Digital Signing Service

User Manual

Version 1.0.0

Employees' Provident Fund Organisation, India

Ministry of Labour & Employment, Government of India

CONTENTS

1. APPLICATION OVERVIEW

The new Digital Signing solution is a browser independent digital signing solution. It is a one-time installation. It is deployed on local client PC and allows for signing using DSC token on EPFO's Employer interface of Unified Portal. The facility is currently enabled only for approval of Joint Declaration form for **Pension on Higher Wages** to be digitally signed by employer.

2. HARDWARE & SOFTWARE PRE-REQUISITES

Operating System	
Windows 11 Pro	64-bit operating system, x64-based processor
Windows 10 Pro	64-bit operating system, x64-based processor
Windows 8.1 Pro	64-bit operating system, x64-based processor

Client's Machine Requirement	
Port	60015
Browser(s)	• Mozilla Firefox • Google Chrome • Microsoft Edge

3. DOWNLOAD

The download facility is available inside the login of Employer interface of Unified Portal, wherever the Digital Signing service based digital signing has been enabled the link to download the same will be provided on the respective screens.

Download the utility (EPFO_DSC_Signer_1.0.0.exe) from the link provided in Unified Portal only.

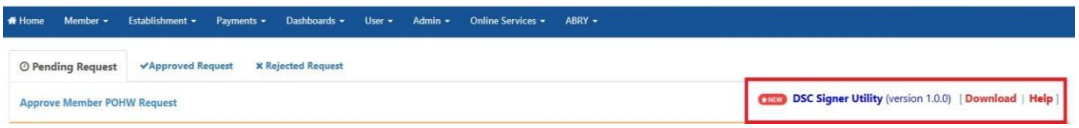

Fig. 3.1

Save the downloaded file from downloads section to a secure location

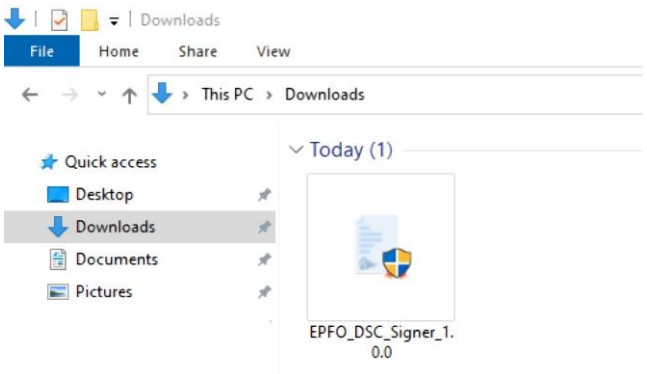

Fig 3.2

Note: *This installable is to be downloaded only once or only when there is a change in version due to upgrades.*

4. INSTALLATION

The Digital Signing Service utility has to be one time downloaded and installed on the client machine from which the Digital Signing is to be performed for facilities provided in the Unified Portal application for EPFO.

4.1. Double click on the downloaded executable file to initiate the installation process. The digital signer Service setup wizard will be displayed, click on <**Next**> to continue.

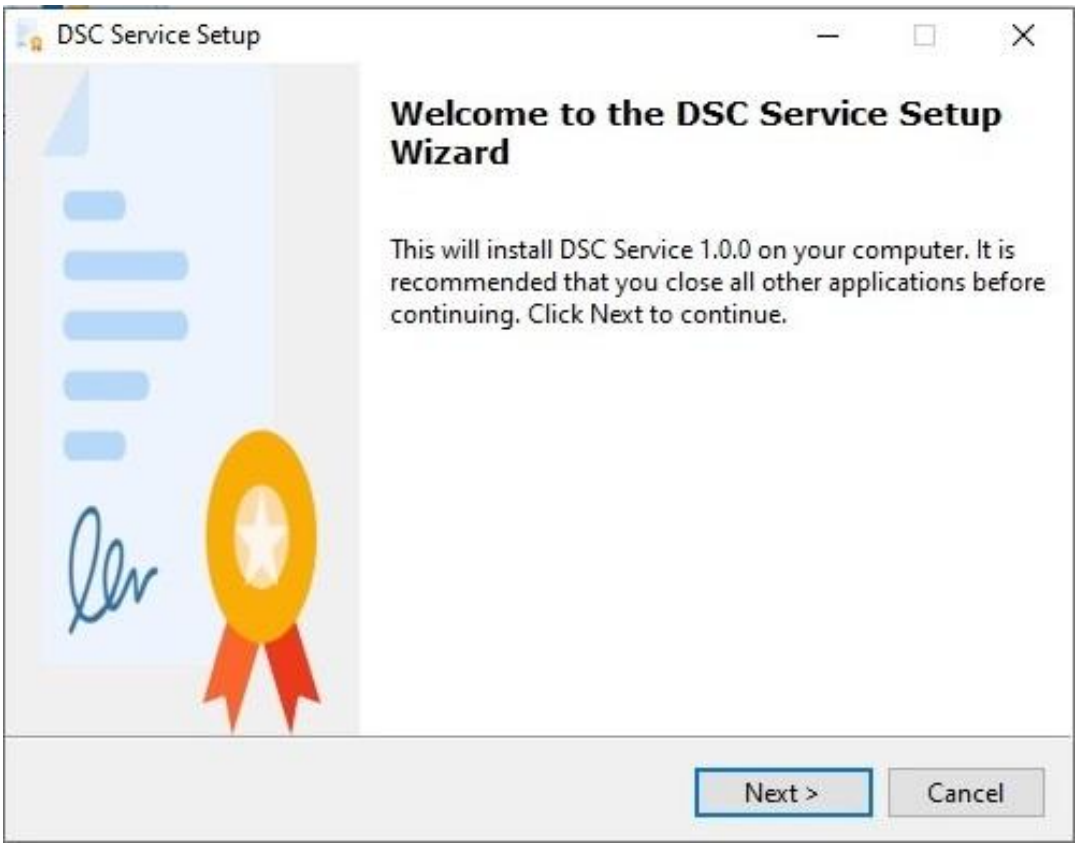

Fig. 4.1

4.2. On some PCs below warning may be shown. Click on <**More info**>

Fig. 4.2

4.3. Click on <**Run anyway**> to continue with the installation process

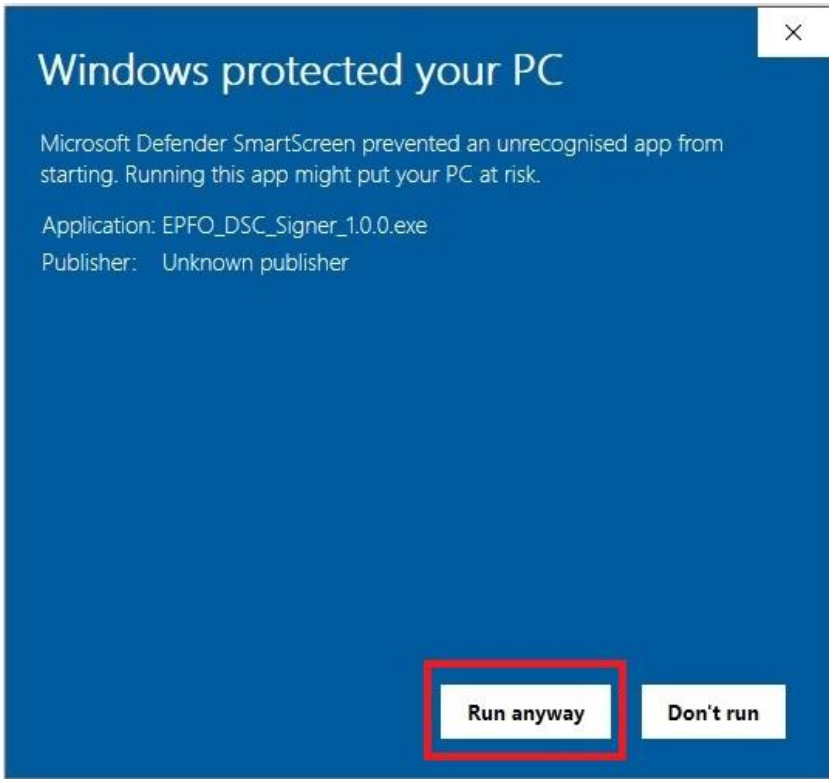

Fig. 4.3

4.4. To proceed further you will have to agree and accept the terms and condition by selecting the I accept the agreement and then click on <**Next**>.

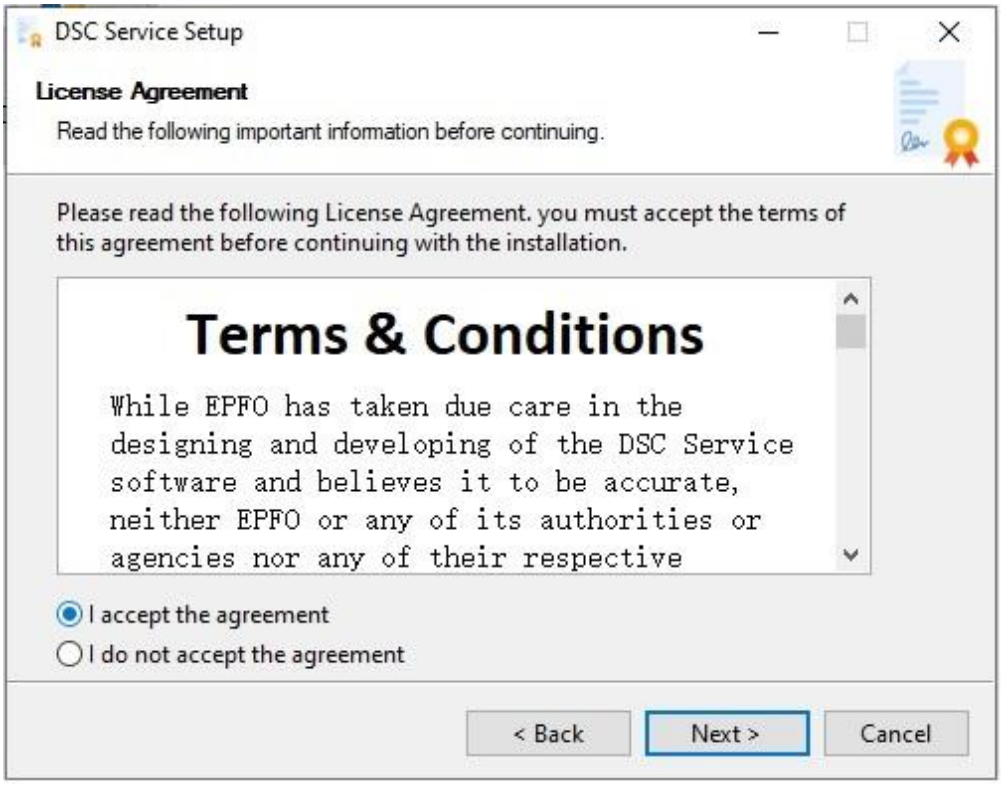

Fig. 4.4

4.5. Select the directory for installation and click on <**Next**>.

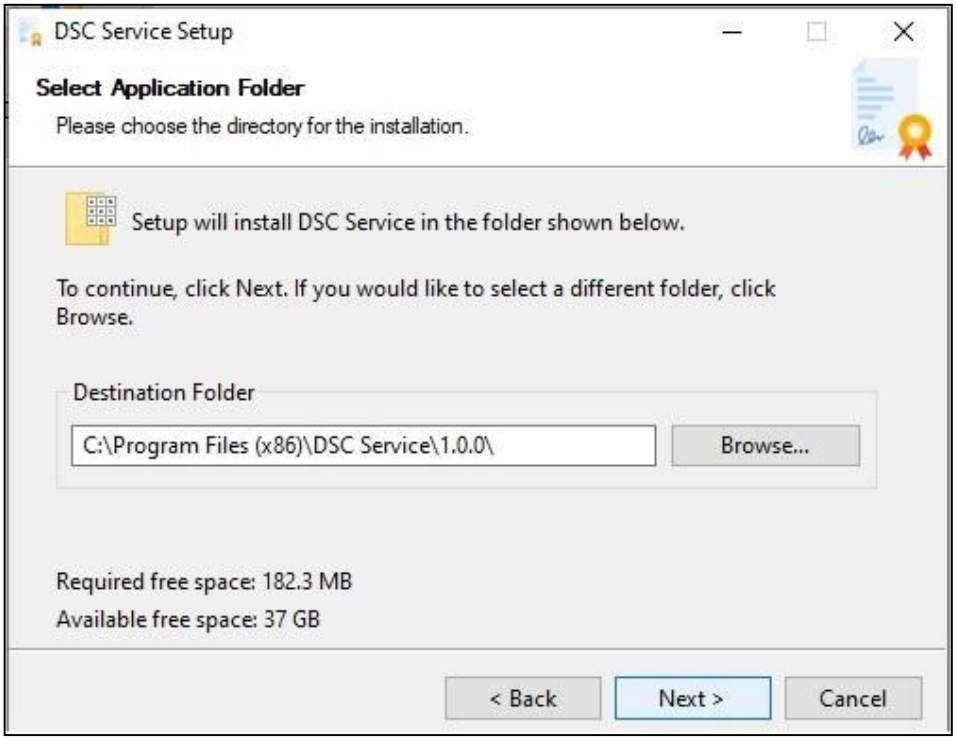

Fig. 4.5

4.6. To create a desktop icon and include the service in start menu click <**Next**>. It is recommended.

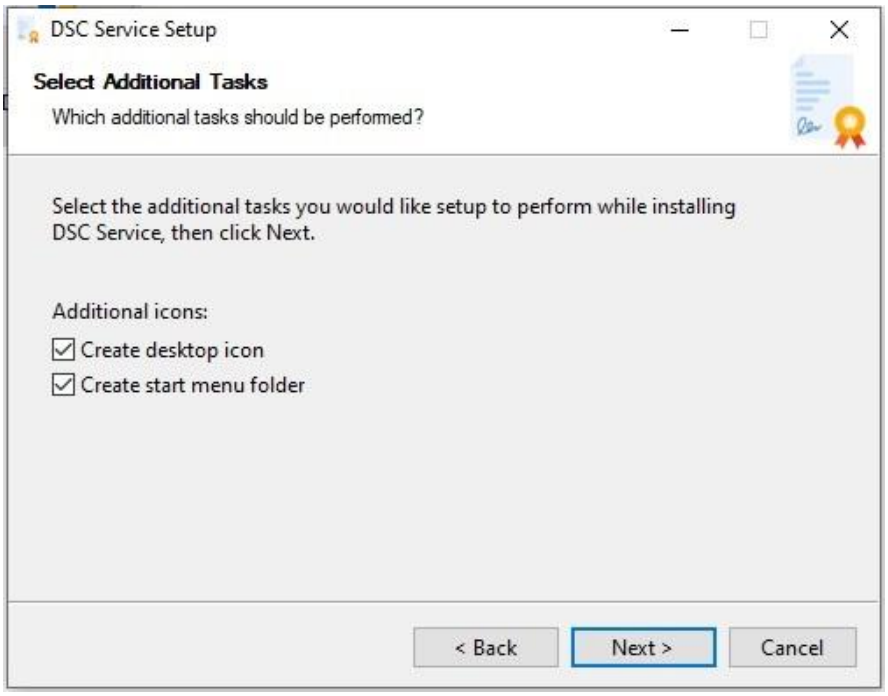

Fig. 4.6

4.7. Select the folder for start menu shortcut.

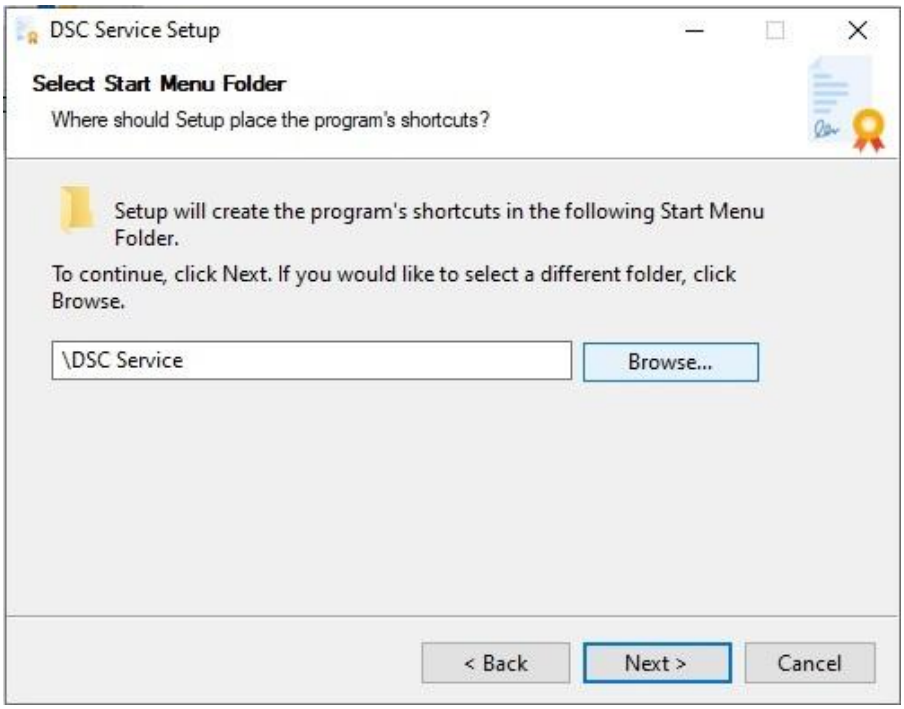

Fig. 4.7

4.8. The application will start installing on your system.

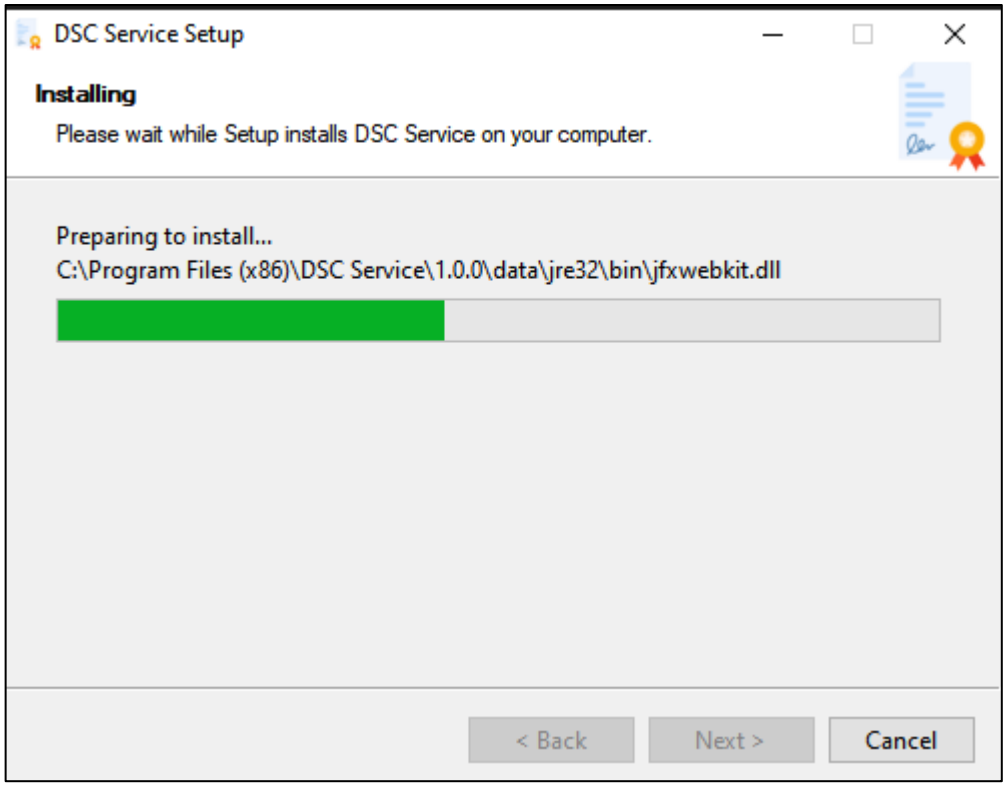

Fig. 4.8

Note: *If any warning related to for **dscCA2023** certificate is encountered please allow it to continue with the installation.*

4.9. Click on Finish to end the setup wizard. Icon for DSC utility will be created on desktop and start menu.

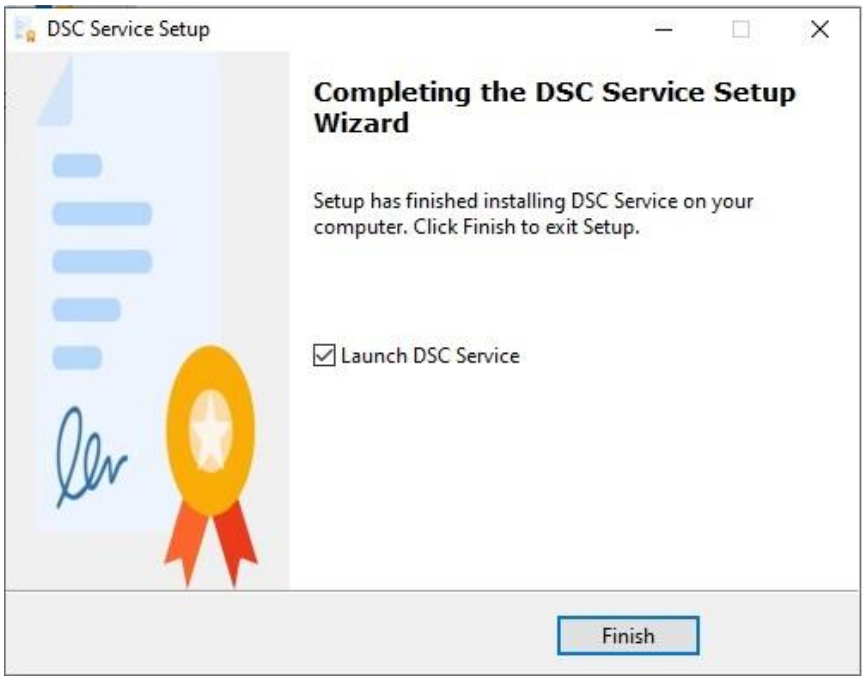

Fig. 4.9

4.10. Double click on DSC Service icon to run the signing service. Now you are ready to sign.

5. BROWSER

Check whether the certificate is already imported into your browser post installation. To verify the same please follow the below process.

5.1. MOZILLA FIREFOX

5.1.1. Go to Mozilla Firefox browser settings.
5.1.2. Click on <**Privacy & Security**> option.
5.1.3. Click on <**View Certificates**> button.

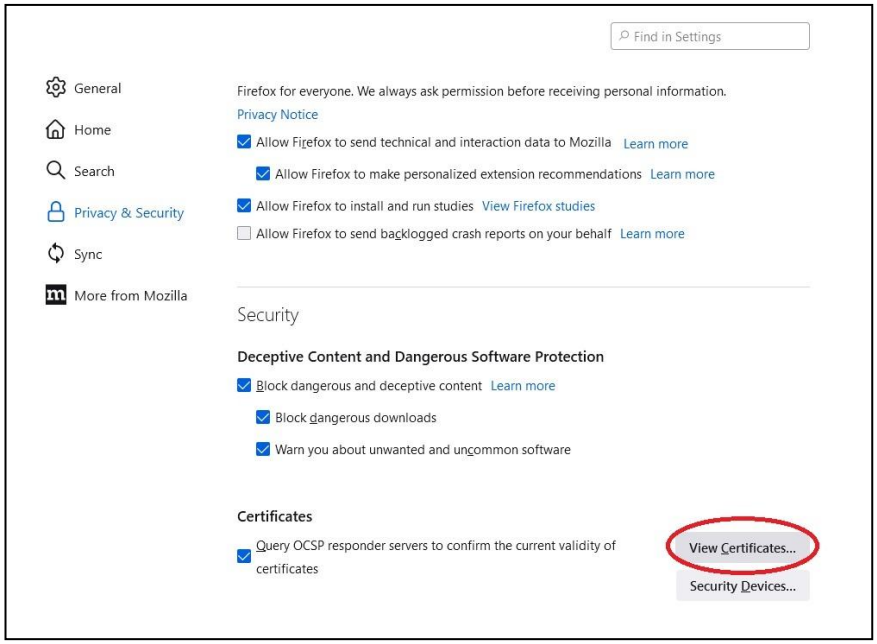

Fig. 5.3

5.1.4. Click on <**Import**> to import DSC certificate.

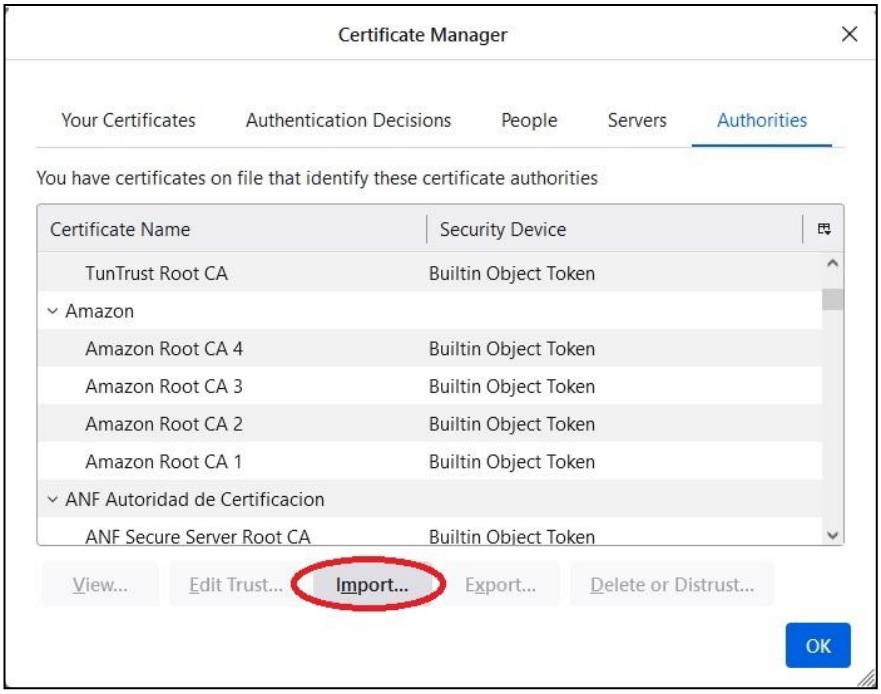

Fig. 5.4

5.1.5. Select the certificate from the installation directory of the digital signing service utility (e.g C:\Program Files (x86)\DSC Service\1.0.0\)

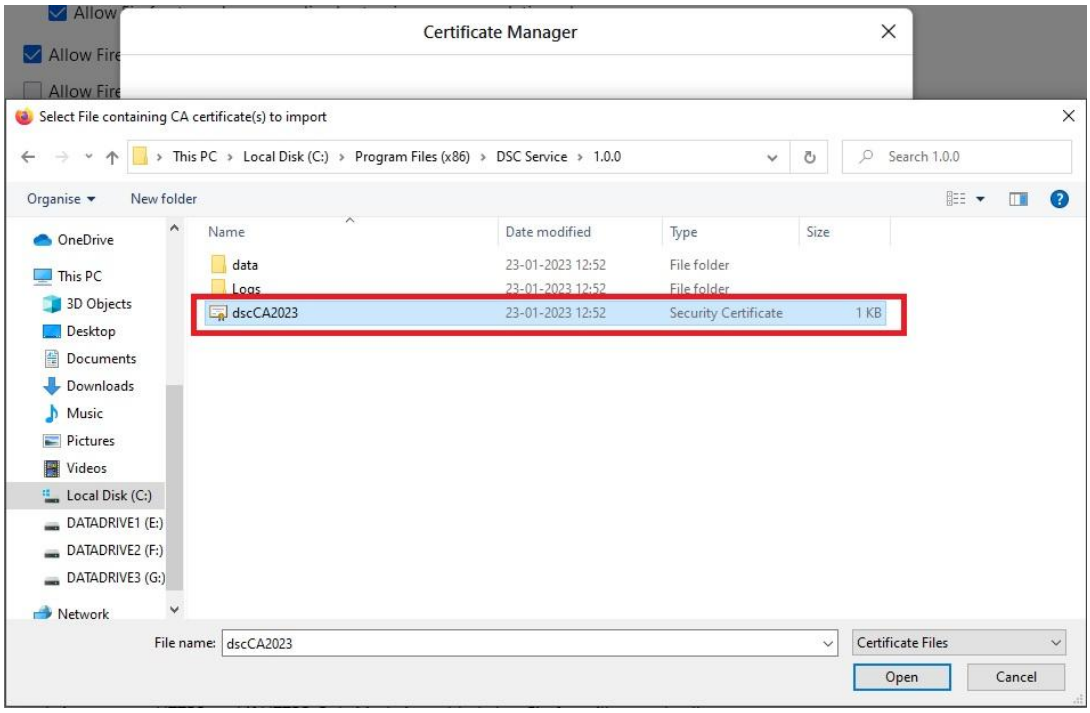

Fig. 5.5

5.1.6. Select <**Trust the CA to identify website**> option and click on <**OK**>.

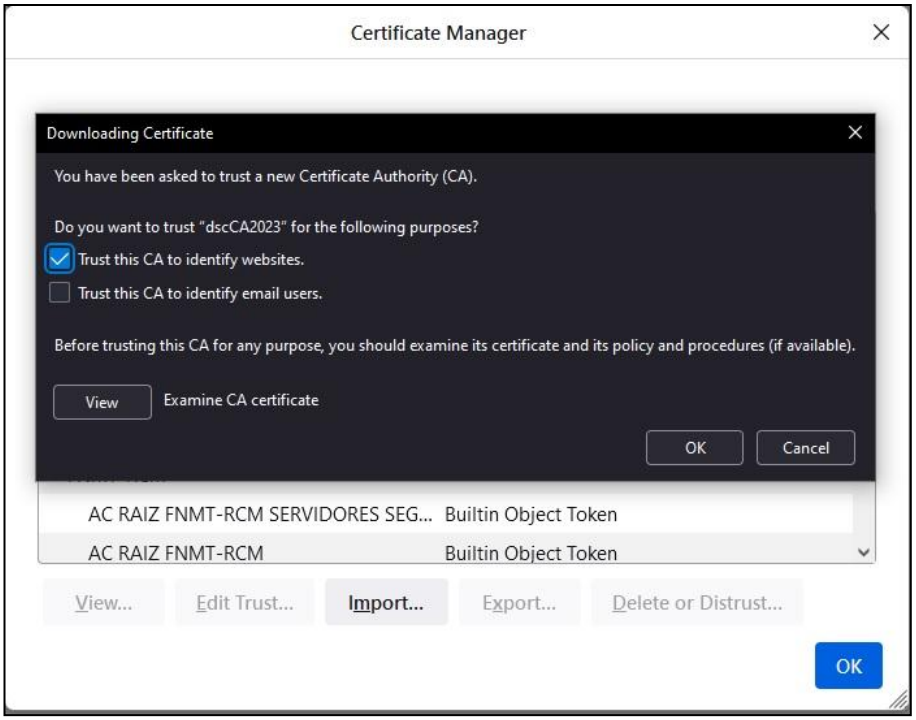

Fig. 5.6

Now, your Mozilla Firefox is ready for digitally signature

5.2. GOOGLE CHROME BROWSERS

Check whether the certificate is already imported into your browser post installation. To check the same please follow the below process

5.2.1. Go to Chrome browser settings.
5.2.2. Click on <**Privacy & Security**> option.
5.2.3. Click on <**Security**> option.

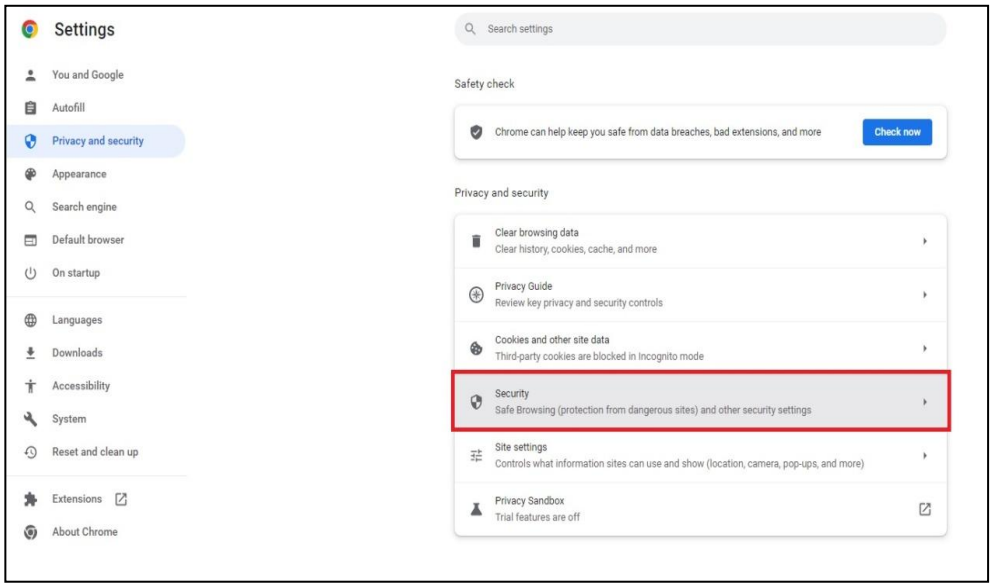

Fig. 5.7

5.2.4. Select on <**Manage device certificates**> option under <**Advanced** > header.

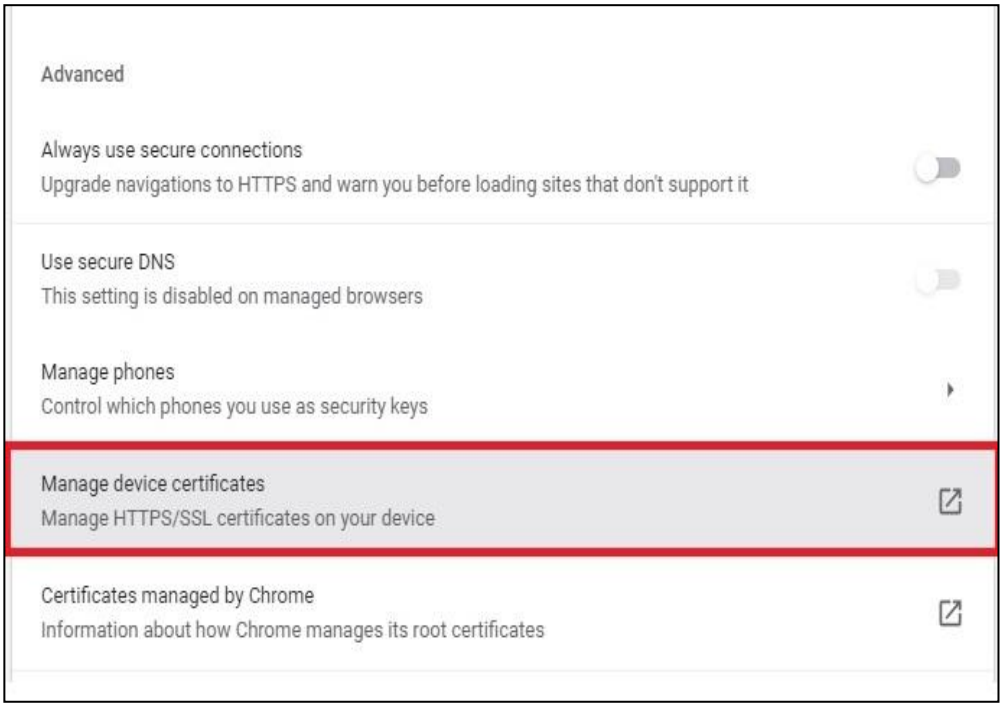

Fig. 5.8

5.2.5. Open <**Trusted Root certification Authorities**> tab.

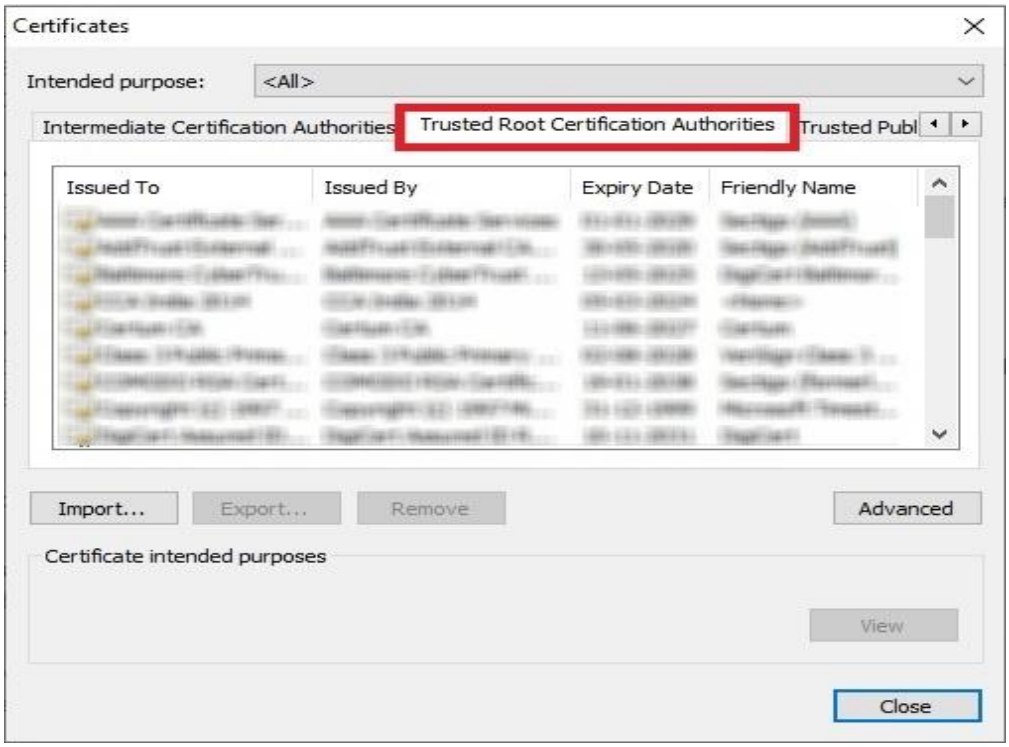

Fig. 5.9

5.2.6. Search for <**dscCA2023**>, if it is not available then Click on <**Import**> to import DSC certificate.

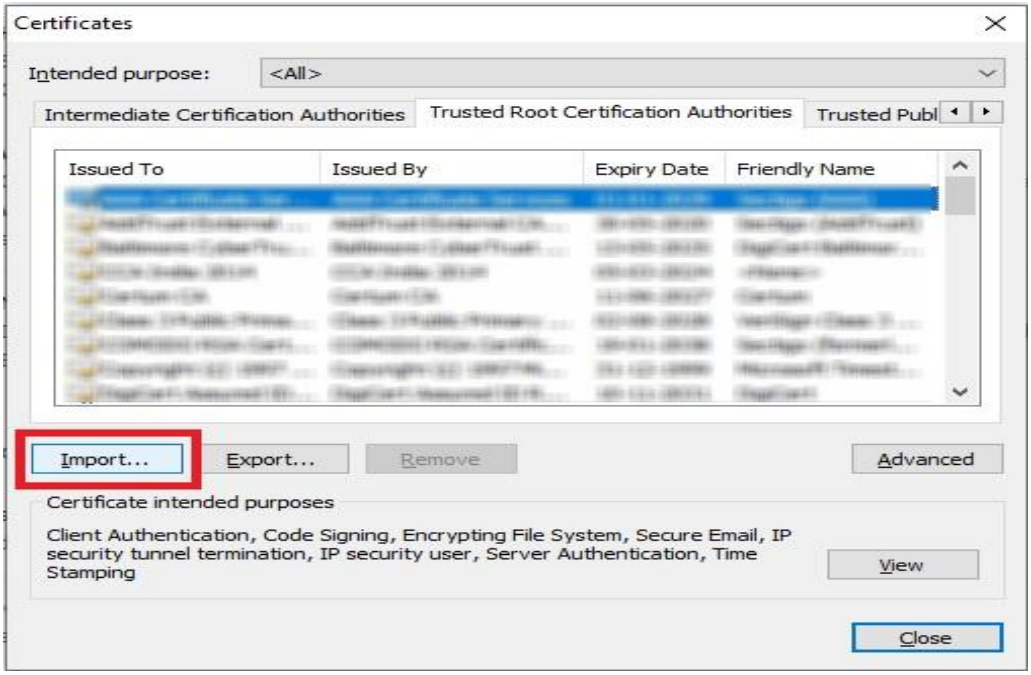

Fig.5.10

5.2.7. Click on <**Next**> to continue.

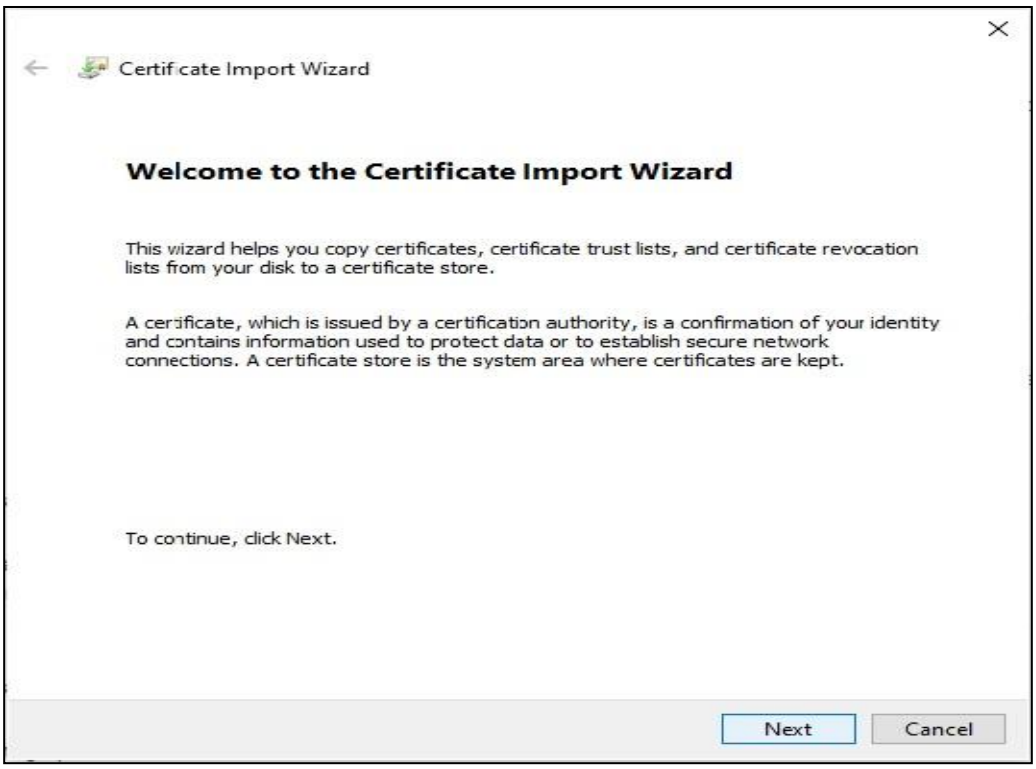

Fig.5.11

5.2.8. Click on <**Browse**> to select the certificate.

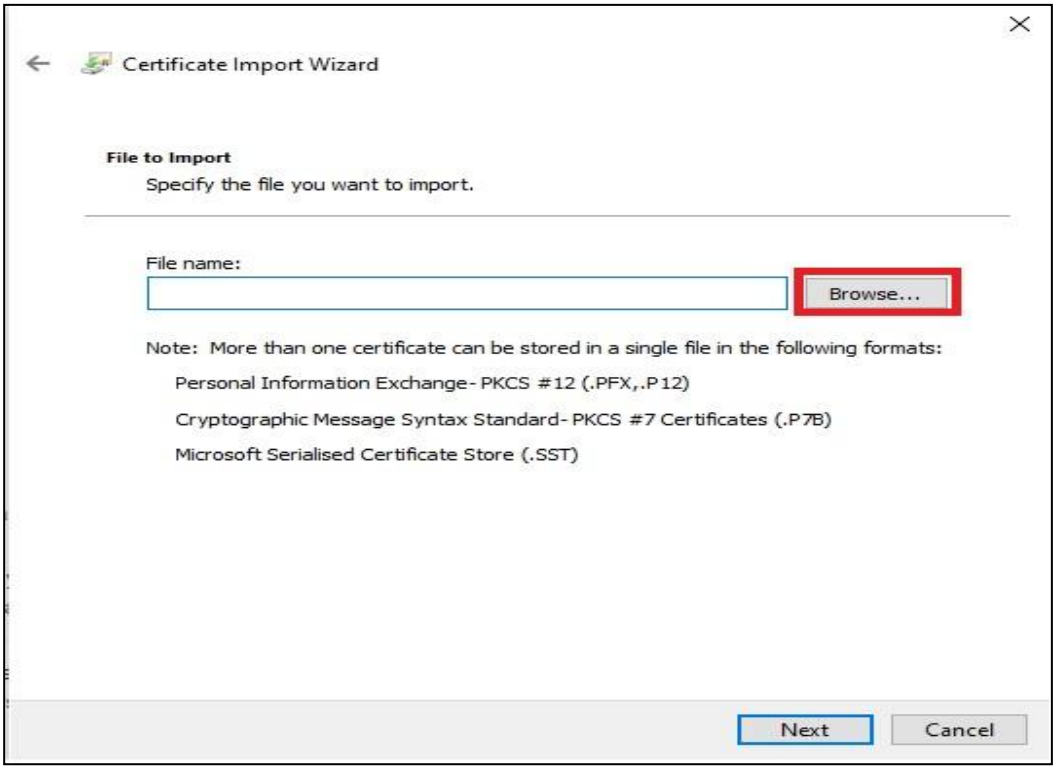

Fig.5.12

5.2.9. Select the certificate from the location where utility is installed.(Default location would be - C:\Program Files (x86)\DSC Service\1.0.0\)

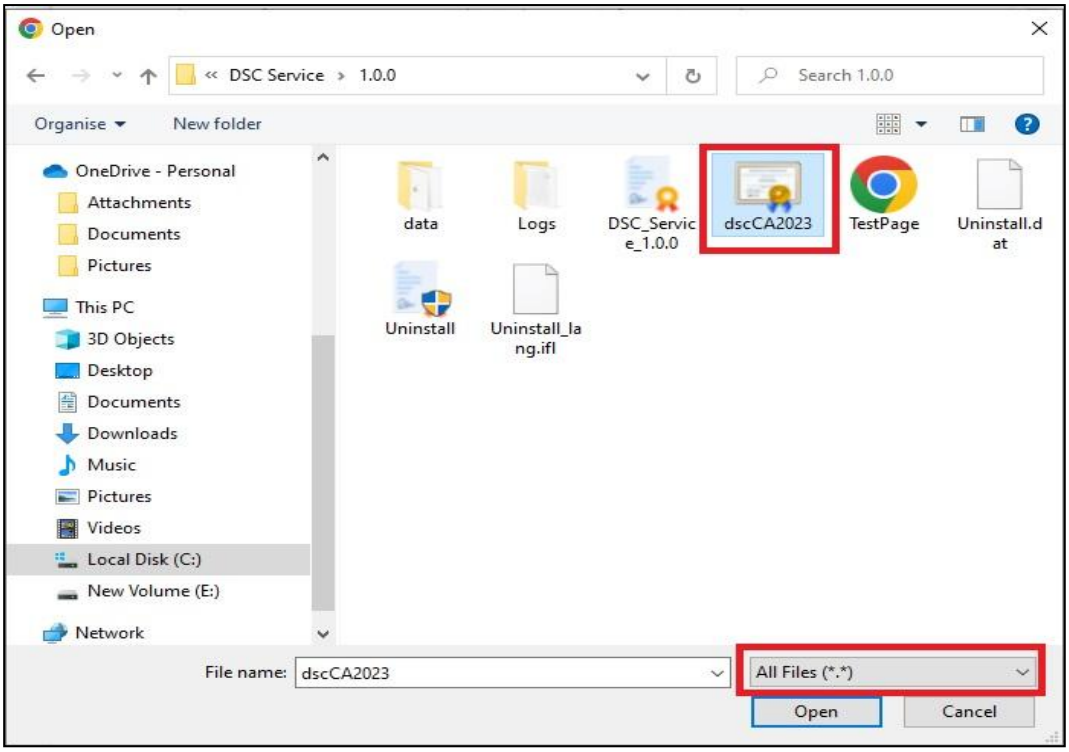

Fig.5.13

5.2.10. Click on <**Next**> to continue.

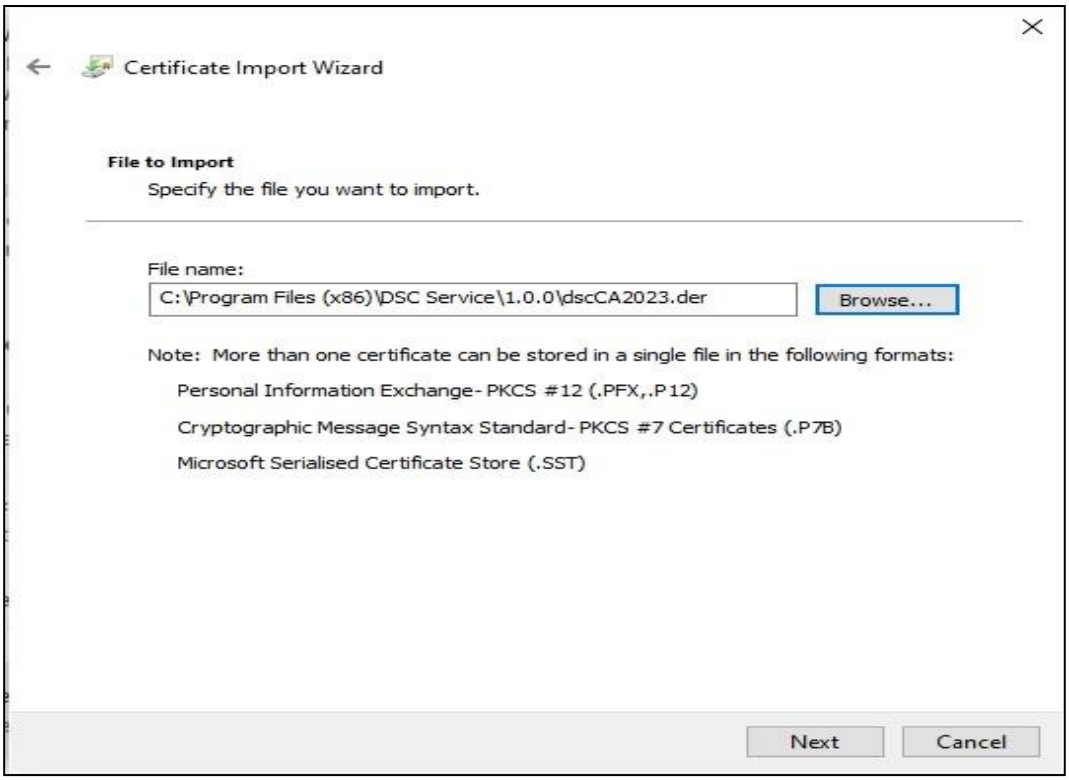

Fig.5.14

5.2.11. Select <**Place all certificate in following store**> & browse certificate store to <**Trusted Root certification Authorities>**.

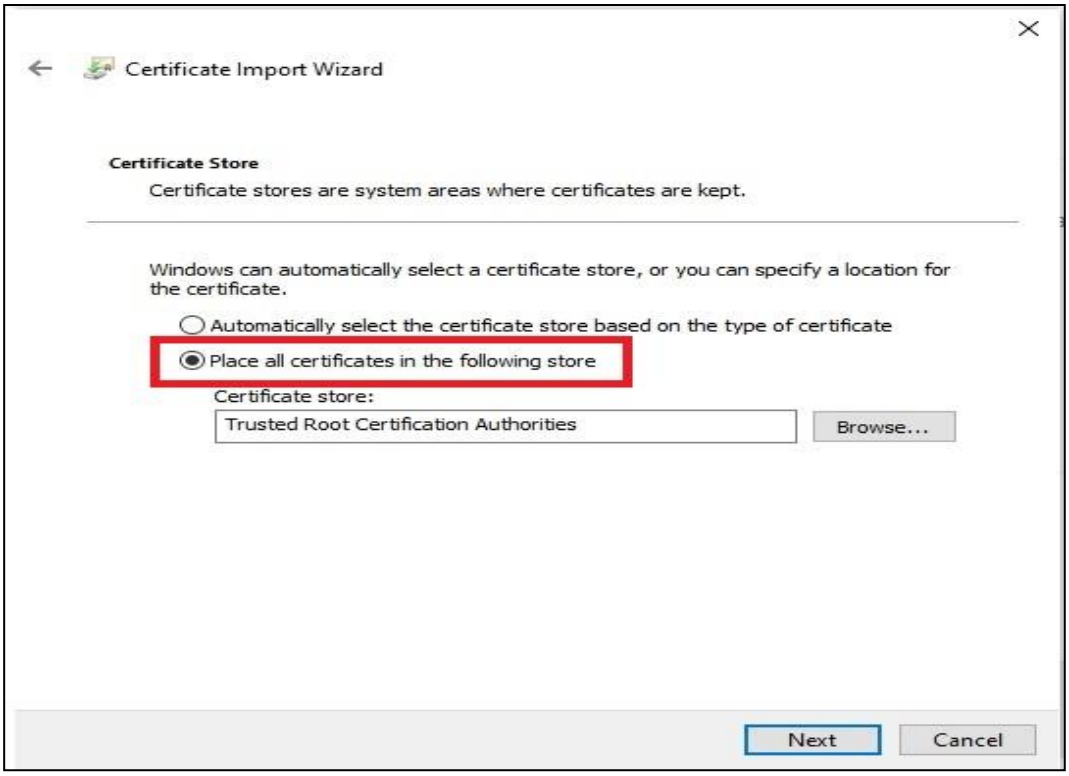

Fig.5.15

5.2.12. Click on <**Finish**> to continue.

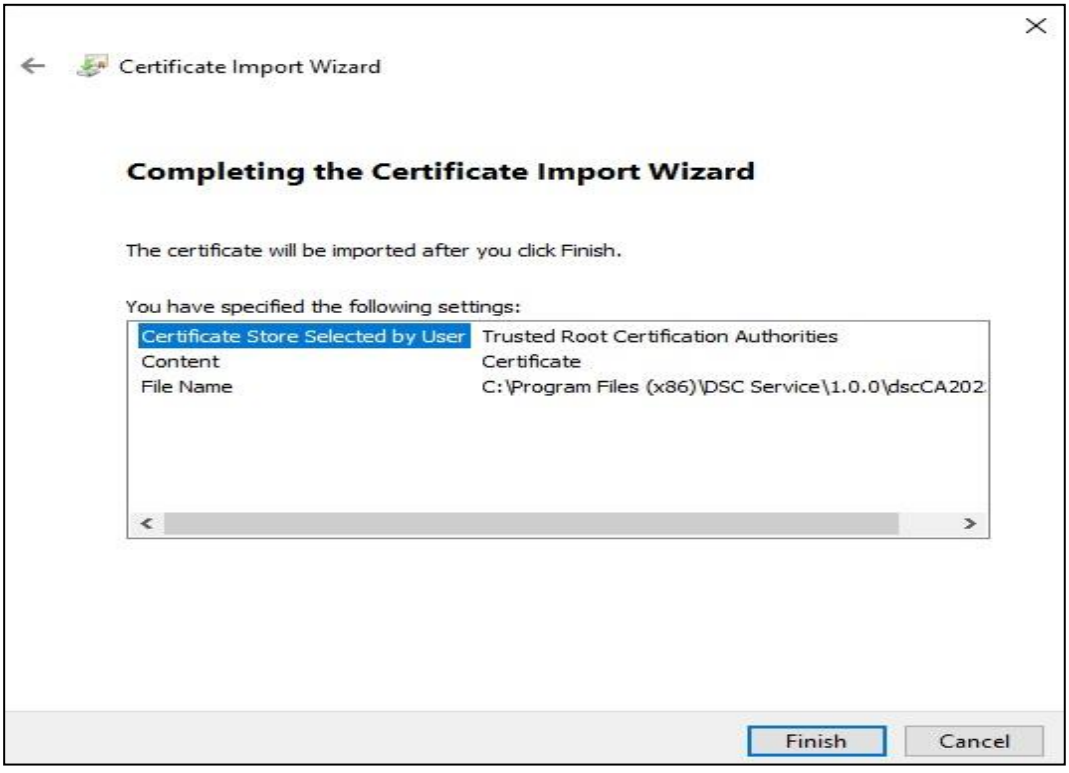

Fig.5.16

5.2.13. Click on <**Yes**> to install the certificate.

Fig.5.17

5.2.14. You will see message for success import. Click on <**OK**>to end the Certificate Import Wizard.

Fig.5.18

5.2.15. Check the imported DSC certificate under <**Trusted Root Certification Authorities**> tab.

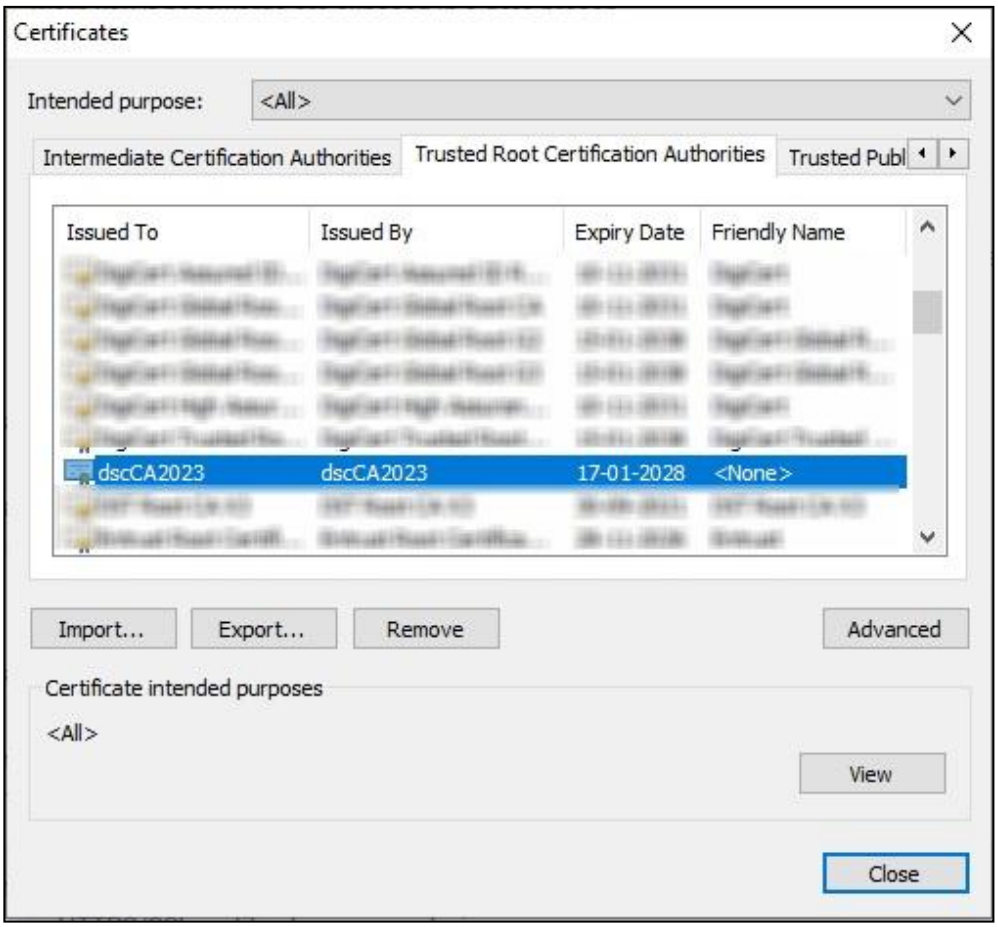

Fig.5.19

5.3. MICROSOFT EDGE BROWSERS

Check whether the certificate is already imported into your browser post installation. To check the same please follow the below process

5.3.1. Go to Edge browser settings.
5.3.2. Click on <**Privacy & Security**> option.
5.3.3. Select on <**Manage certificates**> option under <**Security**>header.

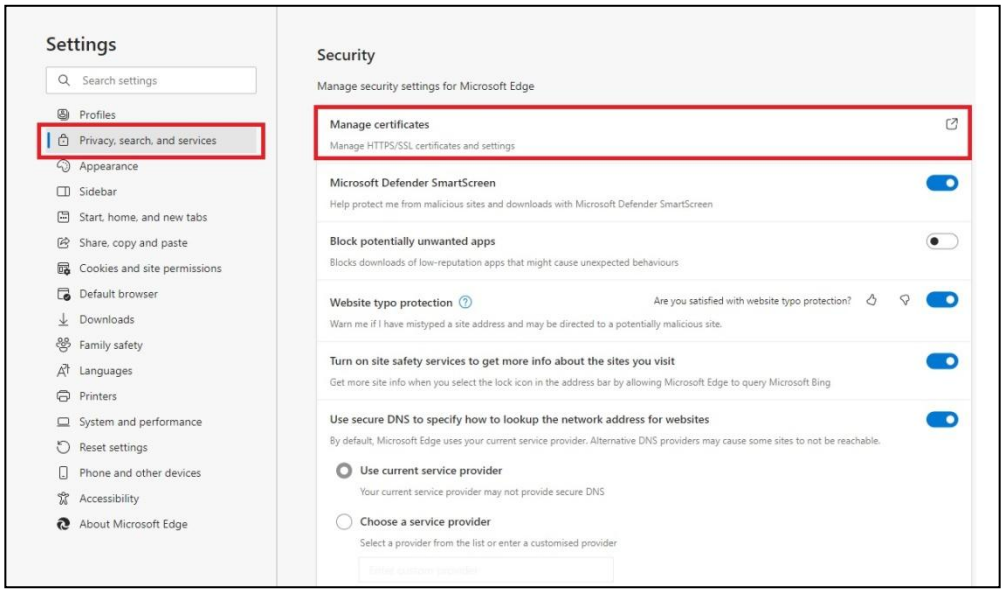

Fig.5.20

5.3.4. Open <**Trusted Root certification Authorities**> tab.

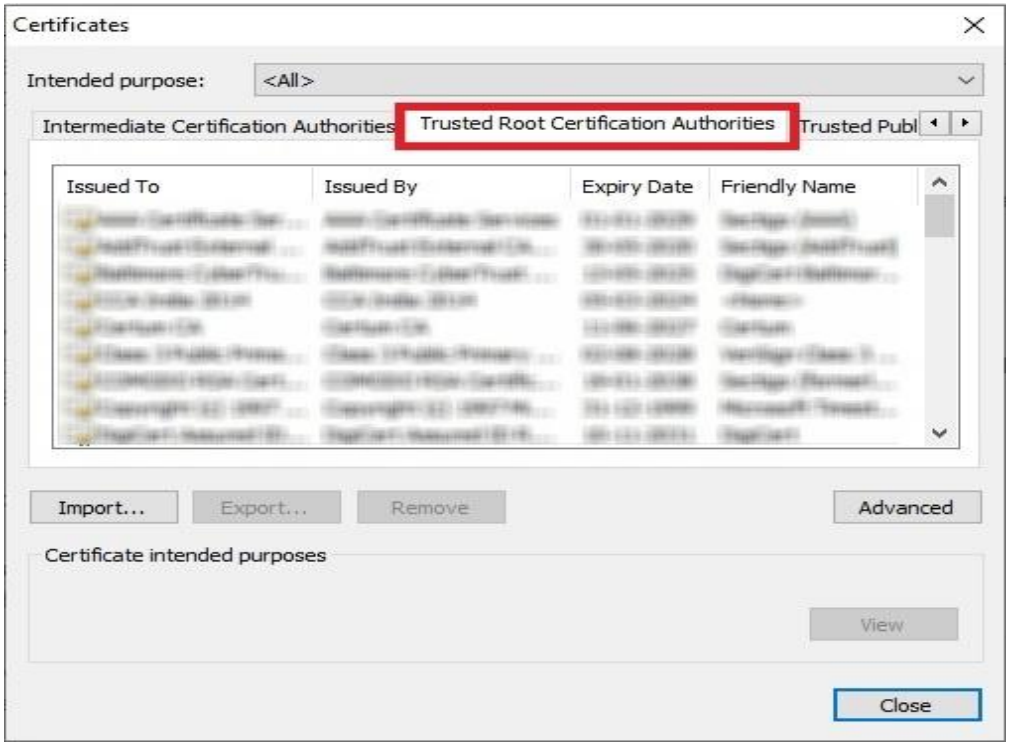

Fig. 5.21

5.3.5. Search for <**dscCA2023**>, if it is not available then Click on <**Import**> to import DSC certificate.

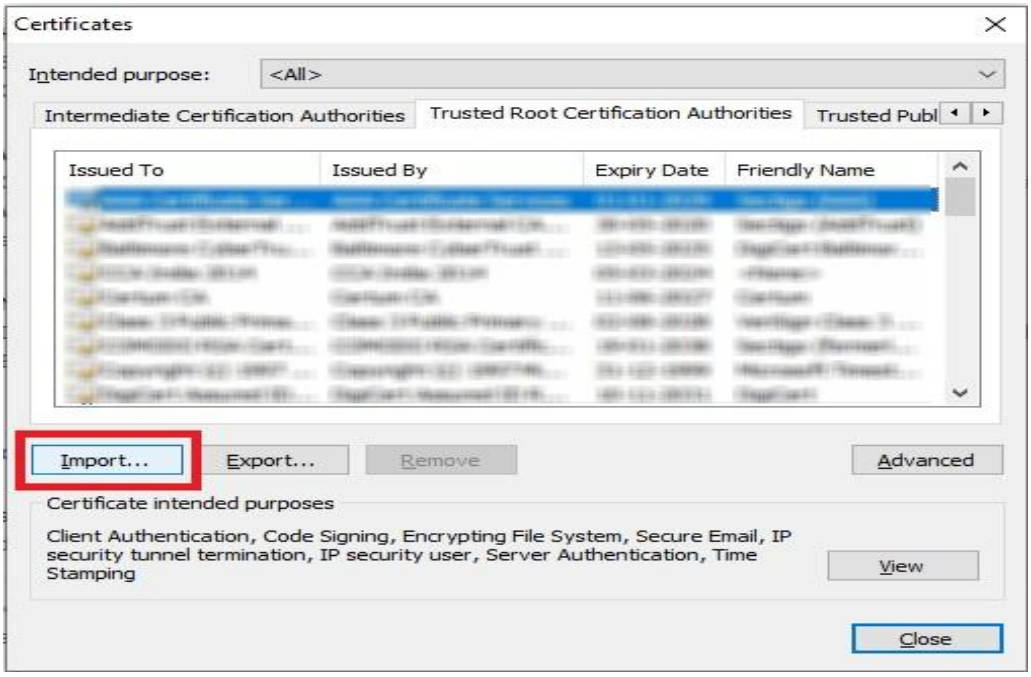

Fig.5.22

5.3.6. Click on <**Next**> to continue.

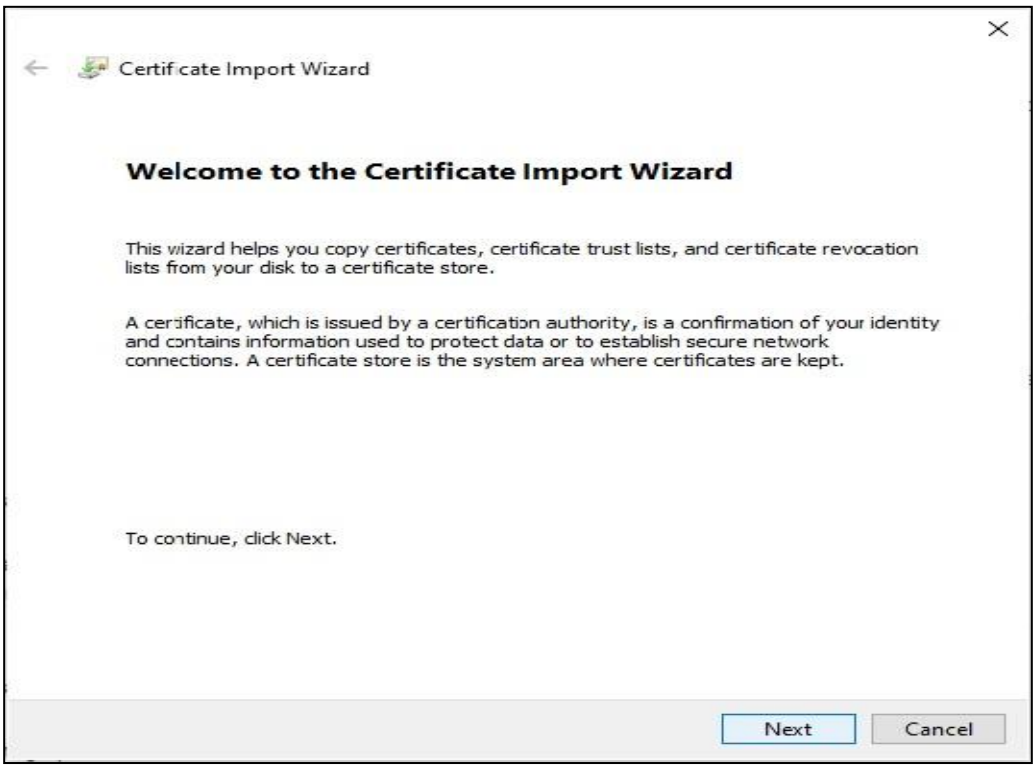

Fig.5.23

5.3.7. Click on <**Browse**> to select the certificate.

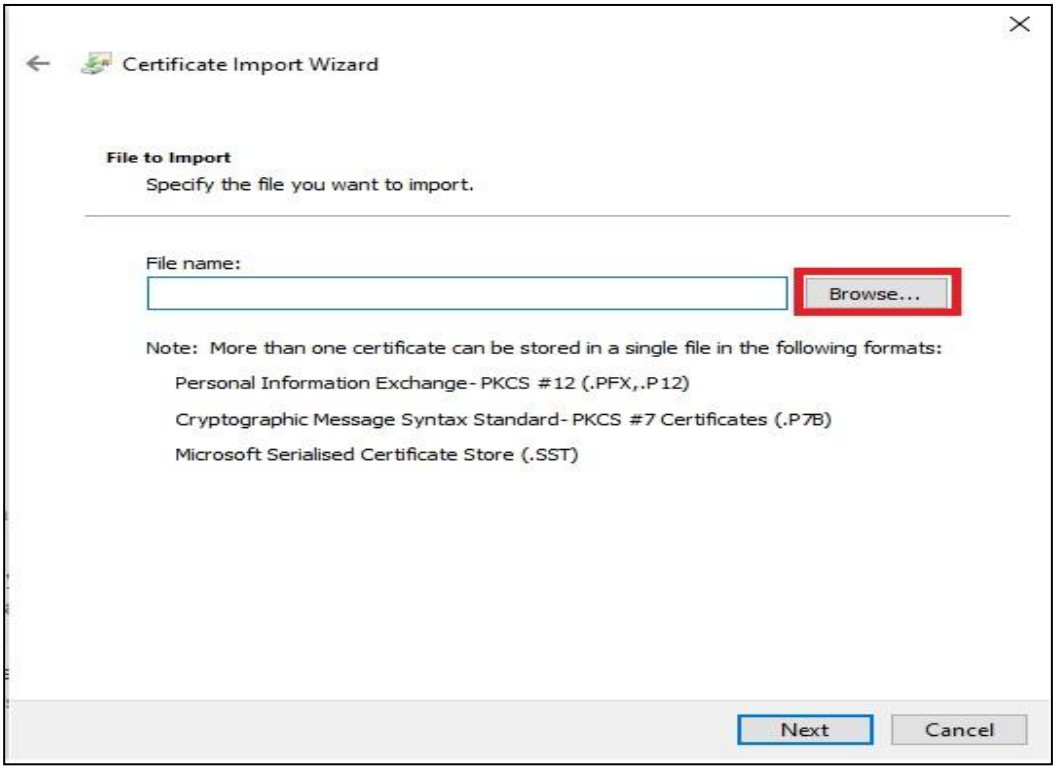

Fig.5.24

5.3.8. Select the certificate from the location where utility is installed.(Default location would be - C:\Program Files (x86)\DSC Service\1.0.0\)

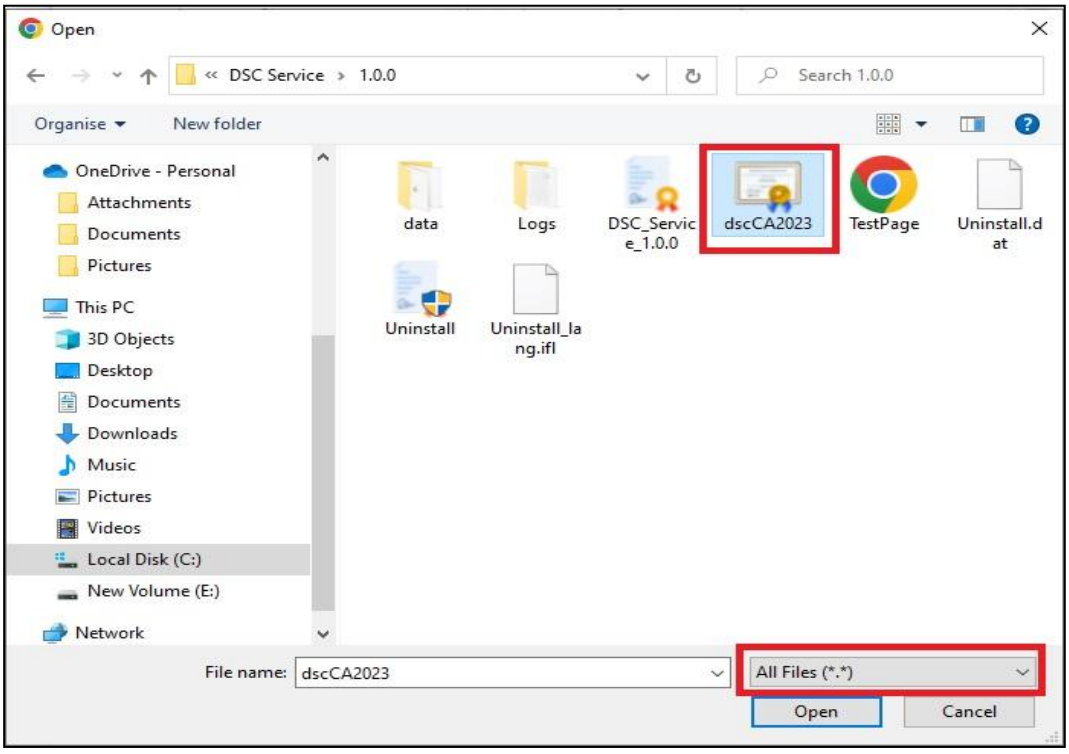

Fig.5.25

5.3.9. Click on <**Next**> to continue.

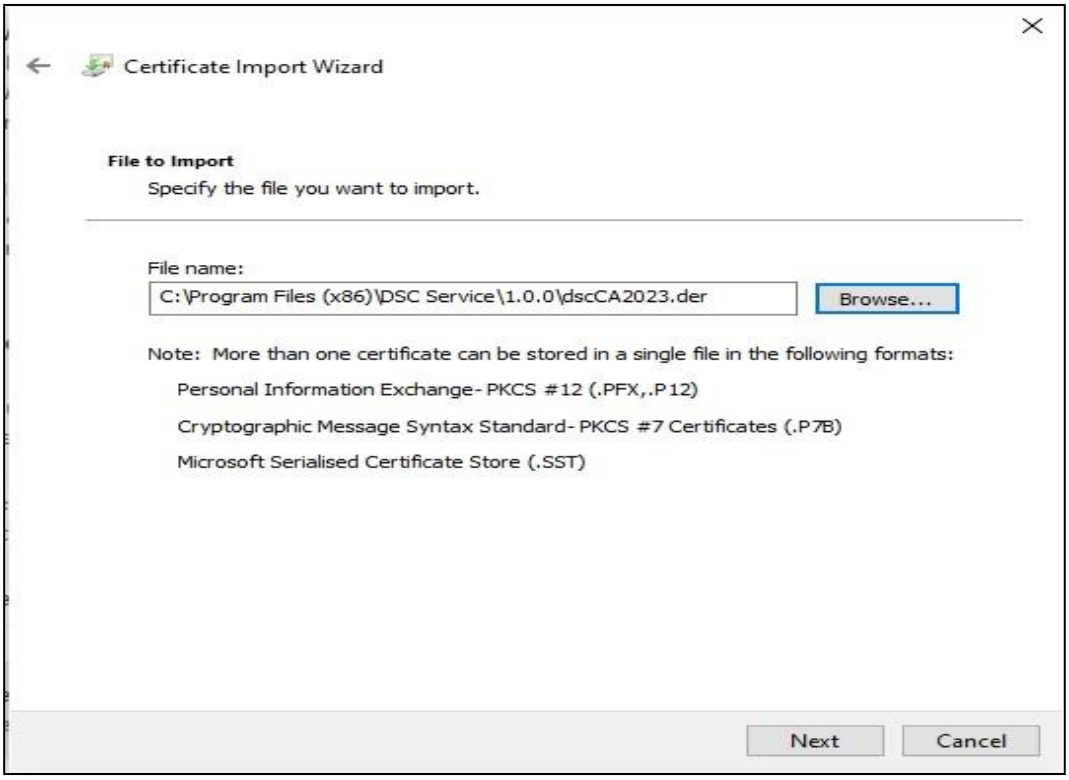

Fig.5.26

5.3.10. Select <**Place all certificate in following store**> & browse certificate store to <**Trusted Root certification Authorities>**.

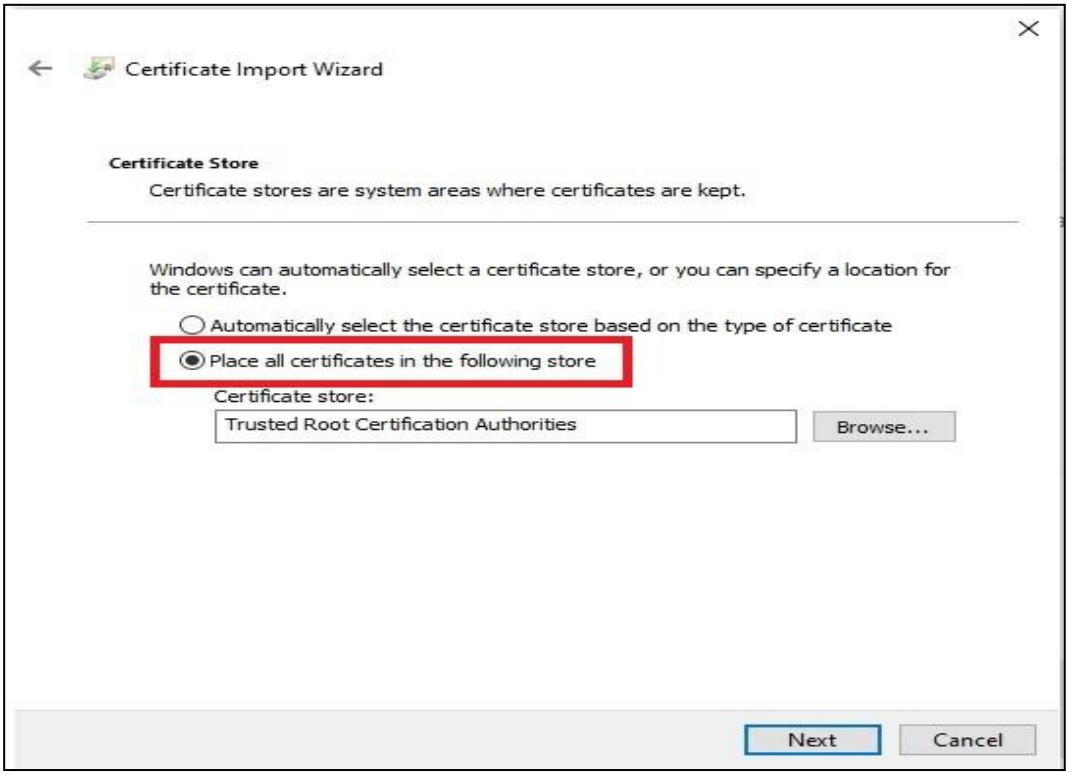

Fig.5.27

5.3.11. Click on <**Finish**> to continue.

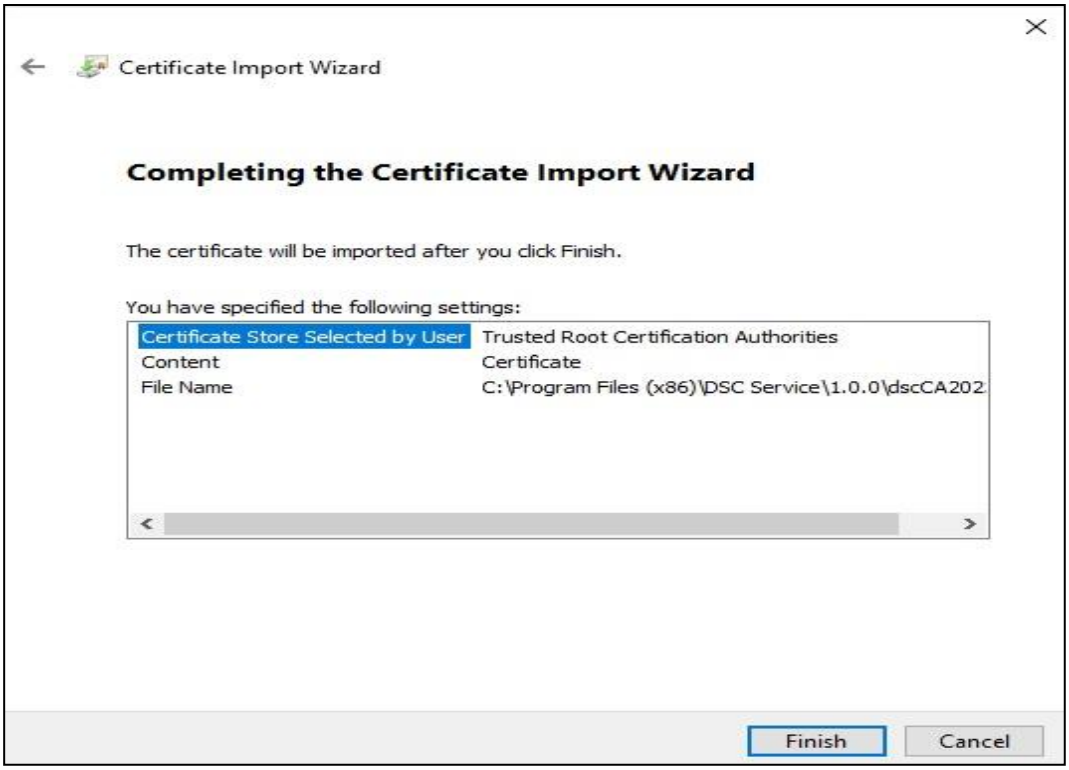

Fig.5.28

5.3.12. You will see message for success import. Click on <**OK**>to end the Certificate Import Wizard.

Fig.5.29

5.3.13. Check the imported DSC certificate under <**Trusted Root Certification Authorities**> tab.

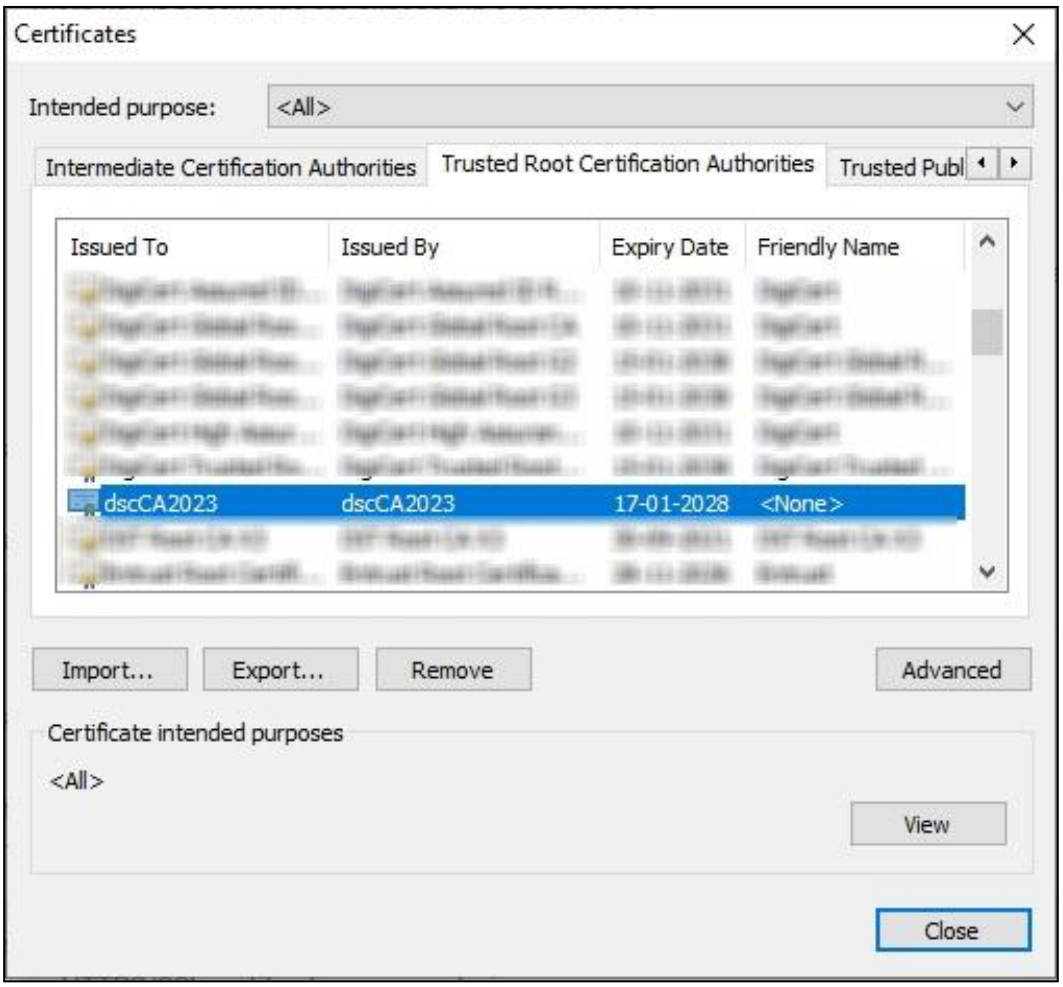

Fig.5.30

6. DIGITAL SIGNING PROCESS AT UNIFIED PORTAL

Once the steps in earlier section of the document are performed your machine is enabled to perform USB-token based Digital signing at EPFO's Employer interface of Unified Portal.

Follow the below steps to perform digital signing. The below is just a example from one of the facility available at EPFO's Employer interface of Unified Portal for digital signing. The steps in other functionalities may differ slightly in terms of the user interface.

8.1. Log in Employer interface of Unified portal.

8.2. Navigate to the functionality where the Digital Signing is to be performed.

Fig. 6.1

Note: above navigation screenshot is for illustration purpose. User has to select the relevant menu.

8.3. Choose the action to be performed (Approve/Reject). Select Digital Signature (DSC) option to initiate the process of signing. Ensure that the Digital Signature token is connected to the machine.

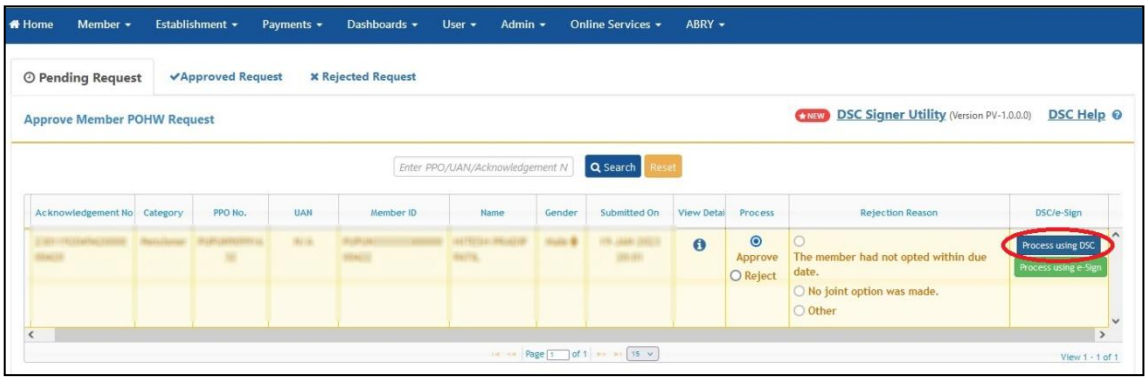

Fig. 6.2

8.4. Select from the list registered signatories who will be signing the document and click on 'Sign PDF' button to proceed.

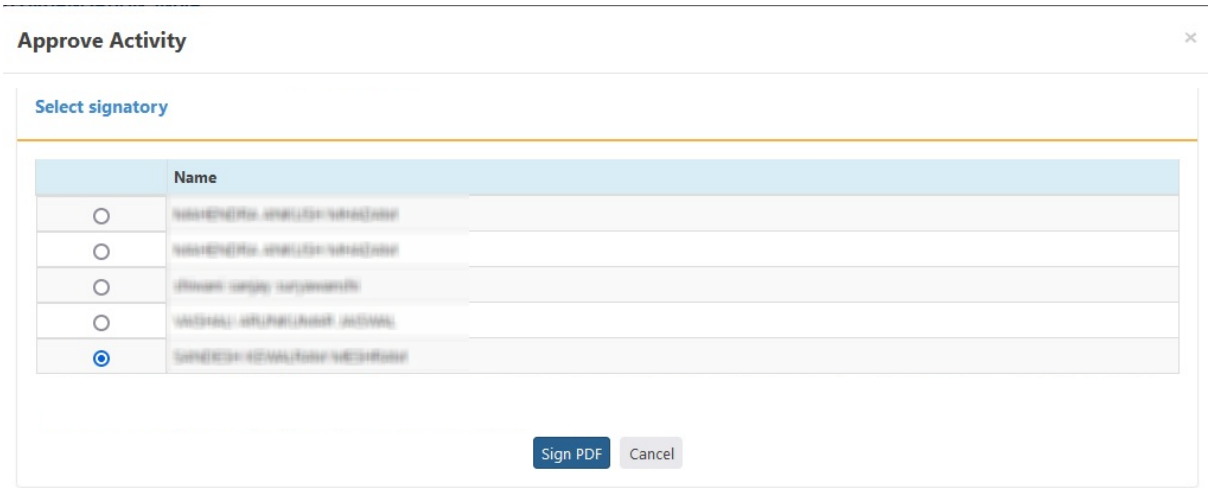

Fig. 6.3

8.5. Signing process will be started

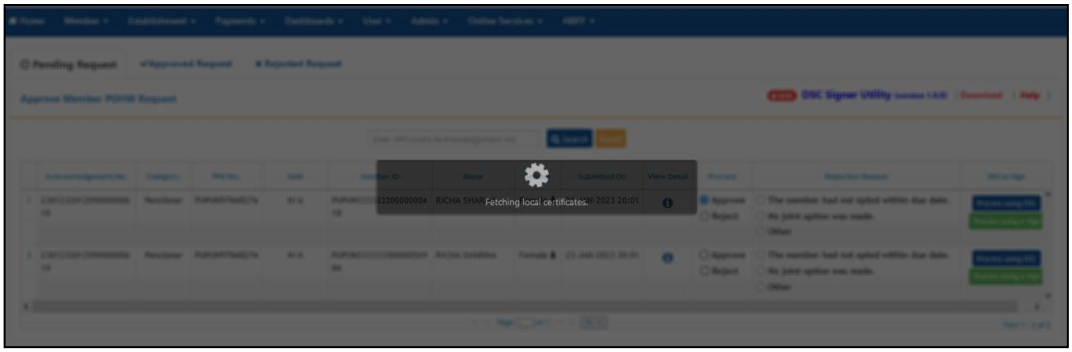

Fig. 6.4

8.6. You will be prompted for PIN corresponding to the attached Digital Signature token connected to the machine.

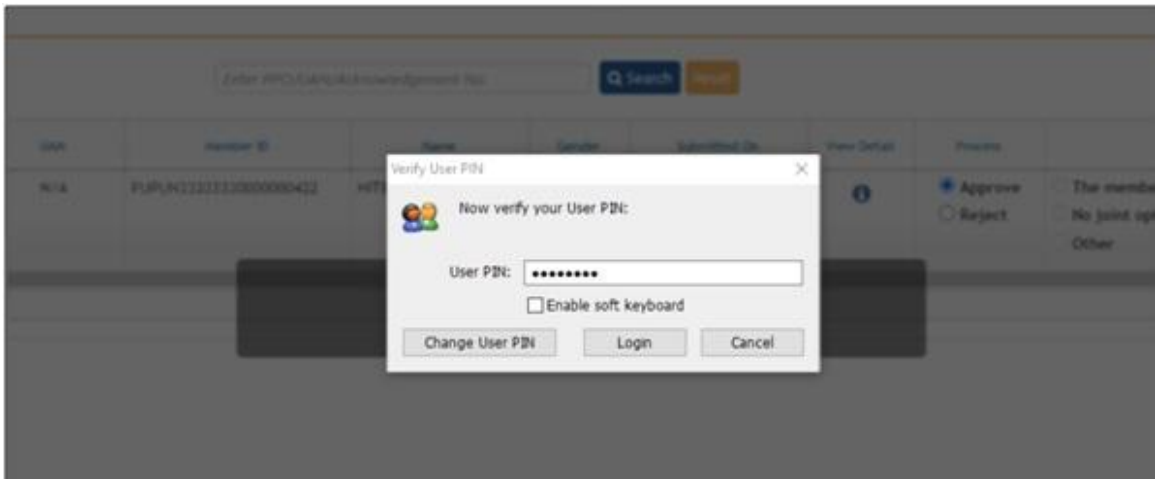

Fig. 6.5

8.7. If there is no issue while digital signature of the document the system will show success message.

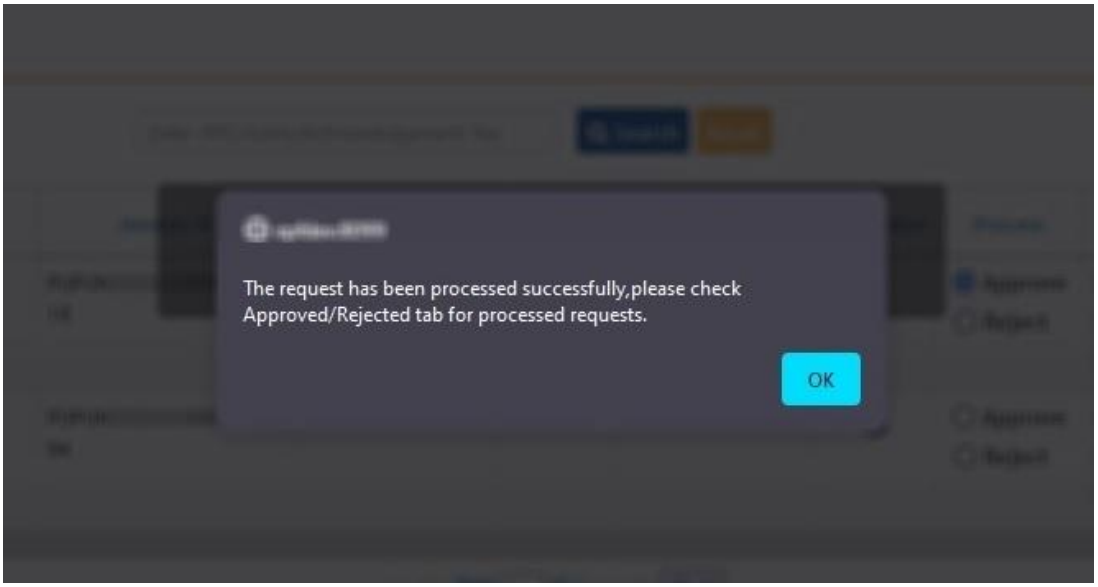

Fig. 6.6

It is recommended that the user verifies that the last document that was signed contains the correct signature.

7. TROUBLESHOOTING

The following section provides you to troubleshoot some of the common issues that can be faced by the user while the process of digital signature using this utility in Unified Portal.

7.1. CRL VERIFICATION TIMEOUT ERROR

In case you are getting CRL verification timeout error, it might be due to following probable reasons –

CRL VERIFICATION WEBSITE IS EITHER DOWN OR UNABLE TO HANDLE REQUEST

The digital signing utility online verifies the validity of the signature from the issuer; this requires the utility to connect to the issuers' website. During this process if the utility is unable connect to the issuers' website the CRL verification timeout error occurs. The following section provides the steps to identify the CRL verification url and suggests further course of action.

HOW TO CHECK

There are different steps to troubleshoot the issue in different browsers. Depending upon the browser you are using follow the below steps

Note: This document covers help for Mozilla Firefox, Google Chrome and Microsoft Edge browsers only

BROWSER: MOZILLA FIREFOX

- Go to Mozilla Firefox browser settings.
- Click on <**Privacy & Security**> option.
- Click on <**View certificates**> button.

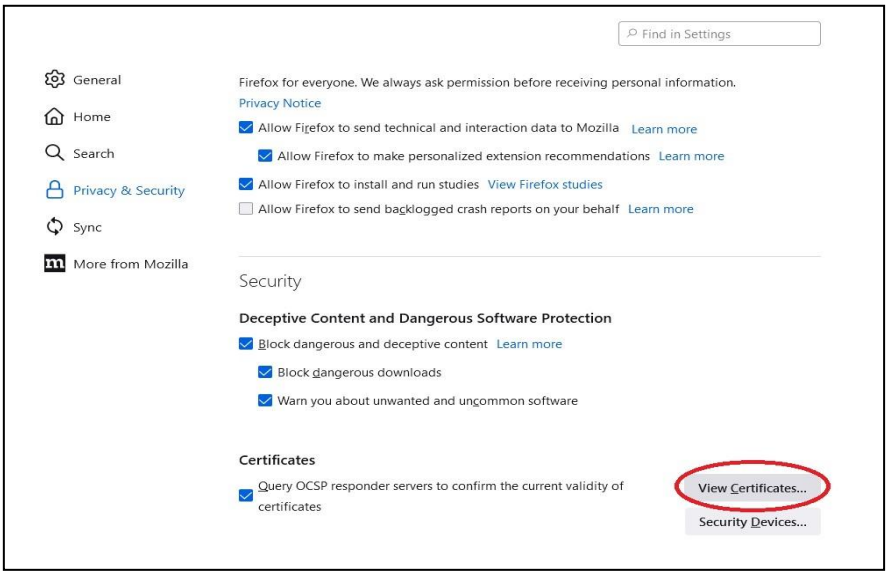

Fig. 7.1

- Select <**Your Certificates**> tab in <**Certificate Manager**>

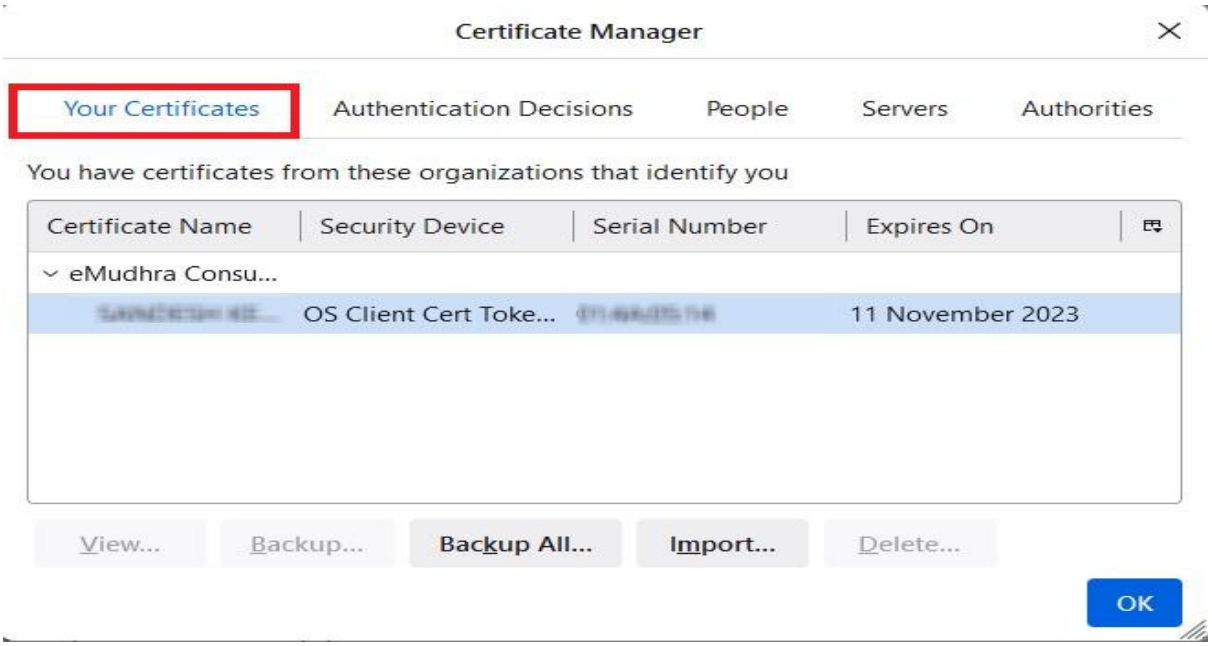

Fig. 7.2

- Select your certificate from the list displayed and double click on it. A new browser tab with the selected certificate details will open.

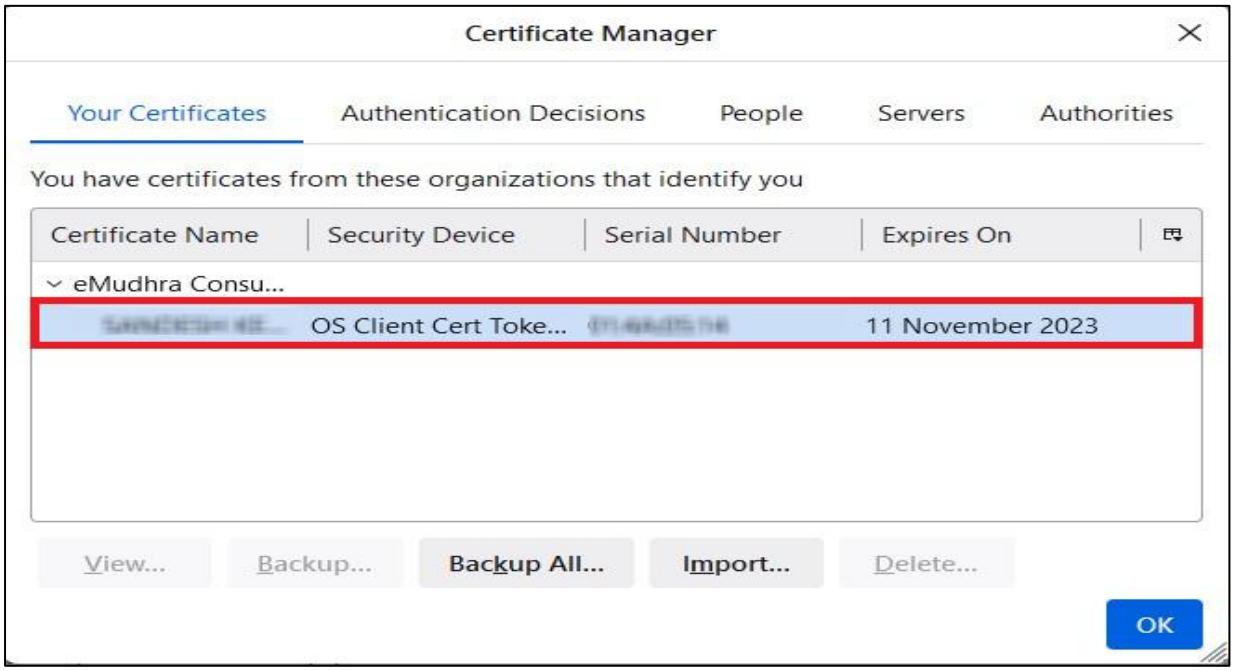

Fig. 7.3

- Search for CRL Endpoints and Copy the complete URL

Fig. 7.4

- Check whether the URL is accessible or not using your browser.
- In case the server is not reachable, please wait and try again later.
- In case it is blocked, contact your admin team to unblock the URL.

- Go to Chrome browser settings.
- Click on <**Privacy & Security**> option.
- Click on <**Security**> option.

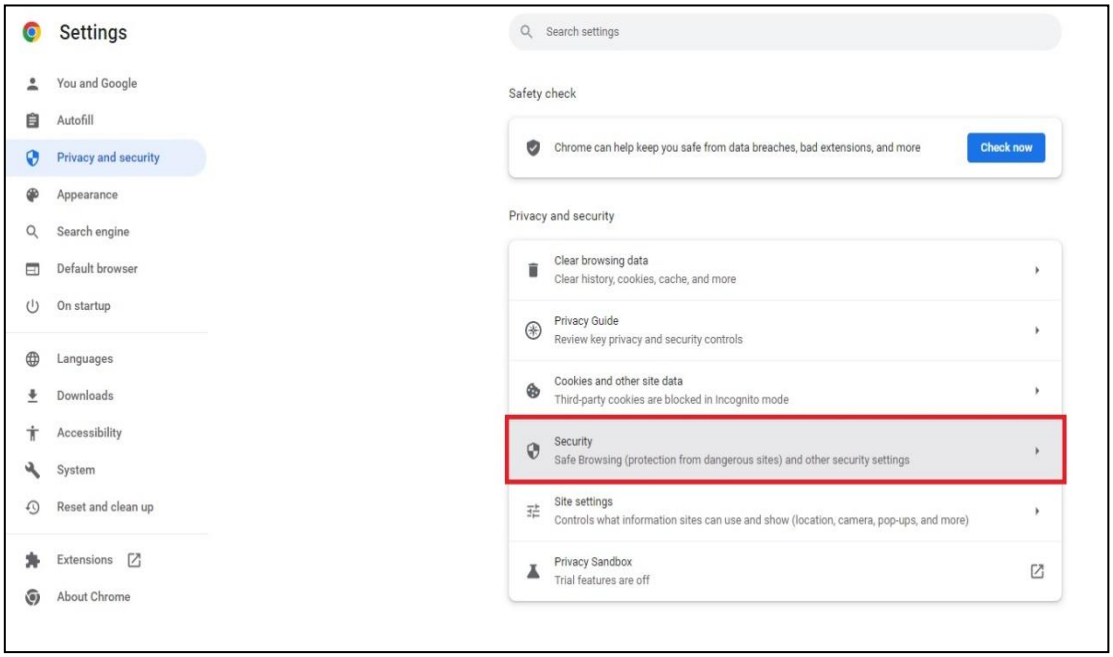

Fig. 7.5

- Select on <**Manage device certificates**> option under <**Advanced**> header.

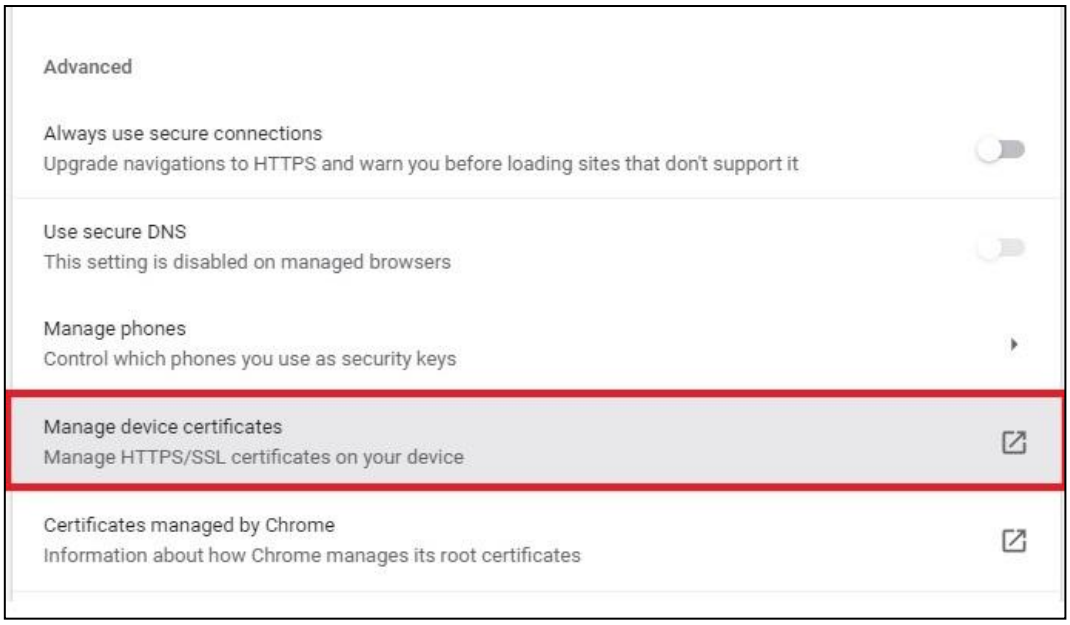

Fig. 7.6

- Select <**Personal**> tab in the <**Certificates**> window.

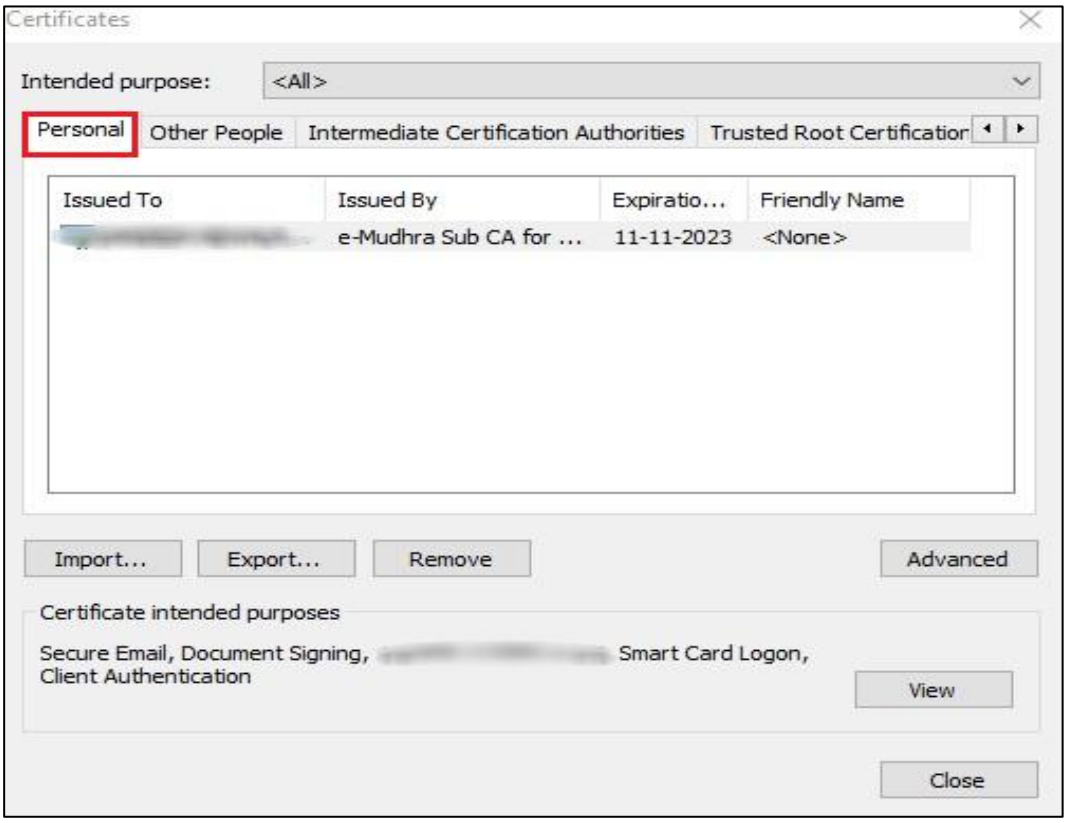

Fig. 7.7

- Select your certificate from the list shown and double click on it. A new window with the details of the selected certificate will open.

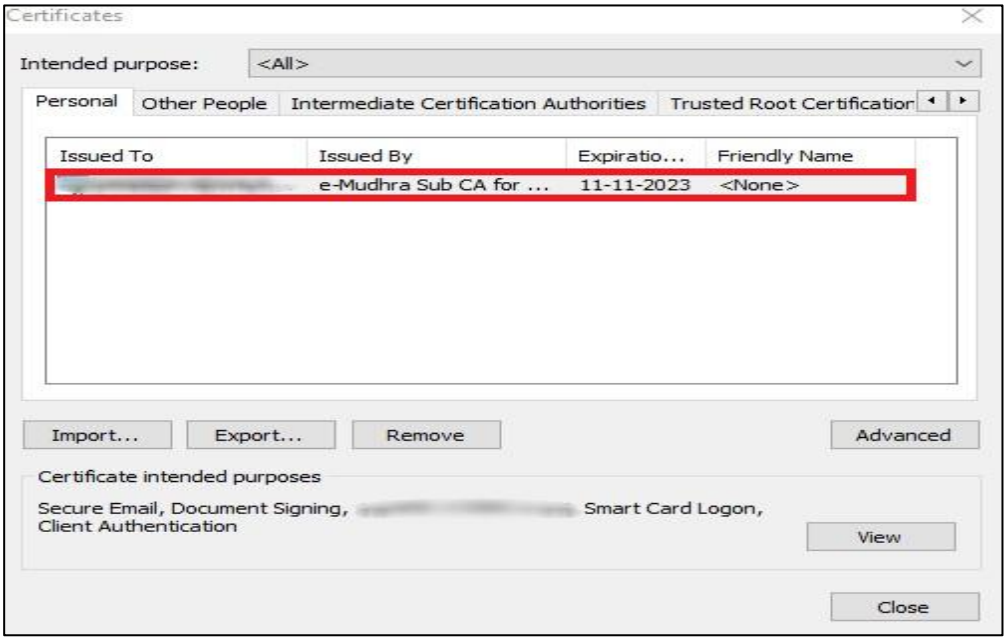

Fig. 7.8

- Select <**Details**> tab in the <**Certificate**> window.

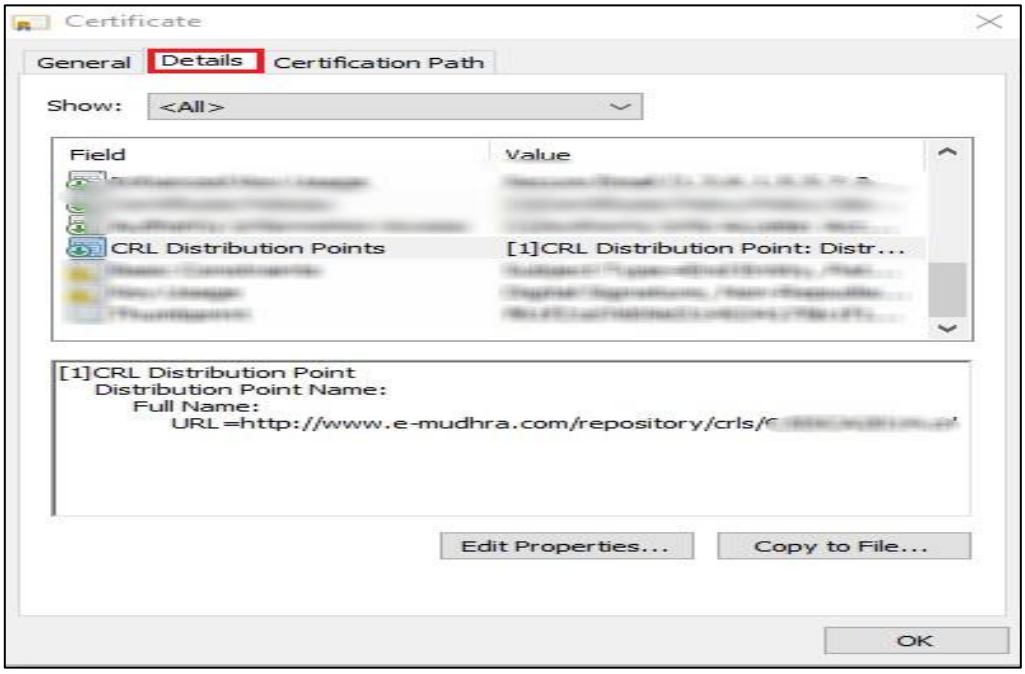

Fig. 7.9

- Search for <**CRL Distribution Points**> and click on it. Copy the URL.

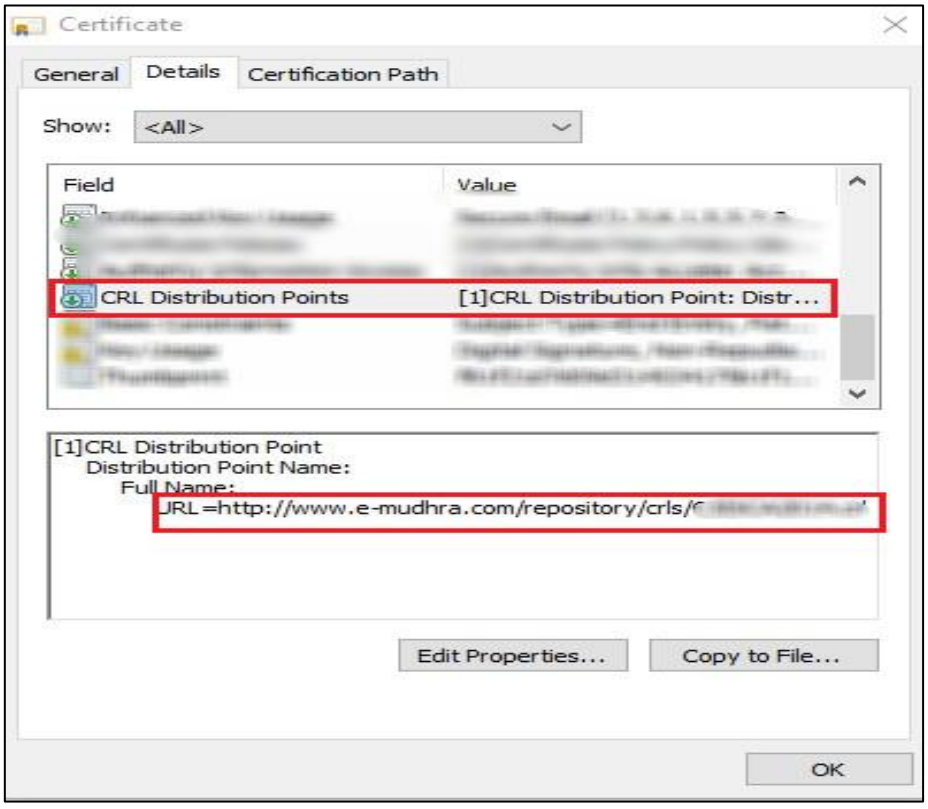

Fig. 7.10

- Check whether the URL is accessible or not using your browser.
- In case the server is not reachable, please wait and try again later.
- In case it is blocked, contact your admin team to unblock the URL.

THE CRL DISTRIBUTION POINT URL IS BLOCKED BY YOUR ORGANIZATION

In case the CRL verification url identified in the above section is blocked, contact your admin team/ internet service provider to unblock the URL