

2. DOWNLOAD ENCRYPTION CERTIFICATE

1. Open NICCA website and click Member Login.



The screenshot shows a web browser window with the URL <https://nicca.nic.in/>. The page title is "NIC Certifying Authority". The navigation menu includes Home, Resources, Support, Repository, and Contact Us. A prominent message states: "Pls read carefully Encryption Key Backup Procedure" and "Pls read carefully Encryption Key Backup Procedure". Below this, there are links for "View DSC Fee Structure", "Download DSC Request Form", and "Download Smart Card/USB eToken Driver". A section titled "Download Certificate chain" is highlighted in green. A yellow box contains a "NOTICE: Implementation of Interoperability Guidelines for Digital Signature Certificates (DSC) issued under Information Technology Act, 2008". It states: "It is to bring to the notice of all concerned that NICCA would start issuing DSC as per new certificate profile as laid down in the Interoperability Guidelines upon communication from CCA. All application vendors are requested to test their application with new certificates (DSC) which can be downloaded from here: [SHA256 with 2048](#) [Trust Chain](#)". A "*** NOTICE ***" section follows, stating: "All CA/RA Administrators/Officers are required to get issued fresh DSC with SHA256/2048 bits for their ROLE CARDS on immediate basis because existing DSC cards with SHA1 will not work for DSC issuance. Pls send your request immediately to NICCA Delhi. Those who have already issued SHA256 card NEED NOT to request fresh DSC for their Role cards. (Pls update your client to JRE 6) [Download JRE 6 \(32 bit\)](#) [FAQs for DLL to select RAA & CAO card/token](#) [Prerequisites for Token Installation](#)". Below this, it says "As per CCA directives: From 1st January 2012, NICCA shall issue DSC with Signature Algorithm SHA256 with 2048 bits key strength only." A "Login" section is visible with radio buttons for "Member Login" and "Administrator Login". A green box at the bottom contains the text: "Instructions for Digital Certificate Enrolment: Digital certificate enrolment & key generation on etoken/ smart card supports only Windows XP/2000/Vista/7.0 with browser IE6/7/8". The Windows taskbar at the bottom shows the time as 10:50 AM on 5/10/2013.

2. Enter user ID and Password and click submit.



3. Go to step 4 on screen and click download Digital Certificate.

The screenshot shows a web browser window with the URL <https://nicca.nic.in/subscriberHome/authenticateLogin.jsp>. The page title is "NIC Certifying Authority". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help".

The main content area features the NICCA logo and a navigation menu with options: "User Home", "Enroll", "View Status", "Revoke", "Suspend", "Activate", "Change Password", "Renewal", and "Log Out".

A table displays user information:

UserID	Name	Last Login Time	Registration Authority
G2_DL_38588	A Banerjee	2013-05-02 16:02:15.0	NIC Registration Authority

Below the table, a section titled "The Enrollment procedure requires you to go through the 4 steps outlined below." contains an "Important" note and a link for "Installation instructions".

The enrollment steps are:

- Step-1: Enroll for a Digital Certificate**
 - Choose the Enroll option or [click here](#) to enroll and generate your Digital Certificate key pairs.
- Step-2: Validation documents**
 - Submit physical copies of the completed [Certificate Request Form](#) and supporting validation documents.
- Step-3: View your request status**
 - Choose the View Status option or [click here](#) to check the status of your Digital Certificate request.
- 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.

At the bottom of the page, there are links for "About Us", "Repository", "Contact Us", "Privacy Policy", and "Legal Disclaimer". The page is powered by "TATA CONSULTANCY SERVICES".

The Windows taskbar at the bottom shows the system clock as 10:54 AM on 5/10/2013.

4. Now click Request No of Encryption certificate.



The screenshot shows a web browser window with the URL <https://nicca.nic.in/subscriberHome/index.jsp>. The page title is "NIC Certifying Authority". The user is logged in as "User: G2_DL_38588" with the role "RA Name: NIC Registration Authority".

The "View Status" section contains the following instructions:

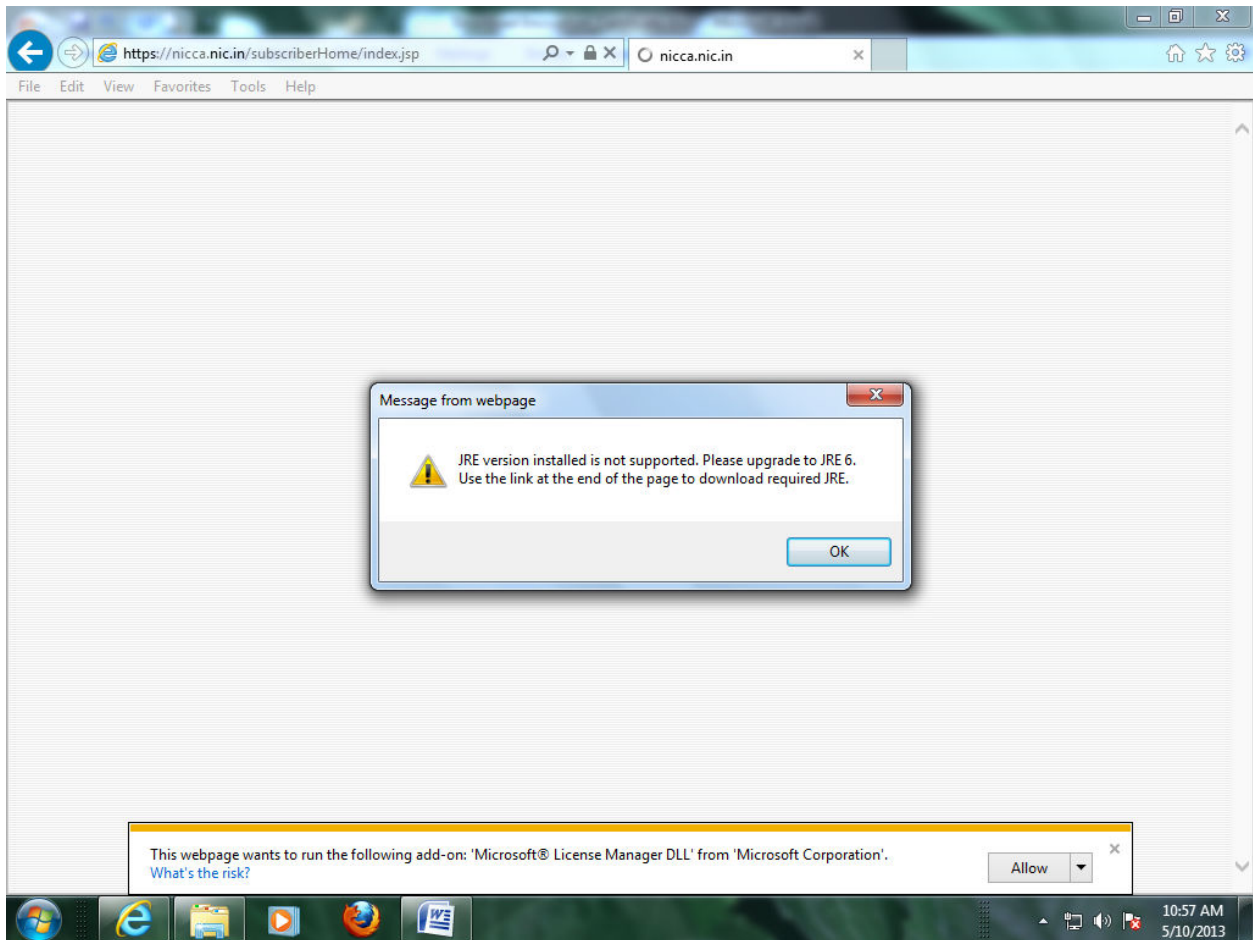
- The hyperlink on Request No. helps you to View/Download the certificate.
- The hyperlink on Status helps you to view the certificate life cycle.
- The sorted column is indicated by image [icon]. Click a column title to sort records on that column.
- The image [icon] gives information/comments given by the Registration Authority/Certifying Authority.

Request No.	Status	Request Type	Certificate Type	Certificate Class	Certificate Profile	Date of Request
129248	Certificate Generated	GENERATION	Signing Certificate	Class 2	Organization	2012-11-27 14:15:35
129257	Certificate Generated	GENERATION	Encryption Certificate	Class 2	Organization	2012-11-27 14:23:15

Page - 1/1

Powered by TATA CONSULTANCY SERVICES

5. Now press OK if JRE version 6 is not there.



6. Insert USB token and Click Download.

The screenshot shows a web browser window with the URL <https://nicca.nic.in/subscriberHome/index.jsp>. The page title is "NIC Certifying Authority". The user is logged in as "User Id: G2_DL_38588" under the "RA Name: NIC Registration Authority".

The main content area is titled "Download Certificate" and includes instructions:

- Click Download to download the certificate into a file.
- You will need to enter the Authentication PIN sent to the Email ID provided in your certificate request.
- Click Back to go back to the 'View Status' page.

Below the instructions is a table titled "Your Digital Certificate Information":

Your Digital Certificate Information	
Common Name	BANERJEE AMITABH
State	NEW DELHI
Postal Code	110001
Organisation Unit	DTE OF IT
Organisation	INDIAN COAST GUARD
Country	IN
Serial Number	330977980701D4438C6E

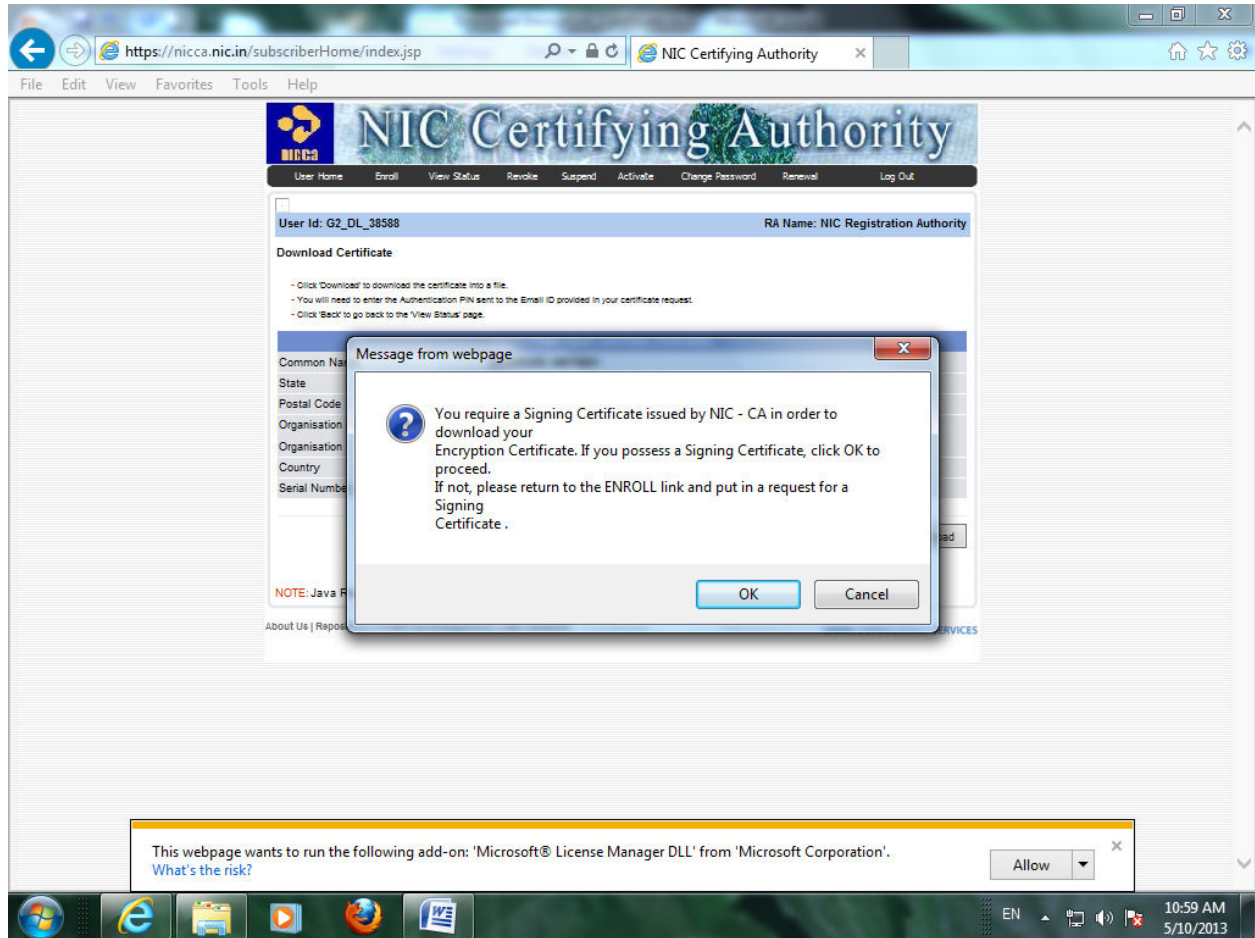
At the bottom of the table area are "Back" and "Download" buttons. A note below the table states: "NOTE: Java Runtime Environment 1.8.0_29 or above is required for loading the applet. [Click here](#) to download JRE 1.8.0_29."

The footer contains "About Us | Repository | Contact Us | Privacy Policy | Legal Disclaimer" and "Powered by TATA CONSULTANCY SERVICES".

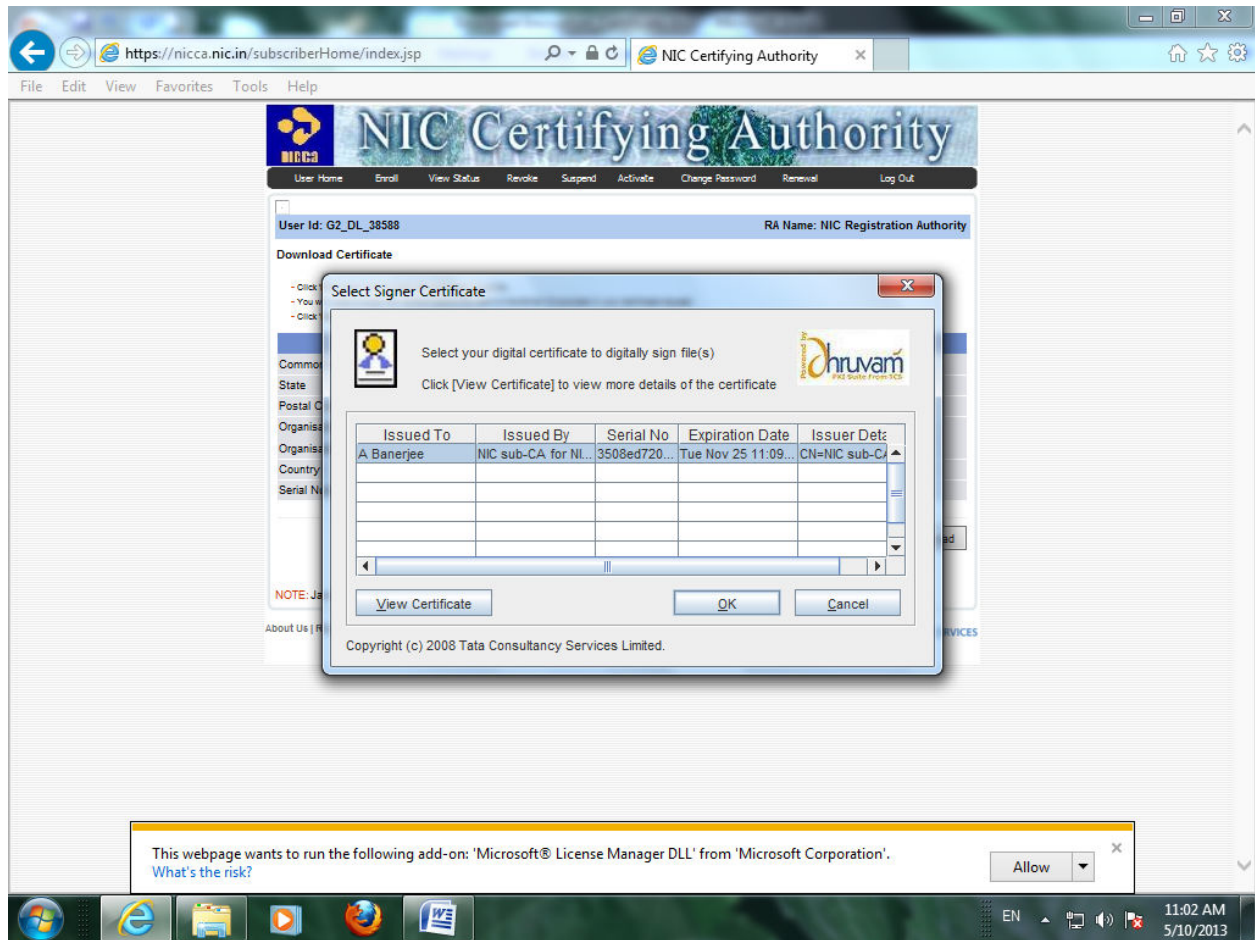
A security warning dialog box is visible at the bottom of the browser window, stating: "This webpage wants to run the following add-on: 'Microsoft® License Manager DLL' from 'Microsoft Corporation'. What's the risk?" with an "Allow" button.

The Windows taskbar at the bottom shows the system tray with the date and time: "10:59 AM 5/10/2013".

7. Click OK.



8. Click OK.



9. Select certificate and click OK.

The screenshot shows a web browser window at the URL <https://nicca.nic.in/subscriberHome/index.jsp>. The page title is "NIC Certifying Authority". The user profile information is as follows:

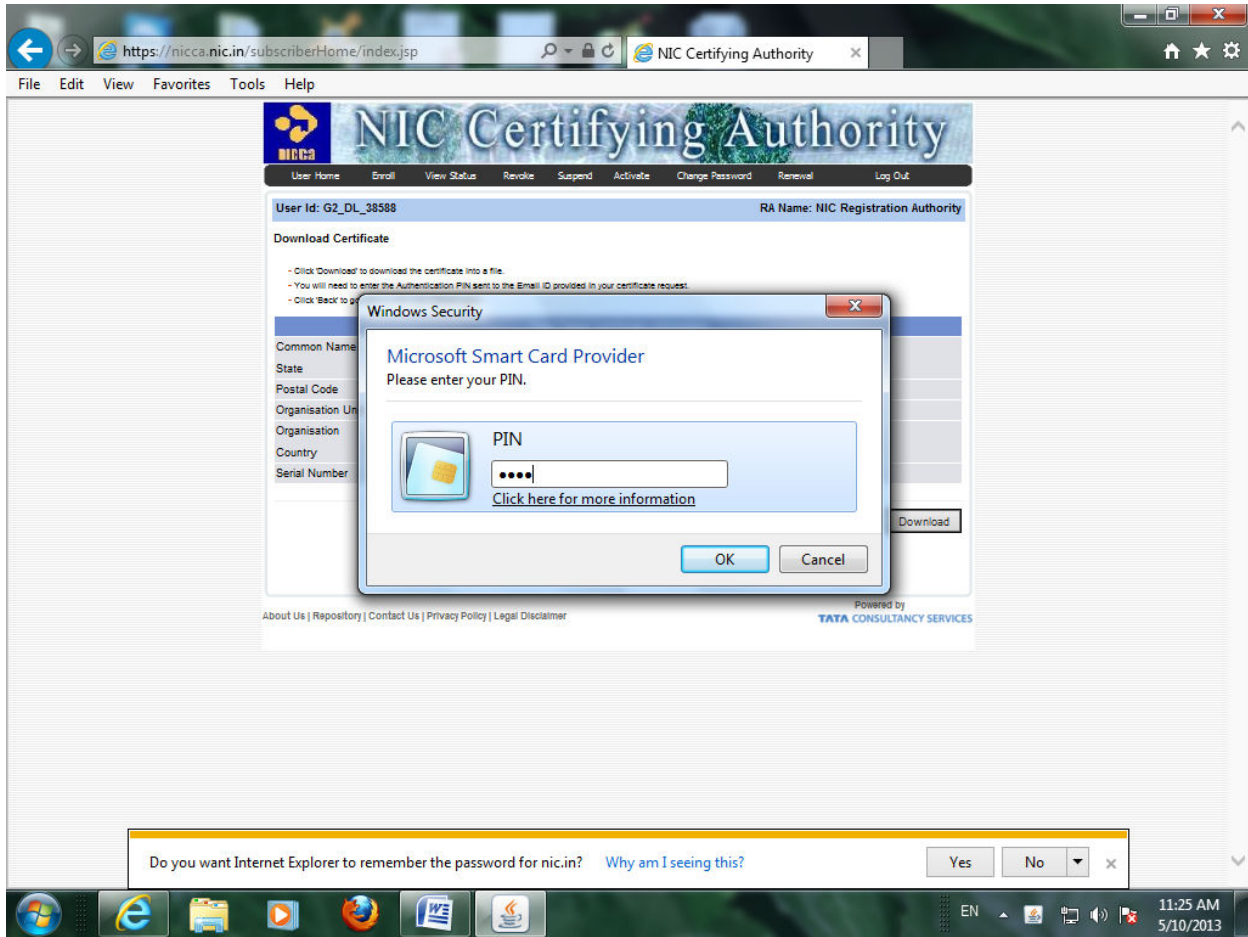
User Id:	G2_DL_38588
Common Name:	BANERJEE
State:	NEW DELHI
Postal Code:	110001
Organisation Unit:	DTE
Organisation:	INDIA
Country:	IN
Serial Number:	33097

The "Select Signer Certificate" dialog box is open, displaying a table of certificates:

Issued To	Issued By	Serial No	Expiration Date	Issuer Det
A Banerjee	NIC sub-CA for NI...	3508ed720...	Tue Nov 25 11:09...	CN=NIC sub-C...

The dialog box also includes a "View Certificate" button, "OK" and "Cancel" buttons, and a copyright notice for Tata Consultancy Services Limited. At the bottom of the browser window, a security warning states: "This webpage wants to run the following add-on: 'Microsoft® License Manager DLL' from 'Microsoft Corporation'. What's the risk?" with an "Allow" button.

10. Enter USB token PIN (0000).



11. Now Select save as option and give path then click save.

