**Step By Step instructions to apply for a DSC**

**Step 1: Applicant**

**Please fill up the Application form for Digital Certificate attached herewith. The application form can also be downloaded from** [**http://idrbtca.org.in**](http://idrbtca.org.in)**.**

Please ensure that

1. Authorization/ Forwarding letter from the bank authorizing the official concerned to apply for a digital certificate is enclosed with the application form.
2. the applicant and the superior authority signs on either side of the application form at the appropriate places
3. the bank stamp is affixed at the appropriate places
4. a passport size Photograph is affixed on the right top corner of the first page of the application
5. the applicant has signed across the photograph.
6. A copy of Photo Identification Document (PAN/Driving License/ Voter ID/Passport) duly attested by the Superior Authority is enclosed with the application form.
7. 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

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

**Step 2: Processing by Registration Authority (RA) officials**

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.

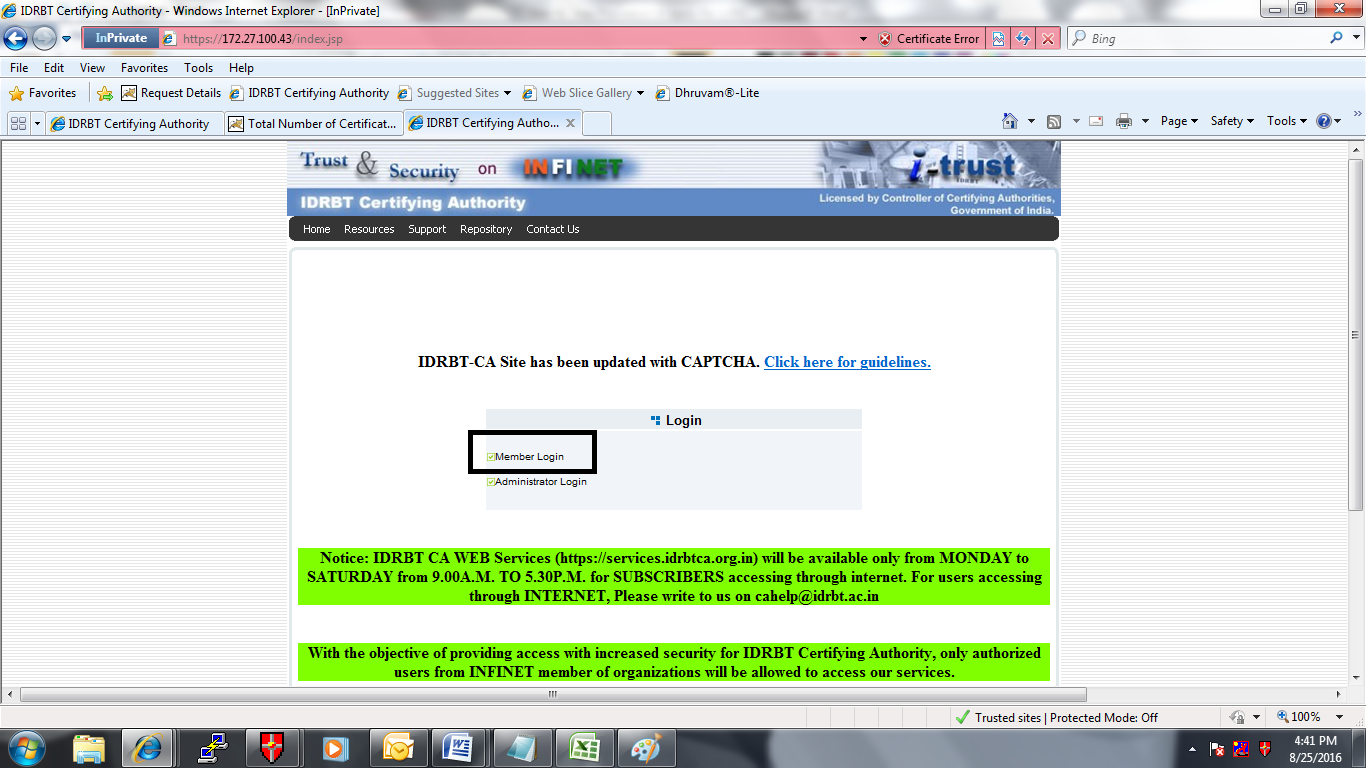
**Step 3: Acknowledgement to be sent to RA by the applicant:**

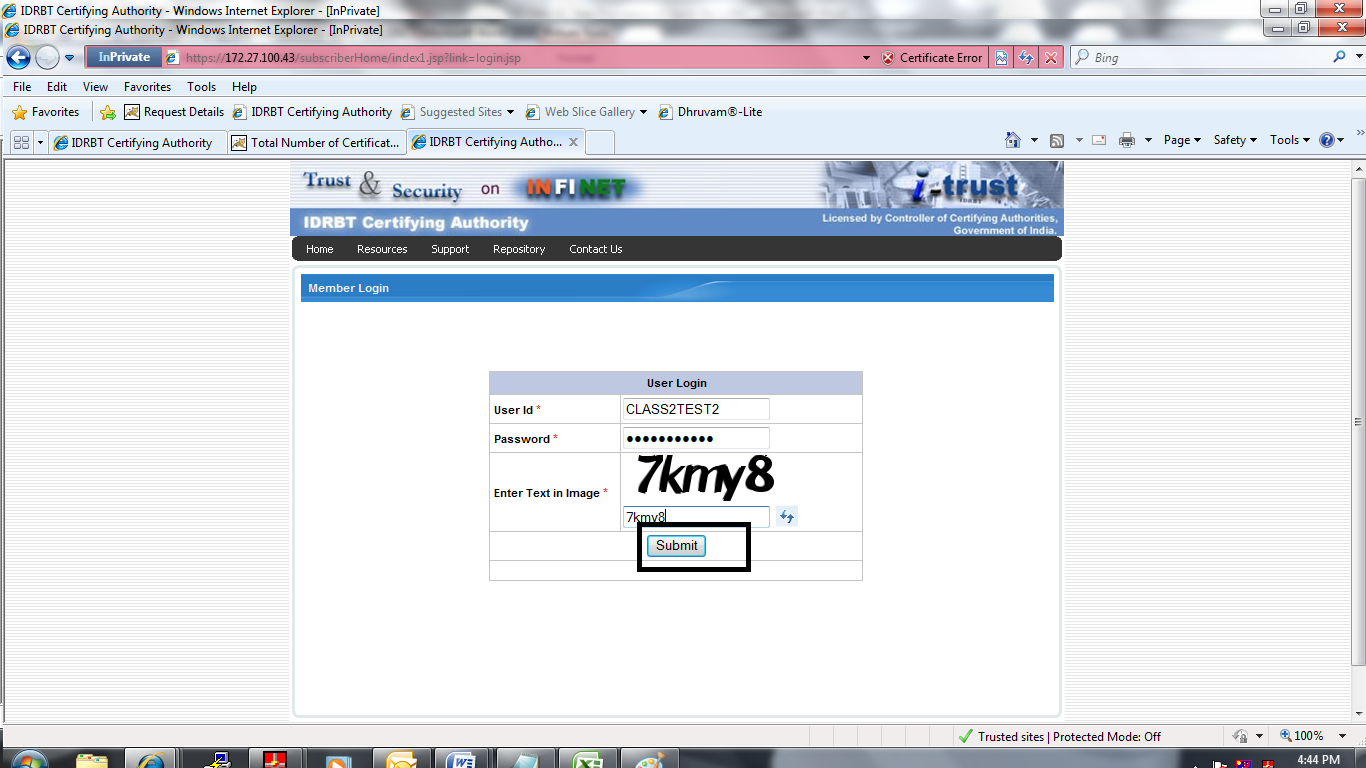
After receiving the mail with User id and Password, the applicant has to take the print out of the mail, sign on it and send the scanned copy of the same to the RA for activating the user id. The applicant will be able to login using the user id and password provided by the RA only upon activation of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

**Step 4: Procedure for Enrolling and Generating key Pairs (Initiating online request):**

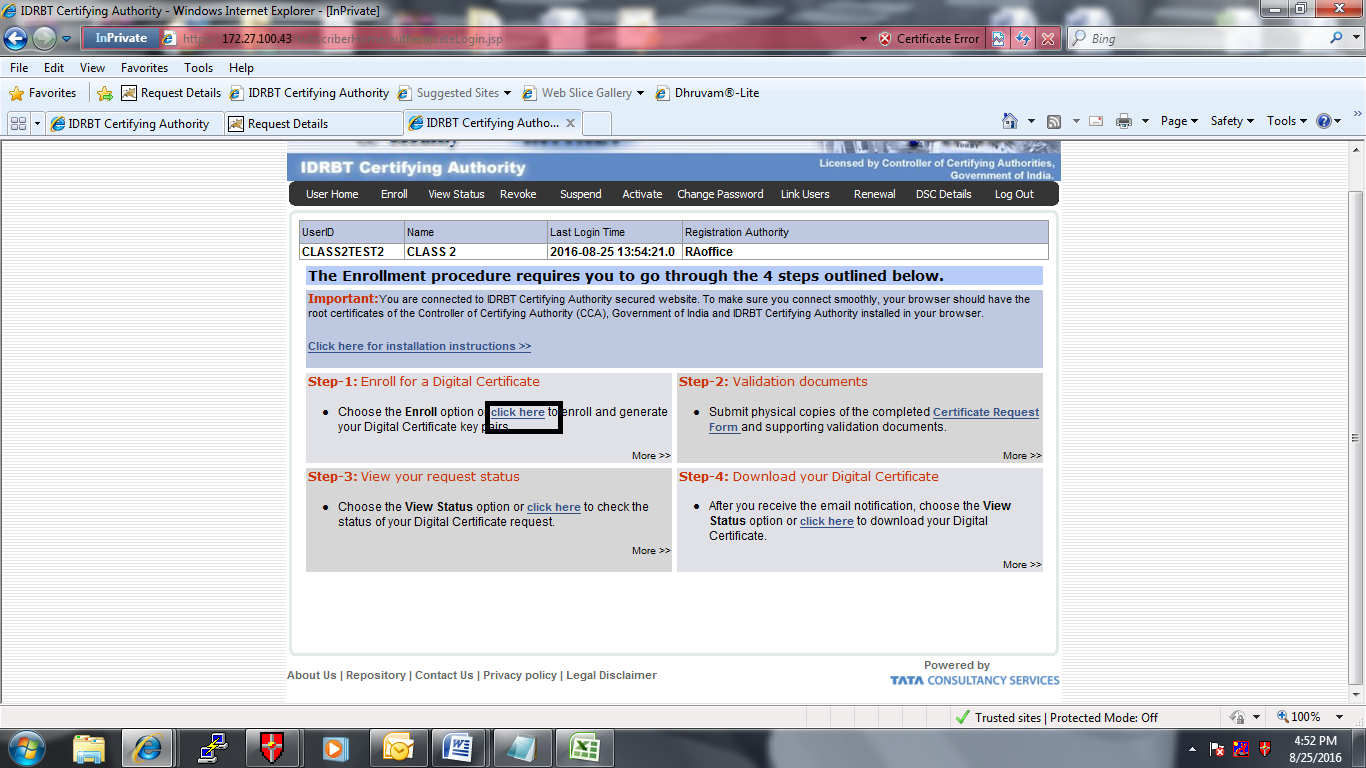
**To apply for the SHA2 2048 Class II/Class III Signing certificate using (crypto token) ikey/e-token (dongle):**

1. Ensure that the Operating System is Windows Vista, Windows 7 or Windows XP with Service Pack 3.
2. Ensure that the version of Internet Explorer is either Version 7 or 9 or 11. **Do not use any other browsers such as Google, Fire Fox etc.**
3. Ensure that the Windows Logon user id has Administrator Privileges.
4. 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.
5. 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> in the window. Then click on Add Button. Check whether the URL <https://services.idrbtca.org.in> is present in Trusted Sites. If not, enter the same in the window and then click add.)
6. 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.
7. Please do the Browser Settings as per the file “Browser Settings” attached. Please ensure that the Protected Mode is turned off.
8. 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](mailto:cahelp@idrbt.ac.in) to facilitate access to the site
9. Please Choose “Click Here to apply for SHA 2 Certificate”.
10. 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.

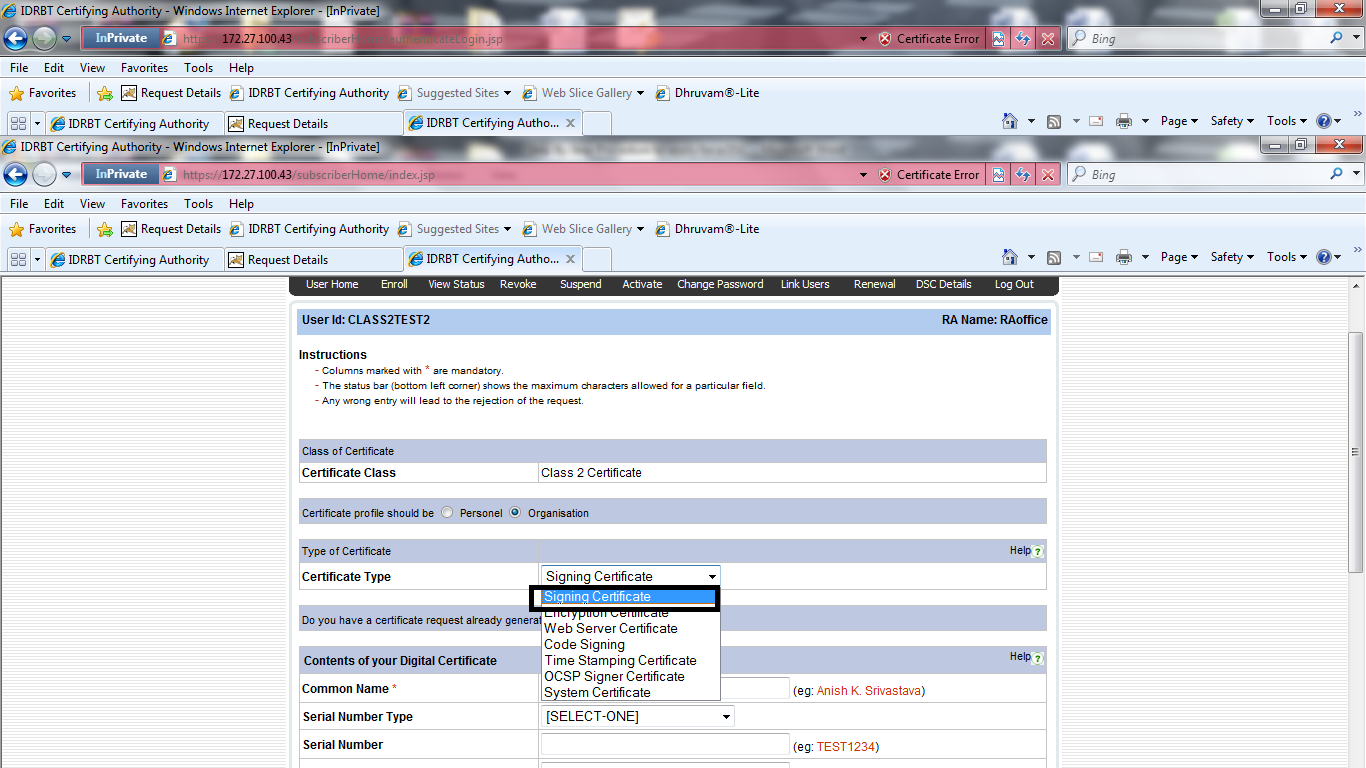




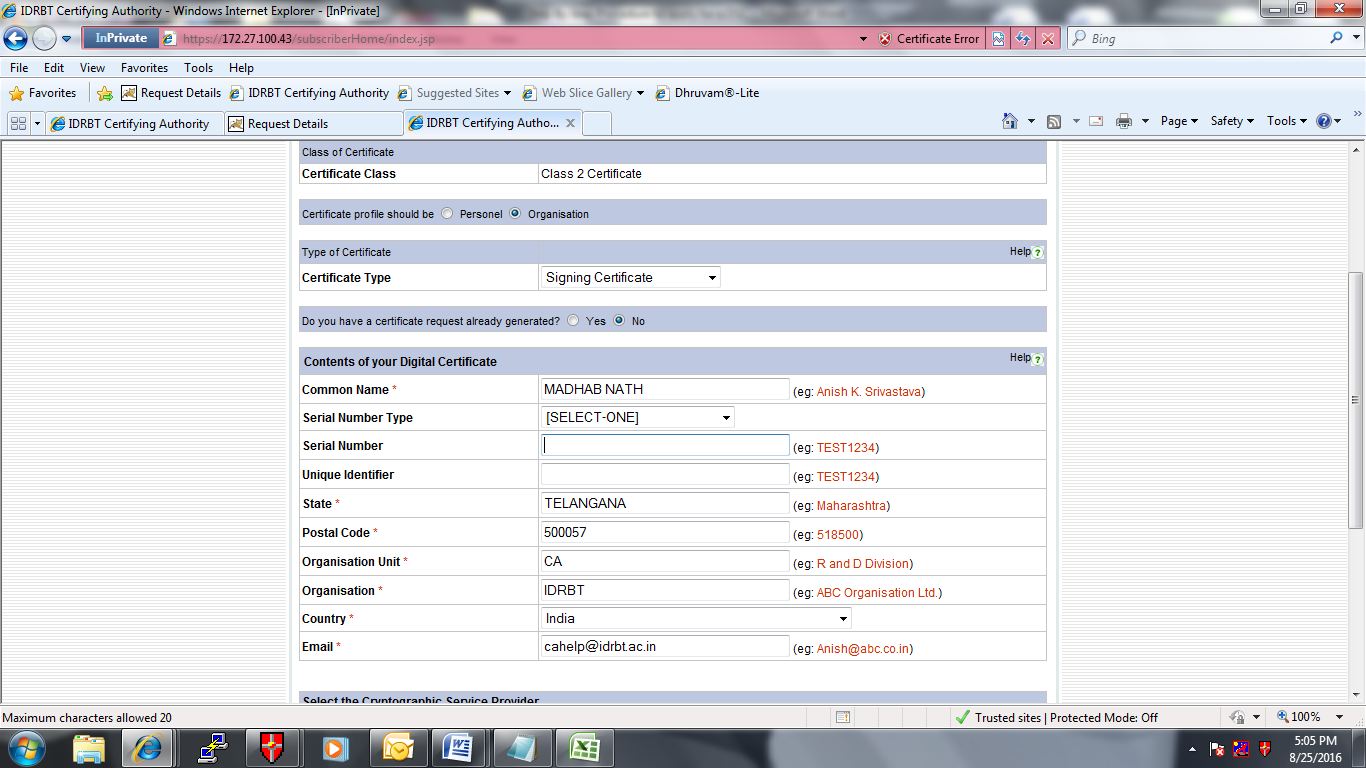
1. After Successful login, Click on “**Enroll”** for Enrolling as a user.



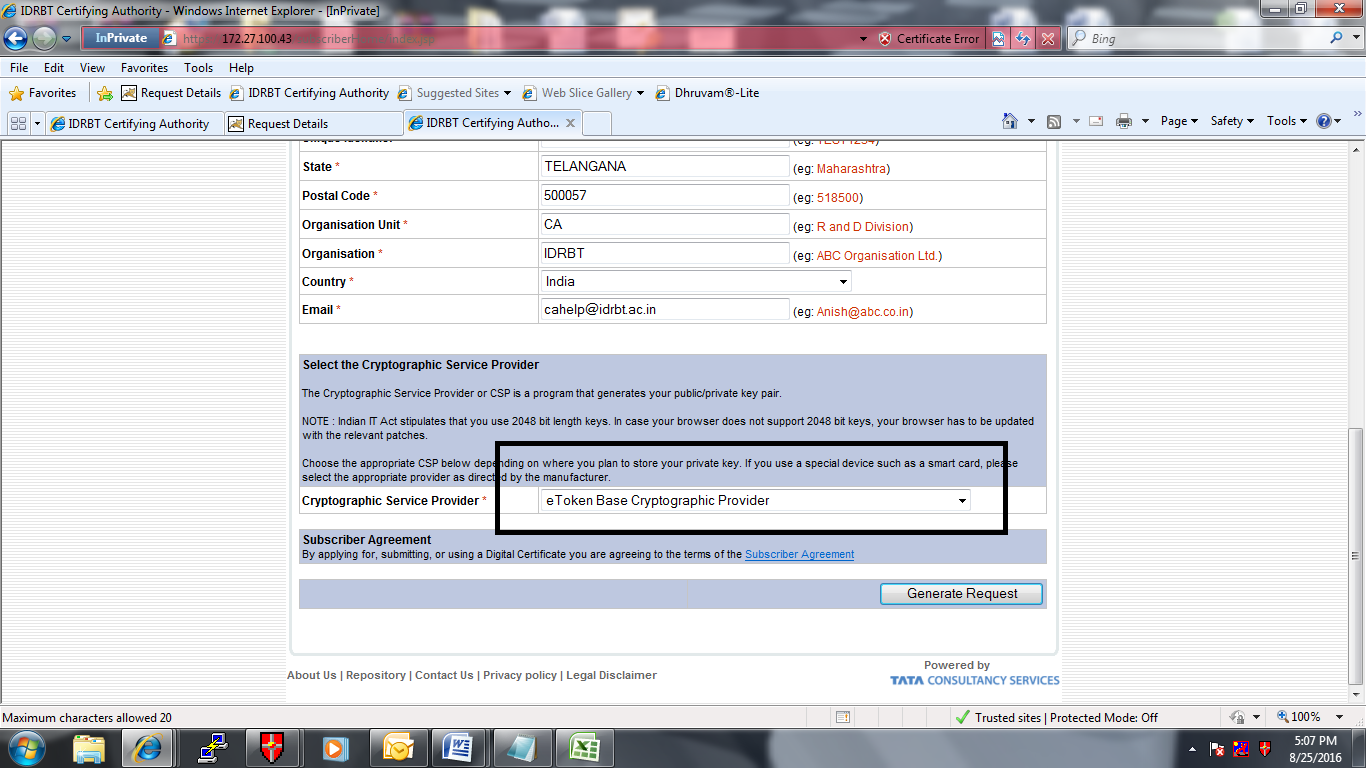
1. After Clicking on “Enroll”, Please select Signing Certificate from the drop down list shown against the field “Certificate Type”.



1. For Signing Certificate, enter the common name as “the name of the applicant”
2. 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
3. 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. Though specifying PAN is optional, entering PAN in online request will give the applicant an additional option to use the certificate for filing the income tax returns of the applicant.

****

1. 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.



**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.

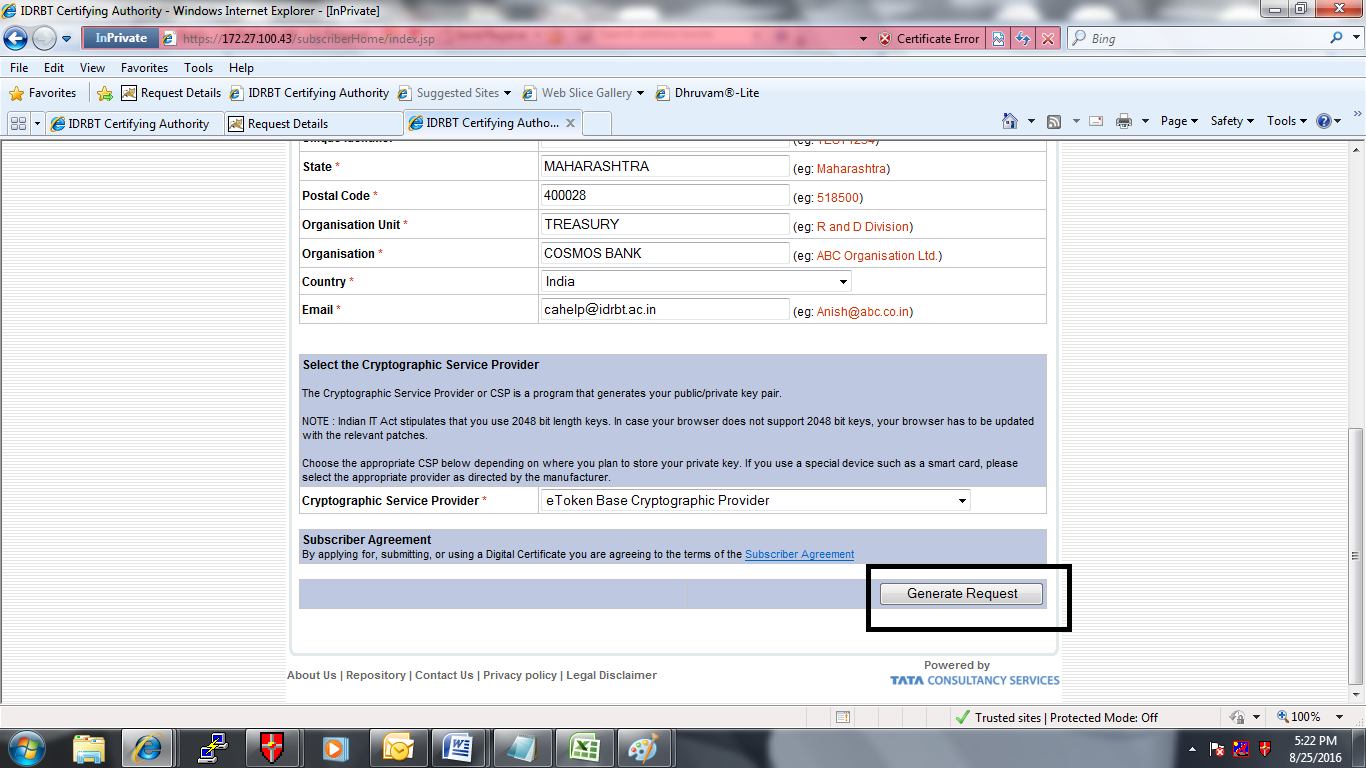
**MoserBaer/Giesecke Token :-**

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”.

1. Click on “Generate Request”.

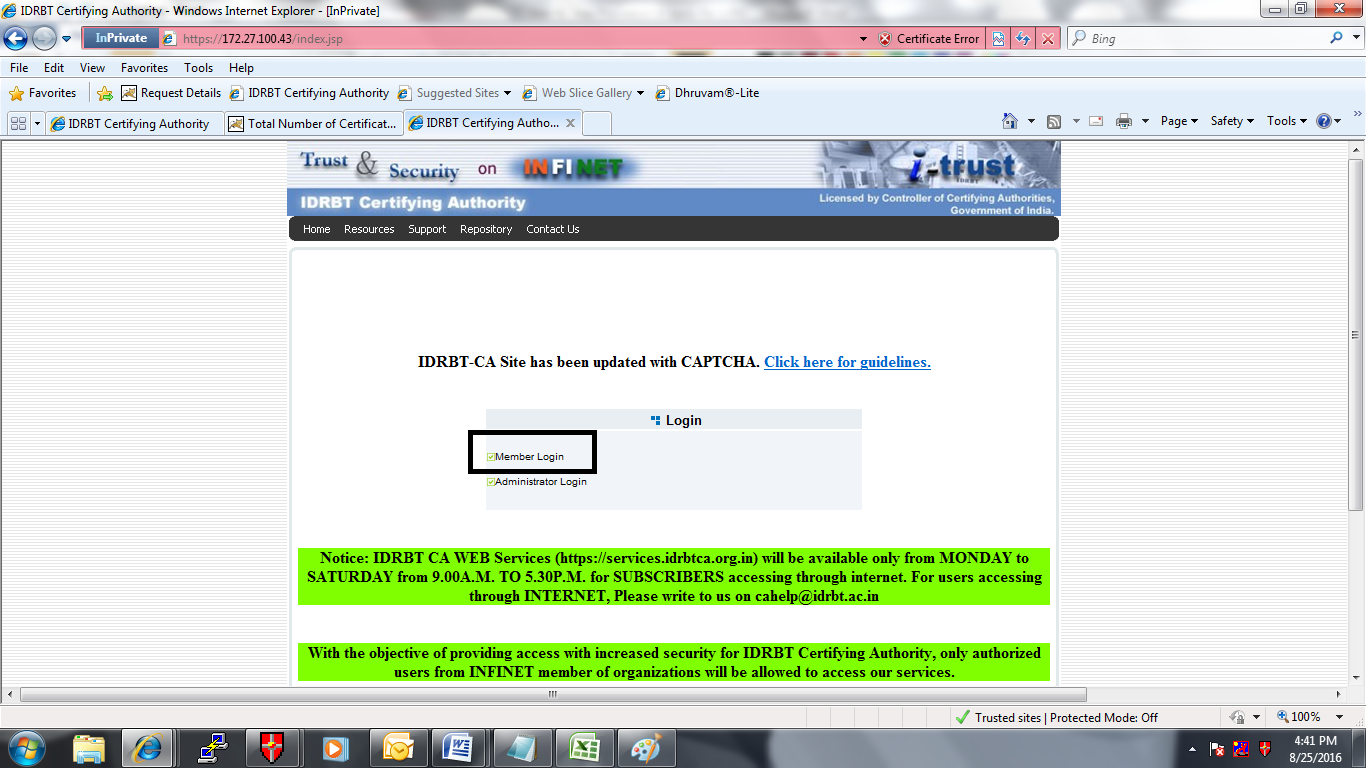


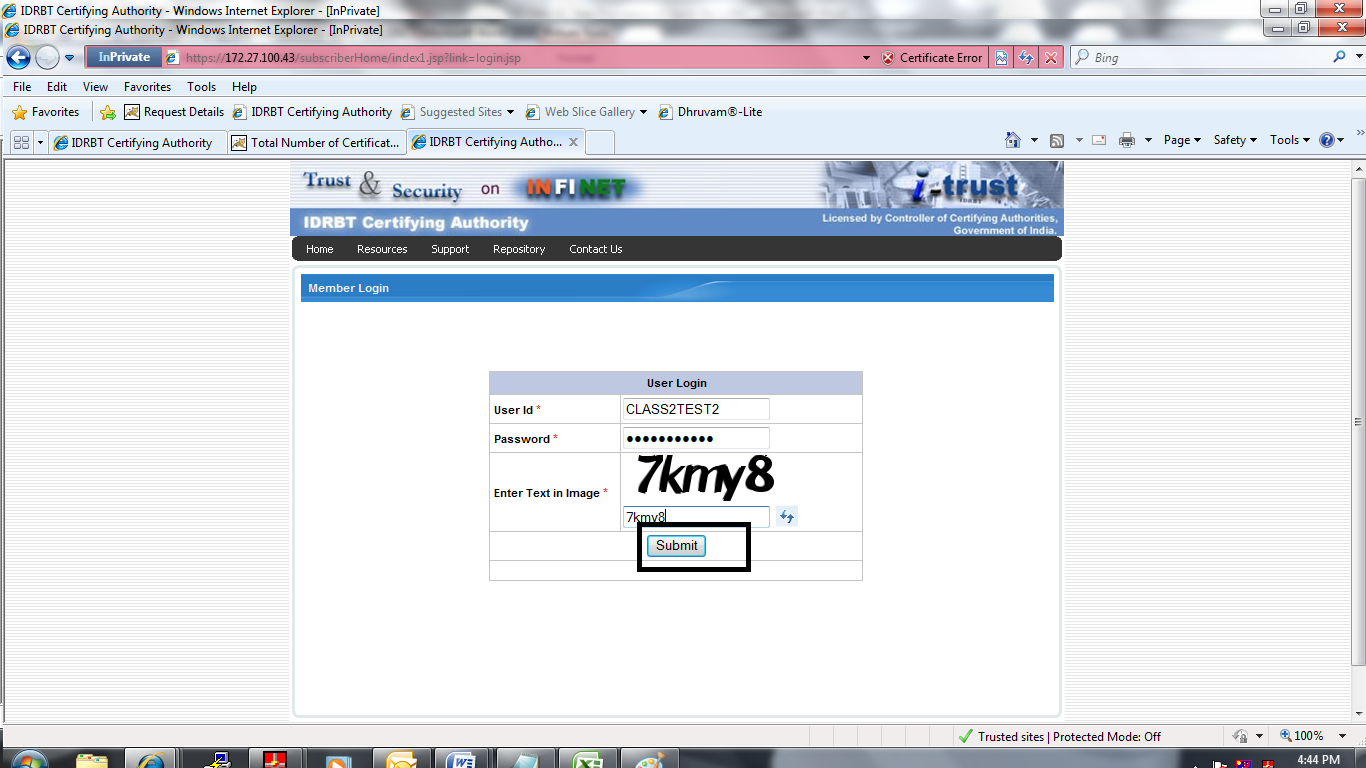
1. After getting the request number, note down the request number and choose the last option “Log Out” from the menu.

\*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).

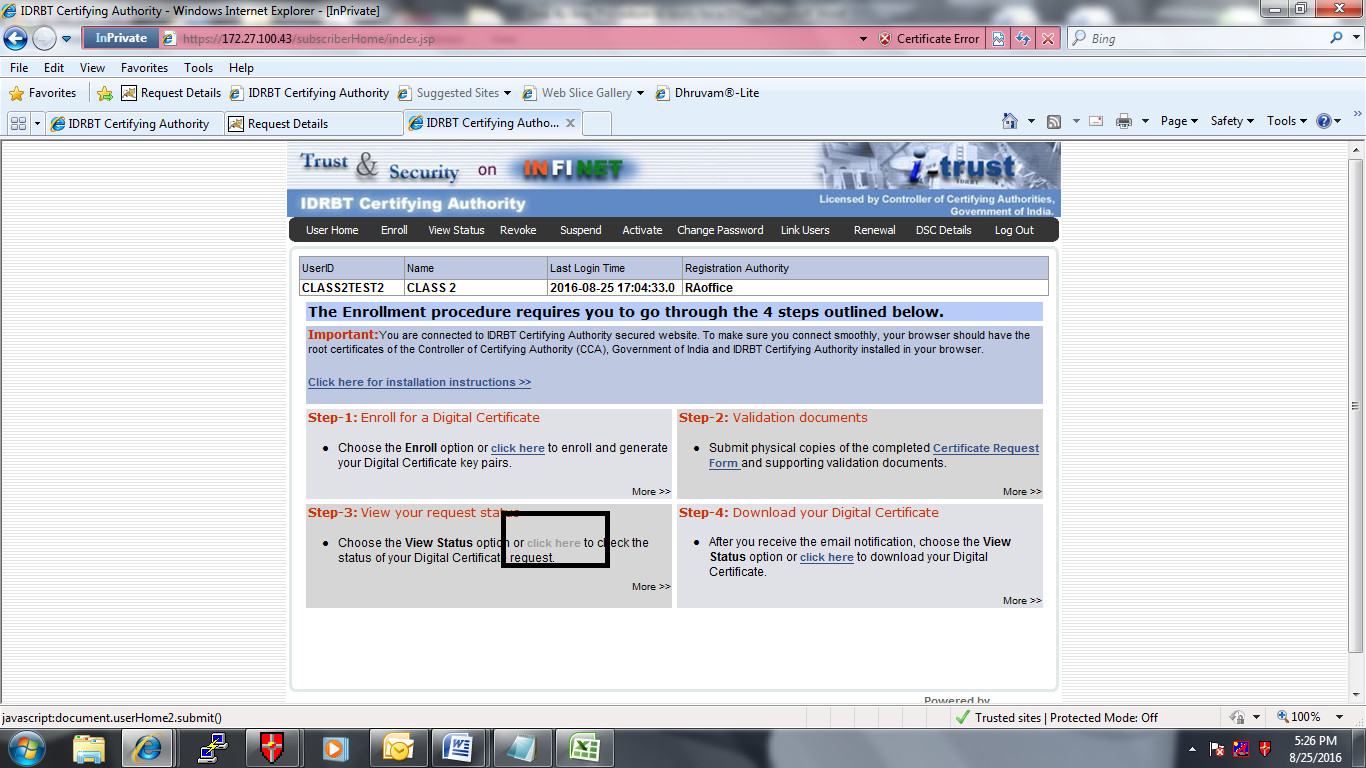
**Step 5: For downloading the SHA2 2048 Class II/ Class III signing certificate by the applicant: (**Download theCertificate on the same Personal Computer from which the request has been initiated)

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.



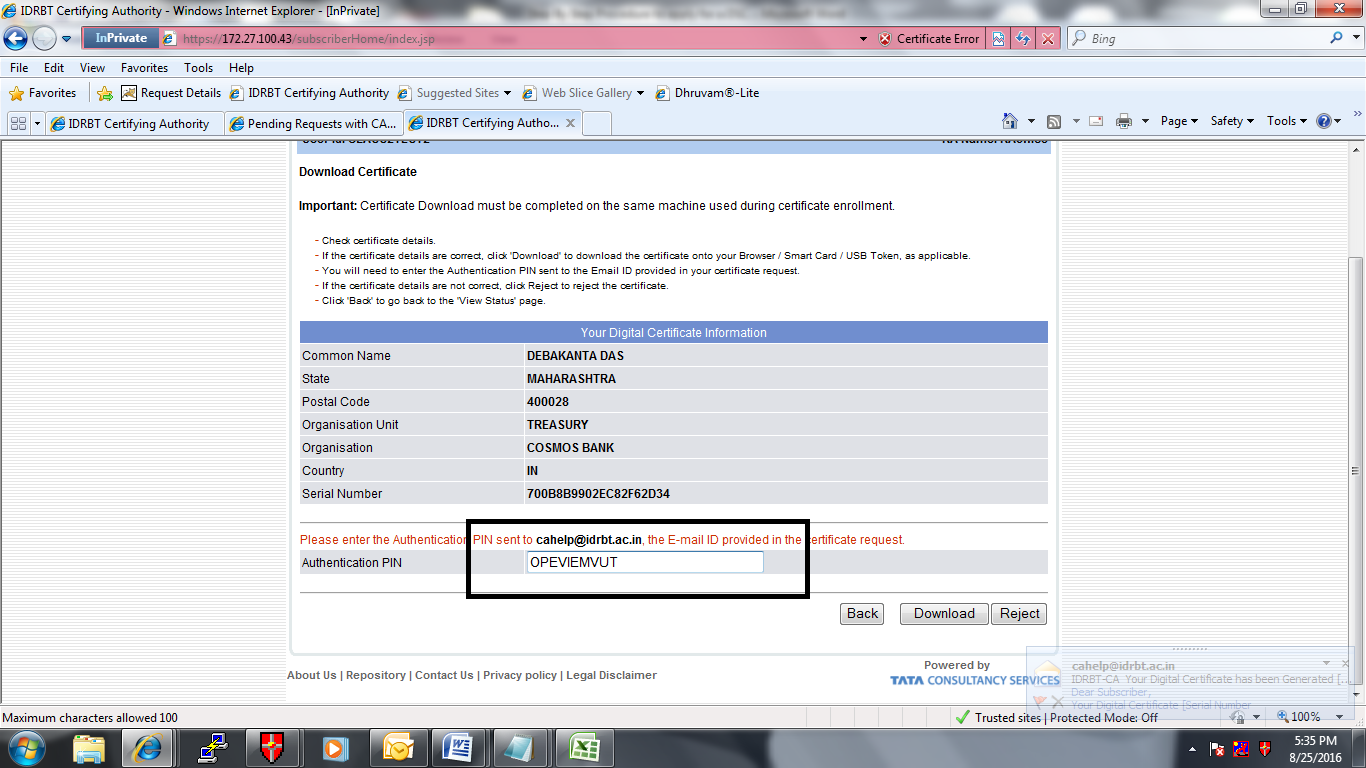


1. Click on Step 3 “View Status”

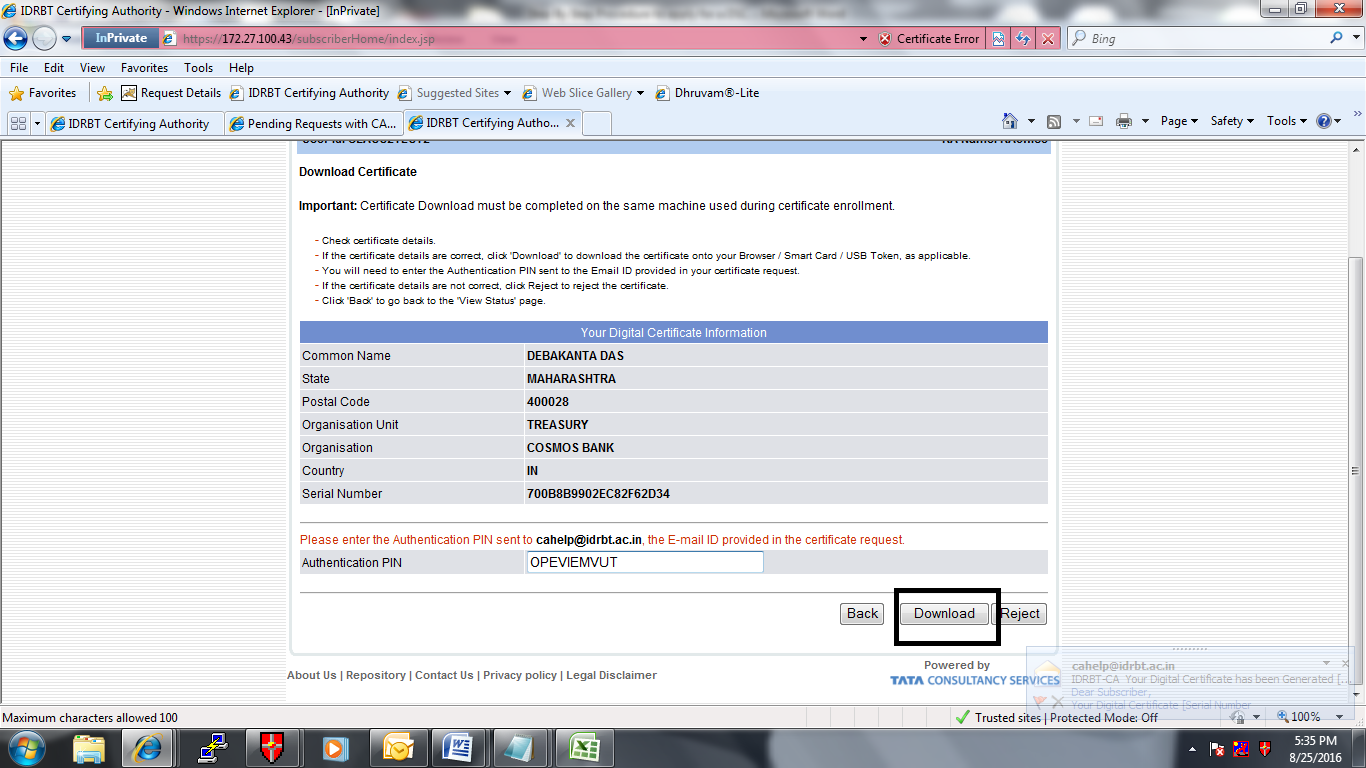


1. List of Certificate Request numbers will appear along with status. Once the Status is shown as

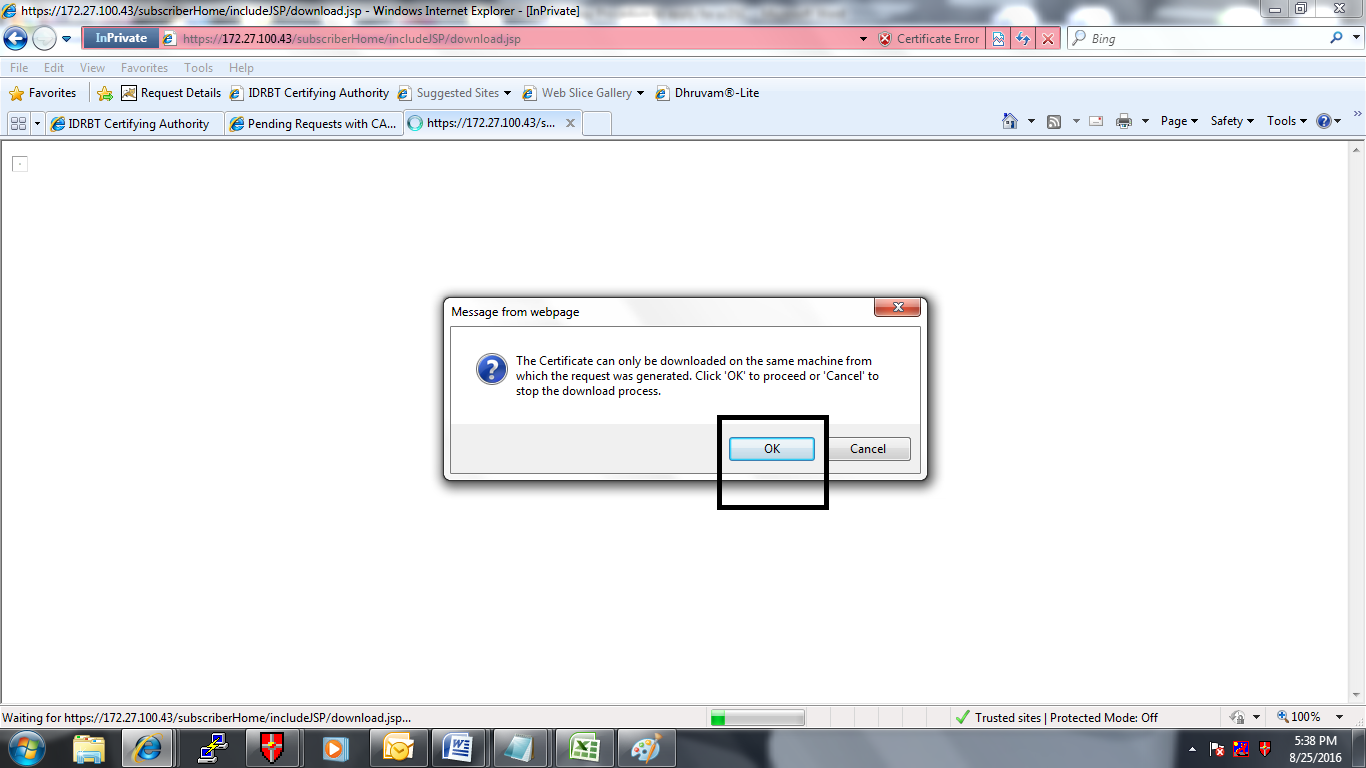
“Certificate Generated” against the request number generated by the applicant, Click on the Request number. Please do not forget to insert the e-token that was used for generating the request. Copy and Paste the Authentication PIN received by E-mail Insert the same e-token which was used at the time of initiating online request generation.



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



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



\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**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 RA Office for Face to Face verification.

She/he should carry the following:

      1.  Authorization/ Forwarding letter from the bank authorizing the official concerned to apply for a digital certificate

2.  The application form along with proof of ID (duly attested) to IDRBT CA during the Face to Face verification.

3.  Original proof of ID to be shown to the officials at RA during Face to Face verification.

**IDRBT RA Cost Structure**

**For class 2 certificates cost details for 1yr validity:**

Rupees 500/ for 1 Years Certificate + Rupees 500/ for Admin Charges + 14% S. Tax + 0.5%(swachh Bharat)+0.5% (krishi kalyancess)🡪 Rs. 1000+15% service tax% 🡪Rs. 1150/- per certificate

**For class 2 certificates cost details for 2yrs validity:**

Rupees 1000/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 14% S. Tax+ 0.5% (swachh Bharat) + 0.5% (krishi kalyancess)🡪 Rs. 1500+ 15% services tax % 🡪Rs.1725/- per certificate

**For Class 3 Certificate Cost Details For 1year**

Rupees 10000/ for 1 Years Certificate + Rupees 500/ for Admin Charges + 14% S.tax + 0.5%(swachh Bharat)+0.5% (krishi kalyan cess) ==> 10500+15% service tax ==> 12075 /- per certificate

**For Class 3 Certificate Cost Details For 2yrs**

Rupees 20000/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 14% S.tax+ 0.5% (swachh Bharat) + 0.5% (krishi kalyan cess) 🡪 20500+ 15% services tax🡪23575/- per certificate.

**Cooperative Banks Cost Structure**

**For class 2 certificates cost details for 1yr validity:**

Rupees 250/ for 1 Year Certificate + Rupees 500/ for Admin Charges + 14% S.tax+ 0.5% (swachh Bharat) + 0.5% (krishi kalyan cess)= Rupees 750/+15% ==>862.50/- per certificate.

**For class 2 certificates cost details for 2yrs validity:**

Rupees 500/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 14% S.tax+ 0.5% (swachh Bharat) + 0.5% (krishi kalyan cess)= Rupees 1000/+15% ==>1150/- per certificate.

**For Class 3 Certificate Cost Details For 1year**

Rupees 10000/ for 1 Years Certificate + Rupees 500/ for Admin Charges + 14% S.tax + 0.5%(swachh Bharat)+0.5% (krishi kalyan cess) ==> 10500+15% service tax ==> 12075 /- per certificate

**For Class 3 Certificate Cost Details For 2yrs**

Rupees 20000/ for 2 Years Certificate + Rupees 500/ for Admin Charges + 14% S.tax+ 0.5% (swachh Bharat) + 0.5% (krishi kalyan cess) 🡪 20500+ 15% services tax🡪23575/- per certificate.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*