IDRBT CA CPS

IDRBT CA CERTIFICATION PRACTICE STATEMENT

IN SUPPORT OF IDRBT CA'S CERTIFICATION SERVICES

VERSION 3.2
(IDRBTCA/DOC/CPS/3.2)

DATE OF PUBLICATION: JANUARY 28, 2013

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 23294217/19/21
FAX: +91 40 23535157
EMAIL: cahelp@idrbt.ac.in

IDRBT CA CERTIFICATION PRACTICE STATEMENT

Document Name	IDRBTCA/DOC/CPS/3.2
Release	Version 3.2
Status	Release
Issue Date	January 28, 2013

Amendment Certificate

RELEASE				
Version No.	**Description**	**Approved by**	**Approval date**	**CCA approved date**
IDRBTCA/DOC/CPS/1.0	Final Draft (not released)	PAC	01/01/2004	NA
IDRBTCA/DOC/CPS/2.0	First release	-do-	10/05/2002	22/07/2002
IDRBTCA/DOC/CPS/2.1	Update on version 2.0 (not released) • Updated section on Classes of certificates • Updated section on CRL issuance frequency	-do-	16/10/2002	NA
IDRBTCA/DOC/CPS/3.0	Update on version 2.1 (not released) • Includes changes and comments incorporated from half yearly and yearly CCA audit • Updated section on policy authorities • Updated sections to incorporate trademark infringement • Updated sections to add information on Client Certificate • Updated sections to include procedures for handling offline certificate requests • Removed sections on certificate renewal • Included Superior Authority under Registration Authority • Updated section on CRL issuance frequency • Updated sections on Certificate and CRL profile	-do-	01/03/2004	NA
IDRBTCA/DOC/CPS/3.1	Update on version 3.0 (Release) • Redefined the responsibilities of Superior Authority • Added more obligations for CA and RA • Updated section 2.5.3 regarding certificate revocation fees • Updated section 2.10 to include offline certificate application • Update section 4.1.2 to include identification for offline subscribers • Updated section 4.6 regarding procedures for certificate suspension and revocation	-do-	02/09/2004	25/10/2004
IDRBTCA/DOC/CPS/3.2	Update on version 3.1 (Release) • Inclusion of Validity period of one or two years for Class 2 certificates in Section 2.11.2- Classes of Certificates • Inclusion of System Certificate in Section 2.12.3 - Types of Certificates • Details of identity verification in Section 3.1.2 • Change in Section 3.2.1 & 3.2.2 as per the Interoperability guidelines. • Email and Domain name validation in Section 4.1.2 • Change of key size from 1024 bits to 2048 bits of the subscriber in Section 6.1.5 • Change in Algorithm from SHA-l to SHA-2 in Algorithm Identifier in Section 7.1.3 • Change in format of application form to include system certificate and validity period in Section 9.1	-do-	03/12/2012	21/01/2013

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 being 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 the IDRBT CA CPS. The definitions are provided in alphabetical order.

- "Act" means the Information Technology Act, 2000
- "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network
- "affixing Digital Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Digital Signature
- "applicant" or "user" means a person, entity, or organization that has applied for, but has not yet been issued with a Digital Certificate by IDRBT CA.
- "auditor" means any internationally accredited computer security professional or agency appointed by the Certifying Authority and recognized by the Controller of Certifying Authorities for conducting technical audit of Certifying Authority operations.
- "CA" refers to the Certifying Authority licenced by the Controller of Certifying Authorities.
- "Controller" means Controller of Certifying Authorities appointed under subsection (1) of Section 17 of the Act
- "Compromise" means a violation (or suspected violation) of a security policy, in which an unauthorized disclosure of or loss of control over sensitive information may have occurred.
- "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and

includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network

- "computer resource" means computer, computer system, computer network, data, computer data base or software
- “CPS” means the IDRBT CA Certification Practice Statement
- "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer
- "Digital Signature" means authentication of any electronic record by a Subscriber by means of an electronic method or procedure
- “Digital Certificate” means Digital Certificate issued by IDRBT Certifying Authority
- “End Entity” or “Entity” refers to either applicant or subscriber of Digital Certificate issued by IDRBT CA
- “INFINET” (INdian FInancial NETwork) is the communication backbone for the Indian banking and financial sector. It is a Closed User Group (CUG) consisting of all Public Sector, Private Sector, Foreign, Cooperative Banks, and Premier financial institutions in India.
- “information asset” means all information resources utilized in the course of any organization's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks)

- "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a Digital Signature created by the private key
- “licence” means a licence granted to Certifying Authorities for the issue of Digital Certificates under the IT Act, 2000
- “licenced CA” refers to a Certifying Authority who has been granted a licence by the Controller of Certifying Authorities to issue Digital Certificates
- “online certificate application” or “online certificate request” is the certificate request generated in PKCS#10 format and submitted online to IDRBT CA or its Registration Authorities using web-based application.
- "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 Certificate
- “person” shall include an individual or a company or an association or body of individuals, whether incorporated or not, or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments
- “Registration Authority” or “RA” means an entity trusted under IDRBT CA hierarchy and has the right to verify the credentials of the applicant/subscriber before putting (affixing) his digital signature and forwarding it to IDRBT CA for issuance of certificate.
- "Subscriber" means a person, entity, or an organization that has been issued a Digital Certificate by IDRBT CA.
- “Subscriber identity verification method” means the method used to verify and authenticate the identity of a Subscriber
- “Superior Authority” or “SA” means an entity who is a bank officer where the applicant/subscriber is having an account and having a valid digital certificate issued by IDRBT CA and who verifies the credentials of applicant/subscriber

before putting his digital signature and forwarding it to IDRBT CA for issuance of certificate.

- "suspect of compromise" means any compromise of the digital certificate or private key of a user reported explicitly to the IDRBT CA within a reasonable period of time.
- "trusted person" means any person who has:
    - direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Rules in respect of a Certifying Authority
    - or 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 licenced Certifying Authority), creation of private keys
    - or administration of a Certifying Authority's computing facilities
- "unverified information" means any information in a digital certificate which is not expressly/explicitly verified by IDRBT CA as per the IDRBT CA CPS, CA's Master Agreement.
- "verification of credentials" means the checking of the identification and supporting documents of applicant/subscriber by the SA or RA as mentioned in the appropriate sections of this document before applying his digital signature on the certificate request.
- "verify" in relation to a Digital Signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether:
    - The initial electronic record was affixed with the Digital Signature by the use of private key corresponding to the public key of the Subscriber
    - The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the Digital Signature.

Note: Words and expressions used herein and not defined shall have the meaning respectively assigned to them in that context.

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, licenced 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 2 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.

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

http://idrbtca.org.in/

or contact

cahelp@idrbt.ac.in

LIST OF ACRONYMS AND ABBREVIATIONS

CA	Certifying Authority
CCA	Controller of Certifying Authorities
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IDRBT	Institute for Development and Research in Banking Technology
INFINET	INdian FInancial NETwork
ISO	International Organization for Standardization
IT ACT	The Information Technology Act, 2000
LDAP	Light weight Directory Access Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RAID	Redundant Arrays of Inexpensive Disks
RFC	Request for comment
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman
SA	Superior Authority
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
VSAT	Very Small Aperture Terminal
X.509	The ITU-T standard for certificates and their corresponding authentication framework

CONTENTS

1. INTRODUCTION

1.1. 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 is the licenced CA for INFINET having obtained the licence for operation from the Controller of Certifying Authorities (CCA), Ministry of Communication and Information Technology, Government of India. IDRBT offers Certification Services primarily for the members of the INFINET (the membership of the INFINET is accorded by the Reserve Bank of India).

More information occurs in the website: http://idrbtca.org.in/

1.1.1. Overview

IDRBT CA Certification Services are designed to support secure electronic transactions as well as for digital signatures and other general security requirements of subscribers. To achieve this, IDRBT CA functions as a Trusted Third Party (TTP), licenced by CCA, issuing, managing, renewing and revoking certificates in accordance with published Certification Practice Statement.

The services offered by IDRBT CA include the following:

- Handling Certificate Request
- Certificate Issuance
- Certificate Publication

- Certificate Suspension
- Certificate Activation (in case of suspended certificates)
- Certificate Revocation
- Certificate Revocation List (CRL) Management

As such IDRBT CA CPS defines the high level policies and practices of IDRBT CA. There are a large number of practices, which support the CPS, and these are documented in a set of procedure manuals, defined in Document Master List (Section 9.4 of Appendix). These manuals, unless specified explicitly, are confidential to IDRBT CA and are open to scrutiny by the CCA office and its approved auditors.

1.1.2. Purpose of CPS

IDRBT CA Certification Practice Statement (CPS) presents the practices in use by IDRBT CA and its Registration Authorities (RAs) taking part in the stipulation of IDRBT CA's Certification Services, in issuing and managing certificates and in sustaining a certificate-based Public Key Infrastructure (PKI). The CPS details the certification process, from commencement of CA operations and repository operations, instituting RAs, to registering subscribers. This CPS provides practices for issuing, managing, using, suspending, re-activating, and revoking of certificates. The CPS is intended to legally bind all parties that create, use, and validate certificates within the context of the Certification services.

This document gives information regarding the IDRBT CA CPS. This CPS is available at the website: http://idrbtca.org.in/

1.1.3. Standards

This CPS is referred to as "IDRBT CA CPS" or "CPS" and hereby also known as "this CPS". The structure of this CPS is based on the "RFC-2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.1.4. Certificates classes and types issued

This CPS supports the operation of:

- All classes and types of IDRBT CA Subscriber Certificates nominated in respective Certification Services (mentioned in detail in section 2.10) including certificates issued to nominated RAs, supporting RA functionalities by IDRBT CA

1.1.5. Definitions

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

Definitions used in this document are contained in the Glossary. The Controller of Certifying Authorities, Ministry of Communication and Information Technology, bases in these definitions on the Schedule V of the Rules and Regulations to Certifying Authorities.

In the occurrence that the reader is unfamiliar with this basic PKI concepts, IDRBT CA would suggest that the reader either

- Contact IDRBT CA at cahelp@idrbt.ac.in ; or
- Visit IDRBT CA's website at http://idrbtca.org.in for further clarifications and explanation prior to the use of any certificate issued under IDRBT CA.

IDRBT CA does not assume, and disclaims any liabilities, damages, losses, costs and all such other expenses that may arise or result from the ignorance or disregard of the reader of these PKI concepts.

1.1.6. Certificate Management Life Cycle

The IDRBT CA Certificate Management Life Cycle is illustrated in Figure 1 below.

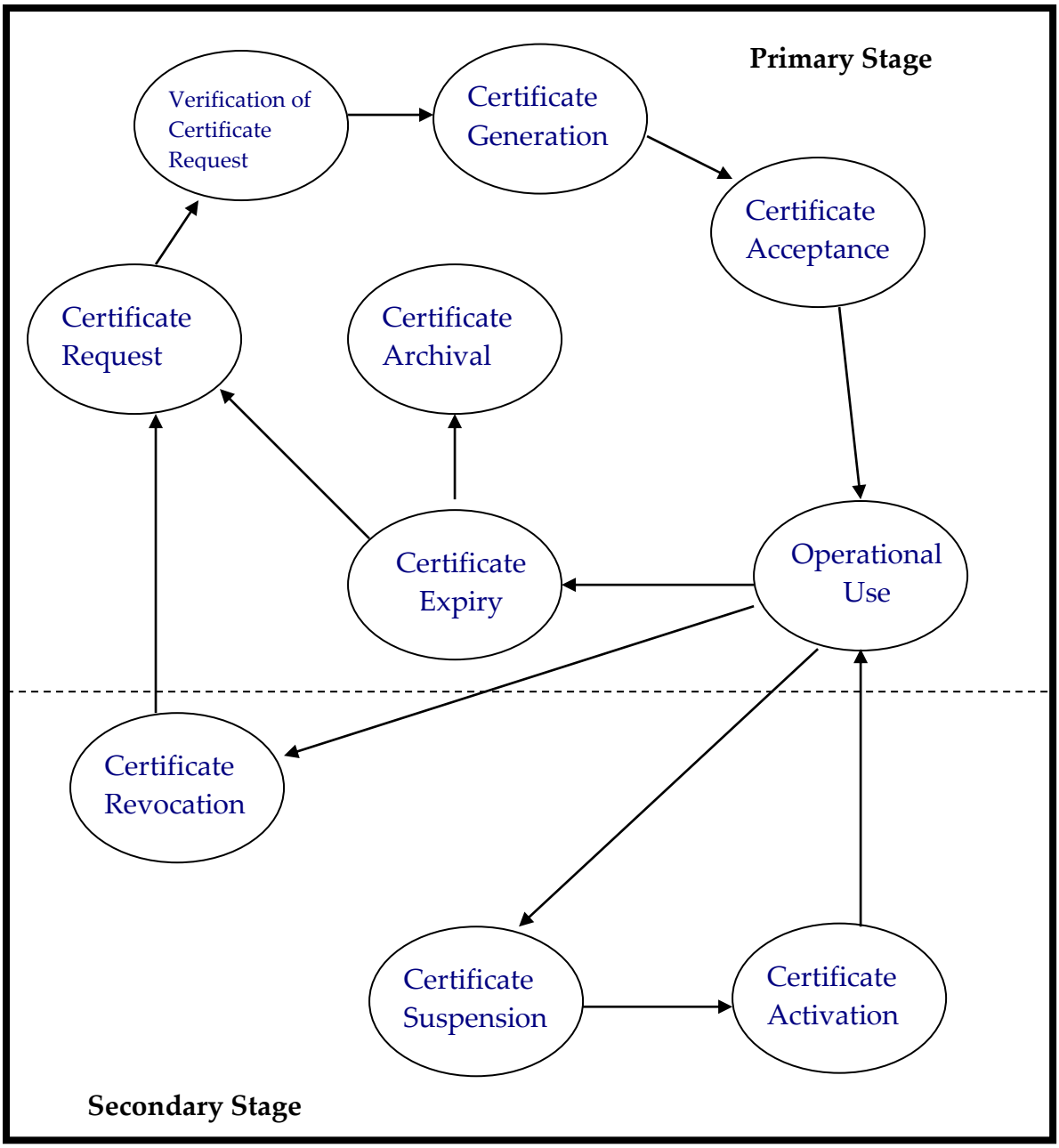

Figure1. Certificate Management Life Cycle

The certificate management life cycle signifies the certificate management process within IDRBT CA PKI which consists of primary and secondary stages.

The primary stages are:

- Certificate request made by applicant/subscriber
- Verification by RA or SA
- Certificate generation by IDRBT CA
- Certificate acceptance by applicant/subscriber
- Operational use of certificate by subscriber
- Certificate expiry; and
- Archival of certificate

All certificate classes (Refer Section 2.10) and types of certificates (Refer Section 2.11) issued by IDRBT CA pass through these primary stages as part of their life cycle.

The secondary stages are:

- Certificate revocation
- Certificate suspension; and
- Certificate activation

The certificates issued by IDRBT CA are deemed to be in operational use in accordance with the applicable procedures.

1.2. Identification

IDRBT CA issues public key certificates that certifies the public key of the subscriber along with the Distinguished Name (DN) details in the name of the organization as detailed below.

Institute for Development and Research in Banking Technology (IDRBT)
Castle Hills, Road No: 1,
Masab Tank,
Hyderabad – 500057
Andhra Pradesh, India.
Ph: +91 – 40 – 23534981
Fax: +91 – 40 – 23535157

This policy is valid from the date of receiving the licence till the expiry of licence with any modifications in consultation with CCA.

1.3. Community and Applicability

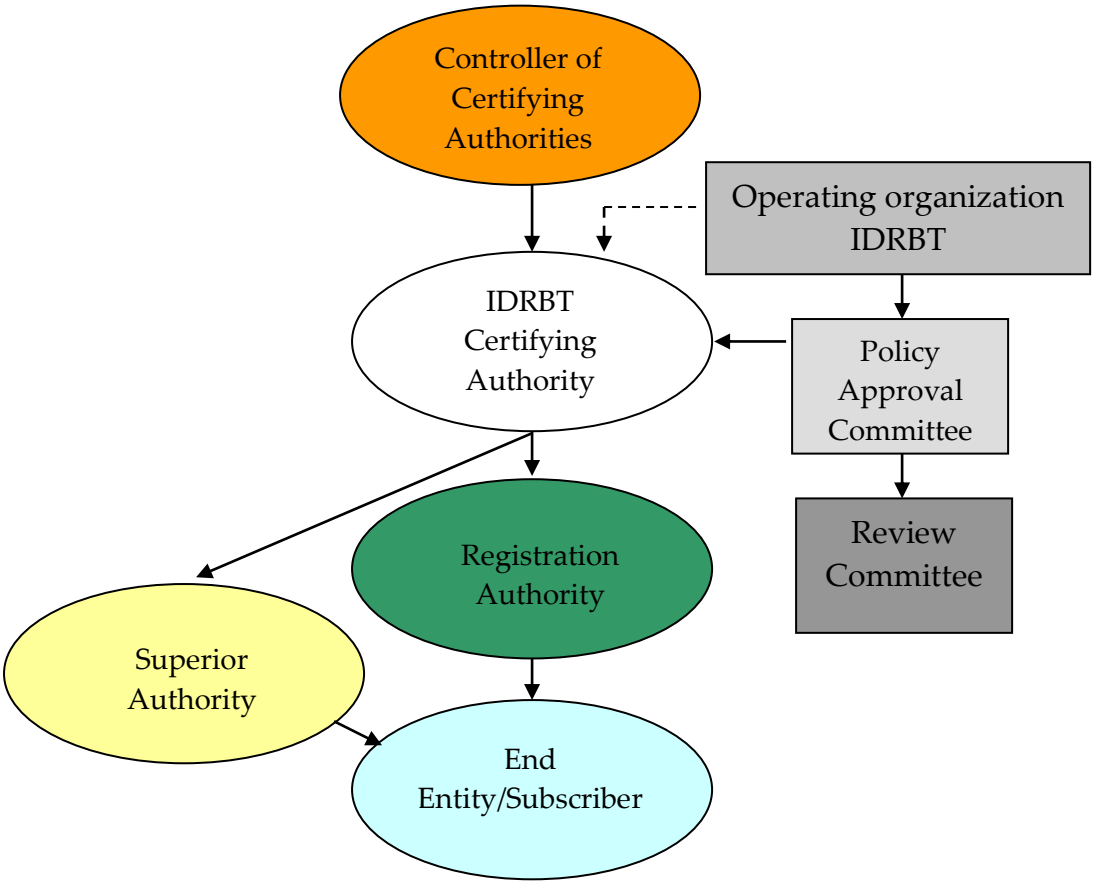

Figure 2. IDRBT CA operational hierarchy

1.3.1. The IDRBT CA hierarchy

IDRBT CA operational hierarchy comprises of two distinct entities i.e. Registration Authorities (RAs), and end entities as described in section 1.3.2 and 1.3.3. On advice of the CCA, IDRBT CA may include Subordinate CA also.

Entity that issue certificates and licenced by the CCA: IDRBT Certifying Authority.

Types of entities that function as Registration Authority (RA): The primary function of an RA is to register applicants/subscribers. RAs have the responsibility of

accepting certificate applications, authenticating the identity or other credentials of the applicant, then approving or rejecting the application. The obligations are enforced in agreement and are set out in a set of RA operating procedures.

The RAs shall be officials preferably not less than the rank of a Deputy General Manager from Public Sector banks, Private Sector banks, Financial Institutions (FIs), and Foreign banks recognized by Reserve Bank of India in the country.

Types of entities that are certified by IDRBT CA as end entities:

IDRBT offers Certification Services primarily for the members of the INFINET (the membership of the INFINET is accorded by the Reserve Bank of India) and individuals recommended by Registration Authority. Later if any change, it will be amended in the IDRBT CA CPS accordingly on the approval of CCA.

A list of PKI enabled applications for which the certificates are issued:

The practices described in this CPS support a large, diverse, and widespread community of users who require PKI certificate services in support of security functions like authentication, non-repudiation, integrity and confidentiality of electronic, financial transactions over networks.

The IDRBT CA PKI user community may regard the practices described in this CPS as:

- ensuring standard operating procedures and uniform quality of service delivery across the PKI;
- fostering and promoting high levels of trust and integrity across the PKI.

1.3.1.1 Policy Authorities

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).

- Review Committee

  IDRBT CA Review Committee has been established to review the operational requirements of IDRBT CA Certification Services and submit new or changed polices to Policy Approval Committee for approval (Ref# IDRBTCA/DOC/SPP: Security Policies and Procedures).

1.3.1.2 Registration Authorities

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 the section 4.1.2 of 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.

1.3.2. End Entities

Applicant – An Applicant is a person, or organization that has applied for, but has not yet been issued a Digital Certificate by IDRBT CA.

Subscriber – A Subscriber is a person, or organization that has been issued a Digital Certificate by IDRBT CA.

Relying party – A Relying Party is a person, or an organization that relies on or uses a Digital Certificate issued by IDRBT CA and/or any other information provided in IDRBT CA Repository to verify the identity and Public Key of a Subscriber and/or use such Public Key to send or receive digitally signed/encrypted communications to or from a Subscriber.

1.3.3. Applicability

The purpose of this Certificate Practice Statement (CPS) is to provide reliable information to applicants, subscribers and to the relying parties. IDRBT CA will issue, administer and revoke Class 1, 2 and 3 digital certificates (refer Section 2.10) which are trust worthy and legally valid under Information Technology Act, 2000. The use of certificates confines with the usage scheme described in Section 4.5 of this CPS. Any other type of usage of certificates which are not mentioned above is explicitly prohibited.

1.4. Contact details

1.4.1. Administration authority and it's functions

This Certificate Practice Statement shall be read with any statement with such particulars as the Controller of Certifying Authorities (CCA) may specify by regulation in exercise of his powers under The Information Technology Act, 2000.

1.4.2. Contact Person

The CA Administrator
IDRBT,
Castle Hills, Road No: 1, Masab Tank
Hyderabad – 500057
Telephone Number: +91-40-23534981
Fax number: +91-40- 23535157
e-mail: cahelp@idrbt.ac.in

1.5. Amendment Procedure

As new standards emerge, or policy and practices are identified for improvement, this CPS will be amended and approved by the Policy Approval Committee. The modified CPS will be communicated to the CCA for approval before its publication. The new document will be under the version control formulated by IDRBT CA.

The right for amending this CPS rests with the IDRBT CA Policy Approval Committee. The electronic copy of the CPS will be available at IDRBT CA's website: http://idrbtca.org.in/

1.6. Other Information

IDRBT CA Applicants and Subscribers accept that IDRBT CA has provided them with adequate information to become familiar with digital certificates before applying for, and for using, and relying on a certificate. Documentation on Digital Signatures, Certificates, Public Key Infrastructure (PKI), and the Certification Services are available from IDRBT CA in their website at:

http://idrbtca.org.in/

For more information about this CPS or information related to IDRBT CA services, the IDRBT Certification Authority can be reached at:

cahelp@idrbt.ac.in

2. GENERAL PROVISIONS

This Chapter describes the obligations, liabilities and responsibilities of the various entities of the IDRBT CA Public Key Infrastructure (PKI) hierarchy. Details of dispute resolutions, applicable law, and audit requirements are also given in this chapter.

2.1. Obligations and Responsibilities

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.

2.1.1. CA obligations

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 as mentioned in section 2.8.1, secured and confidential.
- Collect and keep relevant documents for the corresponding certificates from applicant/subscriber as mentioned in section 4.1.2 as may be required.
- 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 licence.

2.1.2. RA obligations

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 validity 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 as mentioned in section 4.1.2.
- 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 as mentioned in section 2.8.1, secure and confidential and disclosing it only when IDRBT CA instructs to do so.

2.1.3. 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 for issuance.
- Maintain the audit trail of the verification process.
- Not to retain any information related to applicant/subscriber's certificate application

2.1.4. Subscriber obligations

End Entities 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.
- 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 by accepting the certificate.
- Use certificates in accordance with the purpose for which they are issued.
- Prove possession of private keys and establishing their right to use.
- Report their RA or IDRBT CA of any error or defect in their certificates immediately or of any subsequent changes in the certificate information.
- Study this CPS before using their Certificates.
- Inform the RA or IDRBT CA immediately, if a key pair is compromised, by a paper document 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.
- Initiate an online request to get a new certificate on their own after expiry, if required.

2.1.5. Relying party obligations

- It is the sole responsibility of relying party to verify the purpose for which a certificate is used and these purposes should be in line with the purpose for which certificate is issued.
- Relying party has to verify the digital signature of a particular entity and has to satisfy itself with the authenticity.
- Check the CRL available at the IDRBT CA repository whenever relying on a digital signature created by the private key whose public key is certified and presented in the certificate issued by IDRBT CA.

2.1.6. Repository obligations

The LDAP Directory performs the IDRBT CA repository functions. IDRBT CA provides and maintains the operational infrastructure for the LDAP Directory Services, and IDRBT CA post certificates and CRL to the Directory.

IDRBT CA publishes information on issue of certificate and certificate revocation, immediately after a certificate is issued or revoked.

2.2. Liability

IDRBT CA has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

- inhibit misuse of those resources by authorized personnel;
- prohibit access to those resources by unauthorized individuals.

The IDRBT CA services are running on dedicated high-end reliable servers that consist of RAID drives and with redundant infrastructure.

Further IDRBT CA follows the under mentioned measures for the security and protection

- Take regular system data backups

- Take back up of current operating software and keep a record of configuration files and update the Operating System when official bug fixes/patches are released.
- Secure all backups in secure local and offsite storage.
- Regularly test backups to ensure that backup is available properly.
- Periodically review the contingency plans vis-à-vis the identification, analysis, evaluation and prioritization of risks.
- Regularly testing uninterrupted power supplies.

IDRBT CA will not be legally responsible in any way, for any imprecision, mistake, delay, or lapse, in the issuance or verification of any Digital Certificate, or for non-performance including suspension, activation and revocation or the failure to suspend, activate or revoke, or due to any reason beyond IDRBT CA's control.

IDRBT CA will have no legal responsibility to a Subscriber, occurring from or concerning to issuance, management or use of an IDRBT CA Digital Certificate that is issued or sustained in force in reliance upon or as a consequence of any false or deceptive information provided by the Subscriber or any material lapse in any information provided by the Subscriber in connection with his/her request for IDRBT CA Digital Certificate or otherwise.

2.2.1. CA Liability

2.2.1.1 CA Warranties to Subscriber and Relying Parties

The IDRBT CA warrants

- To provide the Digital Signature Certification services such as IDRBT CA repository as specified in this IDRBT CA CPS.
- To provide the PKI infrastructure for the operation of the IDRBT CA as specified in this IDRBT CA CPS.

- To issue the Digital Certificates to the respective applicants as specified in this IDRBT CA CPS.
- To revoke the Digital Certificate based on the suspect of compromise.
- To publish the accepted Digital Certificates in the IDRBT CA repository.
- To put the revoked certificates into the CRL and publish the updated CRL in the IDRBT CA repository as specified in this IDRBT CA CPS.

2.2.1.2 Limitations on warranties

- The IDRBT CA disclaims all other warranties except as expressly stated in this IDRBT CA CPS.
- The IDRBT CA does not warrant accuracy, reliability, correctness and authenticity of the unverified information contained in the Digital Certificate.
- The IDRBT CA does not warrant the reliability of the technique used in generation and storage of the private key by the applicant/subscriber.
- The IDRBT CA does not warrant any loss, damage or consequences arising out of the compromise of digital certificates or private keys of users, which are not expressly brought to the knowledge of the IDRBT CA by the respective users.

2.2.1.3 CA Limitation of Liability

IDRBT CA's liability is as per the IT Act, other governing Indian laws and IDRBT CA's Master Agreement. It includes the following caps limiting IDRBT CA's damages concerning a specific Certificate:

Class	Liability Caps
Class 1	Rs. 20/-
Class 2	Rs. 250/-
Class 3	Rs. 10000/-

Table 1: Liability Caps

In no event shall IDRBT CA or the RA be liable for any indirect, incidental, special, substantial, disciplinary, dependence, cover or liquidated damages, including but not limited to loss of profits, revenue, data or use, incurred by the other party, and resulting from the services provided by the IDRBT CA or the RA, including negligence and fraud.

2.2.2. RA Liabilities

The RA warrants

- To perform adequate verification of the application given by the applicant for obtaining a Digital Certificate as per this CPS.
- To forward the applicant's request for certificate generation and the subscriber's request for the certificate revocation to the IDRBT CA.

2.2.3. Subscriber Liability

IDRBT CA requires Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- No unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application submitted by the Subscriber are true,

- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, specifically for the purpose as stipulated/stated by the submission in the certificate application only, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

2.2.4. Relying Party Liability

Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations as mentioned in section 2.1.4.

2.3. Financial Responsibility

The IDRBT CA does not make any representation and does not give any warranties on the financial transactions, which the subscribers and the relying parties undergo using the Digital Certificate obtained from the IDRBT CA. The subscribers and the relying parties shall be responsible for any losses, damages or any consequences due to such transactions.

2.3.1. Indemnification by Subscribers

To the extent permitted by applicable law, IDRBT CA requires, Subscribers to indemnify IDRBT CA or RAs for:

- Deception or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- 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,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party, 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.

2.3.2. Indemnification by Relying Parties

To the extent permitted by applicable law, IDRBT CA's Relying Party Agreements require, Relying Parties to indemnify IDRBT CA or RAs for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- 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.

2.3.3. Fiduciary relationships

Issuing certificates or assisting in the issue of certificates in accordance with this CPS does not make IDRBT CA or RAs operating under IDRBT CA, fiduciary, trustee, or other representative of subscribers or relying parties.

2.4. Interpretations and Enforcement

Unless otherwise provided, this CPS shall be interpreted consistently in accordance with IT Act 2000.

2.5. Governing law

The Information Technology Act, 2000, by Government of India, and The Rules and Regulations for Certifying Authorities formulated by Controller of Certifying Authorities (CCA), Ministry of Information Technology, Government of India shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of the contract or other choice of legal provisions and without the requirement to establish a commercial nexus.

2.5.1. Severability, Survival, Merger and Notice

2.5.1.1 Severability

In the event that any one or more of the provisions of this CPS shall for any reason be held to be invalid, illegal, or unenforceable by law, such unenforceability shall not affect any other provision, but this CPS shall then be interpreted as if such unenforceable provision or provisions had never been contained herein, and in so far as possible, construed to maintain the original intent of the CPS.

2.5.1.2 Survival

The obligations and restrictions contained within CPS (Audit, Confidential Information, Obligations of the IDRBT CA and the RA, and Limitations upon such obligations) shall survive the termination of this CPS.

2.5.1.3 Merger

In case of merger, no term or provisions of this CPS directly affecting the respective rights and obligations of IDRBT CA may be amended, waived,

supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

2.5.1.4 Notice

Any notice to be given by a Subscriber, Applicant, or Relying Party to IDRBT CA under this CPS, shall be given in writing to the address specified below by registered or speed post, postage prepaid and return receipt requested, or by courier service or by fax.

Any notice to be given by IDRBT CA under the CPS, shall be given by email to the email address of the Subscriber or by post.

Notice address for IDRBT CA: as mentioned in section 1.4.2

2.5.2. Dispute resolution procedures

Dispute resolution between IDRBT CA, RA, the Subscribers, and the Relying parties will be as per the IT Act 2000 by the Ministry of Information Technology, Government of India. Resolution of disputes should overall be governed by the IT Act 2000, and will be referred to the CCA from time to time for arbitration. Any person found violating the principles and procedures mentioned in the this CPS and any other procedures supplementing the operation of IDRBT CA, will be punished according to the rules pertained in the IT Act 2000.

2.6. Fees

The fees for services provided by IDRBT CA in respect of IDRBT CA Certificates are set forth in the IDRBT CA website. These fees are subject to change, and any such changes shall become effective immediately after posting in the IDRBT CA website. Please visit the IDRBT CA website for the latest fee structure for different Class of Certificates at:

http://idrbtca.org.in/

2.6.1. Certificate issuance fees

Fees may be payable in respect to the issue of certificates. Please refer the IDRBT CA website for further details.

2.6.2. Certificate access fees

IDRBT CA may not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties, but IDRBT CA reserves the right to change the fee structure.

2.6.3. Revocation or status information access fees

IDRBT CA shall not charge a fee as a condition of making the CRLs available in a repository or otherwise making it available to Relying Parties. IDRBT CA will not charge any fees for revoking or suspending a certificate.

2.6.4. Fees for other services such as policy information

IDRBT CA shall not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

2.6.5. Refund policy

IDRBT CA adheres to rigorous practices and policies in undertaking certification operations and in issuing certificates. Once subscribers pay an amount for the issuance of certificate, it can't be refunded by IDRBT CA unless the RA rejects the certificate request.

2.7. Publication and repository

2.7.1. Publication of CA information

Upon the subscriber's acceptance of the certificate, the IDRBT CA shall publish a copy of the certificates in the IDRBT CA repository and in one or more other

repositories, as determined by the IDRBT CA. It will also publish IDRBT CA's Public Key Certificate and the Certification Practice Statement (CPS). The Certificate Revocation List that comprises of the revoked certificates will also be published.

2.7.2. Frequency of publication

The IDRBT CA repository will promptly publish certificates, amendments to the CPS, notices of certificate suspension or revocation, and other information, consistent with this CPS and applicable law. The website for the IDRBT CA repository is http://idrbtca.org.in/

After completing the paper and verification formalities, IDRBT CA will be issuing certificate within **five** working days. This CPS prohibits accessing of any data in the repository that is declared confidential by the CPS and/or by the IDRBT CA repository, unless authorized by the IDRBT CA.

2.7.3. Access controls

Information published in the IDRBT CA repository is publicly-accessible information. IDRBT CA entails persons to agree to a Relying Party Agreement (refer Section 9.4) as a condition to access Certificates, Certificate status information, or CRL.

The right to make modification in this CPS rests with IDRBT CA (refer Section 8).

This information is available electronically at IDRBT CA's repository http://idrbtca.org.in/ and CPS in paper form at IDRBT, Road No: 1, Castle Hills, Masab Tank, Hyderabad- 500057, India. An amount of Rs. 500/- will be charged in advance for CPS in paper form.

2.7.4. IDRBT CA Repository

The IDRBT CA repository is a collection of databases for storing and retrieving certificates and other information related to certificates. The IDRBT CA repository's content includes: certificates, CRL, current and prior versions of the IDRBT CA CPS, and other information as prescribed by IDRBT CA from time to time. Any confidential information would not be available in the repository.

2.8. Compliance audit

2.8.1. Frequency of Audit

Every year IDRBT CA conducts a comprehensive compliance audit of the practices mentioned in this CPS as mentioned in the IT Act, Rules, Regulations and Guidelines.

All parties should comply with operating agreements if exists, and this CPS under which certificates are issued. If, there is any non-compliance and it is found to be serious, certificate of the respective party may not be renewed.

2.8.2. Qualifications of auditor

A certified Information Security Auditor empanelled by the CCA will be contracted to audit on IDRBT CA operations.

2.8.3. Auditors relationship to audited party

The auditing firm that is performing the audit shall be independent of the party being audited such as the IDRBT CA and the RAs.

2.8.4. Topics covered by audit

The topics to be covered are as per the IT Act, Rules, Regulations and Guidelines to Certifying Authorities by CCA.

The topics include:

- Physical security

- Security Policy and Planning
- Technology evaluation
- IDRBT CA services administration
- Relevant CPS
- Compliance to relevant CPS
- Contracts / agreements
- Regulations prescribed by the Controller
- Any other topics at the discretion of IDRBT CA.

2.8.5. Actions taken as a result of deficiency

If deficiencies are found in the audit reports, IDRBT CA will implement appropriate correction within a reasonable time frame.

2.8.6. Communication of results

Audit results are considered as confidential information and they will be notified to the parties concerned only.

2.9. Confidentiality

IDRBT CA office and the RAs under the IDRBT CA Certification Services shall take care in protecting the information from being disclosed or used for purposes other than specified in this CPS.

2.9.1. Types of information to be kept confidential

2.9.1.1 Collection and Use of Personal Information

- The practices described in this CPS conform to the CCA Rules and Regulations on the use of PKI.
- Access to confidential information by operational staff is on need-to-know basis. Paper based records and other documentation containing confidential information are kept in secure and locked containers or filing systems, separate from all other records.

2.9.1.2 Registration Information

All registration records are considered to be confidential information, including

- Certificate application records. both accepted and rejected applications.
- Certificate information collected as part of the registration records but not included in the Certificate information.

Not withstanding the aforesaid, IDRBT CA reserves the right to publish such appropriate and necessary information within the registration authorities as defined above, in its Directory Server and/or in the CRL as may be deemed appropriate and necessary by IDRBT CA.

2.9.1.3 Certificate Information

The information contained in the certificate is public but any communication between RA and subscriber of a Certificate being suspended or revoked is considered to be confidential information.

2.9.1.4 IDRBT CA PKI Documentation

The following IDRBT CA PKI documents are considered to be confidential:

- Master Agreement
- Contingency planning and disaster recovery plans
- Information Technology Security Policy and Procedures
- Security Policy and Service Administration Manual
- Operational Procedures regarding IDRBT CA
- Configuration Baseline
- Audit reports of Third Party auditors, if any

2.9.2. Types of information not considered confidential

Certificate information published in Directory Services like

- Certificate status

- The date, time and period of certificate revocation
- The period of Certificate suspension

Similarly the following documents are also considered not confidential

- Privacy Policy and Legal Disclaimer

2.9.3. Voluntary Release/Disclosure of Confidential Information

IDRBT CA shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release from

- the person to whom the IDRBT CA owes a duty to keep such information confidential and
- The person requesting confidential information (if not the same person) may have a court order. The IDRBT CA may require that the requesting person pay a reasonable fee before disclosing such information.
- Confidential information will also be disclosed by the IDRBT CA when ordered by to do so by the CCA.

No information is allowed outside India without the written permission from a Court or Tribunal or any Government or public authority having the power to compel the disclosure.

2.10. Intellectual Property Rights

2.10.1. General provision

IDRBT CA warrants that it is in possession of, or holds licenses for the use of hardware and software in support of this CPS. IDRBT CA further warrants that operational use of this CPS does not infringe any copyright enforceable in India of any third party. IDRBT CA excludes all liability for breach of any other intellectual property rights.

IDRBT CA shall comply with Applicant/Subscriber's information protection as per the IT Act, 2000. The information supplied by the Applicant/Subscriber is the

property of the respective Applicant/Subscriber. All Applicants/Subscribers shall grant to the IDRBT CA and the RAs a non-exclusive, world-wide, paid-up, royalty-free license to use, copy, modify, publish and distribute such information subject to Applicant/Subscriber's information protection as per the IT Act, 2000.

IDRBT CA has got specific restrictions relating to the use of name in a certificate application to prevent trademark infringement. This is done by ensuring that the RA/SA checks that no such names are provided in a certificate application. Should a dispute arise however in spite of better effort of IDRBT CA and its RAs, the appropriate trademark holder shall inform IDRBT CA by written notice in the manner given in the Section 2.4.2.4 of the CPS. The dispute shall be resolved in accordance with procedure given in Section 2.4.3.

2.10.1.1 Public and private keys

If the End Entity generates the public and private key pair to the satisfaction of the IDRBT CA then the End Entity grants to the IDRBT CA the right to publish and propagate in the IDRBT CA Directory the public key that corresponds to the private key that is in the possession of the End Entity. This publication will be through the incorporation of the public key in the certificate (whether electronic or otherwise) that forms part of the IDRBT CA Directory. Nothing in this clause grants to the End Entity any rights whatsoever in relation to the format or structure of the certificate that encompasses the End Entities public key. The end entity grants to the IDRBT CA the right to publish and circulate the certificates that corresponds to the private key that is in the possession of the End Entity in the Directory Servers. This publication will be through the incorporation of the public key in the certificate (whether electronic or otherwise) that forms part of the IDRBT CA Directory. Nothing in this clause grants to the RA or the End Entity any rights whatsoever in relation to the format or structure of the certificate that encompasses the End Entities' public key.

2.10.1.2 Certificate

The IDRBT CA reserves the right at any time to cancel or suspend any certificate in accordance with the procedures and policies set out in this policy statement.

2.10.1.3 Distinguished names

Intellectual property rights in distinguished names vest with the IDRBT CA unless otherwise specified in this CPS, contract or other agreement.

2.10.2. Copyright

The intellectual property in this CPS is the exclusive property of IDRBT CA.

2.11. Classes of Certificate

IDRBT CA supports three 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.

2.11.1. 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 two years.

Assurance level: The verification of the certificate request of this class represent a simple check of the certainty of the subject name within the IDRBT CA repository, plus a limited verification of the address, other personal information and e-mail address as per Section 4.1.2.

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.

2.11.2. Class 2 Certificates

Description: Class 2 certificates are issued to individuals and to the servers used in financial transactions. The RA bases it on the verification of the application form and the certificate request.

In case of online certificate request for Class 2 Certificate, the applicant/subscriber submits online as well as paper application form and the documents (as mentioned in section 4.1.2) to the RA under IDRBT CA. RA verifies the name,

postal address and the e-mail address in the request as per Section 4.1.2. 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 2 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.

Class 2 certificates are issued either for one year validity period or two years validity period as per choice of the subscriber.

Assurance level: Class 2 Certificate processes utilize various procedures to obtain probative evidence of the identity of individual applicants. These validation procedures provide stronger assurance of an applicant's identity.

The Class 2 Certificate is used for Digital Signature and Encryption.

Class 2 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.

2.11.3. 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 (as mentioned in section 4.1.2) will be physically verified by the RA office and after confirmation of facts it will recommend the issuance of the certificate. RA has the right to reject the certificate request if RA finds it not

meeting the criteria. 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. The Domain Name validation will be as per Section 4.1.2.

Class 3 certificates are issued either for one year validity period or two years validity period as per choice of the subscriber.

Assurance level: Class 3 Certificate processes make use of various procedures to obtain strong confirmation of the identity of individual applicants as well as the server. These validation procedures provide stronger guarantee of an applicant's identity. Utilizing validation procedure by the Registration Authorities boosts the practical uses and trustworthiness of Class 3 Certificates.

The Class 3 Certificate is intended to use for Digital Signature, Encryption of messages, Object signing and Secure Web Server.

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.

2.12. Types of Certificates

IDRBT CA issues five types of certificates: Signing, Encryption, System, Web server and Object Signing Certificate.

2.12.1. Signing Certificate

The signing certificate is corresponding to the signing private key. It will be used by individuals for email or servers for signing purpose. The signing certificate for servers should be applied by an individual on behalf of the server. The signing key pair is used to digitally sign the messages. The key pair is generated in a secure medium by the subscriber and is inherent to keep his private key in safe custody. The subscriber attains a Digital Certificate from the IDRBT CA as specified in this CPS, to authenticate the precision of his public key. The subscriber encloses a copy of this certificate with all the messages he sends with his signature. The recipient uses the public key in the enclosed certificate to verify the signature of the subscriber.

2.12.2. Encryption Certificate

The encryption key pair is used by the subscriber for receiving the messages from the sender, which is encrypted by the recipient's public key. The private key of

the subscriber is used for decrypting the messages. The encryption key pair is generated by IDRBT CA and the encryption certificate with private key protected with a password. The password will be communicated to the subscriber by an email to his personal official email id in a secure manner. A copy of the encryption private/ public key pair of the subscriber shall be retained with the safe custody of the IDRBT CA.

The generation of the encryption shall be in conformity with the Indian Telegraphic Act and all other relevant parts of the Indian legal system.

2.12.3. System Certificate

Were certificates need to be issued to computer systems for the purpose of machine to machine authentication, it is of paramount importance that the certificate contains a unique identification relating to the systems. At the same time, it is essential that the application making use of such certificates are designed to verify the system with the digital certificate being used. The Certificate field requirements for the system certificates include:

S.No	Field / Extension	Variation
1	Subject Name	▪ The CN in the Subject Name MUST contain either ▪ IP Address of the system as a printable string in "network byte order", as specified in [RFC791] ▪ MAC Address of primary network interface as a printable string ▪ Serial number (CPU or any electronically verifiable serial number) as a printable string ▪ Unique ID (such as CPU identifier) as a printable string
2	Key Usage	▪ Server authentication ▪ Client Authentication

3	Subject Alternative Name	▪ Subject Alternative Name MUST contain either ▪ IP Address of the system as a octet string in "network byte order", as specified in [RFC791] ▪ dnsName in IA5String format

The private key of the certificates should be held in secure token or smart card. For applications processing sensitive or high value transactions, it is recommended that the private key be stored in a Hardware Security Module (HSM).

2.12.4. Web server Certificate

Web server certificates are digital identifications containing information about Web server and the organization that is sponsoring the server's web content. A web server certificate enables users to authenticate the server, check the validity of the web content, and establish a secure connection. The web server certificate also contains a public key, which is used in creating a secure connection between the client and server.

2.12.5. Client Certificate

Client certificates are electronic documents that contain information about clients. These certificates, like server certificates, contain not only this information but also public encryption keys that form part of the SSL security feature. The public keys, or encryption codes, from the server and the client certificates facilitate encryption and decryption of transmitted data over an open network, such as the Internet. The typical client certificate contains several items of information: the identity of the user, the identity of the certification authority, a public key that is used for establishing secure communications, and validation information, such as an expiration date and serial number.

2.12.6. Object Signing Certificate

Object Signing helps users develop confidence in downloaded code. It allows users to identify the signer, to determine if objects have been modified by someone other than the signer.

Object Signing uses standard techniques of public-key cryptography to let users get reliable information about code they download in much the same way they can get reliable information about shrink-wrapped software. Signed objects can be Java applets, Java Scripts, plug ins, Active X controls or any other kind of code.

3. IDENTIFICATION AND AUTHENTICATION

This Chapter describes how parties involved in the certification process are identified and authenticated.

3.1. General

3.1.1. RA Registration

The fundamental concept supporting the operation of IDRBT CA is based on trust. To ensure the integrity and trustworthiness of the operations throughout the IDRBT CA PKI hierarchy, the RAs must agree and comply with the practices in this CPS. The RA should possess an INFINET/Internet connection and necessary infrastructure to maintain RA Office and keep all physical records of Subscribers in a secured manner under lock and key (Ref# IDRBTCA/DOC/RRA: Rules and Guidelines for RA Office).

3.1.1.1 Submission of application to operate as an RA

An application by any party to establish and operate as an RA within the IDRBT CA PKI hierarchy should be made in a form of letter of request (on Organization letter head) to:

IDRBT CA,
IDRBT, Castle Hills, Road No.1, Masab Tank,
Hyderabad – 500 057.
Andhra Pradesh,
India.

Application to operate, as an RA must include the following details, which may be appended to the letter of request:

- Forwarding letter including his contact details by the Head of the Organization
- The legal name of the party making the application;
- Full contact details
  - Residential and Mailing address
  - Telephone and Fax number(s)
  - Email address
- A statement that the applicant
  - has read this CPS
  - the contractual Master agreement

3.1.1.2 Consideration of the Application

When IDRBT CA receives an application from a third party to operate as an RA:

- An authorized representative of the applicant attempts an identity verification process in person. During the process, their representative produces the documents as mentioned in Section 3.1.1.1.
- The IDRBT CA approves or rejects the application. If IDRBT CA approves the application, the RA will be issued a Class 3 Certificate.
- IDRBT CA reserves the right to revoke its approval if the requirements are not met in full or to its satisfaction.

3.1.2. End Entity Initial Registration

3.1.2.1 Identity Verification

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:

- be attended by an end entity in person (based on the Class of Certificate)

- be conducted by an authorized Registration Authority or Superior Authority as the case may be.
- perform the following functions:
  - 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.
  - The applicant is required to affix the latest passport size photograph on the first page of the application form.
  - 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.
  - 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.
  - 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.

    - Collection of Certificate information
    - Proof of other material certificate information like identification documents as mentioned in Section 4.1.2 of this CPS

Registration Authority has to verify that the keys were generated using an approved application and of required key length. The end entity must adequately provide proof to the RA that they generated the key pair themselves and in possession of the private key.

3.1.2.2 Post- identity Verification

In case of online certificate application by subscriber, after identity verification has been completed, RA considers the Certificate request and approves or rejects it. If the application is approved, RA uses the Web interface to transmit a digitally signed request to IDRBT CA.

If the application is rejected, the applicant is promptly informed by RA by email or by telephone.

3.2. Initial Registration

3.2.1. Types of names

IDRBT CA has a DN (Distinguished name) in its certificate. IDRBT CA may also provide subject alternative name and a URL.

Distinguished Name (DN):

CN = IDRBT CA 2011

House Identifier (2.5.4.51) = Castle Hills

Street = Road No.1, Masab Tank, Hyderabad

S = Andhra Pradesh

Postal Code = 500057

OU = Certifying Authority

O = Institute for Development and Research in Banking Technology

C = IN

End entities and RA are also required to have a DN in their certificate.

3.2.2. Need for names to be meaningful

End Entity's Distinguished Names will follow the convention adopted by their organizations complying with X.500 naming conventions. The distinguished names will contain the following details:

- Common Name (CN) is the unique name of the subscriber.

- E-mail id is the e-mail id of the applicant allotted with official domain name
- State (S), which represents the State in which the organization is located.
- Postal Code, which represents the locality where the organization is located.
- Organizational Unit (OU), which is used to distinguish various organizational groups in the same organization.
- Organization (O).
- Country(C), which is the two-letter identifier for the country to which the subscriber belongs.

The template of DN followed by IDRBT CA is mentioned below:

CN= Name of applicant/subscriber/server

S= Name of State

Postal Code= locality in which the organization is located.

OU= Name of department/organizational unit

O= Name of company/organization

C=IN

Personal name will be a unique name for the entity with respect to the organization to which the entity belongs. IDRBT CA would ensure that all certified entities have a distinct DN.

3.2.3. Rules for interpreting various name forms

See section 3.2.2

3.2.4. Uniqueness of names

DNs will be unique within X.500 Standards. The certificate issued by the IDRBT CA will have a unique Certificate Serial Number.

3.2.5. Name claim dispute resolution procedure

IDRBT CA will determine an entity's DN. (refer section 3.2.2)

3.2.6. Recognition, authentication and role of trademarks

It is as per the trademarks applicability in the Indian Financial sector.
No names shall be allowed in the certificate applications that may infringe upon the trademark protection laws of India (refer Section 2.9.1).

3.2.7. Method to prove possession of private key

IDRBT CA verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS#10, another cryptographically equivalent demonstration. The RAs operating under IDRBT CA will perform validation on the signature of the applicant in certificate request using reversible asymmetric algorithm (such as RSA) with the IDRBT CA certificate application.

This requirement is not applicable in case IDRBT CA generates the key pair for the subscribers (in case of encryption certificates).

3.2.8. Authentication of organizational 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.

3.3. Routine Rekey

IDRBT CA Certification Services support Certificate renewal in the mode of rekey. Subscribers may request Certificate renewal provided that:

- Content of Certificate information as contained in the registration records has not been changed.
- The request is made before the expiry of their current certificates.
- Their current certificates have not been revoked.
- They are not listed in the compromised user.
- Their keys are not included as the compromised keys.

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. IDRBT CA requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

3.4. Rekey after Revocation

The subscriber must apply for a new certificate after the expiration of the certificate or after the revocation of certificate using normal procedure, if required.

3.5. Revocation request

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. OPERATIONAL REQUIREMENTS

This Chapter describes the operational provisions on entities involved in the certificate issuance (and certificate revocation) process.

4.1. Certificate Application Procedure

All online certificate applicants/subscribers requiring a certificate shall complete the following general procedures for each certificate application:

- Generate a key pair
- Protect the private key of this key pair from compromise
- Submit a certificate request, along with the public key of this pair, to the RA under IDRBT CA

4.1.1. Key Generation and Protection

An online certificate applicant shall securely generate his/her own signing key pair as per CCA guidelines, using a reliable system, and acknowledges that he/she will take necessary precautions to prevent its compromise, loss, disclosure, modification, or unauthorized use of keys.

4.1.2. 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 2.

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 of Certificate	Information to be furnished in the application form	Documents to be furnished
Class 1	***Individuals:*** • Full Name • Residential Address • Official Address • Nationality • Email Address • Bank Account details	
Class 2	***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	Attested Xerox 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) + Authorization letter from the higher authority of the subscriber who will be applying for Class 2 Certificate.

Class 3	***Individuals:*** Same as Class 2	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.

	Web Server Certificate: Same as Class 2 (details of the authorized representative), plus The URL/server name/IP address to which the server authentication is needed. Verification of credentials of the bank/ financial institution 1. The PAN number of the bank/ financial institution has to be furnished in the application form 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.

	Object Signing: Same as Class 2 (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	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 Object Signing Certificate on behalf of the bank/ financial institution.

Table 2a: Identification documents required for Online Certificate Application

Email Verification:

E-mail verification is done by the way of sending the user-id 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.

Web Server 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.

For obtaining Web Server (SSL) Certificate, the applicant is required to submit the application form with details of IP Address, URL/Domain name, the Custodian of the web Server, Department to which the server belongs, Official address, Contact Number and Physical Location of the Server etc to the Registration Authority. Only after proper verification of the details of Domain Name contained in the Common Name and Subject Alternative Name (SAN) mentioned in the application form by the subscriber are properly verified by the Registration Authority officials based on which the subscriber will be allotted a User Id to apply online for the Web Server Certificate.

Before issuing SSL certificate, the authenticity of Applicant's registration, ownership or exclusive control of the Domain Name(s) to be listed in the SSL Certificate will be verified by the Certifying Authority that the domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN) approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA). This process would help the Certifying Authority not to issue certificates for non-valid Top Level Domains (TLD).

For GOV.IN the authenticity will be verified by the Certifying Authority from the registry maintained by National Informatics Centre (https://registry.gov.in/).

CA also ensures the correctness of the furnished information by making NSLOOKUP query / WHOIS Lookup query as applicable, and in case of any doubt, the RA is advised to contact the applicant over phone, email or personal interaction for clarifications to resolve the matter. CA will further confirm that the Applicant is aware of its registration or exclusive control of the Domain Name.

4.2. 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 is the person identified in the request (for Class 2 and Class 3 Certificates)
- 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.

4.2.1. Individual Presence

The personal presence before the RA (if required), is needed at least for Class 3 and as and when it is required (depending upon the class of certificate). Refer section 4.1.2 for details.

4.3. Certificate Issuance

In case of online certificate requests, RAs should take care in accepting and processing Certificate requests. They are to comply with the practices described in this CPS and with any requirements imposed by the Certification Services under which the certificate is being issued.

When advice is received that the certificate information is inaccurate or no longer applicable, the IDRBT CA shall investigate and initiate the certificate revocation procedure accordingly.

The generation of the Digital Signature Certificate (DSC) will consists of:

- The receipt of approved and verified certificate request in case of signing, web server, System, client and object signing certificates.
- Generate a key pair in case of encryption certificate.
- Creating a new Digital Certificate.
- Binding the key pair of IDRBT CA associated with the digital certificate to the digital certificate owner.
- Issuing the digital certificate and the associated public key for operational use.
- A distinguished name associated with the digital certificate owner, and
- A recognized and relevant policy as defined in IDRBT CA CPS.

4.3.1. Certificate issue process

End entity attends identity verification process based on the class of certificate requested and provides the following to RA:

- All relevant information of the end entity
- Provide the proof of identity as listed in section 4.1.2
- Understand the terms and conditions in this CPS

Before the approval of the Digital Certificate, RA will confirm that the user's name does not appear in the list of compromised users.

Before the issue of Digital Certificate, IDRBT CA will:

- Comply with the procedure as defined in the IDRBT CA CPS including verification of identification and/or employment
- Comply will all privacy requirements

- Obtain a consent of the person requesting the Digital certificate, that the details of such digital certificate can be published on a directory service

Since, key pairs are generated by the applicant/subscriber, he must prove the possession of private key corresponding to the public key. After verifying the relevant credentials, within three working days, RA or Superior Authority forwards the certificate application to the IDRBT CA office and submits a certificate request along with the public key. After receiving the certificate request, within two working days IDRBT CA generates the certificate for the public key.

In case of online certificate application, the subscriber downloads the certificate from the IDRBT CA's website.

Subscriber stores the private key in a secured manner and restricts the access to the private key.

IDRBT CA reserves the right to issue the certificates and it can reject an application at its discretion.

4.4. Certificate Acceptance

IDRBT CA will provide an opportunity for the subscriber to verify the contents of the Digital Certificate before it is accepted. Downloading a certificate or installing a certificate by accepting a message attached to it constitutes the Subscriber's acceptance of the Certificate.

4.5. Certificate Usage

Based on the certificate usage mentioned in the certificate, the subscriber can use his certificate for the following purposes.

4.5.1. S/MIME Encryption

The sender can use the IDRBT CA Encryption Certificates after verifying the key usage extension (refer section 7.1.2.1) to send encrypted messages to the recipients. The message, which is being sent, will be encrypted by the recipient's public key of the encryption key pair, which can be obtained from the corresponding recipient's certificate for the encryption key pair. While receiving the message, the recipient can decrypt the message with the encryption private key.

4.5.2. S/MIME Signing

The subscriber shall use Signing Certificate (for key usage extensions refer section 7.1.2.1) to sign the messages, which he/she sends. The subscriber signs the messages with the private key of the signing key pair and encloses the certificate for the subscriber's public key of the signing key pair. The recipients shall use the subscriber's public key in the certificate to verify the message.

4.5.3. Object Signing

The subscriber can use Object signing certificate (for key usage extensions refer section 7.1.2.1) for signing a software code or an object, which should be trusted by the relying parties. Object Signing uses standard techniques of public-key cryptography to let users get reliable information about code they download in much the same way they can get reliable information about shrink-wrapped software.

4.5.4. SSL Server

The Web Server Certificate allows the client to authenticate the SSL-enabled server, and allows both server and client to establish an encrypted session. (for key usage extensions refer section 7.1.2.1)

4.5.5. SSL Client

The Subscriber shall use Client Certificate for use in Secure Sockets Layer (SSL) communication between the browser (client) and the Web servers. (for key usage extensions refer section 7.1.2.1)

4.6. Certificate Suspension and Revocation

Suspension is the process of making a certificate to make it invalid temporarily. Revocation is the process of making a certificate to be invalid permanently.

IDRBT CA can activate the suspended certificates. The revoked certificates cannot be reused and are listed in the CRL.

IDRBT CA will be responsible for issuing CRL and for publishing signed versions thereof. The IDRBT CA will continuously update its CRL with revoked certificates.

Details on how CRL can be found and how to use these services can be found at http://idrbtca.org.in/

4.6.1. Circumstances for revocation

A certificate shall be revoked when the information in the certificate is known to be, or suspected be, inaccurate or when the private key associated with the certificate is compromised or suspected to be compromised. This includes situations where:

- The subscriber loses relevant privileges;
- The information provided by the end entity is inaccurate, e.g. when the owner of an identity certificate change their name
- The subscriber changes his organization
- An end entity makes the request for the revocation
- Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of IDRBT CA Digital Certificate

- The Subscriber has breached or failed to meet their obligations under this CPS or any other agreement, regulation or law which may be in force
- Any other circumstances which shall be determined by rules and regulations to governing law

4.6.2. Who can request revocation

A revocation request can be made by the holder of the certificate to be revoked to the IDRBT CA. The process of revocation can be initiated by IDRBT CA also. In case, SA/RA has any information regarding false representation or otherwise, SA/RA will initiate revocation request.

4.6.3. Procedure for revocation request

The practices involved in processing of a revocation request for online certificate application will be as prescribed in the following sub sections. When an End Entity originates the revocation request as per the Certificate Revocation/Suspension form as mentioned in section 9.2:

- The practices employed in processing the request will comply to the fullest extent possible with the practices that are described below;
- The reason for the request must be documented.

4.6.3.1 Processing by IDRBT CA

To process a revocation request initiated by an End Entity, IDRBT CA:

- receives the End Entity revocation request forwarded by RA
- revokes the certificate
- adds the certificate to its CRL in the LDAP Directory
- publishing in the repository
- informs subscriber about revocation of certificate by email

4.6.3.2 Processing by RA

To process a revocation request initiated by an End Entity, an RA

- receives and authenticates the request
- digitally signs and sends the revocation requests to IDRBT CA

4.6.4. Revocation Request Grace Period

Revocation requests are to be verified on receipt and action should be taken as rapidly as possible.

4.6.5. Circumstances for Suspension

Suspension can be described as placing a certificate on hold for a brief period. This is useful for investigation to be carried out as to the validity of the certificate when required. A Certificate is suspended when:

- Verification as to whether the certificate has been issued containing wrong or falsified information is in progress
- Soft copy of Revocation request signed by SA/RA is awaited
- Subscriber requests for suspension

4.6.6. Who can request Suspension

The subscriber shall request for the suspension of the certificate. The process of suspension can be initiated by IDRBT CA also. In case, SA/RA has any information regarding false representation or otherwise, SA/RA will inform IDRBT CA by using any communication means, based on which IDRBT CA will initiate suspension at its discretion.

4.6.7. Procedure of Suspension Request

In case of the online certificate application form, the RAs shall request for the certificate suspension in the same way as for the certificate revocation specified in the section 4.6.3 of this CPS.

To process a suspension request initiated by an RA, IDRBT CA:

- receives and authenticates the digitally signed request from the RA
- suspends the certificate
- adds the certificate to its CRL in the LDAP Directory
- publishing in the repository

4.6.8. Activation of Certificate after Suspension

- The activation request is to be made by the subscriber in the application form.
- Subscriber sends the duly signed application form to IDRBT CA by fax/speed post/courier for activation of certificate.
- IDRBT CA activates the certificate and publishes Certificate Revocation List (CRL).
- IDRBT CA will inform about activation of certificate to subscriber by email.

4.6.9. CRL issuance frequency

After the revocation request is received by IDRBT CA, the concerned certificate will be revoked as per the procedure of certificate revocation, at the earliest. The revoked certificate will be added to the CRL immediately as part of this revocation procedure. The latest CRL is available round the clock for downloading. In unforeseen circumstances the certificate will be revoked in not more than three working days after receiving the certificate revocation request.

On detection of serious key compromise, the corresponding digital certificate is revoked, CRL generated and published immediately.

The IDRBT CA shall update and issue the CRL whenever certificates are revoked or suspended or on the first working day of each month or 30 days after the last update or as and when necessary, whichever occurs first as per CCA guidelines.

But IDRBT CA will make every effort to publish new CRL in every last working day of the week.

IDRBT CA includes the CRL distribution point extension, in the form of a URL, in the issued certificates indicating where the CRL can be found.

4.6.10. CRL checking requirements

CRL checking is the responsibility of the relying party whenever a transaction takes place. IDRBT CA recommends that relying parties should check at least weekly, however where the value, the importance or sensitivity of a message, transaction or other file is high, it is recommended that the relying party checks on the transaction basis.

4.6.11. On-line revocation/ status checking availability

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.

4.6.12. On-line revocation checking requirements

Relying Party should check the status of a Certificate by consulting the most recent relevant CRL as mentioned in section 4.6.10.

4.6.13. Other forms of revocation advertisement available

No other forms of revocation advertisements are currently available. IDRBT CA will use the Directory services for CRL.

4.6.14. Checking requirements for other forms of revocation advertisements

Checking requirements for other forms of revocation is not required until OCSP is implemented.

4.6.15. Key compromise

After Key compromise the revocation process should be initiated.

4.7. Security Audit

The IDRBT CA maintains, and all approved RAs operating under IDRBT CA are obliged under contract to maintain, adequate records and archives of information pertaining to the operations of IDRBT CA PKI (Ref# IDRBTCA/DOC/ITP: Information Technology Policies and Procedures).

4.7.1. Types of event recorded for Audit

The IDRBT CA will archive the records in accordance to the standards specified in the IT Act.

Some important points among those include:

- Registration records, including records of rejected applications
- Certification generation requests, whether or not Certificate generation was successful
- Certificate issuance records, including CRL
- Revocation and suspension events
- Audit records, including security related events

4.7.2. Frequency of processing log

Frequency of processing log will be as per Security Guidelines to Certifying Authorities, Schedule III, Rules to Certifying Authorities by CCA.

4.7.3. Retention period of audit log

Retention period of audit log will be as per Security Guidelines to Certifying Authorities, Schedule III, Rules to Certifying Authorities by CCA.

4.7.4. Protection of audit log

Audit log will be securely protected as mentioned in chapter 5 and will be accessible only by authorized personnel of IDRBT CA.

4.7.5. Audit log backup procedures

Audit logs and audit summaries will be backed up in manual form.

4.7.6. Vulnerability Assessments

Vulnerability assessments will be as per Security Guidelines to Certifying Authorities, Schedule III, Rules to Certifying Authorities by CCA.

4.8. Records Archival

IDRBT CA and RAs operating under IDRBT CA maintains an archive of relevant records described in this policy.

4.8.1. Types of events recorded

Certificate Applications, Registration and verification documents of generated digital certificates, requests for key pair, key pair generation, certificate issue, notices of suspension,, information of suspended digital certificates, information of revoked digital certificates, expired digital certificates, Certificate Revocation Lists, backups, formal correspondence, and audit logs.

4.8.2. Retention period for archive

The retention period for archival will be for seven years from the commencement of IDRBT CA operations.

4.8.3. Protection of archive

Archive media is protected by physical security as mentioned in chapter 5.

4.8.4. Archive backup procedure

IDRBT CA has established archive back up procedures to ensure and enable complete restoration of current service in the event of disaster situation.

4.8.5. Requirements for time stamping of records

Trusted time synchronizing Time Stamping Service may be implemented in future as per CCA guidelines.

4.8.6. Archive collection system

IDRBT CA will establish an archive collection system that meets the requirements of this CPS.

4.8.7. Procedures to obtain and verify archive information

At the discretion of IDRBT CA, a fee will be charged for accessing archived information. This would be in line with the confidentiality terms mentioned in section 2.8. However, at its discretion, the higher entities in the hierarchy can verify the archives of the entities down the line.

4.9. Key changeover

IDRBT CA key pairs are withdrawn from service at the end of their respective maximum lifetimes as defined in Section 6.3.2. The procedures followed will be as per Security Policies and Procedures (Ref# IDRBTCA/DOC/SPP: Security Policies and Procedures). In case of change in IDRBT CA's key pair, the subscribers will be notified through website: http://idrbtca.org.in/.

Entities in the IDRBT CA Certification Services are issued IDRBT CA Digital Certificate for a specific period of time as per requirement. When the entity's private key expires, if required by him/her, a new key pair must be generated by him/her that shall be certified by IDRBT CA.

4.10. 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/DRP: Disaster Recovery and 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. Once in 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.

4.10.1. Computing resources, software, and/or data are corrupted

Using the backups and archives necessary software, hardware and databases shall be restored for functioning. In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to Review Committee and IDRBT CA's incident handling actions (Ref# IDRBTCA/DOC/ITP: Information Technology Policy and Procedures) are endorsed. Such procedures involve appropriate escalation, incident investigation, and incident response. If required, IDRBT CA's disaster recovery procedures will be implemented.

IDRBT CA maintains offsite backups of important CA information which includes, but is not limited to: application logs, database records for all certificates issued.

4.10.2. IDRBT CA key compromise

Upon the suspected or known Compromise of a IDRBT CA private key, IDRBT CA's disaster recovery procedures are enacted (Ref# IDRBTCA/DOC/DRP: Disaster Recovery and Business Continuity Plan).

In case of IDRBT CA key compromise IDRBT CA should:

- Inform subscribers and relying parties through website http://idrbtca.org.in/ .
- All certificates will be revoked and CRL will be generated as per Section 4.6.9.
- No new certificates will be generated with compromised key pair.
- IDRBT CA will generate a new key pair in accordance with Section 4.9, except where IDRBT CA is being terminated in accordance with Section 4.11.
- Subscribers need to reapply for getting new certificate after the notification by IDRBT CA.

4.10.3. Entity key is compromised

In the case of end entity key compromise:

- Inform the RA and relying parties
- Request the revocation of the end entity's certificate.

4.10.4. Secure facility after a natural or other type of disaster

IDRBT CA manages its backup, archive, and offsite storage in accordance with its backup policy, and contingency and recovery plan.

4.11. CA Termination

Before ceasing to act as a Certifying Authority, IDRBT CA shall:

- give notice to the Controller of its intention to cease acting as a Certifying Authority, ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of license;

- advertise sixty days before the expiry of license or ceasing to act as Certifying Authority, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;
- notify its intention to cease acting as a Certifying Authority to the subscriber and Cross Certifying Authority of each unrevoked or unexpired Digital Certificate issued by it, by giving notice of at least sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital Certificate, as the case may be;
- the notice will be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post;
- revoke all Digital Certificates that remain unrevoked or unexpired at the end of the ninety days notice period, whether or not the subscribers have requested revocation;
- make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Certificates;
- make reasonable arrangements for preserving the records for a period of seven years;
- pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Certificate) to subscribers for revoking the Digital Certificates before the date of expiry;
- after the date of expiry mentioned in the licence, IDRBT CA will destroy the certificate–signing private key and confirm the date and time of destruction of the private key to the Controller.

4.12. Cross Certification

Cross Certification is a condition in which either or both IDRBT CA and another certificate issuing entity (of another certification domain) issues a certificate having the other as the subject DN of that certificate.

IDRBT CA will undergo Cross-certification with other operating CAs as per the Rules and Regulations to Certifying Authorities, by CCA, Ministry of Communication and Information Technology.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

This Chapter deals with physical, procedural and personnel requirements and controls of the personnel, systems and workstations required for the certification process.

5.1. Physical Controls

The IDRBT CA operates within a secure physical environment within the office area that meets the standards of IT Security Guidelines of Rules to Certifying authorities by CCA. The IDRBT CA operates within a secure physical environment within the office area that meets the standards of IT Security Guidelines of Rules to Certifying authorities by CCA (Ref# IDRBTCA/DOC/ITP: Information Technology Policies and Procedures).

5.1.1. Site location and construction

IDRBT Site is located in secure premises. All the IT security guidelines in accordance with IT Act 2000 are followed.

5.1.2. Physical access

The physical access to the IDRBT CA would be restricted to the authorized personnel in operation. Entry and exit is logged. IDRBT has well established security system in place in which every visitor is logged in at the entrance and is monitored. The visitors will be accompanied by trusted personnel of IDRBT CA. The strong room is protected with Biometric access controls, smart card access controls and electro-magnetic cage.

RAs are obliged to, and do, protect physical, access to confidential registration records (Ref# IDRBTCA/DOC/RRA: Rules and Guidelines for RA Office).

End Entity should not leave their computers unattended when the private key is in use. The computer that contains private keys (encrypted on a hard disk) must be physically secured or protected with an appropriate access control product.

5.1.3. Power and air conditioning

Adequate facilities are provided. For power a backup generator is in place. All the systems are connected to the UPS. Protective measures have been provided to take care of power fluctuation.

5.1.4. Water exposures

IDRBT CA has taken adequate precautions to minimize the impact of water exposure to IDRBT CA systems.

5.1.5. Fire prevention and protection

All the measures have been taken to prevent the fire and protective measures are in place to face any eventuality. IDRBT employs appropriate safeguards to protect their secure operating area against fire through automatic fire detectors and fire extinguishers.

5.1.6. Media storage

All backup magnetic media would be stored within the premises of the IDRBT CA securely with a copy at offsite.

5.1.7. Waste disposal

IDRBT has got adequate and environmentally safe waste disposal arrangements. The paper waste and other material would be disposed in such a manner that no confidential information could be known, from the waste disposed. This will be according to the Information Technology Guidelines to Certification Authorities by CCA (Ref# IDRBTCA/DOC/SPP: Security Policies and Procedures).

5.1.8. Backup Policy

All the backups of software, databases and records will be stored with all the security measures.

There will be a backup in an offsite location based on the Disaster Recovery Policy.

5.2. Procedural Controls

5.2.1. Trusted roles

(Ref# IDRBTCA/DOC/TPL: Trusted Personnel List)

The operations at IDRBT CA shall be divided into number of split operations so that no single person will be able to take control of the total process.

This is achieved by creating separate roles in the IDRBT CA architecture, each of which has a limited amount of capability. All the roles assigned to the trusted persons are as per IDRBT CA Organizational Structure.

5.2.2. Number of persons required per task

The duties to be performed by each of the trusted personnel in the IDRBT CA Organizational structure are defined in such a manner that no single person would take control of the certificate issuance/revocation process.

5.2.3. Identification and authentication for each role

The persons filling the trusted roles must undergo an appropriate security screening procedure, described as per Human Resource Policy of IDRBT.

5.3. Personnel Controls

5.3.1. Background, qualifications, experience, and clearance requirements

The recruitment and selection practices of trusted personnel in IDRBT CA Organizational structure take into account the background, qualifications, experience, and clearance requirements of each position as per the Human Resource Policy of IDRBT.

5.3.2. Background check procedures

Background checks are conducted on all persons selected to take up a trusted role in accordance with the appropriate security screening procedure, prior to the commencement of their duties. If, any new person were recruited, all the background checks would be conducted to get a reliable and competent person.

5.3.3. Training requirements

The persons identified would have undergone adequate training to handle IDRBT CA Office/RA operations, understand PKI concepts, exposure to software and hardware of PKI, computer security, and operation of IDRBT CA and RA functions.

IDRBT will conduct programmes to train the RA personal before the commencement of RA Operations.

5.3.4. Retraining frequency and requirements

(Ref# IDRBTCA/DOC/SPP: Security Policy and Procedures)

Every year the IDRBT CA personnel would undergo skills up gradation training programs or whenever there is requirement due to the change or up gradation in the technology.

5.3.5. Job rotation frequency

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

5.3.6. Sanctions for unauthorized actions

Unauthorized actions are liable for strict disciplinary action. Anyone who abuses his position would loose authorization permanently. Action will be taken according to the laws pertained in the IT Act against those found dysfunctional.

5.3.7. Contracting personnel requirements

The people who would be contracted in IDRBT CA Office/RA would also be qualified and trustworthy professionals.

5.3.8. Documentation supplied to personnel

(Ref# IDRBTCA/DOC/CAM: CA Administration Manual)

The staff would be provided with all the guidelines and documents for performing various functions in IDRBT CA. Manuals of hardware and software, operational practice and procedural documents, including this CPS are also provided.

6. TECHNICAL SECURITY CONTROLS

This Chapter deals with the technical aspects related to key pair generation, protection, key pair management, activation data, computer security controls, life cycle technical controls, network security controls and cryptographic module engineering controls.

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

IDRBT CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. The CA Key pair will be generated and stored in accordance with FIPS 140-1 level 3 standards. The activities executed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for seven years as per IT Act.

The RA personnel will generate key pair and download certificate in smart card/hardware token.

In the case of end entity, the key pair should be generated preferably by the end entity and certificate to be installed by the end entity.

6.1.2. Private key delivery to entity

Subscribers' private keys (except encryption keys) are generated by them and required no delivery. Encryption Private Key generated by IDRBT CA will be delivered to the end entity in a secured manner.

6.1.3. Public key delivery to certificate issuer

Public keys are delivered to the certificate issuer by means of an on-line exchange utilizing functionalities of IDRBT CA software.

6.1.4. IDRBT CA public key delivery to users

Users have to retrieve the IDRBT CA's public keys by fetching IDRBT CA certificates from IDRBT CA website http://idrbtca.org.in/ .

The IDRBT CA public key will be made available by means that can be trusted by the users, protected in self–signed certificate, licenced by CCA.

6.1.5. Key sizes

The length of a private key must be at least 2048 bits. IDRBT CA cannot certify an entity key pair with key length less than 2048 bits.

Length of IDRBT CA key pair is 2048 bits.

6.1.6. Public key parameters generation

Whichever entity is generating the key pair i.e. RA or subscriber, its application will generate the parameters used to create public keys.

6.1.7. Parameter quality checking

The application software used by subscriber should check the quality of parameter in the case of key pair generation.

6.1.8. Hardware/software key generation

Keys can be generated by hardware or software as per the respective guidelines.

6.1.9. Key usage purposes

The purposes for which a key can be used may be restricted by IDRBT CA through the Key Usage extension (Refer section 7.1.2) in the certificate.

6.2. Private Key Protection

IDRBT CA has put into practice a combination of physical, logical, and procedural controls to ensure the security of private keys. Logical and procedural controls are described in this section. Physical access controls are described in Section 5.1.2. Subscribers are required to take essential precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1. Standards for cryptographic module

Cryptographic modules in use within the IDRBT CA comply with FIPS 140-1 level 3 standards.

6.2.2. Private key (n out of m) multi-person control

(Ref# IDRBTCA/DOC/CAM: CA Administration Manual)

IDRBT CA has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations.

IDRBT CA makes use of split passphrase needed to make use of a CA private key which are held by trained and trusted individuals called CA Coordinators. Two out of Eight multi-person control for particular hardware cryptographic module is required to activate a CA private key stored on the module.

6.2.3. Private key escrow

IDRBT CA will not escrow the private keys of IDRBT CA, RA and subscribers.

6.2.4. Private key backup

IDRBT CA creates backup copies of CA private keys for usual recovery and disaster recovery purposes. Backups of a private key of IDRBT CA will be

encrypted and stored by IDRBT CA. (Ref# IDRBTCA/DOC/SPP: Security Policies and Procedures)

End entity may back up its keys and store them in an encrypted file.

6.2.5. Private key archival

IDRBT CA key pair will be archived for a period for 7 years when it reaches the end of their validity period. Archived key pairs will be securely stored using hardware cryptographic modules that meet the requirements of Section 6.2.1 of CPS. The same will be securely destroyed in accordance with Section 6.2.9 upon the end of the archive period.

IDRBT CA does not archive copies of RA and Subscriber signing private keys.

6.2.6. Private key entry into cryptographic module

Private Key is generated onboard, stored in an encrypted form and remains in an encrypted form and it is decrypted only when it is used. When CA key pair is backed up to another hardware cryptographic module, such key pair is transported between modules in encrypted form.

6.2.7. Method of activating private key

In case of IDRBT CA, activation of Private Key shall require 2 out of 6 persons and will be from the cryptographic hardware device that follows FIPS 140-1 level 3 standards.

In case of subscriber, private keys are activated by the client application. Subscriber private key is activated by a PIN or password.

6.2.8. Method of deactivating private key

IDRBT CA private key is deactivated upon removal from the token reader.

RA and Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, subscribers have an obligation to adequately protect their private key(s) in accordance with Section 2.1.3.

6.2.9. Method of destroying private key

At the expiry of IDRBT CA's private key, remaining copies of the CA private key are securely destroyed after archival in accordance with Section 6.2.5. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods (Ref# IDRBTCA/DOC/SPP: Security Polices and Procedures). The same methods will be followed for destruction of private key in case of key compromise.

In case of a subscriber, for Smart card based keys, the private keys can be deleted by Personalization/Initialization of card/token.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

All certificates containing public keys (including IDRBT CA as well as its subscribers) are archived by the IDRBT CA upon expiry as part of IDRBT CA's routine backup procedures and kept for a period of seven years as per IT Act.

6.3.2. Usage periods for the public and private keys

In case of a subscriber, public and private keys can be used as long as a certificate is valid. Refer Section 2.10 for the validity period of Subscriber's certificate.

In case of IDRBT CA, the certificate validity period is 5 years.

6.4. Activation Data

6.4.1. Activation data generation and installation

After personalization, no activation data other than access control mechanisms (PIN) are required to operate cryptographic modules.

6.4.2. Activation data protection

Pass phrases or PIN shall not be accessible to anyone except the operator and the certificate holder.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

IDRBT CA has established security for both the hardware and software security systems according to the IT Security guidelines.

6.5.2. Computer security rating

As per the IT security standards in Rules for Certifying Authorities by CCA, security is provided.

6.6. Life Cycle Technical Controls

6.6.1. System development controls

Application development takes place in controlled environment. All quality control checks are conducted at regular frequency.

6.6.2. Security management controls

System security management is controlled by the privileges assigned to the trusted roles in the IDRB T CA Organizational Structure.

6.6.3. Life cycle security ratings

All potential life cycle security risks are observed and taken care.

6.7. Network Security Controls

IDRBT CA PKI has undergone extensive threat and risk assessments that identify and address all high or significant network security threats.

The RA will use a workstation that is connected to INFINET or Internet. The RA's environment must, however, be adequately secured from attacks originating from open network by applying adequate protection mechanisms.

6.8. Cryptographic Module Engineering Controls

IDRBT CA shall utilize hardware cryptographic modules rated FIPS-140-level 3 to perform all digital signing operations. All cryptographic module engineering security threats are assessed and addressed.

7. CERTIFICATE AND CRL PROFILES

This Chapter gives the rules related to the use of X.509 certificates and CRL.

7.1. Certificate profile

This section defines IDRBT CA's Certificate Profile and Certificate content for Digital Certificates issued under this CPS.

The Digital Certificates issued by IDRBT CA conform to "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999".

At a minimum, IDRBT CA X.509 Certificates contain the basic fields and indicated prescribed values or value constraints in Table 3 as below:

Field	*Value or Value constraint*
Version	V3 (Refer section 7.1.1.)
Serial Number	Number allocated to a certificate by the issuer CA, unique for a given issuer.
Signature Algorithm	Name of the algorithm used to sign the certificate (refer section 7.1.3)
Issuer DN	Refer section 7.1.4.
Valid From	Time from which the Certificate is valid. Encoded in accordance with RFC 2459.
Valid To	Time to which the Certificate is valid. The Certificates are valid for one year from the date of issue. Encoded in accordance with RFC 2459.
Subject DN	Refer section 7.1.4.
Subject Public Key	Encoded in accordance with RFC 2459 using algorithms specified in section 7.1.3 and key lengths specified in section 6.1.5.
Signature	Generated and encoded in accordance with RFC 2459

Table 3: Certificate Profile Basic Fields

7.1.1. Version number(s)

The version field in the certificate is V3, indicating X.509v3 certificates.

7.1.2. Certificate extensions

The following extensions are minimum extensions provided for the certificates issued by IDRBT CA as per this CPS.

7.1.2.1 Key Usage

Where X.509 Version 3 Certificates are used, IDRBT CA populates the Key Usage extension for the specific usage of the Digital Certificates.

The CA shall contain a key usage extension with KeyCertSign, CRLSign and Digital Signature. The criticality field of this extension shall be set to TRUE.

All the End Entity shall contain the following extension set as per the type of certificate.

- S/MIME (signing): This type of Certificate shall contain the key usage extension with Digital Signature, Non-repudiation and the extended key usage will have email protection (Secure Email).
- S/MIME (encryption): This type of Certificate shall contain the key usage extension with Key Encipherment and the extended key usage will have email protection (Secure Email).
- SSL Server: This type of Certificate will contain the key usage extension with Digital Signature and Key Encipherment. The extended key usage will have Server Authentication and Client Authentication.
- SSL Client: This type of Certificate will contain the key usage extension with Digital Signature and Non-repudiation. The extended key usage will have Client Authentication.
- Object Signing: This type of Certificate will contain the key usage extension with Non-Repudiation, Digital Signature, and the extended key usage will have code signing.

7.1.2.2 Certificate Policies Extension

The Value of the field contains the OID (Object Identifier) representing the RCAI (Root Certification of Authority of India) certificate policy the certificate is valid for, and all the lower levels certificate policies.

The end entity certificate contains User Notice qualifier "explicit text" encoded as IA5 string. The String states the highest Certificate Policy for which the certificate is valid for – as defined by the CCA.

7.1.2.3 Subject Alternative Names

Depending up on the type of certificates, Subject Alternative Name (SAN) will be email id, IP address or domain name. For end entity certificates, email address will be included and for machine certificates IP address as mentioned in RFC791 will be included in the form of Octet string in network byte order.

7.1.2.4 Basic Constraints

IDRBT CA populates X.509 Version 3 CA Certificates with a Basic Constraints extension with the Subject Type set to CA. For end entity certificate the field will not be present.

IDRBT CA X.509 Version 3 Certificates issued will have a Path Length Constraint field of the Basic Constraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. This field is set to "0". The critical field of these extensions shall be set to TRUE.

7.1.2.5 Enhanced Key Usage

IDRBT CA makes use of the Enhanced Key Usage extension for the specific types of X.509 Version 3 Certificates. The value of Object Identifier for the purpose for the certificate to be used is mentioned in this field.

7.1.2.6 CRL Distribution Points

IDRBT CA X.509 Version 3 Certificates use the CRL Distribution Points extension containing the URL of the location where a Relying Party can obtain a CRL to check the IDRBT CA Certificate's status.

7.1.2.7 Authority Key Identifier

IDRBT CA populates X.509 Version 3 Certificates with a Authority Key Identifier extension with the value same as the Subject Key Identifier value of RCAI. For end entity certificates the Authority Key Identifier value is the same as the Subject Key Identifier in the CA's own certificate.

7.1.2.8 Subject Key Identifier

Where IDRBT CA populates X.509 Version 3 Certificates with a Subject Key Identifier extension, the Key Identifier is based on the public key of the Subject of the Certificate generated. The Subject Key Identifier extension provides means of identifying certificates that contain a particular key when the subject has multiple certificates with multiple keys.

7.1.3. Algorithm Identifiers

The following hashing/digest algorithms are supported:

- Secure Hash Algorithm-2 (SHA-2)

The following padding algorithms are supported:

- PKCS# 1
- PKCS# 5

Encryption algorithms are classified into two classes, symmetric and asymmetric. The symmetric encryption algorithms being supported are:

- DES
- Triple DES

The asymmetric encryption algorithms being supported are:

- RSA
- DSA

7.1.4. Names forms

Name fields and extensions shall be consistent with section 3.2

7.1.5. Name Constraints

Anonymous and pseudo names are not supported.

7.1.6. IDRBT CA Certificate Profile

Version Number: *(version3)*

Serial Number:

Signature Algorithm: *(algorithm identifier)*

Issuer:

Validity

Not Before:

Not After:

Subject:

Subject Public Key Info:

Extensions: *(X509v3 Extensions)*

{

Basic Constraints:

(CA: TRUE/FALSE)

Subject Key Identifier:

Key Usage:

{

Digital Signature
Non-Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Key Cert Sign
CRLSign
Encipher only
Decipher only

}

Extended Key Usage

{

Extended Key Usage Syntax

Key Purpose ID

{

Server Authentication
Code Signing
Email Protection

}

}

Signature Algorithm: *(Algorithm Identifier)*

Signature Value:

7.2. CRL Profile

The CRL issued by IDRBT CA confirm to "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999".

At a minimum, IDRBT CA X.509 CRL contains the basic fields and indicated prescribed values or value constraints in Table 4 below:

Field	*Value or Value Constraint*
Version	Refer section 7.2.1.
Issuer Signature Algorithm	Algorithm used to sign the CRL. IDRBT CA CRL are signed using md5RSA in accordance with RFC 2459.
Issuer Distinguished Name	Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in section 7.1.4.
Effective Date	Issue date of the CRL. IDRBT CA CRL is effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of section 4.6.9.e
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 4: CRL Profile and Basic Fields

7.2.1. Version number(s)

X.509 CRL version 2 will be used.

7.2.2. CRL entry extensions

IDRBT CA uses x.509 Version 2 CRL entry extensions.

7.2.3. IDRBT CA CRL Profile

Version: (version 2)

Effective Date:

Issuer:

Next Update:

Revoked Certificates

{

User Certificate (Serial Number)

Revocation Date

Reason Code

{

Unspecified
Key Compromise
CA Compromise
Affiliation Changed
Superseded
Cessation of Operation
Certificate Hold
Remove from Certificate Revocation List

}

}

Signature Algorithm: (Algorithm Identifier)

Authority Key Identifier

Signature Value

8. SPECIFICATION ADMINISTRATION

This Chapter deals with the specification changes and the publication of this CPS in the IDRBT CA repository.

8.1. Specification Change procedures

Policy Approval Committee decides on the changes in this CPS and the corresponding procedural adjustments to be made. Substantial changes will require revision of this policy. It is at the discretion of IDRBT CA to determine the changes required if any, and whether a change is minor or substantial. In the case of major changes all the entities would be informed.

Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be published in the IDRBT CA Repository located at: http://idrbtca.org.in/. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

8.1.1. Items that can change without Notification

IDRBT CA reserves the right to amend the CPS devoid of notification for amendments that are not material, including without restraint corrections of typographical errors, changes to URLs, and changes to contact information. IDRBT CA's decision to designate amendments as material or non-material shall be within IDRBT CA's solitary prudence.

8.1.2. Items that can change with Notification

IDRBT CA shall make material amendments to the CPS in accordance with this section.

8.1.2.1 List of Items

Material amendments are those changes that IDRBT CA, under section 8.1.1, considered to be material.

8.1.2.2 Notification Mechanism

IDRBT CA's Policy Approval Committee will post amendments to the CPS in the IDRBT CA Repository, which is located at: http://idrbtca.org.in/.

8.2. Publication and notification

8.2.1. Items Not Published in the CPS

Security documents considered confidential by IDRBT CA are not revealed to the public. Confidential security documents include the documents identified in section 2.8.1 as documents that are not available to the public.

8.2.2. Distribution of the CPS

This CPS is published in electronic form within the IDRBT CA Repository at http://idrbtca.org.in/. The CPS is available in the IDRBT CA Repository in Adobe Acrobat pdf, and HTML. IDRBT CA also makes the CPS available in Adobe Acrobat pdf upon request sent to cahelp@idrbt.ac.in. The CPS is available in paper form from IDRBT CA upon requests sent to: IDRBT CA, IDRBT, Castle Hills, Road No: 1, Masab Tank, Hyderabad-500057, India.

8.3. CPS approval procedures

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 Information Technology, Government of India.

9 APPENDIX

9.1 Subscriber Application Form

APPLICATION FORM FOR ISSUE OF DIGITAL CERTIFICATE	
Important Notice • * Fields are mandatory • Strike off which are not applicable • Subscriber agreement if required should be submitted along with this application form • This application form is to be filled by the applicant. • All subscribers are advised to read IDRBT CA Certificate Practice Statement (download from http://idrbtca.org.in/) • Copy of identification document should be attached with this application form. • Application form must be submitted in person to the Registration Authority/ IDRBT CA for face-to-face recognition in the case of Class 3 Certificate. • Incomplete/Inconsistent application is liable to be rejected.	

Name of the Organization*		
Bank in which subscriber has account*		
New/ Renewal	**User- ID(in case of Renewal**	

Class of Certificate *:	Certificate for *:	Application *:	Applicant Type*:	Type of Digital Certificate*:
Class 1□ Class 2□ Class 3□	Individual □ Server □ Web server □	SFMS □ RTGS □ Others (Please specify)	Bank Employee/ Officer (Online) □ RA Official (Online) □ Banks Customer (Offline) □	Signing □ Encryption □ System □ Web Server (SSL) □ Object Signing □

PERSONAL DETAILS			
Name*:		**Sex*:**	**Male** □ **Female** □
Email Address*:			
Address for Communication*:			
	Pin Code*:	**Telephone*:**	
Date of Birth*:		**Mobile:**	
Identification Details*: **(Valid and not expired)**	**Any one of : Passport No/PAN Card No/Voter's ID Card No/Driving License No/PF No/Employee ID**		
Bank Details*:	**Bank & Branch Name**		
	Bank Branch Address		
	Bank Account No.		
	Type of Bank Account		

CERTIFICATE REQUEST DETAILS	
The following details will be reflected in the certificate. **Make sure that these details match with those given to generated request using certificate request generation tool or any other PKCS#10 request generation tool. If necessary, contact your application provider for these before filling the form.**	
Common Name*: **(Name of the person, server name, Registered domain name, IFSC code etc)**	
Email*: **(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: Andhra Pradesh)**	
Country*	**India**

Signature of Superior Authority

Signature of 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 in respect of Class 2 and Class 3 Certificates and FIPS 140-1/2 Level 1 validated cryptographic modules in respect of Class 1 Certificates 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 for publishing of 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/REGISTRATION AUTHORITY 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.

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/ operator

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 purposes 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 making this application, he/she is consenting to certificate issue in the event the application is accepted
7. Agrees for publishing of 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 IDRBTCA 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 changes in the information contained herein above. I am submitting this application as an authorized official 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 purpose.

Date:

Place:

Name of the RA official Signature of the RA Official

FOR RA/ IDRBT CA PURPOSE ONLY

Checklist	Date & Time	Initials
Received the application form for digital certificate?		
Verified the photocopies of the identification document (in case of Class 2 Certificate) (Passport/Voter's Identity Card/PAN Card/Domain registration)?		
Verified the identification documents in case of Class 3 Certificate (Passport/Voter's Identity Card/PAN Card/Domain registration)?		
Collected the PKCS#10 request for Secure Web Server Certificate?		
Face-to-Face verification? (in case of Class 3 Certificate)		

CONTACT ADDRESS

IDRBT Certifying Authority,
Road No. 1, Castle Hills, Masab Tank, Hyderabad – 500 057, India
Phone : +91 40 23534981/ Fax: +91 40 23535157
Email: cahelp@idrbt.ac.in
Website: http://idrbtca.org.in/

9.2 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 / Web server / Client / Object 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
Please send the duly filled in request form to: IDRBT Certifying Authority, Road No. 1, Castle Hills, Masab Tank, Hyderabad – 500 057 India Phone/Fax: +91 40 23536297 Email: cahelp@idrbt.ac.in Website: http://idrbtca.org.in/

9.3 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 http://idrbtca.org.in/repository.html and http://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 Web Server 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, if a key pair is compromised, by a paper document 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:

9.4 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 have 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 http://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 http://idrbtca.org.in/repository.html and

http://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 http://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 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:

	Liability Caps
Class 1	Rs 20/-
Class 2	Rs 250/-
Class 3	Rs 10000/-

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.

9.5 Document Master List

The following are the documents in scope of this CPS available for IDRBT CA Operations and Public Key Infrastructure.

Document Index	Document Name
IDRBTCA/DOC/CAM	CA Administration Manual
IDRBTCA/DOC/CPS	IDRBT CA CPS
IDRBTCA/DOC/DRP	Disaster Recovery Plan
IDRBTCA/DOC/IDD	Integration Design Document
IDRBTCA/DOC/INS	Installation Document
IDRBTCA/DOC/ITC	Integration Test Cases
IDRBTCA/DOC/ITP	Information Technology Policies and Procedures
IDRBTCA/DOC/NDS	Certificate Practices for PDO NDS Subscribers
IDRBTCA/DOC/RRA	Rules and Guidelines for RA Office
IDRBTCA/DOC/RTG	Certificate Practices for RTGS Subscribers
IDRBTCA/DOC/SPP	Security Policies and Procedures
IDRBTCA/DOC/SRS	Software Requirement Specification
IDRBTCA/DOC/STC	System Test Cases
IDRBTCA/DOC/STP	Standards and Procedures
IDRBTCA/DOC/TPL	Trusted Personnel List
IDRBTCA/DOC/URD	User Requirement Document
IDRBTCA/DOC/UTC	Unit Test Cases

10 GLOSSARY

Applicant

An Applicant is a person, entity, or organization that has applied for, but has not yet been issued an IDRBT CA Digital Certificate.

Asymmetric Crypto System

A system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Audit

A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analyzing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.

Audit Trail

A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

Authentication

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit.

Authorization

The granting of rights, including the ability to access specific information or resources.

Backup

The process of copying information, data and software for the purpose of recovering essential processing back to the time the backup was taken.

Certificate

A Digital Certificate issued by Certifying Authority.

Certificate Expiration

The time and date specified in the Digital Certificate when the operational period ends, without regard to any earlier suspension or revocation.

Certificate Issuance

The actions performed by a Certifying Authority in creating a Digital Certificate and notifying the Digital Certificate applicant (anticipated to become a subscriber) listed in the Digital Certificate of its contents.

Certificate Revocation

The process of permanently ending the operational period of a Digital Certificate from a specified time forward.

Certificate Revocation List (CRL)

A periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital Certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked Digital Certificates' serial numbers, and the specific times and reasons for suspension and revocation.

Certificate Serial Number

A value that unambiguously identifies a Digital Certificate generated by a Certifying Authority.

Certificate Signing Request (CSR)

A machine-readable form of a Digital Certificate application.

Certificate Suspension

A temporary "hold" placed on the effectiveness of the operational period of a Digital Certificate without permanently revoking the Digital Certificate. A Digital Certificate suspension is invoked by, *e.g.*, a CRL entry with a reason code.

Certifying Authority (CA)

A person who has been granted a license to issue a Digital Certificate under Information Technology Act prescribed by the Ministry of Communication and Information Technology, Government of India.

Certification Practice Statement (CPS)

A statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Certificates.

Certificate Class

A Digital Certificate of a specified level of trust.

Compromise

A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.

Confidentiality

The condition in which sensitive data is kept secret and disclosed only to authorized parties.

Confirm

To ascertain through appropriate inquiry and investigation.

Correspond

To belong to the same key pair.

Cryptographic Algorithm

A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.

Data Integrity

A condition in which data has not been altered or destroyed in an unauthorized manner.

Digital Certificate Application

A request from a Digital Certificate applicant (or authorized agent) to a Certifying Authority for the issuance of a Digital Certificate.

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 the Information Technology Act prescribed by the Ministry of Communication and Information Technology, Government of India.

Digital Certificate

Means a Digital Certificate issued under the Information Technology Act prescribed by the Ministry of Communication and Information Technology, Government of India.

Distinguished Name

A set of data that identifies a real-world entity, such as a person in a computer-based context.

Encryption

The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

Extensions

Extension fields in X.509 v3 certificates.

Generate a Key Pair

A trustworthy process of creating private keys during Digital Certificate application whose corresponding public keys are submitted to the applicable Certifying Authority during Digital Certificate application in a manner that demonstrates the applicant's capacity to use the private key.

Identification / Identify

The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of certificates.

Identity

A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.

Key

A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

Key Generation

The trustworthy process of creating a private key/public key pair.

Key Management

The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

Key Pair

In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

Master Agreement

The agreement executed between a Bank/Financial Institution/Government Agency who want to become a Registration Authority and IDRBT CA for the provision of designated public certification services in accordance with this Certification Practice Statement.

Message

A Digital Representation of Information; A Computer-Based Record. A Subset of Record.

Name

A set of identifying attributes purported to describe an entity of a certain type.

Non-repudiation

Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent.

Operational Period

The period starting with the date and time a Digital Certificate is issued (or on a later date and time certain if stated in the Digital Certificate) and ending with the date and time on which the Digital Certificate expires or is earlier suspended or revoked.

Personal Presence

The act of appearing (physically rather than virtually or figuratively) before a Certifying Authority or its designee and proving one's identity as a prerequisite to Digital Certificate issuance under certain circumstances.

PKI (Public Key Infrastructure)

A set of policies, processes, server platforms, software and workstations used for the purpose of administering Digital Certificates and public-private key pairs, including the ability to generate, issue, maintain, and revoke public key certificates.

PKI Hierarchy

A set of Certifying Authorities whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior Certifying Authority.

Private Key

The key of a key pair used to create a digital signature.

Public Key

The key of a key pair used to verify a digital signature and listed in the Digital Certificate.

Public Key Cryptography

A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

Record

Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form.

Rely / Reliance

To accept a digital signature and act in a manner that could be detrimental to oneself were the digital signature to be ineffective.

Relying Party

A Relying Party is a person, entity, or organization that relies on or uses a CA Digital Certificate.

Renewal

The process of obtaining a new Digital Certificate of the same class and type for the same subject once an existing Digital Certificate has expired.

Repository

A database of Digital Certificates and other relevant information accessible on-line.

Security

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative.

Sign

To create a digital signature for a message, or to affix a signature to a document, depending upon the context.

Signer

A person who creates a digital signature for a message, or a signature for a document.

Subscriber

A Subscriber is a person, entity, or organization that has been issued an IDRBT CA Digital Certificate.

Subscriber Agreement

The agreement executed between a subscriber and IDRBT CA for the provision of designated public certification services in accordance with this Certification Practice Statement.

Subscriber Information

Information supplied to a certification authority as part of a Digital Certificate application.

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.

Transaction

A computer-based transfer of business information, which consists of specific processes to facilitate communication over global networks.

Trust

Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a Certifying Authority. An authenticating entity must be certain that it can trust the Certifying Authority to create only valid and reliable Digital Certificates, and users of those Digital Certificates rely upon the authenticating entity's determination of trust.

Trusted Position

A role that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Digital Certificates, including operations that restrict access to a repository.

Trusted Third Party

In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee.

Trustworthy System

Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Valid Certificate

A Digital Certificate issued by a Certifying Authority and accepted by the subscriber listed in it.

Validate a Certificate

The process performed by a recipient or relying party to confirm that an end-user subscriber Digital Certificate is valid and was operational at the date and time a pertinent digital signature was created.

Validation

The process performed by the Certifying Authority following submission of a Digital Certificate application as a prerequisite to approval of the application and the issuance of a Digital Certificate.

X.509

The ITU-T (International Telecommunications Union-T) standard for Digital Certificates. X.509 v3 refers to certificates containing or capable of containing extensions. X.509 v2 refers to certificate revocation list (CRL).