(n)Code Applet-less PKI component

Help Document

Applet-less PKI component Help document

Contents

Prerequisite

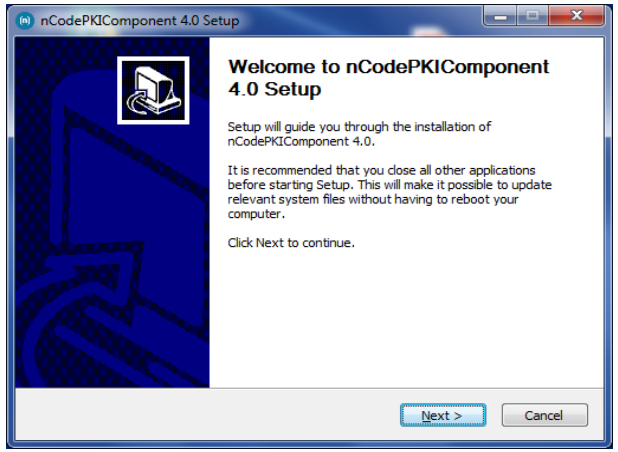
- Java 1.8
- **Local system administrator rights** are required.
  - Note: Do **not** use the "**Run as Administrator**" option.
  - The installation process should not prompt for any username or password.
- Token drivers must be installed on the system.

Steps to Download and install the setup.

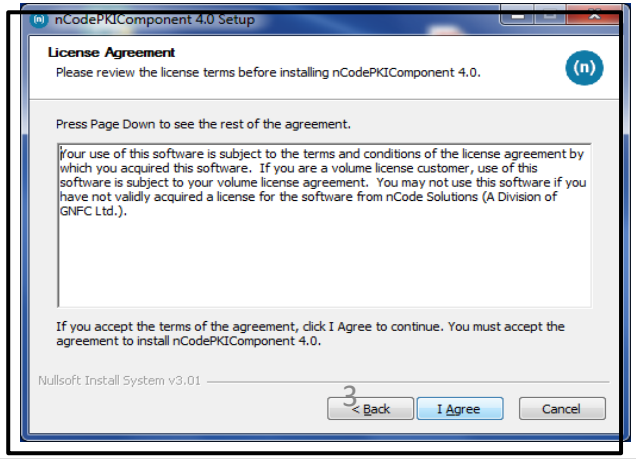
https://esalaryhry.nic.in/Documents/DownloadPKIComponent.zip

Component File Password – ncode@123

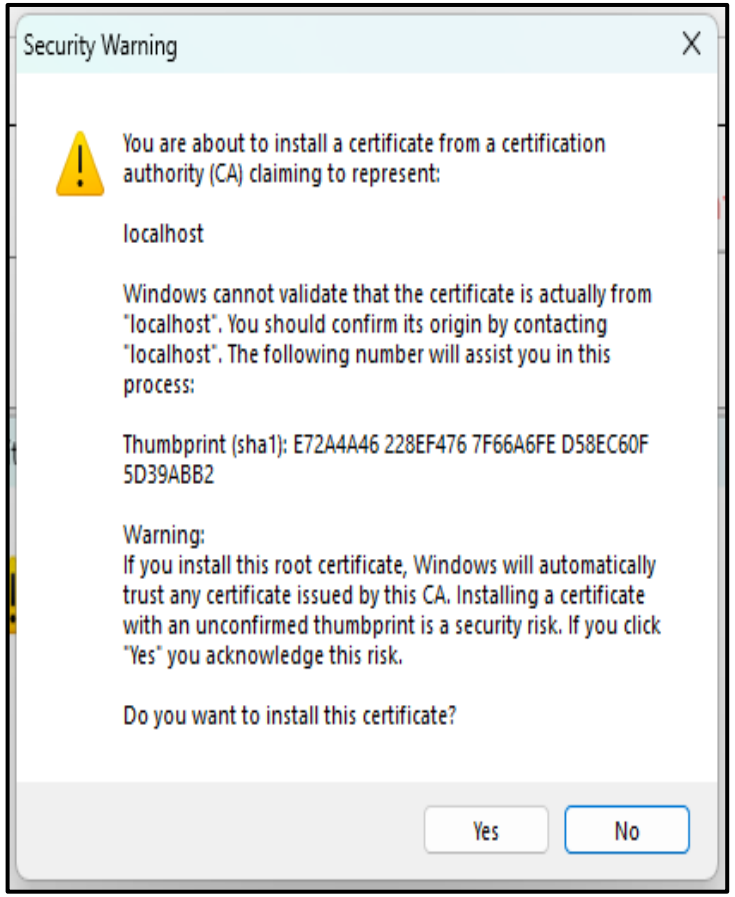
- Click on the '**nCodePKIComponent**' setup. A popup will appear as shown below.



- Click on next, Agree on terms and condition.

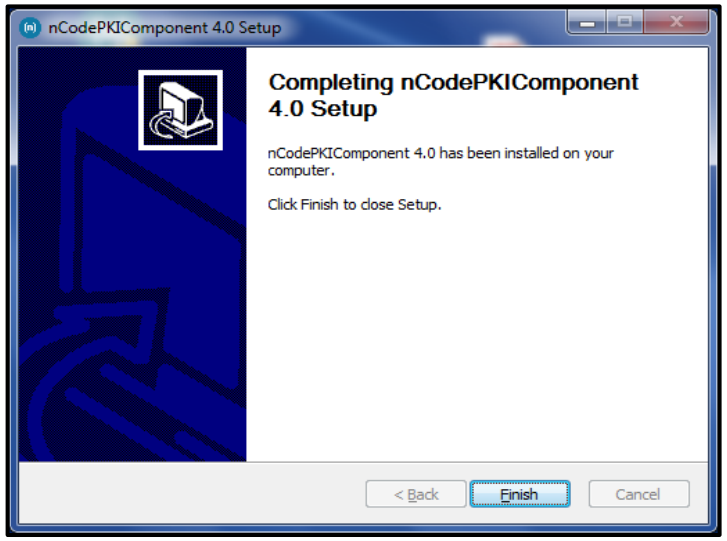


- If a prompt appears during the installation process, click **'Yes'** to proceed.



- Click 'Finish' to complete the installation.

- Click 'Finish' to complete the installation.



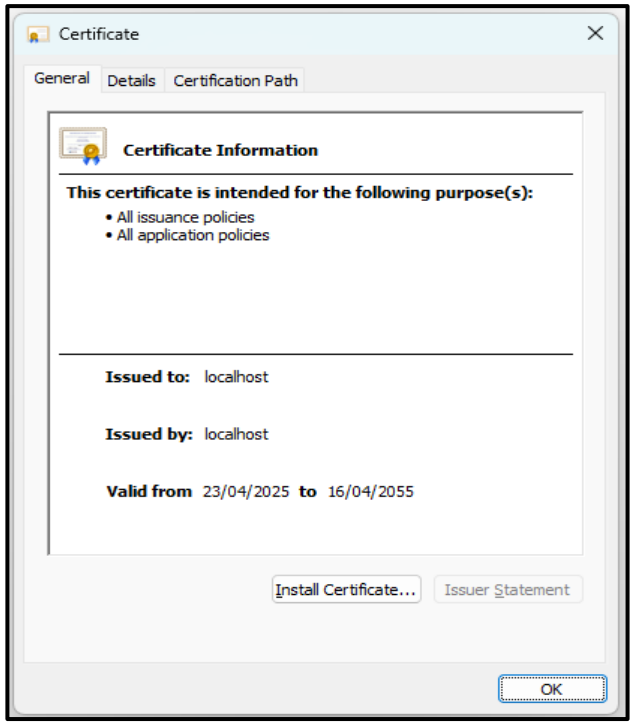
- After clicking the 'Finish' button, the Applet-less PKI component will run automatically, and its icon will appear in the system tray

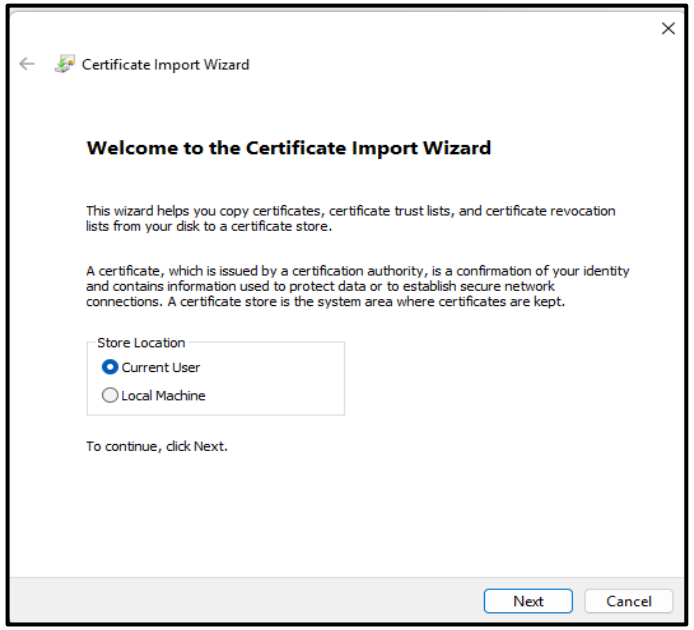
Steps to uninstall / re-install

- Go to Control Panel > Add or Remove Programs (or Programs and Features).
- Search for **nCodePKIComponent V4.0** in the list.
- Right-click on **nCodePKIComponent V4.0** and select Uninstall/Change. This will launch the uninstallation wizard.Follow wizard to uninstall **nCodePKIComponent V4.0**
- Follow the wizard steps to complete the uninstallation process.
- Reinstall **nCodePKIComponent V4.0** by running the setup file.

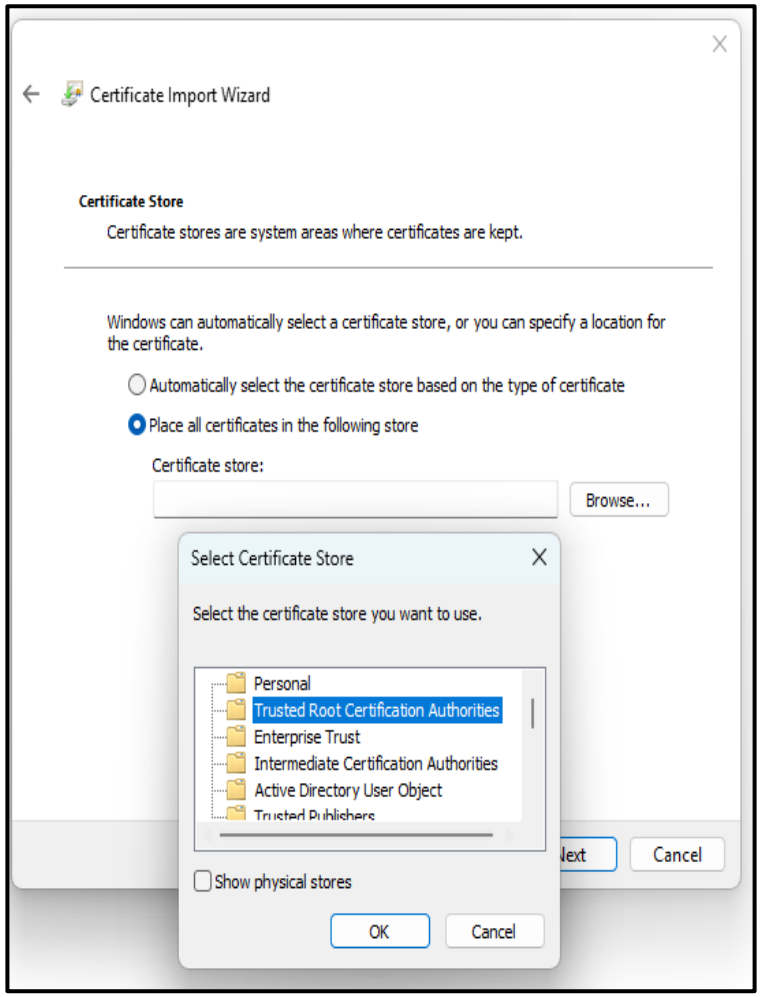
Import security certificate (if you are not able to use applet less PKI component)

- Download the localhost.crt file provided with this help document.Localhost.crt file
- **Download link:** http://103.20.104.57:8080/Download/JAVA/localhost2025.crt
- Close all browsers open in the system.
- Double click on downloaded file “localhost2025.crt”
    - Click on install certificate

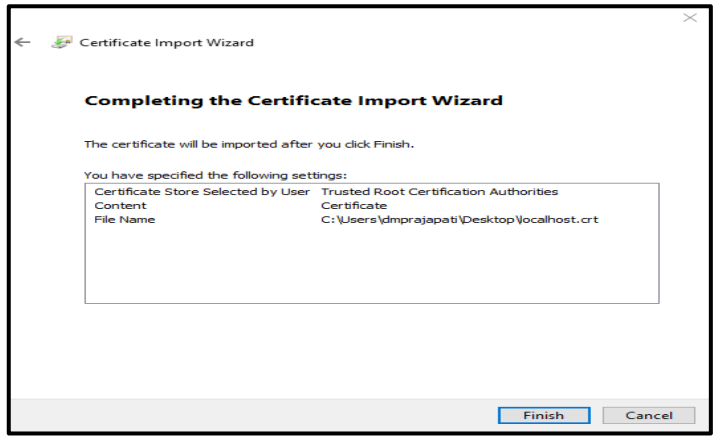




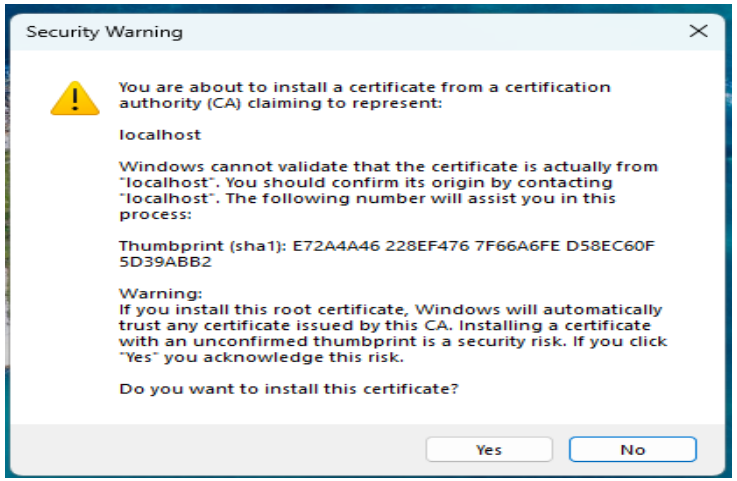
- Click next
- Select **"Place all certificates in the following store"**, then click **Browse**. A new window will open.
- In the new window, select **"Trusted Root Certification Authorities"** and click **OK** to close the window.
- Click **Next**, then click **Finish** to complete the certificate installation wizard.



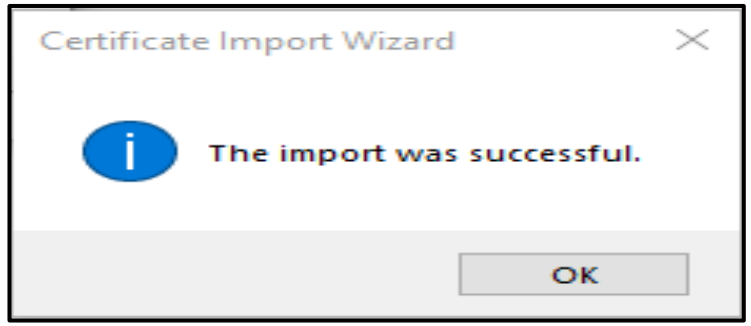
- Click Next to continue



- You will get one more dialog box as show below
  - Click on Yes

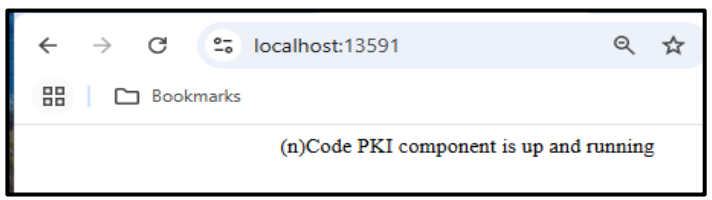


- Then click on Finish
  - After that you will get message " The import was successful"



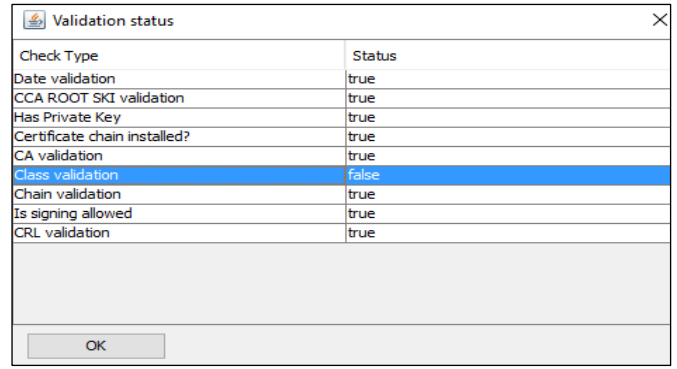
- Close all open windows

- Open Chrome web browser
  - Try to access the following URL https://localhost:13591/
  - **If you are getting the following message changes are applied successfully.**



PKI component validation error

PKI component validation status screen:



Date validation: false

- User is trying to use either expired certificate
- If Certificate is not expired
    - Request user to contact client support team to pass proper server date & time to solve issue
    - Some site has such kind of issue like DGFT etc.

CCA Root SKI Validation: false

- Certificate chain is not installed properly
    - Install certificate chain to solve issue
- CA is not whitelisted in PKI component
    - Request user to communicate site owner to get white listed CA in their component

Has Private Key: false

- Check user has attached token in system and it is accessible
- Check token has valid certificate with private key
- Check if user is not trying to use certificate without private key (installed .cer file or only certificate reference available in the certificate manager)

Certificate chain installed: false

- Check if certificate has valid certificate chain is installed or not
    - If not installed certificate chain and try again

CA validation: false

- Check if user it trying to user certificate issue by CA under CCA India
    - If Yes,
        - Request user to contact web site support team to white list CA in their component
    - If No,
        - User will not be able to use certificate as pki component supports CA under CCA India only

Class validation: false

- User is trying to use wrong class certificate in the web site.
- To allow certificate class please contact web site owner

OR

- New a new DSC with valid class details

Chain validation: false

- Check DSC has valid chain and installed
- If yes,
    - Request user to contact web site support team to whitelist certificate chain in their component
    - CA must be under CCA India
- If no,
    - Install certificate chain and try again to use certificate

Is Signing allowed: false

- User is trying to use encryption certificate for signing / verification process

Is Encryption allowed: false

- User is trying to use signing certificate for encryption / decryption process

CRL validation: false

- User is trying to user revoked certificate
- CRL URL is not reachable :
    - Check if CRL user is opening in the web browser
    - If Yes
        - Check if CRL URL is not blocked by any antivirus / firewall / proxy server
        - If URL is blocked, request user to allow URL to connect from Java application
        - Check Java console log to see any error while checking CRL (connection time out, any java error with CRL URL etc.)
    - If No,
        - Request user to communicate with certificate issuing ca to solve issue

Debugging Applet-less PKI component (Developer only)

- Go to the PKI component installation folder :
  - For 64-bit system
    - Close already running PKI component from the system tray (near system date & time)
    - C:\Program Files\nCodePKIComponent\
    - Search for **run_64.bat** file
    - Double client on **run_64.bat**
      - it will open a command prompt and PKI component in debug mode
  - For 32-bit system
    - Close already running PKI component from the system tray (near system date & time)
    - C:\Program Files\nCodePKIComponent\
    - Search for **run_32.bat** file
    - Double client on **run_32.bat**
      - it will open a command prompt and PKI component in debug mode
- You will see the PKI component logs in the command prompt
  - Copy-paste command prompt content in a text file and send it to us.
  - Note : do not share screen shot of command prompt

Root Certificate Installation Process

- **Installation of Additional Certificates for Existing Bit4id Dongle**
- For users with an existing **Bit4id dongle**, additional certificates must be installed on the DDO's local machine to ensure proper functioning of the DSC.

- **Certificates and Download Links of SignX CA :**
- 1. **Certificate Name:** CCAIndia2022

  Download Link: https://www.signxca.com/repository/aia/CCAIndia2022.cer
- 2. **Certificate Name:** SignX CA 2022

  Download Link: https://www.signxca.com/repository/aia/SignX%20CA%202022.cer
- 3. **Certificate Name:** SignX Sub-CA for Class 3 Organization 2022

  Download Link: https://www.signxca.com/repository/aia/SignX%20sub-CA%20for%20Class%203%20Organization%202022.cer

In case of existing DSC issued by Safe script (Sify) CA, root certificate can be download safe script CA.

Steps to Root Certificate installation

- 1. Download the required certificate files from the links provided above.
- 2. Double-click on each downloaded certificate file (.cer).
- 3. Click on **“Install Certificate”**.
- 4. Select **“Local Machine”** (if prompted) and click **Next**.
- 5. Choose **“Place all certificates in the following store”**.
- 6. Click on **“Browse”** and select:

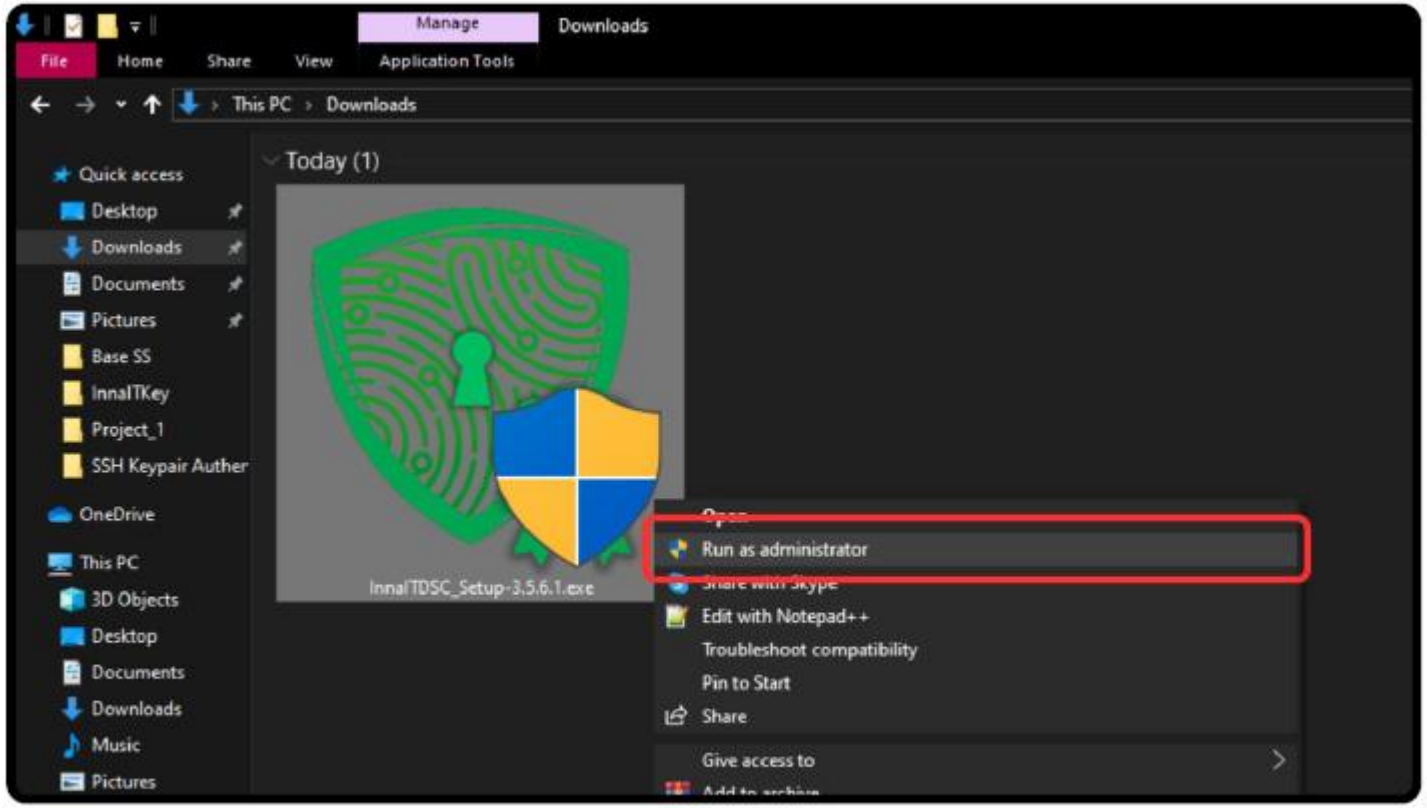
- **Trusted Root Certification Authorities**
- 7. Click **OK**, then **Next**, and finally **Finish**.
- 8. A confirmation message will appear stating that the certificate has been successfully installed.

InnaIT Key Token Driver Installation

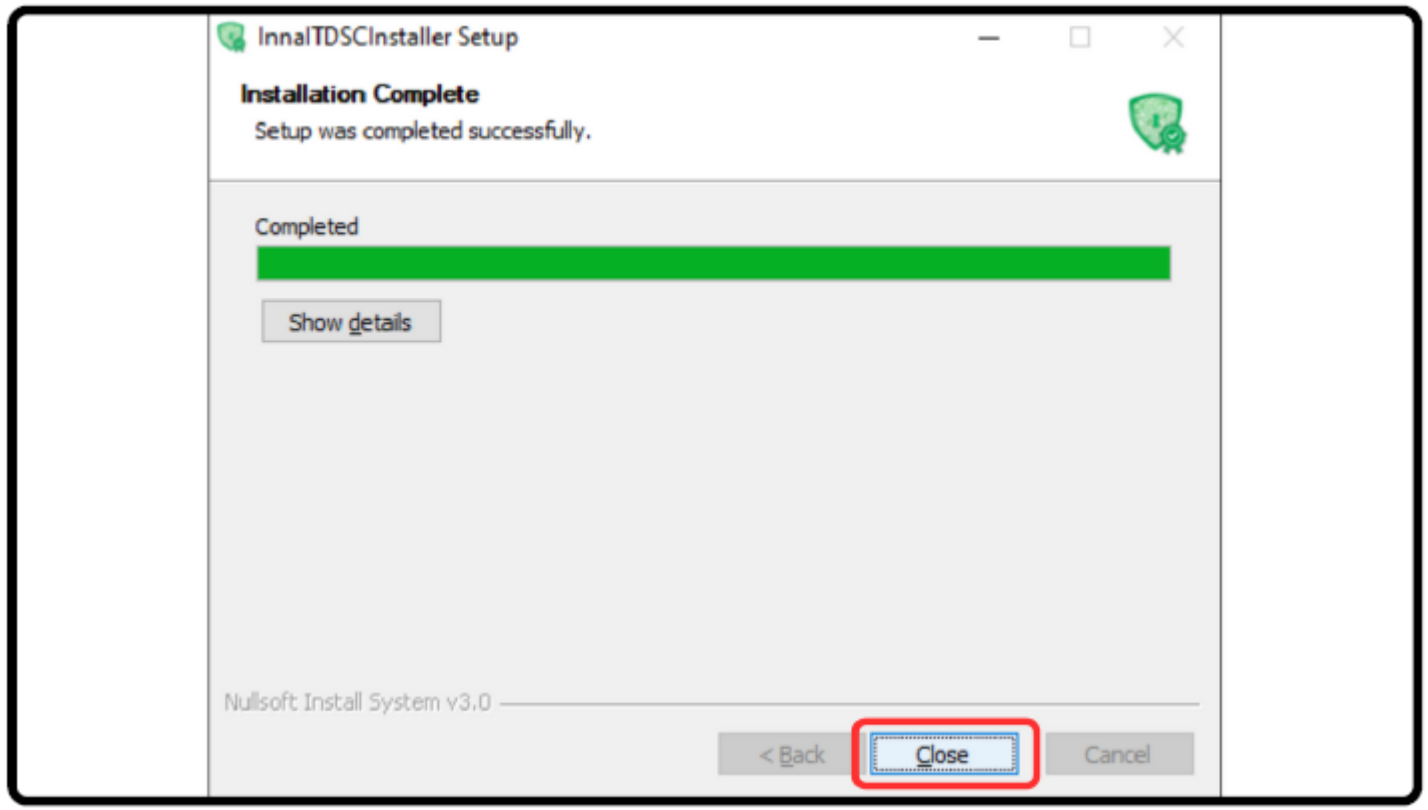
For DSC Dongle issued by GNFC LTD.

InnaIT dongle installation Steps to Download and install the setup.

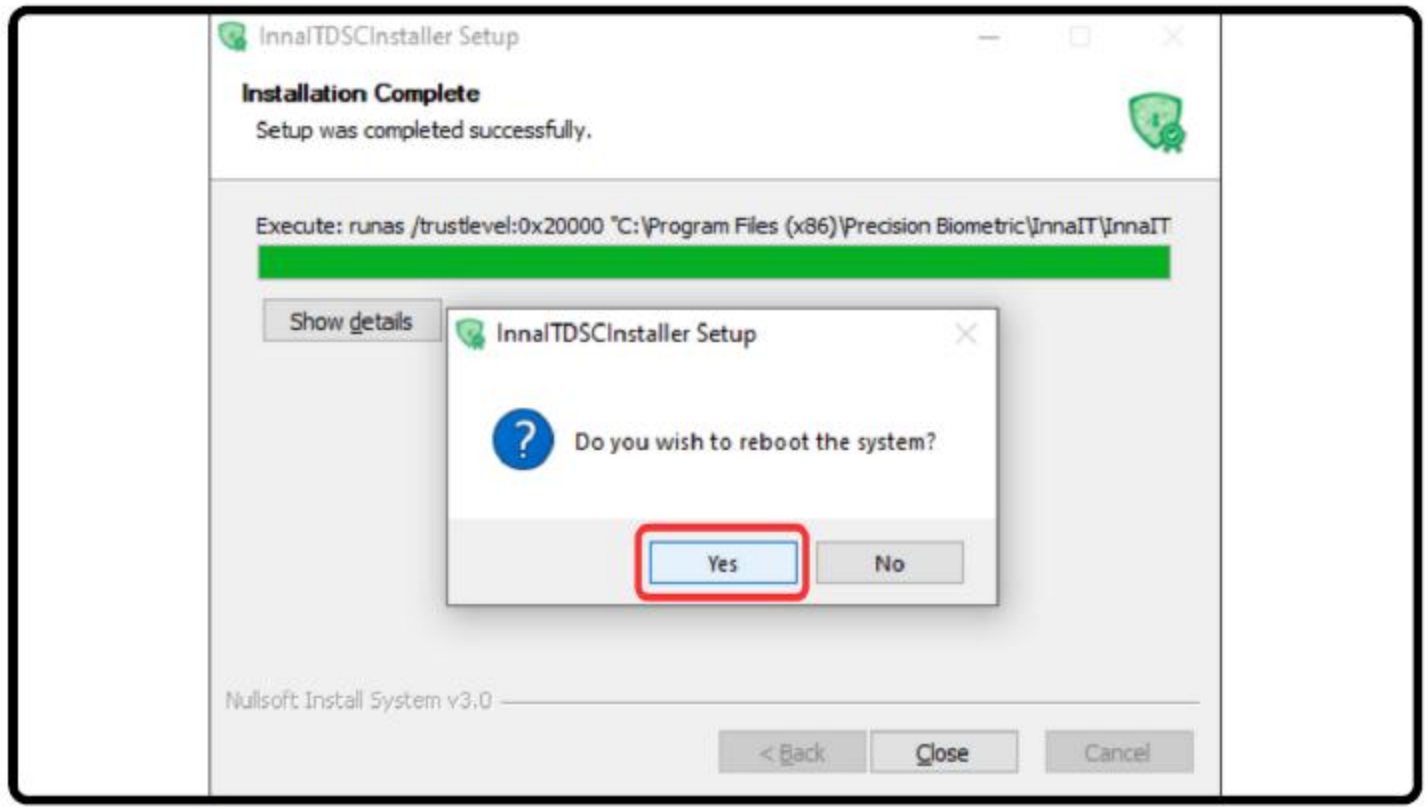
https://www.ncodesolutions.com/drivers/InnaITDSC_Setup_New.zip



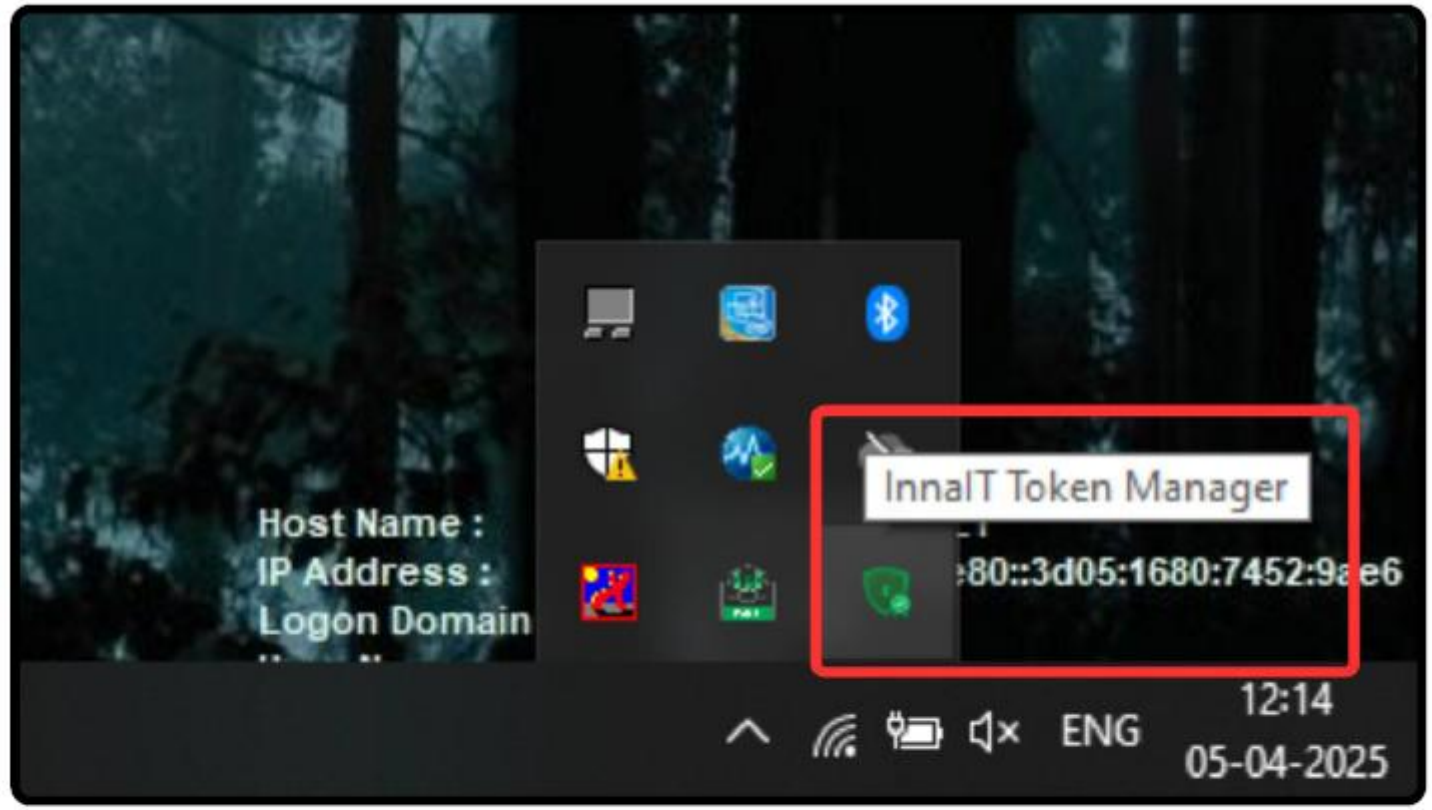
Step 5 – Right-click on the application and choose the “Run as administrator” option.



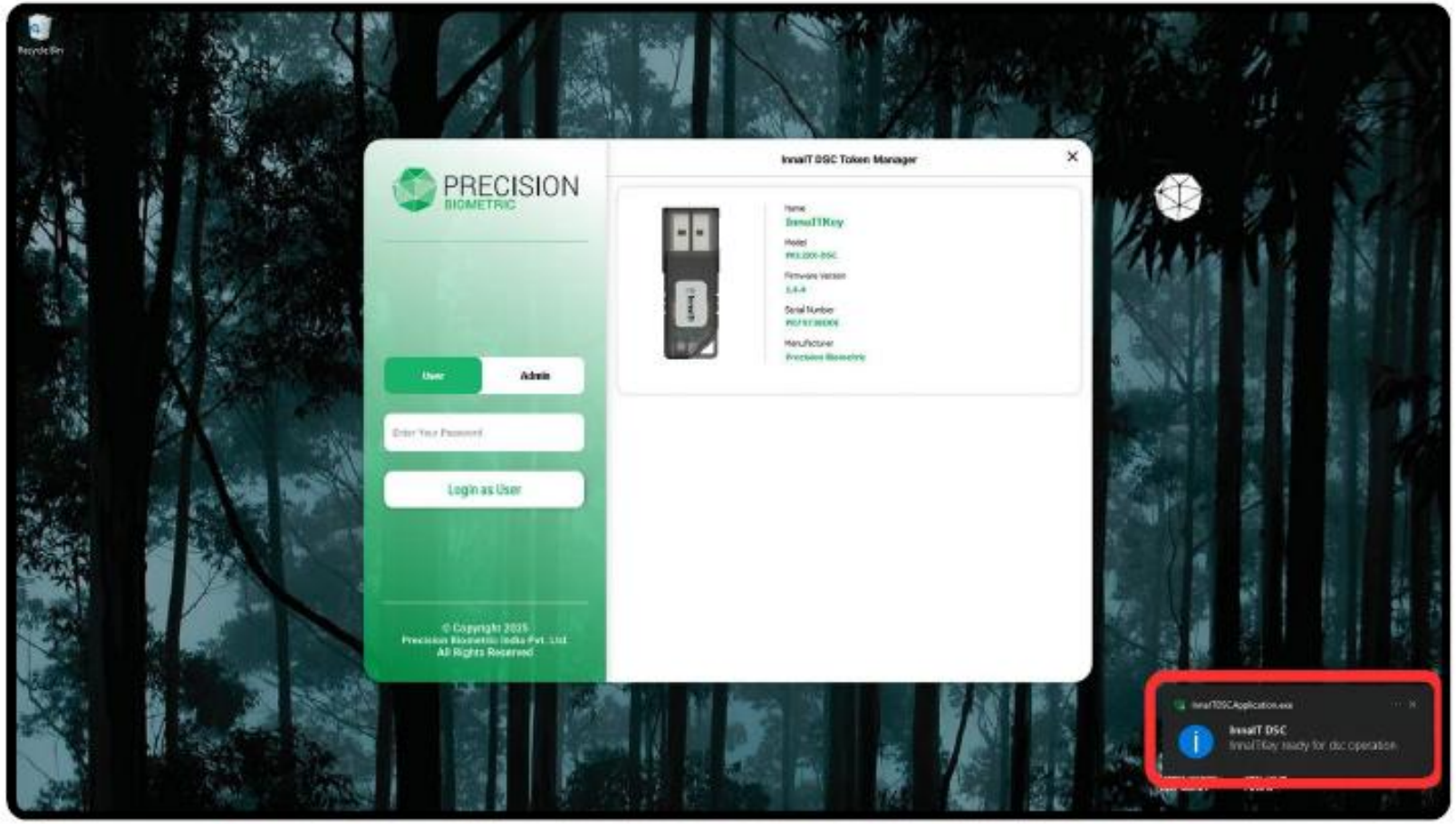
Step 6 – After the installation is complete, click on “Close”.



Step 7 – You will now be asked to reboot your PC. Click on “Yes” to do so.



Info – After the restart is complete, you can start using the InnaIT DSC Token Manager. You can find the icon to open the application in the system tray.



Info – You will get a notification on the bottom right which says “InnaITKey is ready for DSC Operation” once the token is detected. The token’s details will also appear in the application window.

Bit4id Token Driver Link

- **The existing bit4id dongle, latest software should be downloaded from bit4id portal and installed on the local machine for bit4id dongles:**
- **https://b4sc.net/dl/x_kgV6o3oiTq6Qw3**
- **https://b4sc.net/dl/RNPoTQpAGkm48wEQ**

Note -

- **The INNAIT precision dongle set-up should not be installed for BIT4ID dongles.**

Dongle Registration in Treasury

- The **Treasury Office** will register the Digital Signing Dongles of DDOs.

1. Insert the dongle in USB port.
2. Treasury admin logs in to the OTIS portal using a valid **User ID (dtotaa..)**
   and Password.
3. Navigate to the following menu:
   Other Tasks → Register Digital Signing Dongle for DDOs
4. Select the respective DDO and complete the dongle registration process.

- Without registration, the user will not be able to sign the document, and “no DSC Found” message will be displayed in the DSC selection dialog box..