

New SSL certificates have been deployed for PFMS and Bharatkosh portals on 29/02/2016. Some of the users are facing problem to open these sites. To resolve this problem CCA(Chief Certifying Authority) certificate is needed to be enabled “trusted” manually one time for Internet Explorer, Google Chrome and Mozilla Firefox browsers before opening the website for PFMS and Bharatkosh.

Steps to do the above mentioned activity are as under:

## **For Internet Explorer browser**

Following steps are to be followed to “trust”the CCAcertificate in Internet Explorer

### Step 1

- Right click Internet Explorer icon and select ‘**Run as Administrator**’ option from available set of options

### Step 2

- In the Internet Explorer’s browser, Click on ‘Settings’ button available at the right hand side of the browser window.
- After selecting ‘Settings’, click ‘Internet Options’ as shown in the figure below.

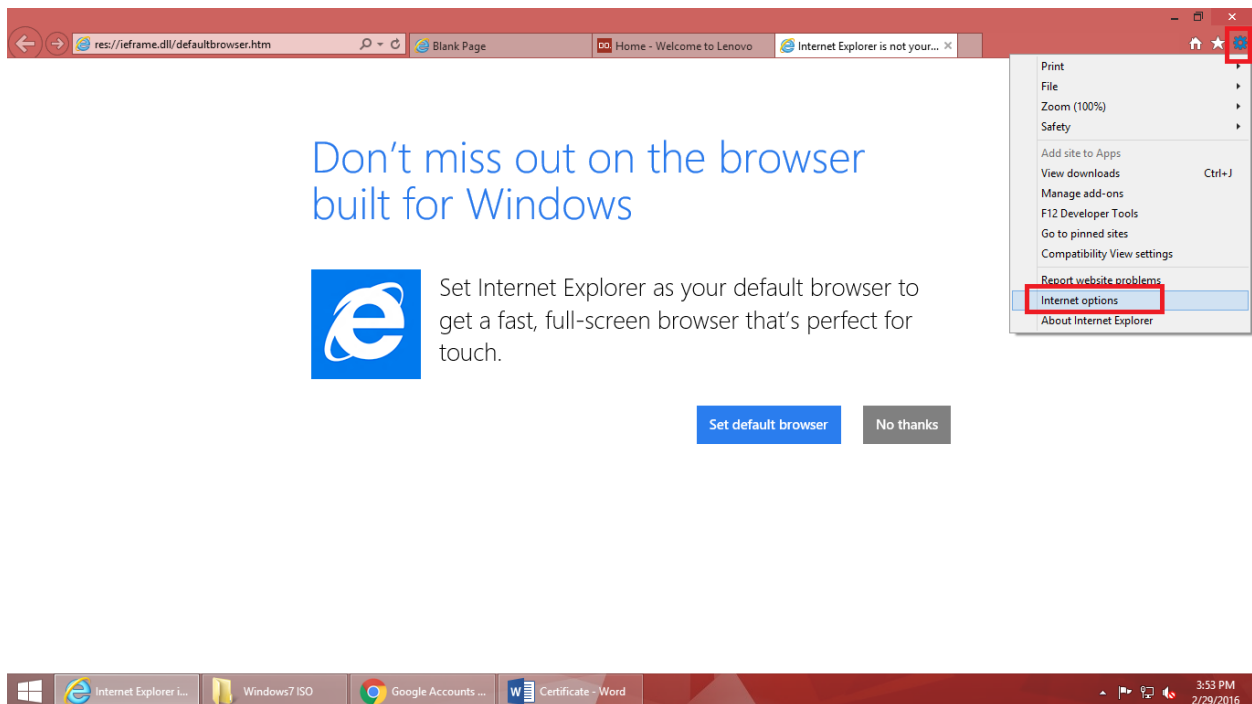


Figure 1: Internet Explorer Browser

### Step3

- After selecting 'Internet Options' in previous step, tab will appear on the screen containing 'Content' as one of the tab.
- Click on 'Content' tab.

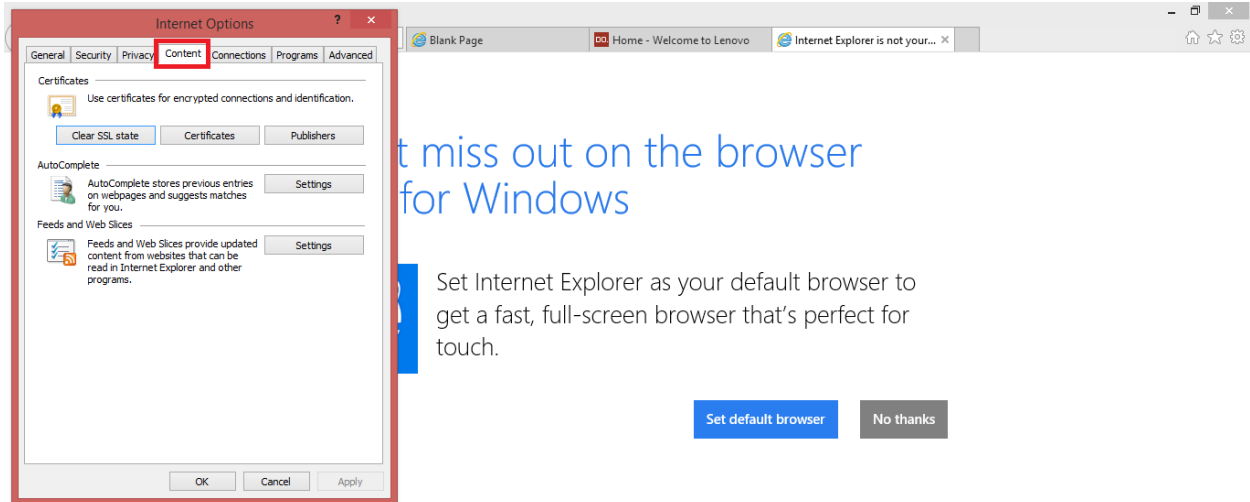


Figure 2: Select Content Tab

## Step 4

At 'Content' tab, click on 'Certificates' button as shown below.

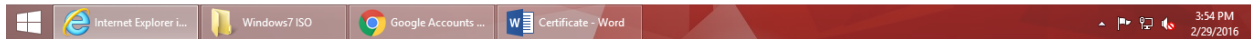
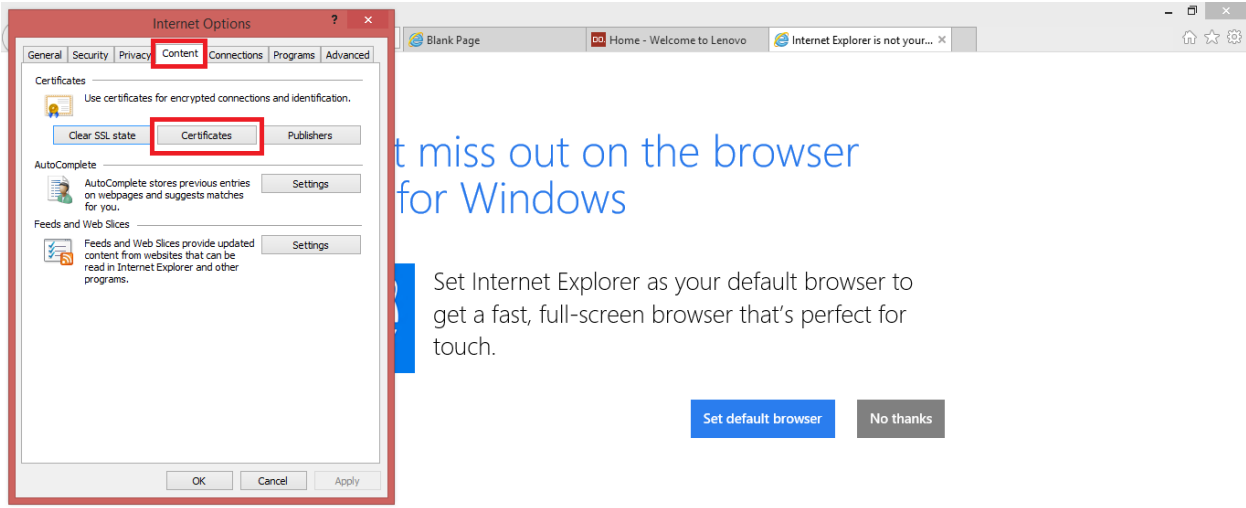


Figure 3: Select Certificate

## Step 5

On the screen that follows, Click on 'Trusted Root Certification Authorities' tab.

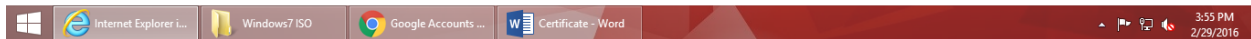
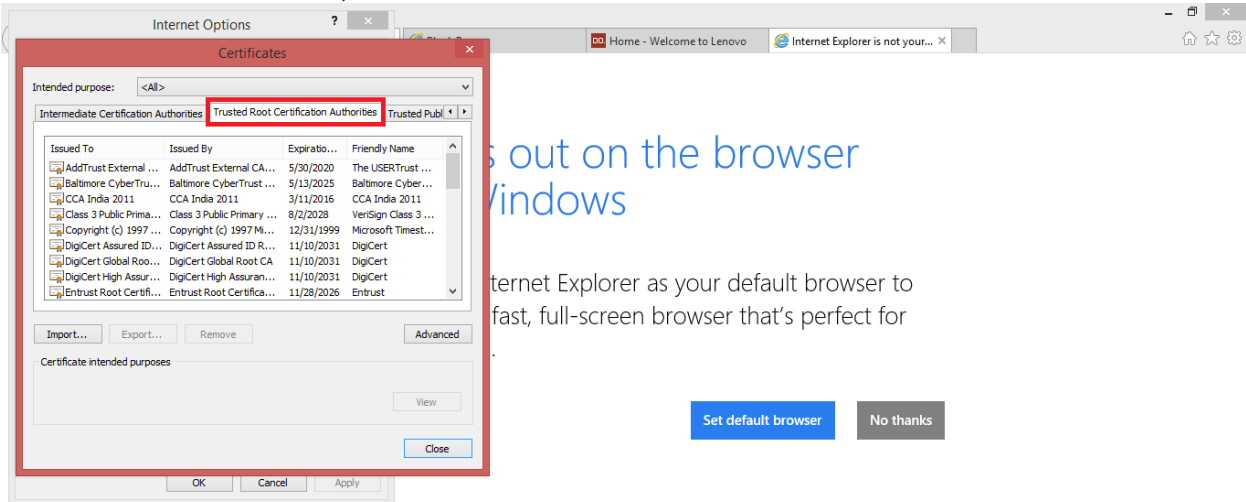


Figure 4: Trusted Root Certification Authorities'

## Step 6

At 'Trusted Root Certification Authorities' tab, look for 'CCA India 2014' certificate option in the presented list of options under the tab.

In case the 'CCA India 2014' certificate option is available, then user shall double click the certificate and proceed as explained in Step 7 and further.

## Step 6(a)

In case, 'CCA India 2014' certificate option is not found in the presented list of options, then user would require to download & install the certificate from the following link:

<https://www.ncodesolutions.com/>

After clicking the mentioned link, user shall be navigated to page required to download the certificate.

At the concerned opened page, user shall click on '**CCA Certificate 2014**' link available on the screen.

Clicking the mentioned '**CCA Certificate 2014**' link would download the required certificate in user's machine as .der file.



Figure 5: Download Certificate

After downloading the required certificate file, user shall select 'Trusted Root Certification Authorities' tab as explained above (Step 1 to Step 6).

At 'Trusted Root Certification Authorities' tab, user shall click 'Import' button to import the downloaded certificate.

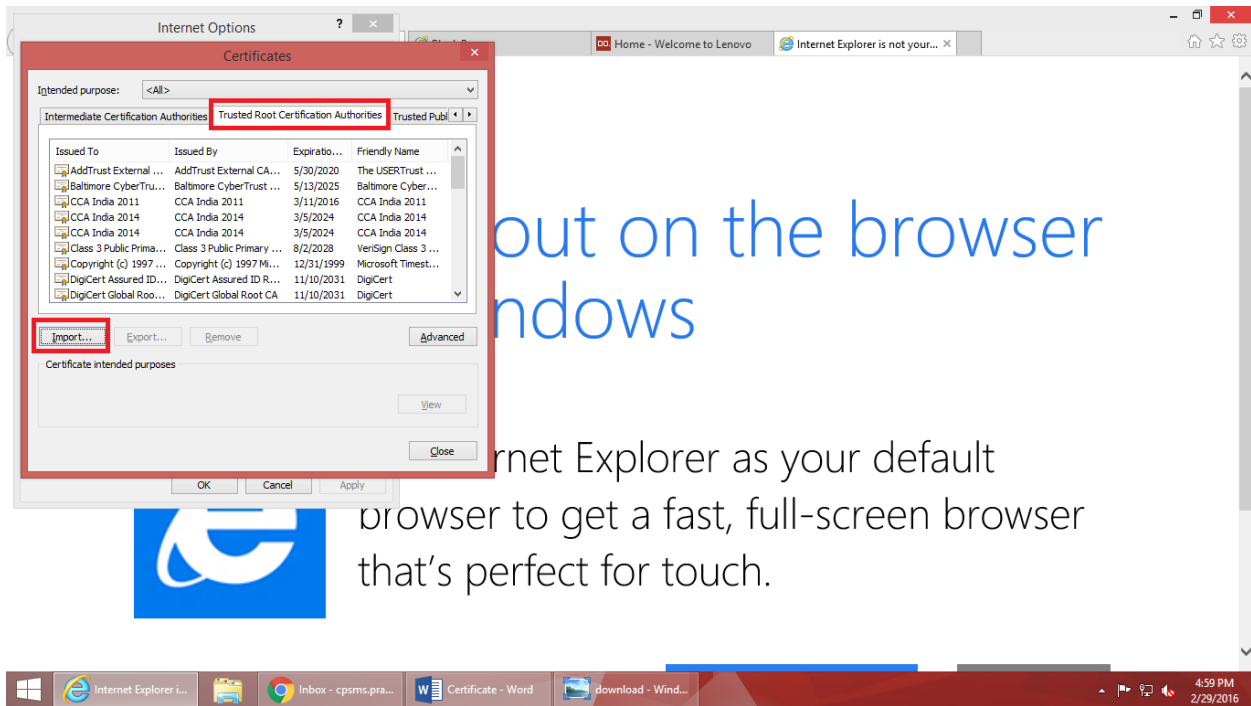


Figure 6: Import Certificate

On the screen that follows, click 'Next' to proceed with certificate import procedure.

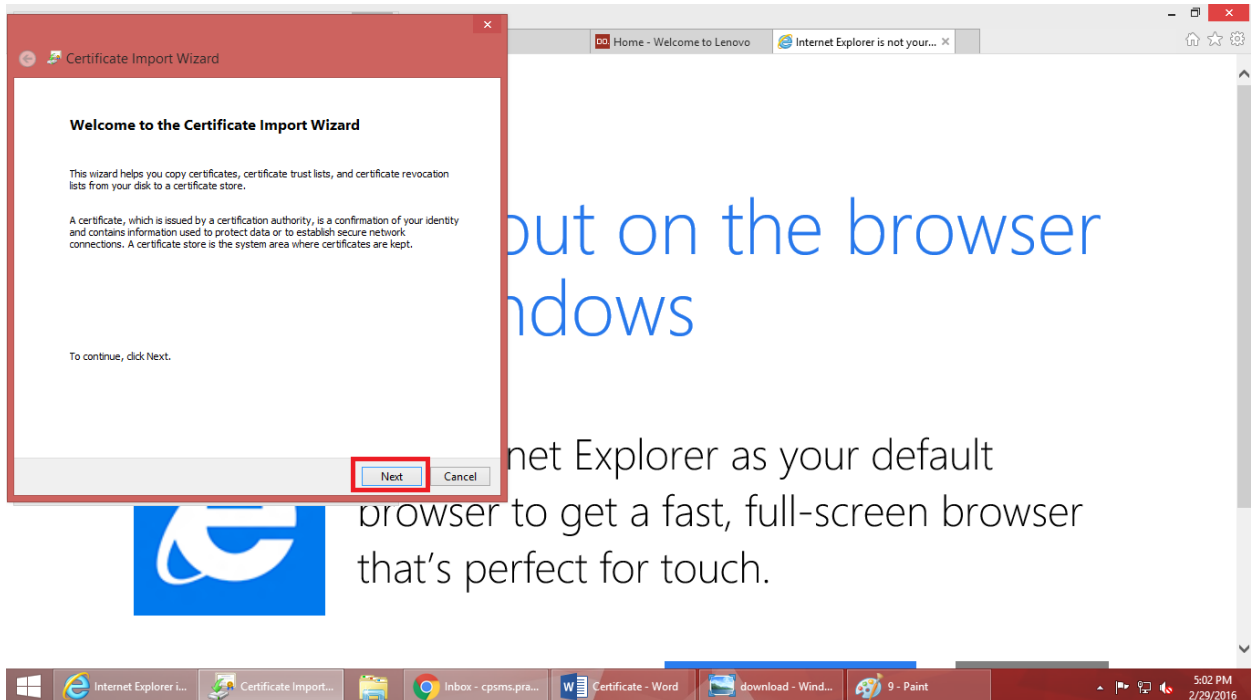


Figure 7: Import Certificate

After clicking 'Next', user shall be directed to upload the downloaded certificate. User shall click 'Browse' to upload the concerned file.

Once the concerned file is uploaded successfully, user shall click 'Next' to proceed to next step of certificate import.

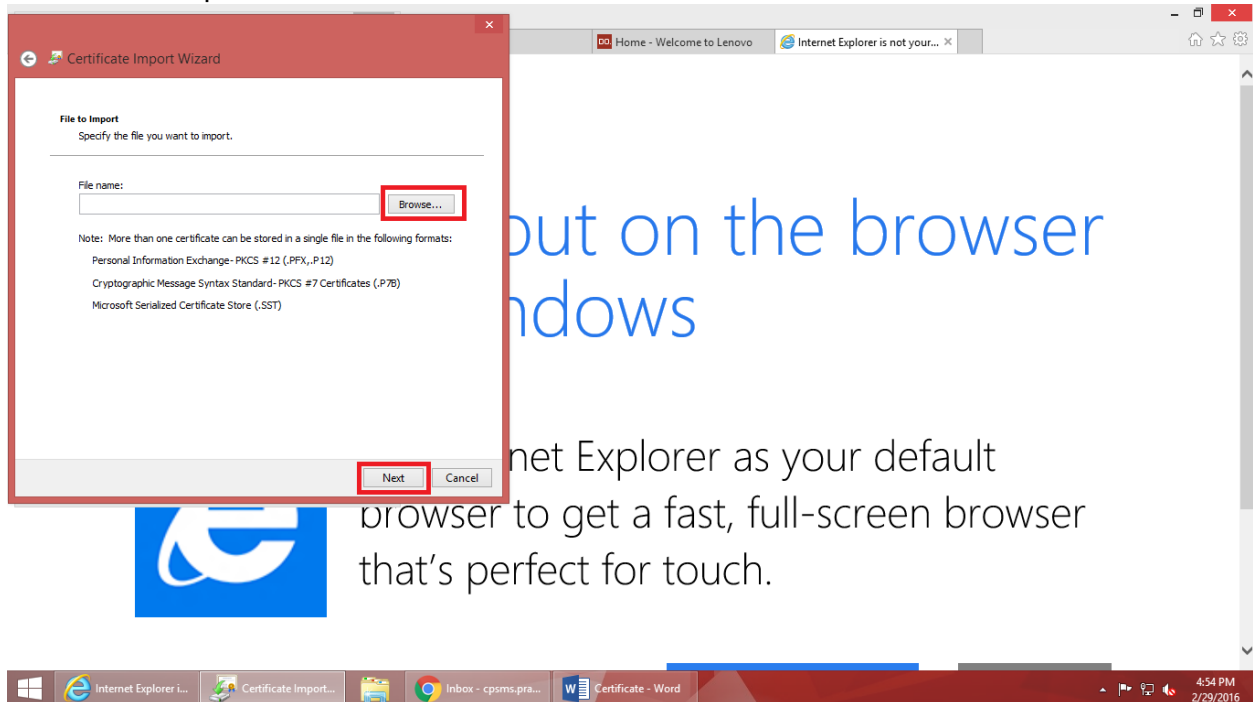


Figure 8: Upload Certificate

## Step 7

The uploaded certificate shall be listed under 'Trusted Root Certification Authorities' tab as shown in the screen below.

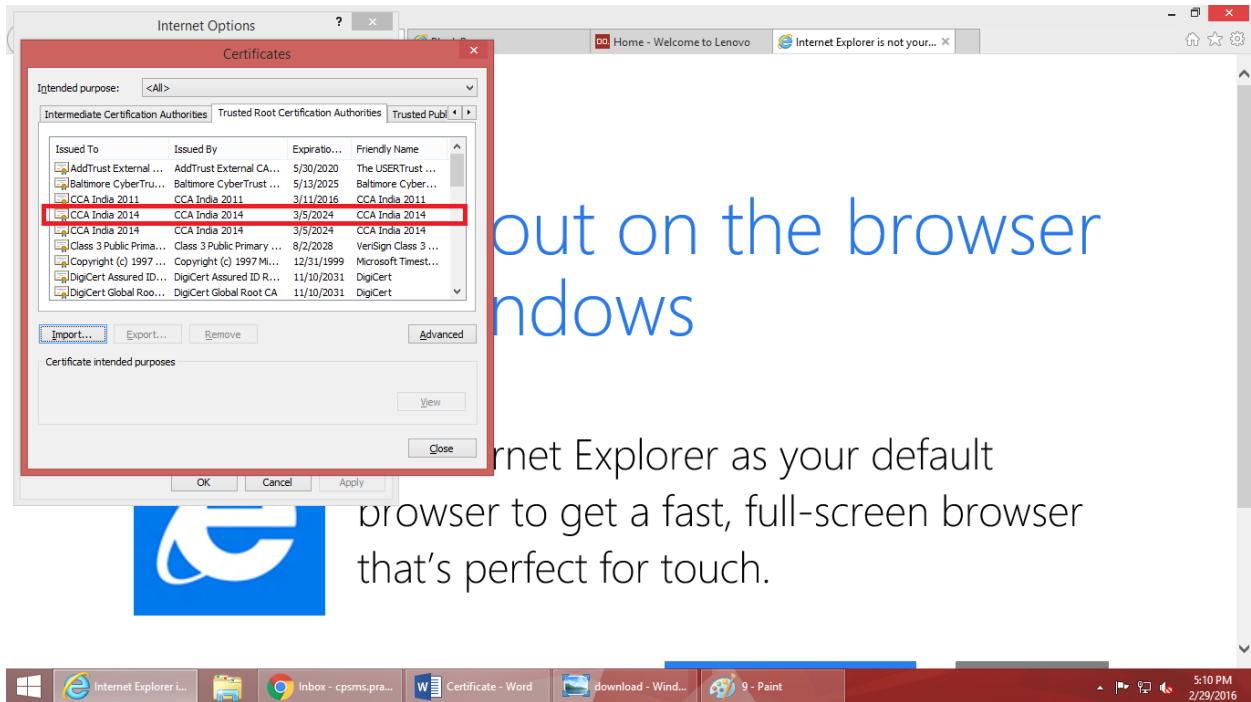


Figure 9: Certificate Uploaded Successfully

## Step 8

Once the certificate is available in list, user shall double click the 'CCA India 2014' link to proceed to next step.

After double clicking the 'CCA India 2014' link, user shall the 'Details' tab.

At 'Details' tab, user shall click 'Edit Properties' button.

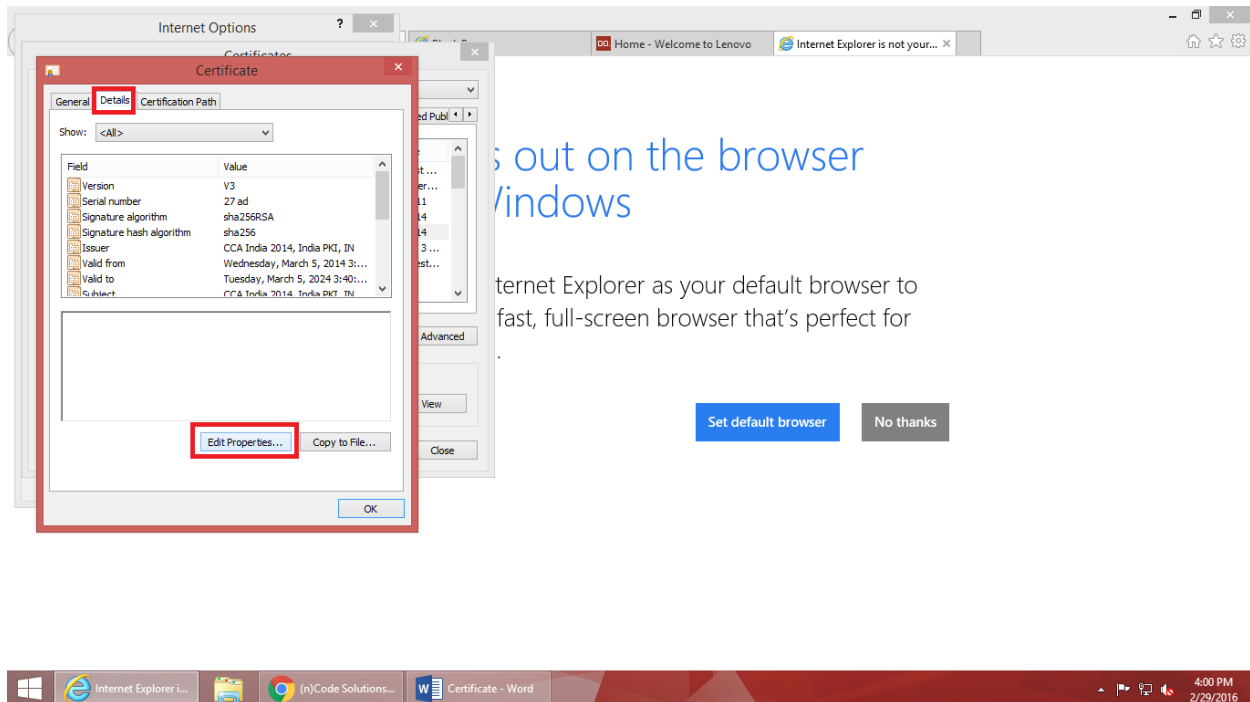


Figure 10: Edit Properties



## Step 9

After clicking 'Edit Properties', user shall be directed to 'Certificate Properties' window.

At 'Certificate Properties' window, user shall select radio button 'Enable all purposes for this Certificate' under 'General' tab.

After selecting the mentioned radio button, click 'Apply' button and then click 'Ok' button.

Certificate would be enabled successfully.

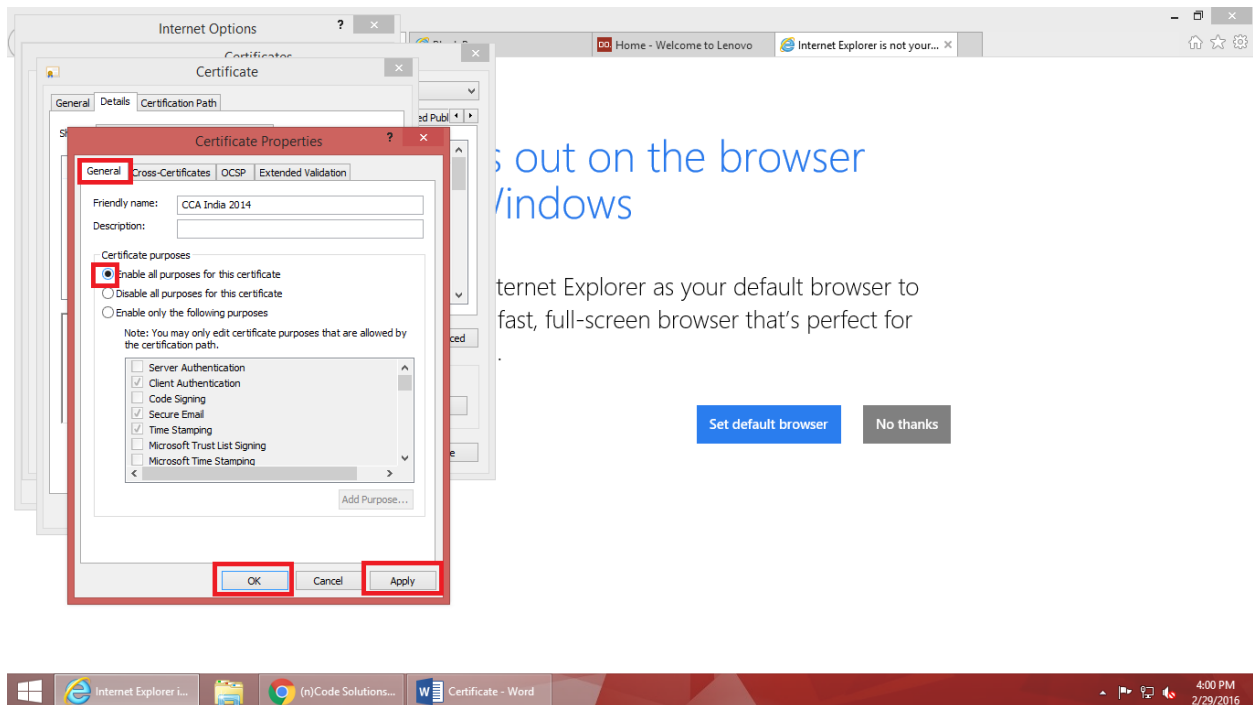


Figure 11: Enable Certificate

## For Google Chrome Browser

User shall perform configuration steps to enable the required certificate in Google Chrome browser.

### Pre-Requisite

- Certificate shall first be imported in Internet Explorer

After importing the certificate in Internet Explorer browser as explained above, user shall select Customize & Control icon on right hand side in Chrome browser.

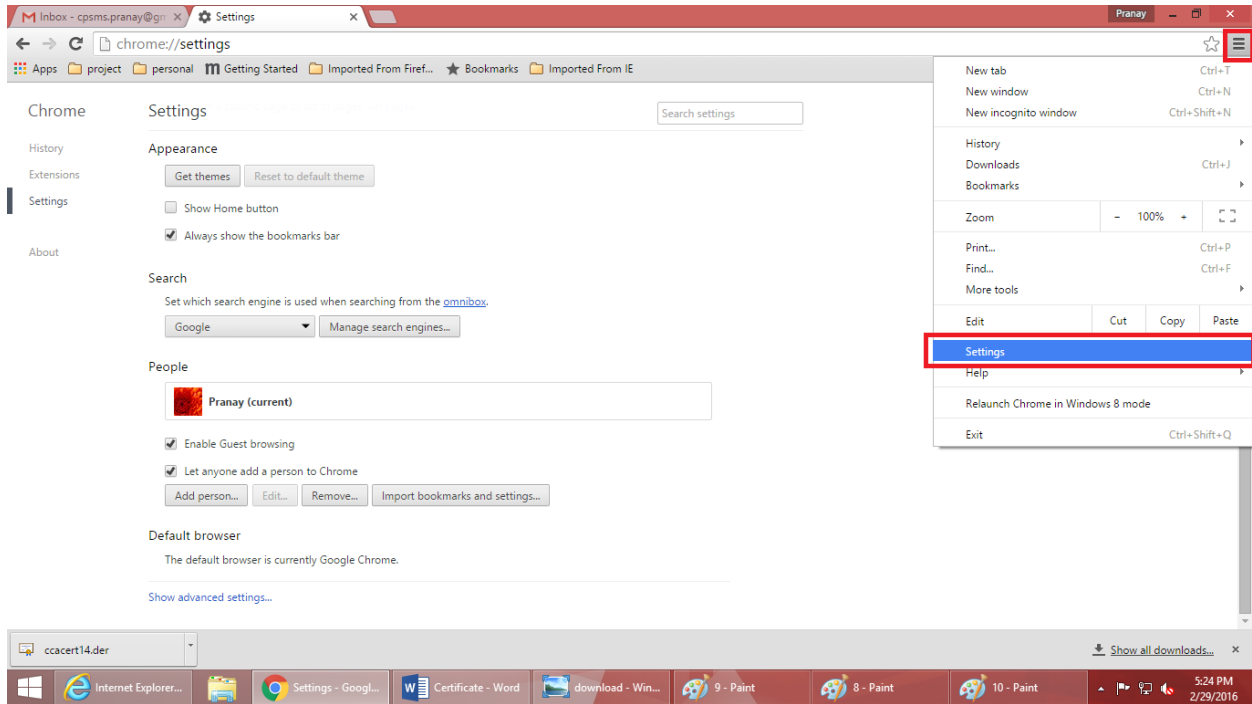


Figure 12: Configure Certificate in Chrome

At 'Settings' screen, user shall select 'Import bookmarks and settings' button.

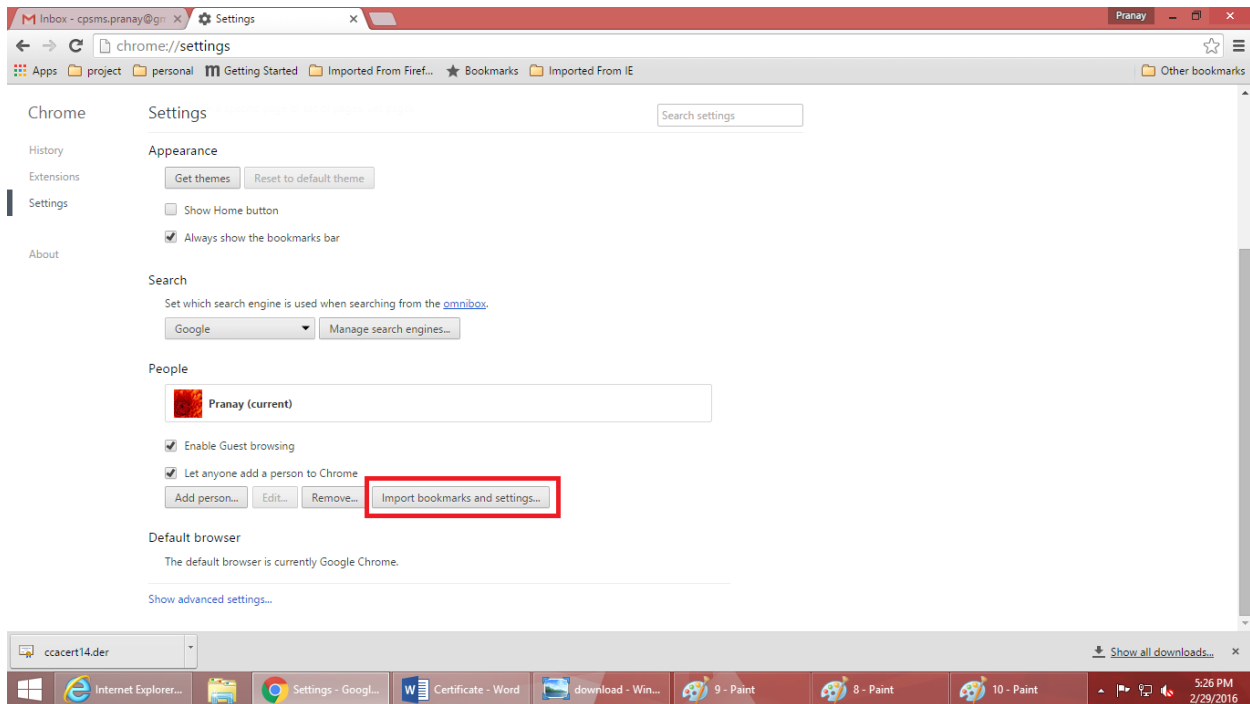


Figure 13: Import Certificate

On the screen that follows, select 'Microsoft Internet Explorer' option from dropdown. Select all the check boxes and click 'Import' button to import the certificate from Internet Explorer to Google Chrome.

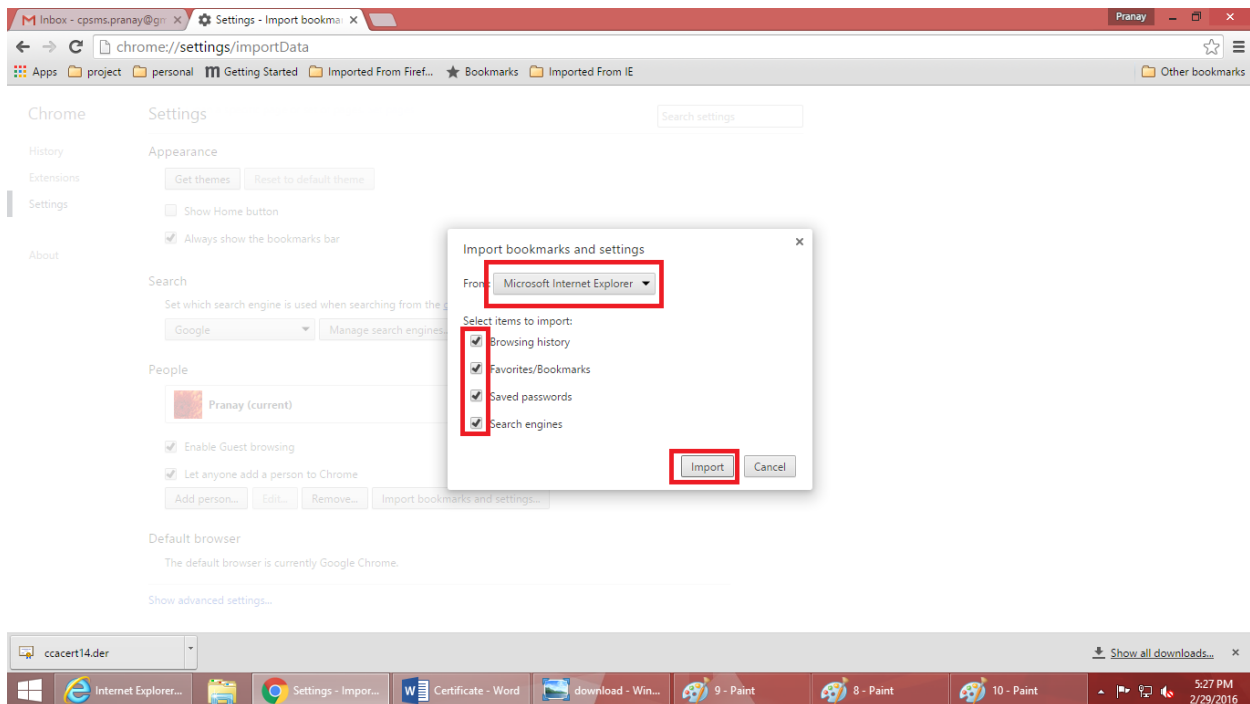


Figure 14: Certificate Imported in Google Chrome

## For Firefox Mozilla Browser

User shall perform configuration steps to enable the required certificate in Firefox Mozillabrowser.

### Pre-Requisite

- Certificate shall first be imported in Internet Explorer

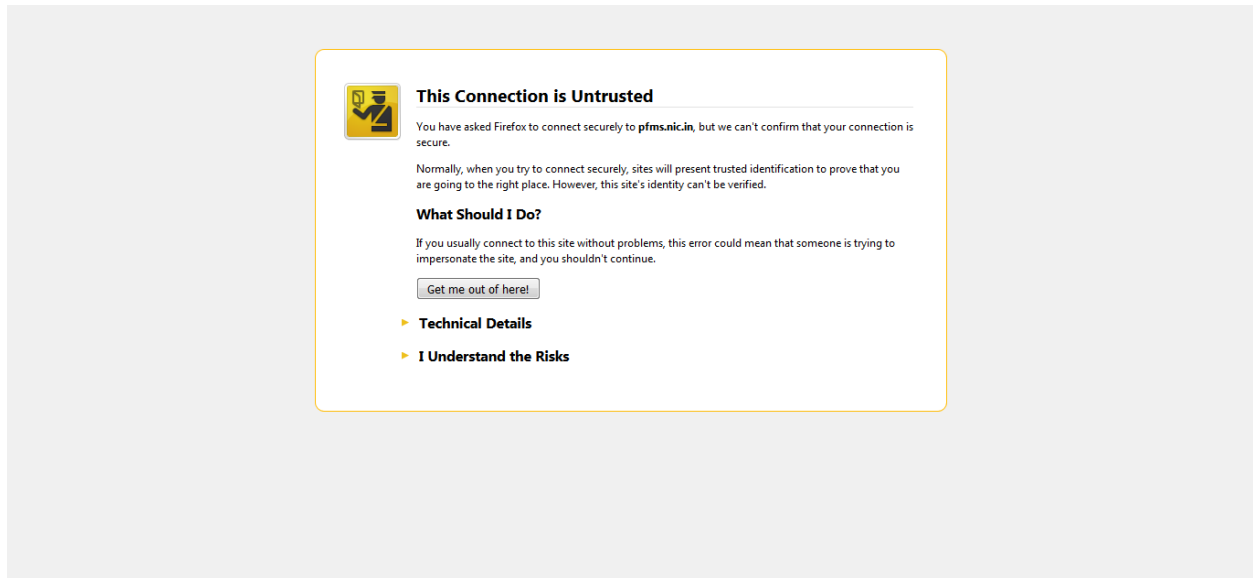


Figure 15: Firefox Mozilla

After importing the certificate in Internet Explorer browser as explained above, user shall click 'I Understand the Risks' link in Firefox Mozillabrowser.

Click 'Add Exception' button that appears after clicking 'I Understand the Risks' link.

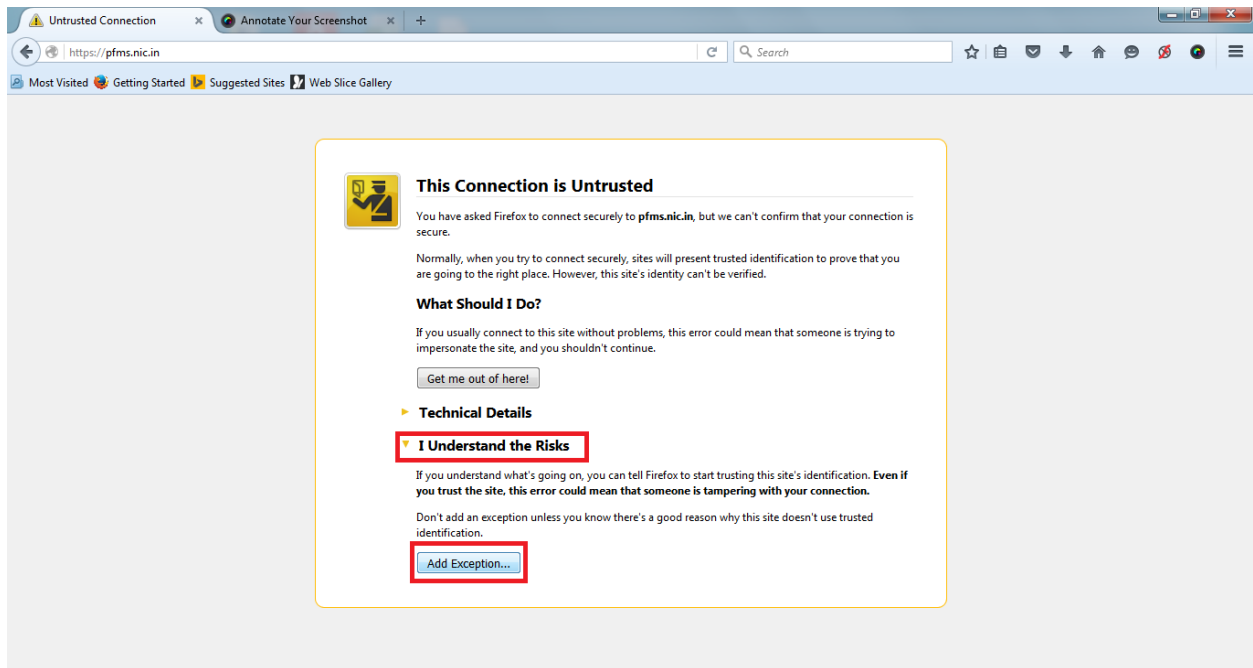


Figure 16:Add Exception

After clicking 'Add Exception' button, user shall be directed to Add Security Exception window.

At this screen, user shall click on 'Get Certificate' button.

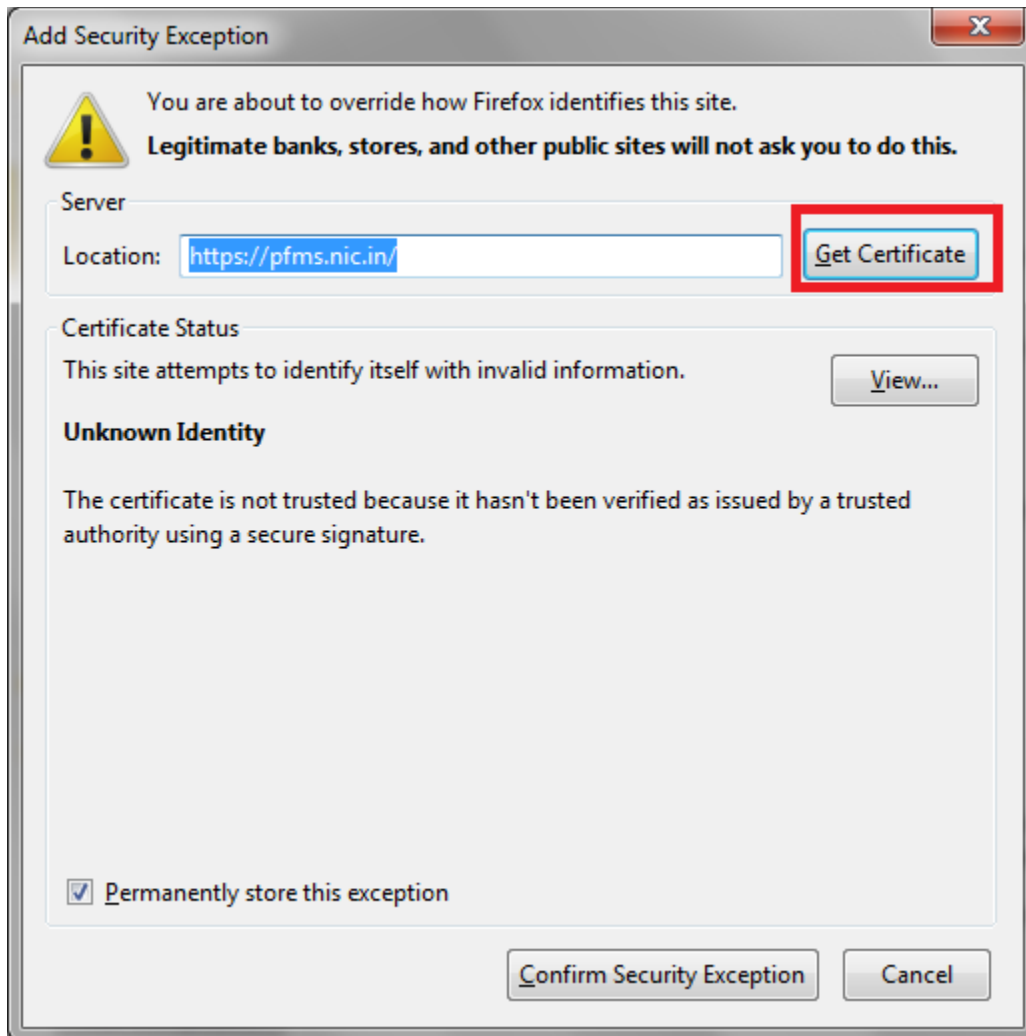


Figure 17: Get Certificate

Click the 'Confirm Security Exception' button at the bottom to successfully trust the required certificate.

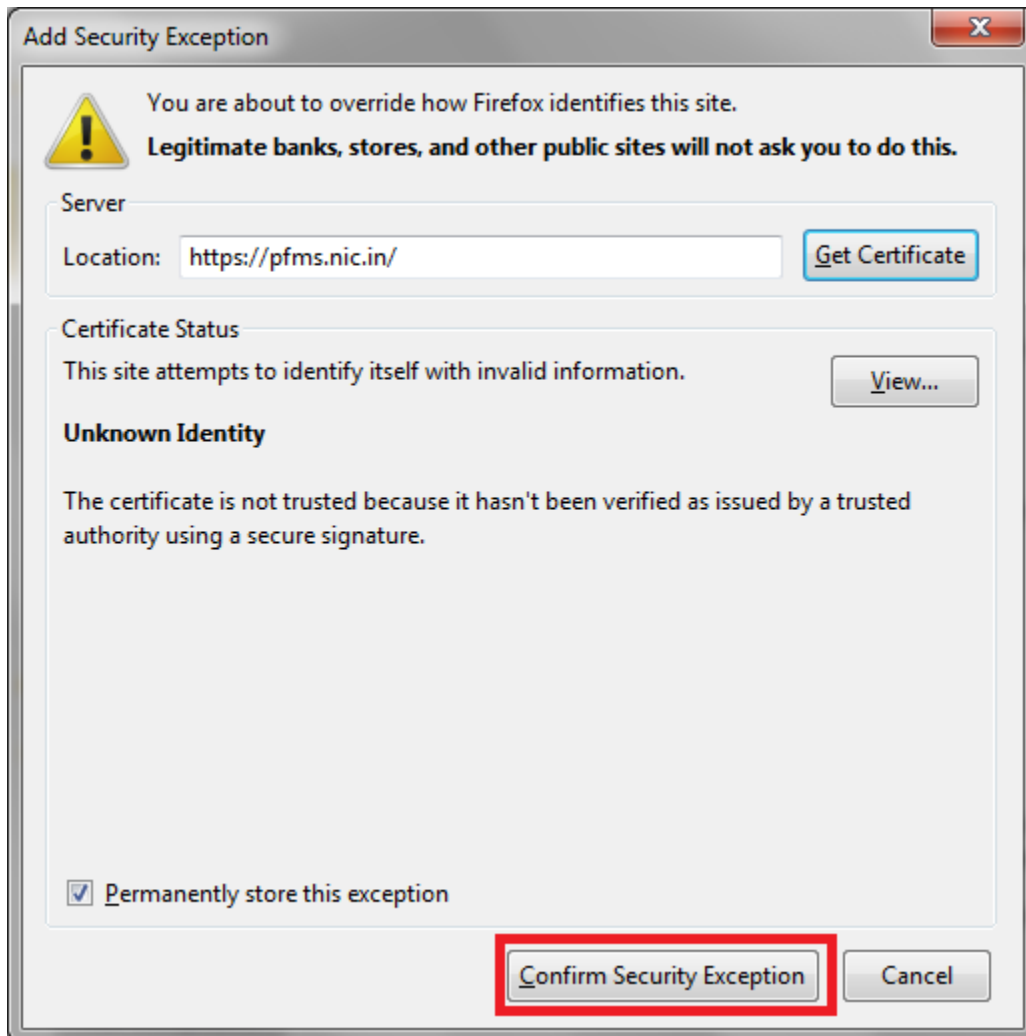


Figure 18: Certificate Imported Successfully