



# IDRBT CERTIFYING AUTHORITY

S01000



Use of this card constitutes acceptance of the terms and conditions mentioned in the written Agreement. Misuse of this card is a criminal offence. If this card is lost or stolen, please contact IDRBT.

IDRBT

Institute for Development and Research  
in Banking Technology  
Casta Hills, Road No. 5, Hydco, Sec-10,  
Hyderabad - 500 007, A.P.

If this card is found, send it along to:  
IDRBT, Post Box No. 121,  
MC, Hyderabad College, Hyderabad-500 007.

***Institute for Development and Research  
in Banking Technology***



## DIGITAL SECURITY FOR BANKING & FINANCE IN INDIA

IDRBT is the Certifying Authority (CA) for the Indian Banking and Financial Sector, licensed by the Controller of Certifying Authorities (CCA), Government of India. The formal approval as Certifying Authority was handed over to Dr. V.P. Gulati, Director, IDRBT, by Dr. K.N. Gupta, CCA, on August 8, 2002.

With the Digital Certificates issued by IDRBT, Banks and Financial Institutions can now look forward to full-fledged security in their electronic communications, intra-bank and inter-bank applications and messaging. This will go a long way in facilitating speedy, secure and cost-effective financial transactions to improve customer service and satisfaction.

The Digital Certificates issued by IDRBT comply with the X.509 Standards to individuals and servers and it will fulfil the need for Trusted Third Party services in Electronic Commerce. All Classes of Certificates issued by IDRBT CA shall be Digital Certificates under the IT Act, and the legal effect, conjecture and evidentiary value of Digital Certificates as provided in the IT Act will be applicable.

A number of Financial and Banking Applications such as Structured Financial Messaging System, Real Time Gross Settlement, Centralised Funds Management System etc., and banks' own applications will benefit from the Secured Messaging and Transactions using Digital Certificates and Digital Signatures.

The CCA approval confirms that IDRBT has attained excellent standards in its overall key management, systems and operations. Significantly, it asserts IDRBT CA's certificate policies and practices to be of high standards, which is critical in its role as a Certifying Authority. As a Certifying Authority, IDRBT's role entails registration, issuance, renewal, suspension and revocation of Digital Certificates to applicants. It also necessitates careful verification of the applicants' identity.

## BACKDROP

The migration of computing environments to distributed, network solutions has radically changed the way companies conduct business. Many Banks and Financial Institutions have enhanced their networks and communication infrastructures to reap the full benefits of computerisation. In such an environment, information is crucial for

success and a key corporate asset, which needs to be protected. Information Security becomes critical to the successful operation of the electronic payment systems, and it is a major area of concern for today's networked world.

Cryptography is one of the main tools for privacy, trust, messaging, electronic payments and corporate security etc. At the very basic level, security can be divided into four elements: confidentiality, authentication, integrity and non-repudiation. While confidentiality and integrity can be provided by basic cryptography, authentication and non-repudiation require more sophisticated schemes.

Public Key Infrastructure systems provide a scalable and policy-based method to offer authentication and non-repudiation. PKI-based security applications such as secure e-mail and secure web-enabled transactions are the cornerstones of e-business and e-commerce solutions. It's PKI that provides the framework and trust infrastructure essential for e-business to thrive, thus ensuring better competitiveness and cost reduction.

*Dr. K.N. Gupta (left), CCA presenting the Certifying Authority Certificate to Dr. V.P. Gulati, Director, IDRBT, in the presence of Dr. R.B. Barman (centre), Executive Director, RBI and Dr. K.K. Bajaj, DCCA*



## WHAT IS PUBLIC KEY INFRASTRUCTURE?

Protecting transactions and communications over computer networks can be equated to an electronic equivalent of signing a letter and sealing it in an envelope. The act of signing the letter is confirmation of authenticity and non-repudiation, and sealing the envelope assures confidentiality and integrity.

**Symmetric Cryptography** guarantees confidentiality by encrypting a message using a secret key in association with an algorithm. A 'jumbled' version of the message is produced and it can be decrypted only by the recipient using the same shared secret key. The key used must be kept secret by both the parties and distributed to each in a secure manner. The difficulty with this form of cryptography is securely managing and distributing the secret key. As the key must be shared between the parties to the communication, evidence of non-repudiation cannot be assured, as both parties have the right to use the same secret key.

**Public Key Cryptography (or Asymmetric Cryptography)** solves this problem by replacing the secret key with a pair of keys; one private and one public, both mathematically linked with each other. The message is encrypted with the Public Key and it can only be decrypted with the corresponding private key from that key pair, thereby ensuring proof of confidentiality. In this system, the public keys of all entities can be published in open directories, facilitating communications between all parties whereas the private key is not shared.

Public Key Cryptography can also be used to generate and verify Digital Signatures, which can be attached to messages to provide proof of authentication, integrity and non-repudiation. However, Public Key Cryptography on its own is not enough for truly re-establishing the conditions for conventional paper based commerce in an electronic scenario. The following too are required:

- ◆ Policies to describe the rules under which the cryptographic systems should function
- ◆ System to generate, store and manage the keys
- ◆ Procedures to specify how the keys and certificates should be created, distributed and used

The solution to the above demands is the **Public Key Infrastructure (PKI)**. PKI presents the core structure for an extensive range of components, applications, policies and practices to combine and achieve the four primary security functions for commercial transactions:

- ◆ **Confidentiality** - to keep messages confidential and prevent eavesdropping
- ◆ **Integrity** - to prove that information has not been manipulated or tampered
- ◆ **Authentication** - to confirm the identity of an individual or application
- ◆ **Non-repudiation** - to ensure that information cannot be disclaimed/disowned.

PKI is a combination of hardware and software products, policies and procedures. It provides the basic security required to carry out electronic business so that entities, which do not know each other, or are widely spread, can communicate securely through a chain of trust.

## CERTIFYING AUTHORITY (CA)

Modern Cryptography offers solutions for secure transactions over the network through a Public Key Cryptography System (PKCS). The PKCS requires a Trusted Third Party (TTP), commonly known as Certifying Authority (CA).

The primary function of CA is to register the public keys generated by the individuals and issue Digital Certificates. These bind a public key to a given person, signed with the CA's private key, which can be safely stored in a public directory and sent over an insecure network, thus allowing everyone to securely communicate and to do business with even people they have not met before.





The IDRBT Certifying Authority (IDRBT CA) is a Trusted Third Party (TTP), licensed by the Controller of Certifying Authorities (CCA), Ministry of Communication and Information Technology, Government of India, for issuing, managing, renewing and revoking certificates in accordance with the standard practices published in the IDRBT CA Certificate Practice Statement (IDRBT CA CPS). The Certifying Services offered by the IDRBT CA (*i-trust PKI Services*) are designed to support secure electronic transactions, digital signatures and other general security requirements of INFINET users.

### **IDRBT CERTIFYING AUTHORITY – LICENSED CA UNDER IT ACT 2000**

IDRBT CA will fulfill the need for Trusted Third Party services in Electronic Commerce by issuing Digital Certificates that attest to some fact about the subject of the certificate, thereby providing independent confirmation of an attribute claimed by a person offering a Digital Signature. IDRBT provides high-end PKI based services and solutions that provide trust and security to individuals, organizations, and the government for securing the transactions through the INFINET.

The IDRBT CA has all facilities in place for issuing any number of Digital Certificates, a primary component of PKI. IDRBT CA will issue, administer and revoke the Digital Certificates over INFINET. IDRBT CA's *i-trust PKI Services* will be available for INFINET users only.

#### **PKI-enabled Applications**

PKI is a means to an end. It provides the security framework by which PKI-enabled applications can be confidently deployed to achieve the required benefits. Some of the applications in various stages of deployment are:

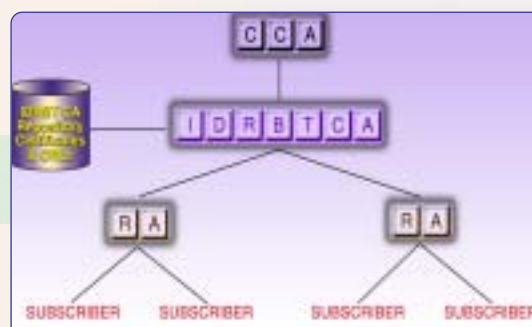
- Structured Financial Messaging System
- Public Debit Office - Negotiated Dealing System
- Secured Web Server
- Electronic Fund Transfer
- Corporate E-mail for Banks and Financial Institutions
- RBI Applications like Real Time Gross Settlement and Centralised Fund Management System

#### **Certificate Classes and Usage**

The IDRBT CA currently offers three distinct classes of Certifying Services. Each class of certificate, which has a validity period of one year, provides specific functionalities and security features, thereby providing the designated level of trust. The Classes are:

- **Class 1 Certificate** : This certificate is meant for individuals for signing (digital signature) purposes.
- **Class 2 Certificate** : This certificate is meant for individuals and server administrators for signing (digital signature) and encryption purposes.
- **Class 3 Certificate** : This certificate is meant for individuals and Web Servers for signing (digital signature), code signing or object signing (certifying a programme or application as genuine and non-malicious) and for secure Web Server (for implementing secure socket layers for server to client communication) purposes.

**Public Key Infrastructure Hierarchy**





All the above Classes of Certificates shall be Digital Certificates under IT Act, 2000, and the legal effect, conjecture and evidentiary value of Digital Certificates as provided in the IT Act will be applicable. The price list of the Digital Certificates is available at <http://idrbtca.org.in/> on INFINET or <http://www.idrbt.com/> on Internet.

### REGISTRATION AUTHORITY FOR IDRBT CA

A Registration Authority (RA) is an office appointed by the IDRBT CA that collects and processes requests for allotment/revocation/suspension of Digital Certificates. The Registration Authority Official will verify the credentials of the Digital Certificate applicants and if found acceptable, will forward them after affixing his/her digital signature to their applications to the IDRBT Certifying Authority.

The Application Form for Digital Certificates is available at IDRBT CA Repository on the website <http://idrbtca.org.in/> on INFINET. The duly filled-in Application Form containing information about the Applicant's/Subscriber's identity, authorization, role and other information, would be used by the Registration Authority to verify the credentials of the Applicant/Subscriber.

#### Creating a Registration Authority

Officials (from the rank of DGM onwards) from banks may approach the IDRBT CA Office along with an official reference letter from his/her Superior Officer for becoming a RA. At least two persons are required to be appointed for each RA office - one RA Administrator and one or more RA Operators. The RA Operator must be a person in the rank of an Officer in the same RA Office. The Superior Officer should designate RA Administrator and RA Operator for a given RA Office of their bank.

Persons authorized by the Superior Officer of the bank would be responsible for the complete operations and management of the Registration Authority Office. The persons so authorised to manage the RA office can apply for Class 3 Individual Signing Certificates in the prescribed Registration Authority Application Form, with all relevant documents mentioned below, and IDRBT CA Registration Authority Agreement Form duly signed on a non-judicial stamp paper of Rs. 100/-. (The details have already been forwarded to all Banks). The Documents to be attached along with the Registration Authority Application Form include:

- IDRBT CA-RA Agreement on stamp paper signed by RA Official.
- Original copy of Passport, Voter's ID or PAN Card to be furnished along with photocopies.
- The RA officials should personally appear before the IDRBT RA Executive for personal verification.
- The RA should discharge the responsibilities as mentioned in the IDRBT CA CPS and be in agreement with the terms and conditions mentioned in the Registration Authority Agreement.

#### RA Office Requirements

The RA Office is created to perform the duties and activities of Registration Authority mentioned under IDRBT CA CPS. RA Office should have in place the infrastructure to support:

- Two RA Officials - RA Administrator and RA Operator
- Two computers with Smart Card reader
- INFINET connectivity for accessing RA Services (for 2 computers)
- Maintenance of Subscriber's confidential information under Secure Lock and Key
- Personal verification of Subscribers requesting a Class 3 Certificate
- Archival of Subscribers records for 7 years as per IT Act 2000
- Generate self-audit trails & retain Audit reports conducted by IDRBT CA





### Hardware/Software Requirements

Two Operational Machines with the following specifications:

- Operating System: Windows NT/2000 • Intel Pentium III (preferable) • CD-ROM Drive
- RAM: 64KB (minimum) • Serial Port for Smart Card • INFINET Connectivity
- Two Reflex-72 Smart Card Readers from Schlumberger

### FAQS ON CERTIFYING AUTHORITY

**Why should I choose IDRBT CA as my Certifying Authority?**

IDRBT CA is a Certifying Authority, licensed by the Controller of Certifying Authorities, Government of India under the IT Act 2000. The licensing of IDRBT CA by the CCA means that it has met all the regulatory requirements under the IT Act, Rules, Regulations and Guidelines. The Digital Certificates and Signatures issued by it will be legally valid in the Indian Courts. For information on the regulatory requirements for obtaining a license as a CA, please visit <http://www.mit.gov.in/>

**What are Digital Certificates?**

A Digital Certificate is an electronic document that is digitally signed by the issuing Certifying Authority i.e. a subscriber's Digital Certificate is signed by the IDRBT CA's private key. Digital Certificates solve the problem of authenticating a sender to a receiver of an electronic message.

**Why do I need a Digital Certificate?**

There are many certificate-enabled applications such as Online Banking, Structured Financial Messaging System, Electronic Data Interchange, Electronic Fund Transfer, Secure Electronic Mail, etc. One will need a Digital Certificate to access these applications securely.

**Who is eligible for a Digital Certificate from the IDRBT CA?**

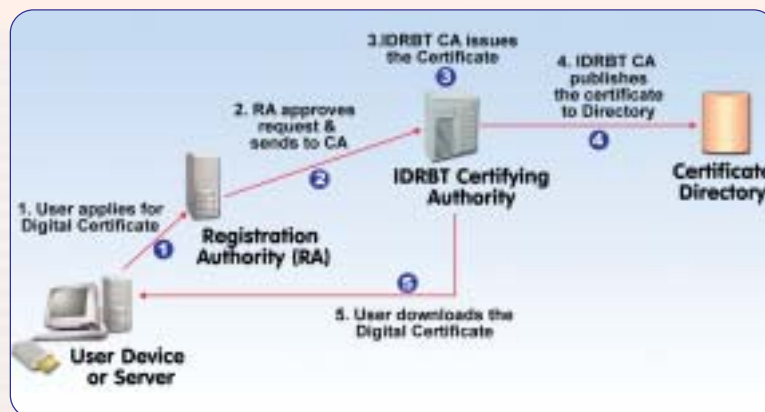
IDRBT CA offers Certifying Services for the employees of Banks and Financial Institutions, Servers used for various bank applications and to Government Organisations that are members of INFINET.

**What is the most essential requirement for getting a Digital Certificate?**

The first and foremost requirement for obtaining a Digital Certificate from the IDRBT CA is that you must be a member of INFINET.

**What does IDRBT CA do with my Public Key?**

When IDRBT CA receives a public key, it waits for the user's Certifying request to be verified and forwarded by the Registration Authority. The Certifying Authority makes further checks and once satisfied that all the requirements have been met with, creates a Digital Certificate. The certificate includes some of the information the user supplied and the user's public key.





#### What information is contained within an IDRBT CA Digital Certificate ?

The following information is contained within a personal and corporate IDRBT CA Digital Certificate:

- The Subscriber's Name and Distinct Name
- The Subscriber's Public Key
- Name and Digital Signature of the issuing Certificate Authority
- Expiry Date of the Certificate

#### How do I register for an IDRBT CA Digital Certificate?

Please contact the Registration Authority operating under IDRBT CA to register for an IDRBT CA Digital Certificate. You are encouraged to download and fill in the application form and send it to the nearest Registration Authority with the necessary details including the personal identification documents mentioned in the IDRBT CA CPS. You must appear in person with the required documents before the RA, if you are applying for Class 3 Certificates.

#### What is the time duration for the issuance of a Digital Certificate?

Once all the subscriber credentials are verified, the certificate will be issued within five working days.

#### How do I store the Digital Certificates?

We recommend devices like Smart Card or hardware token to store the digital certificates. You are advised to store your certificate in the browser by making necessary arrangements for the security of your machine.

#### Do I need a smart card or token?

Smart cards, and other cryptographic tokens, are suitable for very secure applications, and their key features are:

- The private key cannot be removed from the card
- Key pair is generated on the card
- Full support for 128 bit (or greater) scrambling and digital signing
- Affordable.
- All scrambling and unscrambling is done on the card by a specialised processor

#### How will I know if my Certificate has expired?

Certificates issued by IDRBT CA are valid for one year. You may wish to take note of the expiry date of your Certificate and renew it prior to its expiry. The Registration Authority will notify in advance the expiry of the certificate.

#### What is suspension and revocation of a Digital Certificate?

Suspension is the process of making a certificate temporarily invalid whereas Revocation is the process of making a certificate permanently invalid.

IDRBT CA provides a service that allows you to suspend or revoke your certificate. The certificate may be suspended if it has been issued with wrong or falsified information or its payment has not been made according to contractual agreement. The Certificate can be revoked when it was compromised. An organisation can also revoke a certificate e.g. when an employee leaves.

#### How do I revoke my Certificate?

The application form for the Certificate revocation/suspension is available in the IDRBT CA repository. Apply online for a certificate revocation to the IDRBT CA. Your Digital Certificate will be revoked according to the IDRBT CA CPS.

#### **CONTACT**

*For Customer Support and Technical queries, please contact:*

The PKI Coordinator, E - mail: [caservice@idrbt.ac.in](mailto:caservice@idrbt.ac.in)

Ph: 040 - 3534981/82/83/84, Fax: 040 3536361/3535157

Visit us at: On INFINET: <http://idrbtca.org.in/> and <http://infinet.org.in/>

On Internet: <http://www.idrbt.com>





क्र. सं./No. \_\_\_\_\_  
2002 0003 050807 000 0000 999

भारत सरकार  
GOVERNMENT OF INDIA  
प्रमाणन प्राधिकारी नियंत्रक  
CONTROLLER OF CERTIFYING AUTHORITIES



प्रमाणित किया जाता है कि वैकिंग प्रौद्योगिकी विकास एवं अनुसंधान संस्थान  
कीसल हिल्स, रोड नं. १, मासब टैंक, हैदराबाद - ५०००५६.  
को प्रमाण प्रौद्योगिकी अधिनियम २००० के अधीन, ९ जुलाई, २००१ को जारी दिशानिर्देशों के अंतर्गत प्रमाणित किया गया है। यह प्रमाणित आज दिनांक ६  
मास अगस्त, २००२ को प्रमाण प्राधिकारी के नियंत्रक के हस्ताक्षर एवं मुद्रा सहित जारी किया जाता है, और  
प्रमाणित की कल्पना कि यह प्रमाणित के दौरान प्रमाण प्रौद्योगिकी अधिनियम, नियम, दिशानिर्देश और दिशानिर्देशों के अनुपालन में व्यवहार में लाया जाये कि प्रमाणित के लिए है।

This is to certify that INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY  
located at CASTLE HILLS, ROAD NO. 1, MASAB TANK, HYDERABAD - 500 057.  
has been granted licence to act as a Certifying Authority, under Section 21 of the IT Act 2000, subject to terms and conditions specified as part of the Regulations dated 9th July, 2001, issued under the IT Act 2000. This licence is given under the signature and seal of the Controller of Certifying Authorities on this 6<sup>th</sup> day of August, 2002, and is valid for a period of five years, subject to compliance with the IT Act, Rules, Regulations and Guidelines during the entire validity of the licence.

*Debjani Nag*  
DEBJANI NAG

Assistant Controller (Tech.)  
Office of Controller of Certifying Authorities / Authorized  
Department of Information Technology  
Government of India (Ministry) / Secretary  
Electronic Division  
S, C.B.O. Complex, New Delhi-11  
Tel: 4988898

*Levi Raj Gupta*  
LEVI RAJ GUPTA

Assistant Controller (Tech.)  
Office of Controller of Certifying Authorities  
Department of Information Technology  
Government of India (Ministry) / Secretary  
Electronic Division  
S, C.B.O. Complex, New Delhi-11

प्रमाणित की गई  
Public Key

2882 0104 5282 0101 0065 8289 05F3 278e 3271 09ed 77a7 ed17 2e6e 8293 b0bd a93e 2b71 7798 e2d8 be6f9 3d8c  
8e1a 000a 18a8 8f70 186d 8128 a0d1 2547 3791 a03a a338 22a3 014e 3080 2a15 2541 207c 304d 5954 7045 2a1a  
2830 19e0 2e04 c17e c57b 2388 49c5 4838 be9f 78c7 ea37 0f3a 8982 8a65 8a34 8886 6a02 9184 8862 489d 4d87  
2840 c08d 33ac 8a03 8e95 786d 2112 3cc4 d257 641a 8320 457b 8a5e 8295 7f05 87de 8800 a27c 2803 8c49 1293  
823a 8b5e 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d 8e0d  
8f4a 84ca e194 8c4c 2486 8dad 3f4b 2385 7512 a138 1bd1 a601 716a 8806 7010 7ea3 8323 8ac0 7783 1289 2c4a  
27d8 8e0d 1749 8724 2e88 8518 8802 0201 0201

*Debjani Nag*

*Levi Raj Gupta*

Institute for Development and Research in Banking Technology  
(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad - 500 057, India.  
EPABX : 3534981-84 (4 lines), Fax : (040) - 3535157, 3536361

e-mail : [publisher@idrbt.ac.in](mailto:publisher@idrbt.ac.in) • Website: <http://www.idrbt.com>; <http://www.idrbt.ac.in>

