This file has been cleaned of potential threats.

If you confirm that the file is coming from a trusted source, you can send the following SHA-256 hash value to your admin for the original file.

183b85a7ab62a49e3332d864e4f0b7e793275b4e355e460c53f7d16a2bb9f213

To view the reconstructed contents, please SCROLL DOWN to next page.

GNFC

(n)Code® Solutions

License Certifying Authority

(n)Code Signer utility for ICEGATE Help Document

(n)Code Solutions

Restricted Usage: The information contained herein is strictly confidential, privileged and meant solely for the reference of ICEGATE Software team and may not be altered in any way, published, transmitted to, copied or redistributed, in part or in whole, to any other person or to the media or reproduced in any form, without prior written consent of GNFC Limited.

Table of Content

1 REQUIREMENT 3
1.1 MINIMUM REQUIREMENT 3
2 STEPS TO INSTALL THE SETUP 3
3 STEPS TO UNINSTALL / RE-INSTALL 5
4 WEB BROWSER SETTING 5
5 PKI COMPONENT IS NOT GETTING CALLED 6
6 JAVA VERSION ISSUE 6
7 PKI COMPONENT NOT SHOWING CERTIFICATE 7
8 TAKING LONGER TIME AFTER CERTIFICATE SELECTION 7
9 PKI COMPONENT VALIDATION ERROR 8
9.1 DATE VALIDATION: FALSE 8
9.2 CCA ROOT SKI VALIDATION: FALSE 8
9.3 HAS PRIVATE KEY: FALSE 8
9.4 CERTIFICATE CHAIN INSTALLED: FALSE 9
9.5 CA VALIDATION: FALSE 9
9.6 CLASS VALIDATION: FALSE 9
9.7 CHAIN VALIDATION: FALSE 9
9.8 IS SIGNING ALLOWED: FALSE 10
9.9 IS ENCRYPTION ALLOWED: FALSE 10
9.10 CRL VALIDATION: FALSE 10
10 NOT ABLE TO DECRYPT DATA (ENCRYPTION WORKING PROPERLY) 10
11 NOT ABLE TO CONNECT PKI COMPONENT AFTER INSTALLATION 11
12 SUPPORT 11
13 SALES 11

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

1 Requirement

1.1 Minimum requirement

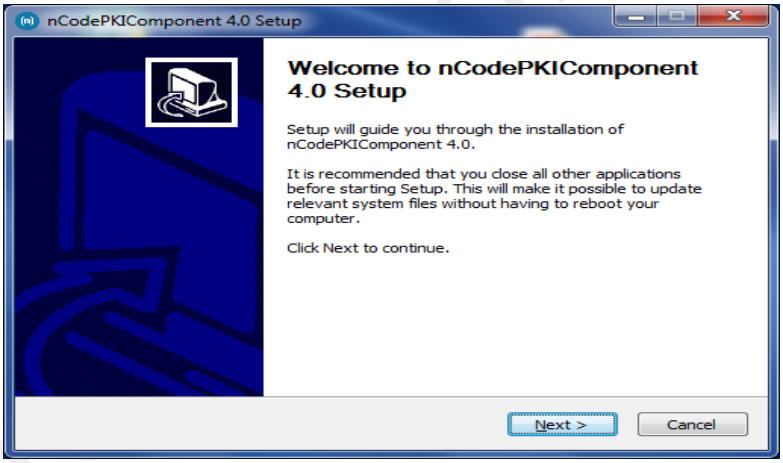
- Java 1.8 (32 bit / 64 bit)
- Read write permission
- Admin rights
  - User must be able to change system setting, install software etc.
- Windows 7, 8, 8.1, 10.

Note:

- Do **not** run setup as "run as administrator".
- If PKI component setup size is less than **100 MB** please download & install Java and install manually

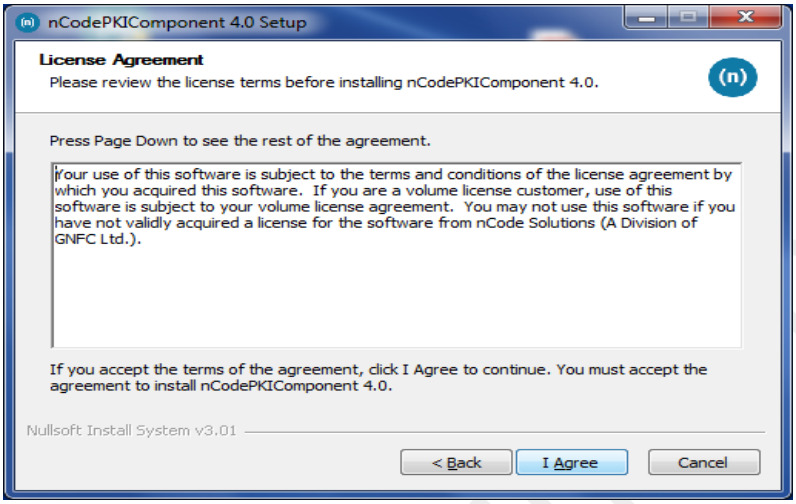
2 Steps to install the setup

- Click on (n)Code PKI Component setup, popup will be shown as below.

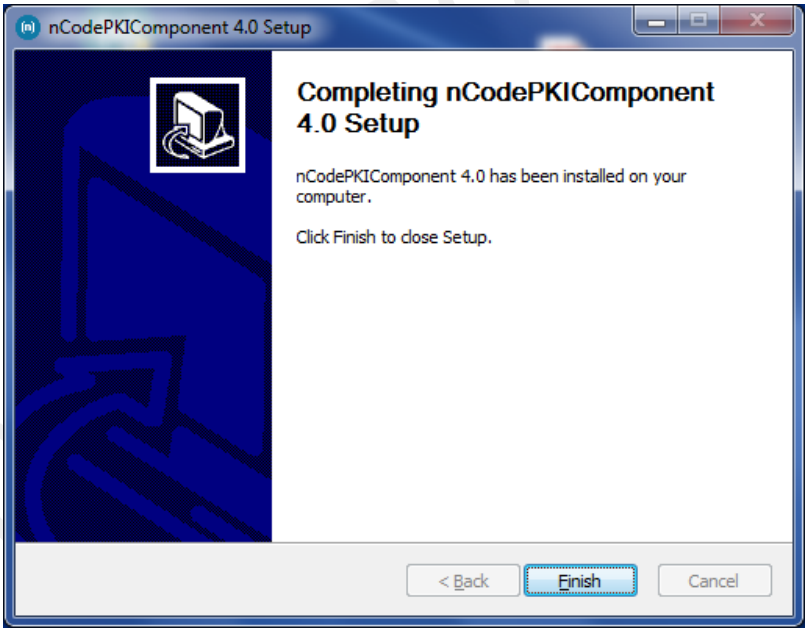


Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

- Click on next, Agree on terms and condition.

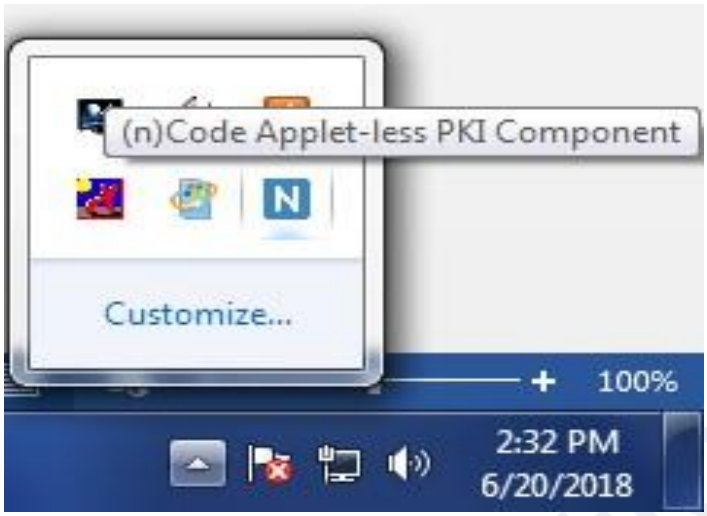


- Click on finish.



After you click the finish button Applet-less pki component will run automatically and you will get icon in the system try

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.



3 Steps to uninstall / re-install

- Go to **control panel** >> **add / remove program** >> search for **nCodePKIComponent**
- Right click on **nCodePKIComponent** and
- Select **uninstall / change** which will open a wizard
- Follow wizard to uninstall **nCodePKIComponent**
- Right click on **Remove_OLD_Settings.bat** (which you have already downloaded with installer) and **run as administrator** to remove configuration if any remaining.

Or

- Please remove PKI component installed folder manually
- Install **nCodePKIComponent** using setup to use it once again

4 Web Browser setting

- **Firefox** – Go to URL https://localhost:13591 and add security exception to allow connections.
  - If connection error still comes, Go to URL **about:config** and set value for **security.mixed_content.block_active_content** to **false** and **security.mixed_content.block_display_content** to **true.**

- **Google Chrome**
  - Go to URL **chrome://flags/#allow-insecure-localhost** and click on **Enable** and restart Chrome to allow connections.
  - Go to URL https://localhost:13591 and add certificate to **Trusted Root Certification Authorities** if certificate error comes.

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

- if pki component is running and still getting error please set value for edge ://flags/#block-insecure-private-network-requests
  - from : **default** to : **disabled**

- **Internet explorer**
  - IE 11 and above - Go to URL https://localhost:13591 and add certificate to **Trusted Root Certification Authorities** if certificate error comes.
- **Microsoft Edge**
  - if pki component is running and still getting error please set value for edge ://flags/#block-insecure-private-network-requests from : **default** to : **disabled**

5 PKI component is not getting called

- Check if following URL is opening in web browser
  - **http://localhost:12951 or https://localhost:13951**
  - If URL is opening
    - Open developer console In the web browser and run pki component from command prompt then request user to perform operation
      - Check Request is received in PKI component or not
      - If request is not received, please check web browser console for java script error also check network tab to check if use application is trying to connect with PKI component or not
      - if any antivirus or firewall is blocking application request, request user to disable & try again to use pki component
  - if URL is not opening
    - Please check pki component is installed properly or not
    - Check for pki component ICON in system tray
    - Try to run pki component from command line (java –jar ncodePKiCompoentV4.jar)
    - Check multiple versions are not running in the system

6 Java version Issue

Currently Java version **1.8.x** is supported for PKI component (recommended to use latest version).

Any other version other than java 1.8 is not supported

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

Note:

- For updating Java version download the latest installed from java.com and install.
- It is not recommended perform auto update.
- PKI component will not work as expected, if multiple JAVA version is installed and running on the system.

Please un-install all older java version and keep only one latest java version only.

7 PKI component not showing certificate

- Check Antivirus or any web browser plugin is not blocking PKI component
- Check user has valid certificate in the dongle
- Check certificate is properly mapped with application
- Check if user has attached proper dongle to system with valid certificate
- Check if any other ca issued certificates are not creating issue with component

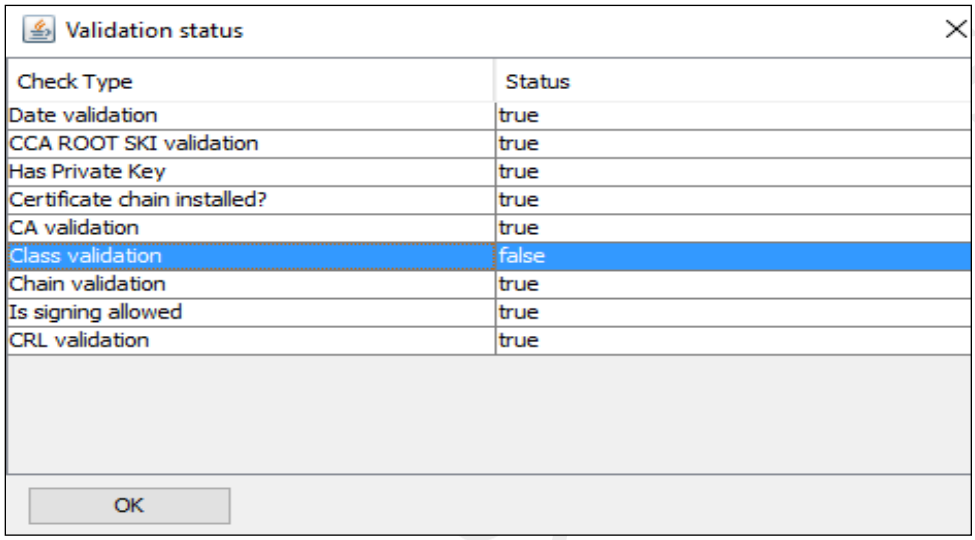
8 Taking longer time after certificate selection

- CRL URL will be available in the certificate details , check CRL is opening in web browser or not
- If not opening
    - Check any antivirus, firewall or proxy server is not blocking CRL URL
    - Check if internet is working properly
    - Check Java console log to see error like connection time out etc.
- If opening check the time taken to download the CRL file
    - If CRL file size is big then CRL checking time will be high for example 2 ~3 MB

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

9 PKI component validation error

PKI component validation status screen:



9.1 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.

9.2 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

9.3 Has Private Key: false

- Check user has attached token in system and it is accessible

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

- 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)

9.4 Certificate chain installed: false

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

9.5 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

9.6 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

9.7 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

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

- If no,
    - Install certificate chain and try again to use certificate

9.8 Is Signing allowed: false

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

9.9 Is Encryption allowed: false

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

9.10 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

10 Not able to decrypt data (encryption working properly)

- Check user is using certificate with private key
- Private key is not corrupted
- Certificate is not expired
- Check Java console log for any error

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.

11 Not able to connect pki component after installation

- Make sure PKI component installed without run as administrator or entering any credential
- Close pki component using exit option in system tray
- run : installCert.bat as administrator (available in the pki component installation folder)
- run_32.bat or run_64.bat as per installation (available in the pki component installation folder)
- Check if user is able to use pki component using the website
- If the issue still persists, then restart the system after performing above steps.

12 Support

- 1800 301 1000
- (10:00 AM to 6:00 PM on working days)
- icegate.helpdesk@icegate.gov.in

13 Sales

- 079-66743309
- (9:30 AM to 5:30 PM on working days)
- pkisales@ncode.in;
- pkisupport@ncode.in

Restricted Usage: No part of this material may be copied or duplicated or redistributed without prior written consent from GNFC Limited.