# CERTIFICATE PRACTICES

# FOR

# PDO NDS SUBSCRIBERS

**Version 2.0**

(IDRBTCA/DOC/NDS/2.0)

**IDRBT CA,**
**IDRBT,**
**Castle Hills, Road No. 1**
**Masab Tank, Hyderabad,**
**Andhra Pradesh – 500057, India**
**Ph: 040 23534981/23534982**
**Fax: 040 23535157/23536365**
**Email: idrbtca@idrbt.ac.in**

# INDEX

## 1. INTRODUCTION

RBI has commenced an integrated project on **Negotiated Dealing System**, which will provide electronic dealing platform for trading in government securities and money market instruments and computerization of its Public Debt Offices for complete automation of the operations (called the **PDO-NDS Project**). The Project will facilitate electronic bidding in auctions and transparency of trades in secondary market transactions in Government securities on a real time basis.

## 2. SCOPE

IDRBT Certifying Authority (IDRBT CA), the licensed Certifying Authority under Controller of Certifying Authorities, Govt. of India will issue digital certificates for Banks and Financial Institutions for PDO NDS application. The certificates are issued for certain period of validity. On reaching the validity IDRBT CA notifies the subscribers regarding the expiry of the same. Subscribers should make new certificate request upon the expiry of the existing certificate.

## 3. PROCEDURES FOR OBTAINING DIGITAL CERTIFICATE FOR PDO NDS APPLICATION

- The digital certificate will be issued to the server, which hosts the PDO NDS application.
- For obtaining the digital certificate the bank/financial institution/organization must authorize an official in charge of the PDO NDS Server.

- The authorized persons will apply for Class 3 digital certificates along with the documents mentioned in sections 3.1 and 3.2 given below.

### 3.1. New applicant* of PDO NDS Application

Present himself before the RA Office with duly filled application form (given in Appendix-1) accompanied with the relevant document mentioned below.

Original copies of **any one** of the documents (Photocopies also must be furnished.)

- ▪ Passport
- ▪ Voter's ID
- ▪ PAN Card
- ▪ Driving License
- ▪ Any other photo identity document issued by government

✓ One Passport size photograph pasted on application form

✓ Three floppies to copy the certificate/key

✓ Three envelopes to store the password of key

The procedures for creating request and applying online are described in detail in Appendix-3.

*** New applicant means an authorized official who is applying for new certificate,**

**or**

**an authorized official who is newly appointed in place of earlier official who was in-charge.**

### 3.2. Existing Subscriber of PDO-NDS Application

An authorized official already holding the responsibility of the PDO NDS application in his organization and is assigned the UserId by RA office has to apply a fresh certificate request along with the duly filled application form as per Appendix-1. **Personal presence in front of RA is not required in this case.** The procedures for creating request and applying online are described in detail in Appendix-3.

## 4. COST OF DIGITAL CERTIFICATE

The validity of the digital certificate will be for two years.

The cost of Class 3 PDO NDS Certificate is as given below:

a. For those who have selected IDRBT RA Office (for Banks/FIs/Govt. Agencies) as RA: **Rs. 21,000/-** for two years (Rs. 20,000/- for certificate fees + Rs. 1,000/- for administrative charges).
b. For those who requests through their own RA Office: **Rs. 20,000/-** for two years

The certificate fee details are published in IDRBT CA's website http://idrbtca.org.in/ . Any changes in the certificate fees will be notified in the website.

The cost must be borne by the Subscriber. The amount must be paid by means of **Demand Draft** taken in favour of **IDRBT payable at Hyderabad**.

## 5. DISTRIBUTION OF DIGITAL CERTIFICATE

The digital certificate issued for PDO NDS subscribers will be taken on media (on floppy) after the verification by RA Office and issuance by IDRBT CA. The copies of the certificate and the private key file will be made in floppies for further use.

## 6. REVOCATION OF DIGITAL CERTIFICATE

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

- The subscriber loses relevant privileges;
- The information provided by the end entity is inaccurate, e.g. when the owner of an identity certificate change their name
- The subscriber changes his organization
- An end entity makes the request for the revocation
- Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of IDRBT CA Digital Certificate
- The Subscriber has breached or failed to meet their obligations under this CPS or any other agreement, regulation or law which may be in force
- Any other circumstances which shall be determined by rules and regulations to governing law

A revocation request can be made by the holder of the certificate to be revoked to the IDRBT CA. The revocation request must be in written format as per **Appendix - 2** and should be propagated to IDBRT CA either by fax, courier or post.

NB: If the revocation of the certificate is initiated due to the negligence or any fault from the user, the certificate fees will be levied for the new certificate application.

## APPENDIX -1

# APPLICATION FORM FOR ISSUE OF DIGITAL CERTIFICATE

*** Fields are mandatory** **#Strike off which are not applicable** **New user /Existing user**

| | |
|---|---|
| **Certificate Applied*:** Class 3 | **Certificate required*:** Individual/ Server |
| **Type of Certificate * :** Signing | **Certificate Validity:** 2yrs |

## Personal Details:

| | | |
|---|---|---|
| **Name*:** | | |
| **Email Address*:** | | |
| **Office Address*:**<br>**(with Designation and Department)** | | |
| | | |
| | | |
| | | |
| | **Pincode*:** | **Telephone*:** |

**Identification Details*** (Passport No/PAN Card No/Voter's ID Card No/Driving License No/PF No/Employee ID)**:**

**Details of Server * (name of the server)**:

**Important Notice:**

- This application form is to be filled by the applicant.
- All subscribers are advised to read IDRBT CA Certificate Practice Statement (download from **http://idrbtca.org.in/**)
- All documents specified in CPS for each Certificate Class must be accompanied with this application form.
- Application form must be submitted in person to the Registration Authority for face-to-face recognition in the case of Class 3 Certificate.
- Incomplete/Inconsistent application is liable to be rejected.

### *Declaration and Undertaking by the Applicant*

All the above information provided by me is true to the best of my knowledge and belief. I am submitting this application as an authorized person for and on behalf of the organisaton/government department for carrying out only authorized transactions by using the Digital Certificate in the discharge of my official duties. 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 Superior Officer/RA/ IDRBT CA in event of key compromise. I agree to publish the Digital Certificate in the IDRBT CA repository and will report my Registration Authority of any error or defect in the certificate and change in the above information.

Date:

Place:

Name of the Applicant: (Signature of the applicant)

### *For Superior Authority of Applicant**

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

Date:

Place:

Name of Officer:

Official Email: (Signature of Officer with stamp of Org./office)

**For RA Purpose only**

| **Checklist** | **Date & Time with Initials** |
|---|---|
| Received the application form for digital certificate? | |
| Verified the photocopies of the identification document(Passport/Voter's ID/PAN Card/Domain registration)? | |
| Face-to-Face verification? (in case of Class 3 Certificate) | |

## APPENDIX - 2

## Certificate Revocation/Suspension Form

□ Certificate Revocation □ Certificate Suspension

(Tick Applicable)

*Certificate Revocation/Suspension Request* Date:

To:

____________________________________________

____________________________________________

____________________________________________

____________________________________________

____________________________________________

**Instructions:**

1. Fill in the Certificate Revocation Request Form and submit to the IDRBT CA authorized Registration Authority in person or fax or post.
2. 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 Identity Card/Income Tax PAN Card.
3. The soft copy of Digital Certificate must be sent as an email to the IDRBT CA mentioning "Certificate Revocation/Suspension Request" as the subject or in a floppy disk accompanying the form if it is by post.

**Certificate Details**

Certificate Serial Number: ________________________________

Category of Certificate: □ Signing □ Encryption □ Server □ Object Signing
(Tick applicable)

Public Key of Holder: (Attach soft copy of Digital Certificate)

**Certificate Owner Details**

Name of Holder: ________________________________

Email Address: ____________________

□ User Compromise □ Key Compromise

Details:
____________________
____________________
____________________

Authorised by: □ Certificate Owner
□ Third Party
(Documentation verifying authorisation must be sighted)

Name: ____________________ Signature: ____________________

Contact No: ____________________ Email: ____________________

**For Registration Authority Use Only**

| ITEM | Completed | Date | Initials |
|---|---|---|---|
| Request form (person/fax/post) | Yes/No | | |
| Digital Certificate soft copy(email/floppy) | Yes/No | | |
| Identification document of the third party if any? | Yes/No | | |

| | |
|---|---|
| Date Received:<br>Subscriber notified by: | □ Person □ Fax □ Post |
| Revoked/Susepended by IDRBT CA<br>Date:<br>Initials: | |

## APPENDIX –3

### User Manual for Digital Certificates for PDO NDS

IDRBT CA's i-trust PKI Services is available on INFINET and Internet.

Visit IDRBT CA's official website on INFINET at http://idrbtca.org.in/. This website contains the information about the IDRBT CA Certification Practice Statement, the classes of digital certificates offered by IDRBT CA, general information about PKI, Registration Authorities, Information Technology Act, Subscriber Agreement, Privacy Statement, Frequently Asked Questions, IDRBT CA support Desk, etc.

**Contacting IDRBT CA Technical Support:**

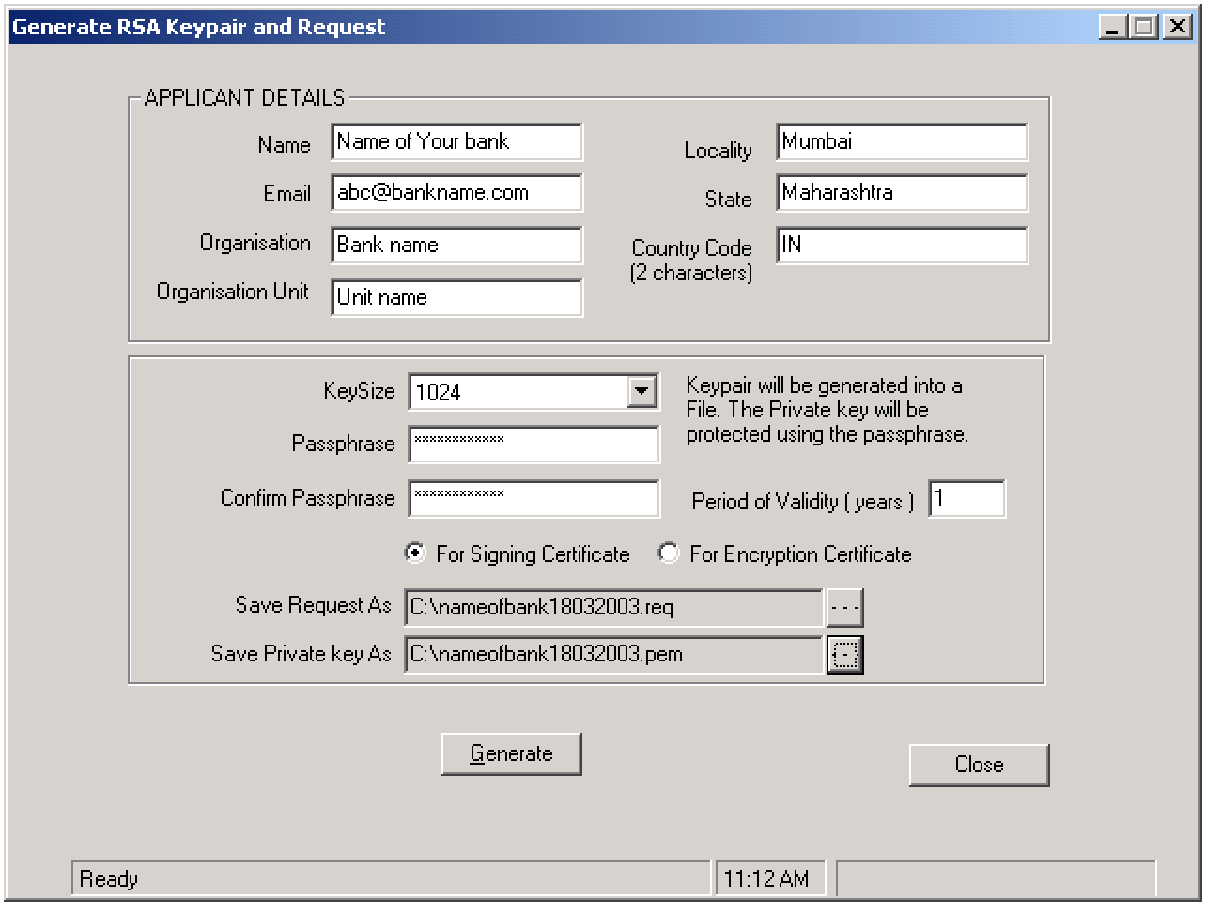
i-trust PKI Customer Services team is committed to supporting the users. If you have any questions, need additional assistance, or encounter a problem, please contact the following:

| IDRBT CA i-trust PKI Services Support Team | |
|---|---|
| INFINET | http://idrbtca.org.in/ , http://infinet.org.in/ |
| INTERNET | http://www.idrbt.com/ |
| E-mail | cahelp@idrbt.ac.in |
| Telephone | +91-40-23536297 or 23534981/82 Extn- 5216/5217 |
| Fax | +91-40-23536371 |

## STEPWISE PROCEDURES FOR REQUESTING A DIGITAL CERTIFICATE:

### 1. Procedure to generate the Certificate Request

- The applicant will generate a certificate request using RequestGen software. The sample of details to be filled is shown in fig 1.



Generate RSA Keypair and Request

APPLICANT DETAILS

Name: Name of Your bank

Email: abc@bankname.com

Organisation: Bank name

Organisation Unit: Unit name

Locality: Mumbai

State: Maharashtra

Country Code (2 characters): IN

KeySize: 1024

Passphrase: *************

Confirm Passphrase: *************

Keypair will be generated into a File. The Private key will be protected using the passphrase.

Period of Validity ( years ): 1

● For Signing Certificate ○ For Encryption Certificate

Save Request As: C:\nameofbank18032003.req

Save Private key As: C:\nameofbank18032003.pem

Fig 1. Details to be filled in RequestGen software.

The details to be filled are as follows:

- Name (the name of bank/financial institution)
- Email (email address of the bank/FI department)

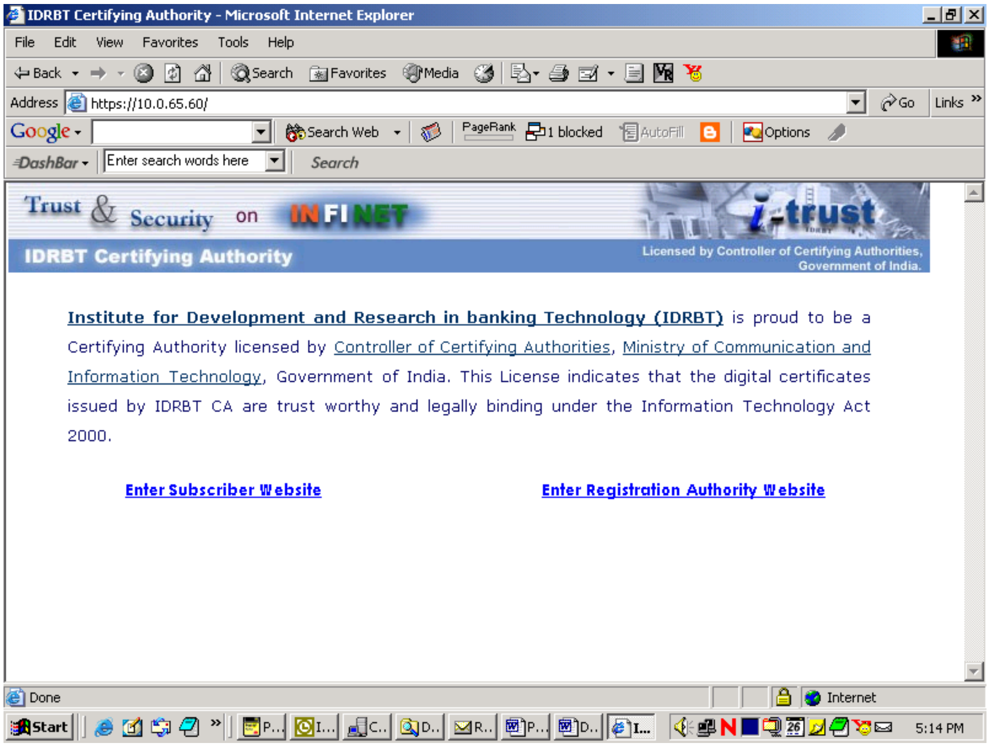
- Organisation (name of the bank/FI)
- Organisation Unit (name of the department/unit)
- Locality (City name where the server is hosted)
- State
- Country code (IN for India)
- Key Size (select 1024)
- Passphrase (give a password not more than 12 characters. This password will be copied in triplicate and to be kept in safe custody.)
- Confirm Passphrase
- Period of validity (Two years)
- For Signing Certificate (select this option)
- Save request as (the file name convention should include name of bank and the date of creation, for e.g. nameofbank18032003.req)
- Save Private Key as (the file name convention should include name of bank and the date of creation, for e.g. nameofbank18032003.pem)

The applicant will then apply for Class 3 Signing Certificate through IDRBT CA Certification Services choosing the RA Office and will paste the request generated using RequestGen software in the corresponding field as mentioned in the below mentioned procedures.

## 2. Online request

After generation of PKCS#10 request (.req) through RequestGen application, the applicant has to login to the IDRBT site through https://10.0.65.60/ (on INFINET) or https://services.idrbtca.org.in/ (on Internet).

Fig 2 shows the home page of IDRBT CA Service


IDRBT Certifying Authority - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.0.65.60/
Go Links
Search Web PageRank 1 blocked AutoFill Options
DashBar Enter search words here Search
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
Done
Internet
Start
5:14 PM

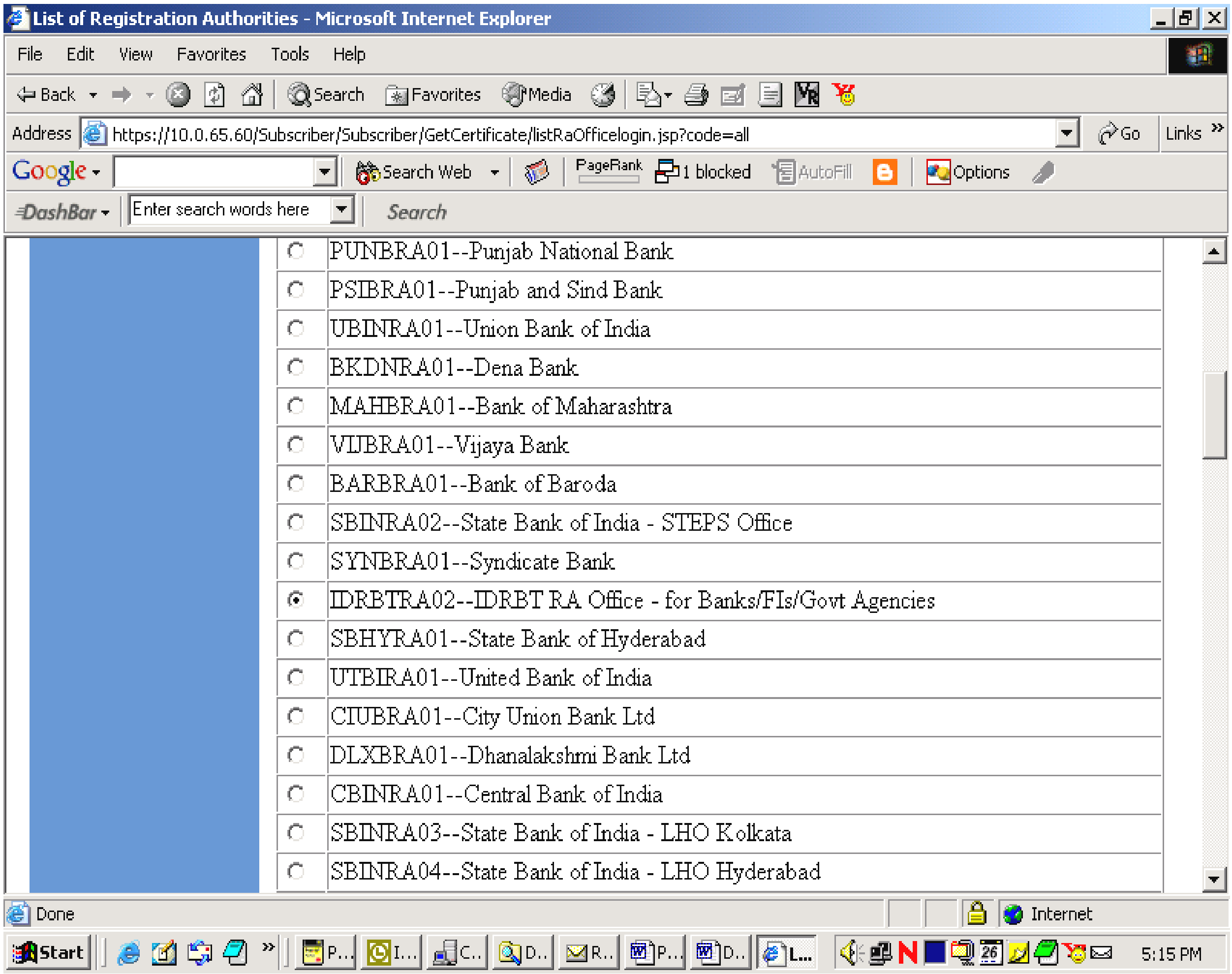
Institute for Development and Research in banking Technology (IDRBT) is proud to be a Certifying Authority licensed by Controller of Certifying Authorities, Ministry of Communication and Information Technology, Government of India. This License indicates that the digital certificates issued by IDRBT CA are trust worthy and legally binding under the Information Technology Act 2000.

Enter Subscriber Website

Enter Registration Authority Website

Fig-2

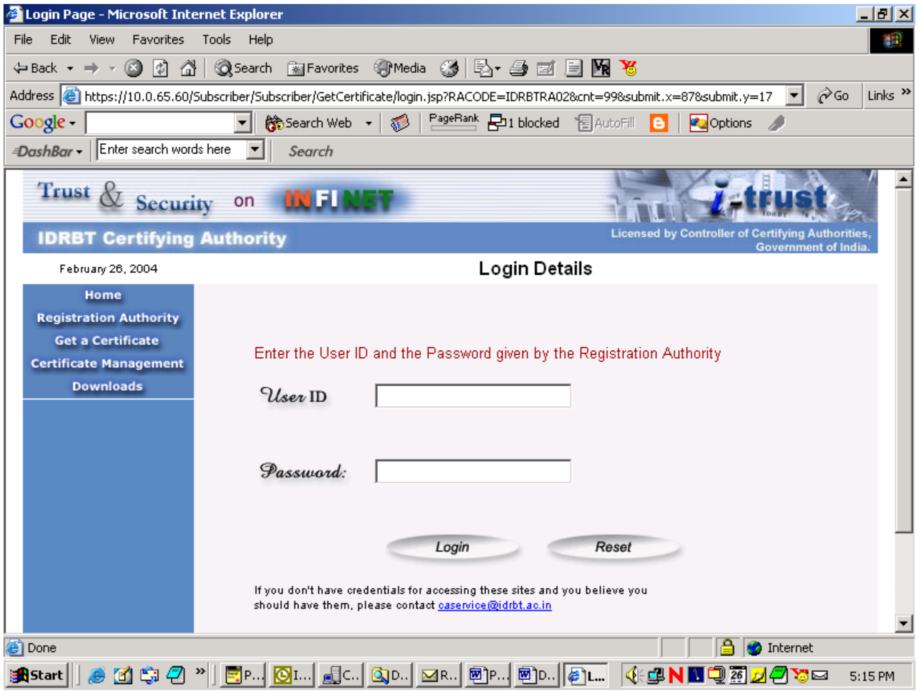
Click on “Enter Subscriber Website”, which will direct you to the main page of Subscriber’s site and select “Get a Digital Certificate” link. Click “Login” button to enter into the page where you can select the Registration Authority (RA) from the list of RAs as shown in Fig 3.


List of Registration Authorities - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.0.65.60/Subscriber/Subscriber/GetCertificate/listRaOfficelogin.jsp?code=all
Go Links
Google Search Web PageRank 1 blocked AutoFill Options
DashBar Enter search words here Search
Done
Internet
Start P... I... C... D... R... P... D... L...
5:15 PM

○ PUNBRA01--Punjab National Bank
○ PSIBRA01--Punjab and Sind Bank
○ UBINRA01--Union Bank of India
○ BKDNRA01--Dena Bank
○ MAHBRA01--Bank of Maharashtra
○ VIJBRA01--Vijaya Bank
○ BARBRA01--Bank of Baroda
○ SBINRA02--State Bank of India - STEPS Office
○ SYNBRA01--Syndicate Bank
● IDRBTRA02--IDRBT RA Office - for Banks/FIs/Govt Agencies
○ SBHYRA01--State Bank of Hyderabad
○ UTBIRA01--United Bank of India
○ CIUBRA01--City Union Bank Ltd
○ DLXBRA01--Dhanalakshmi Bank Ltd
○ CBINRA01--Central Bank of India
○ SBINRA03--State Bank of India - LHO Kolkata
○ SBINRA04--State Bank of India - LHO Hyderabad

Fig-3

Select the RA office from which you have obtained the User ID and Password and click “Submit” button. This will guide you to the login page where you are prompted to enter the UserID and Password as shown in Fig 4.


Login Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.0.65.60/Subscriber/Subscriber/GetCertificate/login.jsp?RACODE=IDRBTRA02&cnt=99&submit.x=87&submit.y=17
Go Links
Google Search Web PageRank 1 blocked AutoFill Options
DashBar Enter search words here Search
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
Home
Registration Authority
Get a Certificate
Certificate Management
Downloads
Login
Reset
Done
Internet
Start
5:15 PM

February 26, 2004

Login Details

Enter the User ID and the Password given by the Registration Authority

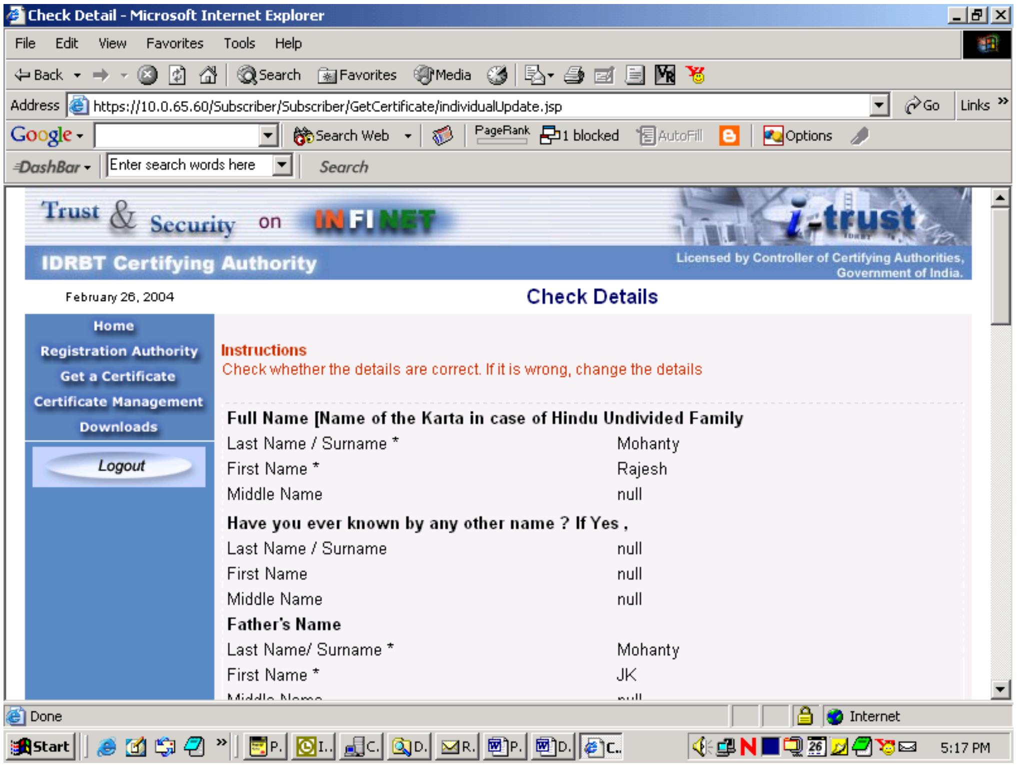
User ID

Password:

If you don't have credentials for accessing these sites and you believe you should have them, please contact caservice@idrbt.ac.in

Fig-4

Enter the User ID and Password given to you and click "Login" button. If you had already applied for a certificate, the details will be displayed as given in Fig 5.


Check Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.0.65.60/Subscriber/Subscriber/GetCertificate/individualUpdate.jsp
Go Links
Google Search Web PageRank 1 blocked AutoFill Options
DashBar Enter search words here Search
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
Home
Registration Authority
Get a Certificate
Certificate Management
Downloads
Logout
Done
Internet
Start
5:17 PM

February 26, 2004

Check Details

Instructions
Check whether the details are correct. If it is wrong, change the details

Full Name [Name of the Karta in case of Hindu Undivided Family

| | |
|---|---|
| Last Name / Surname * | Mohanty |
| First Name * | Rajesh |
| Middle Name | null |

Have you ever known by any other name ? If Yes ,

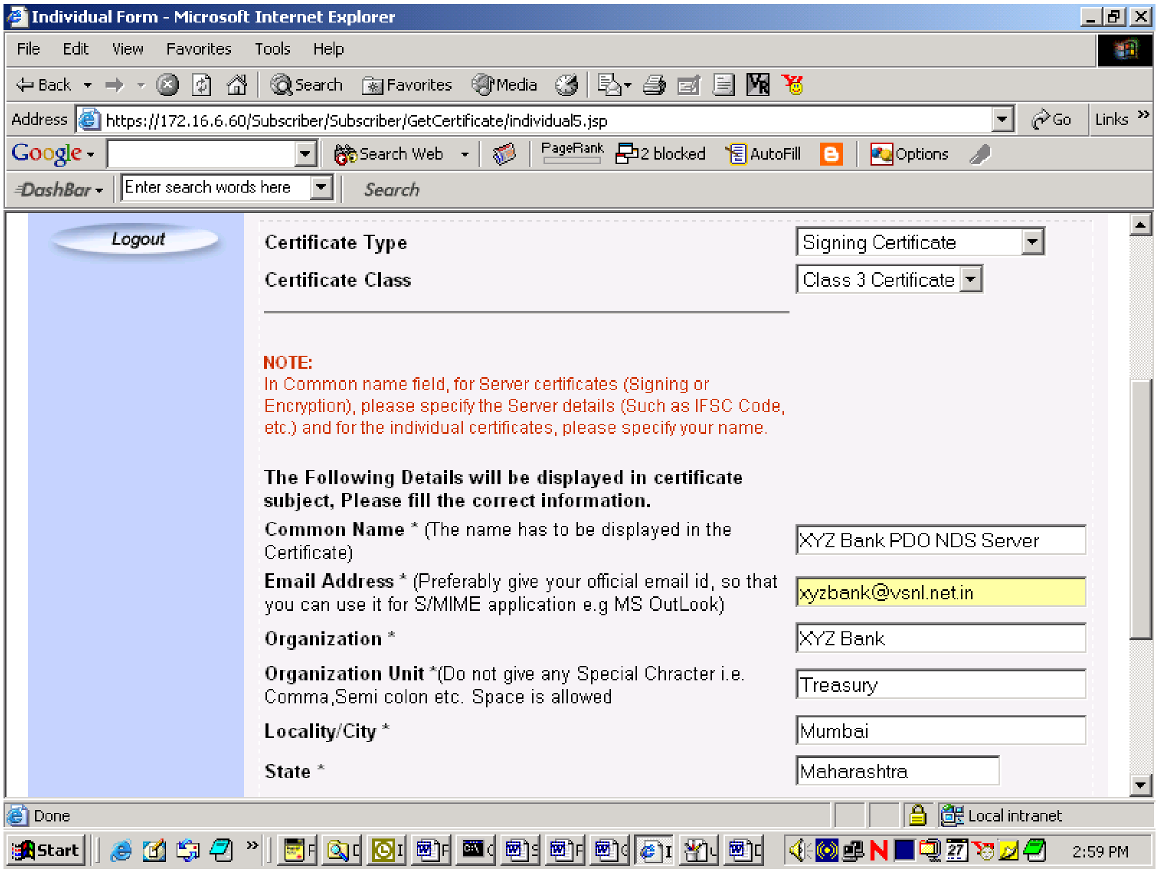
| | |
|---|---|
| Last Name / Surname | null |
| First Name | null |
| Middle Name | null |

Father's Name

| | |
|---|---|
| Last Name/ Surname * | Mohanty |
| First Name * | JK |
| Middle Name | null |

Fig-5

Click on submit button to proceed further to the next page as given in Fig 6.


Individual Form - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.16.6.60/Subscriber/Subscriber/GetCertificate/individual5.jsp
Go Links
Search Web PageRank 2 blocked AutoFill Options
DashBar Enter search words here Search
Logout
Done
Local intranet
Start
2:59 PM

| | |
|---|---|
| **Certificate Type** | Signing Certificate |
| **Certificate Class** | Class 3 Certificate |

NOTE:
In Common name field, for Server certificates (Signing or Encryption), please specify the Server details (Such as IFSC Code, etc.) and for the individual certificates, please specify your name.

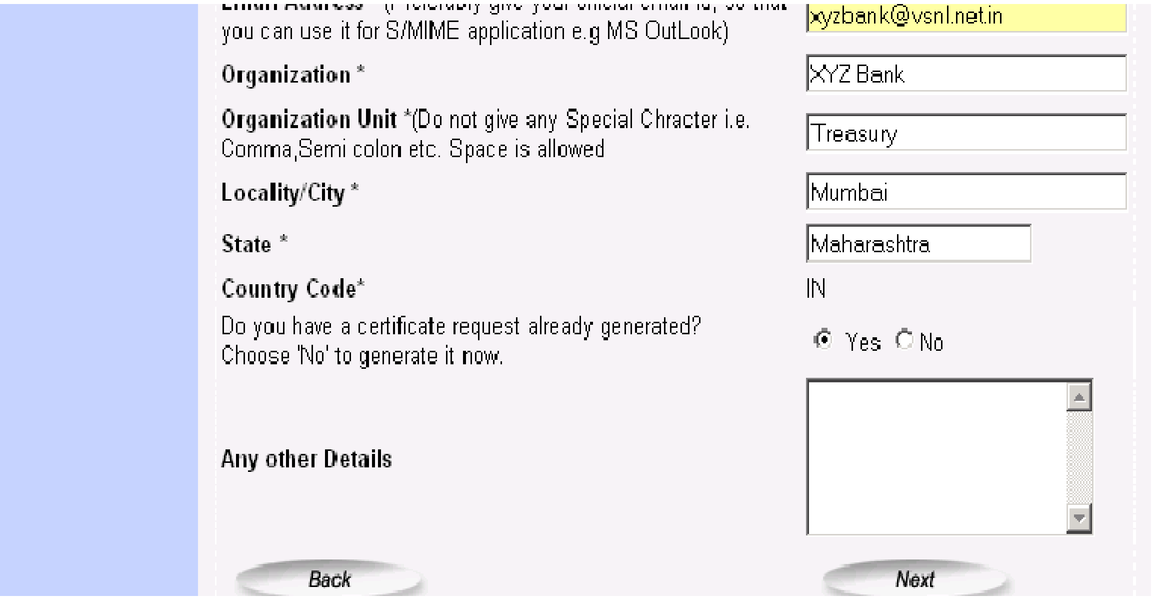
**The Following Details will be displayed in certificate subject, Please fill the correct information.**

| | |
|---|---|
| **Common Name** * (The name has to be displayed in the Certificate) | XYZ Bank PDO NDS Server |
| **Email Address** * (Preferably give your official email id, so that you can use it for S/MIME application e.g MS OutLook) | xyzbank@vsnl.net.in |
| **Organization** * | XYZ Bank |
| **Organization Unit** *(Do not give any Special Chracter i.e. Comma,Semi colon etc. Space is allowed | Treasury |
| **Locality/City** * | Mumbai |
| **State** * | Maharashtra |

Fig-6

Select Certificate type as **"Signing Certificate"** and Certificate class as **"Class 3"**. Fill the details of your PDO NDS server.

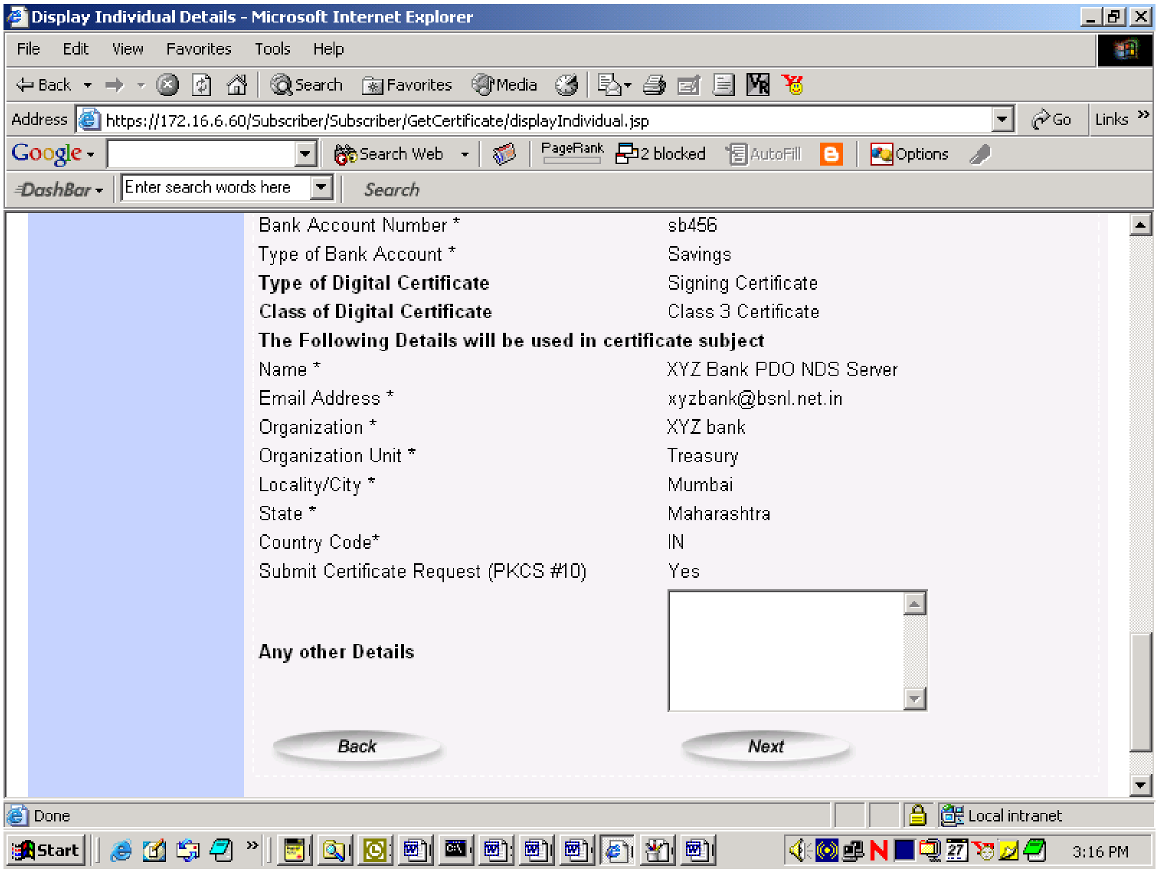
Note: You have already generated PKCS#10 Certificate request **(.req file)** for your PDO NDS server using RequestGen software. Check the 'Yes' radio button as in Fig 7 given below and click "Next" to proceed.



| | |
|---|---|
| Email Address * (Preferably give your official email id, so that you can use it for S/MIME application e.g MS OutLook) | xyzbank@vsnl.net.in |
| **Organization** * | XYZ Bank |
| **Organization Unit** *(Do not give any Special Chracter i.e. Comma,Semi colon etc. Space is allowed | Treasury |
| **Locality/City** * | Mumbai |
| **State** * | Maharashtra |
| **Country Code*** | IN |
| Do you have a certificate request already generated? Choose 'No' to generate it now. | ● Yes ○ No |
| **Any other Details** | |

Fig-7

You can view all the details, which you have filled as shown in the Fig 8.



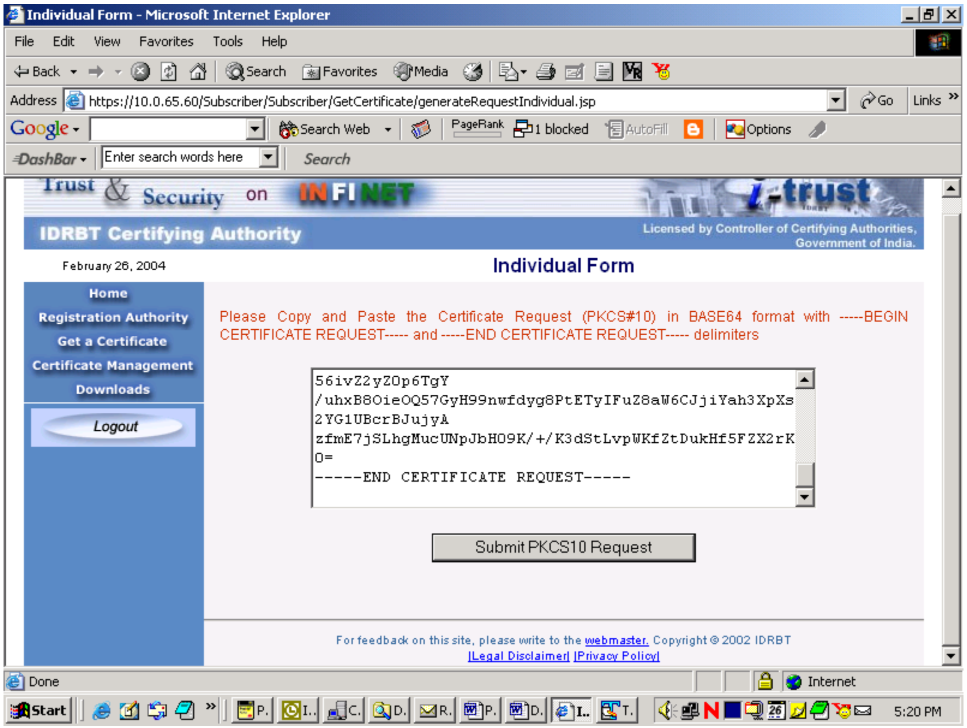
Display Individual Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google Search Web PageRank 2 blocked AutoFill Options
DashBar Enter search words here Search

https://172.16.6.60/Subscriber/Subscriber/GetCertificate/displayIndividual.jsp

| | |
|---|---|
| Bank Account Number * | sb456 |
| Type of Bank Account * | Savings |
| **Type of Digital Certificate** | Signing Certificate |
| **Class of Digital Certificate** | Class 3 Certificate |
| **The Following Details will be used in certificate subject** | |
| Name * | XYZ Bank PDO NDS Server |
| Email Address * | xyzbank@bsnl.net.in |
| Organization * | XYZ bank |
| Organization Unit * | Treasury |
| Locality/City * | Mumbai |
| State * | Maharashtra |
| Country Code* | IN |
| Submit Certificate Request (PKCS #10) | Yes |
| **Any other Details** | |

Fig-8

Click "Next" button to proceed further and will take you the page where you can paste the PKCS#10 certificate request as shown in Fig 9.


Individual Form - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.0.65.60/Subscriber/Subscriber/GetCertificate/generateRequestIndividual.jsp
Go Links
Google Search Web PageRank 1 blocked AutoFill Options
DashBar Enter search words here Search
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
February 26, 2004
Home
Registration Authority
Get a Certificate
Certificate Management
Downloads
Logout
Submit PKCS10 Request
Done
Internet
Start
5:20 PM

Individual Form

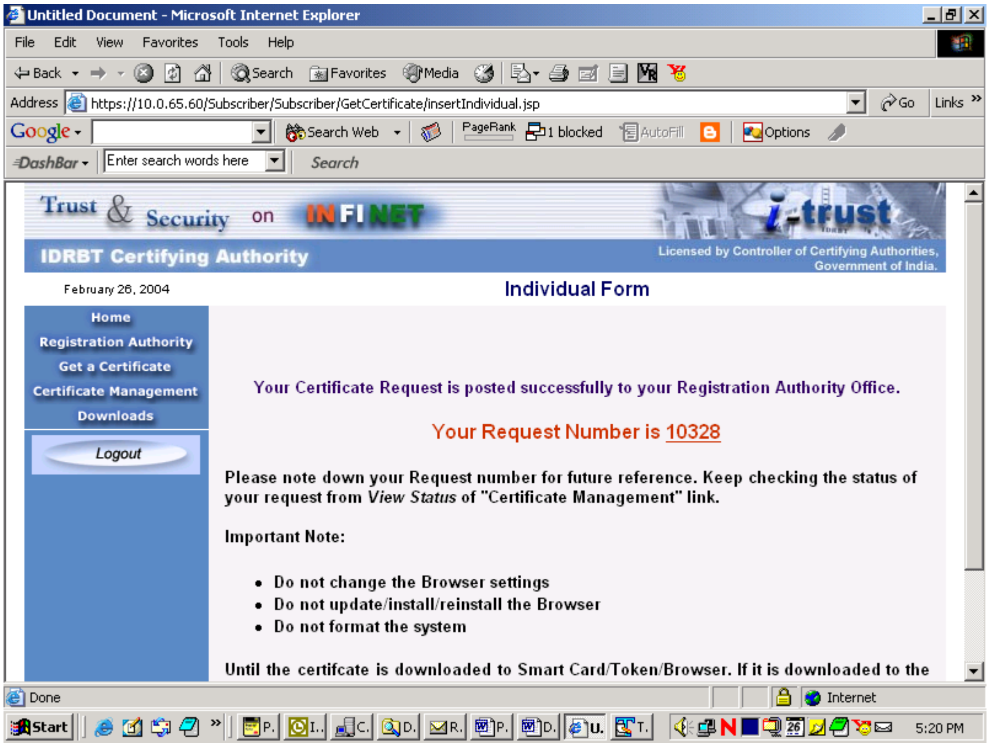
Please Copy and Paste the Certificate Request (PKCS#10) in BASE64 format with -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- delimiters

```
56ivZ2yZOp6TgY
/uhxB8OieOQ57GyH99nwfdyg8PtETyIFuZ8aW6CJjiYah3XpXs
2YG1UBcrBJujyA
zfmE7jSLhgMucUNpJbHO9K/+/K3dStLvpWKfZtDukHf5FZX2rK
O=
-----END CERTIFICATE REQUEST-----
```

For feedback on this site, please write to the webmaster. Copyright © 2002 IDRBT
|Legal Disclaimer| |Privacy Policy|

Fig-9

Copy the entire content of your .req file starting from -----BEGIN CERTIFICATE REQUEST----- to -----END CERTIFICATE REQUEST-----, and paste it in the space provided. Click on "Submit PKCS#10 Request" button. If the request is in correct format, it will give you a request number as given in Fig 10. You can note down this request number for further course of action.



Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.0.65.60/Subscriber/Subscriber/GetCertificate/insertIndividual.jsp
Go Links
Google Search Web PageRank 1 blocked AutoFill Options
DashBar Enter search words here Search
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
Home
Registration Authority
Get a Certificate
Certificate Management
Downloads
Logout
Done
Internet
Start
5:20 PM

February 26, 2004

Individual Form

Your Certificate Request is posted successfully to your Registration Authority Office.

Your Request Number is 10328

Please note down your Request number for future reference. Keep checking the status of your request from *View Status* of "Certificate Management" link.

Important Note:

- Do not change the Browser settings
- Do not update/install/reinstall the Browser
- Do not format the system

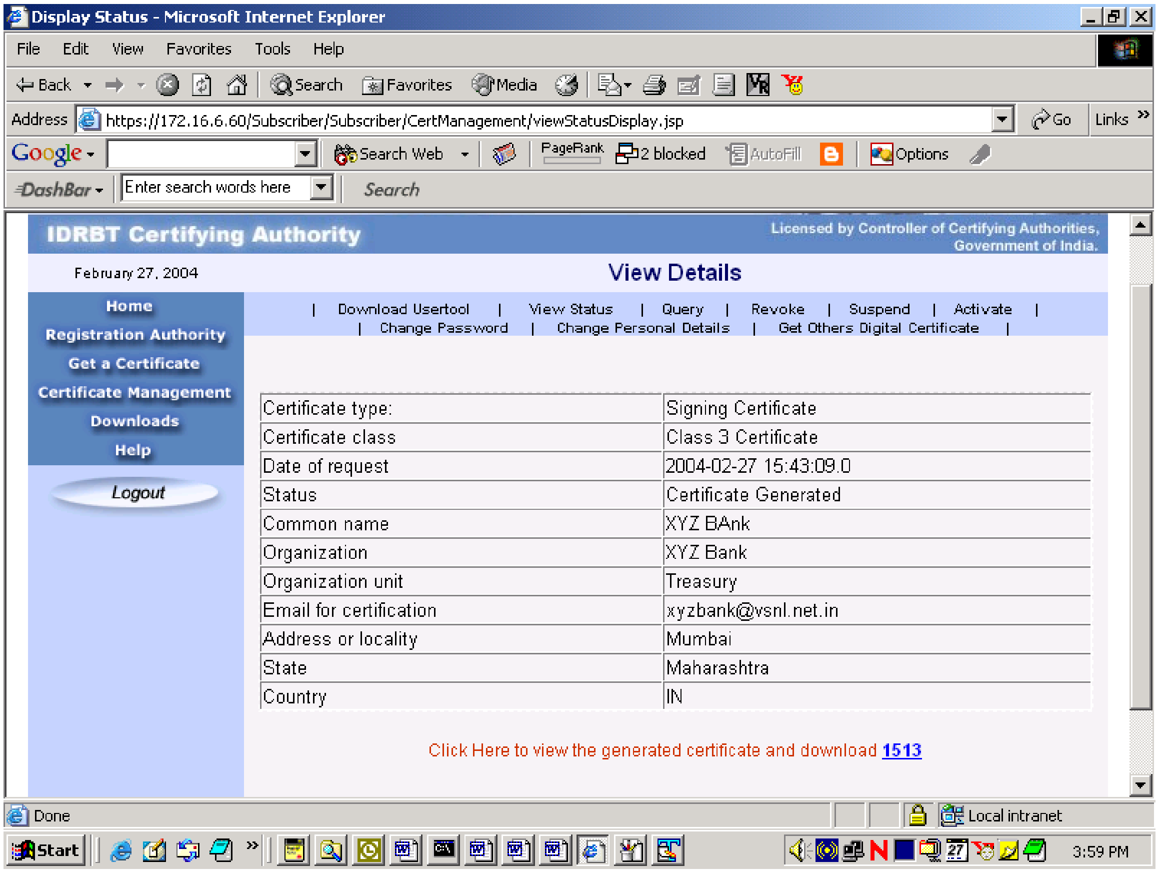
Until the certifcate is downloaded to Smart Card/Token/Browser. If it is downloaded to the

Fig-10.

IDBRT CA will issue the certificate for your certificate request.

## 3. Downloading Certificate

After the certificate is generated you can download the same. You can check the status of the request by querying your certificate request status by clicking the "**Certificate Management"** link in the homepage of IDRBT CA's website (https://10.0.65.65/ on INFINET or https://services.idrbtca.org.in/ on Internet). You should login to the site by selecting the RA Office and click "**View Status"** on the top menu and enter your request number. The status of your request will be displayed as given in Fig 11.

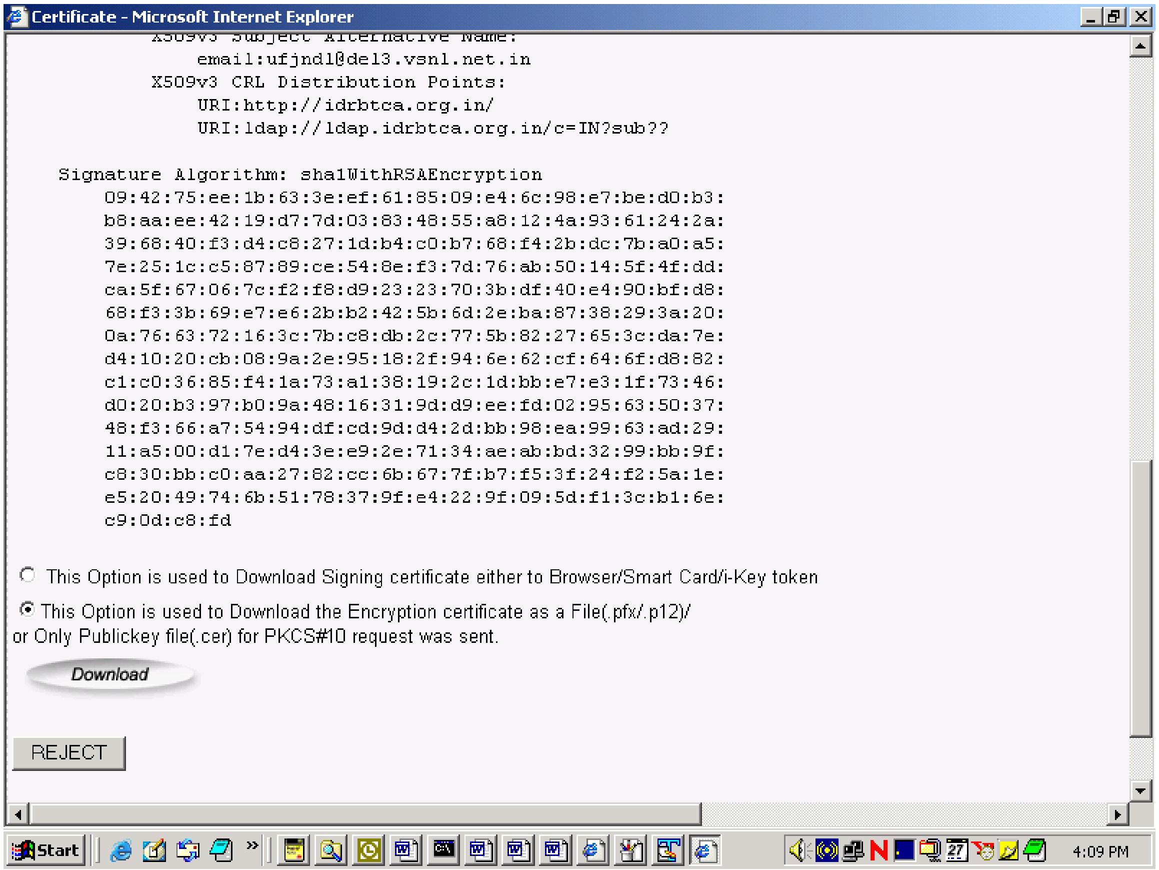

Display Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.16.6.60/Subscriber/Subscriber/CertManagement/viewStatusDisplay.jsp
Go Links
Google Search Web PageRank 2 blocked AutoFill Options
DashBar Enter search words here Search
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
February 27, 2004
View Details
Home
Registration Authority
Get a Certificate
Certificate Management
Downloads
Help
Logout
| Download Usertool | View Status | Query | Revoke | Suspend | Activate |
| Change Password | Change Personal Details | Get Others Digital Certificate |
Done
Local intranet
Start
3:59 PM

| | |
|---|---|
| Certificate type: | Signing Certificate |
| Certificate class | Class 3 Certificate |
| Date of request | 2004-02-27 15:43:09.0 |
| Status | Certificate Generated |
| Common name | XYZ BAnk |
| Organization | XYZ Bank |
| Organization unit | Treasury |
| Email for certification | xyzbank@vsnl.net.in |
| Address or locality | Mumbai |
| State | Maharashtra |
| Country | IN |

Click Here to view the generated certificate and download 1513

Fig-11

If the status of the certificate request is "Certificate Generated", click on the highlighted link corresponding to your request number to proceed for download. On clicking the link, it will prompt you to agree with terms and condition of IDRBT CA. Proceed further by clicking the "I Agree" button. This will guide you to the page where you can download the certificate after viewing the details as shown in Fig 12.



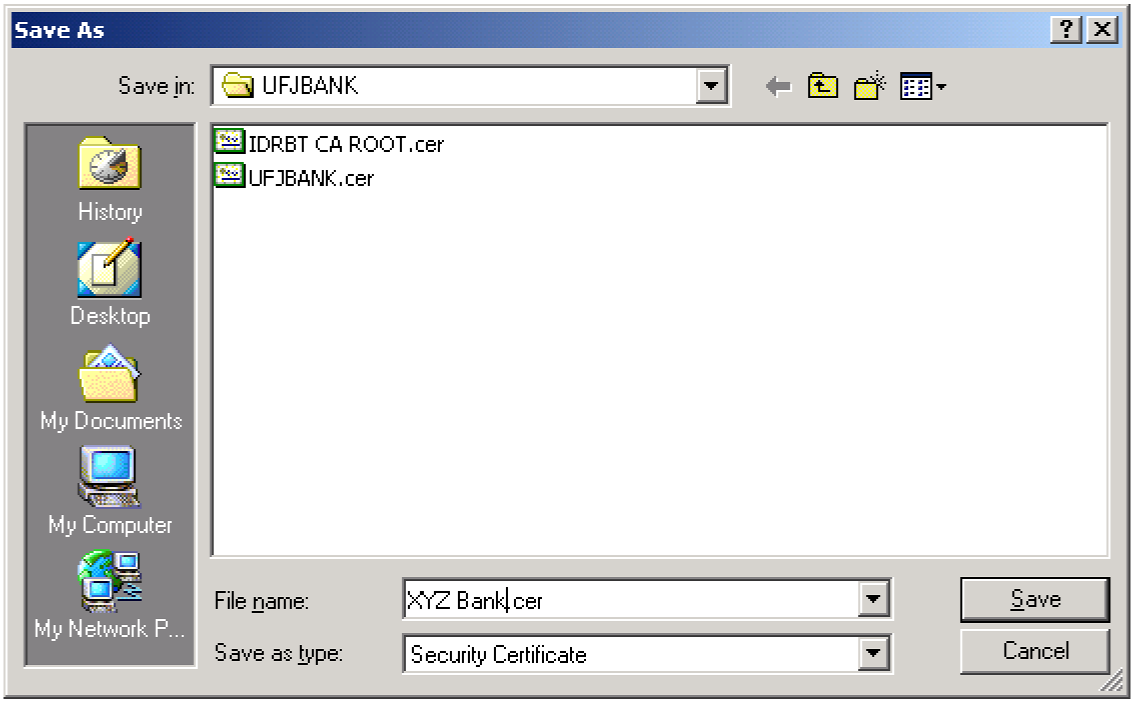
```
            X509v3 Subject Alternative Name:
                email:ufjndl@del3.vsnl.net.in
            X509v3 CRL Distribution Points:
                URI:http://idrbtca.org.in/
                URI:ldap://ldap.idrbtca.org.in/c=IN?sub??

    Signature Algorithm: sha1WithRSAEncryption
        09:42:75:ee:1b:63:3e:ef:61:85:09:e4:6c:98:e7:be:d0:b3:
        b8:aa:ee:42:19:d7:7d:03:83:48:55:a8:12:4a:93:61:24:2a:
        39:68:40:f3:d4:c8:27:1d:b4:c0:b7:68:f4:2b:dc:7b:a0:a5:
        7e:25:1c:c5:87:89:ce:54:8e:f3:7d:76:ab:50:14:5f:4f:dd:
        ca:5f:67:06:7c:f2:f8:d9:23:23:70:3b:df:40:e4:90:bf:d8:
        68:f3:3b:69:e7:e6:2b:b2:42:5b:6d:2e:ba:87:38:29:3a:20:
        0a:76:63:72:16:3c:7b:c8:db:2c:77:5b:82:27:65:3c:da:7e:
        d4:10:20:cb:08:9a:2e:95:18:2f:94:6e:62:cf:64:6f:d8:82:
        c1:c0:36:85:f4:1a:73:a1:38:19:2c:1d:bb:e7:e3:1f:73:46:
        d0:20:b3:97:b0:9a:48:16:31:9d:d9:ee:fd:02:95:63:50:37:
        48:f3:66:a7:54:94:df:cd:9d:d4:2d:bb:98:ea:99:63:ad:29:
        11:a5:00:d1:7e:d4:3e:e9:2e:71:34:ae:ab:bd:32:99:bb:9f:
        c8:30:bb:c0:aa:27:82:cc:6b:67:7f:b7:f5:3f:24:f2:5a:1e:
        e5:20:49:74:6b:51:78:37:9f:e4:22:9f:09:5d:f1:3c:b1:6e:
        c9:0d:c8:fd
```

○ This Option is used to Download Signing certificate either to Browser/Smart Card/i-Key token

● This Option is used to Download the Encryption certificate as a File(.pfx/.p12)/
or Only Publickey file(.cer) for PKCS#10 request was sent.

Fig-12

Select the second option to download the certificate as a file. You can save the file by clicking "Download" button, as given in Fig 13.



Save in: UFJBANK

IDRBT CA ROOT.cer
UFJBANK.cer

File name: XYZ Bank.cer

Save as type: Security Certificate

Fig-13

Assign the name to the file and save it to disk as "Security Certificate" type. This file will be saved with **.cer** extension by default.

Keep this file in the specified location on your PDO NDS server along with your private key file (.pem) generated earlier using the RequestGen tool. Contact NDS Helpdesk for further course of action to implement certificates in PDO NDS application.

For more details contact:

cahelp@idrbt.ac.in

Ph: 040-23536297 (Direct)

Ph: 040-23534981 Extn- 5217/5216