# CERTIFICATE PRACTICES FOR OFFLINE USERS

*IN SUPPORT OF IDRBT CA'S OFFLINE USER CERTIFICATION SERVICES*

**VERSION 1.2**

**(IDRBTCA/DOC/CPO/1.2)**

**DATE OF PUBLICATION: OCTOBER 24, 2005**

IDRBT, CASTLE HILLS, ROAD NO: 1,
MASAB TANK,
HYDERABAD – 500 057
ANDHRA PRADESH, INDIA
PH: +91 40 23534981 FAX: +91 40 23535157
EMAIL: idrbtca@idrbt.ac.in

# IDRBT CA OFFILINE USER CERTIFICATION PRACTICES

## (USER CP)



| | |
|---|---|
| Document Name | IDRBTCA/DOC/CPO/1.2 |
| Release | Version 1.2 |
| Status | Release |
| Issue Date | October 24, 2005 |

## Amendment Certificate

| RELEASE | | | |
|---|---|---|---|
| **Version No.** | **Description** | **Approved by** | **Approval date** |
| IDRBTCA/DOC/CPO/1.0 | First Release | PAC | 15/07/2004 |
| IDRBTCA/DOC/CPO/1.1 | Amendments on first release include:<br>• Certificate issuance process change<br>• Certificate suspension process change<br>• Certificate revocation process change<br>• Superior Authority role and responsibilities redefined<br>• Identification and supporting documents updated<br>• Certificate Application form changed<br>• Certificate revocation/suspension/activation form updated | do | 12/08/2004 |
| IDRBTCA/DOC/CPO/1.1 | Amendments on second release include:<br>• Para 4.2.1 included for facilitating spread sheet preparation for RA | do | 24/10/2005 |

# 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 Digital Certificate applicant
- "CA" refers to the Certifying Authority licensed 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
- "CPS" means the IDRBT CA Certification Practice Statement
- "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
- "Entity" refers to the users of the Digital Certificate

- “End Entity” refers to any entity who is the end user of IDRBT CA Digital Certificates
- "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
- "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
- “Registration Authority” of “RA” means an entity trusted under IDRBT CA Hierarchy and has the right to verify the credentials of the applicant/subscriber before putting his digital signature and forwarding it to IDRBT CA for issuance of certificate.
- "Subscriber" means a person in whose name the Digital Signature Certificate has been issued
- “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 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.
- “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 Subscriber Agreement.
- “verification of credentials” means the checking of the identification and supporting documents by the SA or RA as mentioned in the appropriate

sections of this document before applying his digital signature on the certificate request.

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

## LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ***CA*** | Certifying Authority |
| ***CPS*** | Certification Practice Statement |
| ***CRL*** | Certificate Revocation List |
| ***CSR*** | Certificate Signing Request |
| ***DN*** | Distinguished Name |
| ***HTTP*** | Hypertext Transfer Protocol |
| ***HTTPS*** | Hypertext Transfer Protocol with SSL |
| ***IDRBT*** | Institute for Development and Research in Banking Technology |
| ***IT*** | Information Technology |
| ***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 |
| ***SA*** | Superior Authority |
| ***S/MIME*** | Secure Multipurpose Internet Mail extensions |
| ***SSL*** | Secure Sockets Layer |
| ***URL*** | Uniform Resource Locator |
| ***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) was setup by Reserve Bank of India (RBI) and is an autonomous body to carry out Research and Development in Banking Technology. IDRBT has established the Indian Financial Network (INFINET) based on VSAT and Leased Line Technologies. INFINET is a countrywide communication backbone for the Banks and Financial Institutions for payment system.

IDRBT is the licensed Certifying Authority having obtained the license for operation from the Controller of Certifying Authorities (CCA), Ministry of Communication and Information Technology, Government of India. IDRBT CA offers Certification Services for individuals from the public domain under IDRBT CA CPS.

IDRBT CA Certification Services are designed to support secure electronic transactions, digital signatures and other general security requirements of users. To accomplish this, IDRBT CA serves as a Trusted Third Party (TTP), licensed by CCA, issuing, managing, renewing and revoking certificates in accordance with published practices.

For more information refer the website: http://idrbtca.org.in/

### 1.1.1. Purpose of User CP

IDRBT CA Offline User Certification Practices (User CP) presents the practices in use by IDRBT CA, Registration Authority, Superior Authority and Subscribers 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, to registering subscribers. This CP provides practices for issuing, managing, using, suspending, re-activating, and revoking of certificates.

This document gives information regarding the User CP. This document is available at the website:

http://idrbtca.org.in/

### 1.1.2. Certificates classes and types issued

This CPS supports the operation of:

- All classes and types of IDRBT CA End Entity Certificates nominated in respective Certification Services (mentioned in detail in section 2.4)

## 1.2. Community and applicability

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

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

Customers and employees of Public sector banks, Private sector banks, Financial Institutions (FIs), Foreign banks recognized by Reserve Bank of India in the country and individuals recommended by Superior Authority (see Glossary). Government of India and various State Governments as part of e-governance are initiating electronic transactions for their legacy applications which will integrate Public Key Infrastructure (PKI). IDRBT CA will also issue digital certificates for those who will require digital certificate to participate in such government projects.

### 1.2.1. End Entities

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

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

***Relying parties*** – A Relying Party is a person, or organization that relies on or uses a Digital Certificate issued by IDRBT CA and/or any other information provided in a 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.

### 1.2.2. Applicability

The purpose of this User CP is to provide reliable information to subscribers and to the relying parties. Certificates are issued with the intention that they can be used for purposes like authentication, integrity, confidentiality and non-repudiation. The digital certificates will be issued for signing, encryption, web server, client and object signing purposes.

## 1.3. Contact details

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

## 1.4. Amendment Procedure

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

# 2. GENERAL PROVISION

This Chapter describes the obligations, liabilities and responsibilities of the various entities of the IDRBT CA Public Key Infrastructure (PKI) hierarchy.

## 2.1. Obligations

### 2.1.1. CA obligations

IDRBT CA discharges its obligations as per IDRBT CA CPS as published in IDRBT CA's website: http://idrbtca.org.in/

### 2.1.2. RA obligations

The RAs under IDRBT CA discharges its obligations as per IDRBT CA CPS as published in IDRBT CA's website: http://idrbtca.org.in/

### 2.1.3. Subscriber obligations

Subscriber discharges 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 specified in IDRBT CA CPS.
- Provide the SA/RA 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 sending the completed and signed Certificate Acceptance form.
- Use certificates in accordance with the purpose for which they are issued.
- Prove possession of private keys and establishing their right to use.
- Report IDBRT CA of any error or defect in their certificates immediately or of any subsequent changes in the certificate information.
- Study IDBRT CA CPS before using their Certificates.
- Inform IDBRT CA immediately, if a key pair is compromised, by Certificate Revocation/Suspension/Activation form.
- 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.
- Get a new certificate on their own after expiry, if required.

### 2.1.4. 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.

## 2.2. Superior Authority Responsibilities

- Accept a certificate request from an end entity.
- Collect and verify the relevant document for the corresponding certificates from applicant/subscriber.

- Digitally sign the certificate request of applicant/subscriber
- Send the application form and the certificate requests to IDRBT CA for issuance.
- Maintain the audit trail of the verification process.

## 2.3. Interpretations and Enforcement

### 2.3.1. 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 Communication and Information Technology, Government of India shall govern the enforceability, construction, interpretation, and validity of IDRBT CA CPS, irrespective of the contract or other choice of legal provisions and with out the requirement to establish a commercial nexus.

### 2.3.2. Dispute resolution procedures

Dispute resolution between IDRBT CA, RA, the Subscribers, and the Relying parties will be as per IDRBT CA CPS as published in IDRBT CA's website: http://idrbtca.org.in/.

## 2.4. Fees

The fees for services provided by IDRBT CA in respect of IDRBT CA Certificates are set forth in the IDRBT CA website. This may include administrative changes as specified by IDRBT CA Policy Approval Committee. These fees are subject to change, and any such changes shall become effective immediately after posting in the IDRBT CA Repository. Please visit the IDBRT CA website for the latest fee structure for different Class of Certificates at:

http://idrbtca.org.in/

## 2.5. Classes of Certificate

IDRBT CA supports three distinct certificate classes within its Certification services. IDRBT CA reserves the right to introduce more classes than what has been specified herein and IDRBT CA 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.

### 2.5.1. 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 environments. Class 1 Encryption Certificates are used for e-mail purposes.

In case of offline certificate request for Class 1 Certificate, the applicant/subscriber submits the application form and certificate request to IDRBT CA after verification of identification by Superior Authority. Superior Authority has the right to reject the certificate request if he finds the application is not meeting the criteria.

The validity period of Class 1 Certificates is two years.

**Assurance level:** For Class 1 Certificates the verification of the certificate request 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.

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.

### 2.5.2. Class 2 Certificates

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

In case of offline certificate request for Class 2 Certificate, the applicant/subscriber submits the application form along with identification documents and certificate request to IDRBT CA after verification of identification documents by Superior Authority. Superior Authority has the right to reject the certificate request if he finds the application is not meeting the criteria.

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

The Class 2 Certificate is use 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.

### 2.5.3. 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 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.

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.

In case of offline certificate request for Class 3 Certificate, the applicant/subscriber personally submits the application form along with identification documents and certificate request to RA. RA 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.

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 technical and 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.

## 2.6. Types of Certificates

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

### 2.6.1. 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.

### 2.6.2. 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 is communicated to subscriber 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.

### 2.6.3. 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.

### 2.6.4. 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.

### 2.6.5. 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, JavaScripts, plugins, 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. End Entity Initial Registration

#### 3.1.1.1 Identity Verification

The practices described in this section apply to all applicants making their initial application for a certificate and any subsequent application for a new certificate under IDRBT CA CPS. The identity verification process is to:

- be attended by end entity in person (based on the Class of Certificate)
- be conducted by a Superior Authority or Registration Authority as the case may be.
- perform the following functions:
  - Collection of Certificate information
  - Proof of other material Certificate information

## 3.2. Initial Registration

### 3.2.1. Need for names to be meaningful

Subscribers' 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) that is the unique name of the subscriber.
- Organization (O).
- Organizational Unit (OU), which is used to distinguish various organizational groups in the same organization.

- City or Locality (L), which represents the City where the organization is located.
- State (S), which represents the State the organization is located.
- Country(C), which is the two-letter identifier for the country to which the subscriber belongs.
- Email (E), is the email address of the subscriber.
- The Country , and Organization (O) are added as "IN" and "India PKI" respectively as per the CCA guidelines. Beneath this IDRBT CA follows its naming convention of adding one Organizational Unit (OU) indicating the Class of Certificate.

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

CN= Name of applicant/subscriber/server

E= name@company.com

O= Name of company/organization

O= India PKI

OU= Name of department/organizational unit

OU= Class x* Certificate

L= Name of Locality or City

S= Name of State

C=IN

(* x denotes either 1, 2 or 3)

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.

### 3.2.2. 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.

## 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 records has not been changed.
- 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.

## 3.5. 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.

# 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 offline certificate applicants/subscribers needing 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, which contains the public key of this pair, to IDRBT CA

### 4.1.1. Key Generation and Protection

An offline certificate applicant shall securely generate his/her own signing key pair using a utility provided by IDRBT CA and acknowledges that he/she will take necessary precautions to prevent its compromise, loss, disclosure, modification, or unauthorized use through Subscriber Agreement (refer Section 5.2).

### 4.1.2. Certificate Application Information and Communication

Certificate application information and the documents to be furnished along with the application include the items listed in the following Table 1.

| Class of Certificate | Information to be furnished in the application form | Documents to be furnished |
|---|---|---|
| **Class 1** | *Individuals:*<br>• Full Name<br>• Address for communication<br>• Sex<br>• Date of Birth<br>• Email Address<br>• Identification details of either Passport, Voter's ID Card, Income Tax PAN Card, Driving License or | Letter of the subscriber's higher authority in the organization and letter from officer in the bank branch where he has account |

| | | |
|---|---|---|
| | Employee Photo ID Card containing staff code, PF No. etc.<br>• Bank details | |
| **Class 2** | ***Individuals:***<br>• Same as Class 1 | Attested (officer in the bank branch) Photocopies of any of the documents<br>• Passport<br>• Voter's ID Card<br>• PAN Card<br>• Driving License<br>• Employee Identification Card issued by the Organisation (in case of employees of banks/FIs)<br>+<br>Letter of the subscriber's higher authority in the organization and letter from officer in the bank branch where he has account |

| | | |
|---|---|---|
| **Class 3** | ***Individuals:***<br>Same as Class 2 | Original copies of any of the documents<br>• Passport<br>• Voter's ID<br>• PAN Card<br>• Driving License<br>• Employee Identification Card issued by the Organisation (in case of employees of banks/FIs)<br>(to be furnished and physical presence before RA for personal verification)<br>+<br>Letter of the subscriber's higher authority in the organization and letter from officer in the bank branch where he has account |
| | ***Web Server Certificate:***<br>Same as Class 2 (details of the authorized representative), plus<br>The URL to which the server authentication is needed. | Same as those mentioned in Class 3 Individual<br>+<br>Details of the domain registration<br>(to be furnished and physical presence before RA for personal verification)<br>+<br>PKCS#10 format Certificate Request generated from the Server |

| | | |
|---|---|---|
| | ***Object Signing:***<br>Same as Class 2 (details of the authorized representative | Same as those mentioned in Class 3 Individual<br>+<br>Company/Firm details including:<br>• Registration Number of the Company/Firm<br>• Date of Incorporation/Agreement<br>• Particulars of Business<br>• Turnover in the last financial year |

Table 1: Required Certificate Request Application

#### 4.1.2.1 Signing Certificate

1. The subscriber fills the application form for digital certificate as per the section 5.1.
2. Subscriber fills the subscriber agreement as section 5.2 on Rs. 10/- non-judicial stamp paper.
3. The application form should be attached with an attested copy of photo identification document as mentioned in Table 1. The document should be attested by the officer in the bank branch.
4. The subscriber creates the certificate signing request (CSR) using the utility provided by IDRBT CA. The private key file will be stored in smart card, token, browser or hard disk. The following information will be required for creating request:
   - Common Name (Name as to be displayed in certificate)
   - Email address
   - Organisation or Company
   - Organisational Unit or Department
   - Locality or City

- State
- Country

5. In case of Class 1 or 2 certificates, Subscriber copies the CSR on media and submits the same along with the duly filled application form, identification and supporting documents if any, and subscriber agreement to the Superior Authority. The SA will check the identification and supporting document of the subscriber and will sign the application form by affixing his official stamp on the same. SA will digitally sign the certificate request using the utility given by IDRBT CA.
6. In case of Class 3 certificate, subscriber physically presents before RA along with the CSR on media, duly filled application form, identification and supporting documents, and subscriber agreement. The RA will check the identification and supporting document of the subscriber and will sign the application form by affixing his official stamp on the same. RA will digitally sign the certificate request using the utility given by IDRBT CA.
7. SA or RA as the case may be, then forwards the duly filled application form, subscriber agreement, identification and supporting document and soft copy of digitally signed certificate request in media by post/courier to IDRBT CA.
8. IDRBT CA generates the certificate and sends by email to subscriber.
9. Subscriber loads the certificate to smart card/token/browser/hard disk.
10. After getting certificate subscriber has to accept certificate as per section 5.4 by signing on paper and faxing and couriering it to IDRBT CA.
11. IDBRT CA publishes the certificate in LDAP repository.

#### 4.1.2.2 Encryption Certificate

The subscriber should have signing certificate before getting encryption certificate. In case if he is applying along with the signing certificate request, he should load the signing certificate to smart card/token/browser/hard disk before loading encryption certificate.

Note: Separate application form is not required to be submitted if the subscriber submits the signing and encryption requests together. If he is submitting it separately, he should follow steps 1 to step 3 as mentioned in previous section 4.1.2.1.

1. The subscriber creates the certificate encryption request using the utility provided by IDRBT CA. The following information will be required for creating request:
   - Common Name (Name as to be displayed in certificate)
   - Email address
   - Organisation or Company
   - Organisational Unit or Department
   - Locality or City of domicile
   - State
   - Country
2. In case of Class 1 or 2 certificates, Subscriber copies the encryption request on media and submits the same along with the duly filled application form, identification and supporting documents if any, and subscriber agreement to the Superior Authority. The SA will check the identification and supporting documents of the subscriber and will sign the application form by affixing his official stamp on the same. SA will digitally sign the certificate request using the utility given by IDRBT CA.
3. In case of Class 3 certificate, subscriber physically presents before RA along with the encryption request on media, duly filled application form, identification and supporting documents, and subscriber agreement. The RA will check the identification and supporting document of the subscriber and will sign the application form by affixing his official stamp on the same. RA will digitally sign the certificate request using the utility given by IDRBT CA.
4. SA or RA as the case may be, then forwards the duly filled application form, subscriber agreement, identification and supporting document and soft copy of digitally signed certificate request in media by post/courier to IDRBT CA.

5. IDRBT CA issues the encryption certificate and encrypts it with subscriber's signing public key and e-mails it to subscriber.
6. Subscriber uses the utility provided by IDRBT CA to load the certificate by decrypting with signing private key.
7. After getting certificate subscriber has to accept certificate by signing on paper and faxing and couriering it to IDRBT CA.
8. IDBRT CA publishes the certificate in LDAP repository.

#### 4.1.2.3 Web Server/Client/Object Signing Certificate

1. The subscriber fills the application form for digital certificate as per the section 5.1.
2. Subscriber fills the subscriber agreement as section 5.2 on Rs. 10/- non-judicial stamp paper.
3. The application form should be attached with an attested copy of photo identification document of either Passport, Voter's ID card, PAN Card or Driving License. The document should be attested by officer of the bank branch.
4. The subscriber creates the certificate signing request using the utility provided by application.
5. Subscriber physically presents before RA along with the CSR on media, duly filled application form, identification and supporting documents, and subscriber agreement. The RA will check the identification and supporting documents of the subscriber and will sign the application form by affixing his official stamp on the same. RA will digitally sign the certificate request using the utility given by IDRBT CA.
6. RA then forwards the duly filled application form, subscriber agreement, identification and supporting document and soft copy of digitally signed certificate request in media by post/courier to IDRBT CA.
7. IDRBT CA generates the certificate and e-mails it to subscriber.

8. Subscriber uses the utility provided by application to load the certificate.
9. After getting certificate subscriber has to accept certificate by signing on paper and faxing & couriering it to IDRBT CA.
10. IDBRT CA publishes the certificate in LDAP repository.

## 4.2. Validation of Certificate Requests

After the receipt of the Certificate request, the Superior Authority or RA as the case may be shall perform all required validations as the precondition to certificate issuance.

The Superior Authority or RA as the case may be shall validate that

- The certificate applicant/subscriber has agreed to the terms and conditions as stated in IDRBT CA CPS according to subscriber agreement
- The certificate applicant is the person identified in the request
- The identification and supporting documents are authentic
- The information listed in the certificate request is accurate

### 4.2.1 Maintenance of Records by RA

RA will maintain a spreadsheet (e.g MS Excel) in the format prescribed in Appendix 5.5. This spreadsheet file, which contains all signed certificate requests in the batch, is to be mailed to IDRBT CA (cahelp@idrbt.ac.in) for certificate issuance by CA. Fields such as date of certificate download, certificate serial number etc. need to be updated by RA on receipt of certificates generated from IDRBT CA.

## 4.3. Certificate Acceptance

IDRBT CA will provide an opportunity for the subscriber to verify the contents of the Digital Certificate before it is accepted. After getting certificate subscriber has to accept the certificate by signing Certificate Acceptance / Non-acceptance form as per section 5.4 and send it to IDRBT CA by fax or post. The certificate will be published in IDBRT CA repository after the acceptance.

## 4.4. Certificate Usage

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

### 4.4.1. S/MIME Encryption

The sender can use the IDRBT CA Encryption Certificates after verifying the key usage extension 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.

### 4.4.2. S/MIME Signing

The subscriber shall use Signing Certificate 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.

### 4.4.3. Object Signing

The subscriber can use Object signing certificate 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.

### 4.4.4. 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.

### 4.4.5. SSL Client

The Subscriber shall use Client Certificate for use in Secure Sockets Layer (SSL) communication between the browser (client) and the Web servers.

## 4.5. 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. 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/

### 4.5.1. 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

### 4.5.2. 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 IDBRT CA by using any communication means, based on which IDBRT CA will initiate suspension at its discretion.

### 4.5.3. Procedure of Suspension Request

- The suspension request is to be made by the subscriber in the application form specified in section 5.3.
- Subscriber sends the duly signed application form to IDRBT CA by fax/speed post/courier for suspension of certificate.
- IDRBT CA suspends the certificate and publishes Certificate Revocation List (CRL).
- IDRBT CA will inform about revocation of certificate to subscriber by email.

### 4.5.4. Activation of Certificate after Suspension

- The activation request is to be made by the subscriber in the application form specified in section 5.3.
- 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.

### 4.5.5. 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
- Subscriber 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 IDRBT CA 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

### 4.5.6. 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.

### 4.5.7. Procedure for revocation request

- The revocation request is to be made by the subscriber in soft copy in the application form specified in section 5.3 and submitted to SA/RA.
- SA/RA digitally signs and sends the revocation request to IDRBT CA by e-mail.
- IDRBT CA revokes the certificate on receipt of SA/RA digitally signed certificate revocation form and publishes Certificate Revocation List (CRL).
- IDRBT CA will inform about revocation of certificate to subscriber by email.

# 5. APPENDIX

## 5.1. Subscriber Application form

| APPLICATION FORM FOR DIGITAL CERTIFICATE | |
|---|---|
| NEW /RENEWAL | |
| **Important Notice:**<br>• * Fields are mandatory<br>• Strike off which are not applicable<br>• All certificates will be issued for 2 years validity period.<br>• Subscriber agreement should be submitted along with this application form.<br>• This application form is to be filled by the applicant.<br>• All subscribers are advised to read IDRBT CA Certificate Practice Statement (download from http://idrbtca.org.in/)<br>• Copy of identification document should be attached along with this application form.<br>• Application form must be submitted in person to the Registration Authority/IDRBT CA for face-to-face verification in case of Class 3 Certificate. | Paste your recent passport size photograph. |

| | |
|---|---|
| **Bank in which subscriber has account*** | |

| **Class of Certificate applied*:** | **Certificate required for *:** | **Type of Digital Certificate*:** |
|---|---|---|
| Class 1 ☐ | Individual ☐ | Signing ☐ SSL Client ☐ |
| Class 2 ☐ | Server ☐ | Encryption ☐ Object Signing ☐ |
| Class 3 ☐ | Webserver ☐ | SSL Server ☐ |

| PERSONAL DETAILS | | | |
|---|---|---|---|
| **Name*:** | | **Sex*:** | Male ☐ Female ☐ |
| **Email Address*:** | | | |
| **Address for communication*:** | | | |
| | **Pin code*:** | **Telephone*:** | |
| **Date of Birth*:** | | | *(dd/mm/yyyy) For Ex: 10th May, 1975 is 10051975* |
| **Identification Details* (Valid and not expired)** | ***Any one of:*** Passport No./PAN Card No./Voter's ID Card No./Driving License No. | | |
| **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.*<br>*Make sure that these details match with those given to generate request using certificate request generation tool or any other PKCS #10 request generation tool.*<br>*If necessary, contact your application provider for these details before filling the form.* | |
| **Common Name***<br>*(Name of the person, Server Name, Registered domain name, IFSCode etc)* | |
| **E-Mail***<br>*(Valid email address to which the communication be made)* | |
| **Organization***<br>*(Name of the organization)* | |
| **Organization Unit***<br>*(Name of the department)* | |
| **City/Locality***<br>*(Name of the city/town)* | |
| **State/Union Territory***<br>*(Name of State/UT)* | |
| **Country*** | **India** |

| | | |
|---|---|---|
| Signature of Superior Authority | | Signature of the Applicant |

## DECLARATION AND UNDERTAKING BY THE APPLICANT*

All the above information provided by me is true to the best of my knowledge and belief. I accept the responsibility for the safety and integrity of the private key by controlling the access to the computer/device containing the same, so that it is not compromised and I will immediately notify my RA/ IDRBT CA in event of key compromise. I agree to publish the Digital Certificate in the IDRBT CA repository and will report IDBRT 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 had verified the relevant documents corresponding to the Class of certificate. I hereby authorize him/her, to apply for obtaining Digital Certificate from IDRBT CA for the purpose specified above. I'm forwarding the digitally signed certificate request to IDRBT CA and maintaining the audit trail for the operations.

Date:

Place:

Name of the Officer: (Signature)

Official Email: (Stamp of Org./office)

## FOR SA/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

**Please send the duly filled in application 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/

## 5.2. Subscriber Agreement

The purpose of this agreement is to establish the contractual relationship between the IDBRT CA and the Applicant/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: idrbtca@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 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 IDRBT CA in the event that this information changes;
2. to immediately inform IDRBT CA if it is known or suspected that a private key has or may have been compromised or any revocation reasons specified in IDRBT CA CPS and corresponding User CP;
3. the use of the Digital Certificates are at their sole risk;

4. to use Digital Certificates strictly for lawful purposes and will not infringe a third party's rights; and
5. the use of the private key and/or its associated Digital Certificate constitutes acceptance of the terms of the IDRBT CA CPS.
6. 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.
7. 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.

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 IDBRT 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:**

## 5.3. Certificate Revocation/Suspension/Activation Form

| CERTIFICATE REVOCATION/SUSPENSION/ACTIVATION REQUEST FORM |
|---|
| **Certificate Revocation / Certificate Suspension / Certificate Activation** |
| **Important Notice:**<br>• * Fields are mandatory<br>• Strike off which are not applicable<br>• This application form is to be filled by the applicant.<br>• Fill this application form and send it to IDRBT CA in person or fax or post.<br>• 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***<br>Note:<br>▪ *Check **"Certificate Hold"** for suspension request*<br>▪ *Check **"Remove from Certificate Revocation List"** for activation request*<br>▪ *Check **"Unspecified or Key Compromise or Affiliation Changed or Superseded or Cessation of Operation"** for revocation request.* | ☐ Unspecified<br>☐ Key Compromise<br>☐ Affiliation Changed<br>☐ Superseded<br>☐ Cessation of Operation<br>☐ Certificate Hold<br>☐ Remove from Certificate Revocation List |
| **Details***<br>*(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:**<br>IDRBT Certifying Authority,<br>Road No. 1, Castle Hills,<br>Masab Tank,<br>Hyderabad – 500 057<br>India<br>Phone/Fax: +91 40 23536297<br>Email: cahelp@idrbt.ac.in<br>Website: http://idrbtca.org.in/ |

## 5.4. Certificate Acceptance Form

| CERTIFICATE ACCEPTANCE / NON-ACCEPTANCE FORM |
|---|
| **Important Notice:**<br>• * Fields are mandatory<br>• Strike off which are not applicable<br>• This application form is to be filled by the applicant.<br>• Fill this form and send it to IDRBT CA fax or post. |

| 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*** | |

**ACCEPTANCE / NON-ACCEPTANCE OF DIGITAL CERTIFICATE**

**I _____ , accept the Digital Certificate with the above mentioned details issued by IDRBT CA. I agree to publish my Digital Certificate in IDRBT CA Repository.**

**I _____, is not accepting the Digital Certificate because _____**

_____

_____

**Date:** **Signature :**

**Name :**

**CONTACT ADDRESS**

**Please send the duly filled in 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/

# 6. GLOSSARY

**Applicant**

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

**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.

**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).

**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 those 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 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.

**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.

**Record**

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

**Relying Party**

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

**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.

**Subscribers**

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 a Registration Authority 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.

**Superior Authority**

"Superior Authority" means an entity operating in the same organization as of Registration Authority (RA) functioning under IDRBT CA (or an entity to whom applicant reports in the organisation where applicant is working in case application is forwarded to IDRBT RA) and has the right to verify the credentials of applicant/subscriber before forwarding it to RA for approval.

**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 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)