IDRBT CA

CERTIFICATION PRACTICE STATEMENT

VERSION 4.0.3

DATE OF PUBLICATION: 08.06.2022

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: 2022.06.14 13:23:21 +05'30'

CERTIFICATION PRACTICE STATEMENT

Document Name	CPS of IDRBT CA
Release	Version 4.0.3
Status	Release
Issue Date	08.06.2022

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	

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 offence affecting IDRBT CA's policies and practices. Such 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 system, 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 shall have the meaning respectively assigned to them in the Act.

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

"Act" means Information Technology IT Act, 2000

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

"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 sign the content through any empanelled ESP.

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

"CA" refers to IDRBT CA, a Certifying Authority, licensed by 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 work stations, used for the purpose of administering Digital Signature Certificates and keys.

"**CA Verification Officer**" means trusted person involved in identity and address verification of DSC applicant and according 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 prior to 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 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 by means of an electronic method or procedure in accordance with the provisions of section 3 of 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—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 definition in Second Schedule of 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” is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of applicant’s credentials

“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 certificate issued or facilitated the digital signature creation.

"Subscriber Identity Verification method" means the method used for the verification of the information (submitted by subscriber) that is required to be included in the Digital Signature Certificate issued to the subscriber in accordance with 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 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 in accordance with this Certification Practice Statement

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

Time Stamp—A notation that indicates (at least) the correct date and time of an action, and 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 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 Controller of Certifying Authorities (CCA) for issuing, managing, renewing and revoking Digital Certificates in accordance with published practice (IDRBT CA CPS).

At present IDRBT issues Digital Certificates to Banks and Financial Institutions who are members of INdian FInancial NETwork (INFINET) as per the policy in force. The policy, if required, may be changed from time to time, at the discretion of Top Management.
IDRBT CA currently offers 3 distinct classes of certification services. Each class of certificate provides specific functionality and security features. The Classes are:

- Class 1 Certificate
- Class 3 Certificate

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 the 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 compromise 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

The Institute for Development and Research in Banking Technology (IDRBT) is an, autonomous institution performing Research and Development in Banking Technology for the benefit of Banks and Financial Institutions in India. IDRBT has established the INdian FINancial NETwork (INFINET) based on VSAT and Terrestrial Communication Technologies. INFINET is a countrywide communication backbone for the Banks and Financial Institutions used for electronic payment systems and for other communication transfers.

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 Controller of Certifying Authorities (CCA) for issuing, managing, renewing and revoking Digital Certificates in accordance with published practice (IDRBT CA CPS).

At present IDRBT issues Digital Certificates to Banks and Financial Institutions who are members of INdian FInancial NETwork (INFINET) as per the policy in force. The policy, if required, may be changed from time to time, at the discretion of Top Management

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

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

(i) intended to be applicable 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 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, 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 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 are 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

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

Sl No	CA Name	Certified by
1	IDRBT CA 2014	CCA India 2014
2	IDRBT CA 2015	CCA India 2015 SPL
3	IDRBT CA 2022	CCA India 2022

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

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, organisational person and special type of certificates. These special types of Certificates include System Certificate, Document Signer, and 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) Time Stamping Service: CA Provides Time Stamping Service in accordance with CCA-TSP.

1.3.3 Registration Authority (RA)

Registration Authorities will be nominated by the banks concerned with IDRBT and trusted with IDRBT CA, serving as a point of contact for registration of users, i.e. to have a certificate issued. The IDRBT CA will create RA Office at the request of the bank concerned. The RAs will be appointed by IDRBT CA with set criteria of physical verification and with the approval of IDRBT CA Office.

After verification of the credentials of the RA by IDRBT CA, the RA has to appear in person (if required/ necessary) for face to face verification and will be issued a Class 3 Certificate from IDRBT CA. The RA Office will verify the credentials of the subscribers as mentioned in this CPS and will approve the certificate request and release the request to IDRBT CA Office for the issuance of the certificate.

Under the IT Act, all functions of RA are subsumed within the IDRBT CA. IDRBT CA is responsible for all actions of RAs including correctness of the subscriber information given by RA which is incorporated using contractual Master Agreement.

1.3.4 Subscribers

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

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 3	This certificate will be issued to bank officials 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.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization administering the document

This CPS is administered by 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 suitability of a CPS will be based on an independent auditor's results and recommendations.

1.5.4 CPS Approval Procedures

The CCA approve CPS of the CA and 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 shall be 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
2. Certificate Revocation List (CRL)
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 there under. Before issuing a Certificate, the CA ensure that all Subject information in the Certificate conforms to the requirements that has been verified in accordance with 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 pursuant to this CPS shall taken care of the following

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

(ii) The DNs and associated directory information tree 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 shall be in accordance with applicable Standards.

3.1.5 Uniqueness of Names

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

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 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 own keys that 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 providing 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 applicant's identity verification as specified under CCA-IVG. CA provides software interface for key generation by 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 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 attested document as a proof of residential address.
4. Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant;
5. The date and time of the verification; and
6. A declaration of identity signed by the applicant using a handwritten signature or equivalent per Indian Laws.
7. Identity is established by in-person proofing before CA or equivalent mechanism like or 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 human sponsor in the case of computing and communications components (routers, firewalls, servers, etc.), which is 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 applicant 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 organisation is as specified under CCA-IVG.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

The subscribers have to undergo 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 fresh certificate is as per the table below:

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

When current Signing Key is used for identification and authentication purposes, the life of the new certificate will not exceed beyond 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 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 RA or IDRBT CA as the case may be for the certificate revocation specifying the reason. RA should approve and forward the revocation request to the IDRBT CA. Where sufficiently reliable authentication of the revocation list is not possible, the IDRBT CA shall accept or reject the request

on a best possible judgment basis. If IDRBT CA is in doubt and cannot receive further information on whether to revoke or not, priority shall be given to the revocation. The certificate holder shall be informed that the certificate has been revoked and the reasons for revocation shall be presented. The IDRBT CA shall log all actions taken during a revocation process.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Communication among the CA, RA, and 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 up with appropriate algorithms and key sizes satisfies 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, need to submit DSC application form filled with identity details, address, photo, 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 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 CA trusted person for 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 or RA. The application forms for various types of certificates are available on the CA web site 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 the that information in certificate applications is accurate based on the attested 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 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 crypto medium is opted for the 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 link.

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 subscriber for downloading the certificate. The content of the certificate will be displayed to subscriber along with 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 pair in FIPS 140-2 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 time remaining in validity and other information as the old one, but a new, extended validity period and a new serial number. Certificates are renewed 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 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. Request 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 the normal scenario,

A Subject may request the renewal of its certificate.

A PKI Sponsor may request renewal of component certificate.

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

4.6.3 Processing Certificate Renewal Requests

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

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

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

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 certificate Re-Key option to subscribers.

4.7.1 Circumstance for Certificate Re-key

CA issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled for a certificate subjected 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 may request re-key of component certificate.

4.7.3 Processing Certificate Re-keying Requests

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

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

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

No Stipulation

4.9 Certificate Revocation and Suspension

CA authenticates the request for revocation prior to revocation. Subscribers are required to submit paper based revocation request 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 Circumstance 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. Private key is lost
6. Subscriber is not in a position to use certificate(Death – 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 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 subscriber about revocation of 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 best efforts to process revocation request so that it is posted in the next CRL unless a revocation request is received and approved within two hours of next CRL generation.

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

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

CA publishes CRLs not later than the next scheduled update.

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

In addition, CA issues CRLs and posts the CRL immediately if a certificate is revoked for the reason of 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 on-line certificate status checking. Client software using on-line certificate status checking need not obtain or process CRLs.

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

IDRBT CA provides an on line 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 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 implementation of CRLs and on-line revocation status, no other forms of on-line 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

Suspension will be permitted in the event that a user's token holding private key is temporarily unavailable to them.

4.9.14 Who can Request Suspension

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

4.9.15 Procedure for Suspension Request

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 shall be revoked for the reason of "Key Compromise".

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

4.10 Certificate Status Services

IDRBT CA provides an on line 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 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 mechanism to protect equipments 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 entry/exits are monitored either manually or electronically.
4. access logs are maintained and inspected periodically

5. Multiple layers of increasing security are provided in areas such as perimeter, building, and CA room
6. Two person physical access controls are required to 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 operation in the absence of commercial power, to support 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 only authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic exposure).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed in accordance with the manufacturer's guidance prior to disposal. Other waste is disposed of in accordance with the 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 that 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 shall 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 accuracy of information included in certificates;
3. Approving and executing the issuance of certificates, and;
4. Requesting, approving and executing the revocation of certificates.

5.2.1.3 Audit Administrator

The Audit Administrator is responsible for:

1. Reviewing, maintaining, and archiving audit logs;
2. Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with 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 Organisational Registration Authority

For organisational RA, the responsibilities are:

1. Verifying organisational identity of the applicant.
2. Entering applicants information, and verifying correctness;
3. Securely communicating requests and responses from/to the CA;

The roles of RAs engaged by CAs are limited only to the collection of DSC application form and supporting documents and facilitation of issuance of DSC to applicants.

5.2.1.6 PKI Sponsor

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

5.2.2 Number of Persons Required per Task

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

5.2.3 Identification and Authentication for Each Role

All personnel seeking to become trusted persons are required to be in the payroll of CA. Thorough background checks are carried out prior to 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 have achieved trusted status and approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities
- Issued electronic credentials to access and perform specific functions on 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 shall be selected on the basis of trustworthiness, and integrity, and shall be subject to background investigation. Personnel will be appointed to trusted roles (CA trusted roles) on the basis of:

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

5.3.2 Background Check Procedures

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

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

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

The background will be verified every three years.

5.3.3 Training Requirements

CA ensures that all personnel performing duties with respect to 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 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 and 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 either automatically collected or if not possible, a logbook, paper form, or other physical mechanism are used. All security audits logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2.

5.4.1 Types of Events Recorded

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

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

The following events shall be audited:

Auditable Event	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	

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

Auditable Event	CA
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	
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	

Auditable Event	CA
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	
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	

Auditable Event	CA
Resetting Operating System clock	

5.4.2 Frequency of Processing Audit Logs

Audit logs are examined for key security and operational events at least on a weekly basis. 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 recording of significant events in an audit log summary. It includes a verification that the log has not been tampered with, a brief inspection of all log entries, and a detailed investigation of any irregularities in the logs. Actions taken based on audit log reviews are recorded.

5.4.3 Retention Period for Audit Logs

See Section 2.

5.4.4 Protection of Audit Logs

System configuration and procedures are implemented together to ensure that:

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

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level. 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 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 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 a period of 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 other tampering, by storage within a trustworthy system. The media holding the archive data and the systems required to process the archive data are maintained to ensure that the archive data can be accessed for the time period

5.5.4 Archive Backup Procedures

CA creates back-up copies of archives compiled as and when the archives are created. Backup copies of the archive and copies of paper-based records are maintained in an off-site disaster recovery/ warehouse facility. 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 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 shall 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 digital certificate for a specified period of time. The subscribers generates 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 life times for certificates and associated private keys.

Key	2048 Bit Keys	
	Private Key	Certificate
Intermediate CA	10 years	10 years
Time Stamping	3 years	3 years
OCSP Responder	1 years	1 years
Human Subscriber Signature	2 years	2 years
Human Subscriber Encryption	2 years	2 years
SSL	2 years	2 years
Device/System	2 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 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 form of compromise, it will perform an investigation in order 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 shall be followed. Otherwise, the scope of potential damage shall be assessed in order 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 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 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 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 shall be notified at the earliest feasible time so that RCAI can revoke the CA certificate;

1. A CA key pair shall be generated by CA in accordance with procedures set forth in this applicable CPS;
2. New CA certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;

3. If the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e., not expired or revoked), the CA may re-issue (i.e., renew) those certificates with the not After date in the certificate as in original certificates; and
4. The CA shall 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 shall request that its certificates be revoked. The CA shall 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 prior to 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 which are followed and the same will be documented. The process is validated by an Auditor.

6.1.2 Private Key Delivery to Subscriber

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 a 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 deliver 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 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 in accordance with FIPS 186-2.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, 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 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 prior to 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. Numbers of backup copies are limited to three and securely stored under the same multi-person control as the operational key.

6.2.4.2 Backup of Subscriber Private Signature Key

The CA is never in possession of Subscribers 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 in secure manner and transferred in an encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

The user must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, Personal Identification Numbers (PINs) or biometrics. Entry of activation data is protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Methods of Deactivating Private Key

Cryptographic module that has been activated is never left unattended or otherwise available to unauthorized access. After use, cryptographic modules are deactivated. After deactivation, the use of the cryptographic modules based CA key pair requires the presence of the trusted roles with the activation data in order 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 key 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 in order 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 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 net 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 so as to reduce the likelihood that any particular component was tampered with..

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

3. The hardware and software are dedicated to performing the PKI activities. There are no other applications; hardware devices, network connections, or component software installed which 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 performing the PKI operations is 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 unauthorized modification to the CA software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system. The CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

CA employs appropriate security measures to ensure that they are guarded against 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) is 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 is accurate to within three minutes. Electronic or manual procedures are used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.1.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

Certificate profiles are 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 in accordance with 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 shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessments

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

8.2 Identity and Qualifications of Assessor

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

8.3 Assessor's Relationship to Assessed Entity

The auditor is independent from the entity being audited. 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

Office of CCA may determine that a CA is not complying with its obligations set forth in this CPS or the applicable CP. When such a determination is made, the office of CCA may suspend operation of CA, or may revoke the CA certificate, or may direct that other corrective actions be taken which allow 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 note the discrepancy;
2. The auditor notify the audited CA; and
3. The auditor notifies the office of CCA.

8.6 Communication of Results

On completion of audit by an empanelled auditor, Auditor submit an Audit Report, including identification of corrective measures taken or being taken by 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 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 payments 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 clearly marked or labeled as confidential, or by its nature reasonably is understood to be confidential, and treat such information with the same degree of care and security as the CA treats its own most confidential information.

9.4 Privacy of Personal Information

CA stores, process, and disclose personally identifiable information in accordance with the provisions of 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 claims all Intellectual Property Rights in and to the Certificates and revocation information that they issue. However, permission to reproduce and distribute Certificates and revocation information on a nonexclusive royalty-free, world-wide basis, may be granted provided that the recipient agrees to distribute them at no cost.

9.5.2 Property Rights in the CPS

This CPS is based on the proforma CPS published by Office of CCA for Licensed CAs and as amended from time-to-time. All Intellectual Property Rights in this CPS pertaining to 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 in accordance with provisions of IT Act, 2000 & Rules made thereunder that;

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

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

3. Only verified information appears in the certificate

9.6.2 Subscriber

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

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

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

1. Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
2. Check each certificate for validity, using procedures described in RFC 5280, prior to reliance;
3. Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and 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 set forth in this CPS.

9.8 Limitations of Liabilities

CA limit liabilities as long as CA meet the liability requirements stated in ITAct, 2000 and 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 in accordance with 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 shall not be liable for any indirect, exemplary, special, punitive, incidental, and 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 shall not be liable for any delay, default, failure, 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 Agreement. If the liability is not dealt 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 3	Indian Rupees One Lakh

9.9 Indemnities

Indemnification by Subscribers

To the extent permitted by applicable law, 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) that 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 the 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. The sections 5.5 and 9 of this CPS shall survive the termination or expiration of this CPS.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, 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 is made publicly available within seven days of approval.

9.12.3 Circumstances under Which OID Must be changed

CCA determines the requirement for changing the Certificate Policy OIDs.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among Licensed CAs and Customers

Unless the provision for dispute resolution under the 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 shall be resolved by CCA.

9.13.2 Alternate Dispute Resolution Provisions

No stipulations.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Waiver of Rights

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

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation.

10 BIBLIOGRAPHY

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

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

12 ANNEXURE-1

12.1 Authentication of organization user identity

The RA needs to verify that an entity belongs to the set of entities that the IDRBT CA recognizes as qualified to become an end user. A representative of an organization should come with a letter authorizing him/her to represent the organization for the given purpose.

The practices described in this section apply to all end entities making their initial application for a certificate and any subsequent application for a new certificate under this CPS. The identity verification process (if required) is to:

i) be attended by an end entity in person (based on the Class of Certificate)
ii) be conducted by an authorized Registration Authority or Superior Authority as the case may be.
iii) perform the following functions:
   a) The identity of the person performing the identity verification will be established from the Trusted Personnel List. The verification procedure pertaining to identity and background screening of the Trusted Personnel will be as per IDRBT policy.
   b) The applicant is required to affix the latest duly signed passport size photograph on the first page of the application form.
   c) The applicant is required to include the details of the unique identifying number from the photo identity document that was enclosed by the subscriber along with the application form.
   d) The application form should contain the declaration of identity signed by the applicant using a handwritten signature that should be duly certified by the Superior Authority of the Organization where the subscriber is employed.
   e) The date and time pertaining to the receipt of application and a signed declaration by the person verifying the identity of the applicant that he or she has verified the identity of the applicant will be recorded on the second page of the application form.
      - Physical Verification
      - Collection of Certificate information
      - Proof of other material certificate information like identification documents
   f) The inspection and approval of Physical DSC application form should be carried out by a trusted person of CA. Such approval should be clearly indicated on the physical DSC application form in the form of ink signature of trusted person of CA along with name, designation and date.

12.2 Certificate Application Information Verification and Communication

Certificate application information and the documents to be furnished along with the application include the items listed in the following Table.

In case of online certificate application, in order to avoid fake requests for certification, entities must physically visit the RA (if RA asked them to do so) with proof of identity they want to be certified and submit an application. RA must verify the credentials of the applicant/subscriber complying with the procedures for different Classes of Certificates mentioned in this CPS.

In case of Class 3 application, the applicant/subscriber should appear for personal verification before RA of the bank (if required) in which the applicant/ subscriber is employed.
The certificate application can be made by applicant/subscriber only and not by any other people.

Class	Information to be furnished in the application form contents	Documents to be furnished
Class 1	***Individuals:*** • Full Name • Residential Address • Official Address • Nationality • Email Address • Bank Account details • The PAN/AADHAR number of the applicant has to be furnished in the application form. In case PAN or AADHAR number not having been issued to a Digital Signature Certificate(DSC) applicant, CA shall issue DSC only after obtaining an undertaking from the DSC applicant stating the following: "I hereby declare that neither PAN nor AADHAR number has been issued to me".	

Class 3	***Individuals:*** Same as Class 1, in addition either of the following: • Passport Details • Voter's Identity Card • Income Tax PAN Number • Driving License • Employee Identification Card • The PAN/AADHAR number of the applicant has to be furnished in the application form. In case PAN or AADHAR number not having been issued to a Digital Signature Certificate(DSC) applicant, CA shall issue DSC only after obtaining an undertaking from the DSC applicant stating the following: "I hereby declare that neither PAN nor AADHAR number has been issued to me".	Original copies of any of the documents • Passport • Voter's ID • PAN Card • Driving License • Employee Identification Card issued by the Organisation (in case of employees of Banks/FIs) (to be furnished and physical presence before RA (if required) for personal verification) + Authorization letter from the higher authority of the subscriber who will be applying for Class 3 Certificate.
	SSL Certificate: Same as Class 3 Individuals (details of the authorized representative), plus The issuances of SSL certificate are limited only to .IN domain. The URL/server name/IP address to which the server authentication is needed. Verification of credentials of the bank/ financial institution The PAN/AADHAR number of the authorized representative of the bank/ financial institution has to be furnished in the application form In case PAN or AADHAR number not having been issued to a Digital Signature Certificate(DSC) applicant, CA shall issue DSC only after obtaining an undertaking from the DSC applicant stating the following: "I hereby declare that neither PAN nor AADHAR number has been issued to me". Balance sheet of the bank/ financial institution for the last financial year	Details of the domain registration along with proof. (Details of the domain registration to be furnished and physical presence before RA (if required) for personal verification) + Attested photo copy of PAN card of bank/ financial institution + PKCS#10 format Certificate Request generated from the Server + Authorization letter from the higher authority of the subscriber who will be applying for SSL Certificate on behalf of the bank/ financial institution.

	Code Signing: Same as Class 3 Individual (details of the authorized representative), plus • PAN number of the bank/ financial institution • Balance sheet of the bank/ financial institution for the last financial year • The PAN/AADHAR number of the authorized representative of the bank/ financial institution has to be furnished in the application form. In case PAN or AADHAR number not having been issued to a Digital Signature Certificate(DSC) applicant, CA shall issue DSC only after obtaining an undertaking from the DSC applicant stating the following: "I hereby declare that neither PAN nor AADHAR number has been issued to me".	Original copies of any of the documents • Passport • Voter's ID • PAN Card (to be furnished and physical presence before RA (if required) for personal verification) + Details of the bank/ financial institution + Authorization letter from the higher authority of the subscriber who will be applying for Code Signing Certificate on behalf of the bank/ financial institution.

	Document Signer Certificate Same as Class 3 Individual (details of the authorized representative), plus • Bank ID card of the Authorized Signatory / Bank Manager • Copy Bank PAN Card • Copy of Bank incorporation certificate or Banking License Certificate • Declaration by Subscriber as 1) I hereby declare and understand that Organizational Document Signer Certificate issued to us will be used only for automated signing of documents/information and will not be used in any other context including individual signature. 2) I hereby declare that necessary controls have been built in software applications to ensure that there is no misuse 3) I hereby declare and understand that the documents/messages authenticated using Organisational Document Signer Certificate issued to us is having organisational accountability.	Self-attested Bank ID card of the Authorized Signatory / Bank Manager + Bank PAN card attested by Superior Authority + Attested copy of Bank incorporation Certificate or Banking License Certificate + Authorization letter from the higher authority of the subscriber who will be applying for Document Signer Certificate on behalf of the bank + Declaration by Subscriber as 1) I hereby declare and understand that Organizational Document Signer Certificate issued to us will be used only for automated signing of documents/information and will not be used in any other context including individual signature. 2) I hereby declare that necessary controls have been built in software applications to ensure that there is no misuse 3) I hereby declare and understand that the documents/messages authenticated using Organisational Document Signer Certificate issued to us is having organisational accountability

Table: Identification documents required for Online Certificate Application

12.3 Email Verification:

E-mail verification is done by sending the OTP to subscriber to enable the submission of the Certificate Signing Request to CA system. This ensures that the subscriber, who has requested for the certificate, also has the control over the e-mail mentioned in the request form.

12.4 SSL Certificate:

Domain Name Validation:

Domain and E-mail validation are performed by the Registration Authority officials of Registration Authority offices of IDRBT CA. The Certifying Authority issues the digital

certificates only after validating/verifying the Distinguished Name Details such as Common Name, E-mail id, Organization, Organization Unit, Postal Code of the Locality, State and Country in online requests digitally signed and released by the Registration Authority Officials.

The issuance of SSL certificates by Licensed CAs are limited only to .IN domain. Only organizational persons are eligible to apply for SSL certificates on behalf of their organizations. The applicant (requestor) shall make an application to the CA in a digitally signed / physically signed application form. This shall contain the domain name(s) to be certified, the Certificate Signing Request (CSR) and the information of the requestor and the organization. This shall be accompanied with necessary supporting documents. The minimum set of documents to be submitted includes:

1 DSC Application Form
2 Applicant ID Proof
3 Authorization Letter by Organization Authorized Signatory
4 Authorized Signatory Proof
5 Proof of Organizational Existence

Verification of Subscriber

For issuance of SSL/TLS certificates, below verification shall be followed.

1. **Domain Name Verification:**

   a. Each value provisioned for subject alternative names (dnsNames) shall undergo domain name verification to prove the ownership / control of the domain by the requestor of the certificate.

   b. This shall be accomplished by

      i. Validating the request by communication to: webmaster@domainname.com,administrator@domainname.com,admin@domainname.com, hostmaster@domainname.com, postmaster@domainname.com, or any email ID listed in the technical, registrant, or administrative contact field of the domain's Registrar record;

   OR

      ii. Requiring a practical demonstration of domain control (Eg: making changes to DNS zone file or adding a unique file / filename on the domain under verification); This is achieved by CA sharing a unique Request Token or a Random Value, valid for a short duration, with the applicant and validating this data against the content of the file name provided or the DNS value (CNAME, TXT or CAA record) of the domain.

c. In case of wildcard domains, these shall undergo additional checks, to not to wrongly issue, for a domain listed in public suffix list (PSL). If the domain is listed in PSL, the application shall be refused, unless applicant proves ownership of entire domain namespace.

d. In case of IP Address, in place of domain name, it shall be verified to have the applicant's control over the IP, by means of (i) change in agreed information in an URL containing the IP address, OR (ii) IP assignment document of IANA or Regional Internet Registry, OR (iii) performing r-DNS lookup resulting in a domain name verified by above procedure

2. **Organization Person verification: The** verification of the identity & address of the applicant shall be made using, any one or more the following

a. Identity of the applicant shall be verified by obtaining a legible copy of employment ID and PAN card which noticeably shows the Applicant's face. The copy of the document shall be inspected for any indication of alteration or falsification. A video verification as per the procedure mentioned in section 2.4 (10) of Identity Verification Guidelines should be carried out by CA to ascertain the photo match of applicant with the photo presented in the identity proof & DSC application form. The PAN number should be electronically verified with income tax database for matching of name as submitted in the DSC application form.

b. The applicant should submit an authorization letter from the authorized signatory of the organization stating the authorization to apply for SSL certificate. The letter should contain name, photo, designation and address of the applicant. CA may ask additional documents for the confirmation of applicant's affiliation to organization.

c. Additional verification may be made by the CA the applicant's name & address for consistency with a website of the organization.

d. CA should confirm that the applicant is able to receive communication to organisational telephone and email.

3. **Organization Verification:**

a. The organization verification includes authorization proof to applicant and existence of organization.

b. Sufficient document evidence should be provided by the applicant for proof of authorized signatory.

c. Apart from the organizational person verification, the additional process documentation and authentication requirements for SSL certificate shall include the following:

- The organization owns the domain name, or the organization is given the exclusive right and authority to use the domain name
- Proof that the applicant has the authorization to apply for SSL certificate on behalf of the organization in the asserted capacity.(e.g. Authorization letter from organization to applicant)

(As per para 4.1 of "IDENTITY VERIFICATION GUIDELINES v1.9" dated: 05.09.2019).

Validation of Certificate Requests

a. After the receipt of the online certificate request, the RA shall perform all required validations as the precondition to certificate issuance.

The RA shall validate that

- The certificate applicant rightfully holds the private key corresponding to the public key listed in the certificate
- The certificate applicant/subscriber has agreed to the terms and conditions as stated in IDRBT CA CPS
- The certificate applicant mentioned in the application form is the person identified in the electronic request.
- The information listed in the certificate request is accurate
- Subscriber does not own a revoked certificate, and incase subscriber's certificate is revoked he should conduct investigation to determine whether it is necessary to suspend or revoke other Digital Certificates owned by that particular subscriber.

Individual Presence

The personal presence before the RA, is needed depending upon the class of certificate.
IDRBT CA will undergo Cross-certification with other operating CAs as per the Rules and Regulations to Certifying Authorities, by CCA, Ministry of Electronics & Information Technology.

Classes of Certificate

IDRBT CA supports two distinct certificate classes within its Certification services. IDRBT CA may introduce more classes than what has been specified herein if stipulated by the Controller of Certifying Authorities and this CPS shall be appropriately amended as and when such classes are introduced. Each class provides for designated level of trust. The following subsections describe each certificate class.

12.5 Document Signer Certificate

This section specifies the verification requirements for issuance of Document Signer Certificate. The certificate profile requirements shall be as per the Interoperability Guidelines for Digital Signature Certificates (CCA-IOG). The Key generation requirements for the Document Signer Certificate shall be as per X.509 Certificate Policy for India PKI (CCA-CP). The following direction is issued for strict Compliance:

1.	The applicant of Document Signer certificate shall be an organisational person of that organisation. The verification requirements for Document Signer Certificate shall be as per Section 2.3 of IVG ver 2.1
2.	The following declarations shall be obtained from subscriber 1. I hereby declare and understand that Organizational Document Signer Certificate issued to us will be used only for automated signing of documents/information and will not be used in any other context including individual signature. 2. I hereby declare that necessary controls have been built in software applications 3. I hereby declare and understand that the documents/messages authenticated using Organisational Document Signer Certificate issued to us is having organisational accountability.

(As per 3.2 of "IDENTITY VERIFICATION GUIDELINES v 2.1" dated 09.0.2022)

12.6 Class 1 Certificates

Description: Class 1 certificates are issued only to individuals. Class 1 certificates confirm that a user's name (or alias) and e-mail address form a distinct subject name within the IDRBT CA repository. Class 1 certificates are added to his/her set of available certificates in the directory services. They are used primarily for digital signature, to enhance the security of environment. Class 1 Encryption Certificates are used for e-mail purposes.

In case of online certificate request for Class 1 Certificate, the applicant/subscriber submits online as well as paper application form to the RA under IDRBT CA. RA verifies the name, e-mail address, organization and the postal address in the request. He has the right to reject the certificate request if he finds the application is not meeting the criteria. RA then digitally signs and sends to IDRBT CA for the issuance of the certificate.

Although IDRBT CA's Class 1 Certificate identification process is a method of authenticating a certificate applicant's identity, it does not require the applicant's personal appearance before the RA in case of online certificate application. Physical presence is not necessary but may be required at discretion of RA in case of online certificate application.

The validity period of Class 1 Certificates is one or two years as per choice of the subscriber.
The Class 1 Signing Certificate is intended to be used for Digital Signature and Class 1 Encryption Certificate is used for encrypting e-mails.

Class 1 Signing Certificates shall be Digital Certificates under IT Act, and the legal effect, conjecture and evidentiary value of Digital Certificates as provided in the IT Act will be applicable.

12.7 Class 3 Certificates

Description: Class 3 Certificates are issued to Individuals as well as Servers. Class 3 Certificates provide important assurances of the identity of individual subscribers by

requiring their personal (physical) appearance before an RA. All the personal details will be physically verified by the RA office and after confirmation of facts it will recommend the issuance of the certificate.

IDRBT CA is furnishing below various options to RAs to fulfil CCA guidelines with regard to Physical Verification of Class 3 DSC subscribers.

Option 1: The subscriber will present himself/herself at the respective Bank's RA office physically with required documents as stipulated in CA application form. The RA Officer has to performphysical verification of the subscriber and satisfy himself of the identification taking full responsibility and confirm the same in the application form.

Option 2: The video verification of subscriber should be carried out by RA in accordance with the guidelines specified under IVG and the recording must be preserved by CA office for seven years. On demand, the video recording must be shown to auditors during the audit. The subscriber should undergo video verification with respective RA with required documents for minimum 20 seconds using CA Video recording setup.

Option 3: The subscriber's superior authority should submit a letter stating that the subscriber is not able to appear physically/through VC before RA/CA office and that he has done physical verification of the subscriber and satisfied himself of the identification taking full responsibility.The letter should also be countersigned by the RA.

The RA bases the verification of applicant by one of the above options, application form and the certificate request. The Superior Authority and RA Official are solely responsible for identification of Subscriber and correctness of the documents.

For issuance of a Digital Certificate, the applicant/subscriber submits online as well as paper application form and the required documents to the RA. RA verifies the name, postal address, e-mail address and other particulars in the request. He has the right to reject the certificate request if he finds the application is not meeting the criteria. RA then digitally signs and submits to IDRBT CA for the issuance of the certificate online.

The private key corresponding to the public key contained in a Class 3 certificate must be generated and stored in a trustworthy manner according to applicable requirements.

If the organization wants to be a Registration Authority Office under IDRBT CA, the authorized representative of the organization must personally appear before the IDRBT CA office with the necessary documents mentioned above. The IDRBT CA will issue Class 3 Individual Certificate to RA Officials nominated by the Banks/Financial Institutions after verification. All RA certificates will be Class 3 Certificates.

Class 3 Certificates for Secure Server will help web servers to enable secure communications through the use of Secure Sockets Layer (SSL) technology. As a matter of practice, IDRBT CA issues Class 3 certificates to web servers. IDRBT CA Secure Server Certificate boosts the credibility and scope of website with today's strongest encryption available for secure communications. Along with the application form the authorized person must give the domain name or the Server IP address on which it needs the Certificate. The domain name must be registered and the proof must also be accompanied with the application. Class 3 certificates are issued either for one year validity period or two years validity period as per choice of the subscriber.

The Class 3 Certificate is intended to use for Digital Signature, Encryption of messages, Code signing and SSL.

Class 3 Signing Certificates shall be Digital Certificates under IT Act, and the legal effect, conjecture and evidentiary value of Digital Certificates as provided in the IT Act will be applicable.

From a functional standpoint there is no difference between a Class 1, Class2 and Class 3 Certificate, and the only difference is in the verification process used prior to issuing a Certificate.

Class 2 OID is included in the Certificate Policies field of Class 3 Certificate.

13 ANNEXURE II

13.1 Subscriber Application Form

IDRBT CA

APPLICATION FORM FOR DIGITAL CERTIFICATE

Important Notice:

- Subscriber agreement should be submitted along with this application form filled by the applicant.All subscribers are advised to read IDRBT CA Certification Practice Statement available at http://idrbtca.org.in/
- Copy of identification document of applicant (PAN or Aadhar and Employee ID card) attested by superior authority with seal should be attached along with the application form.
- Self-attested copy of identification document of superior authority (PAN and Emp. ID) should be attached along with this application form.
- Application form must be submitted to the Registration Authority/IDRBT CA for face-to-face verification in case of Class 3 Certificate.
- Incomplete/Inconsistent application is liable to be rejected.
- Section 71 of IT Act stipulates that if anyone makes a misrepresentation or suppresses any material fact from the CCA or CA for obtaining any DSC such person shall be punishable with imprisonment up to 2 years or with fine up to one lakh rupees or withboth.
- *Fields are mandatory. Strike off which are not applicable.

Paste your self-attested recent passport size photograph and sign across the photo

Name of the Organization*			
Bank in which subscriber has account			
New / Renewal	**User- ID (in case of Renewal)**		**Validity** 1 Year ☐ 2 Years ☐

Class *:	Certificate for *:	Application*:	Applicant Type*:	Type of Digital Certificate*:
Class 1 ☐	Individual ☐	SFMS ☐	Bank Employee/Officer ☐	Signing ☐
Class 3 ☐	Server (System) ☐	NGRTGS ☐	RA Official ☐	Encryption ☐
	Web Server (SSL) ☐	CTS ☐		System ☐
	Doc. Signer ☐	Others		Web Server (SSL) ☐
		(Please specify)		Code Signing ☐
				Doc. Signer ☐

PERSONAL DETAILS

Name*:		**Sex*:**	Male / Female
Email Address*:			
Address for communication*:			
	Pin code*:	**Telephone:**	**Mobile No*:**
Date of Birth*:		*(dd/mm/yyyy) For Ex: 10th May, 1975 is 10051975*	
Identification Details*	**Aadhaar No:**	**PAN No*:**	
Bank details:	*Bank & Branch Name*		
	Bank Branch Address		
	Bank Account No.	*Type of Bank Account SB* ☐ *CA* ☐	

CERTIFICATE REQUEST DETAILS

The following details will be reflected in the certificate.
Make sure that these details match with those given to generate request using certificate request generation tool or any other PKCS #10 request generation tool.
If necessary, contact your application provider for these details before filling the form.

Common Name* *(Name of the person, Server Name, Registered domain name, IFSC Code etc)*	
E-Mail* *(Valid email address to which the communication be made)*	
Organization* *(Name of the organization eg: IDRBT)*	
Organization Unit* *(Name of the department eg: Certifying Authority)*	
City/Locality* *(Name of the city/town eg: Hyderabad)*	
State/Union Territory* *(Name of State/UT eg: Telangana)*	
Pin Code*	
Country*	**India**

Signature of the Superior Authority -1- **Signature of the Applicant**

DECLARATION AND UNDERTAKING BY THE APPLICANT

All the above information provided by me is true to the best of my knowledge and belief. I agree to use only FIPS 140-1/2 Level 2 validated cryptographic modules for key generation and storage. I accept the responsibility for the safety and integrity of the private key by controlling the access to the computer/device containing the same, so that it is not compromised and I will immediately notify my RA/ IDRBT CA in event of key compromise. I agree to download the certificate within 30 days from the date of issue, failing which the certificate will be revoked automatically. I also agree to publish the Digital Certificate in the IDRBT CA repository and will report IDRBT CA of any error or defect in the certificate and change in the above information.

Date:

Place:

Name of the Applicant: Signature of the Applicant

FOR SUPERIOR AUTHORITY/BRANCH MANAGER OF APPLICANT*

This is to certify that Mr/Ms .....has provided correct information in the "Application Form for Digital Certificate" to the best of my knowledge and belief. I hereby authorize him/her, to apply for obtaining Digital Certificate from IDRBT CA for the purpose specified above.

Have done physical verification of the subscriber and take responsibility of identification.

Date:

Place:

Name of the Officer:

Official Email: (Signature)

Phone No: (Official Seal)

DECLARATION AND UNDERTAKING BY RA OFFICIALS APPLYING FOR NEW/RENEWAL CERTIFICATE*

The Applicant who is an authorized official, for and on behalf of .....Submits this application to act as RA Administrator/Officer

1. Agrees to accept responsibility for the safety and integrity of the private key so that it is not compromised.
2. Agrees to use only FIPS 140-1/2 Level 2 validated cryptographic modules for key generation and storage of keys.
3. Agrees to immediately notify IDRBT CA, in the event of compromise or any reasonable suspicion of compromise of his/her private key / Digital Signature Certificate.
4. Agrees to use keys & Digital Signature Certificate strictly for authorized purpose viz. to discharge the functions as Registration Authority only.
5. Acknowledges that for wrongful utilization of the Digital Certificates, the applicant shall be liable under the Information Technology Act, 2000 or/and any other relevant law(s) of the land.
6. Acknowledges that in submitting this application, he/she is consenting to certificate issuance in the event the application is accepted.
7. Agrees to publish the public key and certificate in the IDRBT CA directory Services.
8. Agrees to use certificates in accordance with the purpose for which they are issued.
9. Agrees to prove possession of private keys and establishing the right to use in case of necessity.
10. Agrees to report to IDRBT CA any error or defect in the certificates immediately or of any subsequent changes in the certificate information.
11. Agrees to exercise due diligence and sensible judgment before deciding to rely on a digital signature, including whether to check on the status of the relevant certificate.
12. Agrees to renew the certificate(s) as and when required to do so.

All the information provided by me above is true to the best of my knowledge and belief and the documents of which details are furnished are valid and not expired. I undertake to promptly notify the IDRBTCA in the event of any change in the information contained herein above. I am submitting this application as an authorized person for carrying out only authorized functions as RA by using the Digital Certificate in the discharge of my official duties. I shall not use the Digital Certificate for any other purpose except the aforesaid purposes.

Date:

Place:

Name of the RA Official: Signature of the RA Official

FOR RA PURPOSE ONLY

Checklist	Date & Time	Initials
Received the application form for digital certificate		
Physical Verification(in person/VC/Certified by SA or RA)		
Verified the identification documents(Aadhar card/PAN Card/ Passport /Domain registration)		
Collected the PKCS#10 request for Secure Web Server Certificate		
Creation of user ID		
Request from Subscriber with Request Number.		
Processing		

CONTACT ADDRESS

IDRBT Certifying Authority,
Road No. 1, Castle Hills, Masab Tank, Hyderabad – 500 057, India.
Phone: +91 40 23294217/19/21/23 /Fax: +91 40 23535157
Email: cahelp@idrbt.ac.in
Website: http://idrbtca.org.in

13.2 Certificate Revocation/Suspension/Activation Form

CERTIFICATE REVOCATION/SUSPENSION/ACTIVATION REQUEST FORM
Certificate Revocation / Certificate Suspension / Certificate Activation
Important Notice: • * Fields are mandatory • Strike off which are not applicable • This application form is to be filled by the applicant. • Fill this application form and send it to IDRBT CA in person or fax or post. • Request from authorized third party must be accompanied with an authorized letter from the certificate owner and the third party's identification document like Passport/Voter's ID/PAN Card/Driving License

CERTIFICATE DETAILS	
Certificate Serial Number*:	
Certificate Type*:	**Signing / Encryption / SSL / Code Signing**
Common Name in the Certificate*	

CERTIFICATE OWNER DETAILS	
Name of Certificate Owner *	
E-Mail*	

REASON	
Reason for Revocation / Suspension / Activation* Note: ▪ *Check **"Certificate Hold"** for suspension request* ▪ *Check "**Remove from Certificate Revocation List**" for activation request* ▪ *Check **"Unspecified or Key Compromise or Affiliation Changed or Superseded or Cessation of Operation"** for revocation request.*	☐ Unspecified ☐ Key Compromise ☐ Affiliation Changed ☐ Superseded ☐ Cessation of Operation ☐ Certificate Hold ☐ Remove from Certificate Revocation List
Details* *(Give a brief explanation about the reason for revocation/suspension/activation)*	

AUTHORIZATION		
Authorized by *	**Certificate Owner / Third Party / SA / RA**	
Name*:	**Signature***	**Date*:**
Contact Phone No:	**E-mail:**	

FOR RA/ IDRBT CA PURPOSE ONLY			
Checklist	**Date**	**Time**	**Initials**

Received the request form? (person/fax/post)			
Received identification document of third party, if any?			

CONTACT ADDRESS
IDRBT Certifying Authority, Road No. 1, Castle Hills, Masab Tank, Hyderabad – 500 057, India. Phone: +91 40 23294217/19/21/23 /Fax: +91 40 23535157 Email: cahelp@idrbt.ac.in Website: http://idrbtca.org.in

13.3 Subscriber Agreement (sample)

The purpose of this agreement is to establish the contractual relationship between IDRBT Certifying Authority and a Subscriber. The issue and subsequent use of public keys and Certificates issued, constitutes acceptance of this agreement, the terms and conditions of the IDRBT CA Certification Policy Statement ("IDRBT CA CPS") associated with the keys and Certificates issued to the Subscriber. The IDRBT CA CPS is amended from time to time, and is published on the INFINET in IDRBT CA's repository at https://idrbtca.org.in/repository.html and https://idrbtca.org.in/cps.html and is available via E-mail from: cahelp@idrbt.ac.in.

Important Notice:

THE SUBSCRIBER MUST READ THIS SUBSCRIBER AGREEMENT BEFORE APPLYING FOR, ACCEPTING, OR USING A DIGITAL CERTIFICATE FROM IDRBT CA. IF THE SUBSCRIBER DO NOT AGREE TO THE TERMS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE DIGITAL CERTIFICATE.

THE SUBSCRIBER AGREES TO USE THE DIGITAL CERTIFICATE AND ANY RELATED IDRBT CA CERTIFICATION SERVICES ONLY IN ACCORDANCE WITH THE IDRBT CA CPS.

Indemnity

The Subscriber agrees to:

1. accept responsibility for the safety and integrity of private keys, in the event that keys or Certificates are compromised the Subscriber will immediately notify the Registration Authority under IDRBT CA, as well as any other users with whom you exchange information;
2. indemnify IDRBT CA for any loss to any person or Organization arising from the failure to ensure the safety and integrity of your private keys and Digital Certificates;
3. indemnify and hold harmless IDRBT CA from any and all damages and losses arising out of
   a) use of an IDRBT CA issued Digital Certificate in a manner not authorized by IDRBT CA;

b) tampering with the Digital Certificate; or

c) any misrepresentations made during the application and use of the Digital Certificate.

4. assure and hold harmless IDRBT CA from and against any and all damages (including legal fees) of lawsuits, claims or actions by third-parties relying on or otherwise using a Certificate relating to:

   a) Subscriber's breach of its obligations under this agreement;

   b) Subscriber's failure to protect its Private Keys;

   c) Claims arising from content or other information or data supplied by Subscriber; or

Use of Keys and Certificates

The subscriber agrees that:

1. true complete and accurate information has been provided in applying for these keys and Certificates, and further undertakes to promptly notify the Registration Authority in the event that this information changes;
2. he/she is solely responsible for the protection of its Private Key;
3. to immediately inform the Registration Authority under IDRBT CA if it is known or suspected that a private key or a Certificate has or may have been compromised;
4. the use of the public keys and Digital Certificates are at their sole risk;
5. to use Keys and Digital Certificates strictly for lawful purposes and will not infringe a third party's rights; and
6. no implied or express warranties are given by the Registration Authority in relation to the Keys or the Digital Certificates and all statutory warranties are to the fullest extent permitted by law specifically excluded.
7. in case of SSL Certificate, he/she is solely responsible for the generation of server public and private key pair, Server Certificate Signing Request file in PKCS#10 format and protection of server's Private Key;

Others

1. The use of the private key and/or its associated Digital Certificate constitutes acceptance of the terms of the IDRBT CA CPS.

2. In no event shall IDRBT CA be liable to subscriber or any third-party relying upon or otherwise making use of the IDRBT CA certificate for any indirect, special, punitive, incidental or consequential damages even if IDRBT CA has been advised of the likelihood of such damages in advance.
3. 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 system, where breakdown may lead directly to death, personal injury or severe environmental damage.
4. Erroneous utilization of the Digital Certificates or violation to the practices specified in IDRBT CA CPS shall be liable to be proceeded against, both under the relevant civil and criminal laws, and shall be subject to punishment under the Information Technology Act, 2000 or/and 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.
5. IDRBT CA disclaims all warranties, except as expressly provided in the IDRBT CA CPS. IDRBT CA makes no representations or warranties, express, implied or otherwise relating to IDRBT CA Digital Certificate or any services provided by IDRBT CA in connection therewith, including without limitation any warranty of non-infringement, merchantability or fitness for a particular purpose.

Subscriber Obligations

End Entities discharge their obligations under IDRBT CA CPS by:

- Request the issue, renewal and if, necessary revocation of their certificates.
- Generating the key pair (except in the case of Encryption Certificate) on a secure medium as per CCA guidelines.
- Provide the Registration Authority true and correct information at all times and provide sufficient proof of material certificate information to meet user registration or certificate renewal requirements.
- Acknowledge that in making a certificate application, they are consenting to certificate issue in the event the application is issued.
- Ensure the safety and integrity of their private keys, including:
    - controlling access to the computer containing their private keys.

- protecting the access control mechanism used to access their private keys.

- Agree to publish the public keys and certificates in the IDRBT CA directory services.
- Use certificates in accordance with the purpose for which they are issued.
- Prove possession of private keys and establishing their right to use.
- Sign a subscriber agreement.
- Report their Registration Authority of any error or defect in their certificates immediately or of any subsequent changes in the certificate information.
- Study IDRBT CA CPS before using their Certificates.
- Inform the Registration Authority immediately by a paper document, if a key pair is compromised, and should seek immediate acknowledgement for the same.
- Exercise due diligence and sensible judgment before deciding to rely on a digital signature, including whether to check on the status of the relevant certificate.
- Renew their certificate on their own, if required.

The Subscriber demonstrates his/her knowledge and acceptance of the terms of this subscriber agreement by either (i) submitting an application for a Digital Certificate to IDRBT CA, or (ii) using the Digital Certificate issued by IDRBT CA, whichever occurs first.

Declaration by the Subscriber

I, hereby declare that I have read and understood the IDRBT CA CPS and the terms and conditions of this Subscriber Agreement. I shall abide with IDRBT CA CPS and the terms and conditions of this Subscriber Agreement.

Date:

Place: *Subscriber's Signature*

Name of the Subscriber:

13.4 Relying Party Agreement

THE RELYING PARTY MUST READ THIS RELYING PARTY AGREEMENT BEFORE VALIDATING A IDRBT CA TRUST DIGITAL CERTIFICATE OR USING IDRBT CA'S DATABASE OF CERTIFICATE REVOCATIONS AND OTHER INFORMATION ("REPOSITORY") OR ANY CERTIFICATE REVOCATION LIST ISSUED BY IDRBT CA. IF THE RELYING PARTY DO NOT AGREE TO THE TERMS OF THIS RELYING PARTY AGREEMENT, HE/SHE ARE NOT AUTHORIZED TO USE IDRBT CA'S REPOSITORY OR ANY CRL.

THIS RELYING PARTY AGREEMENT becomes effective when the Relying Party submit a query to search for a Digital Certificate, or to verify a digital signature created with a private key corresponding to a public key contained in a Digital Certificate, or when you otherwise use or rely upon any information or services provided by IDRBT CA's Repository, IDRBT CA's website, or any CRL.

1. The Relying Party acknowledges that he/she has access to sufficient information to ensure that he/she can make an informed decision as to the extent to which you will choose to rely on the information in a Digital Certificate. For more information, see the resources contained in IDRBT CA's website at https://idrbtca.org.in/. THE RELYING PARTY IS RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A DIGITAL CERTIFICATE. The Relying Party acknowledge and agree that his/her use of IDRBT CA's Repository and Directory Services, his/her use of any CRL of IDRBT CA, and his/her reliance on any Digital Certificate shall be governed by IDRBT CA's Certification Practice Statement (IDRBT CA CPS) as amended from time to time, which is included by reference into this Agreement. The IDRBT CA CPS is published on the INFINET in the Repository at https://idrbtca.org.in/repository.html and https://idrbtca.org.in/cps.html and is available via E-mail by sending a request to: cahelp@idrbt.ac.in Amendments to the IDRBT CA CPS are also posted in IDRBT CA's Repository at https://idrbtca.org.in/repository.html. The steps necessary to validate a Digital Certificate and verify a Digital Signature are contained in the IDRBT CA CPS. The IDRBT CA CPS permits you to use a CRL issued by IDRBT CA solely in connection with the reliance upon a Digital Certificate.

2. Except as permitted in this Agreement, the Relying Party shall not download, access, copy, or use any CRL issued by IDRBT CA. In any event, the Relying Party shall not sell, rent, lease, transfer, assign, or sublicense any CRL issued by IDRBT CA, in whole or in part, to anyone; shall not use or permit the use of the CRL by or on behalf of any other person or entity; and shall not modify or create a derivative work of any CRL issued by IDRBT CA. Without limiting the generality of the foregoing:

   (a) the Relying Party shall not create a compilation or aggregation of information based on any information from CRL issued by IDRBT CA, and he/she shall not use any software that creates any such compilation or aggregation; and

   (b) the Relying Party shall not use any information in any CRL issued by IDRBT CA, directly or indirectly, to provide or offer to provide Certificate status checking products and/or services to anyone outside your organization.

3. For purposes of this agreement, "Subscriber" shall mean a person who is the subject of and has been issued an IDRBT CA Digital Certificate.

4. The limited warranties, the disclaimers of warranty, and limitations of liability are according to the section 2.2 of IDRBT CA CPS.

Section 2.2 of the IDRBT CA CPS sets forth a limited warranty. Except as expressly provided in there, IDRBT CA disclaim all warranties and obligations of every type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of the information provided, and further disclaim any and all liability for negligence or lack of reasonable care.

In no event shall IDRBT CA be liable for any indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, performance, nonperformance, or unavailability of digital certificates, digital signatures, or any other transactions or services offered or contemplated herein, even if IDRBT CA, have been advised of the possibility of such damages.

The combined aggregate liability of IDRBT CA to any and all persons concerning a specific digital certificate shall be limited to an amount not to exceed the following, for the aggregate of all digital signatures and transactions related to such certificate as shown in Table 5 below:

Class	Liability Caps/per Certificate
Class 1	Indian Rupees Ten Thousand
Class 3	Indian Rupees One Lakh

Table 5: Liability Caps.

The Relying Party demonstrate his/her knowledge and acceptance of the terms of this Relying Party Agreement by submitting a query to search for, or to verify the revocation status of, a Digital Certificate, by downloading a CRL issued by IDRBT CA or verifying the revocation status of a Digital Certificate using such CRL issued by IDRBT CA, or by otherwise using or relying upon any information or services provided by IDRBT CA's Repository or website. If the Relying Party do not agree, do not submit a query and do not download, access, or use any CRL issued by IDRBT CA.

14 ANNEXURE III

14.1 CA Representations and Warranties (Additional)

Certificate owners are:

- informed through this CPS of their duties and obligations to ensure the safety, protection and integrity of their private keys;
- required for specific classes of certificates to enter into an agreement that clearly defines these obligations;
- advised/ asked not to interfere with or damage, or attempt to interfere with or damage, or reverse engineer the operational infrastructure of the IDRBT CA PKI or any component thereof. The IDRBT CA PKI has:
  - been structured and is operated in such a manner as to minimize the risk of compromise or willful damage by a Certificate owner;
  - defined a security policy that provides for the early detection of an attempt to damage the infrastructure and to collect sufficient evidence for a prosecution.

CA

The IDRBT CA discharges its obligations under this CPS by:

- Acting in accordance with the law prevailing in the country to provide operational infrastructure, certification services and publishing directory services over network.
- Approve the policies and certificate practice statement and enforcing the practices specified in this CPS.
- Generate its Signing key pair and protect the private key from compromise.
- Submit its public keys to the CCA before the commencement of operation.
- Receive a license from CCA to operate as CA.
- Publish its Public Key Certificate in the Directory server and in website.
- Appoint Registration Authorities, executing an operating Master Agreement and approve the RAs to be established below in the hierarchy
- Issue certificates to RAs on the receipt of signed requests and the physical presence (if necessary/required) before IDRBT CA.
- Delegate responsibilities to RA to be used in the authentication process.

- Execute the CA services in accordance with this CPS and documented operational procedures.
- Accept certification requests from entities through RA within the naming domain managed by the IDRBT CA.
- Advise the naming conventions.
- Issue certificates that are factually correct for the information known at the time of issue and are free from data entry errors, information given by subscriber without any change by RA or CA which will comply with X.509v3 standards based on authenticated entities' requests.
- Publish subscribers' Public Key Certificate without alteration in the LDAP directory after he/she accepts the certificate
- Provide access to relying parties to repository of public key certificates.
- Handle certificate revocation requests and certificate revocation.
- Revoke certificates if requested by the end entity or when deemed necessary because of compromise or suspected compromise.
- Inform subscribers if IDRBT CA initiates a certificate revocation process.
- Communicate to subscriber when the certificate is revoked or suspended.
- Update revoked certificates and publishes CRL in directory server.
- Periodically post the CRL and in emergency publishing it immediately.
- Maintain a list of compromised/revoked certificates and compromised users with all the details.
- Keep the entire information of Subscriber and other information that should be kept confidential secured and confidential.
- Collect and keep relevant documents for the corresponding certificates from applicant/subscriber
- Conduct internal security audits.
- Conduct compliance audit as required by CCA.
- Submission of Digital Certificates/CRL to the CCA for publication in National Repository.
- Assist in all respects, pertaining to IT Act 2000 for the audits conducted by CCA to validate the renewal of license.

RA

The Registration Authorities operating under the IDRBT CA hierarchy discharge their obligations under this CPS by:

- Enforcing practices described in this CPS.
- Submitting their public keys in the form of digitally signed certification requests to IDRBT CA Office.
- Accept a request for certificate from an end entity.
- Verify the integrity and possession of, and establishing the End Entity's right to use, user generated keys presented for certification.
- Advise End Entities of their obligations under this CPS, and provide information to them how these documents can be accessed.
- Confirm that an applicant's name does not appear in their list of compromised users.
- Submit Certificate requests that are free from data entry errors and that comply with PKCS standards.
- Check for trademark infringement by the end entity if any before forwarding certificate requests to IDRBT CA
- Verify identity of individual and organization identity before forwarding certificate requests to IDRBT CA.
- Meet the requirements mentioned in this CPS for approved subscriber certificate requests.
- Initiate investigation to determine whether to revoke or suspend subscriber's other certificate(s), in case one of his certificates is revoked.
- Approve an online certificate application of end entity and forward to IDRBT CA.
- Authenticate requests from the end entities for the revocation of their certificates and send revocation requests to the IDRBT CA.
- Inform IDRBT CA if its certificate is compromised.
- May notify the end entities regarding the expiry of certificates in advance before the expiry period.
- Maintain a list of compromised keys and compromised users.
- Verify with the list of compromised users before he approves a certificate request.

- Collect the relevant document for the corresponding certificates from applicants/subscribers.
- Keep such registration records as may be required.
- Creating and maintaining an accurate audit trail of all RA operations.
- Keep the entire information of Subscriber and other information that should be kept confidential , secure and confidential and disclosing it only when IDRBT CA instructs to do so.

Superior Authority responsibilities

The Superior Authorities' responsibilities include:

- Accept a certificate request from an end entity.
- Collect and verify the relevant documents for the corresponding certificates from applicants/subscribers.
- Digitally sign the certificate request of applicant/subscriber
- Send the application forms and the certificate requests to IDRBT CA/ RA for issuance.
- Maintain the audit trail of the verification process.
- Not to retain any information related to applicant/subscriber's certificate application
- Verify identity of Subscriber.

14.2 Subscriber

Subscriber discharge their obligations under this CPS by:

- Request the issue, renewal and if necessary, revocation of their certificates.
- Generating the key pair (except in the case of Encryption Certificate) on a secure medium as per CCA guidelines.
- Provide the RA or SA as the case may be, true and correct information at all times and provide sufficient proof of material certificate information to meet user registration or certificate renewal requirements.
- Acknowledge that in making a certificate application, they are consenting to certificate issue in the event the application is issued.

- Agree to publish the public keys and certificates in the IDRBT CA directory services by accepting the certificate.
- Use certificates in accordance with the purpose for which they are issued.
- Study this CPS before using their Certificates.
- Exercise due diligence and sensible judgment before deciding to rely on a digital signature, including whether to check on the status of the relevant certificate.
- Initiate an online request to get a new certificate on their own after expiry, if required.