IDRBT

FAST FORWARD

NEWSLETTER

Volume 5 • Number 2 • September 2002

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

Dawn of Digital Security for Banking & Finance in India

It's a moment of immense pride for all of us. IDRBT is now 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, at an impressive function organised at Mumbai.

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, Executive Director, RBI

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 Solution, 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.

SPECIAL ISSUE ON IDRBT CERTIFYING AUTHORITY SERVICES

Public Key Infrastructure & IDRBT Certifying Authority

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 benefits of computerisation.

In such an environment, information, a key corporate asset and a crucial factor for success needs to be protected at all costs. Information Security becomes critical to the successful operation of the electronic payment systems, and it is precisely the major area of concern for today's e-commerce world.

Cryptography is one of the main tools for privacy and trust in messaging, electronic payments, corporate security, and countless other fields. 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 (PKI) Systems provide a scalable and policy-based method to offer authentication and non-repudiation. PKI-based security applications such as secure email and secure web-enabled transactions are the cornerstones of e-business and e-commerce solutions. It is PKI that provides the framework and trust infrastructure essential for e-business to thrive, thus ensuring better competitiveness and cost reduction.

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 other 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 and /or operate from different locations geographically 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 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 fulfil the need for Trusted Third Party (TTP) 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 INdian FInancial NETwork (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.**

Registration Authorities (RA)

Registration Authorities (RAs) will be entities nominated and trusted by IDRBT CA for registering the users for issuing certificates. Banks are advised to set up a Registration Authority (RA), headed by a senior officer of a rank not lower than the DGM for management and issuance of Digital Certificates by IDRBT CA to their employees and servers.

The Rules, Guidelines, Procedures, and copies of RA Application Form, Subscriber Application Form, RA - IDRBT CA Agreement and Subscriber-RA agreement have been circulated to the Banks already. For further information please visit our CA site at http://idrbtca.org.in, which is hosted on the INFINET. (Please check out more on Registration Authority on the next page)

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 major applications listed below, which are in use / different stages of developement and deployment in the financial sector will strongly relay on PKI support from IDRBT CA services :

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

Certificate Classes and Usage

The IDRBT CA currently offers three distinct classes of Certification 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
- Class 2 Certificate
- Class 3 Certificate

What are these Classes?

The Class 1 certificates are meant for individuals for signing (digital signature) purposes.

The Class 2 certificates are meant for individuals and server administrators for signing (digital signature) and encryption purposes.

The Class 3 certificates are 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.

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.

Digital Certificates issued by IDRBT CA can be used for Digital Signature, encryption of messages, secure server, and code signing. The price list of the Digital Certificates is available at http://idrbtca.org.in on INFINET or http://www.idrbt.com on Internet.

Contact

IDRBT CA Support Services provide all the required technical assistance to its customers based over the INFINET. An online Help Desk is also available to resolve the queries. *For Customer Support and Technical queries, please contact:*

The PKI Coordinator
Ph: 040 3534981/3534982/3534983/3534984
Fax: 040 3536365
Email: caservice@idrbt.ac.in / idrbtca@idrbt.ac.in
Visit us at: http://idrbtca.org.in or http://infinet.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 for becoming a Registration Authority.

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 authorized 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. The 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 and retain Audit reports conducted by IDRBT CA Office.

Hardware/Software Requirements

Two Operational Machines with the following specifications:

- Operating System: Windows NT/2000
- Intel Pentium III (preferable)
- RAM: 64KB (minimum)
- Serial Port for Smart Card
- CD-ROM Drive
- 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 (CCA), Government of India under the Information Technology 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, and 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 IDBRT CA?

IDRBT CA offers Certification Services for the employees of Banks and Financial Institutions, Servers used for various bank applications and to Government Organisations who are the members of the INdian FInancial NETwork (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 certification request to be verified and forwarded by the Registration Authority. The Certification 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 Certifying Authority
- Expiry Date of the Certificate

What are Class 1, Class 2 and Class 3 Certificates?

Digital certificates issued by IDRBT CA fall into three categories:

- Class 1 Certificate
- Class 2 Certificate
- Class 3 Certificate

The Class 1 certificates are meant for individuals for signing (digital signature) purposes.

The Class 2 certificates are meant for individuals and server administrators for signing (digital signature) and encryption purposes.

The Class 3 certificates are 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.

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 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:

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

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 is 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.

Structured Financial Messaging System

SFMS has already been installed in Canara Bank, Bank of Maharashtra, Punjab National Bank, Bank of Baroda, Andhra Bank, Indian Overseas Bank and CCIL. There were certain issues related to having a common cluster server for PDO NDS and SFMS and these have been resolved. The Installation of SFMS at Dena Bank, UCO bank, Central Bank of India, Bank of India and United Bank is now being taken up.

In the meantime, the new SFMS 2.0, released in early August 2002, is ready for deployment. The main features of SFMS Release 2.0 are:

- Off-line creation of messages in PCs in remote branches.
- Off-line branches to connect to an online Common Branch Server to send/receive messages.

- Three levels of authorization - Creator, Verifier & Authoriser as against two levels - Creator & Authoriser in the earlier version.
- In the earlier versions, Creators who are normally computer operators, had to be provided with smart cards and banks didn't find it convenient. SFMS Release 2.0 allows password-based access for creators. Verifiers & Authorisers will need smart cards.

Even as the SFMS Release 2.0 was being readied for release, several user banks felt that SFMS should allow both gateway and branch server modules to be installed on a single server. Hence SFMS Release 2.2, which allows this functionality, is also being made ready. SFMS Release 2.2 allows banks to deploy offline modules in all remote branches to connect to a single Common Gateway-cum-Branch Server (CGBS). The CGBS architecture has the following advantages:

- Banks can cut down on the number of servers and also on software such as operating system, RDBMS, Middleware etc.
- Banks can provide for Fault Tolerance at a single point i.e., the CGBS level only, instead of building redundancy at multiple Common Branch Servers.
- As there will be no Common Branch Servers, there will be no need to post system administrators to maintain the Common Branch servers at major locations.

Most of the Public Sector Banks are ready to roll out their applications using SFMS Release 2.2. Since IDRBT is now the Certifying Authority for the Banking and Financial sector, it is necessary to bring the certifying procedure for SFMS in line with that approved by the CCA.

Banks have already been advised on the procedure to be followed to obtain signing and encryption certificates for SFMS usage and as soon as the Banks are able to obtain the Public Key Certificates, they can commence their applications.

Executive Development Programmes

Wide Area Network for Central Bank of India

This customised programme was exclusively held for the Central Bank of India from Jan 21- 26, 2002.

The programme aimed at disseminating knowledge, which would come in handy for designing, managing and operating the Wide Area Network of Central Bank of India.

WAN Technologies, Domain Name System, Routing Protocols, Network Security, Firewall, Public Key Infrastructure and Structured Financial Messaging Solution were some of the issues discussed.

The programme was co-ordinated by Shri N. Rajendran and Ms V. Radha, Faculty, IDRBT.

Emerging Trends in Banking Technology for Bank of Baroda

Two Customised Executive Development Programmes for Bank of Baroda were held from Feb 11-16, and March 04-09, 2002.

The entire gamut of technology development in Banking was covered with topics like IT Reforms in Banking, Wide Area Networking with INFINET, Internet and Intranet Technologies and Applications, Security Policy and Information System Audit for Banks, Security and Encryption for Financial Services, SFMS and Bank Applications, Data Warehousing and Data Mining for Banks, Internet Banking,

ALM and Risk Management, RBI Initiatives in Technology upgradation in Banks etc.

The programmes were co-ordinated by Shri. M.V. Sivakumaran, Faculty and Ms.T.K.Srivani, Project Consultant, IDRBT.

Programmes on Structured Financial Messaging Solution

As part of the Institute's initiative to prepare the bankers for the successful implementation of the Structured Financial Messaging Solution, six programmes, exclusively on SFMS, were conducted at the Institute.

Apart from providing extensive hands-on experience, just about every aspect of SFMS was discussed threadbare during these six-day programmes. Issues such as SFMS Security, Network, Technical Overview, Configuring Dial-in RAS on Branch Servers, Integration with RBI Applications, APIs, Installation, and Server Troubleshooting were dwelt upon in detail.

These programmes, conducted between March 11 & July 6 , 2002 were co-ordinated by Shri A.P. Raja, Project Consultant, IDRBT.

New Dimensions in Banking Technology for Allahabad Bank

Two Customised Executive Development Programmes for Allahabad Bank were conducted at the Institute from April 15-20 and May 06-11, 2002.

Networking Concepts, Wide Area Networking, Corporate E-Mail, Intranet & Internet, Plastic Money and ATM Network, SFMS, CRM Strategy for Banks, RBI Initiatives in Technology Upgradation, IT Act & Cyber Crimes, Internet Security, IS Audit and Data Warehousing and Data Mining were some of the topics deliberated upon.

While the first programme was co-ordinated by Shri M.V. Iyer, Project Consultant, the second was co-ordinated by Shri N.P. Dhavale, Faculty, IDRBT. Both the programmes had thirty participants each.

Programme on Information System Audit

A two-day programme on Information System Audit was exclusively held for the Reserve Bank of India on May 02-03, 2002.

Need for Information System Control & Audit, Information Security Audit and Management Concerns, COBIT Management Overview, Business Continuity and Disaster Recovery Planning, and Information System Control – Type & Needs were some of the topics discussed.

The programme was co-ordinated by Shri D.P. Dube, Project Consultant, IDRBT.

Workshop on SFMS Implementation Issues

A Workshop on SFMS Implementation Issues was conducted at the Institute on June 17, 2002.

The Workshop reviewed progress of SFMS implementation in different banks, and discussed various issues such as Procurement of Oracle/MQ Series Servers, Installation of SFMS Software, SFMS Training Programmes at IDRBT, RBI Applications interface for SFMS, and IDRBT recommendations on Disaster Recovery at SFMS Gateway etc.

Experts from the Reserve Bank of India, Ministry of Communication and Information Technology, and Executives from various Public Sector Banks participated in this one-day workshop.

Information Security for Punjab National Bank

This three-day Customised Executive Development Programme on Information Security was conducted exclusively for Punjab National Bank from June 24-26, 2002.

Topics of immediate relevance such as Enterprise Network Security, Operating System Security, Top Management Security Policy, PKI/RSA/SSL, Internet Banking Security, & Security Integration were some of the issues that were deliberated upon.

Thirty-eight participants from different branches of Punjab National Bank participated in the Programme, which was co-ordinated by Shri D.P. Dube, Project Consultant, IDRBT.

Information System Audit for Canara Bank

This Customised Executive Development Programme was conducted for Canara Bank from July 22 - 27, 2002.

The programme started off with a Seminar on Information Security and Audit. Dr. R.B. Barman, ED, RBI, Dr. K.N.Gupta, Controller of Certifying Authority (CCA), GoI, Dr. K.K. Bajaj, (DCCA) and Dr. V.P. Gulati, Director, IDRBT participated in it. The seminar discussed the emerging Information Security scenario and ways and means to protect the resources in this ever-changing scenario.

Various other topics of immediate relevance such as Communication Control and Network Operating System, Intranet and Internet Security, PKI & SSL, Application and Processing Control, BCP & DRP were discussed. This highly appreciated programme was co-ordinated by Shri D.P. Dube, Project Cosultant, IDRBT.

Business Continuity and Disaster Recovery Plans

The three-day programme on Business Continuity and Disaster Recovery Plans, held from August 21-23, was of special significance because it was the first programme on these topics.

Right from BCP Methodologies and Strategy, the BCP Process, Business Impact Analysis and Risk Analysis, DRS for Network and Communication Systems to BCP & IS Audit, this programme provided a forum to strategise for Business Continuity and Disaster Recovery.

The programme was co-ordinated by Shri Aditya Gaiha, Faculty, IDRBT.

Corporate Messaging & Intranet

A programme on Corporate Messaging and Intranet was held at the Institute from August 26 -31, 2002. Some of the topics discussed in the programme include Intranet and Internet Technologies, Corporate E-Mail, Enterprise Application Integration, Security in Internet Application, E-Learning using Internet and Auditing Web Based Applications.

Participants from State Bank of Saurashtra, Punjab National Bank, Indian Bank, Vijaya Bank, State Bank of Patiala, Syndicate Bank, and Canara Bank participated in this programme, which was co-ordinated by Shri D.P. Dube and Shri M.V. Iyer, Project Consultants, IDRBT.

Workshop of Structured Financial Messaging Solution

A one-day workshop, on Structured Financial Messaging Solution, specifically for the Private Sector Banks, was held on Sep 17, 2002 at the Institute.

As the requirements and deployment environment of Private Sector Banks is different from that of Public Sector Banks, the Workshop attempted to clarify, discuss and thrash out the specific implementation issues related to SFMS, PKI and Certification Authority.

There was also an open house where all the queries were clarified. Most of the Private Sector Banks participated in this programme.

Use of PKI in Banking Applications

This programme was conducted at the Institute from Sep 02-07, 2002. The programme was of urgent relevance in the light of IDRBT becoming the Certification Authority and the SFMS being implemented by the Banks.

Traditional Authentication Techniques, PKI Basics and SSL, PKI in SFMS, IDRBT CA Certification Services, PKI-enabled Applications and Smart Card Technologies were some of the issues deliberated upon.

This programme was co-ordinated by Shri A.P. Raja, Project Consultant and Dr. N.P Dhavale, Faculty, IDRBT.

M.Tech. in Information Technology

Our M.Tech programme in Information Technology (with specialisation in Banking Technology and Information Security) has taken off very well. We have got an enthusiastic and enterprising bunch of students for the second batch, which started off in the first week of August. This time, apart from the regular students, we have also got sponsored candidates from the Banking and Financial Sector.

Meanwhile, the first batch of students have completed the Course Work and started their project work. Most of them have proceeded to various banks and financial Institutions to pursue their projects and some of the students are involved in the Institute's research projects. The duration of the project is six months and it is expected to be completed by December 2002.

Our students have been provided adequate exposure to various concepts related to Banking Technology & Information Security and we have specifically focussed on imparting them hands-on experience in various technological areas of immediate relevance to the Banking and Financial Sector. In addition, we have also equipped them with knowledge on the latest innovations in the area of Banking Technology. Our students are fully competent enough to provide a major thrust to the technology initiatives of banks.

GATE SCORE - Must for M.Tech (IT)

From 2003 onwards:

- Valid GATE SCORE is a compulsory requirement for getting admission into M.Tech (IT).
- M.Tech (IT) students would also be provided stipend on par with GATE scholarships.

We strongly believe that these students should be absorbed in the Banking sector as a priority, because the M.Tech programme has focussed on Information Technology in Banking and Finance and these students will be the ideal candidates to strengthen the banking sector technologically.

Banks and Financial Institutions are invited to visit the Institute for Campus Recruitment. The M.Tech students are good enough to be placed in Scale-II and above, and we are sure that our students will live upto the expectations. The Reserve Bank of India has already evinced keen interest in our students and they will be visiting the Institute for Campus Recruitments shortly.

Five seats in M.Tech (IT) are reserved for sponsored candidates from Banks and hence the identification process may be initiated in Banks right now so that they are able to sponsor their candidates in time for the next batch.

For further information and/or fixing up Campus Recruitment Visits, Banks/Financial Institutions are requested to write to:

Dr. P. Radhakirshna,
M.Tech Co-ordinator,
e:mail:prkrishna@idrbt.ac.in

Certificate Course in Enterprise Network Technologies & Security (CENTS)

(Nov 07 - 16 & Dec 19 - 28, 2002)

Here's your chance to become a specialist in the most *critical area of concern* for Banks and Financial Institutions. Just join IDRBT's unique ***Certificate Course in Enterprise Network Technologies & Security (CENTS).***

Networking of branches is essential for deploying any Electronic Business Application, but it also brings along insecurity and the risk factor increases manifold. Therefore, banks need to have the security expertise to counter these threats, cope up with the new advancements in technology and explore new ways of conducting business.

The CENTS is specifically designed to equip and train bankers in applying Technology to meet their specific needs in the ever changing scenario. It would provide detailed inputs and hands-on on Networking, Security Essentials, Protecting the Enterprise Network, PKI Technologies, Application Information Security, Back Up and Disaster Recovery. Participants will also have to execute a Project.

The programme would be ideal for Specialist Officers from IT departments, who have the overall responsibility of managing the Bank's Network and Security.

Passport to PGPBTM

Those who successfully complete the CENTS can straight away carry the credits awarded to them into the Post Graduate Programme in Banking Technology Management (PGPBTM) being launched by IDRBT shortly. They will be allowed to transfer the CENTS credits for the two courses on **Corporate Network Management** and **Information Security and Audit**. Above all, these participants can get free enrolment into PGPBTM and save on the entire course fee for PGPBTM, which comes to Rs 20,000 as of now.

Duration & Methodology

CENTS is a twenty-day programme, divided into two modules of 10 days each, and spread over a period of two months. The programme would rely predominantly on providing hands-on exercise and the modules would be spaced out equally so as to provide enough time for the participants to have a good grasp of the concepts involved. Participants would be given a project at the end of the first module and they are expected to submit the project report before the commencement of the final module.

Twenty-day in person Instructor-led training:

Participants would have to attend the programme at IDRBT for twenty days, divided into two modules of ten days each. The First Module would be conducted from **November 07-16, 2002** and the second module from **December 19-28, 2002**. During this period, participants will be receiving value added inputs on technical expertise through Technical Sessions, Demonstrations, Lecture Notes, Lab Exercise and Case Studies etc

Thirty-two day Distance Training:

Participants can interact with the IDRBT Faculty through chat, e-mail for guidance on the project and for clearing any other doubts on the course. Course inputs will also be made available to the participants on IDRBT's academic website: **http://www.idrbt.ac.in.m**

The fee for the programme is Rs.70,000 (Rupees Seventy Thousand only) per participant. It includes boarding and lodging when attending the program at IDRBT, and training, course material, kit and other infrastructural overheads.

For further details visit these links:
www.idrbt.com./idr/forth.html
www.idrbt.ac.in/acin/forth.html

IDRBT invites applications from young and dynamic professionals with the requisite qualifications and skill sets for the following positions:

FACULTY

Position	Scale	Experience	Skill Profile
PROFESSOR	18400-500 -22400	Min. 10 yrs. teaching/research/ professional experience of which 3 yrs. at the level of Associate Prof. or equivalent, leadership & innovation qualities and publications in reputed journals.	• Ph.D. with First Class or equivalent at the preceding degree in Computer Science or related areas and with outstanding research experience • Interdisciplinary backgrounds in IT, Banking and Finance
ASSOCIATE PROFESSOR	16400-450 -20000	Min. 8 yrs. teaching/research/ professional experience of which 3 yrs. at the level of Asst. Prof. or equivalent and publications in reputed journals.	
ASSISTANT PROFESSOR	12000-420 -18300	Min. 3 yrs. teaching/research/ professional experience. Criteria relaxable in case of outstanding academic record / Experience.	

Compensation will not be a constraint for the right candidate and Faculty are also entitled to liberal perks, comparable with the best in Banking Industry. Professional bankers with relevant experience may also be considered on Deputation basis as Consultants (equivalent to Faculty).

Candidates pursuing/interested to pursue Ph.D. would be considered for the position of Research Officer (Equivalent to Lecturer) / Faculty Research Associate (Equivalent to Senior Lecturer), on long-term contract basis, based on their skill sets and educational profiles. Freshers can be considered for Research Fellowship and to start with they will be paid a consolidated amount of Rs 8000/- per month.

PROJECT/TERM BASED POSITIONS

PROGRAMME OFFICER : First Class Post Graduation in Management/Public Administration, around 27 yrs and 2–3 yrs. experience in managing programmes in training/academic institutions.

RELATIONSHIP EXECUTIVE: Engineering graduates with specialization in E&C/CS/related areas and Post Graduation in Management, around 27 years and possessing 2–3 yrs. of experience in Marketing of IT products/services and flair for relationship building.

PROJECT MANAGER (FINANCIAL MESSAGING SYSTEMS / NETWORK / SECURITY): Post Graduates in IT/ CS/E&C or related areas, preferably M. Tech., around 35 years and should possess 5–6 yrs of experience in (i) Banking & Finance, (ii) Networking (VSAT/Leased Line), routers, modems (iii) Encryption & Decryption, CA, PKI, respectively. The Institute is also looking for suitable candidates with the above profile, for the position of Project Manager, at IDRBT Centre, Pune.

PROJECT ENGINEER/SYSTEMS ENGINEER: Engineering Graduates/Post Graduates with specialization in IT and related areas, around 25 yrs, 2-3 yrs experience and possessing expertise in configuring/ maintaining modems, switches, routers and firewalls, maintaining all back office products and installation, maintenance and administration of Windows, UNIX, Sun Solaris and LINUX operating system, advance knowledge of configuring and implementing various utilities viz., mail messaging system. Candidates with Diploma in E&C or related areas with relevant experience may be considered.

DOCUMENTATION, MULTIMEDIA ASSISTANT: (i) Proficiency in Documentation & Web Designing Tools with experience in writing User Manuals for Software Products etc. (ii) Graphic Designing with experience in computer designing and graphics with a creative bent of mind, around 25 years, and possessing 2-3 yrs. of experience.

TECHNICAL ASSISTANT: Diploma in Electrical Engineering with experience in O & M of electrical installations like DG Sets, UPS Units, Air- Conditioners, general electrical equipment, working knowledge of computers, around 25 yrs. and 4-5 yrs. experience in related areas.

RECEPTIONIST: Graduate with Typing (Higher) and proficiency in computers, handling EPABX systems, handling courier and travel desks, VMS etc., around 23 yrs. and 1-2 yrs. of experience in computerised environment.

RESEARCH ASSOCIATES: Post graduates preferably with specialization in IT/CS/Management or related areas, with 1 – 2 yrs. of experience in Communication/Networking, Crypto API, Security Technology, Financial Management, IT Management and having proficiency in Software Development and Programming.

Candidates fulfilling the above criteria may mail their detailed resumes clearly superscribing on the envelope the Post Applied for to: The Director, IDRBT at the address below or email to: recruit2002@idrbt.ac.in at the earliest.

Forthcoming Programmes

Nov : 07 - 16
Certificate Course in Enterprise Network Technologies & Security – Part I

Nov :18 – 19
Principals' Conference on E-Learning

Nov :27 – 29
Network Security and Audit

Dec: 02 – 07
Electronic Banking and Payments

Dec: 16 – 18
INDOCRYPT 2002 – International Conference on Cryptology in India

Dec: 19 – 28
Certificate Course in Enterprise Network Technologies & Security – Part II

Dec: 23 – 24
Symposium on Technology Projects for Banks

Jan 2003: 06 – 11
Data Warehousing and Data Mining

Jan: 20 – 25
Leveraging Linux for Banks

Feb: 03 – 08
Networking Technologies

Feb: 10 – 15
CRM for Banking

Feb 24 – Mar 01
Decision and Control Technologies for Banks

Mar 17 - 18
Workshop on Data Warehousing Technologies

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 • Website:http://www.idrbt.com; http://www.idrbt.ac.in