.

5.1.1 Site Location & Construction

The system components and operation of CA are contained within a physically protected environment to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information. The physical security standards are modeled as per the physical and operational security guidelines mentioned in the Information Technology Act.

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

Tier 1: The common area in the vicinity of the CA operations set-up where in physical access check is performed. This is the area where common facilities are incorporated.
Tier 2: This is the first level where CA operations commence. This is manned by physical security personnel and also enforces physical proximity access control restricting entries only to CA-authorized personnel.
Tier 3: Enables two-factor authentications (biometrics and physical proximity). The receiving and dispatch are carried out in this area.
Tier 4: This is where the core CA operations are housed. Servers are installed in this area.
Tier 5: Certificate issuance and revocation is done in this area which houses the Certificate Manager server. The Key Ceremony is also done here. The HSM module is housed in this area.

5.1.2 Physical Access

5.1.2.1 CA Physical Access

CA has implemented a mechanism to protect equipment from unauthorized access.

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

1. No unauthorized access to the hardware is permitted

2. All removable media and paper containing sensitive plain-text information is stored in secure containers
3. All entries/exits are monitored either manually or electronically.
4. access logs are maintained and inspected periodically
5. Multiple layers of increasing security are provided in areas such as the perimeter, building, and CA room
6. Two-person physical access controls are required for both the cryptographic module and computer system for CAs.

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention & Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed following the manufacturer's guidance before disposal. Other wastes are disposed of as per the CA's normal waste disposal requirements.

5.1.8 Off-Site backup

Full system backups of the CAs sufficient to recover from system failure, are created on a periodic schedule, and incrementally backup copies are stored at an offsite location. Backups are performed and stored off-site not less than once every 7 days. The data is properly secured based on the classification of data, which is defined by the Certifying Authority in the security policy.

5.2 Procedural Controls

5.2.1 Trusted Roles

CA ensures that

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

CA operations are carried out by four roles which are 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 keys runnel for section system communication.
2. CA Officer – authorized to verify and approve certificates or certificate revocations.
3. Audit Administrator – authorized to view and maintain audit logs.
4. System Administrator – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.1.1 CA Administrator

The administrator is 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.
5. Administrators will not issue certificates to subscribers.

5.2.1.2 CA Officer

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

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

5.2.1.3 Audit Administrator

The Audit Administrator is responsible for:

1. Reviewing, maintaining, and archiving audit logs;
2. Performing or overseeing internal compliance audits to ensure that the CA is operating as per its CPS;

5.2.1.4 System Administrator

The System Administrator is 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

The RA optionally supports applicants in completing the subscriber identity verification process, ensuring the required information and documentation are properly provided to the Certifying Authority (CA)

5.2.1.6 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components that are named public key certificate subjects. The PKI Sponsor works with the CAs to register components (routers, firewalls, etc.) following 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

Separate individuals are identified for each trusted role to ensure the integrity of the CA operations. Two or more persons are 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.

In addition, sensitive CA operations like operations of the cryptographic units and certificate manager require the m-out-of-n control to handle the operations of these sensitive functions. Also, split control is implemented to ensure segregation between physical and logical access to systems. Personnel having secret shares do not have physical access and vice-versa. All roles are assigned to multiple persons to support the continuity of operations.

5.2.3 Identification and Authentication for Each Role

All personnel seeking to become trusted persons are required to be in the payroll of CA. Thorough background checks are carried out before engaging such personnel for CA Operations. The Certifying Authority follow the procedures approved by management for the background check and there are documented for audit purpose.

CA ensures that personnel has achieved trusted status and approval has been given before such personnel is:

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

5.2.4 Roles Requiring Separation of Duties

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

1. Individuals who assume an Officer role will not assume CA Administrator or Audit Administrator role;
2. Individuals who assume an Audit Administrator role will not assume any other role on the CA; and
3. Under no circumstances any of the four roles will perform its own compliance audit function.
4. No individual will be assigned more than one identity

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles will be selected based on trustworthiness, and integrity, and are subject to a background investigation. Personnel will be appointed to trusted roles (CA trusted roles) based on:

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

5.3.2 Background Check Procedures

All persons filling trusted roles (including CA trusted roles) should have completed a favorable background investigation. The scope of the background check includes the following areas covering the past five years:

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

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

The background will be verified every three years.

5.3.3 Training Requirements

CA ensures that all personnel performing duties concerning the operation of a CA receive comprehensive training. Training will be conducted in the following areas:

1. CA 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. Subscriber verification requirements

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

IDRBT CA personnel will undergo job rotation practices as per the Human Resources Policy of IDRBT.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Documentation Supplied To Personnel

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA operating system and the CA applications required by this CPS are enabled. Each audit record includes 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 are audited:

Auditable Event	CA
SECURITY AUDIT	
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	
Any attempt to delete or modify the Audit logs	
IDENTITY-PROOFING	
Successful and unsuccessful attempts to assume a role	
The value of the *maximum number of authentication attempts* is changed	
The number of unsuccessful authentication attempts exceeds the maximum *authentication attempts* during user login	
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	
An Administrator changes the type of authenticator, e.g., from a password to a biometric	
LOCAL DATA ENTRY	
All security-relevant data that is entered in the system	

Auditable Event	CA
REMOTE DATA ENTRY	
All security-relevant messages that are received by the system	
DATA EXPORT AND OUTPUT	
All successful and unsuccessful requests for confidential and security-relevant information	
KEY GENERATION	
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	
PRIVATE KEY LOAD AND STORAGE	
The loading of Component private keys	
All-access to certificate subject Private Keys retained within the CA for key recovery purposes	
TRUSTED PUBLIC KEY ENTRY, DELETION, AND STORAGE	
All changes to the trusted Component Public Keys, including additions and deletions	
PRIVATE AND SECRET KEY EXPORT	
The export of private and secret keys (keys used for a single session or message are excluded)	
CERTIFICATE REGISTRATION	
All certificate requests	
CERTIFICATE REVOCATION	
All certificate revocation requests	
CERTIFICATE STATUS CHANGE APPROVAL	
The approval or rejection of a certificate status change request	
CONFIGURATION	
Any security-relevant changes to the configuration of the Component	
ACCOUNT ADMINISTRATION	
Roles and users are added or deleted	
The access control privileges of a user account or a role are modified	
CERTIFICATE PROFILE MANAGEMENT	

Auditable Event	CA
All changes to the certificate profile	
CERTIFICATE STATUS PROVIDERMANAGEMENT	
All changes to the CSP profile (e.g. OCSP profile)	
REVOCATION PROFILE MANAGEMENT	
All changes to the revocation profile	
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	
All changes to the certificate revocation list profile	
MISCELLANEOUS	
Appointment of an individual to a Trusted Role	
Designation of personnel for multiparty control	
Installation of the Operating System	
Installation of the PKI Application	
Installation of hardware cryptographic modules	
Removal of hardware cryptographic modules	
Destruction of cryptographic modules	
System Startup	
Logon attempts to PKI Application	
Receipt of hardware / software	
Attempts to set passwords	
Attempts to modify passwords	
Back up of the internal CA database	
Restoration from back up of the internal CA database	
File manipulation (e.g., creation, renaming, moving)	
Posting of any material to a PKI Repository	
Access to the internal CA database	
All certificate compromise notification requests	
Loading tokens with certificates	
Shipment of Tokens	

Auditable Event	CA
Zeroizing Tokens	
Re-key of the Component	
CONFIGURATION CHANGES	
Hardware	
Software	
Operating System	
Patches	
Security Profiles	
PHYSICAL ACCESS / SITE SECURITY	
Personnel Access to room housing Component	
Access to the Component	
Known or suspected violations of physical security	
ANOMALIES	
Software error conditions	
Software check integrity failures	
Receipt of improper messages	
Misrouted messages	
Network attacks (suspected or confirmed)	
Equipment failure	
Electrical power outages	
Uninterruptible Power Supply (UPS) failure	
Obvious and significant network service or access failures	
Violations of Certificate Policy	
Violations of Certification Practice Statement	
Resetting the Operating System clock	

5.4.2 Frequency of Processing Audit Logs

Audit logs are examined for key security and operational events at least every week. In addition, CA reviews its audit logs as required in the event of any suspicious or unusual activity based on irregularities and incidents within CA systems.

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

5.4.3 Retention Period for Audit Logs

See Section 2.

5.4.4 Protection of Audit Logs

System configuration and procedures are implemented together to ensure that:

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

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

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are archived as per Section 5.5.1.

5.4.6 Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application, network, and operating system levels. Manually generated audit data is recorded by CA personnel.

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

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Events in the audit log are recorded, in part, to monitor system vulnerabilities. A vulnerability assessment is performed, reviewed, and revised following an examination of these monitored events.

5.5 Records Archival

5.5.1 Types of Records Archived

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

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

CA protects its archived records so that only authorized persons can access the archived data. CA protects the archive against unauthorized viewing, modification, deletion, or tampering, by storage within a trustworthy system. The media holding the archive data and

the systems required to process the archive data are maintained to ensure that the archive data can be accessed for the period

5.5.4 Archive Backup Procedures

CA creates backup copies of archives compiled as and when the archives are created. Backup copies of the archive and copies of paper-based records are maintained in an off-site disaster recovery/ warehouse facility. CA has implemented a process to scan and digitize the physical documents to ensure tracking and easy retrieval.

5.5.5 Requirements for Time-Stamping of Records

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

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

5.5.6 Archive Collection System (internal or external)

The archive collection system is internal to the CA.

5.5.7 Procedures to Obtain & Verify Archive Information

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

5.6 Key Changeover

CA keys are changed periodically as stipulated by the ITAct and the key changes are processed as per key generation specified in this CPS. If CA private key is used to sign CRLs, then the key will be retained and protected.

CA provides reasonable notice to the subscriber's Relying Parties of any change to a new key pair used by CA to sign digital certificates under its trust hierarchy. The subscribers is issued a digital certificate for a specified period. The subscribers generate a new private-public key pair and submit the public key along with the new application to the CA for generating a new Certificate, preferably before the existing certificate expires.

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

Key	2048 Bit Keys	
	Private Key	Certificate
Intermediate CA	10 years	10 years
Sub-CA	10 years	10 years
Time Stamping	3 years	3 years
OCSP Responder	1 year	1 year
Human Subscriber Signature	3 years	3 years
Human Subscriber Encryption	3 years	3 years

SSL	2 years	2 years
Device/System	3 years	2 years

5.7 Compromise and Disaster Recovery

IDRBT CA has implemented a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key Compromise or disaster. (Ref# IDRBTCA/DOC/BCP: Business Continuity Plan).

This plan would consist of a detailed manual covering all the aspects of compromise and disaster recovery like key compromise, crashing of systems both software and hardware, corruption of systems both the hardware and software, communication failures, problems arising out of the strike, fire, flood or any other natural disaster.

The staff would be identified and trained to conduct these operations if, any disaster happens. Twice a year, a dry run will be conducted to test the efficacy and adequacy of the systems to take care of the compromise situation and disaster recovery plan.

5.7.1 Incident and Compromise Handling Procedures

If a CA detects a potential hacking attempt or other forms of compromise, it will perform an investigation to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 will be followed. Otherwise, the scope of potential damage will be assessed to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

CA will inform CCA if any of the following cases occur:

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

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

CA have a Disaster Recovery center as per the guidelines of the IT Act. The disaster recovery site will be made operational using the latest available backup data.

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

If both primary and Disaster recovery sites cannot be used to establish revocation capability in a reasonable time frame, the CA may request for revocation of its certificate(s) to CCA.

5.7.3 Private Key Compromise Procedures

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

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

1. A CA key pair will be generated by CA following procedures outlined in this applicable CPS;
2. New CA certificates will be requested as per 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 the date in the certificate as in original certificates; and
4. The CA will also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA will request that its certificates be revoked. The CA will follow steps 1 through 4 in Section 5.7.3 above.

5.8 CA Termination

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

CA will archive all audit logs and other records before termination.

CA will destroy all its private keys upon termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

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

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

6.1.2 Private Key Delivery to Subscriber

The subscriber private key is generated by the end subscriber and hence there is no delivery to the end subscribers. In the case of hardware-based tokens or smart cards, pre-formatted tokens are sent to the subscribers and the associated PIN is sent by an out-of-band process. The end user then uses the token and the client software provided to him to generate and store the private key and also initiates an online session with the CA server for certificate generation.

6.1.3 Public Key Delivery to Certificate Issuer

End-user subscribers generate PKCS#10 requests containing their public key and send it to the CA. This is accomplished using the client software which initiates an online session

with the CA server and delivers the signed certificates to the subscriber. The online session is secured by SSL.

6.1.4 CA Public Key Delivery to Relying Parties

CA makes its Public Keys available to Relying Parties in the repository available at https://idrbtca.org.in/.

6.1.5 Key Sizes

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

RSA and ECC keys are generated following FIPS 186-2.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, Security Requirements for Cryptographic Modules. The additional requirements for cryptographic modules are covered in CCA-CRYPTO

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 requires action by at least two persons.

6.2.3 Private Key Escrow

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

The end entity private keys used solely for decryption are escrowed before the generation of the corresponding certificates. The subscriber can keep the escrowed keys.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

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

6.2.4.2 Backup of Subscriber Private Signature Key

The CA is never in possession of the Subscriber's private signing keys.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

CA stores Private Keys in the hardware cryptographic module and keys are not accessible without an authentication mechanism that complies 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 is 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 module that has been activated is never left unattended or otherwise available for unauthorized access. After use, cryptographic modules are deactivated. After deactivation, the use of the cryptographic modules-based CA key pair requires the presence of the trusted roles with the activation data to reactivate said CA key pair.

6.2.10 Method of Destroying Private Key

Private signature keys will be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Destroying private keys inside cryptographic modules requires destroying the key(s) inside the HSM using the 'zeroization' function of the cryptographic modules in a manner that any information cannot be used to recover any part of the private key. All the private key back-ups are destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of cryptographic modules are not accessible to destroy the

key contained inside, then the cryptographic modules will be physically destroyed. The destruction operation is realized in a physically secure environment

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 is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

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

6.4.2 Activation Data Protection

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

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

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

6.4.3 Other Aspects of Activation Data

CA changes the activation data whenever the HSM is re-keyed or returned from maintenance. Before sending a cryptographic module for maintenance, all sensitive information contained in the cryptographic module is destroyed.

Subscribers are responsible to ensure the protection of their activation data

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of the operating system, software, and physical safeguards.

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

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

CA has implemented a combination of physical and logical security controls to ensure that the CA administration is not carried out with less than two-person control.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the CA are as follows:

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

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

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

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

5. CA hardware and software are scanned for malicious code on first use and periodically thereafter.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modification and upgrade is documented and controlled. There is a mechanism for detecting an unauthorized modification to the CA software or configuration. A formal configuration management

methodology is used for the installation and ongoing maintenance of the CA system. The CA software, when first loaded, is verified as being supplied by the vendor, with no modifications, and is the version intended for use.

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

CA employs appropriate security measures to ensure that they are guarded against denial of service and intrusion attacks. Such measures include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. Unused network ports and services are turned off. Protocols that provide network security attack vector(s) are not permitted through the boundary control devices.

Any boundary control devices used to protect the network on which PKI equipment is hosted will 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 components are regularly synchronized with a time service such as Indian Standard Time Service. Time derived from the time service is used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates
- OCSP

Asserted times are accurate to within three minutes. Electronic or manual procedures are used to maintain the 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 listed under CCA-IOG, Annexure III - Reference Certificate Profiles. The CA Certificates issued under this CPS conform to X-509 Version 3 digital Certificate.

The End User Certificate Profile (issued for personal use) and CA certificate profiles are listed below

1. CA Certificate Profile

CA CERTIFICATE -BASIC FIELDS	
Version	Version 3
Serial number	Positive number of maximum Length 20 bytes and unique to each certificate issued by issuer CA
Signature Algorithm	SHA256 with RSA Encryption (null parameters)
Issuer DN	Subject DN of the issuing CA
Validity	Validity expressed in UTC Time for certificates valid through 2049
Subject DN	The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate (Common Name (CN),House Identifier, Street Address, State / Province, Postal Code, Organisational Unit (OU),Organisation (O),Country (C))
Subject Public Key	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent
Signature	Issuer CA's signature
EXTENSIONS	
authorityKeyIdentifier	Identifies the CA certificate that must be used to verify the CA certificate. It contains subjectKeyIdentifier of the issuing CA certificate
subjectKeyIdentifier	unique value associated with the Public key
basicConstraints	CA Boolean = True, pathLenConstraints 0
keyUsage	keyCertSign and cRLSign
certificatePolicies	The value must contain the OID representing the India PKI certificate policy the certificate is valid for . (Policy

	Identifier=2.16.356.100.2)
cRLDistributionPoints	location of CRL information
authorityInfoAccess	location of OCSP Responder (only required if OCSP is needed to check revocation status of CA Certificate)

2. User Certificate Profile(personal)

END ENTITY CERTIFICATE -BASIC FIELDS	
Version	Version 3
Serial number	Positive number of maximum Length 20 bytes and unique to each certificate issued by a issuer CA
Signature Algorithm	SHA256 with RSA Encryption (null parameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}
Issuer DN	Subject DN of the issuing CA
Validity	Validity expressed in UTC Time for certificates valid through 2049
Subject DN	The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate (Common Name, Serial Number,State or Province Name, Postal Code, Telephone number, Pseudonym, Organisation, Country)
Subject Public Key	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent OR ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
Signature	Issuer CA's signature
EXTENSIONS	
authorityKeyIdentifier	Identifies the CA certificate that must be used to verify the subscriber's certificate. Issuing CA SubjectkeyIndetifier
subjectKeyIdentifier	Octet String of unique value associated with the Public key
basicConstraints	CA=False
keyUsage	DigitalSignature, nonRepudiation(optional)
Extended Key Usage	Document Signing: {1.3.6.1.4.1.311.10.3.12}
certificatePolicies	The value must contain the OID representing the India PKI certificate policy the certificate is valid for .((Policy Identifier=2.16.356.100.2.4.1 or 2.16.356.100.2.4.2)
cRLDistributionPoints	location of CRL information

7.2 CRL Profile

The CRL profiles are listed below.

7.2.1 Full and Complete CRL

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

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

7.2.2 Distribution Point-Based Partitioned CRL

CA issues only full and complete CRL signed by CA

7.3 OCSP Profile

OCSP requests and responses are as per RFC 2560 as listed below.

7.3.1 OCSP Request Format

Requests sent to Issuer CA OCSP Responders are not required to be signed. The following table lists the fields that are expected by the OCSP Responder.

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

7.3.2 OCSP Response Format

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

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

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

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessments

Annual compliance audit by CCA empanelled Auditor is carried out of CAs infrastructure apart from half yearly internal audit. The internal audit includes all RAs (self-audit by the parent organization of RA) and the annual compliance audit covers randomly selected RAs. IDRBT CA may perform an RA audit and keeps checks on the functioning of the RAs to ensure compliance.

8.2 Identity and Qualifications of Assessor

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

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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

8.5 Actions Taken as a Result of Deficiency

The office of CCA may determine that a CA is not complying with its obligations outlined in this CPS or the applicable CP. When such a determination is made, the office of CCA

may suspend the operation of CA, or may revoke the CA certificate, or may direct that other corrective actions be taken which allow the operation 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 take the following actions:

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

8.6 Communication of Results

On completion of the audit by an empanelled auditor, Auditor submits an Audit Report, including identification of corrective measures taken or being taken by CA, to the office of CCA and a copy to CA. The report identifies the version of the CPS used for the assessment.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

The fees for various types of certificates are made available on the CA website at https://idrbtca.org.in/ and will be updated from time to time.

9.1.2 Certificate Access Fees

CA is not charging any fees to Relying Parties or other public for accessing the certificate information from the repository. The certificate search facility is provided free of cost at its website https://idrbtca.org.in/

9.1.3 Revocation Status Information Access Fees

CA does not charge a fee for access to any revocation status information through CRL. CA may charge a fee for providing certificate status information via OCSP.

9.1.4 Fees for Other Services

No stipulation

9.1.5 Refund Policy

The refund policy and other payment terms are governed as per the terms in the subscriber agreement. In case the application is rejected the full amount would be refunded to the subscriber.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CA maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to PKI Participants described in Section 1.3 of this CPS

9.2.2 Other Assets

CA also maintains 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 CPS.

9.2.3 Insurance or Warranty Coverage for End-Entities

CA offers no protection to end entities that extends beyond the protections provided in this CPS

9.3 Confidentiality of Business Information

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

9.4 Privacy of Personal Information

CA stores, process, and disclose personally identifiable information following the provisions of the IT Act 2000 & Rules made thereunder.

9.5 Intellectual Property Rights

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

9.5.1 Property Rights in Certificates and Revocation Information

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

9.5.2 Property Rights in the CPS

This CPS is based on the proforma CPS published by the Office of CCA for Licensed CAs and as amended from time to time. All Intellectual Property Rights in this CPS of CA are owned by the CA.

9.5.3 Property Rights in Names

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

9.5.4 Property Rights in Keys

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

Subject to any agreements between CA and its customers, ownership of and property rights in key pairs corresponding to Certificates of Subscribers is specified in this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

9.6.1.1 CA

CA represents and warrants the following provisions of the IT Act, 2000 & Rules made thereunder that;

1. signing private key is protected and no unauthorized person will ever have access to that private key;

2. Each Subscriber has been required to represent and warrant that all information supplied by the Subscriber in connection with, and/or contained in the Certificate is true.

3. Only verified information appears in the certificate

9.6.2 Subscriber

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

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

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

7. The subscriber should follow the duties as mentioned in the IT Act.

9.6.3 Relying Party

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

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, before 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 should 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, CA disclaims all warranties other than any express warranties contained in such agreements or outlined in this CPS.

9.8 Limitations of Liabilities

CA limit liabilities as long as CA meets the liability requirements stated in ITAct, 2000 and the Rules made thereunder. CA is responsible for verification of any Subscriber to whom it has issued a certificate and to all Relying Parties who reasonably rely on such certificate following this CPS, for damages suffered by such persons that are caused by the failure of the CA to comply with the terms of its CPS or its Subscriber Agreement, and sustained by such persons as a result of the use of or reliance on the certificate.

The verification requirements for certificate issuance by CA are as specified under ITAct 2000 and Rules made thereunder and reasonable effort by CA. CA cannot guarantee the activities or conduct of the subscribers.

CA will not be liable for any indirect, exemplary, special, punitive, incidental, or consequential losses, damages, claims, liabilities, charges, costs, expenses, or injuries (including without limitation loss of use, data, revenue, profits, business and for any claims of Subscribers or Users or other third parties including Relying parties).

CA will not be liable for any delay, default, failure, or breach of its obligations under the Subscribers Agreement, Relying Party Terms & Conditions, and Registration Authority Agreement

All liability is limited to actual and legally provable damages. CA's liability is as per the ITAct,2000 other governing Indian laws, and Agreements. If the liability is not dealt with under the provisions of ITACT 2000, the following caps limit CA's damages concerning specific certificates.

Class	Liability Caps/per Certificate
Class 1	Indian Rupees Ten Thousand
Class 2	Indian Rupees Fifty Thousand
Class 3	Indian Rupees One Lakh
e-kyc Single Factor	Indian Rupees One Thousand
e-kyc Multi Factor	Indian Rupees Two Thousand

9.9 Indemnities

Indemnification by Subscribers

To the extent permitted by applicable law, the subscriber agreement requires Subscribers to indemnify CA for:

- False and misrepresentation of fact by the subscriber on the subscriber's certificate application,
- Suppression of a material fact on the certificate application, if the omission was made negligently or with intent to deceive any party,
- The subscriber's failure to protect the subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key, or
- The subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) infringes upon the Intellectual Property Rights of a third party.

Indemnification by relying parties

To the extent permitted by applicable law, relying party agreement requires, Relying Parties to indemnify CA for:

- The relying party's failure to perform the representations and warranties as outlined in section 9.6.3 of this CPS.
- The relying party's reliance on a certificate that is not reasonable under the circumstances, or
- The relying party's failure to check the status of such certificate to determine if the certificate is expired or revoked.

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon approval by the Office of CCA. Amendments to this CPS become effective upon ratification by approval by CCA and publication by CA at https://idrbtca.org.in/. There is no specified term for this CPS.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, CA is nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. Sections 5.5 and 9 of this CPS will survive the termination or expiration of this CPS.

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

If the Office of CCA wishes to recommend amendments or corrections to this CPS, such modifications will be submitted to CCA for approval.

CA will use reasonable efforts to notify subscribers and Relying Parties of changes.

9.12.2 Notification Mechanism and Period

Errors and anticipated changes to this CPS resulting from reviews are published online at https://idrbtca.org.in/

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

9.12.3 Circumstances under Which OID Must be changed

CCA determines the requirement for changing the Certificate Policy OIDs.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among Licensed CAs and Customers

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

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

9.13.2 Alternate Dispute Resolution Provisions

No stipulations.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Waiver of Rights

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

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation.

10 BIBLIOGRAPHY

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

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

11 ACRONYMS AND ABBREVIATIONS

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