Step by Step Procedure to apply for a DSC

Procedure to apply for Digital Certificate:

Please fill up the Application form for Digital Certificate attached herewith. The application form can also be downloaded from https://idrbtca.org.in.

Please ensure that following to be include in and along with application form:

1) Authorization letter from Bank - on Bank's letter head requesting for issue of Digital Certificate
2) Application duly filled in signed by Applicant and Superior Authority with Official Seal affixed on Second page of the Application
3) One Passport Size Photograph to be affixed on the Right corner of the First page of the Application and **to be signed across the Photograph**
4) Photocopies of PAN and Aadhar card of the Applicant attested by **Superior Authority with Seal** to be attached to Application form
5) Self-attested PAN and ID card of Superior Authority to be attached to the Application form
6) Subscriber Agreement Form duly signed by Applicant
7) GST Number of the Bank / Financial Institution
8) Share the payment details along with UTR Number

Kindly share below the payment details:

Name of Bank	UTR No	Date of Payment	Amount	TDS(if deducted)	Total Amount	GST Number

Physical Verification for Class-2 Subscribers:

With reference to our earlier mails regarding Physical Verification for Class 2 Subscribers, we are furnishing below various options to Registration Authorities to fulfil CCA guidelines with regard to Physical Verification Class 2 DSC subscribers.

Option 1: The subscriber will present himself/herself at the respective Bank's RA office physically with required documents as stipulated in CA application form.

Option 2: The subscriber should participate in video conference with respective RA office with required documents for minimum 30 seconds. The recording must be preserved by respective RA office and shown to auditors for verification, on demand.

Option 3: The subscriber can submit a letter duly authorized by the subscriber's superior authority to the respective RA in the format attached herewith. This option should be exercised by RA only in selective and exceptional cases only and not as matter of routine.

The application form is to be sent to the following address.

Address: -

Institute for Development and Research in Banking Technology [Certifying Authority - PKI Services]
Castle Hills, Road No.1,Behind NMDC, Masab Tank, Hyderabad,500057

Processing by RA:

After scrutiny of the application form, if the details in the application submitted by the subscriber are complete and correct, User Id and Password will be created by CA team and the same will be sent by an automated mail to the mail address of the applicant specified in the application form.

Acknowledgement to be sent to RA by the applicant:

After receiving the mail with User id and Password, the applicant has to take the print out of the mail, sign on it and send the scanned copy of the same to the RA for activating the user id. The applicant will be able to login using the user id and password provided by the RA only upon activation of the user id by the RA concerned.

Procedure for Enrolling and Generating Key Pairs (Initiating online request):

To apply for the SHA2 2048 Class II/Class III Signing certificate using (crypto token) i-key/e-token (dongle):

1. Ensure that your PC and IE Browser Version meet any of the following requirements:

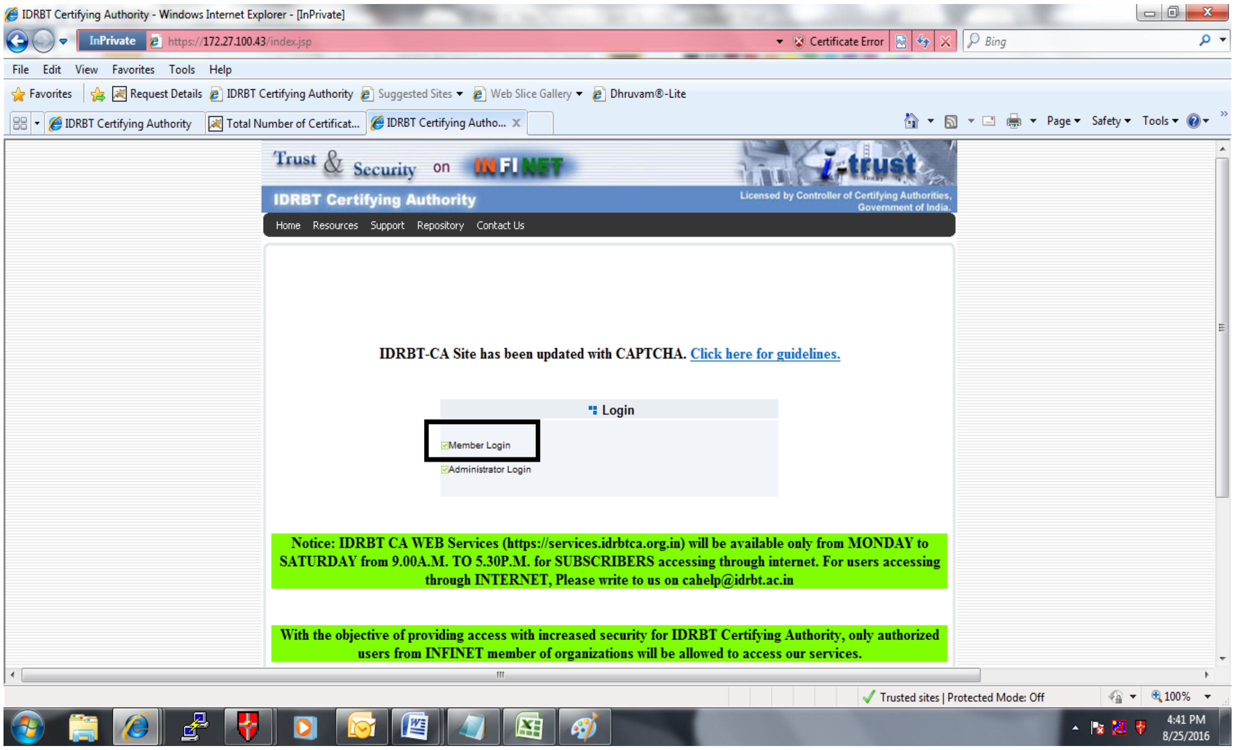
Operating System	OS Bit	Browser	Browser Bit
Windows 7	32	IE10	32
Windows 7	32	IE11	32
Windows 7	64	IE10	32
Windows 7	64	IE10	64
Windows 7	64	IE11	32
Windows 7	64	IE11	64
Windows 8	32	IE10	32
Windows 8	64	IE10	32
Windows 8	64	IE10	64
Windows 8.1	64	IE11	32
Windows 8.1	64	IE11	64
Windows 10	64	IE11	32
Windows 10	64	IE11	64
Windows 10	32	IE11	32

2. Ensure that the Windows Logon user id has Administrator Privileges.

3. Ensure that the drivers for e-token has been loaded on to the PC from which the online request will be initiated for Digital Certificate. Ensure also that e-token has been already initialized, Administrator Password enabled by the IT Department of the Organization (Ask the e-token vendor for technical help for initialization, Administrator Password enabling etc. or read the user manual for E-token.) before distribution of e-tokens to the Subscribers/Applicants for Digital Certificates. Advise the users to change default passwords assigned to e-token by the vendor.

4. Ensure that the site URL https://services.idrbtca.org.in has already been added through the option (Open any internet explorer window, Click on Tools→ Internet Options → Security →Trusted Sites → Sites→Enter the URL https://services.idrbtca.org.in or https://10.0.67.18 in the window. Then click on Add Button. Check whether the URL https://services.idrbtca.org.in or https://10.0.67.18 is present in Trusted Sites. If not, enter the same in the window and then click add.)

5. Please ensure that Popup Blocker is turned off. Go to Tools→ Popup Blocker→Turn on Popup Blocker indicates that the Pop up Blocker is turned off and is ready to be turned on. Please see the attached file
6. Please do the Browser Settings as per the file “Browser Settings” attached. Please ensure that the Protected Mode is turned off.
7. Please browse https://10.0.67.18 (INFINET Users) or https://services.idrbtca.org.in (Internet Users). For accessing site through Internet, the static/dynamic IP of the system from which online request will be initiated is to be mailed to cahelp@idrbt.ac.in to facilitate access to the site
8. Please Click on “Member Login” and Fill in the User id and password provided to the applicant/subscriber by the RA Office by an automated e-mail and click on submit.


IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
InPrivate
https://172.27.100.43/index.jsp
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Request Details
IDRBT Certifying Authority
Suggested Sites
Web Slice Gallery
Dhruvam®-Lite
IDRBT Certifying Authority
Total Number of Certificat...
IDRBT Certifying Autho...
Page Safety Tools
Trust & Security on INFINET
i-trust
Licensed by Controller of Certifying Authorities, Government of India.
Home Resources Support Repository Contact Us
Trusted sites | Protected Mode: Off
100%
4:41 PM
8/25/2016

IDRBT Certifying Authority

IDRBT-CA Site has been updated with CAPTCHA. Click here for guidelines.

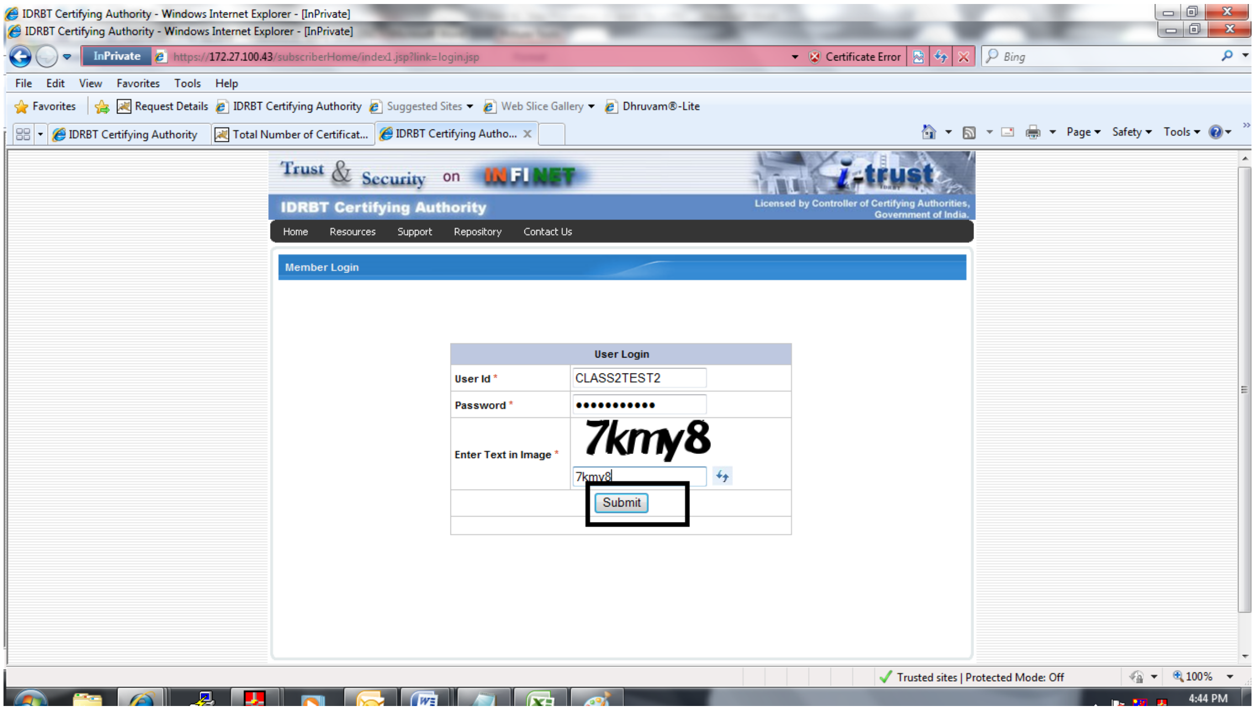
Login

☑Member Login

☑Administrator Login

Notice: IDRBT CA WEB Services (https://services.idrbtca.org.in) will be available only from MONDAY to SATURDAY from 9.00A.M. TO 5.30P.M. for SUBSCRIBERS accessing through internet. For users accessing through INTERNET, Please write to us on cahelp@idrbt.ac.in

With the objective of providing access with increased security for IDRBT Certifying Authority, only authorized users from INFINET member of organizations will be allowed to access our services.

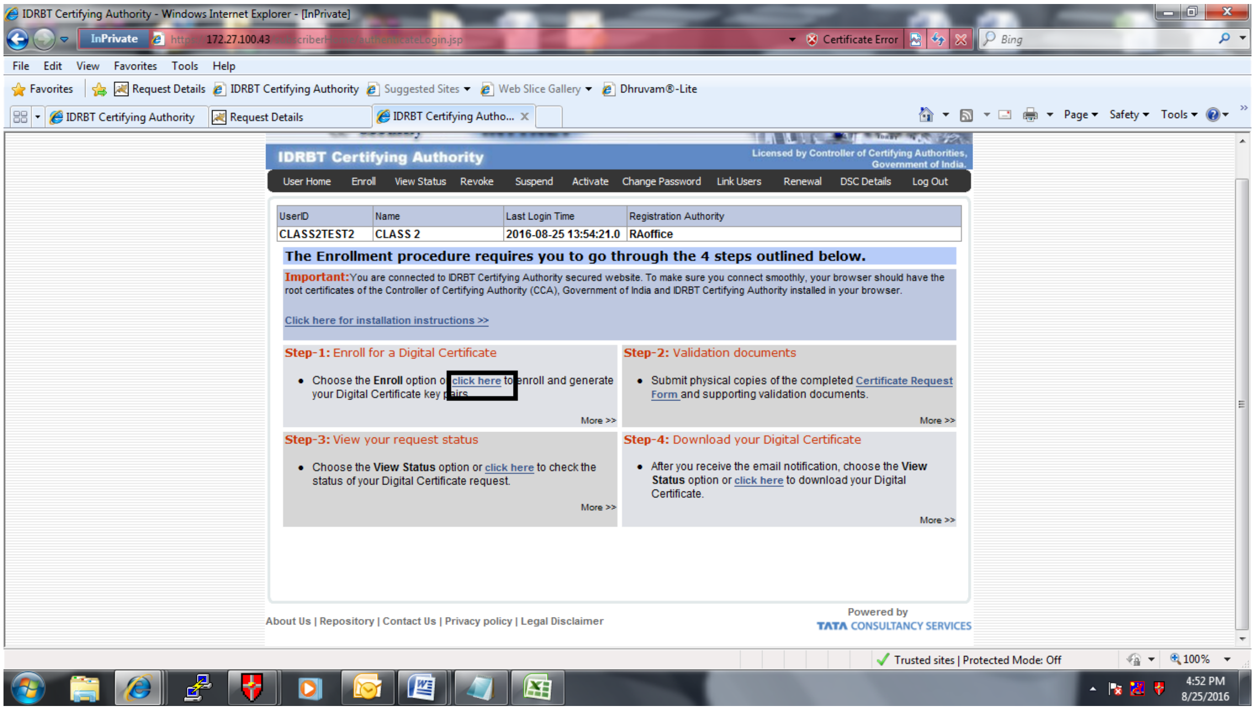

IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
InPrivate
https://172.27.100.43/subscriberHome/index1.jsp?link=login.jsp
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Request Details
IDRBT Certifying Authority
Suggested Sites
Web Slice Gallery
Dhruvam®-Lite
IDRBT Certifying Authority
Total Number of Certificat...
IDRBT Certifying Autho...
Page Safety Tools
Trust & Security on INFINET
i-trust
Licensed by Controller of Certifying Authorities, Government of India.
Home Resources Support Repository Contact Us
Trusted sites | Protected Mode: Off
100%
4:44 PM

IDRBT Certifying Authority

Member Login

User Login	
User Id *	CLASS2TEST2
Password *	●●●●●●●●●●●
Enter Text in Image *	7kmy8 7kmy8
	Submit

9. After Successful login, Click on “**Enroll”** for Enrolling as a user.



IDRBT Certifying Authority

Licensed by Controller of Certifying Authorities, Government of India.

UserID	Name	Last Login Time	Registration Authority
CLASS2TEST2	CLASS 2	2016-08-25 13:54:21.0	RAoffice

The Enrollment procedure requires you to go through the 4 steps outlined below.

Important: You are connected to IDRBT Certifying Authority secured website. To make sure you connect smoothly, your browser should have the root certificates of the Controller of Certifying Authority (CCA), Government of India and IDRBT Certifying Authority installed in your browser.

Click here for installation instructions >>

Step-1: Enroll for a Digital Certificate

- Choose the **Enroll** option or click here to enroll and generate your Digital Certificate key pairs.

More >>

Step-2: Validation documents

- Submit physical copies of the completed Certificate Request Form and supporting validation documents.

More >>

Step-3: View your request status

- Choose the **View Status** option or click here to check the status of your Digital Certificate request.

More >>

Step-4: Download your Digital Certificate

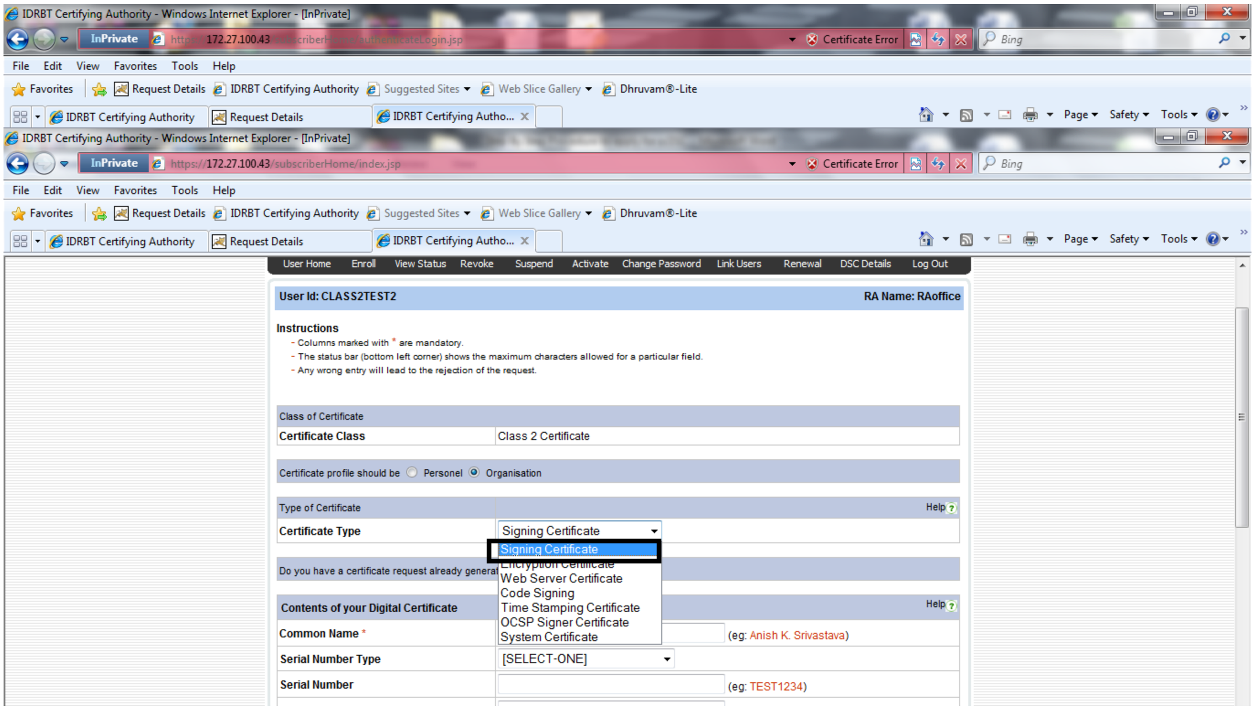
- After you receive the email notification, choose the **View Status** option or click here to download your Digital Certificate.

More >>

About Us | Repository | Contact Us | Privacy policy | Legal Disclaimer

Powered by TATA CONSULTANCY SERVICES

10. After Clicking on “Enroll”, Please select Signing Certificate from the drop down list shown against the field “Certificate Type”.



User Id: CLASS2TEST2 **RA Name: RAoffice**

Instructions

- Columns marked with * are mandatory.
- The status bar (bottom left corner) shows the maximum characters allowed for a particular field.
- Any wrong entry will lead to the rejection of the request.

Class of Certificate

Certificate Class	Class 2 Certificate

Certificate profile should be ○ Personel ● Organisation

Type of Certificate

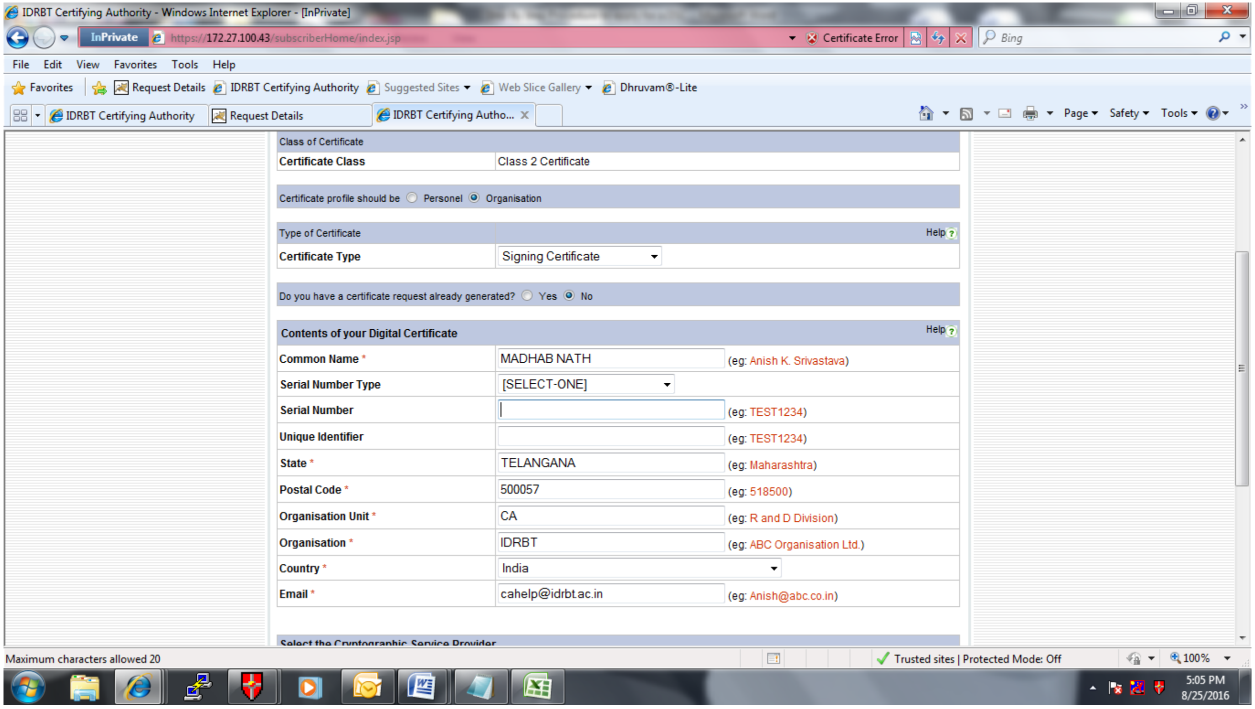
Certificate Type	Signing Certificate

Do you have a certificate request already generat

Contents of your Digital Certificate

Common Name *	(eg: Anish K. Srivastava)
Serial Number Type	[SELECT-ONE]
Serial Number	(eg: TEST1234)

11. For Signing Certificate, enter the common name as “the name of the applicant”
12. Enter the e-mail id with official domain name in the “Email for communication”. Enter other details. If the applicant doesn’t have an email id with official domain name, please send an authorization letter duly signed by the superior authority permitting/allowing the use of personal email id to apply for a Digital Certificate
13. The Distinguished Name (DN) details viz. Common Name, E-mail id, Organization, Organization Unit, Locality (PIN Code), State and Country are filled in without any type of errors.


IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
InPrivate
https://172.27.100.43/subscriberHome/index.jsp
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Request Details
IDRBT Certifying Authority
Suggested Sites
Web Slice Gallery
Dhruvam®-Lite
IDRBT Certifying Authority
Request Details
IDRBT Certifying Autho...
Page
Safety
Tools
Help
Maximum characters allowed 20
Trusted sites | Protected Mode: Off
100%
5:05 PM
8/25/2016

Class of Certificate

Certificate Class	Class 2 Certificate

Certificate profile should be ○ Personel ● Organisation

Type of Certificate

Certificate Type	Signing Certificate

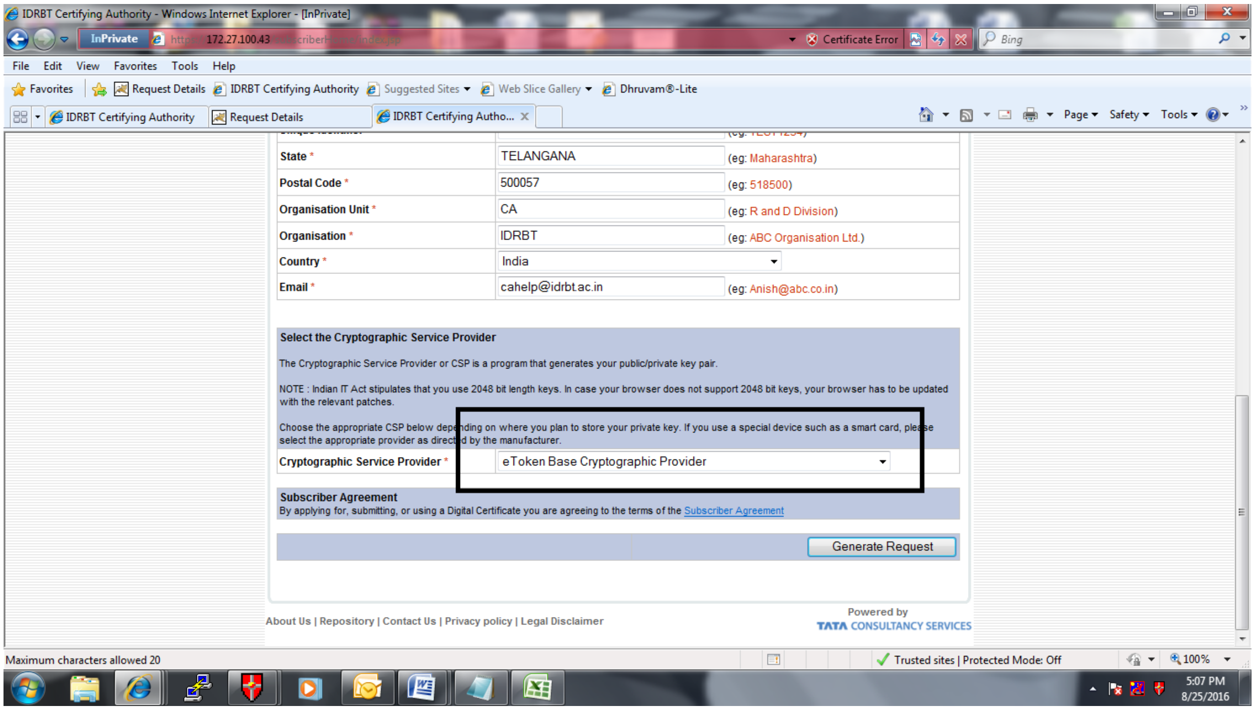
Do you have a certificate request already generated? ○ Yes ● No

Contents of your Digital Certificate

Common Name *	MADHAB NATH	(eg: Anish K. Srivastava)
Serial Number Type	[SELECT-ONE]	
Serial Number		(eg: TEST1234)
Unique Identifier		(eg: TEST1234)
State *	TELANGANA	(eg: Maharashtra)
Postal Code *	500057	(eg: 518500)
Organisation Unit *	CA	(eg: R and D Division)
Organisation *	IDRBT	(eg: ABC Organisation Ltd.)
Country *	India	
Email *	cahelp@idrbt.ac.in	(eg: Anish@abc.co.in)

Select the Cryptographic Service Provider

14. Insert the e-token. Then select the cryptographic provider name as “e-token based cryptographic Provider” (if you are using alladin token/Safenet key). In case of other brand e-tokens from other vendors such as Watch Data, Feitian token, Moser Bear Token, the proper Cryptographic provider name will be in User Manual or check with the Vendor of E-token of particular brand.


IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
InPrivate
172.27.100.43
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Request Details
IDRBT Certifying Authority
Suggested Sites
Web Slice Gallery
Dhruvam®-Lite
IDRBT Certifying Authority
Request Details
IDRBT Certifying Autho...
Page
Safety
Tools
Maximum characters allowed 20
Trusted sites | Protected Mode: Off
100%
5:07 PM
8/25/2016

State *	TELANGANA	(eg: Maharashtra)
Postal Code *	500057	(eg: 518500)
Organisation Unit *	CA	(eg: R and D Division)
Organisation *	IDRBT	(eg: ABC Organisation Ltd.)
Country *	India	
Email *	cahelp@idrbt.ac.in	(eg: Anish@abc.co.in)

Select the Cryptographic Service Provider

The Cryptographic Service Provider or CSP is a program that generates your public/private key pair.

NOTE : Indian IT Act stipulates that you use 2048 bit length keys. In case your browser does not support 2048 bit keys, your browser has to be updated with the relevant patches.

Choose the appropriate CSP below depending on where you plan to store your private key. If you use a special device such as a smart card, please select the appropriate provider as directed by the manufacturer.

Cryptographic Service Provider * eToken Base Cryptographic Provider

Subscriber Agreement

By applying for, submitting, or using a Digital Certificate you are agreeing to the terms of the Subscriber Agreement

Generate Request

About Us | Repository | Contact Us | Privacy policy | Legal Disclaimer

Powered by TATA CONSULTANCY SERVICES

Safenet/Alladin E-Token based :-

While initiating online request, kindly choose cryptographic service provider as “**E-Token based Cryptographic service provider**” for safenet/ ALaddin E-Token.

Epass Token based

While initiating online request, kindly choose cryptographic service provider as “**EnterSafe ePass2003 CSP v1..0**” for Epass 2003 E-Token.

Watchdata Token: -

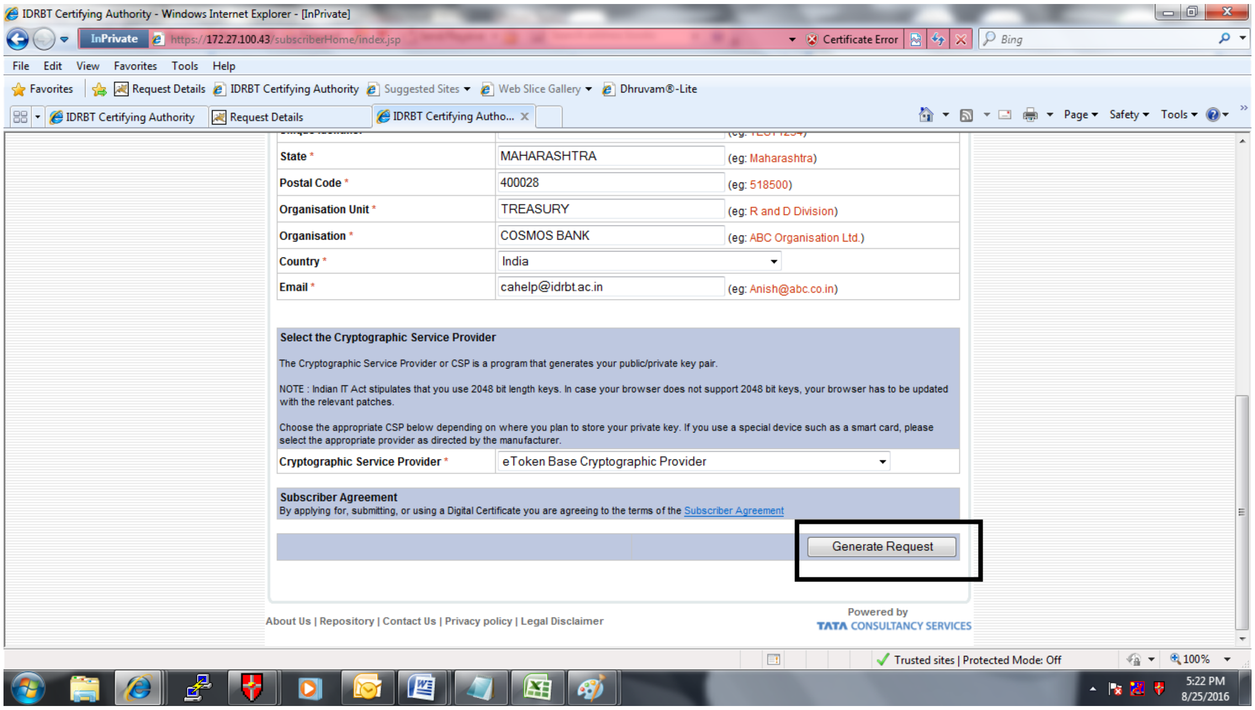
While initiating online request, kindly choose cryptographic service provider as “**WatchKey CSP India V1.0**” for Watch data Token. The jargons may vary for different versions of the e-token from the same vendor. Please always refer the user manual for e-token or take the help from e-token vendor.

MoserBaer/Giesecke Token: -

While initiating online request, kindly choose cryptographic service provider as “**Safe Sign Standard-I Cryptographic Service Provider**” for Moserbaer/ Giesecke Token

Ensure that the E-token is inserted, proper Cryptographic provider has been chosen from the drop down list depending upon the brand of e-token inserted in the system before Clicking on “Generate Request”.

15. Click on “Generate Request”.


IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
InPrivate
https://172.27.100.43/subscriberHome/index.jsp
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Request Details
IDRBT Certifying Authority
Suggested Sites
Web Slice Gallery
Dhruvam®-Lite
IDRBT Certifying Authority
Request Details
IDRBT Certifying Autho...
Page
Safety
Tools
Trusted sites | Protected Mode: Off
100%
5:22 PM
8/25/2016

State *	MAHARASHTRA	(eg: Maharashtra)
Postal Code *	400028	(eg: 518500)
Organisation Unit *	TREASURY	(eg: R and D Division)
Organisation *	COSMOS BANK	(eg: ABC Organisation Ltd.)
Country *	India	
Email *	cahelp@idrbt.ac.in	(eg: Anish@abc.co.in)

Select the Cryptographic Service Provider

The Cryptographic Service Provider or CSP is a program that generates your public/private key pair.

NOTE : Indian IT Act stipulates that you use 2048 bit length keys. In case your browser does not support 2048 bit keys, your browser has to be updated with the relevant patches.

Choose the appropriate CSP below depending on where you plan to store your private key. If you use a special device such as a smart card, please select the appropriate provider as directed by the manufacturer.

Cryptographic Service Provider * : eToken Base Cryptographic Provider

Subscriber Agreement

By applying for, submitting, or using a Digital Certificate you are agreeing to the terms of the Subscriber Agreement

Generate Request

About Us | Repository | Contact Us | Privacy policy | Legal Disclaimer

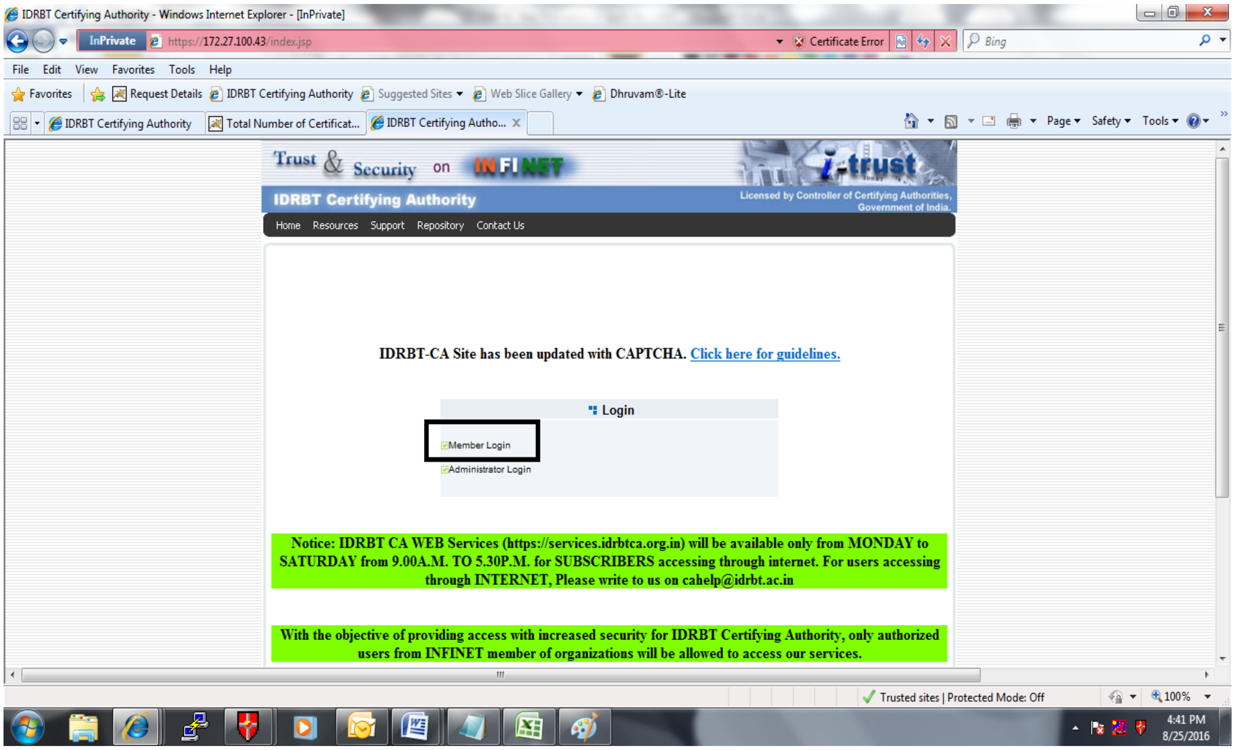
Powered by TATA CONSULTANCY SERVICES

16. After getting the request number, note down the request number and choose the last option “Log Out” from the menu.

    *Note: **Do not change the settings of the system from which the request has been generated.** Do not upgrade Operating System or Internet Explorer or apply patches for Operating System. Certificate Generation by IDRBT CA will take one to two days after the online request reaches IDRBT CA. Please check “View Status” within 3 days of generation of request and download when the status is shown as “Certificate Generated.” Or when the applicant receives an automated mail with Authentication PIN (OTP) stating that “Certificate has been Generated with Authentication PIN (to be entered in the screen for downloading the certificate).

For downloading the SHA2 2048 Class II/ Class III signing certificate: (Download the Certificate on the same Personal Computer from which the request has been initiated)

1. A Confirmation mail along with Authentication PIN will be sent by E-mail to the e-mail id provided by the Subscriber in DN Details after the generation of Digital Certificate.
2. Please use the same logon credentials (Windows logon user id) for logging in that was used at the time of initiating the request.
3. Please Click on “Member Login” and Fill in the User id and password provided to the applicant/subscriber by the RA Office by an automated e-mail and click on submit.


IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
InPrivate
https://172.27.100.43/index.jsp
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Request Details
IDRBT Certifying Authority
Suggested Sites
Web Slice Gallery
Dhruvam®-Lite
IDRBT Certifying Authority
Total Number of Certificat...
IDRBT Certifying Autho...
Page Safety Tools
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
Home Resources Support Repository Contact Us
Trusted sites | Protected Mode: Off
100%
4:41 PM
8/25/2016

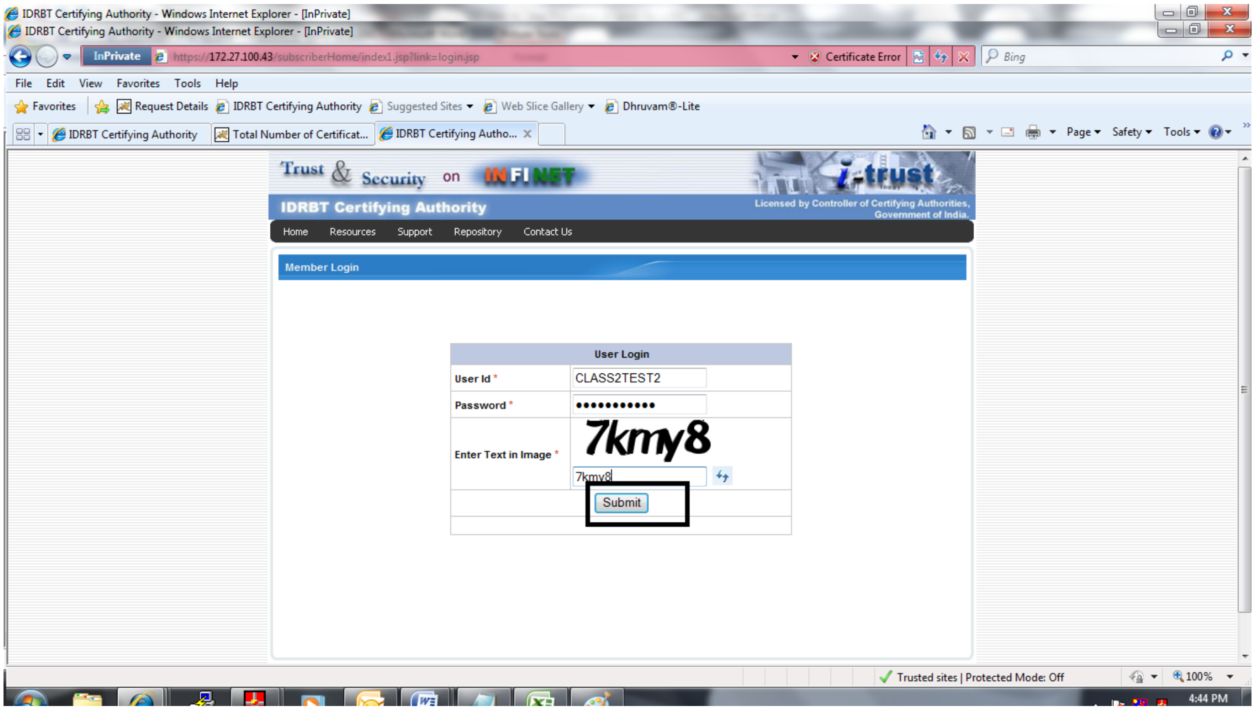
IDRBT-CA Site has been updated with CAPTCHA. Click here for guidelines.

Login

- Member Login
- Administrator Login

Notice: IDRBT CA WEB Services (https://services.idrbtca.org.in) will be available only from MONDAY to SATURDAY from 9.00A.M. TO 5.30P.M. for SUBSCRIBERS accessing through internet. For users accessing through INTERNET, Please write to us on cahelp@idrbt.ac.in

With the objective of providing access with increased security for IDRBT Certifying Authority, only authorized users from INFINET member of organizations will be allowed to access our services.

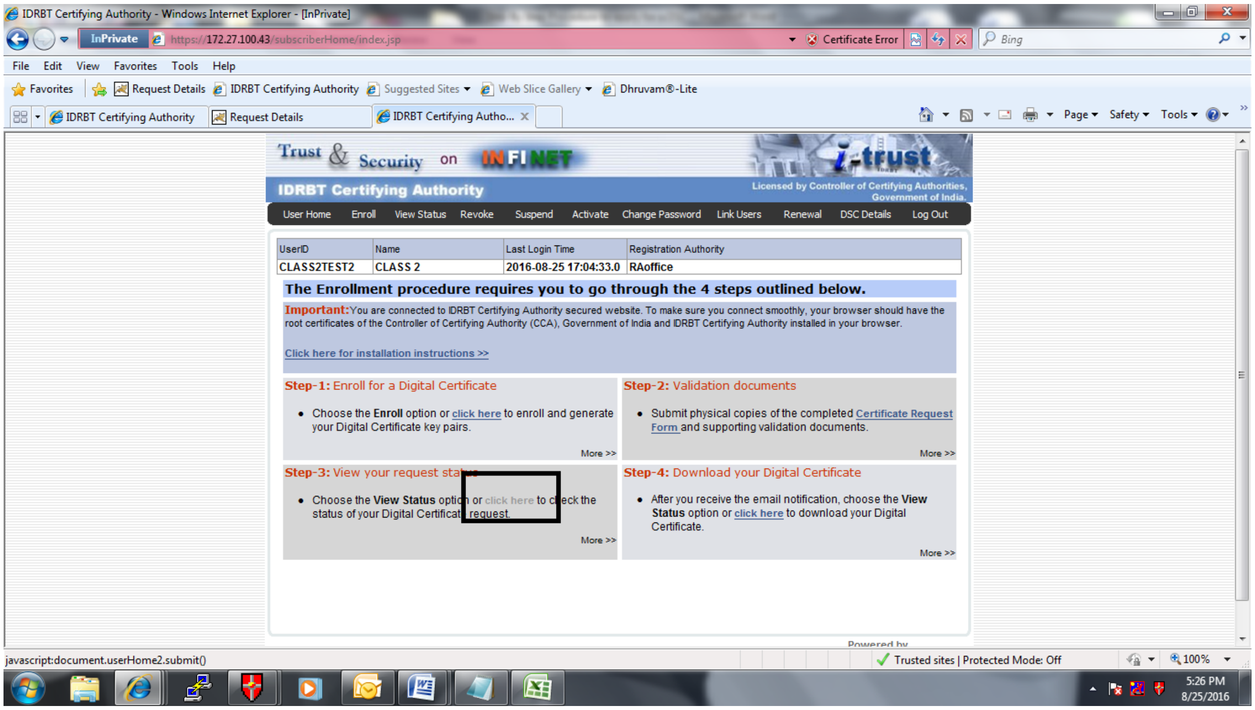

IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
InPrivate
https://172.27.100.43/subscriberHome/index1.jsp?link=login.jsp
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Request Details
IDRBT Certifying Authority
Suggested Sites
Web Slice Gallery
Dhruvam®-Lite
IDRBT Certifying Authority
Total Number of Certificat...
IDRBT Certifying Autho...
Page Safety Tools
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
Home Resources Support Repository Contact Us
Trusted sites | Protected Mode: Off
100%
4:44 PM

Member Login

User Login

User Id *	CLASS2TEST2
Password *	•••••••••••
Enter Text in Image *	7kmy8 7kmy8
	Submit

4. Click on Step 3 “View Status”



IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
https://172.27.100.43/subscriberHome/index.jsp
Certificate Error
File Edit View Favorites Tools Help
Trust & Security on INFINET
i-trust
IDRBT Certifying Authority
Licensed by Controller of Certifying Authorities, Government of India.
User Home
Enroll
View Status
Revoke
Suspend
Activate
Change Password
Link Users
Renewal
DSC Details
Log Out

UserID	Name	Last Login Time	Registration Authority
CLASS2TEST2	CLASS 2	2016-08-25 17:04:33.0	RAoffice

The Enrollment procedure requires you to go through the 4 steps outlined below.

Important: You are connected to IDRBT Certifying Authority secured website. To make sure you connect smoothly, your browser should have the root certificates of the Controller of Certifying Authority (CCA), Government of India and IDRBT Certifying Authority installed in your browser.

Click here for installation instructions >>

Step-1: Enroll for a Digital Certificate

- Choose the **Enroll** option or click here to enroll and generate your Digital Certificate key pairs.

More >>

Step-2: Validation documents

- Submit physical copies of the completed Certificate Request Form and supporting validation documents.

More >>

Step-3: View your request status

- Choose the **View Status** option or click here to check the status of your Digital Certificate request.

More >>

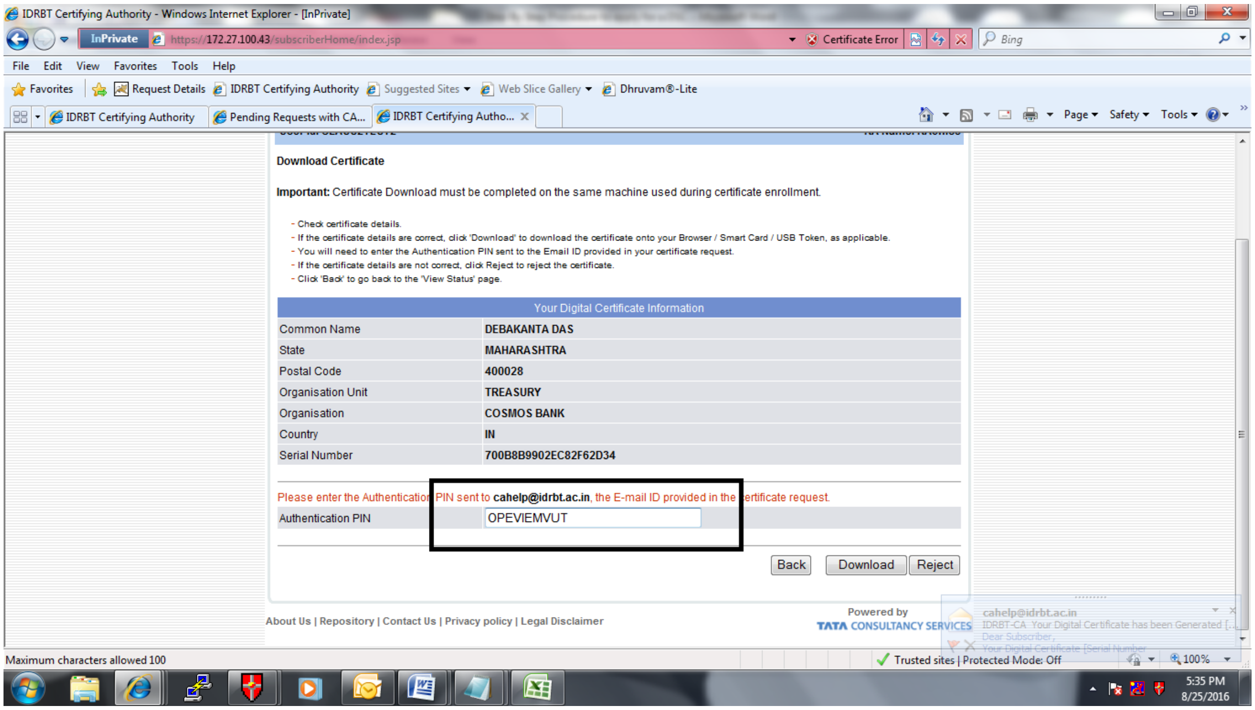
Step-4: Download your Digital Certificate

- After you receive the email notification, choose the **View Status** option or click here to download your Digital Certificate.

More >>

javascript:document.userHome2.submit()

5. List of Certificate Request numbers will appear along with status. Once the Status is shown as “Certificate Generated” against the request number generated by the applicant, Click on the Request number. Please do not forget to insert the e-token that was used for generating the request. Copy and Paste the Authentication PIN received by E-mail Insert the same e-token which was used at the time of initiating online request generation.



IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]
https://172.27.100.43/subscriberHome/index.jsp
Certificate Error
File Edit View Favorites Tools Help
Pending Requests with CA...
IDRBT Certifying Autho...

Download Certificate

Important: Certificate Download must be completed on the same machine used during certificate enrollment.

- Check certificate details.
- If the certificate details are correct, click 'Download' to download the certificate onto your Browser / Smart Card / USB Token, as applicable.
- You will need to enter the Authentication PIN sent to the Email ID provided in your certificate request.
- If the certificate details are not correct, click Reject to reject the certificate.
- Click 'Back' to go back to the 'View Status' page.

Your Digital Certificate Information	
Common Name	DEBAKANTA DAS
State	MAHARASHTRA
Postal Code	400028
Organisation Unit	TREASURY
Organisation	COSMOS BANK
Country	IN
Serial Number	700B8B9902EC82F62D34

Please enter the Authentication PIN sent to **cahelp@idrbt.ac.in**, the E-mail ID provided in the certificate request.

Authentication PIN: OPEVIEMVUT

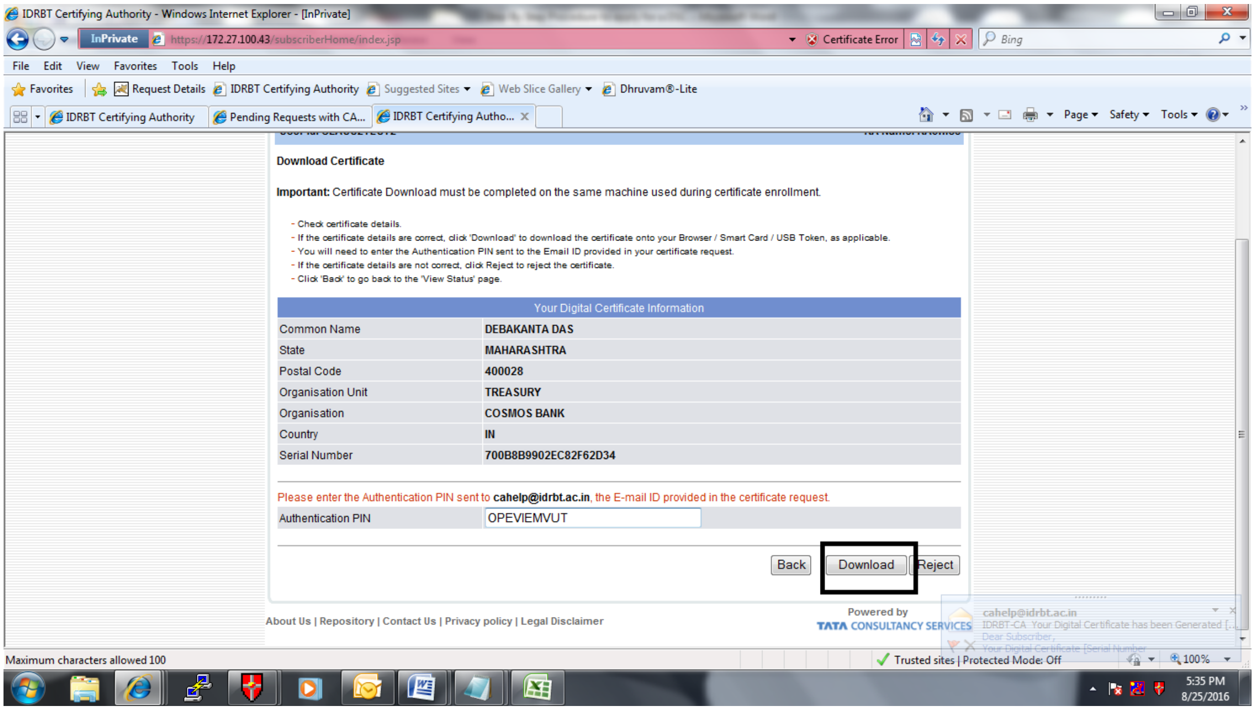
Back | Download | Reject

About Us | Repository | Contact Us | Privacy policy | Legal Disclaimer

Powered by TATA CONSULTANCY SERVICES

Maximum characters allowed 100

6. Then Click on download. Enter the E-Token Password.



IDRBT Certifying Authority - Windows Internet Explorer - [InPrivate]

https://172.27.100.43/subscriberHome/index.jsp

Download Certificate

Important: Certificate Download must be completed on the same machine used during certificate enrollment.

- Check certificate details.
- If the certificate details are correct, click 'Download' to download the certificate onto your Browser / Smart Card / USB Token, as applicable.
- You will need to enter the Authentication PIN sent to the Email ID provided in your certificate request.
- If the certificate details are not correct, click Reject to reject the certificate.
- Click 'Back' to go back to the 'View Status' page.

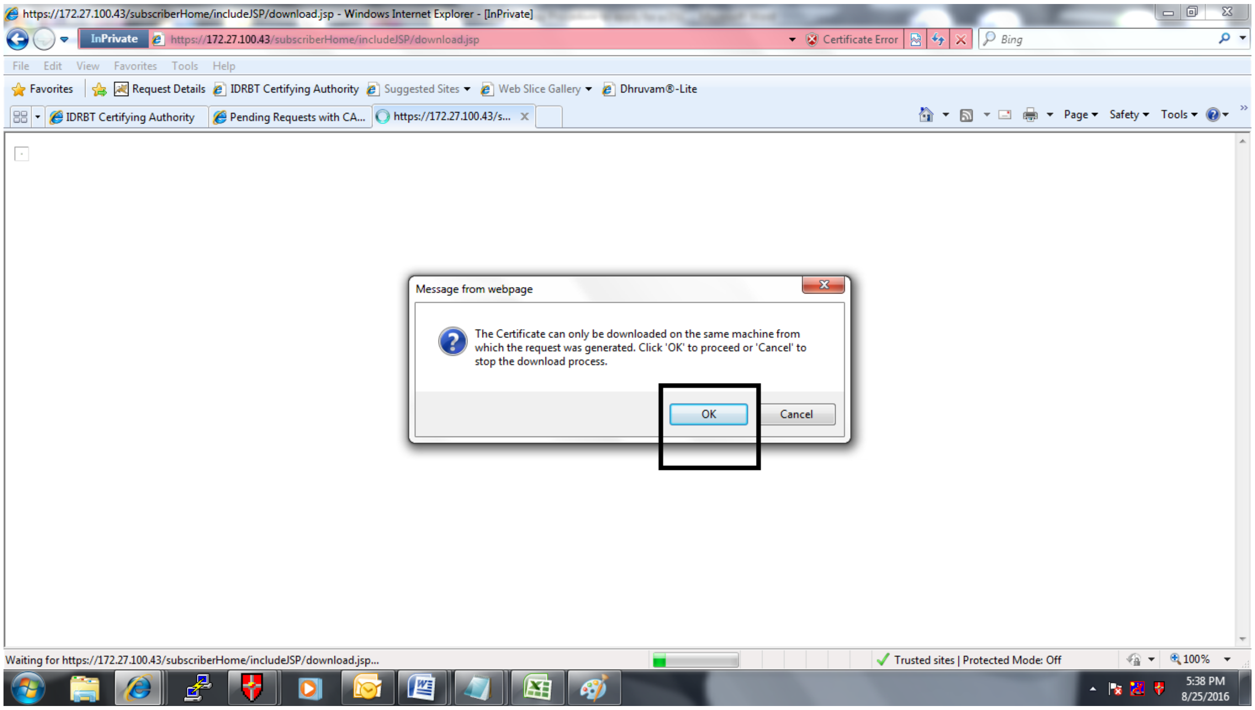
Your Digital Certificate Information	
Common Name	DEBAKANTA DAS
State	MAHARASHTRA
Postal Code	400028
Organisation Unit	TREASURY
Organisation	COSMOS BANK
Country	IN
Serial Number	700B8B9902EC82F62D34

Please enter the Authentication PIN sent to **cahelp@idrbt.ac.in**, the E-mail ID provided in the certificate request.

Authentication PIN: OPEVIEMVUT

Back
Download
Reject
About Us | Repository | Contact Us | Privacy policy | Legal Disclaimer
Powered by TATA CONSULTANCY SERVICES
Maximum characters allowed 100
Trusted sites | Protected Mode: Off
5:35 PM
8/25/2016

7. An alert message will appear to download the Certificate on the same Personal Computer from which the request has been initiated. Click on ok.



https://172.27.100.43/subscriberHome/includeJSP/download.jsp - Windows Internet Explorer - [InPrivate]

Message from webpage

The Certificate can only be downloaded on the same machine from which the request was generated. Click 'OK' to proceed or 'Cancel' to stop the download process.

OK
Cancel
Waiting for https://172.27.100.43/subscriberHome/includeJSP/download.jsp...
Trusted sites | Protected Mode: Off
5:38 PM
8/25/2016

****

Procedure to apply for a class 3 Digital Certificate:

To Apply for Class 3 Digital Certificate for Servers, the Bank official who is authorised to apply for Class 3 Certificate should appear in person at IDRBT for Face to Face verification.
She/he should carry the following:

1) Authorization letter from Bank on Bank's letter head authorizing an Official to obtain a **Class 3** certificate on behalf of the Bank.
2) Application duly filled in signed by Applicant and Superior Authority with Official Seal affixed on Second page of the Application.
3) One Passport size Photograph to be affixed on the Right corner of the First page of the Application.
4) Photocopies of PAN and Aadhar card of the Applicant attested by **Superior Authority with Seal** to be attached to the Application form.
5) Self- attested photocopies PAN and ID card of Superior Authority to be attached to the Application.
6) Original PAN Card, Aadhaar card and ID card of the Applicant to be shown during face- to face verification.
7) GST Number of the Bank / Financial Institution.
8) Copy of Reserve Bank of India approval letter to participate in Centralized Payment System.
9) Share the payment details along with UTR Number

<u>Procedure to generate online request for system certificate</u>:

Please visit URL https://services.idrbtca.org.in through Internet or visit https://10.0.67.18 from INFINET.

Kindly Login-->Member Login-->Click on Enroll-->

A) If you have .CSR file, select **<u>Yes</u>** at "Do you have a certificate request already generated?"

upload .CSR file and fill all the mandatory fields -->Generate Online Request-->Share the Enrollment Reference number.

B) If you do not have .CSR file:

Fill the details which are mandatory-->Generate Online Request-->Share the Enrollment Reference number.

Note: Select always CSP as Microsoft Enhanced Cryptographic Provider V.10 for system certificate.

IDRBT CA Cost Structure for Non-RA's and Non-cooperative banks:

For Class 2 Certificate Cost Details for 1yr

Rupees 500/- for 1 Year Certificate + Rupees 500/- for Admin Charges + 18% GST ➔ 1000+ 18% services tax ==> 1180/- per certificate.

For Class 2 Certificate Cost Details for 2yr

Rupees 1000/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 18% GST ==> 1500+18% service tax ==> 1770/- per certificate.

For Class 3 Certificate Cost Details for 1yr

Rupees 10000/ for 1 Year Certificate + Rupees 500/ for Admin Charges + 18% GST==> 10500+18% service tax ==> 12390 /- per certificate

For Class 3 Certificate Cost Details for 2yrs

Rupees 20000/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 18% GST==> 20500+ 18% services tax➔24190/- per certificate.

IDRBT CA Cost Structure for Co-operative banks:

For Class 2 Certificate Cost Details For 1yr

Rupees 250/ for 1 Year Certificate + Rupees 500/ for Admin Charges + 18% GST==> 750 + 135 services tax ==> 885/- per certificate.

For Class 2 Certificate Cost Details For 2yr

Rupees 500/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 18% GST==> 1000+ 180 service tax ==> 1180/- per certificate.

For Class 3 Certificate Cost Details For 1yr

Rupees 10000/ for 1 Year Certificate + Rupees 500/ for Admin Charges + 18% GST==> 10500+ 1890 service tax ==> 12390 /- per certificate

For Class 3 Certificate Cost Details For 2yrs

Rupees 20000/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 18% GST==> 20500+ 3690 services tax➔24190/- per certificate.