सत्यमेव जयते

eOffice

A DIGITAL WORK PLACE SOLUTION

DSC

Digital Signer Service

User Guidelines

NIC-EOF-DSC-UG-001

Prepared by

एनआईसी National Informatics Centre

Amendment History

S.No.	Application Version	Date of Release	Date of Amendment	Amended By	Amendments
1.	2.0	13-06-2018	13-06-2018	eOffice Project Division	User Guidelines
2.	3.0	03-10-2018	03-10-2018	eOffice Project Division	User Guidelines
3.	3.5	29-11-2018	29-11-2018	eOffice Project Division	User Guidelines
4.	4.1	05-03-2019	05-03-2019	eOffice Project Division	User Guidelines
5.	6.0	13-08-2019	13-08-2019	eOffice Project Division	User Guidelines
6.	4.1.01	26-02-2020	26-02-2020	eOffice Project Division	User Guidelines (change in installation steps for windows)
7.	6.0.1	27-03-2020	27-03-2020	eOffice Project Division	User Guidelines
8.	6.1.1	26-06-2020	26-06-2020	eOffice Project Division	User Guidelines (NG)
9.	6.1.2	12-11-2020	12-11-2020	eOffice Project Division	• Annexure I *(installation steps for SSL Certificate on different browsers of different operating systems)/* • Change in name of signer Certificate and URL
10.	7.0.0	21-01-2022	21-01-2022	eOffice Project Division	• Change in name of signer Certificate and URL • Language change option (English & Hindi)
11.	7.x.x	22-09-2022	22-09-2022	eOffice Project Division	• Change in installation steps for MAC machine.

Table of Contents

Abbreviations

DSC	Digital Signature Certificate
NPAPI	Netscape Plug-in Application Programming Interface
NICNET	National Informatics Center Network
OS	Operating System
SSL	Secure Socket Layer
LTV	Long Term Validation

Introduction

Till recently the web-based applications were using applet-based technology to achieve digital signing that used Java plug-ins (NPAPI plug-in) provided by browsers (Chrome, Firefox, and Internet Explorer etc.) to run applet inside the browser.

The latest versions of all browsers started discontinuing the applet support (around the Year 2016-2017) essentially to firm up the security. The signing mechanisms that eOffice (or for that matter any other web application) was using earlier, therefore, also had to change. Digital Signer Service 4.1 was developed and released and it works with the latest browsers which do not require applet to run.

In version 4.1, multiple URLs were being used for signing/authentication/registration purposes, and this was quite complex for consuming applications. To make it simple, in the version 6 of Digital Signer Service a single URL was provided for signing/authentication/registration purposes. A new functionality was also provided for single or multiple signatures on a single PDF document as well as for bulk signing of PDF documents. Also, user(s) can add multiple token drivers in MAC/Ubuntu machines.

In the previous versions, each response was containing CRL files inside of it, and the response was being kept inside database due to which it was taking database too heavy. To overcome this issue, in the current version CRL files are being stored in database separately from response. And the reference of CRL files is being passed with each transaction. In current version, custom CA signed SSL certificate is being used as self-signed SSL certificate is no longer supported by all major browsers after some security updates, while in previous versions, Self-Signed SSL certificate was being used. Also, multi-language support is added with the UI to make it more interactive, currently two languages are being supported – English & Hindi. In future, more languages will be provided.

It is essentially a service that would require to be installed one time in the individual windows/MAC/Ubuntu client's machines of the user.

This document provides very simple steps that will guide the user to install the signer service smoothly on his/her local client machine and also provide help to the users of eOffice in their respective departments/states.

New Features and Enhancements

1. Log4j vulnerability has been removed.
2. New SSL certificate has been provided with the expiration date of 27th Aug 2028.
3. This version of Digital Signer Service comes with bundled JRE, thus there is no need to install Java manually. Also it is independent of Java installed in a user's machine.

Existing Features

1. Enhanced Light weight response due to CRL files are being kept separately from response object, which require less space inside database.
2. Multi-language support is added with UI. User can choose language as per his/her convenience. Currently supporting English & Hindi language only.
3. Enhanced password window for MAC OS.
4. Backward compatibility with previous version 6.1.3
5. Improved message & exception handling.
6. Improved logs.
7. Multiple signatures on a single PDF
8. An enhanced & modified interface is created for all platforms (Windows/MAC/Ubuntu) additionally; the user(s) can add/configure new token(s) to work with MAC/Ubuntu client machines.
9. Improved messages & exception handling.
10. Users can remove the signature from pdf files(s) and can also get details of previously signed pdf file(s).
11. In a single go, Digital Signer Service 7.0.0 can be installed silently on multiple machines.
12. Updates can now install automatically.
13. Windows users can remove/uninstall Digital Signer Service 7.0.0 from Control Panel.
14. Quick Help.
15. Custom CA signed SSL Certificate is added to provide secure channel communication with consuming application(s).

Section1: Digital Signer Service

Procedure to download Digital Signer Service

The Digital Signer Service 7.0.0 can be downloaded from (as per client's machine OS):

https://docs.eoffice.gov.in (NICNET user(s))

OR

https://eoffice.gov.in, shown in **Fig.1.1** & **Fig1.2**:

Fig.1.1

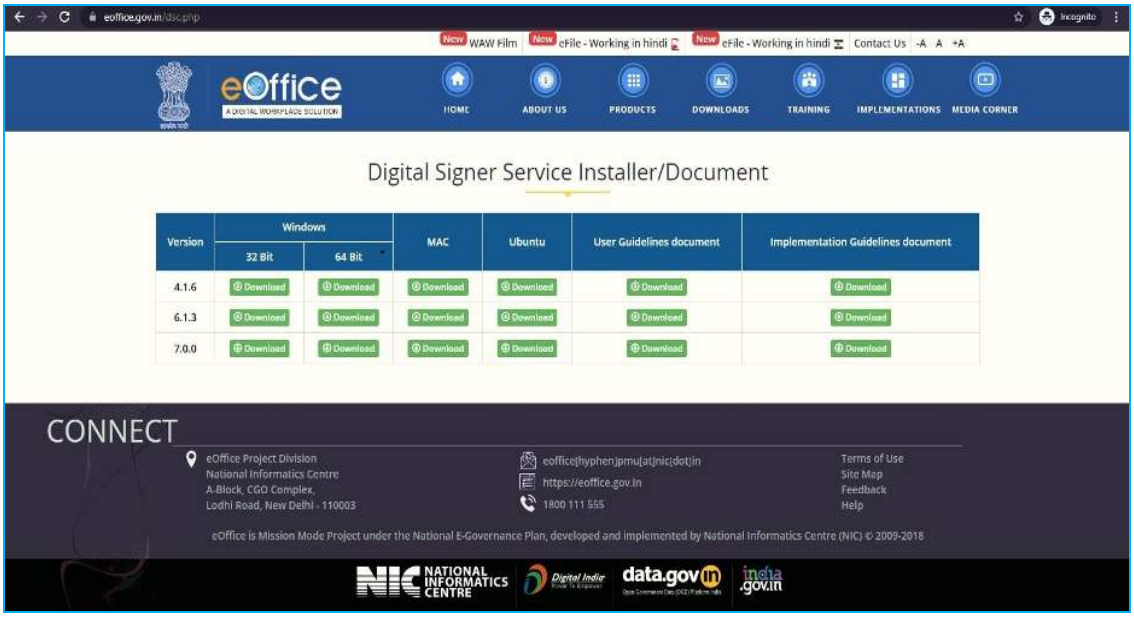


Fig.1.2

1. **Windows (For installation steps refer Section 2 Windows)**
2. **MAC (For installation steps refer Section 3 MAC)**
3. **Ubuntu (For installation steps refer Section 4 Ubuntu)**

Client's Machine Requirement:

The Digital Signer Service is available for following **OS** client's machine:

Minimum client's machine Requirements	
Windows OS	Windows 10 & above.
MAC OS	MAC 10.7 & above.
Ubuntu OS	Ubuntu 18 & above.
Availability of port 55103	

Note:

For Digital Signer Service 4.1 the available ports is 55101.

Section2: Windows OS

Download the Digital Signer Service 7.0.0 and related utilities (available as a single bundled zip file) from one of the URLs mentioned previously.

Identifying Your System

- Unzip the downloaded folder, locate and run **Check_System_Details.bat** file from downloaded bundle (**Digital Signer Service 7.0.0 Windows Installer folder, Fig.2.1**) to check if user machine has java installed or not.

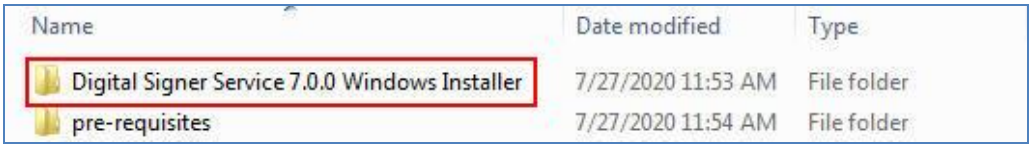


Fig.2.1

- This also checks that if port 55103 is free or not and displays an appropriate message as shown in **Fig.2.2:**

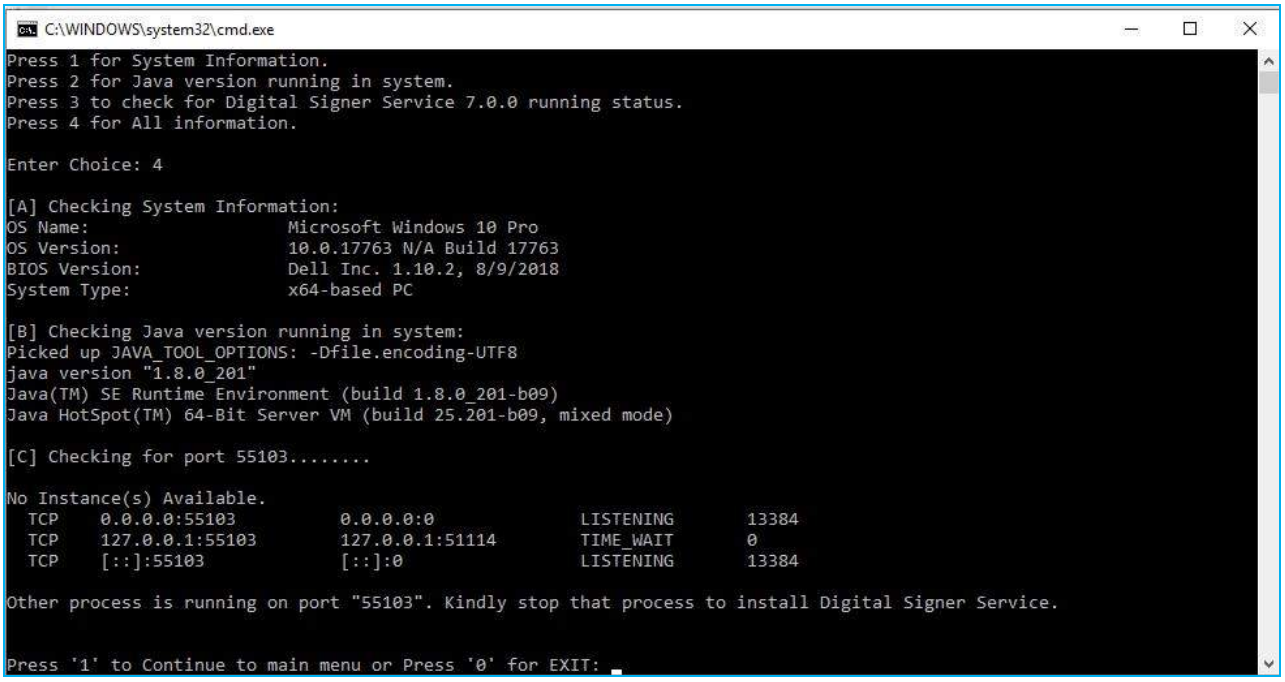


Fig.2.2

Note:

1. In case .bat file does not run, refer to **Annexure IV** for manually identifying the JAVA, OS and Digital Signer Service status details.

Pre-requisites for Digital Signer Service Installer for Windows

Following four activities to be completed by User(s).		
S. No.	**Activities**	**Remarks**
1.	Add/ Import SSL certificate to the browsers.	To Add/ Import SSL certificate to the browsers (Refer **Annexure I** for steps).
2.	Internet connectivity is required to check for certificate revocation status.	Check the Internet connectivity at every client machine.

Note for System Administrator(s)		
S. No.	**Activities**	**Remarks**
1.	For eOffice instances hosted in a closed environment (i.e. where internet connectivity is not available, or servers are hosted locally) System Admin should keep updated CRL(s) at CRL download location.	CRL should be downloaded manually by the System Administrator.

Installation Guidelines for Windows OS

For Bulk User:

Administrator(s) can install the Digital Signer Service in silent mode on multiple systems through windows server.

For Single User:

- Locate and select the **Digital Signer Service 7.0.0_x64.msi** file from the downloaded bundle as per the system configuration **(64 bit respectively)**.
- Double click required **msi** file to start the installation as shown in **Fig.2.3:**

Fig.2.3

- A welcome page appears, click **Next** (Next >)button to continue as shown in **Fig.2.4:**

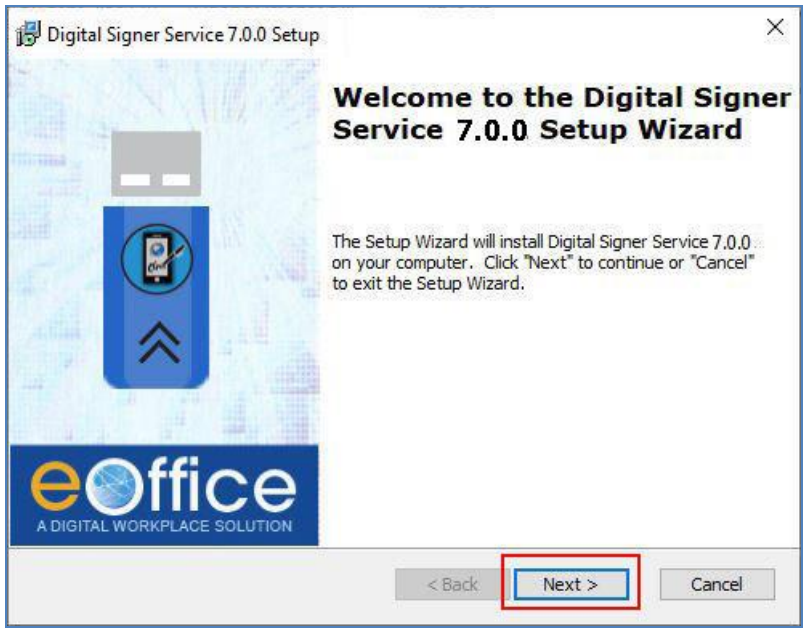


Fig.2.4

- **End-User License Agreement** window appears, read the agreement. Click **I Accept** radio button and then click **Next** (Next >) button as shown in **Fig.2.5**:

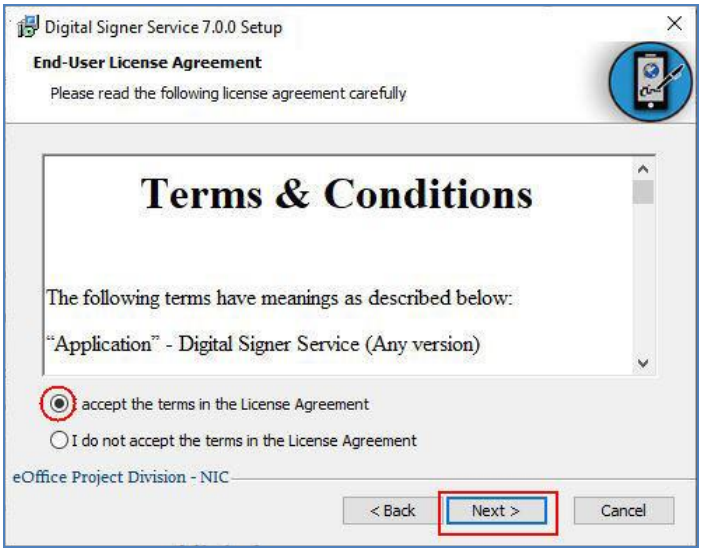


Fig.2.5

- For custom installation, click **Browse (** Browse... **)** button, select the directory as shown in **Fig.2.6** and click **Next (** Next > **)** button.

OR

- For default installation, click **Next (** Next > **)** button, as shown in **Fig.2.6:**

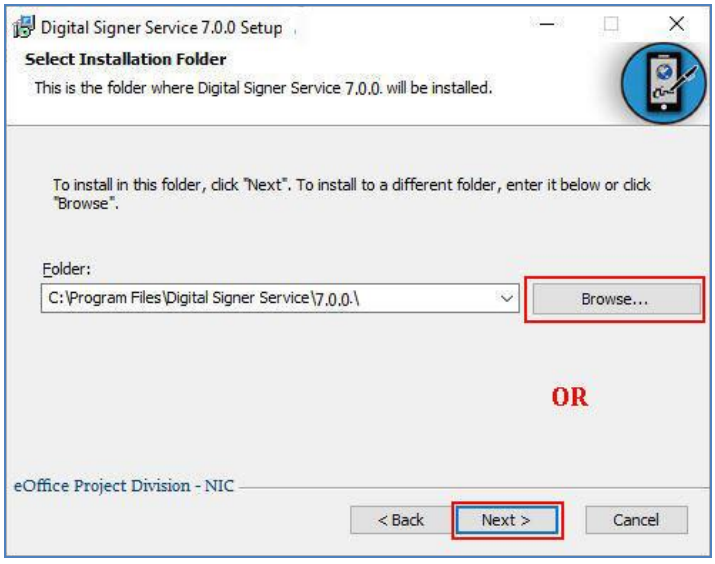


Fig.2.6

- **Install SSL Certificate** (for first time installation at clients' machine) screen appears, select **Yes** radio button and then click **Install** (Install) button as shown in **Fig.2.7 (a):**

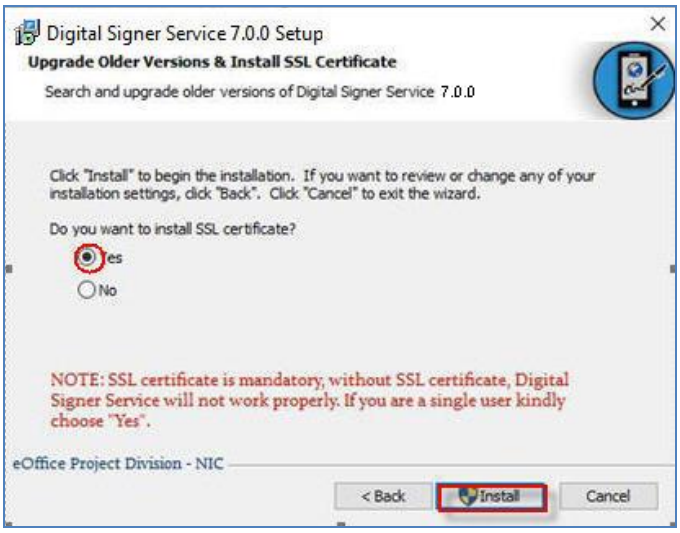


Fig.2.7 (a)

OR

- **Upgrade Older Version & Install SSL Certificate** (previous version exists in clients' machine) window appears asking for **SSL certificate**, now, to remove the older version or for side-by-side installation select the respective option.
- Also, to add **SSL certificate** in Internet Explorer browser, select **Yes** radio button and then click **Install** (Install) button as shown in **Fig.2.7 (b):**

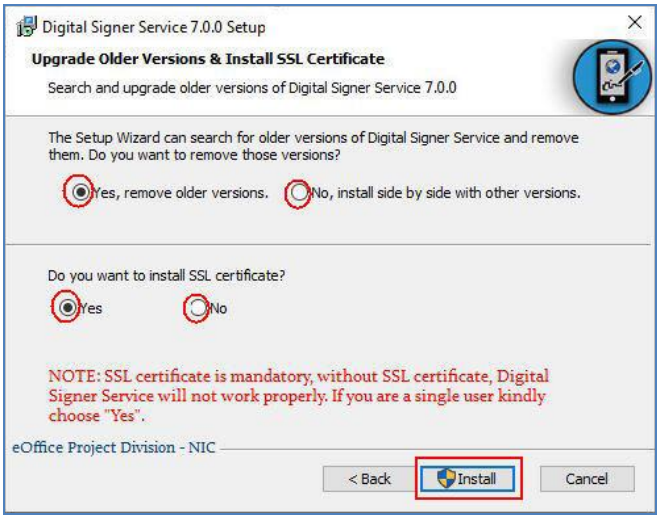


Fig.2.7 (b)

Note:

SSL certificate is mandatory for signing purpose, if user clicks **No** option while installing the Digital Signer Service, then they have to install the certificate manually in Internet Explorer as well (To Add/ Import SSL certificate to the browsers refer **Annexure I**).

- **Side by Side installation:** Process will take some moments to complete the installation and click **Finish** (Finish) button as shown in **Fig.2.8.**
- **Upgrade to new version:** Process will take some moments to uninstall the **Digital Signer Service 6.1.x series** and complete the installation of **Digital Signer Service 7.0.0** and click **Finish (Finish)** button as shown in **Fig.2.8**:

Fig.2.8

Note:
User(s) can run the two different versions of Digital Signer Service simultaneously as per the requirement of consuming applications.

- This completes the installation of **Digital Signer Service 7.0.0** for Windows user(s).
- A shortcut will be created on the desktop, named **Digital Signer Service 7.0.0**.
- Also, a **Digital Signer Service icon** ( ) will appear in the system tray (in the bottom-right corner of monitor) which indicates that Digital Signer Service is running in the system, as shown in **Fig.2.9:**

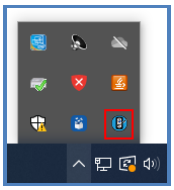


Fig.2.9

- Now, whenever the system is turned on the Digital Signer Service will start automatically.

Steps to manually START/ STOP the Digital Signer Service 7.0.0 are:

- To start the service, double click the desktop icon **"Digital Signer Service 7.0.0"**.
- The service will take a few seconds to start and once it is started it will appear in system tray.
- Right click on the **Digital Signer Service Icon** ( ) from the system tray & select **Open/ Stop** button as per requirement, as shown in **Fig. 2.10**:

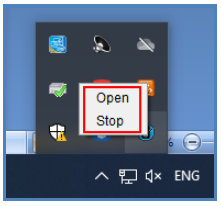


Fig.2.10

- Digital Signer Service application window appears, to stop the service click **Stop Service**(Stop Service) button, as shown in **Fig.2.11**:

Fig.2.11

- **Warning** pop-up window appears, click **Yes** (Yes) button to stop the Digital Signer Service, as shown in **Fig.2.12:**

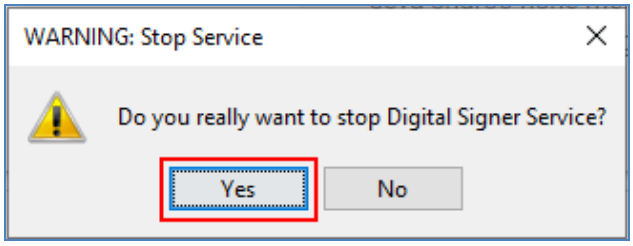


Fig.2.12

- The Digital Signer Service gets stopped and icon will disappear from the system tray.

Change language in Digital Signer Server 7.0.0 (Windows OS)

- To change the language, click  button as shown in **Fig.2.13:**

Fig.2.13

- Select the language and click **Save** button as shown in **Fig.2.14**:

Fig.2.14

- The Digital Signer Service will appear in the selected language as shown in **Fig.2.15**:

Fig.2.15

Note:

1. To import the SSL certificate refer **Annexure I** (Add/ Import SSL certificate to the Browsers).

Section3: MAC

Download the Digital Signer Service 7.0.0 and related utilities (available as a single bundled zip file) from one of the URLs mentioned previously.

Pre-requisites for Digital Signer Service Installer

Following four activities to be completed by User(s).		
S. No.	**Activities**	**Remarks**
1.	Add/ Import SSL certificate to the browsers.	To Add/ Import SSL certificate to the browsers (Refer **Annexure I** for steps).
2.	Internet connectivity is required to check for certificate revocation status.	Check the Internet connectivity at every client machine.
3.	Account password setting.	Account Password is required for installing Digital Signer Service.

Note for System Administrator(s)		
S. No.	**Activities**	**Remarks**
1.	For eOffice instances hosted in a closed environment (i.e. where internet connectivity is not available, or servers are hosted locally) System Admin should keep updated CRL(s) at CRL download location.	CRL should be downloaded manually by the System Administrator.

Installation Guidelines for MAC OS

- Locate the **DigitalSignerService-macos-installer-x64-7.0.1.pkg** file in the downloaded folder as shown in **Fig.3.1**.

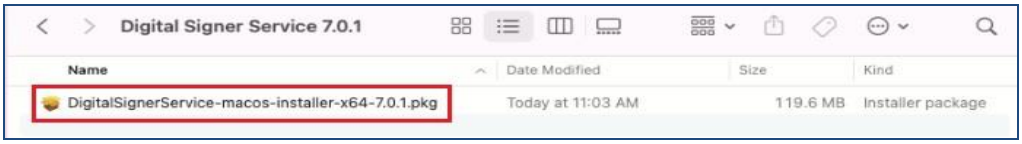


Fig.3.1

- Open the **DigitalSignerService-macos-installer-x64-7.0.1.pkg** file.

- While installing the Digital Signer Service 7.0.1 for the first time, a security prompt will prevent the installation process as MAC OS cannot identify the developer of the application, so click OK (OK) button as shown in **Fig.3.2**:

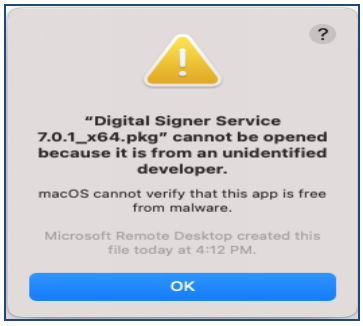


Fig.3.2

- In order to allow the installation process, open **Security & Privacy** in **System Preferences** as shown in **Fig.3.4**:

Fig.3.3

- Under **General Tab**, Click **Open Anyway** (Open Anyway) button shown adjacent to the Digital Signer Service 7.0.1 application in **Allow apps downloaded from** as shown in **Fig.3.4**:

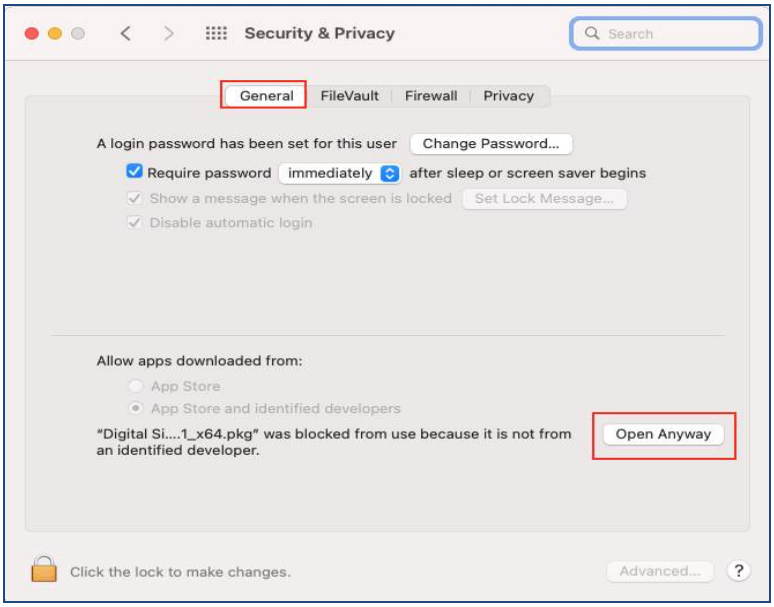


Fig.3.3

- After this, again open the **DigitalSignerService-macos-installer-x64-7.0.1.pkg** file.

- Click **Open** (Open) button on the security prompt that appears in order to allow and start the installation process as shown in **Fig.3.4**:

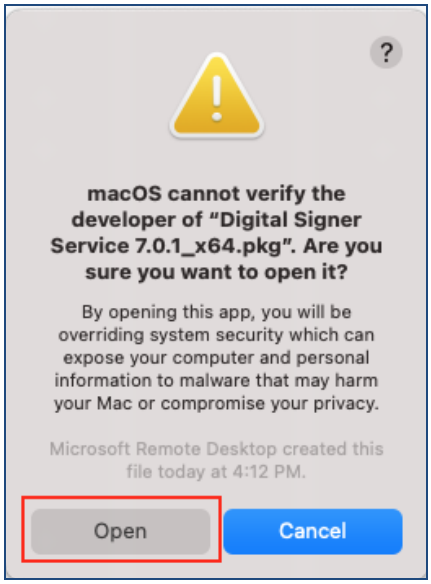


Fig.3.4

- Click **Continue** (Continue) button on the screen that appears as shown in **Fig.3.5**:

Fig.3.5

Note:

When the application is not being installed the first time (**i.e. Second time installation or later**), then on opening the installer, the next screen/window that will appear will be as shown in **Fig.3.5**.

- Again, Click **Continue** (Continue) button on the screen that appears as shown in **Fig.3.6**:

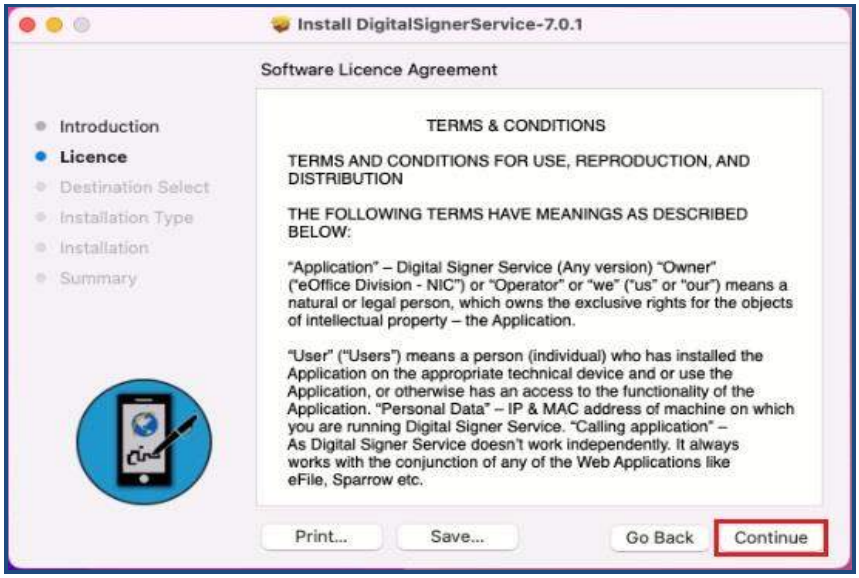


Fig.3.6

- In the following screen, click **Agree** (Agree) button as shown in **Fig.3.7:**

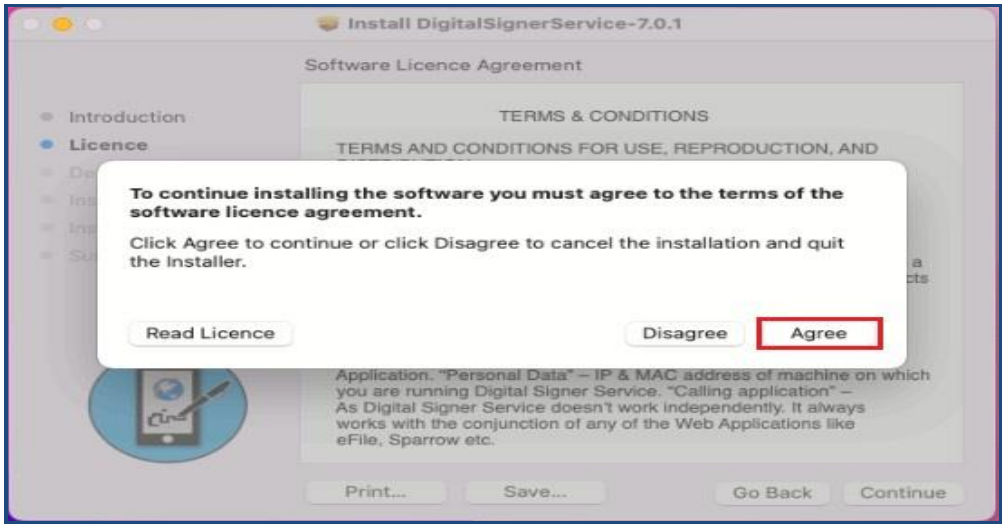


Fig.3.7

- Then, Click **Install** (Install) button as shown in **Fig.3.8**:

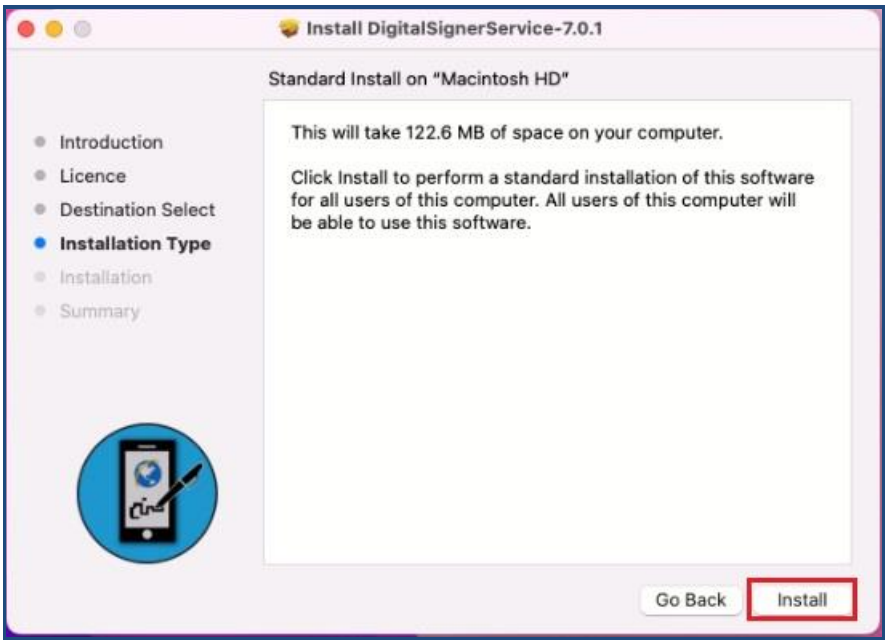


Fig.3.8

- User will be required to enter the System Password in order to proceed the system security pop-up as shown in **Fig.3.9:**

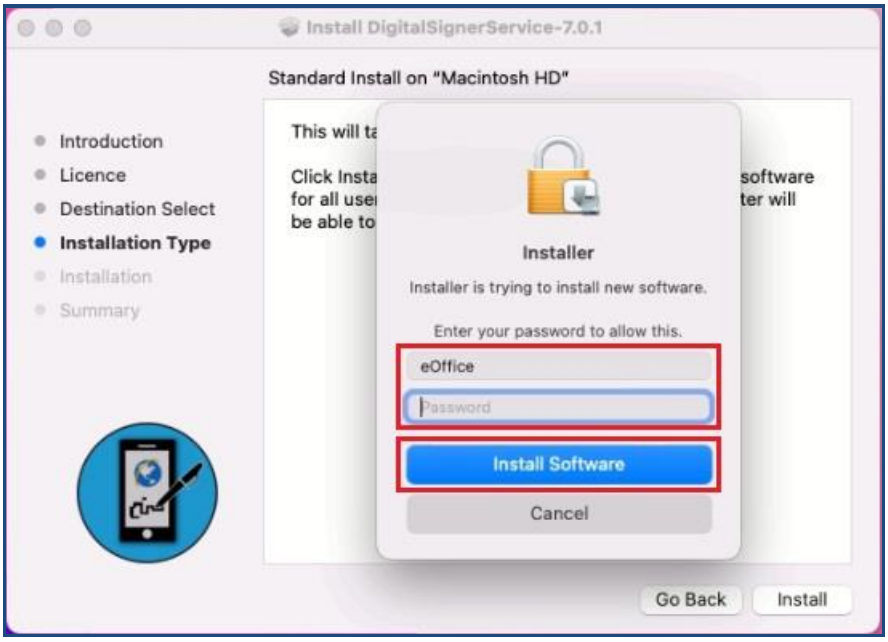


Fig.3.9

- User will be again required to enter System Password in the system security pop-up in order to add SSL Certificate in the browsers as shown in **Fig.3.10**:

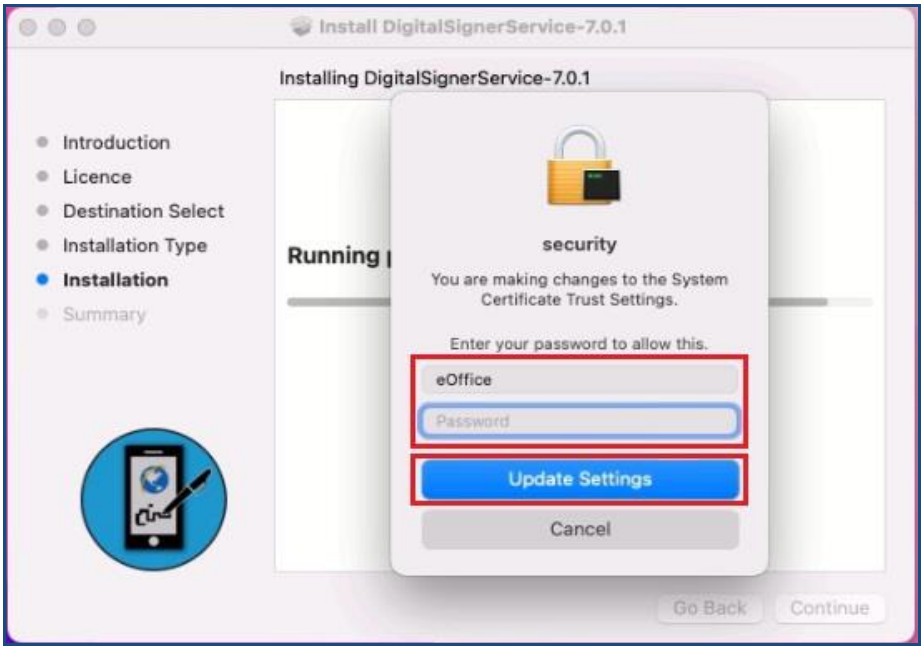


Fig.3.10

- This completes the installation of Digital Signer Service **7.0.1** for MAC and user can close the installation window using the **Close** (Close) button as shown in **Fig.3.11**:

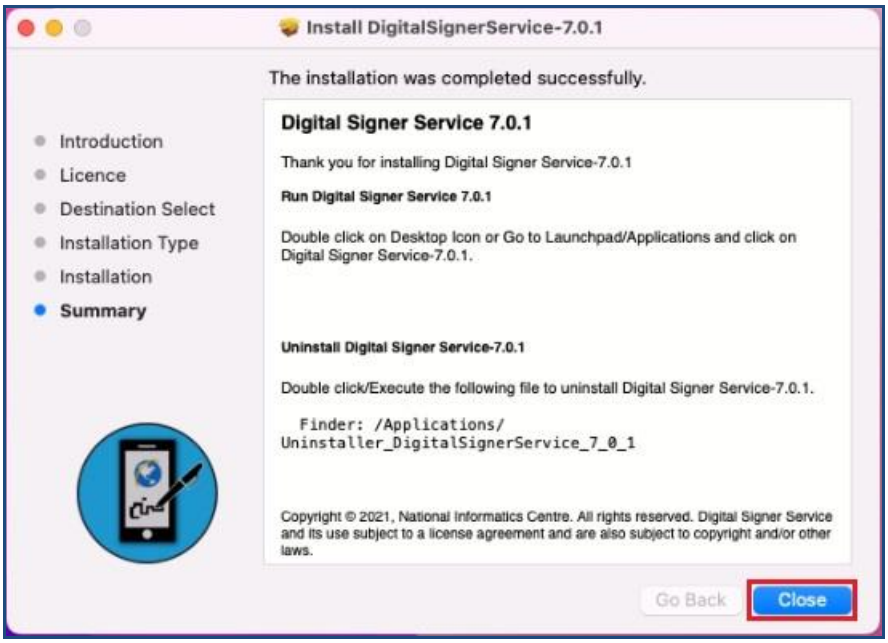


Fig.3.11

- After successful installation, in the pop-up message that appears, user can either retain the installer in the system using **Keep** (Keep) button or delete the installer using **Move to Bin** (Move to Bin) button as shown in **Fig.3.12**:

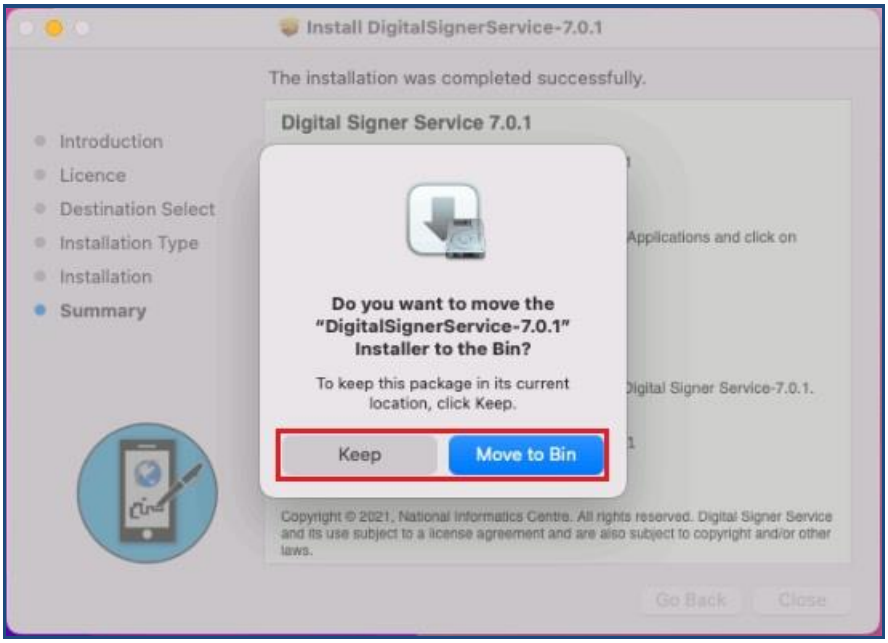


Fig.3.12

- The application can now be accessed either through the Desktop Icon or through the Launchpad icon.

Uninstallation Guidelines for MAC OS

- Open **Finder** window and then Click **Applications** from the left menu as shown in **Fig.3.13**.

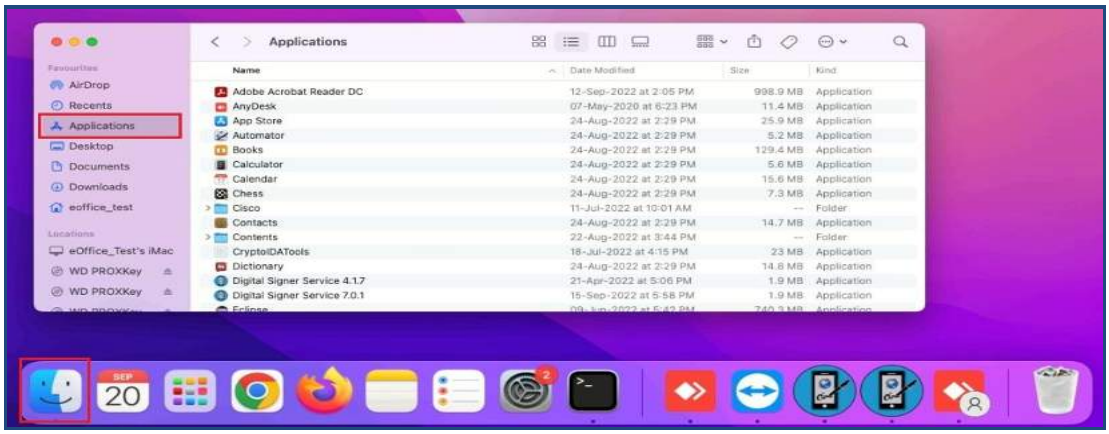


Fig.3.13

- Locate **Uninstaller_DigitalSignerService_7_0_1** from list of applications and Open it as shown in **Fig.3.14**:

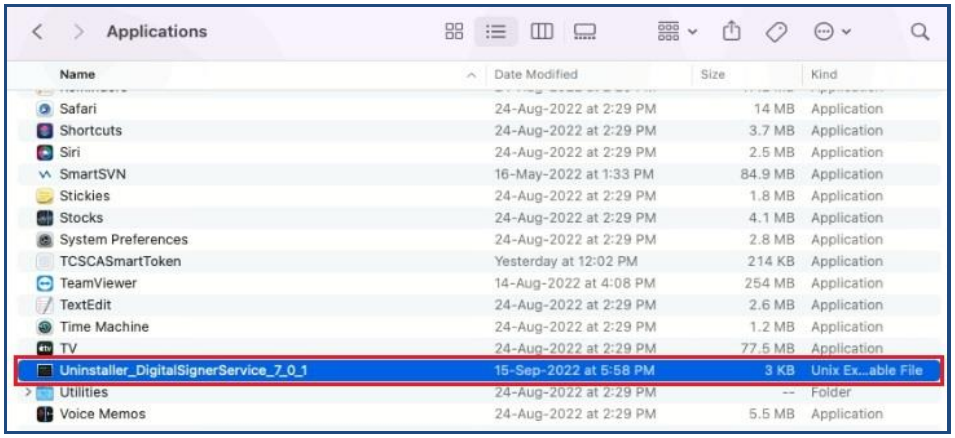


Fig.3.14

- In the following window, enter the System Password in order to proceed with uninstallation process as shown in **Fig.3.15**:

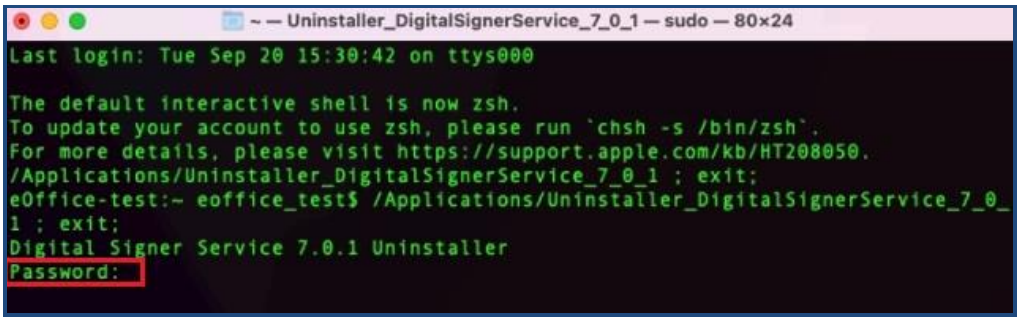


Fig.3.15

- As prompted, enter **Y** to continue the process as shown in **Fig.3.16**:

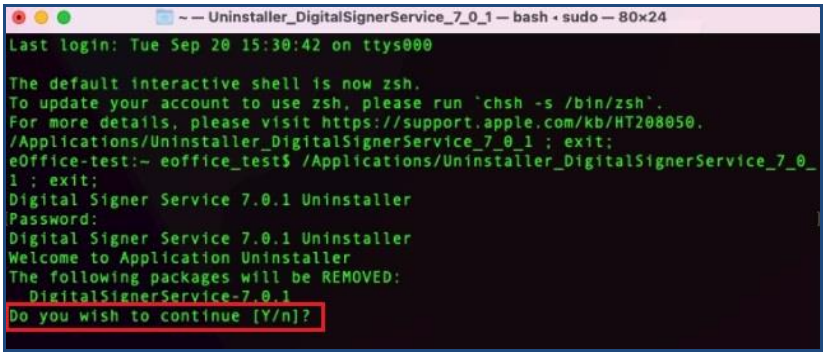


Fig.3.16

- After this, the Digital Signer Service 7.0.1 gets successfully uninstalled from the system as shown in **Fig.3.17**:

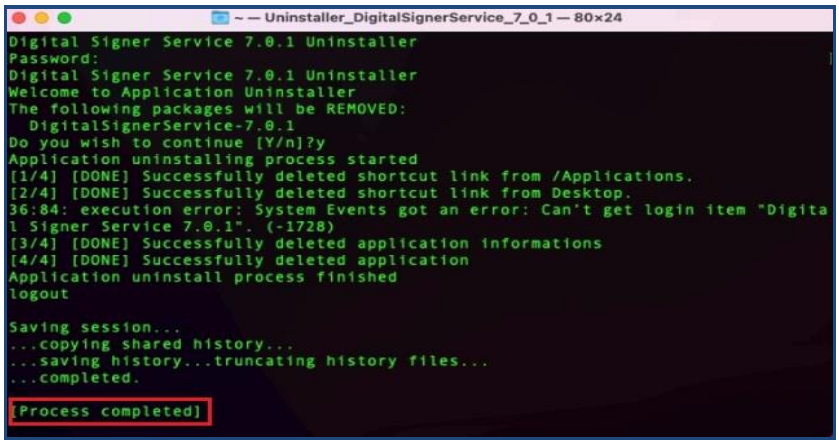


Fig.3.17

In case the Digital Signer Service does not start automatically with system startup, follow the below steps:

- Go to **System Preferences** and click **Users & Group**, as shown in **Fig.3.18**:

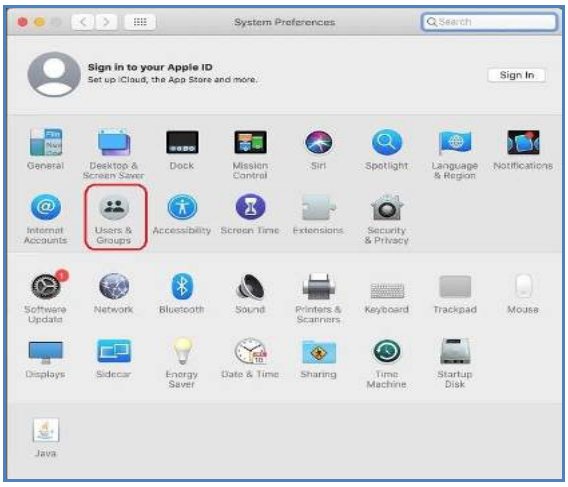


Fig.3.18

- Select **Current Login User**, click **Login Items** tab and then click **+** icon, as shown in **Fig.3.19**:

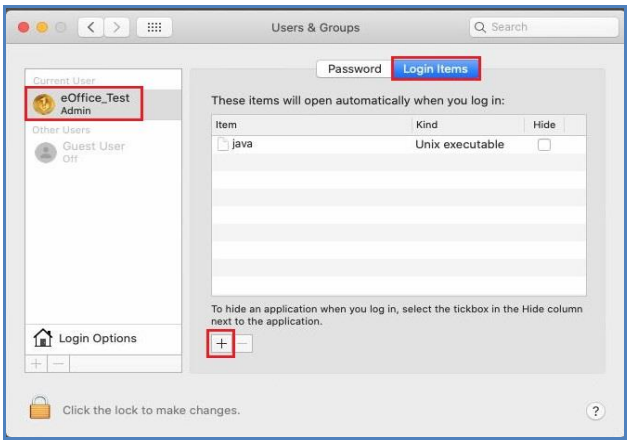


Fig.3.19

- Browse the Digital Signer Service and click the **Add** (

) button, as shown in **Fig.3.20:**

Fig.3.20

- Now, the **Digital Signer Service** will appear under **Users & Group** screen (**Fig.3.21**) and whenever the system is turned on the Digital Signer Service will start automatically.

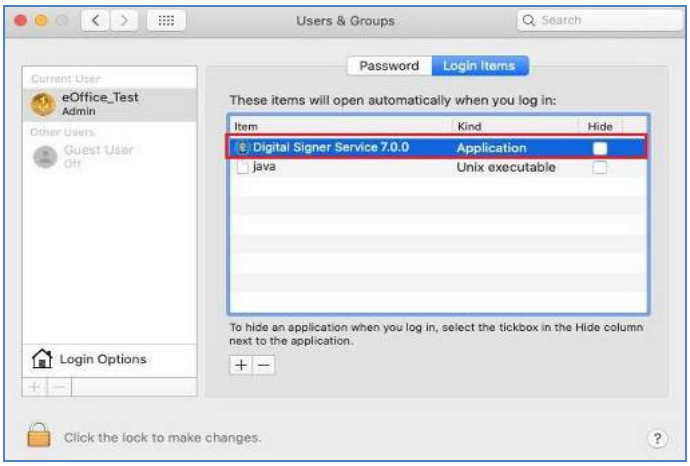


Fig.3.21

Steps to manually START/ STOP the Digital Signer Service 7.0.0 are:

- To start the service, double click the desktop icon () **"Digital Signer Service 7.0.0"**.
- The service will take a few seconds to start and once it is started it will appear in menu bar.
- Left click on the **Digital Signer Service icon** from the menu bar & select **Configure/ Stop** button as per requirement, as shown in **Fig. 3.22**:

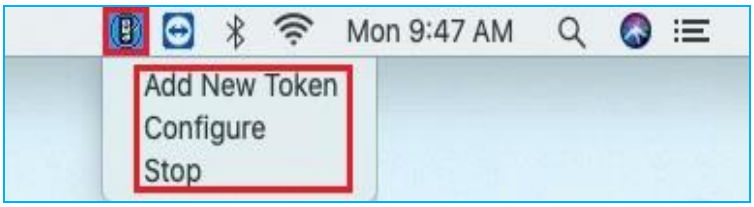


Fig.3.22

- Digital Signer Service application window appears, to stop the service click **Stop Service** (

) button, as shown in **Fig.3.23**:

Fig.3.23

- **Warning** pop-up window appears, click **Yes** (Yes) button to stop the Digital Signer Service, as shown in **Fig.3.24:**

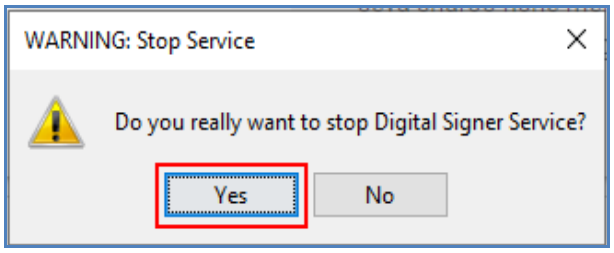


Fig.3.24

- The Digital Signer Service gets stopped and icon will disappear from the menu bar.

Note:

1. While using the Digital Signer Service application if a token is plugged-out or not properly plugged-in before signing, then, occasionally user has to manually restart the Digital Signer Service. This issue is tokens specific, so to avoid this ensure that token is properly plugged-in before proceeding for Signing/Authentication/Registration process. For restarting the Digital Signer Service manually, refer Annexure II (Troubleshooting →**Problem 1**).
2. There are many providers for DSC tokens and sometimes issue(s) specific to DSC token hardware may come, for which the respective vendor may be approached.
3. To import the certificate refer **Annexure I** (Add/ Import SSL certificate to the Browsers).
4. Refer to **Annexure IV** for manually identifying the JAVA, OS and Digital Signer Service status details.

Add Token(s) in Digital Signer Service (MAC OS):

This feature allows the user to use a new token which is not listed in the application. For this first, check whether the token is listed in this application or not. If it is listed then just register this token as default token by checking "register as default token" otherwise proceed to follow the steps to add a new token.

Steps to add new token in Digital Signer Service are:

- Open Digital Signer service app and click **Add New Token** (Add New Token) button, as shown in **Fig.3.25:**

Fig.3.25

Note:

Help: Click Settings ( ) icon for "About and How to add token?" steps.

Fig.3.26

Home ( ): To go back to Home screen of Digital Signer Service

- Provide Token Name, Token Path and click **Save** (

) button, as shown in **Fig.3.27:**

Fig.3.27

Note:

1. Token Name & Token Path is mandatory.
2. User can also copy & paste the Token path in the Digital Signer Service (**Fig.3.27**).
3. The token name should be relevant like if a user is adding token of epass then the token name must include "epass" in its name e.g. epass-new, new-epass, etc.

- Login window appears, enter the **Token Pin** and click **OK** (

) button as shown in **Fig.3.28:**

Fig.3.28

- The certificate list appears, if valid certificate is displayed, click **Confirm** (Confirm) button, else click **Reject** (Reject) button, as shown in **Fig.3.29:**

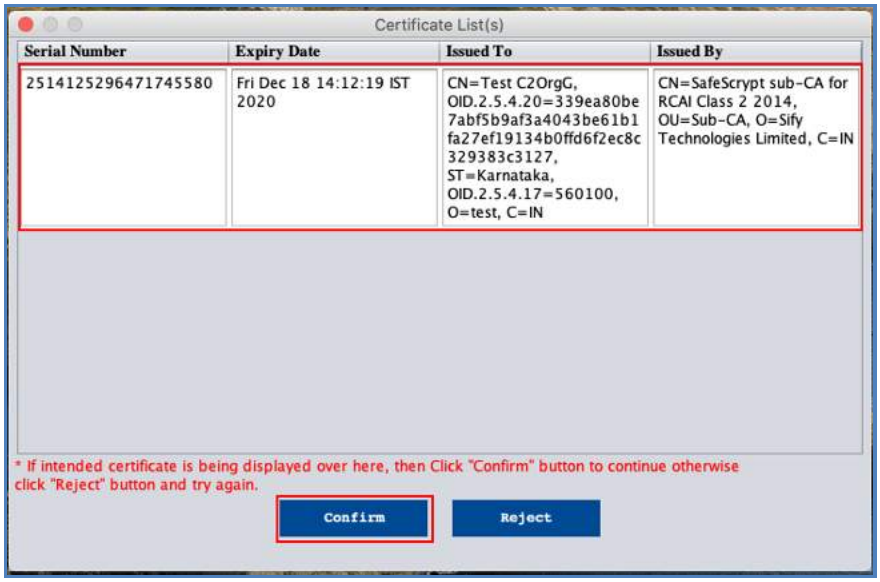


Fig.3.29

- Token details get added successfully, click **OK** (OK) button as shown in **Fig.3.30:**

Fig.3.30

Note:

1. Similarly, user can add more new token(s).
2. This is a one-time activity, so it is not required to add already existing/added token again while using the Signer Service.

Register Token in Digital Signer Service (MAC OS):

Steps to register the token with Digital Signer Service are:

- Left click the menu bar icon "  ", click **Configure** option, as shown in **Fig.3.31**:

Fig.3.31

- The digital Signer Service window appears, select token from the drop-down list, as shown in **Fig.3.32:**

Fig.3.32

- Token path for the selected token gets populated in the Token Path Field.
- Select checkbox for setting the token as default token, as shown in **Fig.3.33:**

Fig.3.33

- Confirmation window appears, click **Yes** (Yes) button as shown in **Fig.3.34**:

Fig.3.34

Change language in Digital Signer Server 7.0.0 (MAC OS)

- To change the language, Click **Settings** button as shown in **Fig.3.35:**

Fig.3.35

- Following window will appear as shown in **Fig.3.36**:

Fig.3.36

- Select the language as shown in **Fig.3.37**:

Fig.3.37

- Click the **Save** (

) button as shown in **Fig.3.38**:

Fig.3.38

- The Digital Signer Service will appear in the selected language as shown in **Fig.3.39**:

Fig.3.39

Note:

1. It is mandatory for singing purpose to set the selected token as default.
2. In case the Token is not availabe in Token Name dropdown list, then Add the token (refer Steps to add new token in Digital Signer Service)

Section4: Ubuntu

Download the Digital Signer Service 7.0.0 and related utilities (available as a single bundled zip file) from one of the URLs mentioned previously.

Pre-requisites for Digital Signer Service Installer for Ubuntu OS

Following four activities to be completed by User(s).		
S. No.	**Activities**	**Remarks**
1.	Add/ Import SSL certificate to the browsers.	To Add/ Import SSL certificate to the browsers (Refer **Annexure I** for steps).
2.	Internet connectivity is required to check for certificate revocation status.	Check the Internet connectivity at every client machine.
3.	Account password setting.	Account Password is required for installing Digital Signer Service.

Note for System Administrator		
S. No.	**Activities**	**Remarks**
1.	For eOffice instances hosted in a closed environment (i.e. where internet connectivity is not available, or servers are hosted locally) System Admin should keep updated CRL(s) at CRL download location.	CRL should be downloaded manually by the System Administrator.

Installation Guidelines for Ubuntu OS

- Locate the **Digital_Signer_Service-7.0.0.sh** file from the downloaded bundle (**Digital Signer Service 7.0.0 Ubuntu Installer folder, Fig.4.1**).

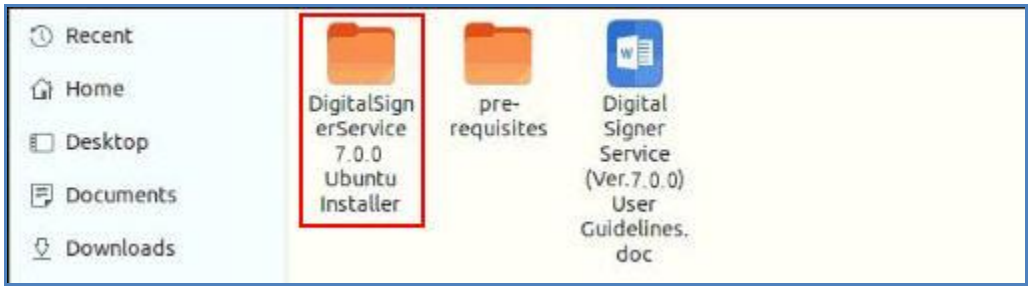


Fig.4.1

- Go to the downloaded location of **Digital_Signer_Service-7.0.0.sh** file and open the terminal.
- Run the command "***sudo bash Digital_Signer_Service-7.0.0.sh***" on the terminal for Ubuntu OS.
- Then, provide account password (if required) and press **Enter**.
- In case other process is using port 55103, system will ask user for **YES/NO** as shown in **Fig.4.2**:
- Type '**Y**' for terminating that process and continue installation of Digital Signer Service otherwise type '**N**' for terminating the Digital Signer Service installation.

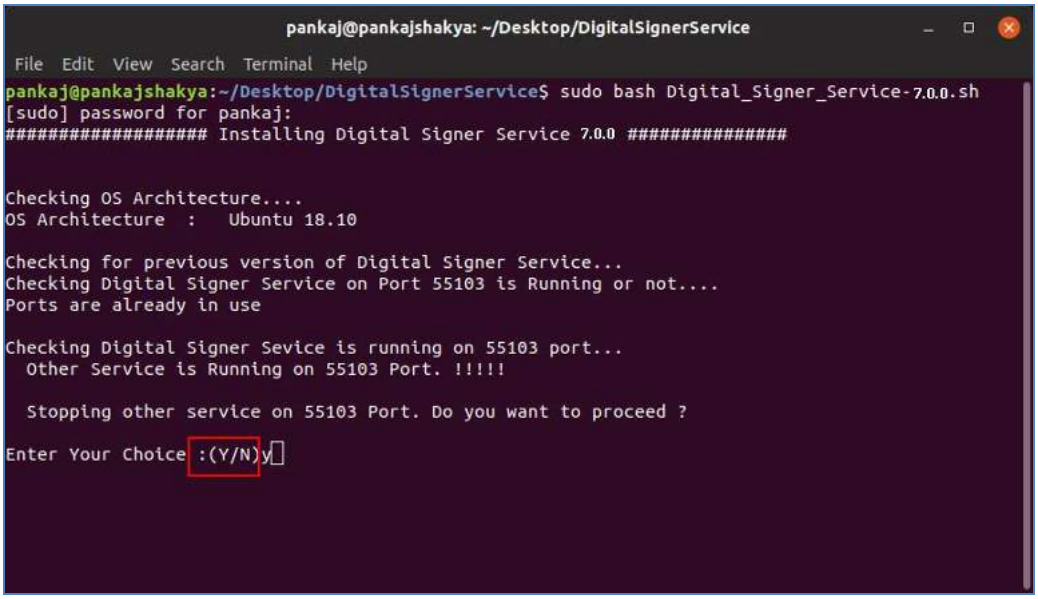


Fig.4.2

- This completes the installation of Digital Signer Service for Ubuntu user(s).

- After successful installation, a message "**Digital Signer Service 7.0.0 installed successfully**" will be displayed as shown in **Fig.4.3:**

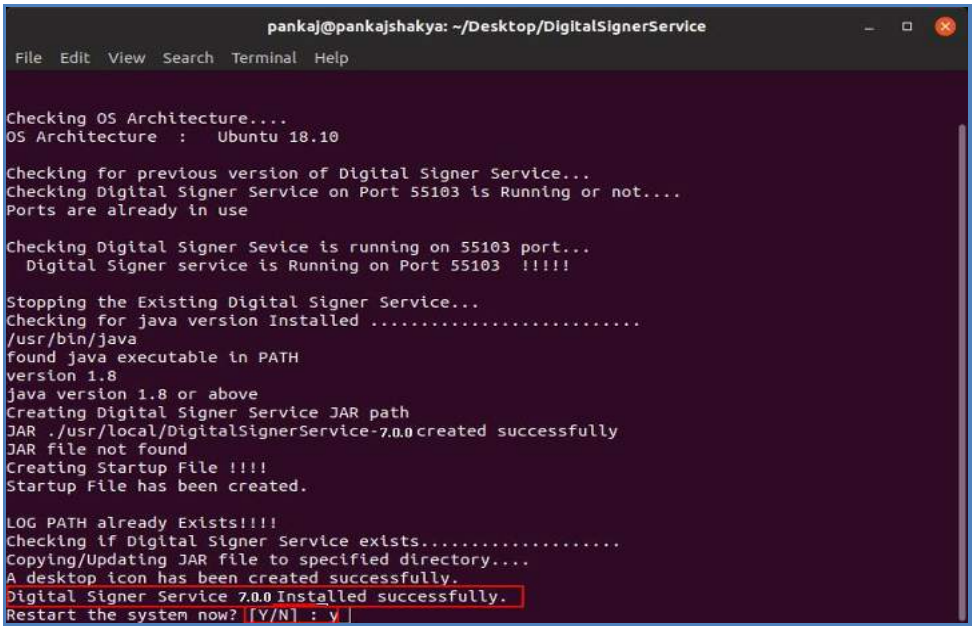


Fig.4.3

- Press '**Y**' to restart the system (**Fig.4.3**) or manually reboot the system.
- Restart is mandatory to run Digital Signer Service 7.0.0 effectively.

Steps to manually START/ STOP the Digital Signer Service 7.0.0 are:

- Double click the desktop icon () **"Digital Signer Service 7.0.0"**.
- The Digital Signer Service pop-up window appears and the service gets started, as shown in **Fig.4.4:**

Fig.4.4

- Now, click **Hide Service** (Hide Service) or ( ) button to hide the screen.
- To Stop the service, click **Stop Service** (Stop Service) button.
- Warning window appears, click Yes (Yes) button to stop the Digital Signer Service, as shown in **Fig.4.5:**

Fig.4.5

- The Digital Signer Service gets stopped.

Note:

1. While using the Digital Signer Service application if a token is plugged-out or not properly plugged-in before signing, then, occasionally user has to manually restart the Digital Signer Service. This issue is tokens specific, so to avoid this ensure that token is properly plugged-in before proceeding for Signing/Authentication/Registration process. For restarting the Digital Signer Service manually, refer Annexure II (Troubleshooting→Problem 1).
2. There are many providers for DSC tokens and sometimes issue(s) specific to DSC token hardware may come, for which the respective vendor may be approached.
3. To import the certificate refer Annexure I (Add/ Import SSL certificate to the Browsers).
4. Refer to Annexure IV for manually identifying the JAVA, OS and Digital Signer Service status details.

Add Token(s) in Digital Signer Service (Ubuntu OS):

This feature allows the user to use a new token which is not listed in the application. For this first, check whether the token is listed in this application or not. If it is listed then just register this token as default token by checking "register as default token" otherwise proceed to follow the steps to add a new token.

Steps to add new token in Digital Signer Service are:

- Open Digital Signer service app and click **Add New Token** (Add New Token) button, as shown in **Fig.4.6:**

Fig.4.6

Note:

Help:Click Seetings ( ) icon for "About and How to add token?" steps.

Fig.4.7

Home ( ): To go back to Home screen of Digital Signer Service

- Provide Token Name, Token Path and click **Save** (

) button, as shown in **Fig.4.8:**

Fig.4.8

Note:

1. Token Name & Token Path is mandatory.
2. User can also copy & paste the Token path in the Digital Signer Service (**Fig.4.8**).
3. The token name should be relevant like if a user is adding token of epass then the token name must include "epass" in its name e.g. epass-new, new-epass, etc.

- Login window appears, enter the **Token Pin** number and click **OK** (

) button as shown in **Fig.4.9:**

Fig.4.9

- The certificate list appears, if valid certificate is displayed, click **Confirm** (Confirm) button, else click **Reject** (Reject) button, as shown in **Fig.4.10:**

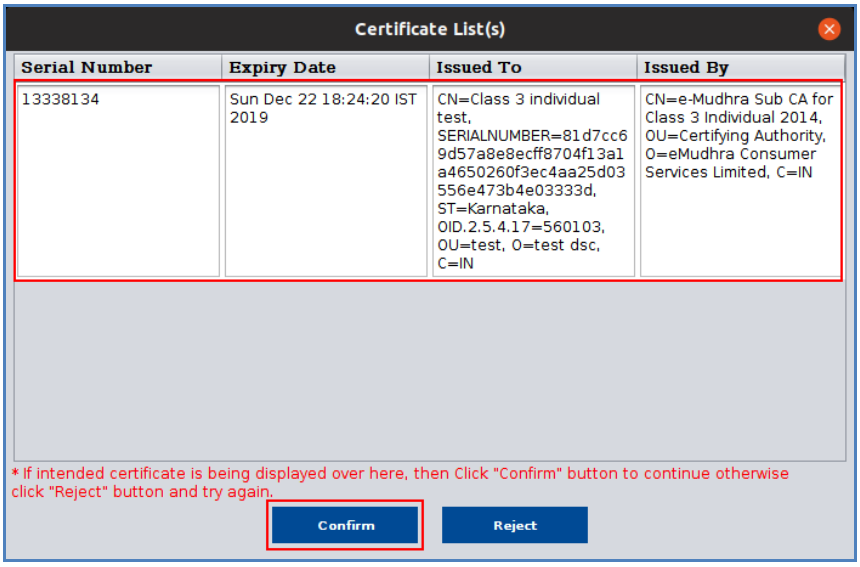


Fig.4.10

- Token details get added successfully, click **OK** (OK) button as shown in **Fig.4.11:**

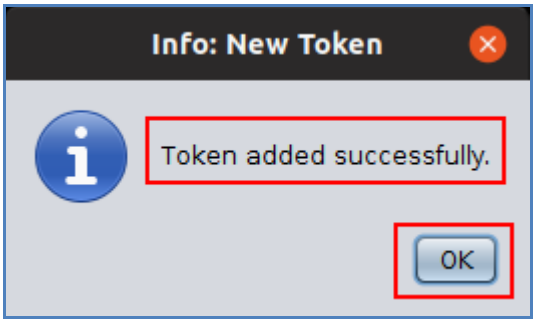


Fig.4.11

Note:

1. Similarly, user can add more new token(s).
2. This is a one-time activity, so it is not required to add already existing or added token again while using the Signer Service.

Register Token in Digital Signer Service(Ubuntu OS):

Steps to register the token with Digital Signer Service are:

- Double click the desktop icon "**Digital Signer Service 7.0.0**".
- The digital Signer Service window appears, select token from the drop-down list, as shown in **Fig.4.12:**

Fig.4.12

- Token path for the selected token gets populated in the Token Path Field.
- Select checkbox for setting the token as default token, as shown in **Fig.4.13:**

Fig.4.13

- Confirmation window appears, click **Yes** (Yes) button as shown in **Fig.4.14**:

Fig.4.14

Change language in Digital Signer Server 7.0.0 (Ubuntu OS)

- To change the language, click **Settings** button as shown in **Fig.4.15:**

Fig.4.15

- Following window will appear as shown in **Fig.4.16**:

Fig.4.16

- Select the language as shown in **Fig.4.17**:

Fig.4.17

- Click the **Save** (

) button as shown in **Fig.4.18**:

Fig.4.18

- The Digital Signer Service will appear in the selected language as shown in **Fig.4.19**:

Fig.4.19

Note:

1. It is mandatory for singing purpose to set the selected token as default.
2. In case the Token is not availabe in Token Name dropdown list, then Add the token (refer Add new token in Digital Signer Service)

Section 5: Checking the Service Status

For Windows/MAC/Ubuntu

Digital Signer Service uses 55103 port.

https port: 55103

The user(s) should check for availability on 55103 port:

1. To check service running status, go to the "**Pre-requisites"** folder inside **Digital Signer Service Installer** folder and then, locate the **DigitalSignerServiceTest.html file**.

2. Open **DigitalSignerserviceTest.html** file in preferred browser and then click **Check Digital Signer Service Status** (Check DSC Signer Service Status) as shown in **Fig.5.1**:

Fig.5.1

3. The running status for HTTPS is shown in **Fig.5.2**:

Fig.5.2

4. To check for service status manually use https://eoffsigner.eoffice.gov.in:portNumber/check/isLive
   For Ex. https://eoffsigner.eoffice.gov.in:55103/check/isLive

"**Success**" message on the screen states that the service is running successfully otherwise may refer to the Annexure II (Troubleshooting).

Note :

1. The Digital Signer Service SSL certificate will expire on 15 Oct 2023. After that, a new installer will be provided with the new SSL certificate.

Annexure I

Add/Import SSL Certificate to the Browsers

Digital Signer Service runs on https port by using a self-signed certificate, browser may not import certificate automatically to their trusted root certificate store, for this client needs to import the certificates explicitly.

- Download & unzip the Installer file (For windows/ For MAC/ For Ubuntu), go to the "**Pre-Requisites**" folder and locate the **DSC Self sign → eOfficeCA2022.der/eOfficeCA2022.cer (SSL Certificates)**.

Note:

1. If certificate revocation check is not performed, the application will not be able to perform any of the operations (Registration, Authentication, and Signing).

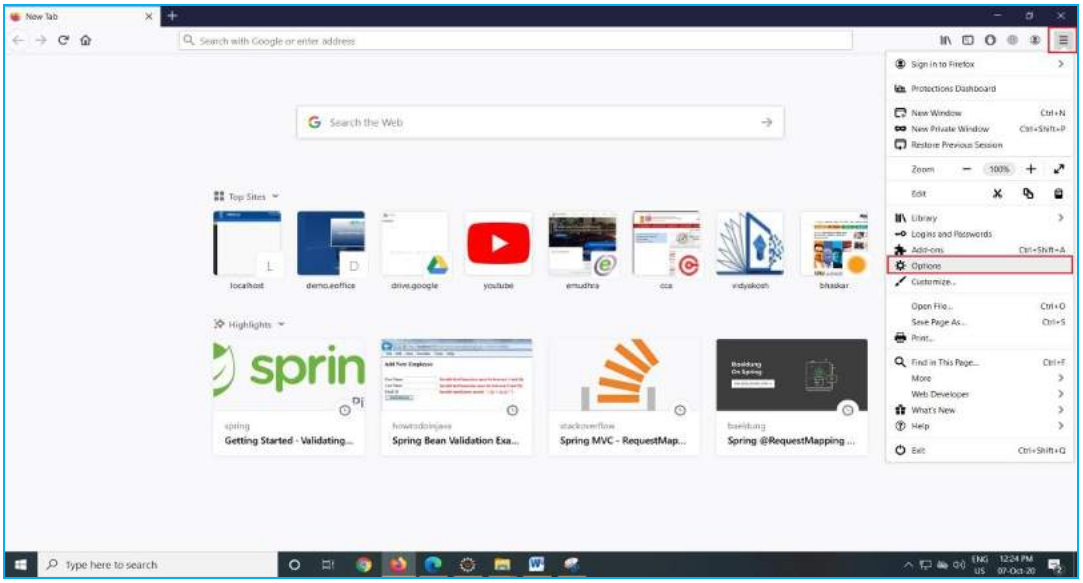
To add/ Import the certificate the steps for browsers are mentioned below:

For Windows

For Mozilla Firefox

To add a self-signed certificate for https in Mozilla Firefox, perform the below actions to import SSL certificate:

- Open Mozilla Firefox browser and Click (☰) icon on Top right Corner and then Click on **Options** (Options) link as shown in **Fig.A.1.1**:



FigA.1.1

- Following window will appear:

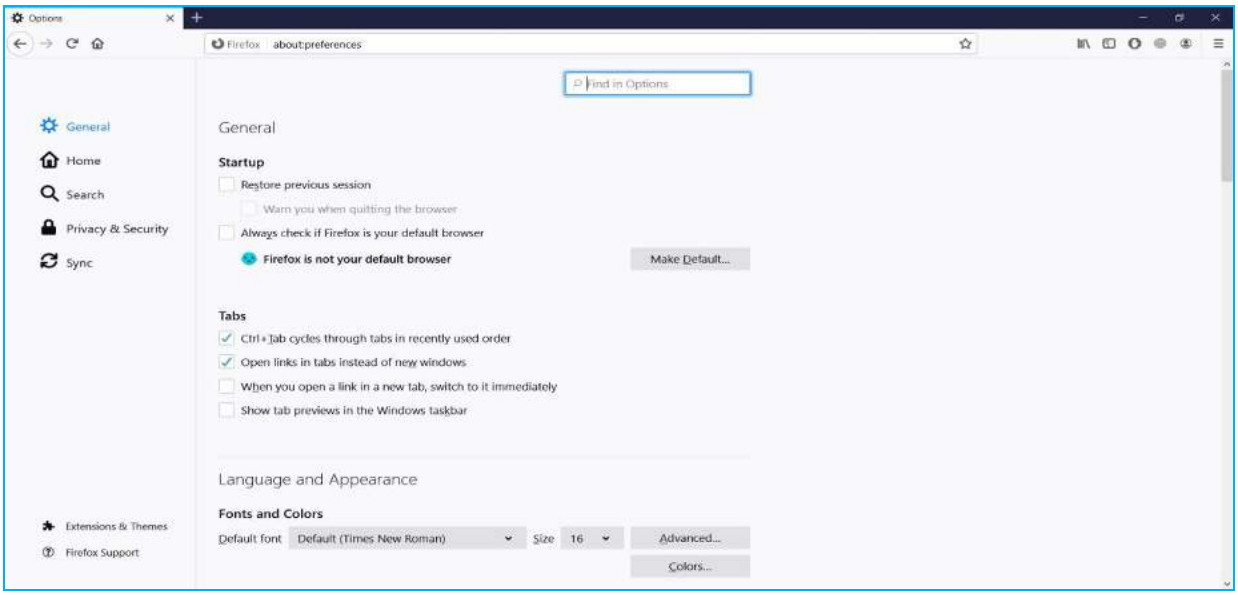


Fig.A.1.2

- Click on **Privacy & Security** (Privacy & Security) link, scroll down and Click **View Certificates** (View Certificates...) button as shown in **Fig.A.1.3**

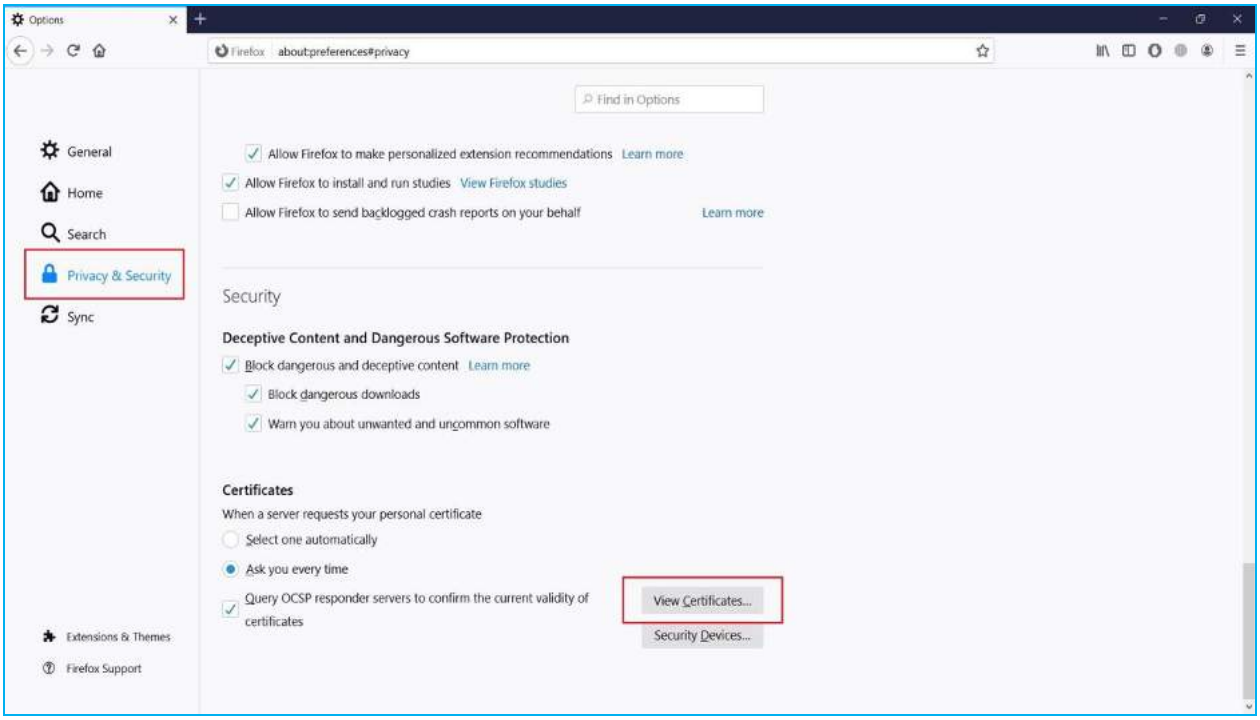


Fig.A.1.3

- A **Certificate Manager** window will appear as shown in **Fig.A.1.4:**

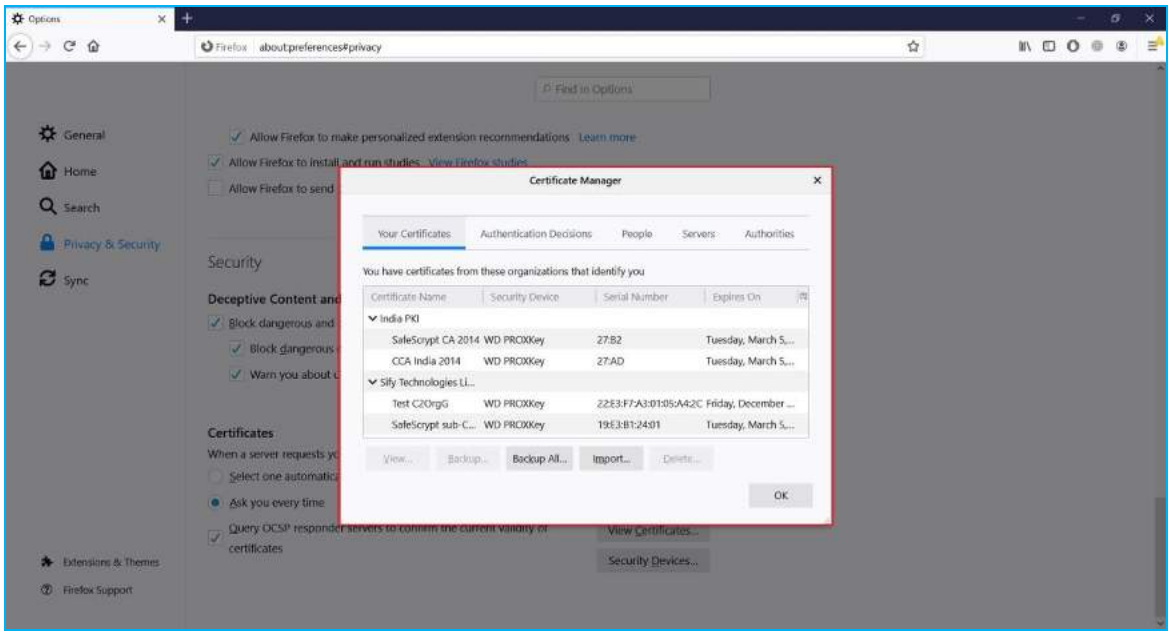
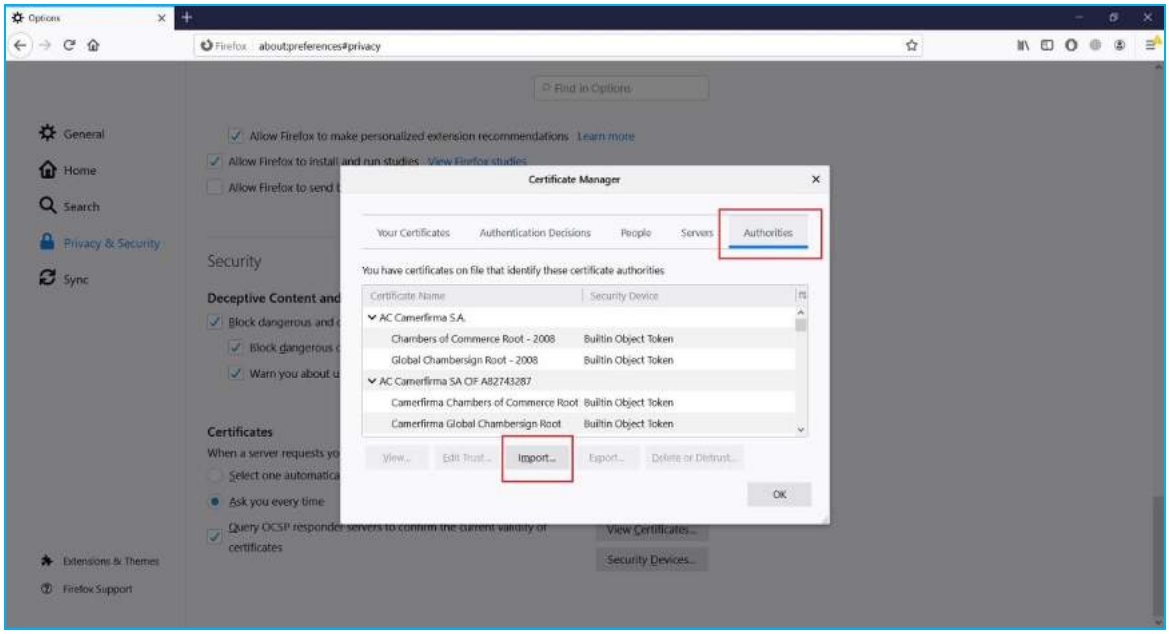


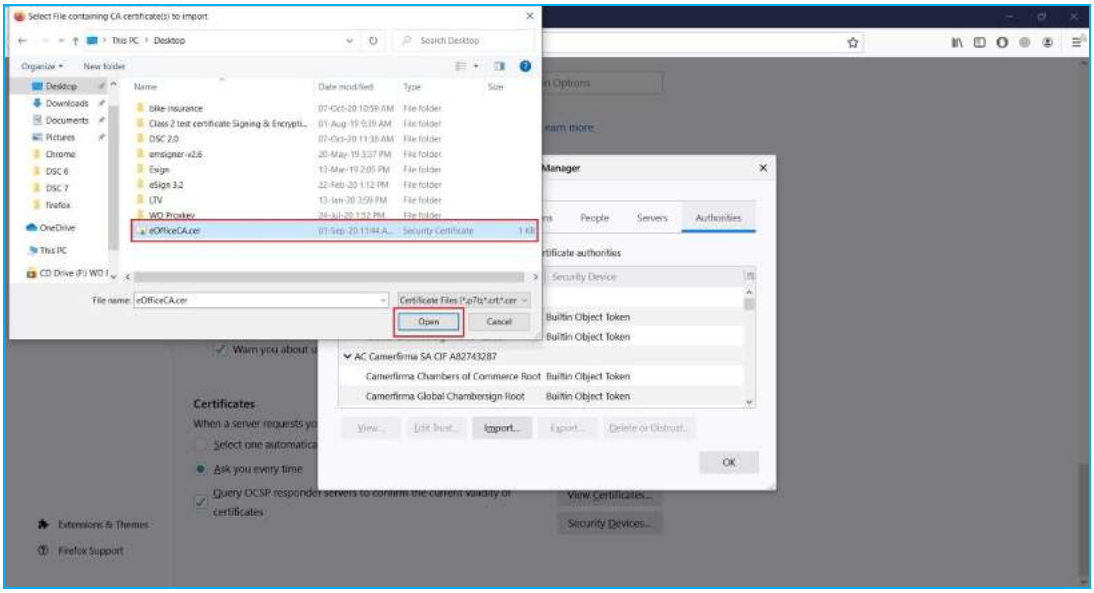
Fig.A.1.4

- Click on **Authorities** (Authorities) tab and then Click **Import** (Import...) button as shown in **FigA.1.5:**



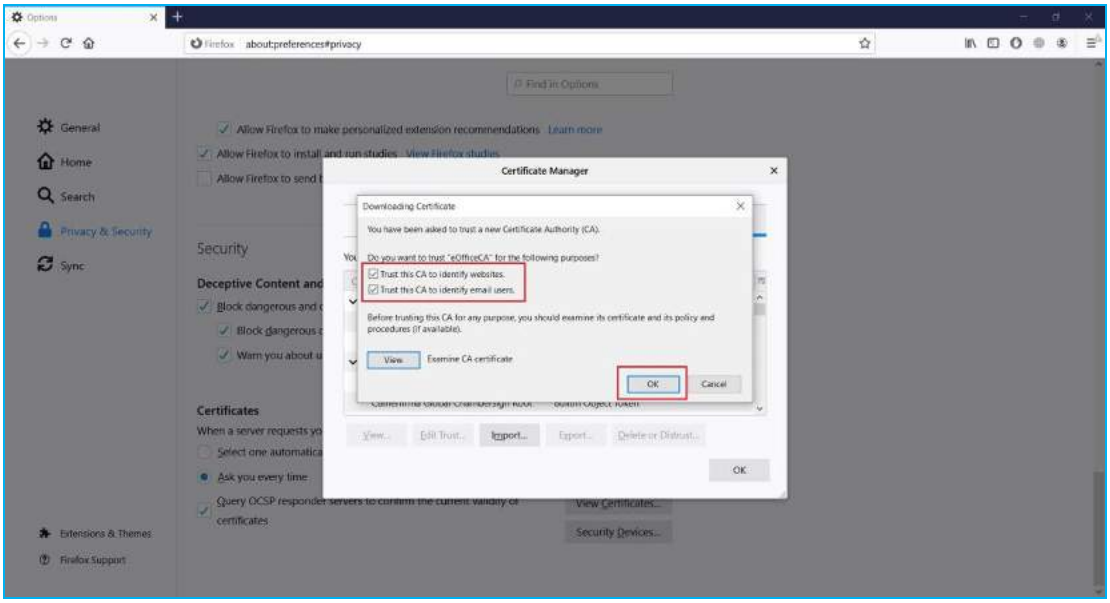
FigA.1.5

- Select the **Certificate** and Click **Open** (Open) button as shown in **FigA.1.6**:



FigA.1.6

- Check both Checkboxes and click on **Ok** (OK) button as shown in **FigA.1.7**:



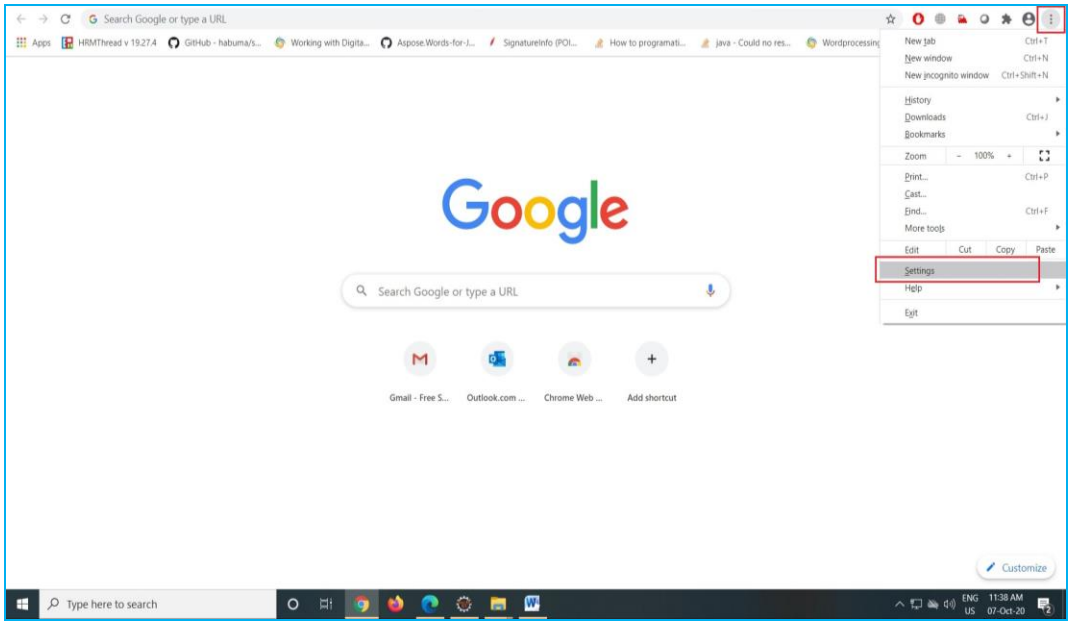
FigA.1.7

- This will import eOffice CA certificate to the Authorities store.

For Chrome

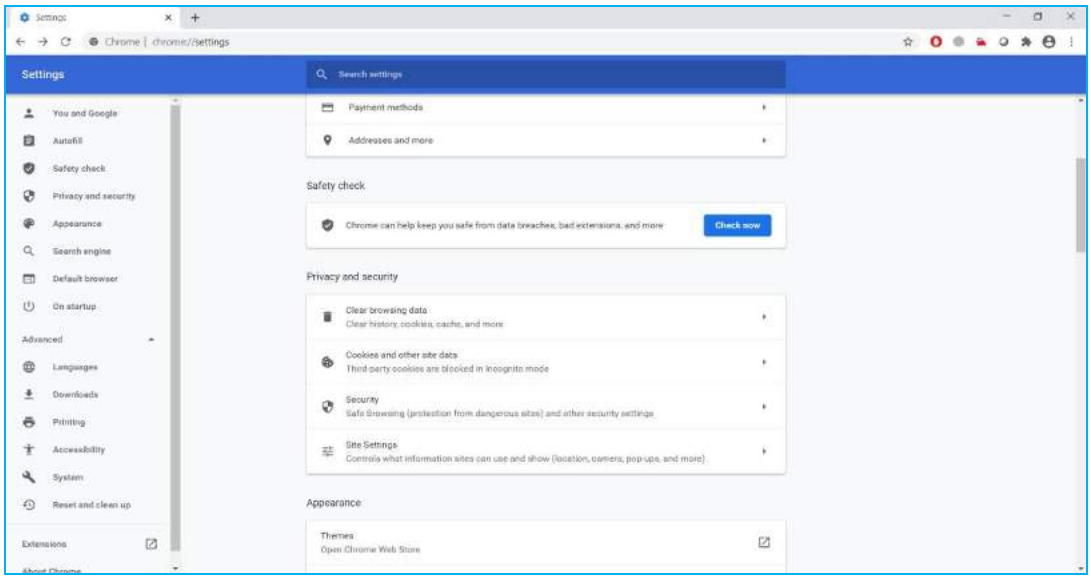
To add a self-signed certificate for https in chrome browser, perform the below actions to import SSL certificate:

- Open Google Chrome and click (⋮) icon on top right corner icon and then click on **Settings** (Settings) link as shown in **FigA.1.8**:



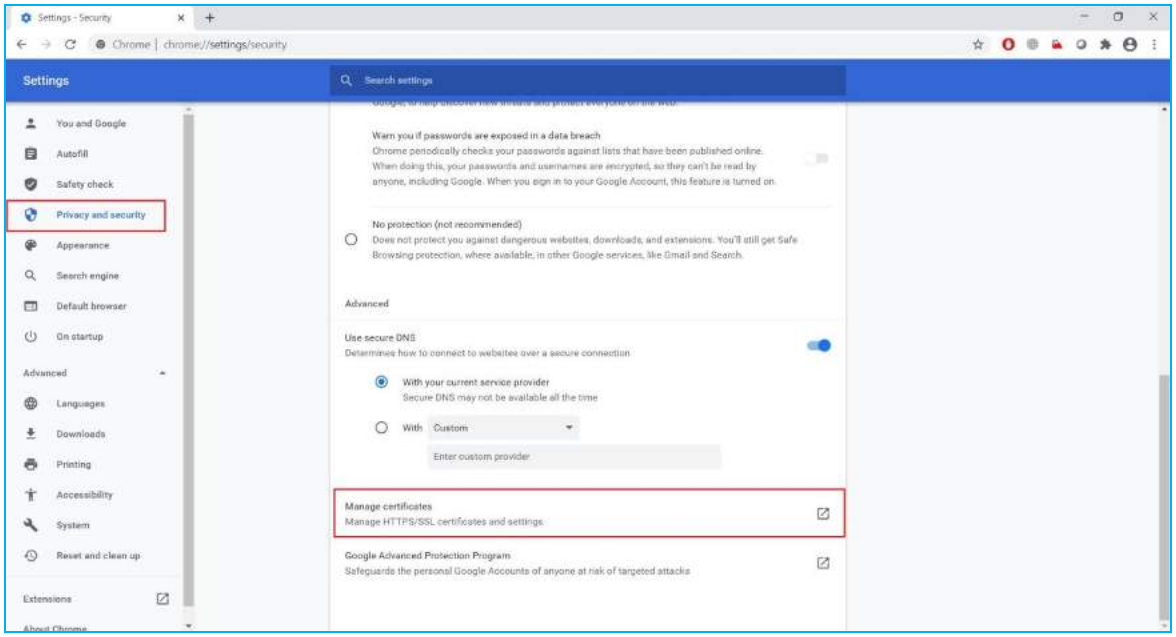
FigA.1.8

- Following window will appear as shown in **FigA.1.9**:



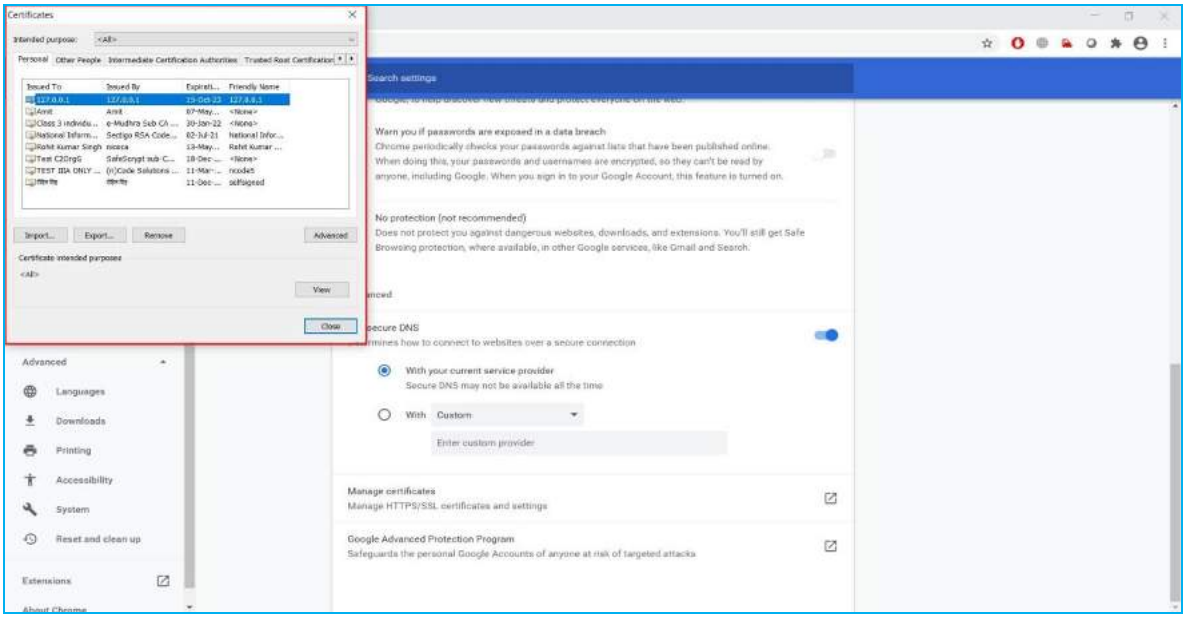
FigA.1.9

- In Left menu, click **Privacy and Security** (Privacy and security) link. Scroll down and click on **Manage certificates** (Manage certificates
Manage HTTPS/SSL certificates and settings) link as shown in **FigA.1.10**



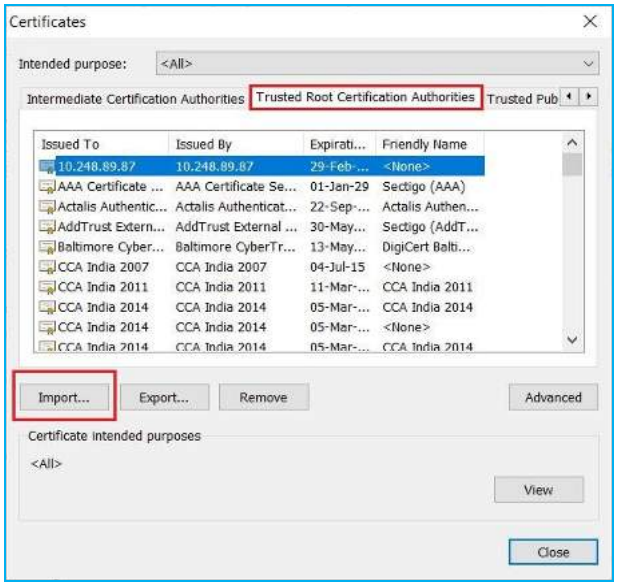
FigA.1.10

- Following Certificates window will appear as shown in **FigA.1.11**:



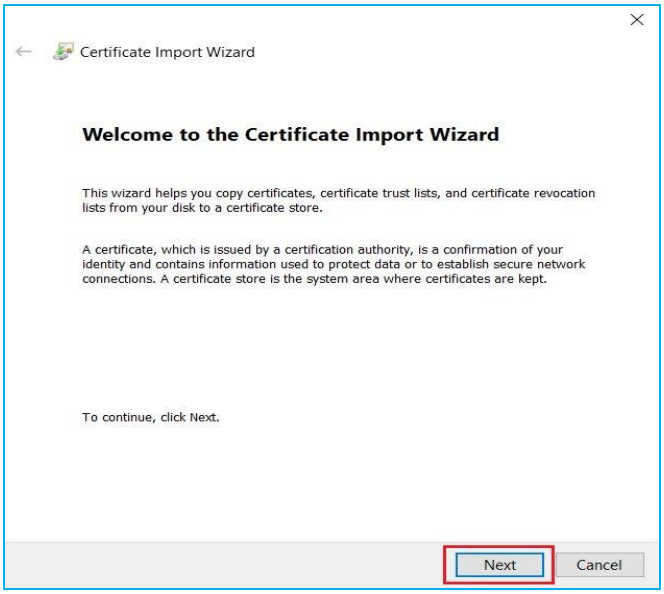
FigA.1.11

- Click **Trusted Root Certification Authorities** (Trusted Root Certification Authorities) tab and click **Import** (Import...) button as shown in **FigA.1.12**.



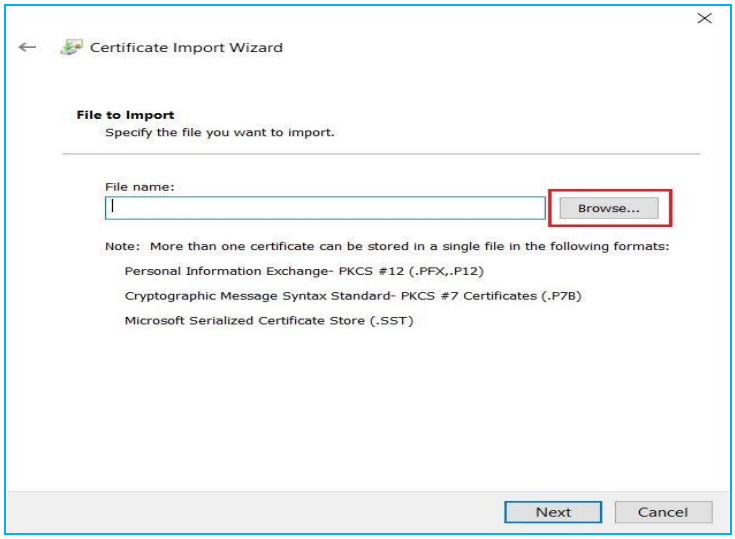
FigA.1.12

- On window that appears, click **Next** (Next) button as shown in **FigA.1.13**:



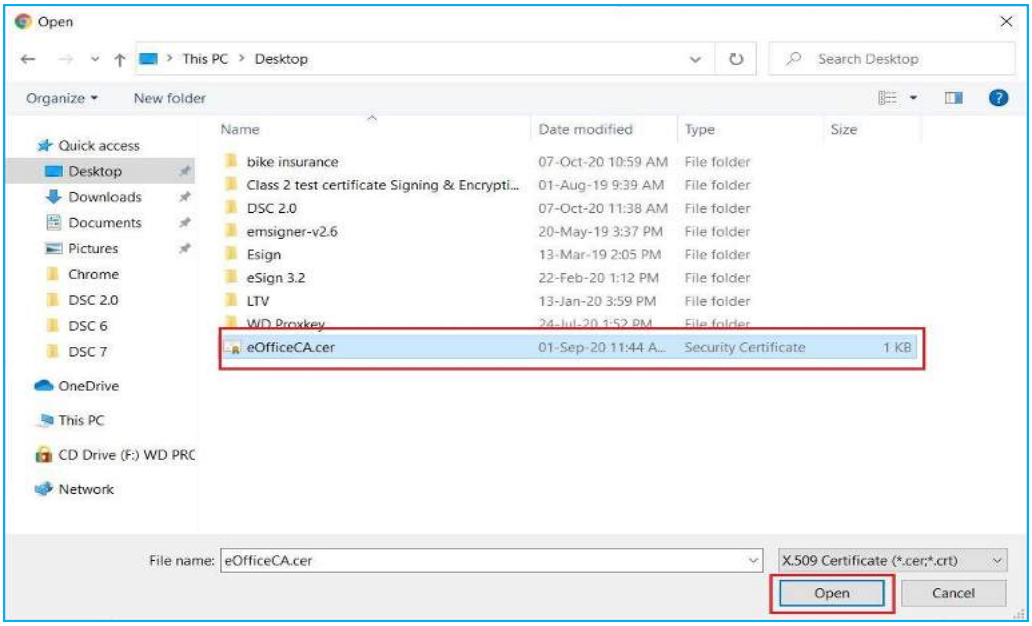
FigA.1.13

- On following window, click **Browse** (Browse...) button as shown in **FigA.1.14**:



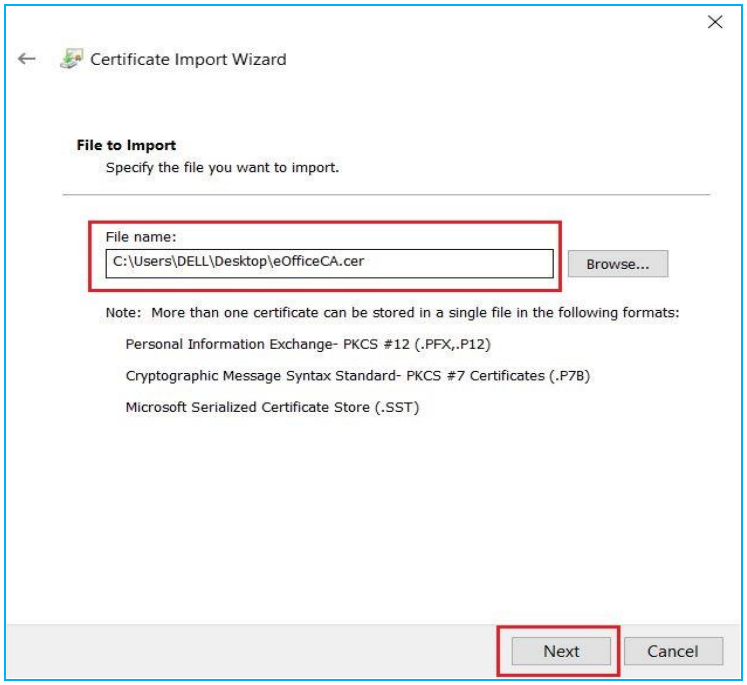
FigA.1.14

- From Dialog window, select the **Certificate** and Click **Open** (Open) button as shown in **FigA.1.15:**



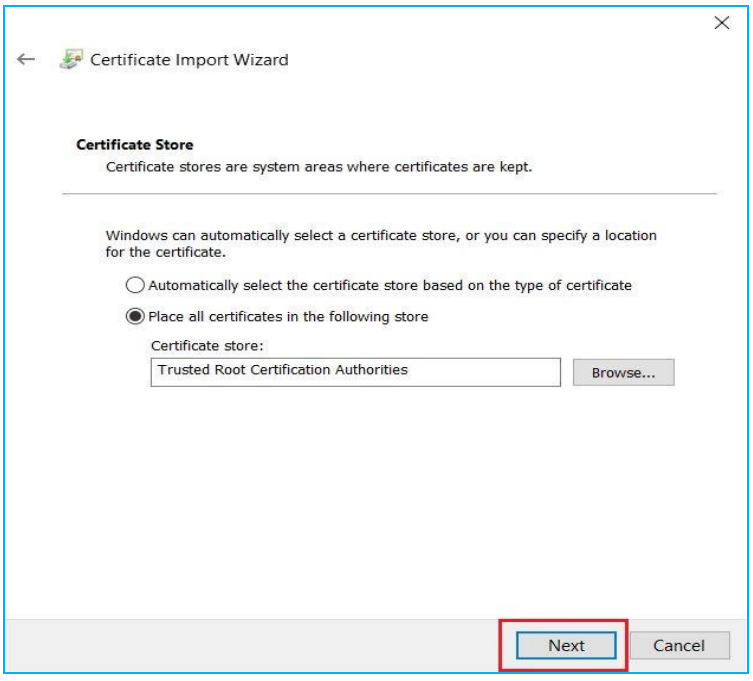
FigA.1.15

- Click the **Next** (Next) button as shown in **FigA.1.16**:



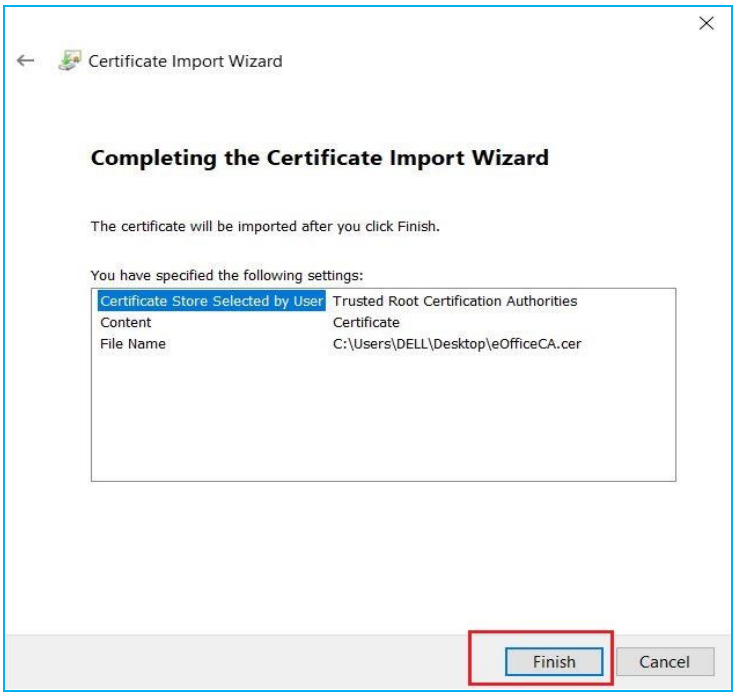
FigA.1.16

- Again click **Next** (Next) button as shown in **FigA.1.17:**



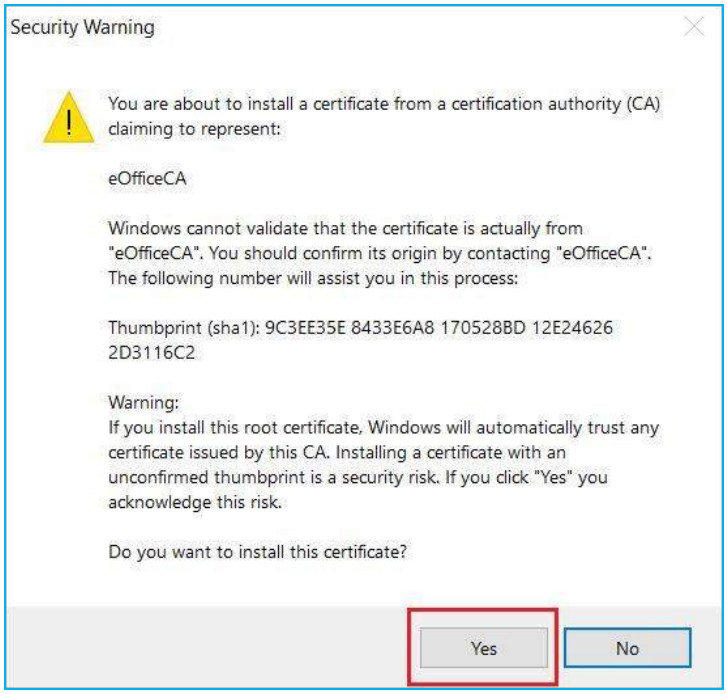
FigA.1.17

- Click on **Finish** (Finish) button as shown in **FigA.1.18**



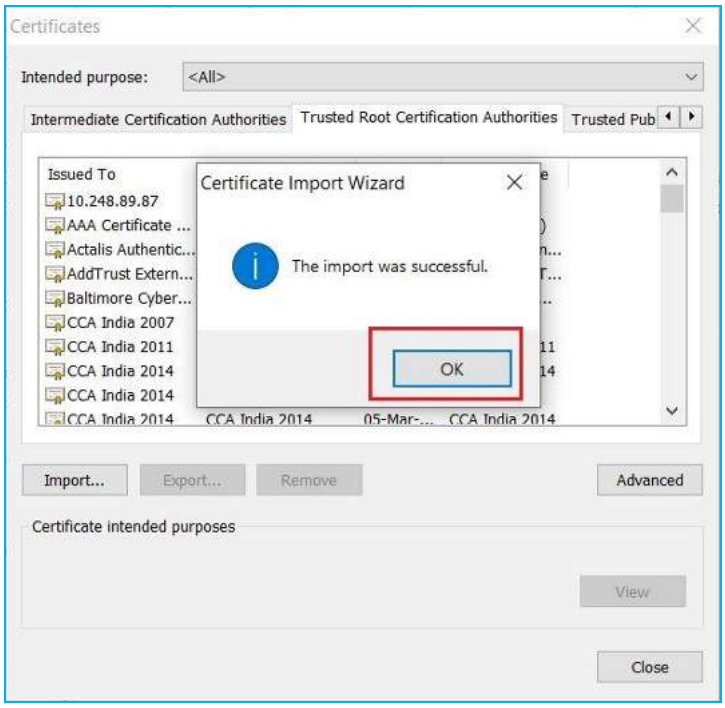
FigA.1.18

- A prompt window will appear, Click **Yes** (Yes) button as shown in **FigA.1.19:**



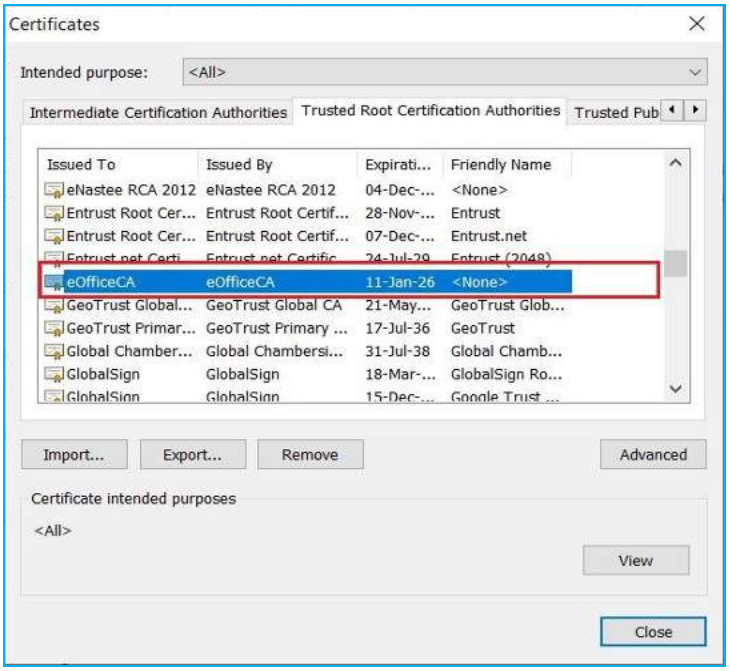
FigA.1.19

- Then Click **Ok** (OK) button in prompt window as shown in **FigA.1.20:**



FigA.1.20

- This will import eOffice CA certificate to Trusted Root Certification Authorities store as shown in **FigA.1.21:**



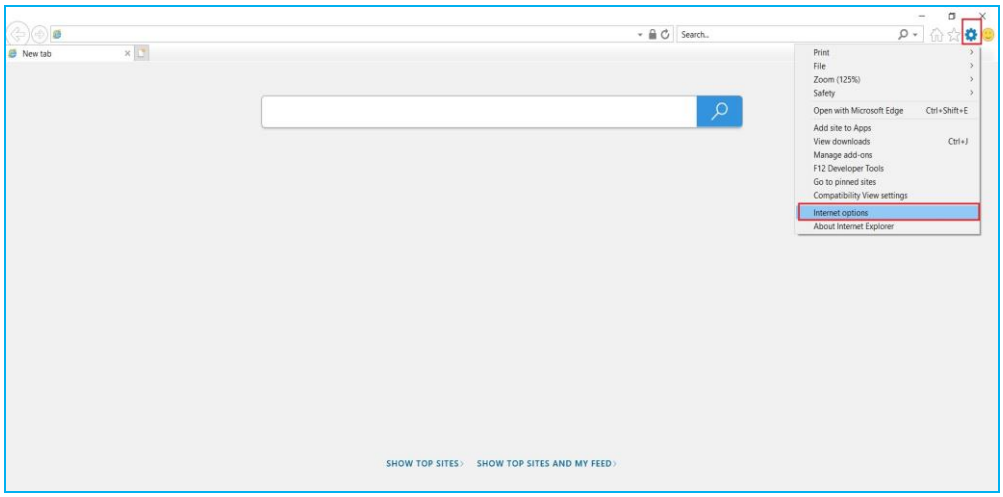
FigA.1.21

For Internet Explorer

In case of Internet Explorer, SSL certificate gets automatically imported by the installer.

Steps to check SSL certificate are:

- Open Internet Explorer and Click ( ) button at top right corner and then Click **Internet options** (Internet options) link as shown in **FigA.1.22:**

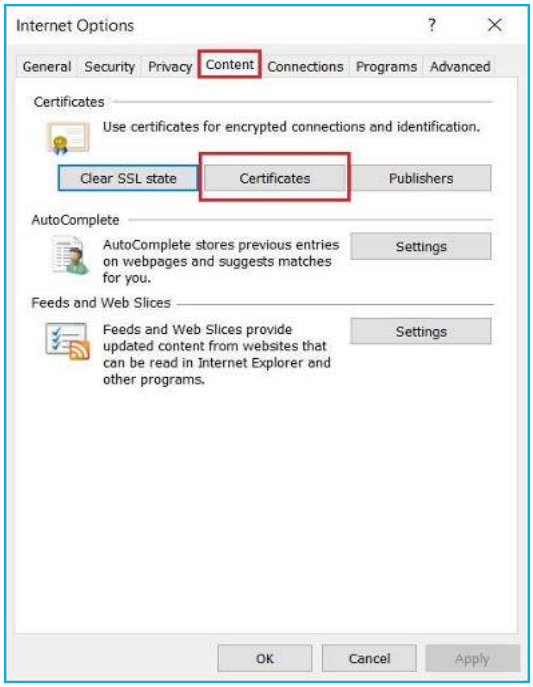


FigA.1.22

- Following Dialog box will appear as shown in **FigA.1.23:**

FigA.1.23

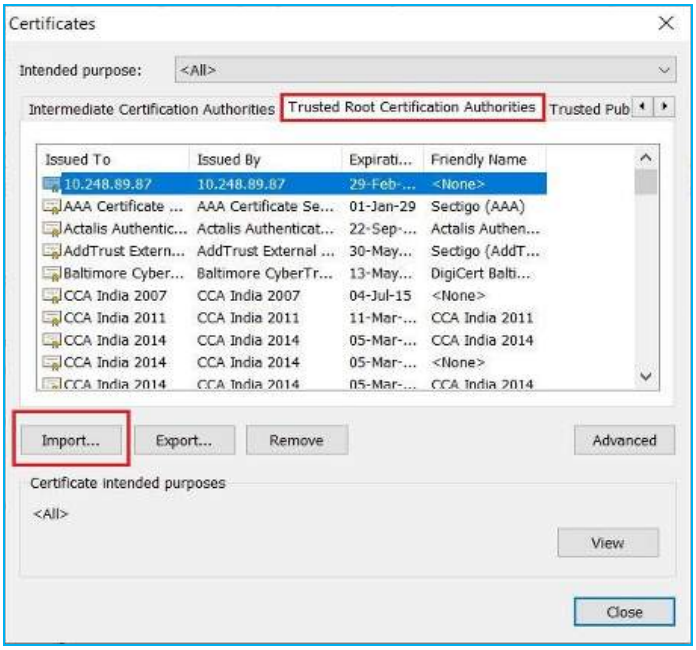
- Click **Content** (Content) tab and then Click **Certificates** (Certificates) button as shown in **FigA.1.24:**



FigA.1.24

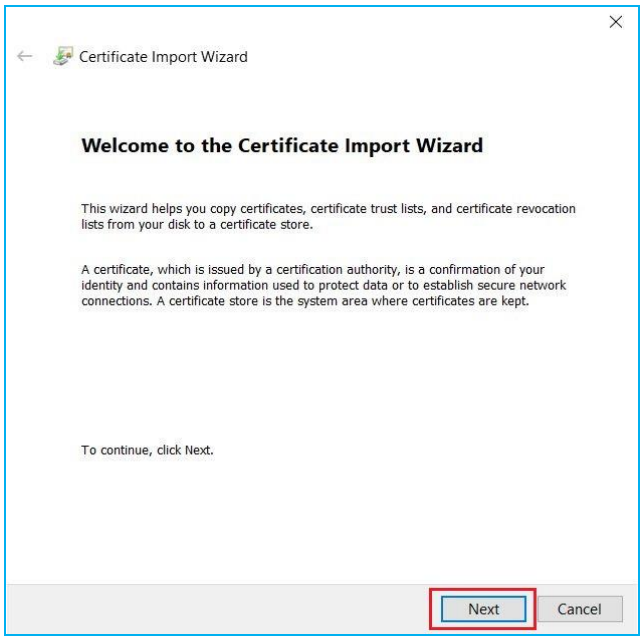
- In the following window, Click **Trusted Root Certification Authorities** (Trusted Root Certification Authorities) tab and then Click **Import** (Import...) button as shown in **FigA.1.25:**

.



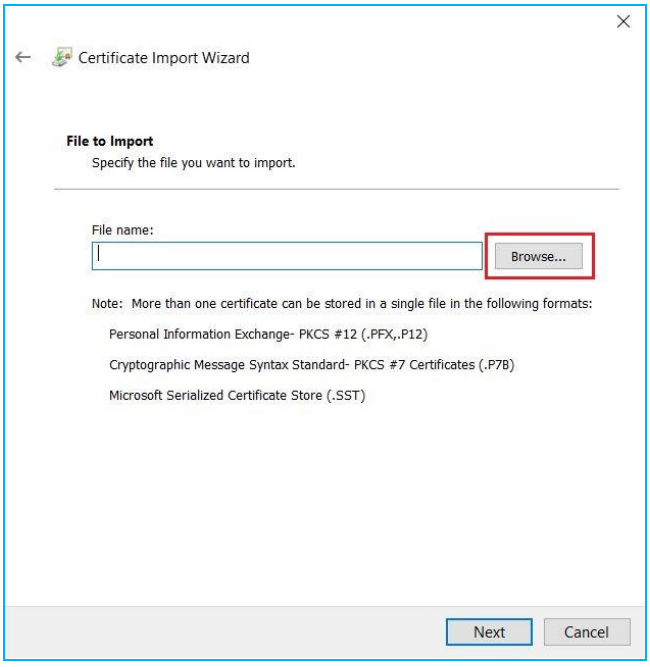
FigA.1.25

- On following window, click **Next** (Next) button as shown in **FigA.1.26:**



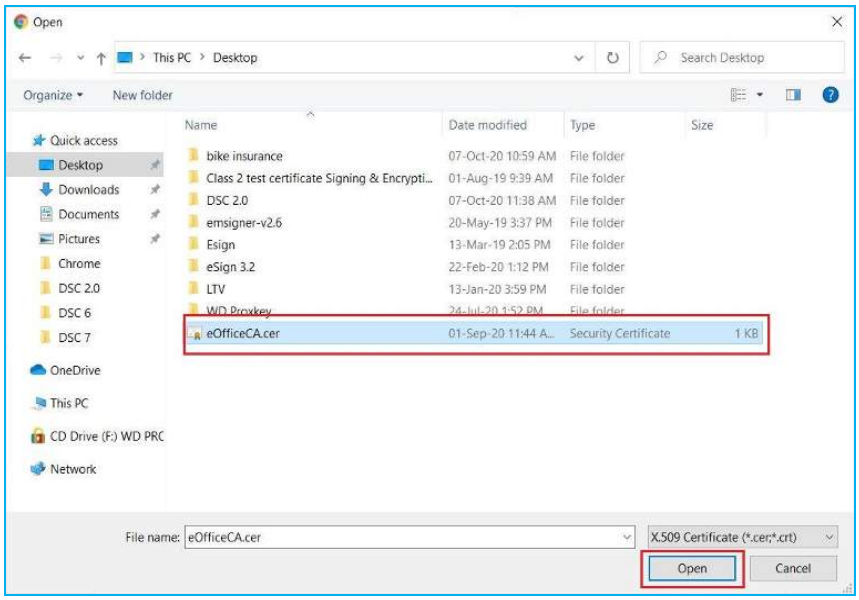
FigA.1.26

- On following window, click **Browse** (Browse...) button as shown in **FigA.1.27:**



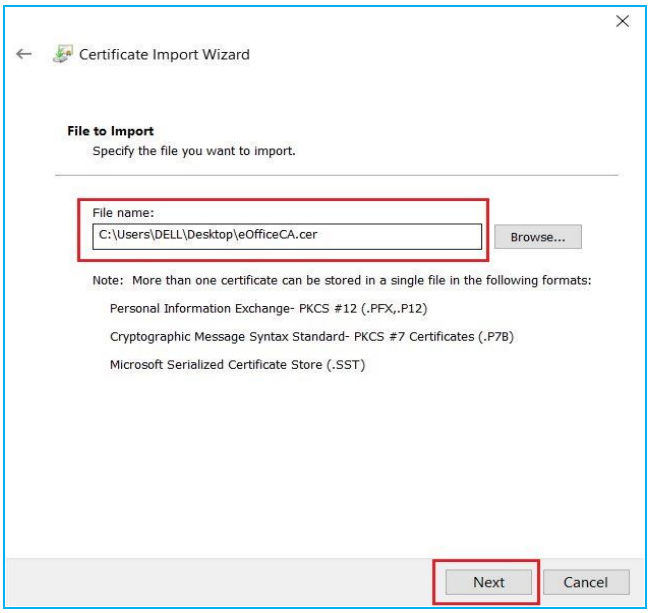
FigA.1.27

- On the Dialog box, select the **Certificate** and click **Open** (Open) button as shown in **FigA.1.28:**



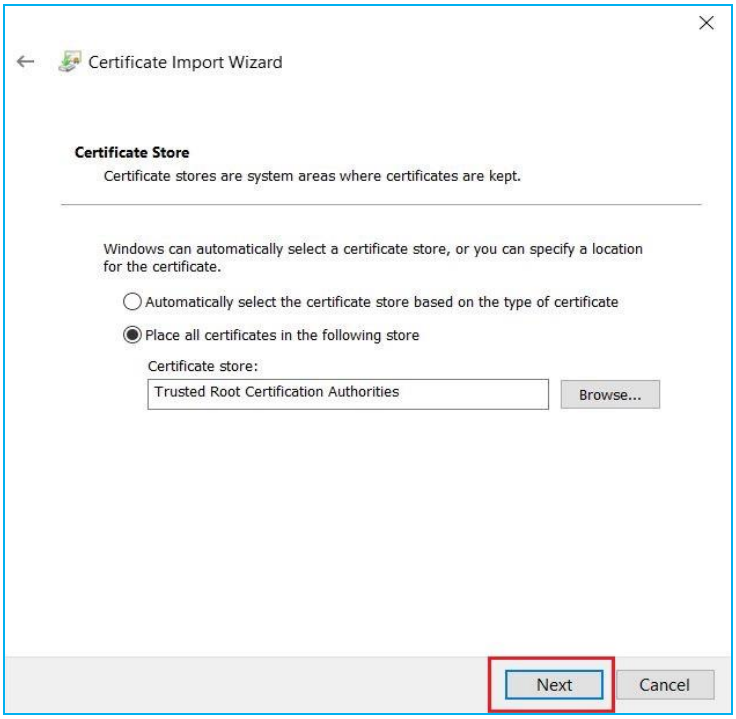
FigA.1.28

- Click **Next** (Next) button as shown in **FigA.1.29:**



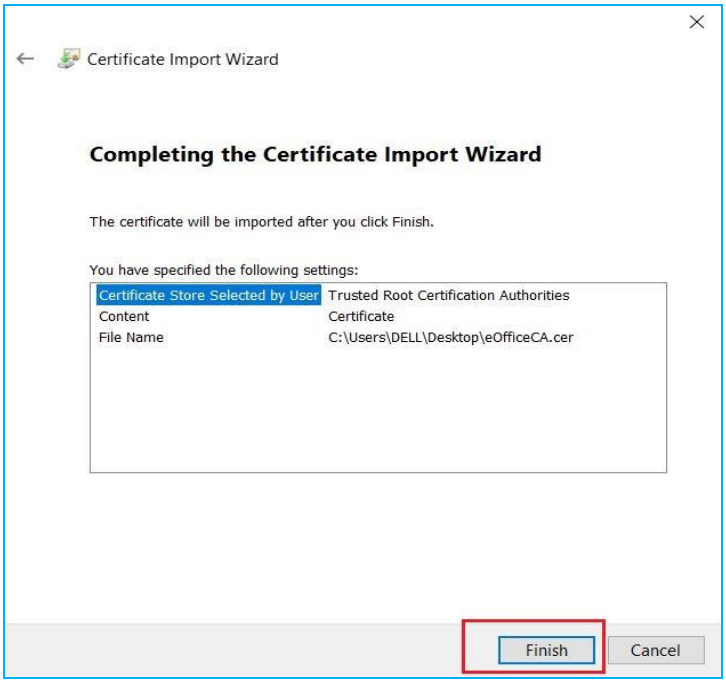
FigA.1.29

- On following window, click **Next** (Next) button as shown in **FigA.1.30:**



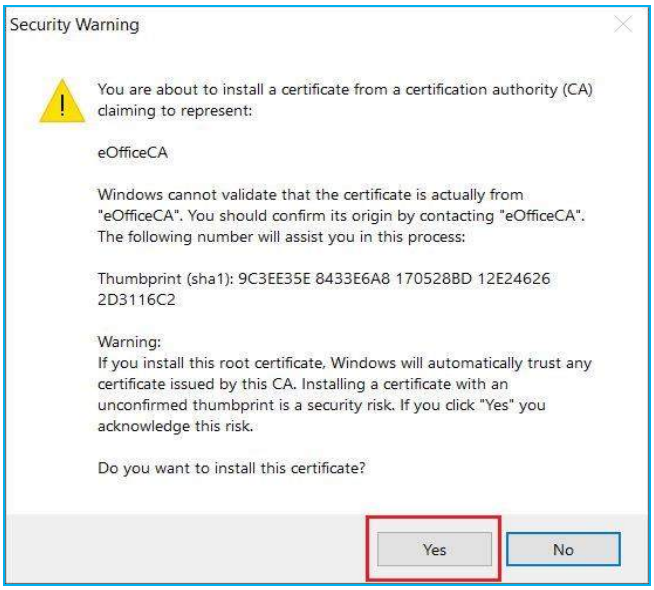
FigA.1.30

- Click **Finish** (Finish) button as shown in **FigA.1.31:**



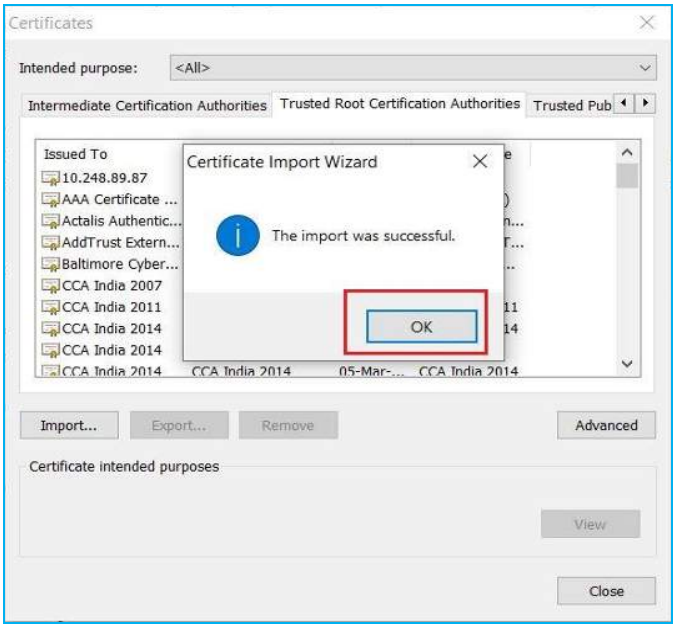
FigA.1.31

- Click **Yes** (Yes) button on prompt window as shown in **FigA.1.32:**



FigA.1.32

- Click **Ok** (OK) button on Dialog box as shown in **FigA.1.33:**



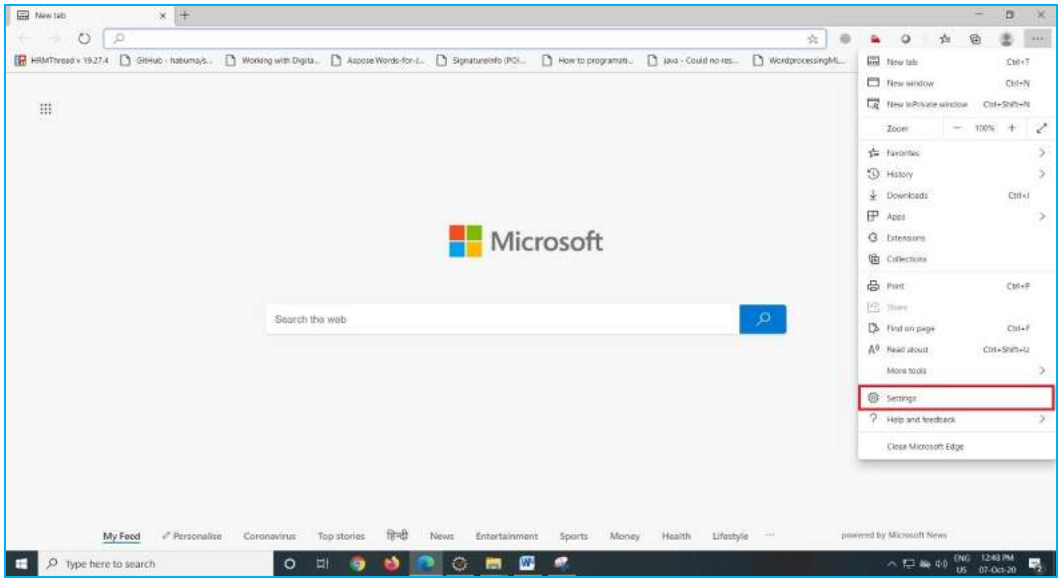
FigA.1.33

- This will import eOffice CA certificate to the Trusted Root Certification Authorities store.

For Microsoft Edge

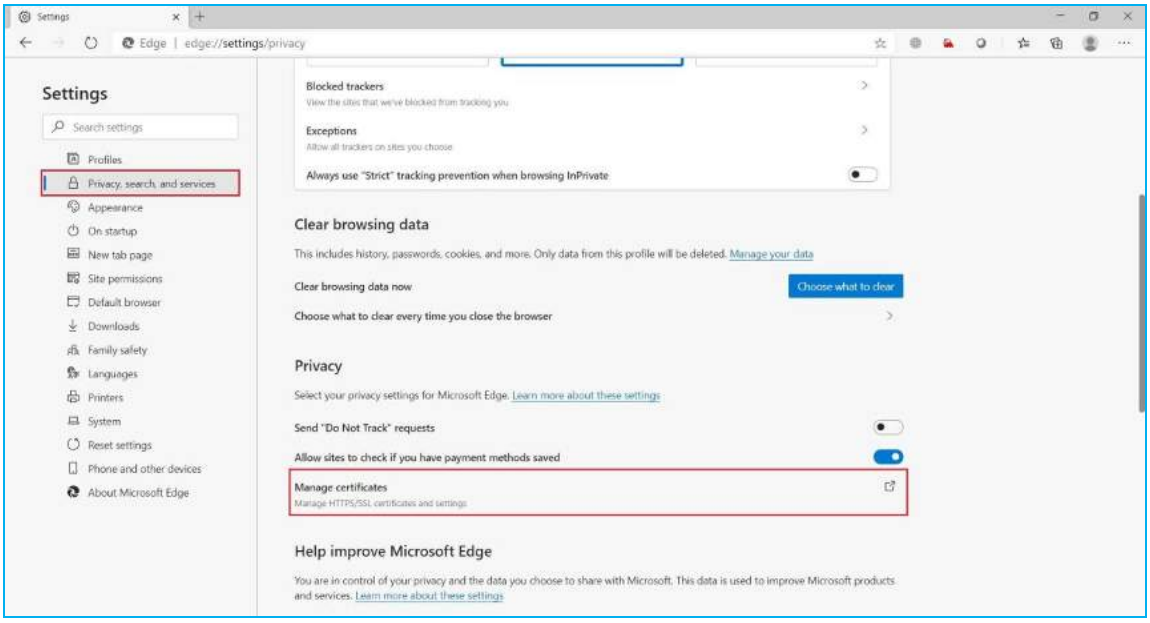
To add a self-signed certificate for https in Microsoft Edge, perform the below actions to import SSL certificate:

- Open Microsoft Edge browser, Click (···) icon at top right corner and then Click **Settings** (Settings) link as shown in **FigA.1.34**:



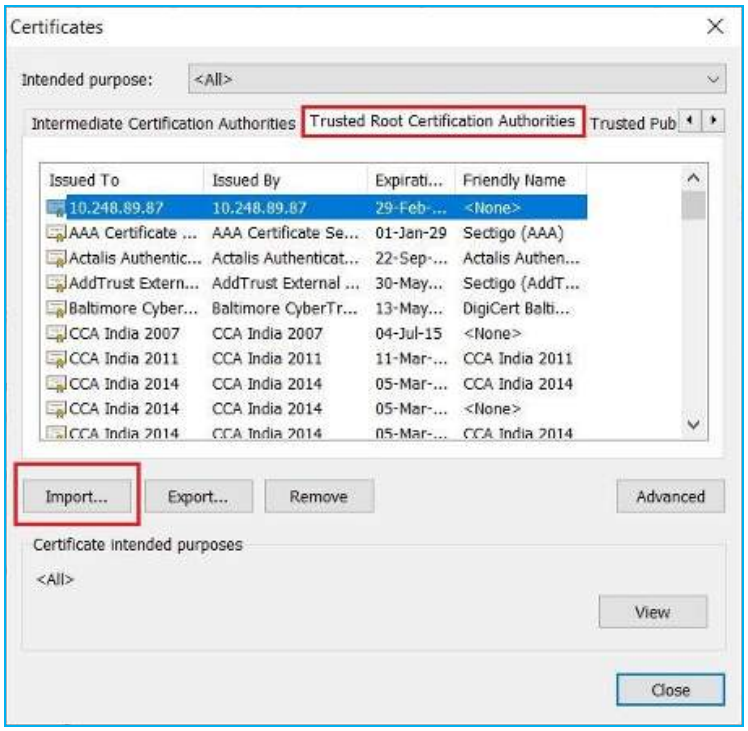
FigA.1.34

- On following window, Click **Privacy, search, and services** (Privacy, search, and services) link in left menu panel. Scroll down and Click **Manage certificates** (Manage certificates
Manage HTTPS/SSL certificates and settings) link as shown in **FigA.1.35:**



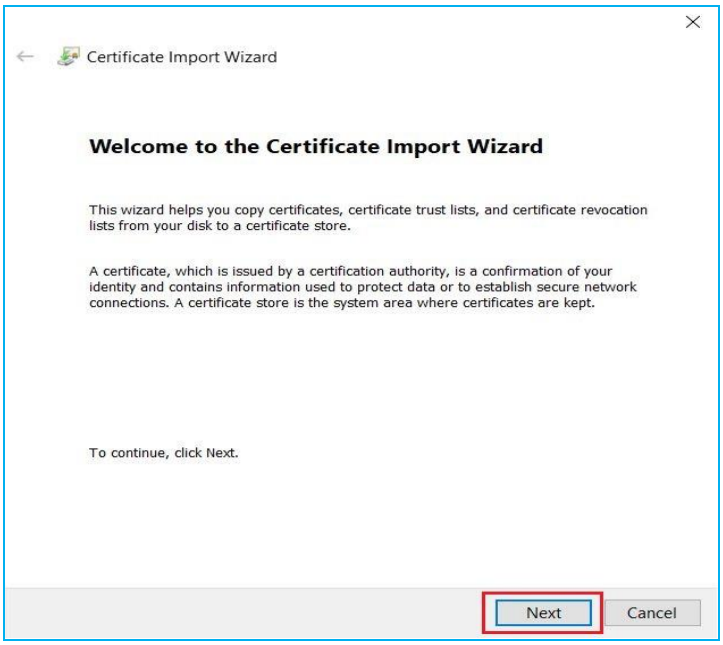
FigA.1.35

- On following window, Click **Trusted Root Certification Authorities** (Trusted Root Certification Authorities) tab and Click **Import** (Import...) button as shown in **FigA.1.36:**



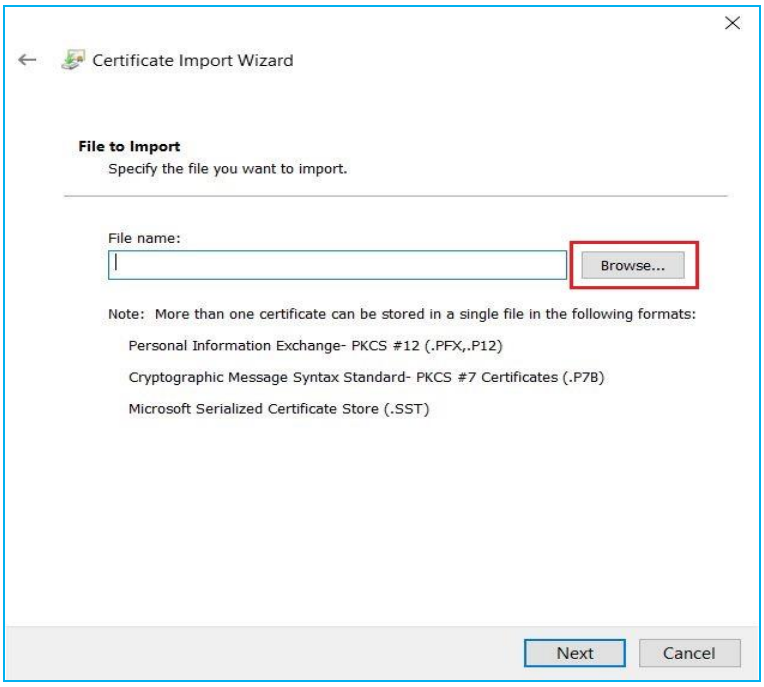
FigA.1.36

- On following window, click **Next** (Next) button as shown in **FigA.1.37:**



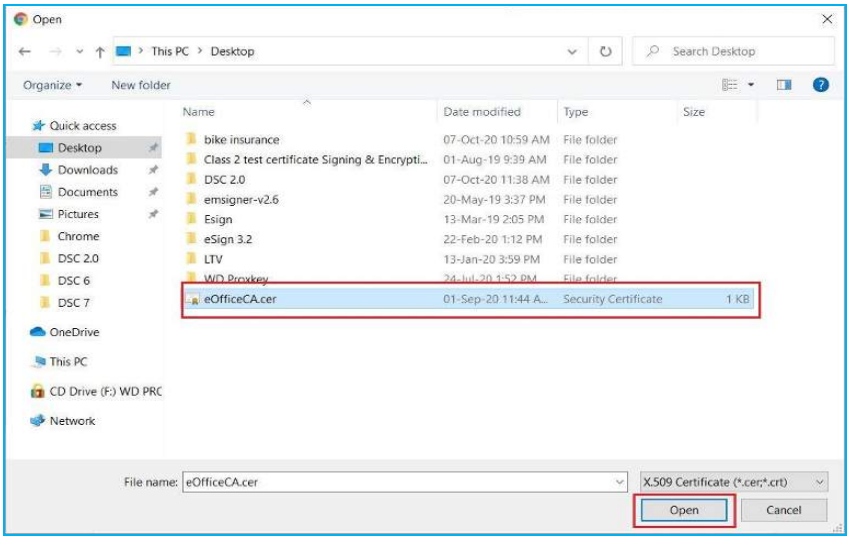
FigA.1.37

- On following window, Click **Browse** (Browse...) button as shown in **FigA.1.38:**



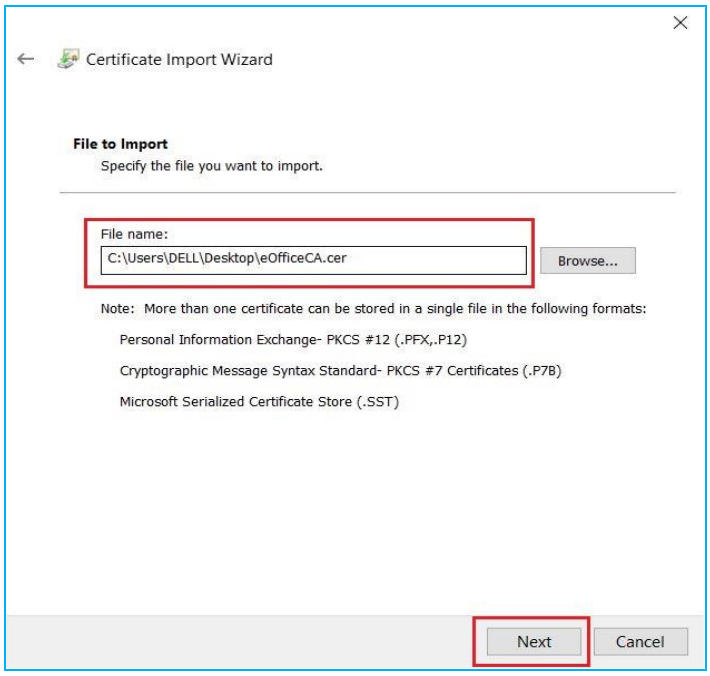
FigA.1.38

- From the Dialog box, select the **certificate** and Click **Open** (Open) button as shown in **FigA.1.39**.



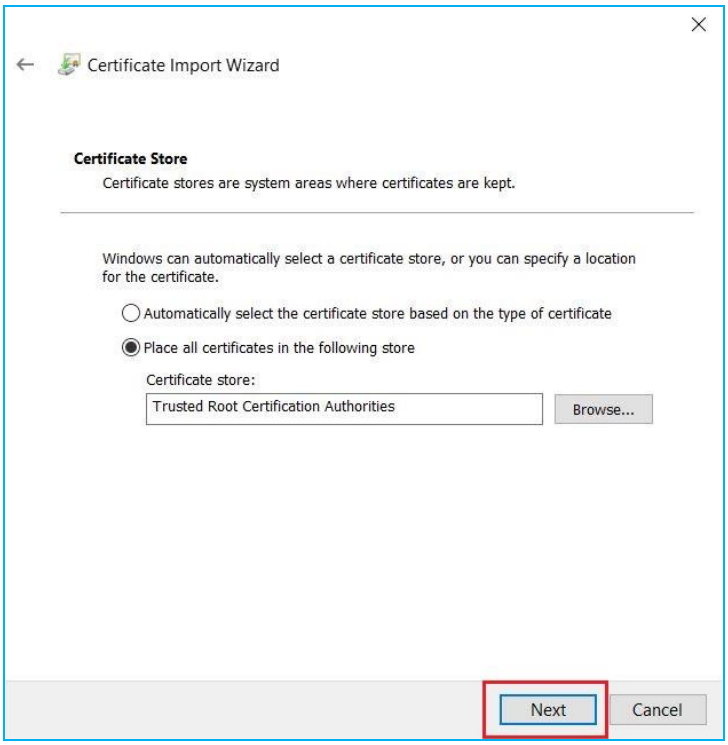
FigA.1.39

- Then Click **Next** (Next) button as shown in **Fig.A.1.40:**



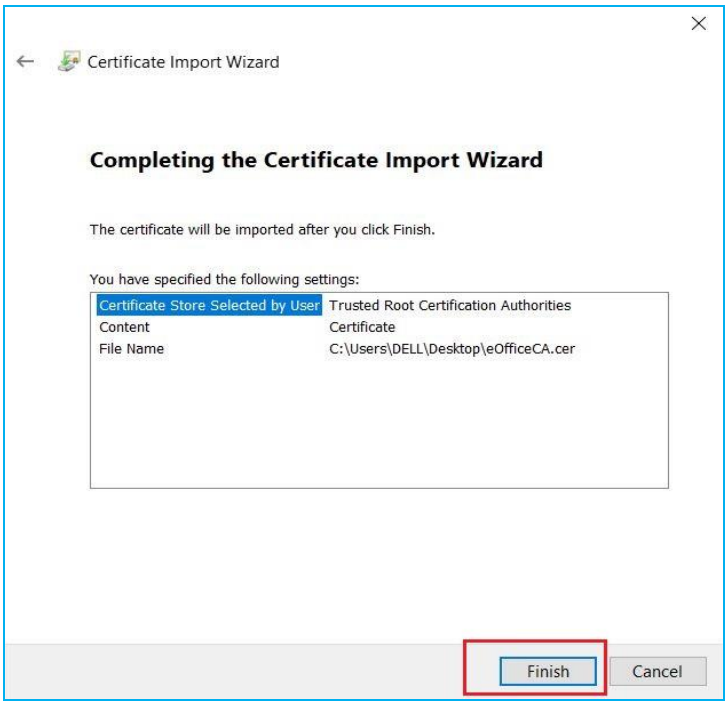
FigA.1.40

- On following window, Click **Next** (Next) button as shown in **Fig.A.1.41:**



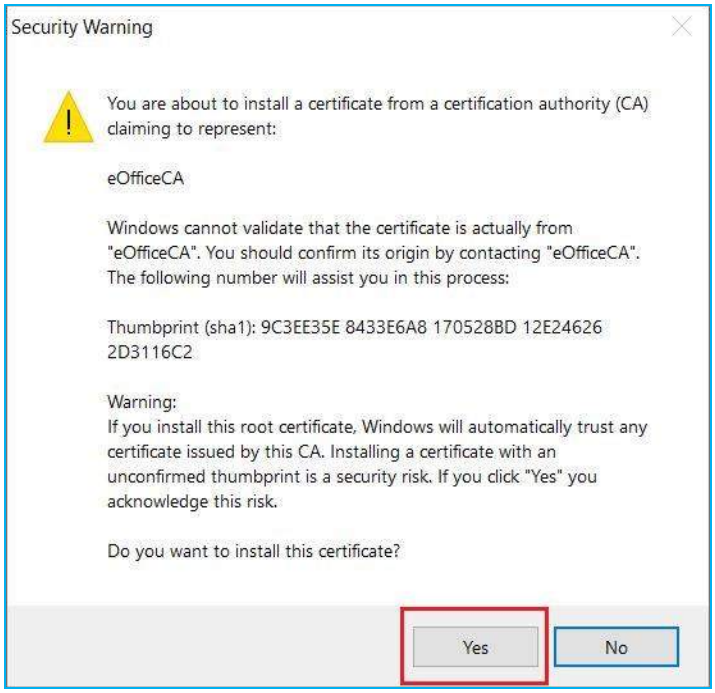
FigA.1.41

- Click **Finish** (Finish) button as shown in **FigA.1.42:**



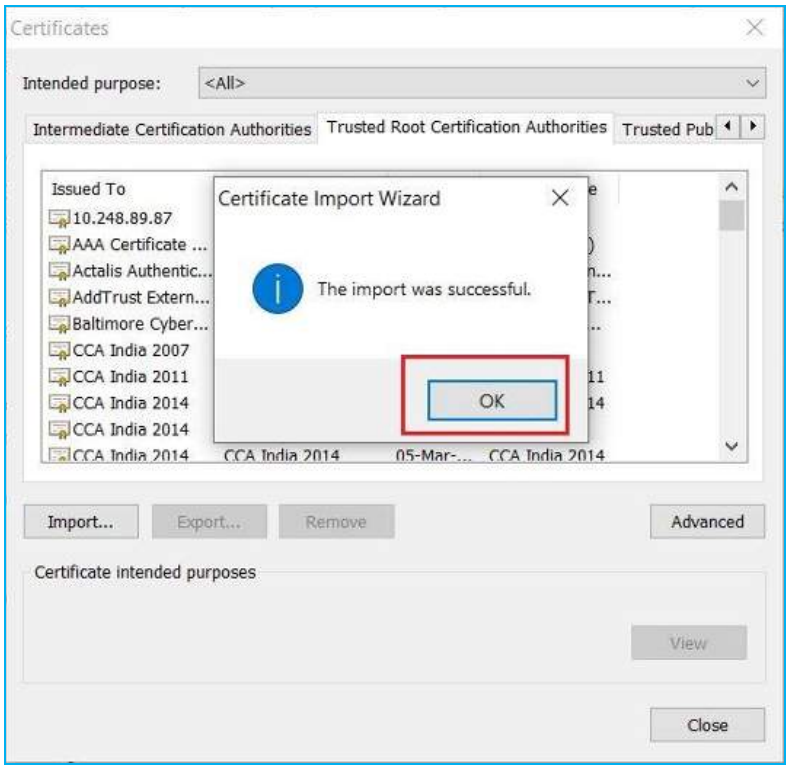
FigA.1.42

- On prompt window, click **Yes** (Yes) button as shown in **FigA.1.43:**



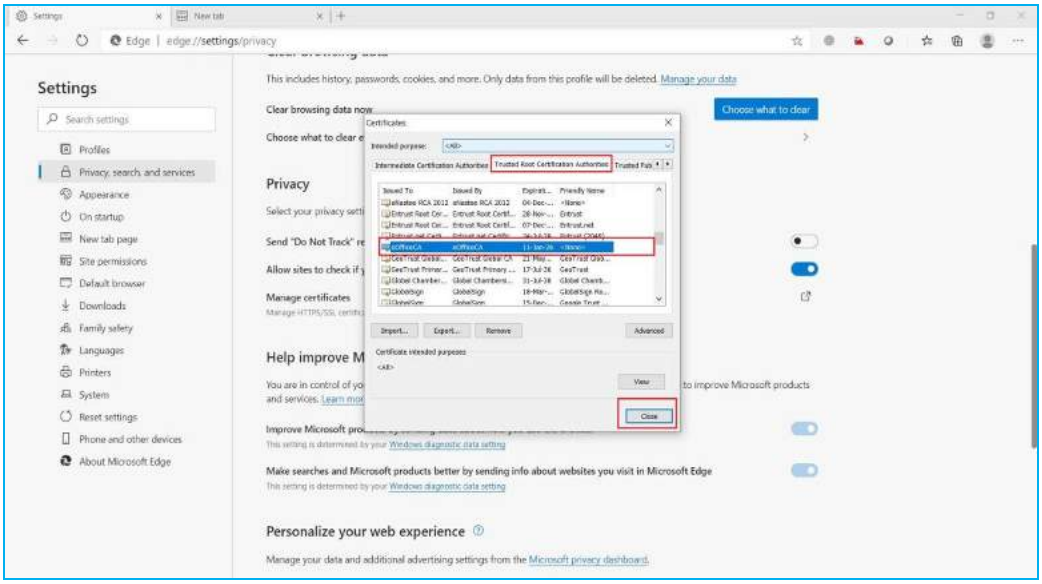
FigA.1.43

- On Dialog box, click **Ok** (OK) button as shown in **FigA.1.44:**



FigA.1.44

- This will import eOffice CA certificate to the Trusted Root Certification Authorities store as shown in **FigA.1.45:**



FigA.1.45

For MAC

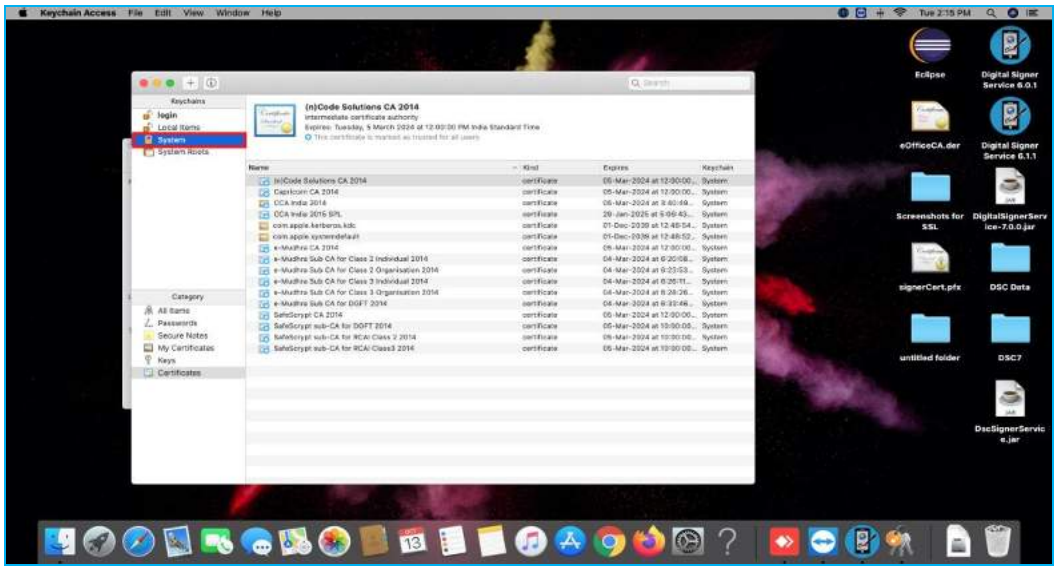
For Google Chrome and Safari

To add a self-signed certificate for https in Google Chrome and Safari, perform the below actions to import SSL certificate:

- Open **Launchpad** & search for "**Keychain Access**" as shown in **FigA.1.46**;

FigA.1.46

- Select **System** (System) link from left panel as shown in **FigA.1.47:**



FigA.1.47

- Click on **'+'** icon at upper left corner, Navigate & select **eOfficeCA.der** certificate & Click **Open** (Open) button as shown in **FigA.1.48:**

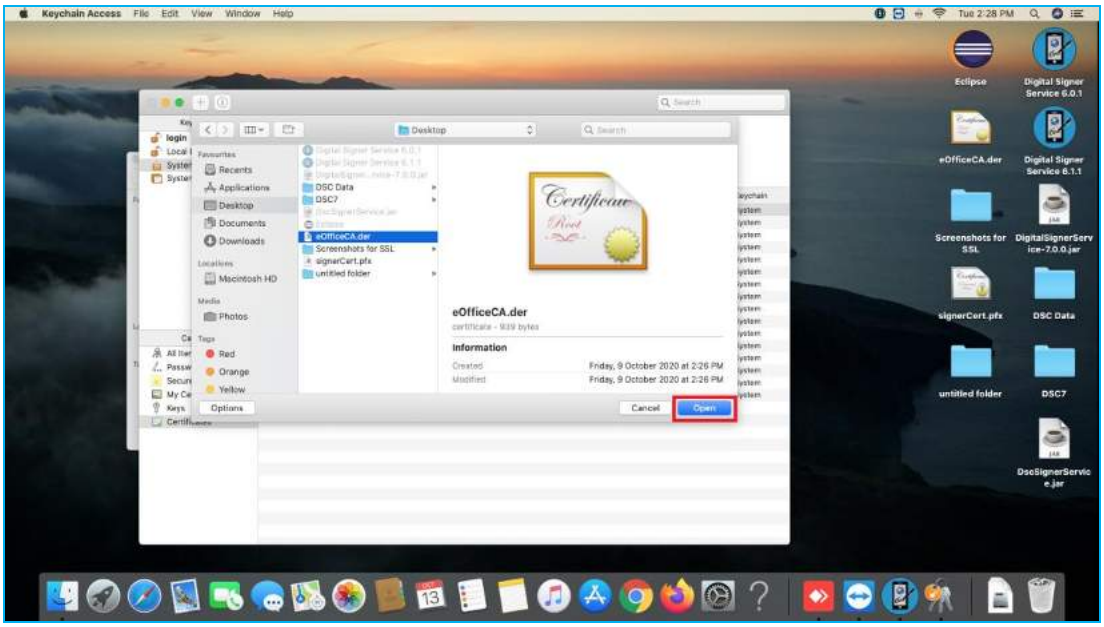
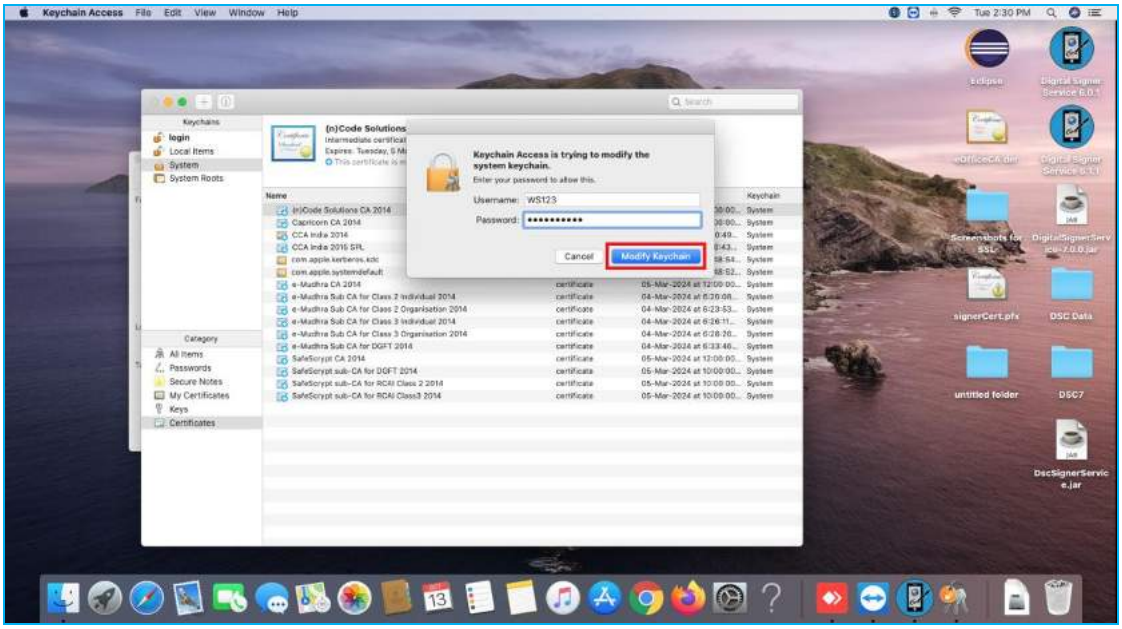


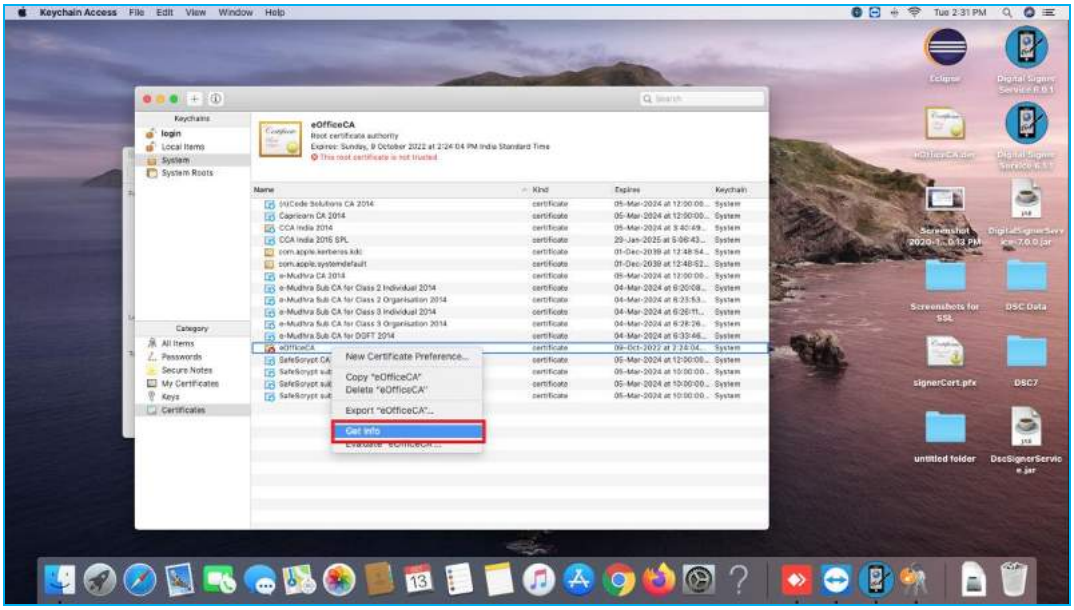
Fig.1.48

- Password window will appear, provide the Account Password & Click **Modify Keychain** (Modify Keychain) button as shown in **FigA.1.49**.



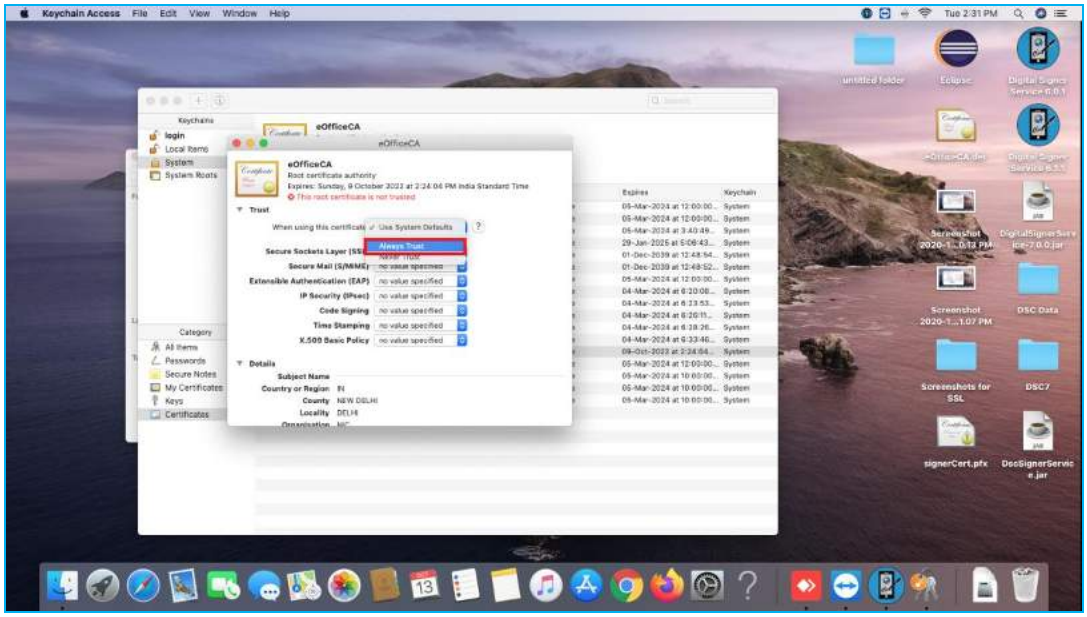
FigA.1.49

- Select added certificate from list, Right click and then Click **'Get Info'** (Get Info) option as shown in **FigA.1.50:**



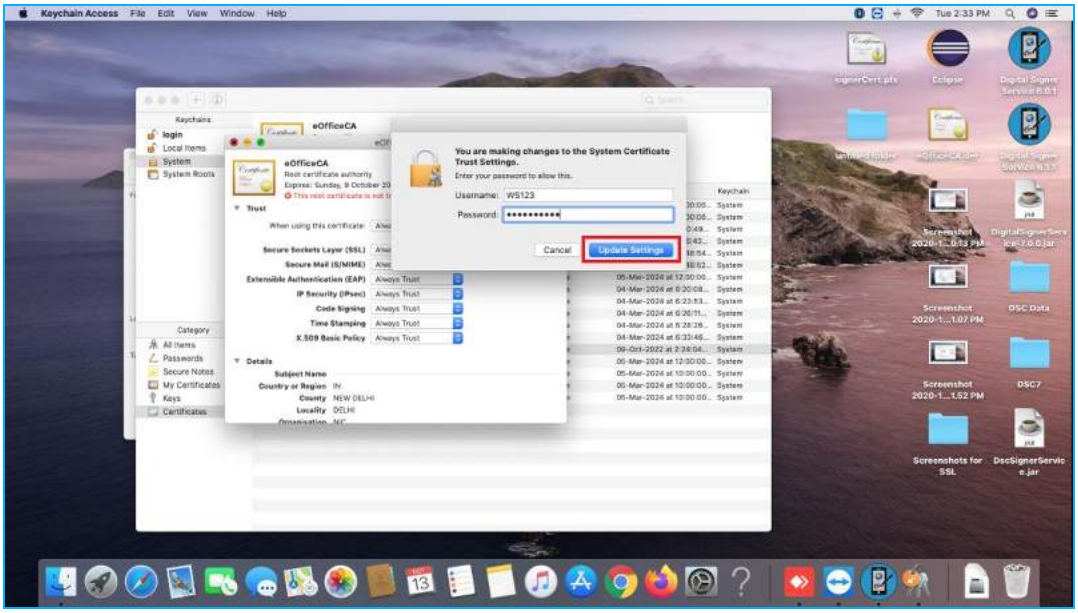
FigA.1.50

- Click on "**Trust**", select "**Always Trust**" (Always Trust) option "**When using this certificate**" as shown in **FigA.1.51:**



FigA.1.51

- Close the window. Password window will Appear. Provide the Account Password & Click **Update Settings** (Update Settings) button as shown in **FigA.1.52**.

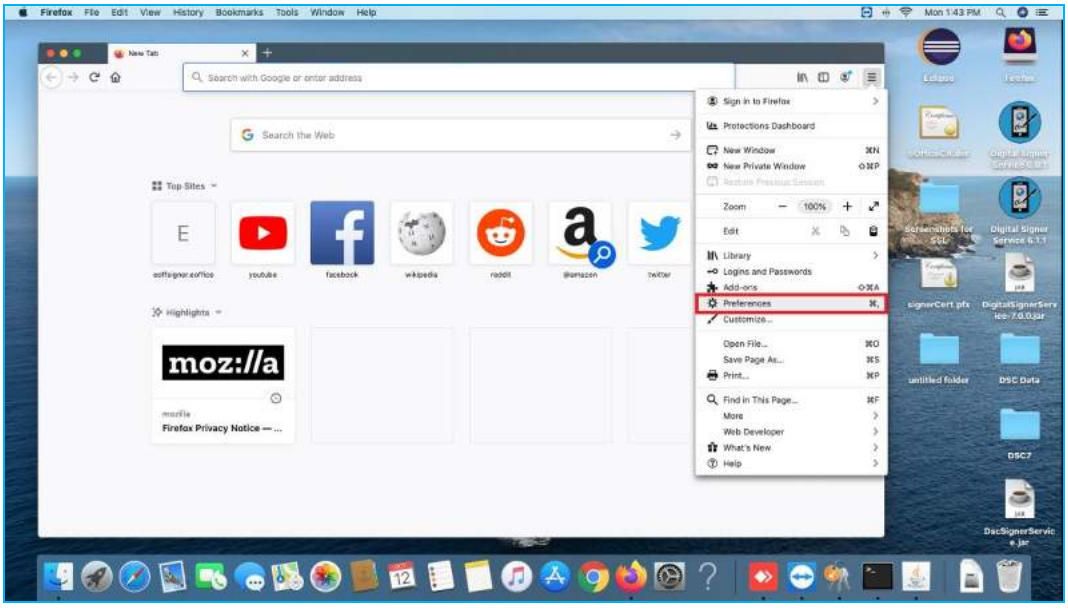


FigA.1.52

For Mozilla Firefox

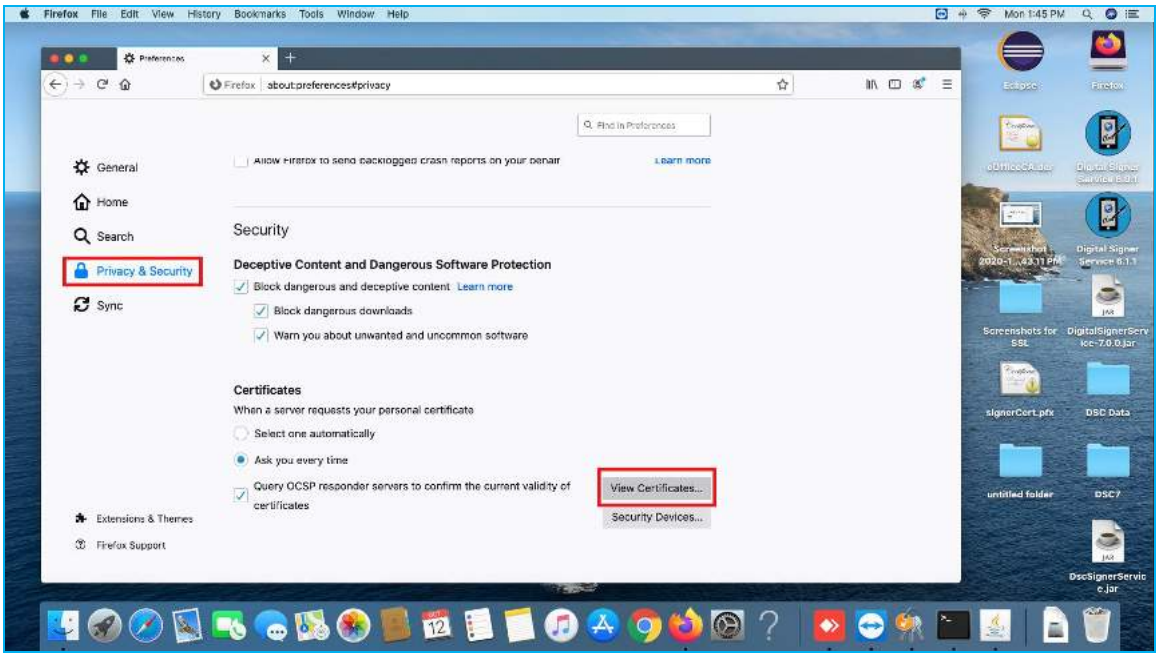
For adding a self-signed certificate for https in Mozilla Firefox, perform the below actions to import SSL certificate:

- Open Mozilla Firefox browser. Click (☰) icon at top right corner and Click **Preferences** (Preferences) link as shown in **FigA.1.53:**



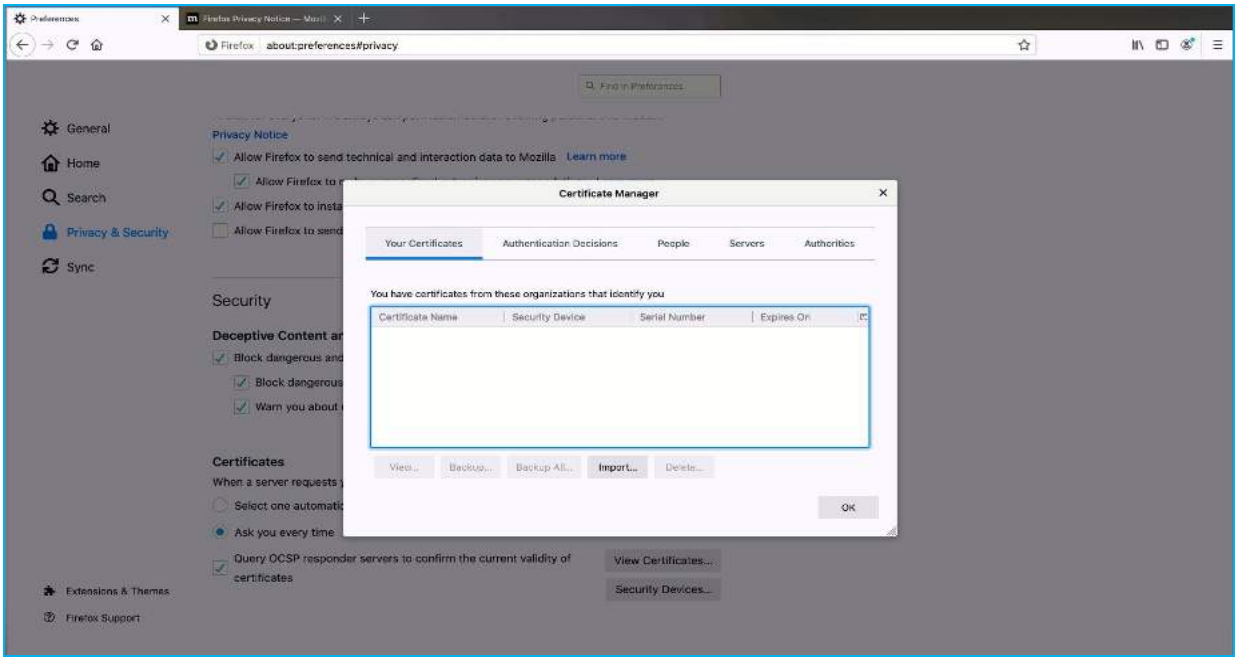
FigA.1.53

- In left menu panel, Click **Privacy & Security** (Privacy & Security) link. Scroll down and Click **View Certificates** (View Certificates...) button as shown in **FigA.1.54**:



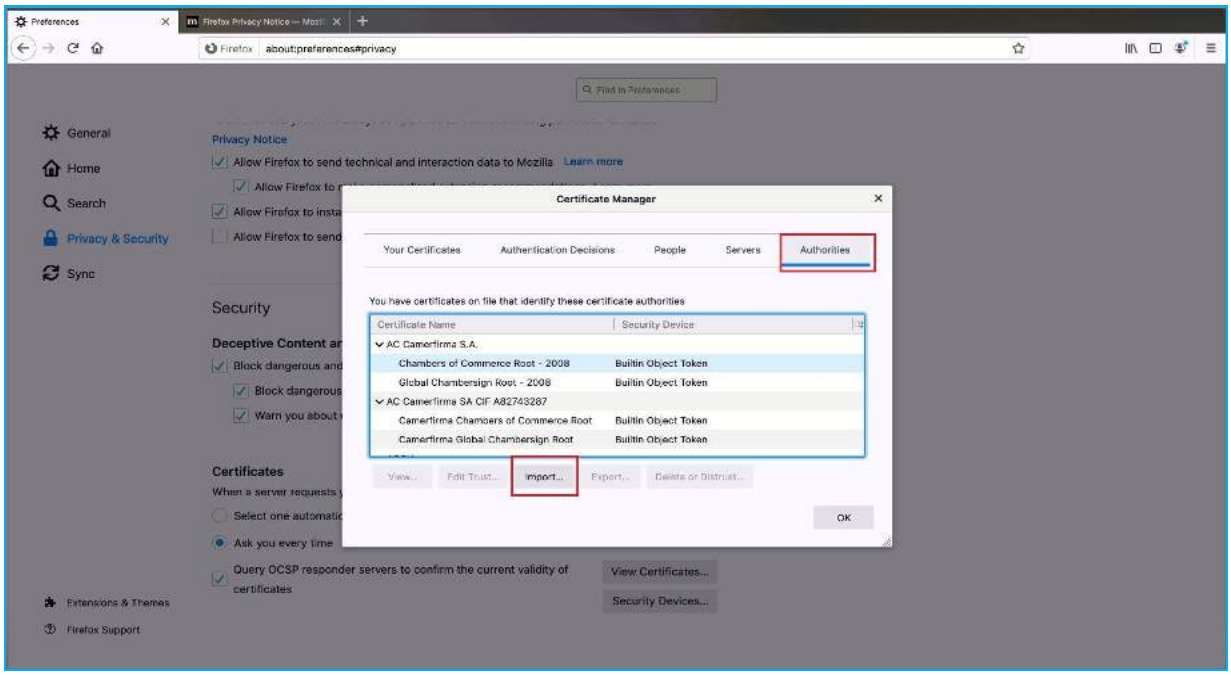
FigA.1.54

- Following Certificate Manager Window will appear as shown in **FigA.1.55**:



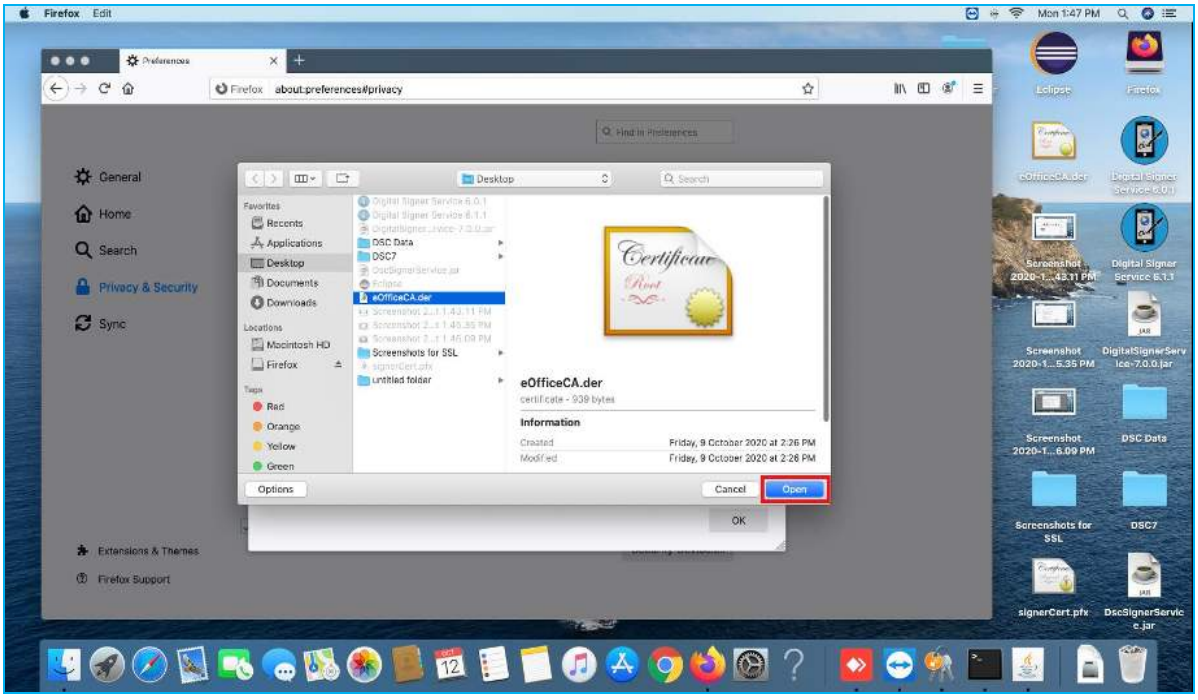
FigA.1.55

- Click on **Authorities** (Authorities) tab and then Click **Import** (Import...) button as shown in **FigA.1.56**:



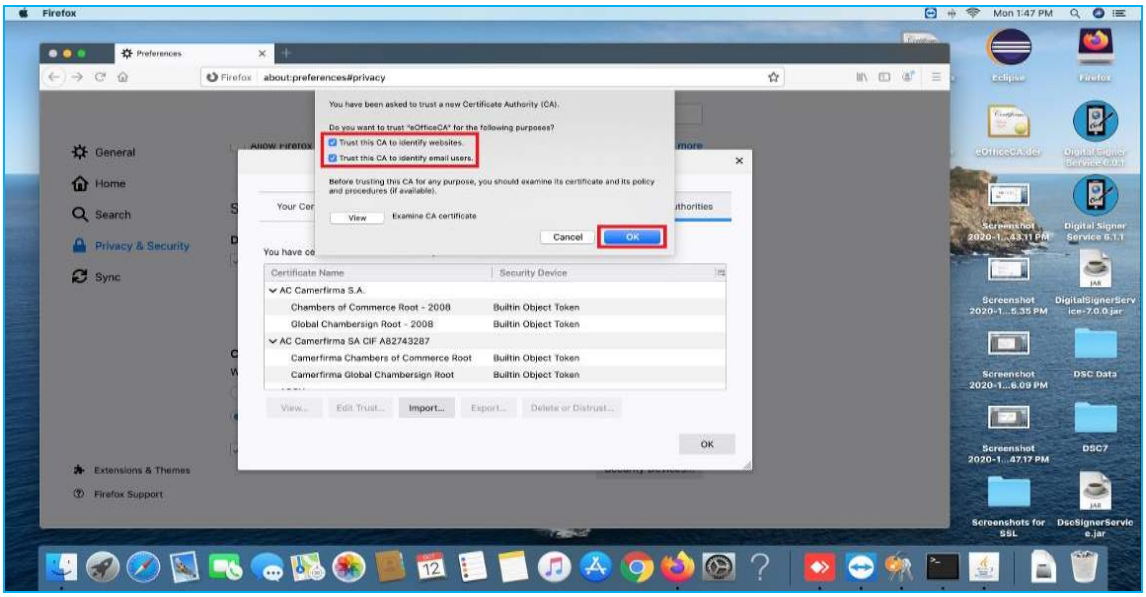
FigA.1.56

- Select the **certificate** and Click **Open** (Open) button as shown in **FigA.1.57**:



FigA.1.57

- Check both checkboxes and Click **Ok** (OK) button as shown in **FigA.1.58**;



FigA.1.58

- This will import eOffice CA certificate to the Authorities store.

For Ubuntu

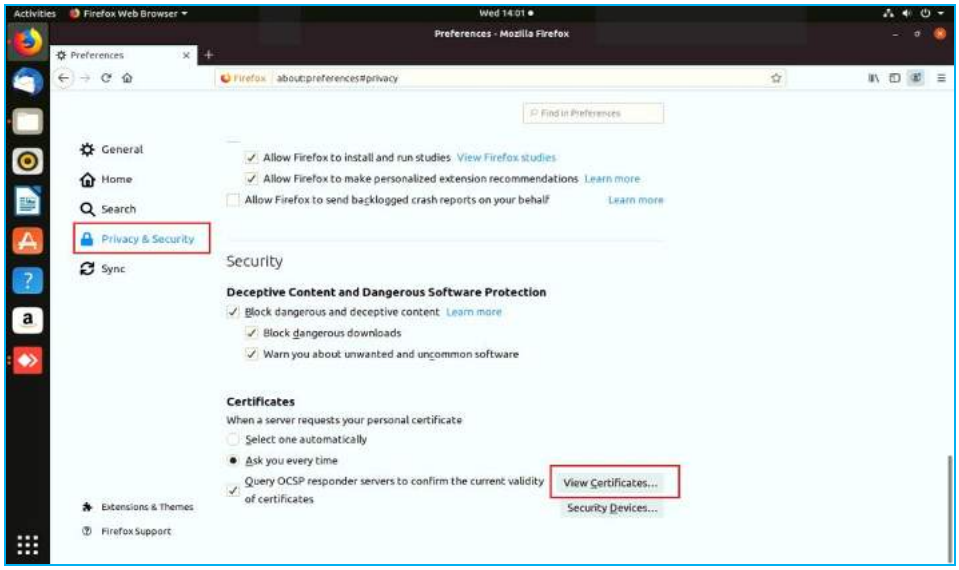
For Mozilla Firefox

To add a self-signed certificate for https in Mozilla Firefox, perform the below actions to import SSL certificate:

- Open Mozilla Firefox browser, Click (☰) icon at top right corner and then Click **Preferences** (Preferences) link as shown in **FigA.1.59:**

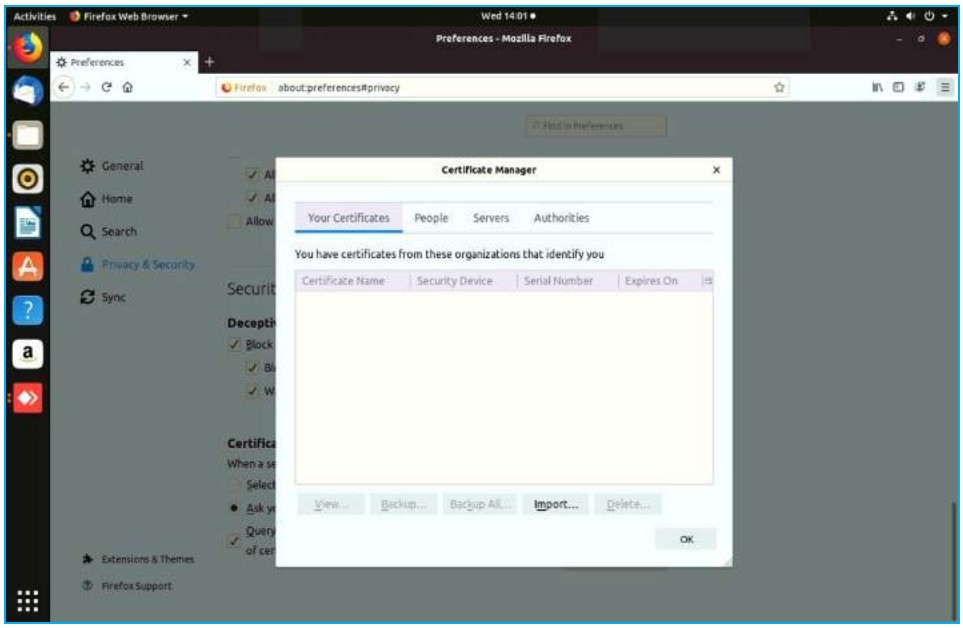
FigA.1.59

- In left menu panel, Click **Privacy & Security** (Privacy & Security) link. Scroll down and click **View Certificates** (View Certificates...) button as shown in **FigA.1.60**:



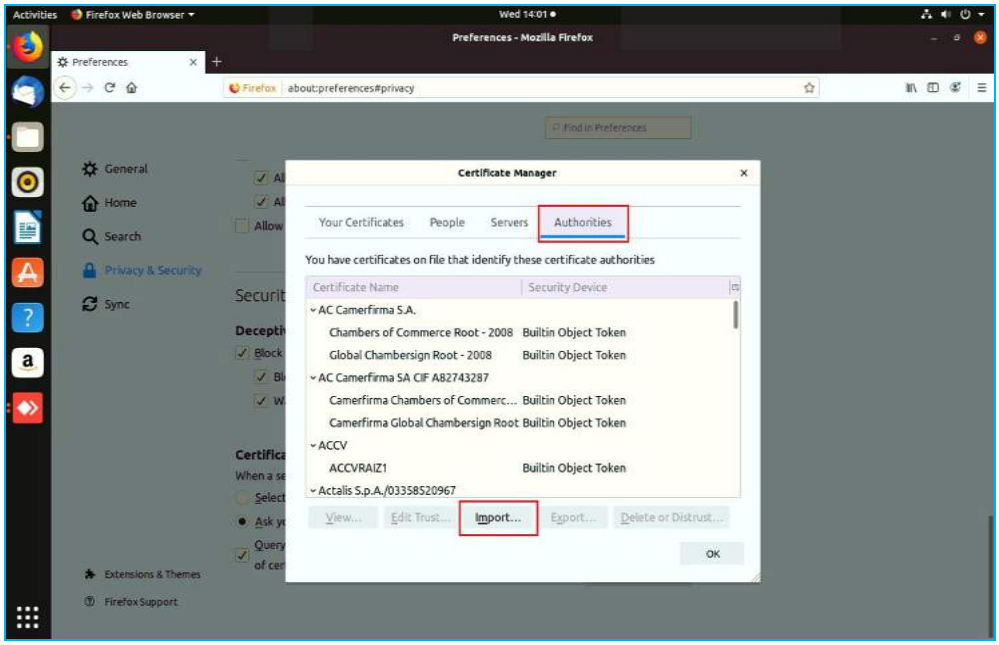
FigA.1.60

- Following Certificate Manager Window will appear as shown in **FigA.1.61**:



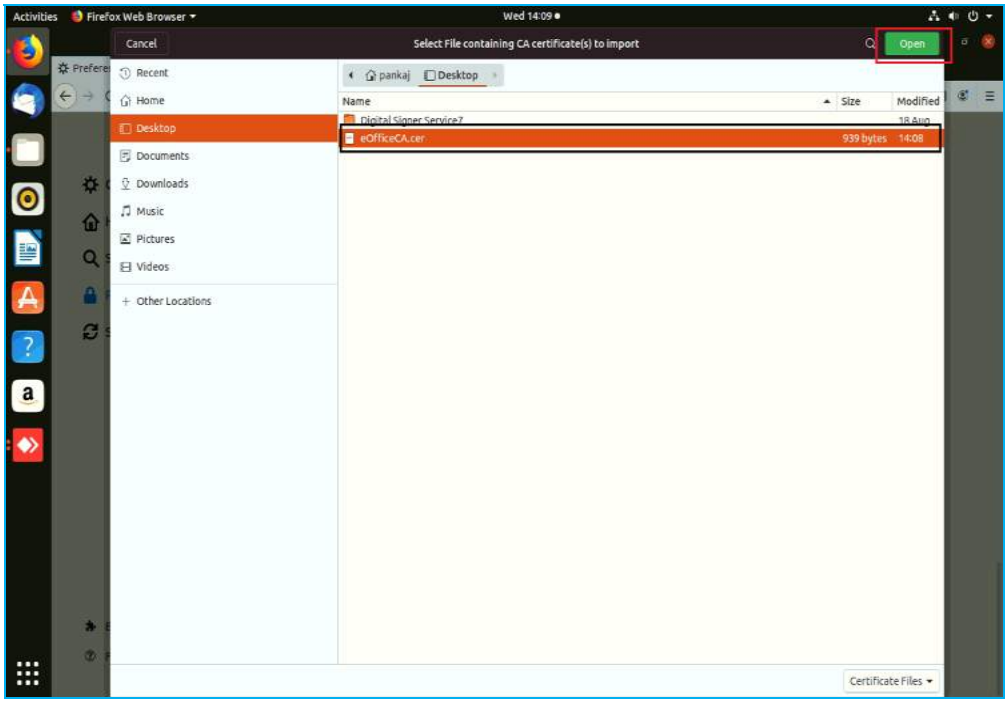
FigA.1.61

- Click **Authorities** (Authorities) tab and Click **Import** (Import...) button as shown in **FigA.1.62:**



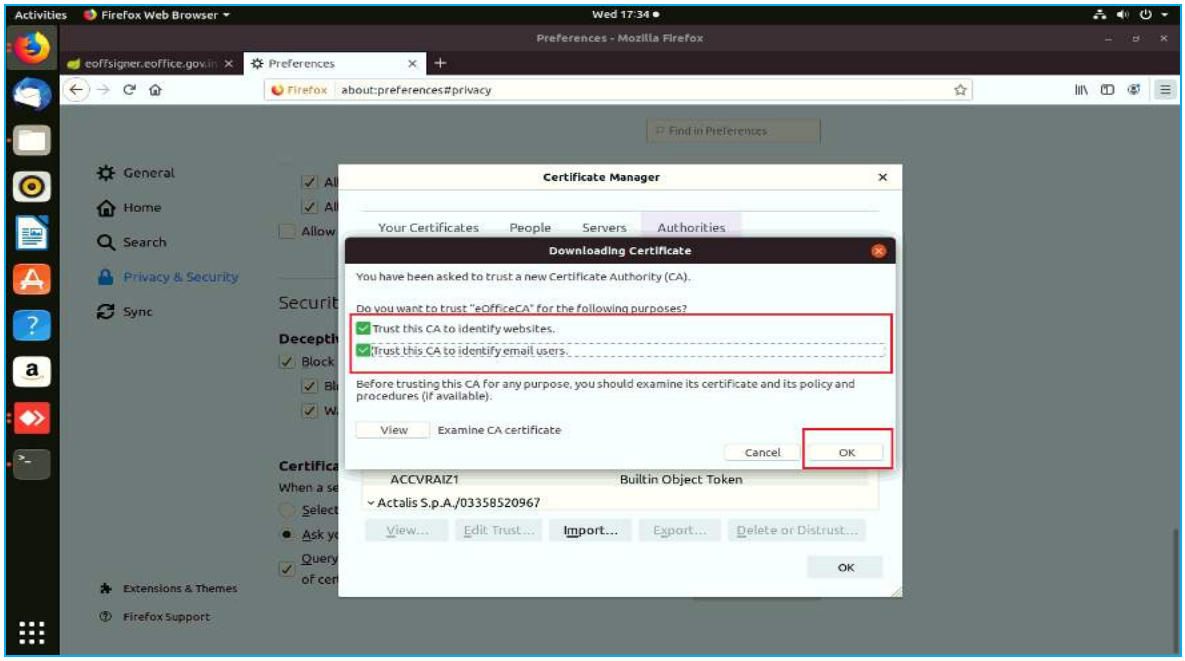
FigA.1.62

- Select the **Certificate** and Click **Open** (Open) button as shown in **FigA.1.63:**



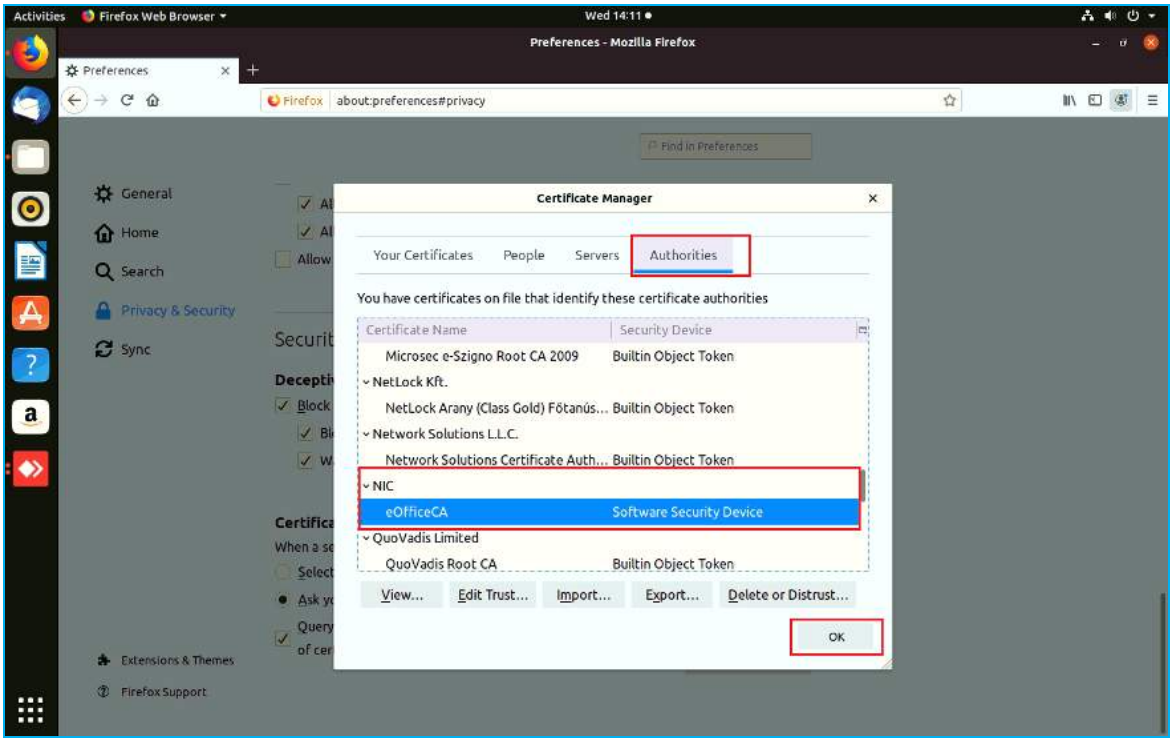
FigA.1.63

- Check both checkboxes and Click **Ok** (OK) button as shown in **FigA.1.64**:



FigA.1.64

- This will import eOffice CA certificate to the Authorities store as shown in **FigA.1.65**:



FIgA.1.65

Annexure II

Troubleshooting (For Digital Signer Service)

Problem 1

Service is not running after successful installation.

Solution

Check Java is installed properly or not and then, restart the **Digital Signer Service** manually.

For Windows

- Double click the desktop icon () **"Digital Signer Service 7.0.0"**.
- Digital signer Service icon () will appear in the system tray (in the bottom-right corner of monitor) which indicates that Digital Signer Service 7.0.0 is running in the system, as shown in **Fig.A.2.1:**

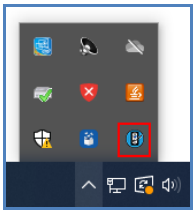


Fig.A.2.1

For MAC

- Restart the **Digital Signer Service** by clicking desktop icon () **"Digital Signer Service 7.0.0"**.
- Digital Signer Service icon () will appear in the menu bar (in the upper-right corner of monitor) which indicates that Digital Signer Service 7.0.0 is running in the system, as shown in **Fig.A.2.2:**

Fig.A.2.2

For Ubuntu

- Restart the **Digital Signer Service** by clicking desktop icon () **"Digital Signer Service 7.0.0"**.

Note:

1. While using DSC application in MAC OS and Ubuntu OS, if a token is plugged-out, then, occasionally user has to manually restart the Digital Signer Service.

Problem 2
Service is not running even after starting manually.

Solution
Check availability of port HTTPs
https port: 55103

Commands to check for availability of port are mentioned below:

For Windows
Use cmd/power Shell to run following commands in windows.
Command: netstat–ano | find "port" (**Fig.A.2.3**).

Screen-shot

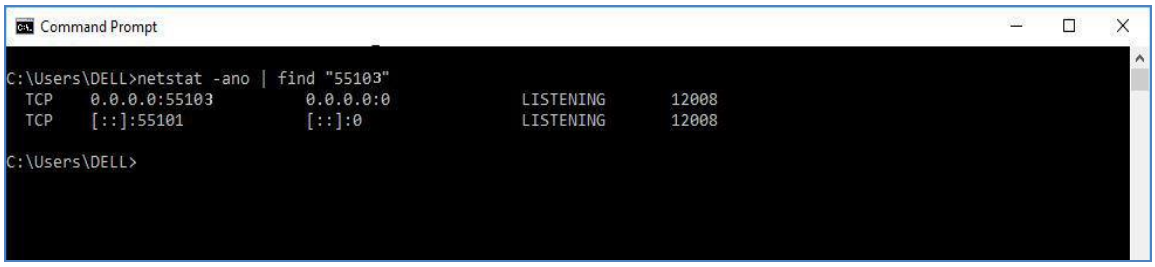


Fig.A.2.3

For Ubuntu
For Ubuntu use Terminal.
Command: netstat -tunlp | grep port (**Fig.A.2.4**).

Screen-shot

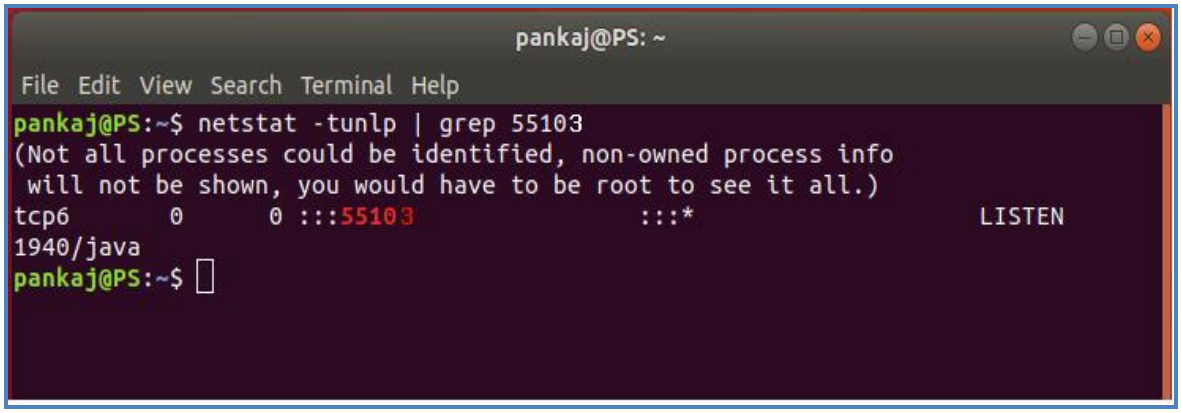


Fig.A.2.4

For MAC

For MAC use Terminal.

Command: netstat –vanptcp | grep port **(Fig.A.2.5).**

Screen-shot

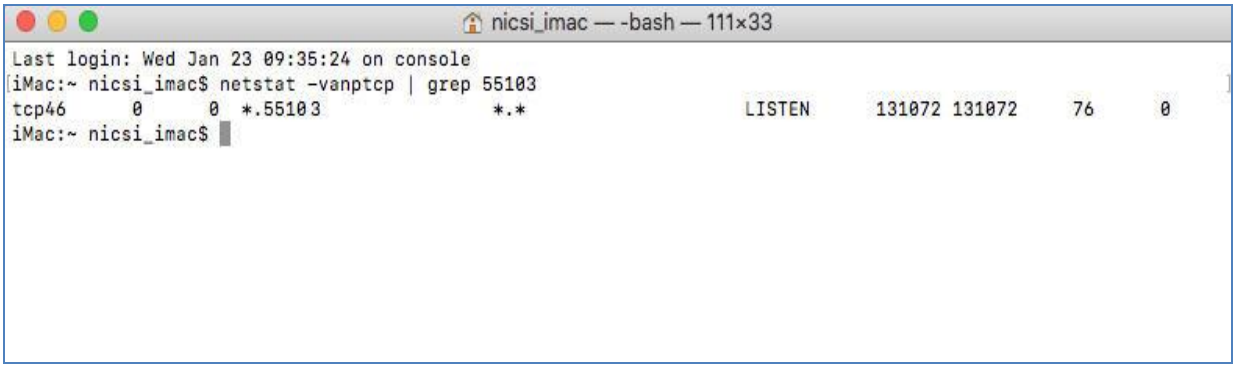


Fig.A.2.5

If no service is running on port, manually start the service. If still it does not start, contact the administrator.

Problem 3
In case, the port 55103 is in use with some other service.

Solution
Kill the service running from port 55103
Commands to **Kill** the services from port are:

For Windows
Use cmd/powerShell to run following commands in windows.
Command: taskkill /f /pid [PID] (**Fig.A.2.6**).

Screen-shot

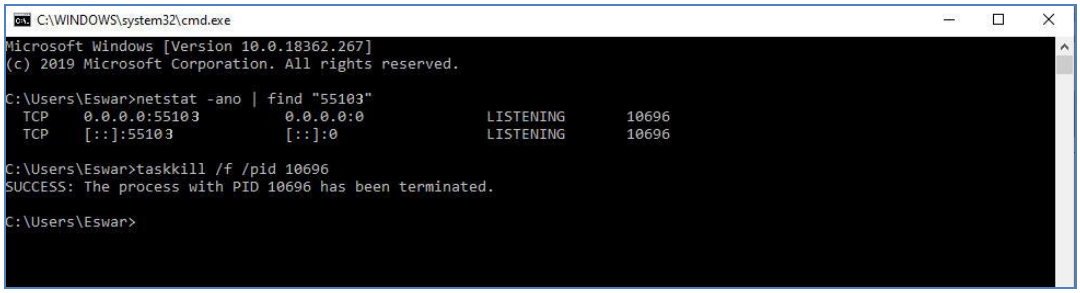


Fig.A.2.6

For Ubuntu
For Ubuntu use Terminal.
Command: Sudo kill -9 [PID] (**Fig.A.2.7**).

Screen-shot

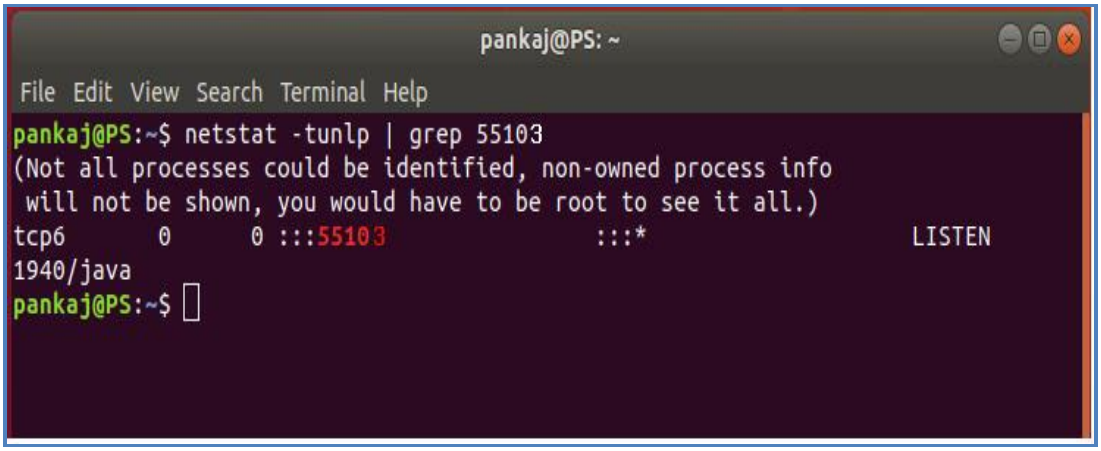


Fig.A.2.7

For Mac

For MAC use Terminal.
Command: sudo kill -9 [PID] **(Fig.A.2.8).**

Screen-shot

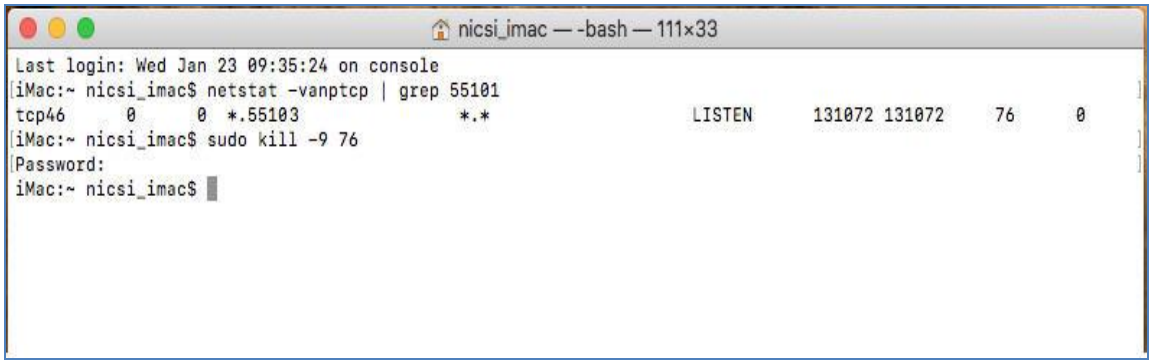


Fig.A.2.8

After killing the service, manually start the service. If still it does not start, contact the administrator.

Problem 4

In case a new token is added in MAC/Ubuntu machine and the user certificate is not visible.

Solution

- Manually stop the Digital Signer Service.
- Properly plug-in the desired token.
- Start Digital Signer Service again and continue to add a token.

Annexure III

Signature Validity Checkmark Visibility

The visual representation of signature verification:

In previous version of DSC, signature verification visibility was displayed on the same page along with the page content. But now as per ISO 32000-2 standard compliance **signature verification visibility is not to be displayed** along with the page content, it will be displayed on the different panel apart from the main content panel. However, there is no change in signature visibility. For example, in case of adobe there is a signature panel, in which signature verification result will be displayed and page content is being displayed on different panel.

In previous signed pdf files verification status visibility will still be displayed, as Adobe Reader supports them for backward compatibility reasons only.

Thus, since Acrobat 9 Adobe displays its own icons only in the signature panel, not the document itself, and requires evaluation of signature validity by business users by inspecting the signature panel and generates signatures accordingly.

Display of Valid Signature in previous version of Digital Signature:

In case of previous DSC, green check and Red Cross sign were being used to display verification status of signature inside pdf content.
Green check sign was used for **Valid Signature** (**Fig.A.3.1**: **Valid Signature**) and **Red Cross sign** was used for **Invalid Signature** (**Fig.A.3.2**: **Invalid Signature**).

Fig.A.3.1: Valid Signature

Fig.A.3.2: Invalid Signature

Display of Valid Signature in Current Version of Digital Signature:

In current version, only signature details are being displayed along with the original content of the page. Refer to **Fig.A.3.3:**

Fig.A.3.3

How to verify signature in current scenario:

After opening the pdf file, click on Signature Panel located at upper right corner of adobe reader. A window will open on left side of document, where all information regarding signature validation is displayed along with the signature details. In case of **Valid signature**, **Green Check** will be shown at upper left corner of adobe reader and also inside signature panel itself, as shown in **Fig.A.3.4: Valid Signature**:

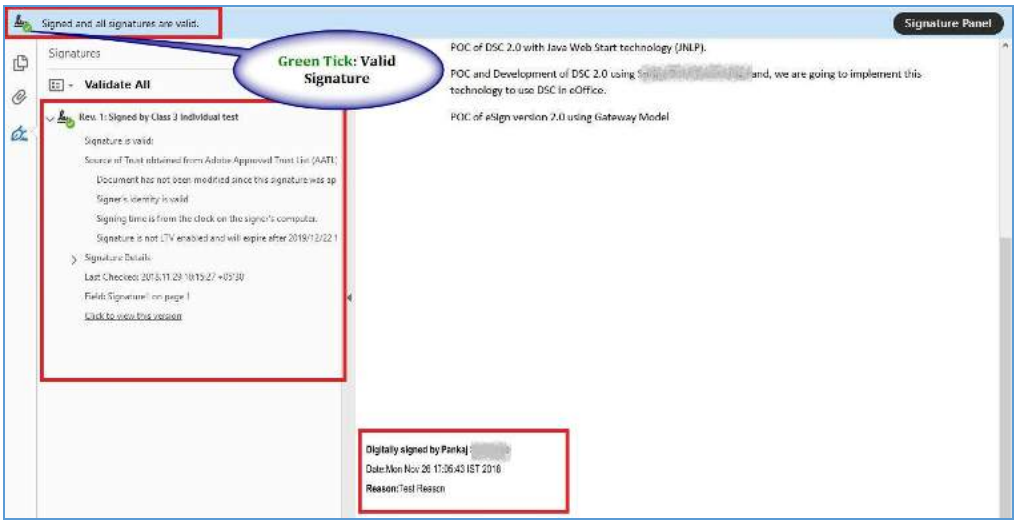


Fig.A.3.4: Valid Signature

In case of **Invalid Signature**, **Red Cross sign** is displayed at upper left corner of adobe reader and inside signature panel itself, as shown in **Fig.A.3.5: Invalid Signature:**

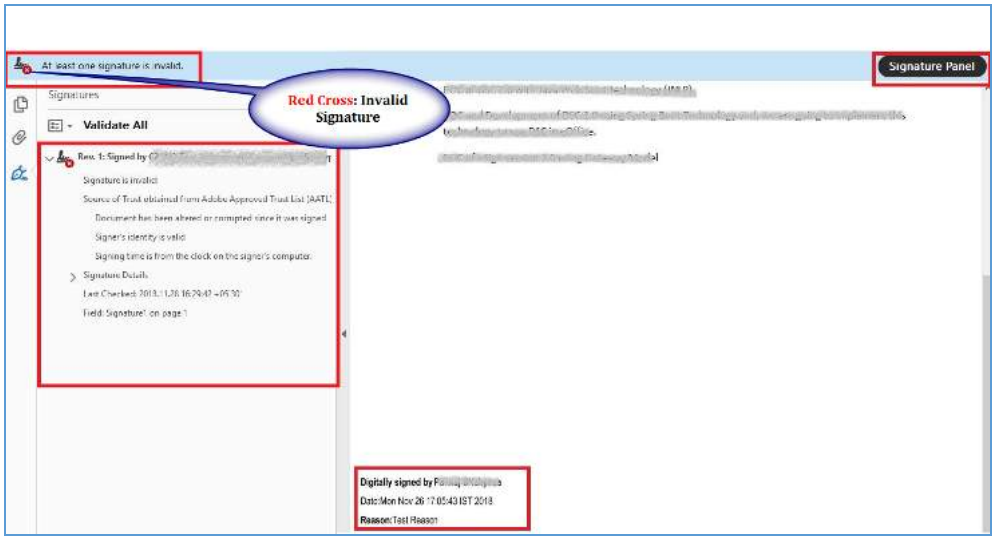


Fig.A.3.5: Invalid Signature

Annexure IV

Identifying Your System

Windows OS

Check Windows version:

- Right click **My Computer/ This PC** icon on desktop or start menu and select "**Properties**" tag.
- A screen appears displaying the **OS Version** is shown in **Fig.A.4.1:**

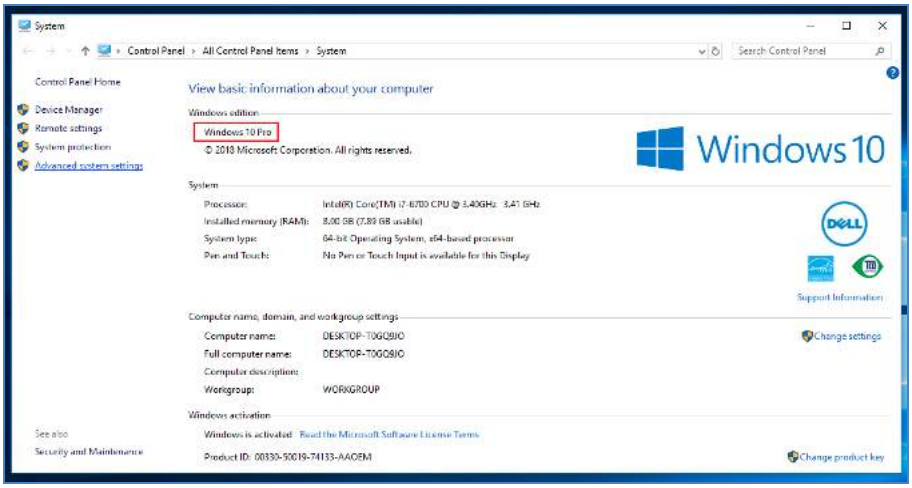


Fig.A.4.1

MAC OS

Checking MAC version:

- Open the **Terminal.**
- Type the command **"sw_vers",** and press enter **(Fig.A.4.5)**, and the version of MAC will gets displayed (marked in red color box).

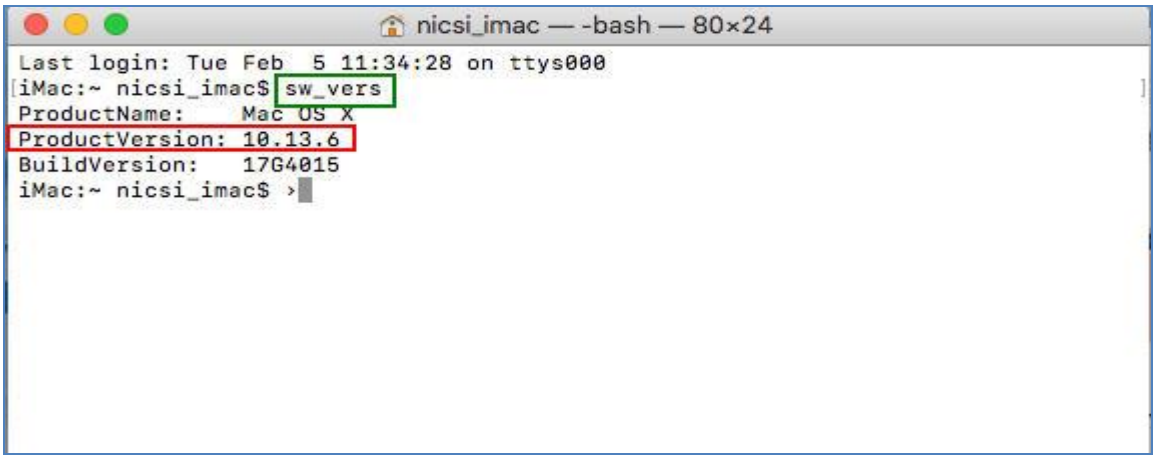


Fig.A.4.5

Ubuntu OS

Checking Ubuntu version:

- Open the **Terminal.**
- Type the command **"lsb_release -a",** press enter **(Fig.A.4.7)**, and the version of Ubuntu will gets displayed (marked in red color box).

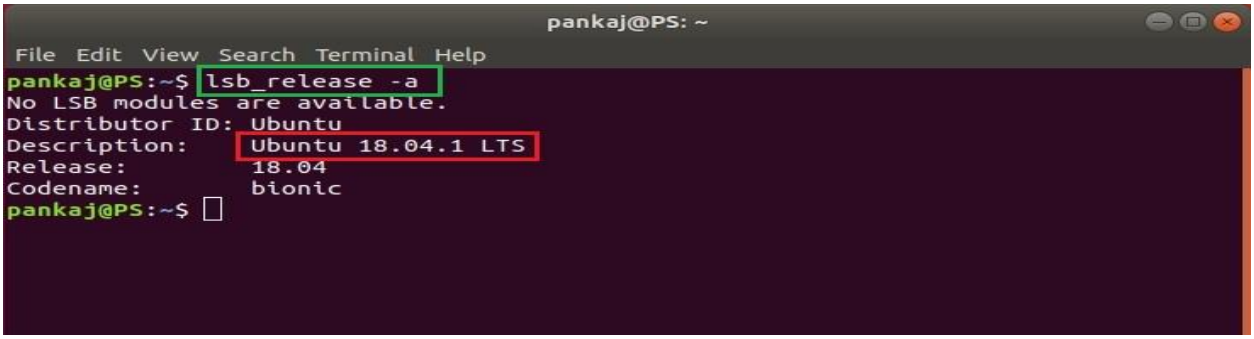


Fig.A.4.7

Created By	Reviewed By	Approved By
Maheep Singh	Pankaj Shakya	Navneet Kaur Scientist- C eOffice Project Division

eOffice Project Divison

National Informatics Centre

Ministry of Electronics and Information Technology
A-Block, CGO Complex, Lodhi Road, New Delhi - 110003 India