सत्यमेव जयते

eOffice

A DIGITAL WORK PLACE SOLUTION

DSC

Digital Signature Certificate(DSC) Signer Service

User Guidelines

NIC-EOF-DSC-UG-001

Prepared by
National Informatics Centre

Amendment History

Date	Document Version	Description	Author
13 June 2018	2.0	User Guidelines	eOffice Project Division
03 October 2018	3.0	User Guidelines	eOffice Project Division
29 November 2018	3.5	User Guidelines	eOffice Project Division
05 March 2019	4.1	User Guidelines	eOffice Project Division
26 February 2020	4.1.01 **(change in installation steps for windows)**	User Guidelines	eOffice Project Division

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.

Latest versions of browsers started discontinuing the applet support (around the Year 2016-2017) essentially to firm up the security. Accordingly the signing mechanisms that eOffice (or for that matter any other web application) was using earlier, therefore, also had to change. Consequently, eOffice Team developed, a new signer that would work with latest browsers and would not require applet to run. It is essentially a service that would require to be installed, one time, on individual client's machines of the user. This service will work on windows/MAC/Ubuntu Operating System.

This document provides very simple steps that will guide the user to install the signer service smoothly on his/her local client machine.

Section 1: DSC Signer Service

The new DSC signer service can download 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**:

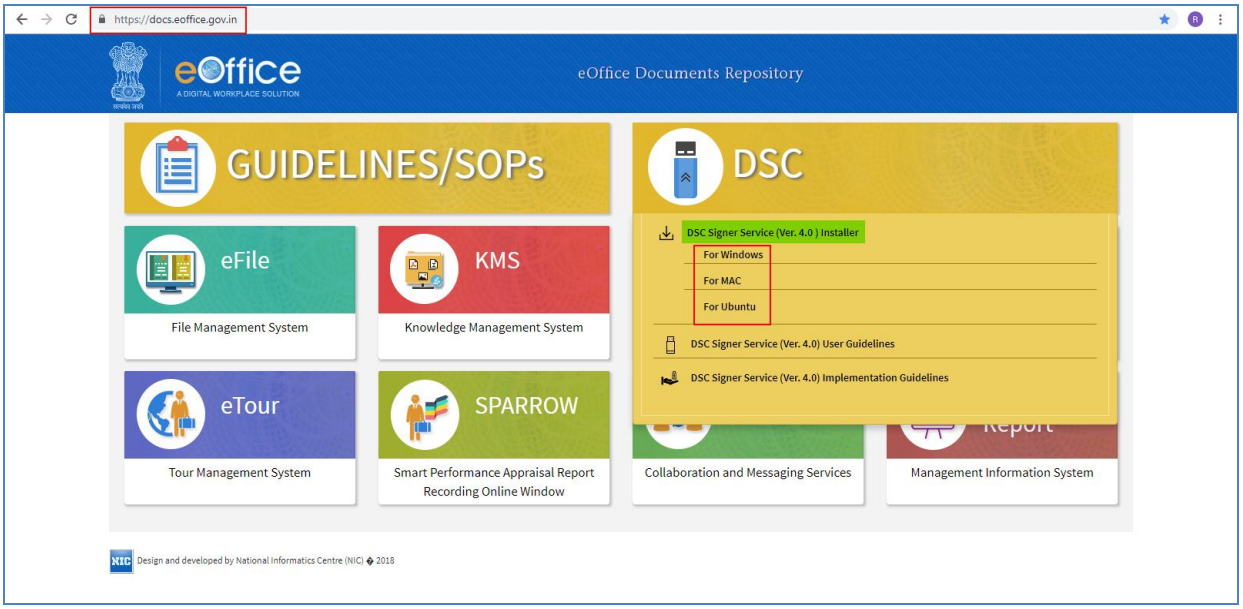


Fig.1.1

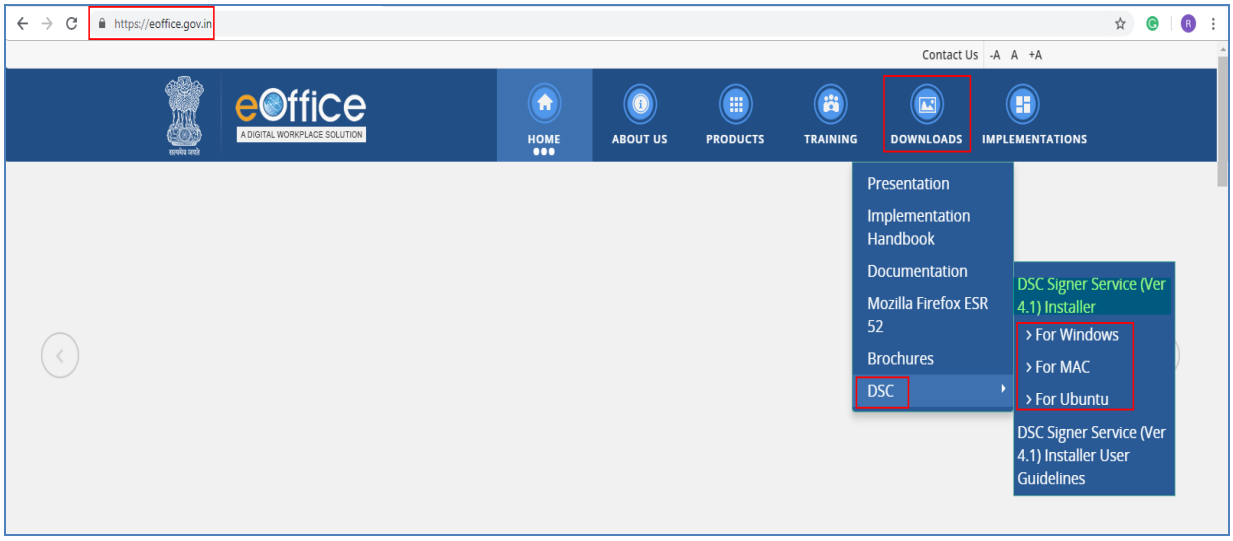


Fig.1.2

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

Minimum client's machine Requirements	
Windows OS	Windows 7 & above.
MAC OS	MAC 10.7 & above.
Ubuntu OS	Ubuntu 18 & above.
JRE	Version 1.8 or above appropriate as per OS
Availability of ports 55100 and 55101	

Section 2: Windows OS

Download the Signer 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 to check if user machine has java installed or not.
- This also checks that if ports 55100 and 55101 is free or not and displays appropriate message as shown in **Fig.2.1:**

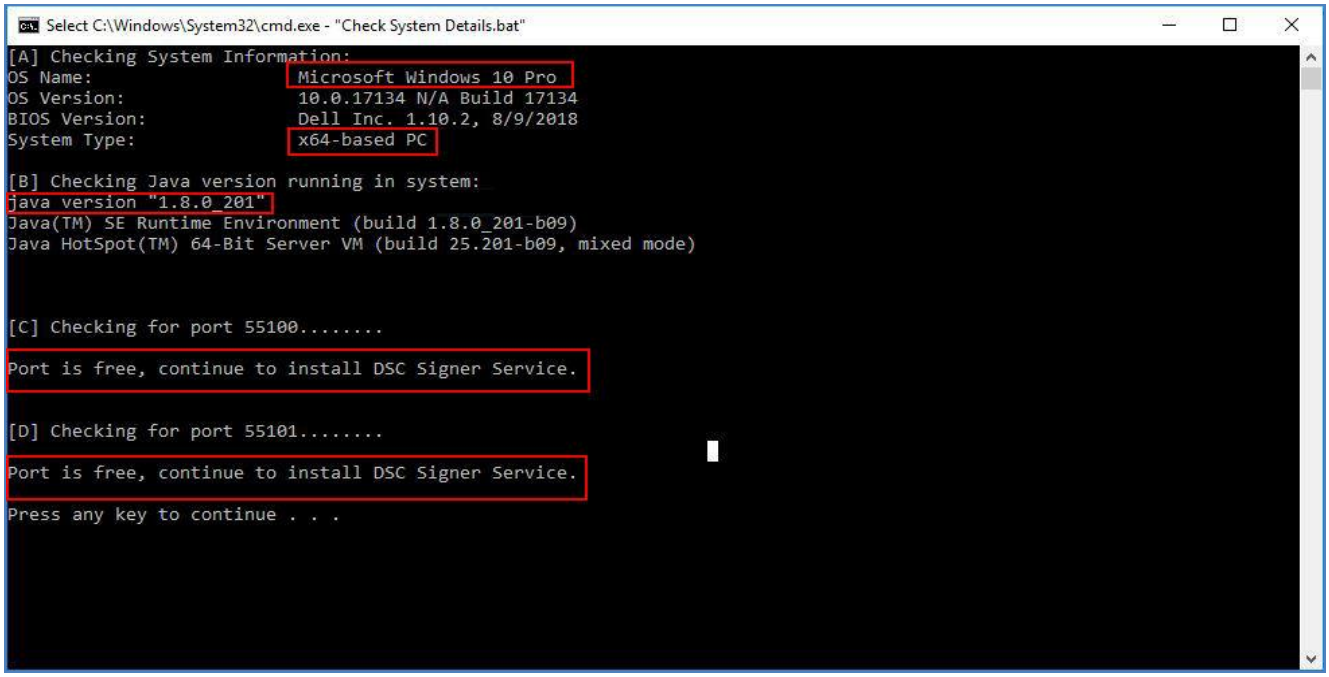


Fig.2.1

Note:

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

Pre-requisites for DSC Signer Service Installer for Windows

Following four activities to be completed by User(s).		
S. No.	**Activities**	**Remarks**
1.	Version 1.8 or above appropriate as per OS.	To be Downloaded by Individual User at client machine. (Refer website https://www.java.com/en/ for JRE installation). **Note:** 1. User(s) with 32-bit windows OS needs to install 32-bit JRE. 2. User(s) with 64-bit windows OS needs to install 64-bit JRE.
2.	Add/ Import SSL certificates to the browsers.	To Add/ Import SSL certificates to the browsers (Refer **Annexure I** for steps).
3.	Re-register DSC certificate.	For user(s) who have already DSC registered in the eOffice application, then to use new DSC Signer Service, they have to de-activate already registered certificate and register again one time. (Refer **Annexure V** for steps).
4.	Internet connectivity is required to check for certificate revocation status.	Check the Internet connectivity at every client machine.

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 Windows OS

For Bulk User:

To install Digital Signer Service on multiple systems through windows server, administrator can install this service in silent mode.

For Single User:

- Locate the **Digital Signer Service 4.1_x64.msi / Digital Signer Service 4.1_x86.msi** file from downloaded bundle.
- Select the **Digital Signer Service 4.1_x64.msi / Digital Signer Service 4.1_x86.msi** file as per the system configuration **(32 bit or 64 bit respectively).**
- Double click required **msi** file to start the installation as shown in **Fig.2.2 :**

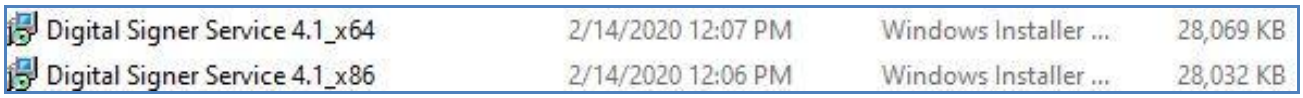


Fig.2.2

- A welcome page appears, click **Next** (Next >) button to continue as shown in **Fig.2.3:**

Fig.2.3

- Digital Signer Service: License Agreement window appears, read the agreement. Click I Accept Radio button and then click Next (Next >) button as shown in **Fig.2.4**:

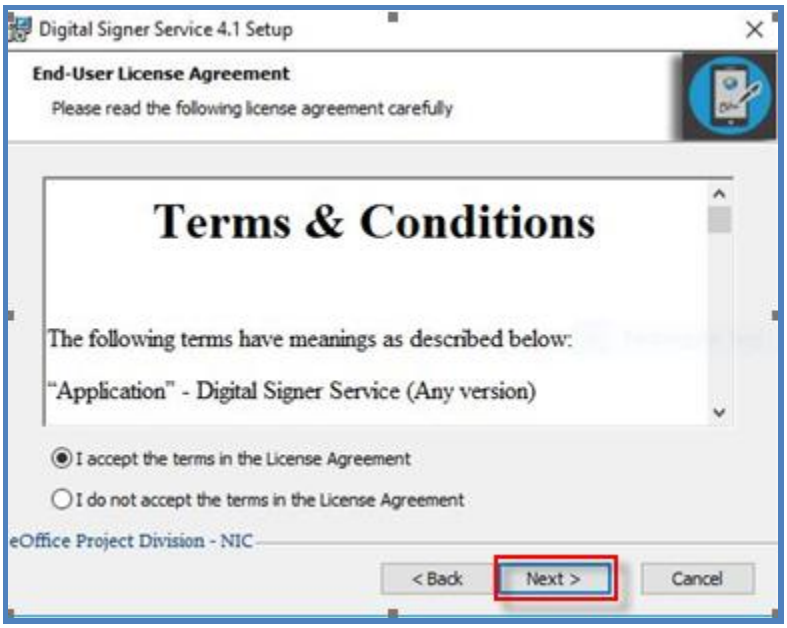


Fig.2.4

- For custom installation, click **Browse (** Browse... **)** button, select the directory as shown in **Fig.2.5** and click **Next (** Next > **)** button.

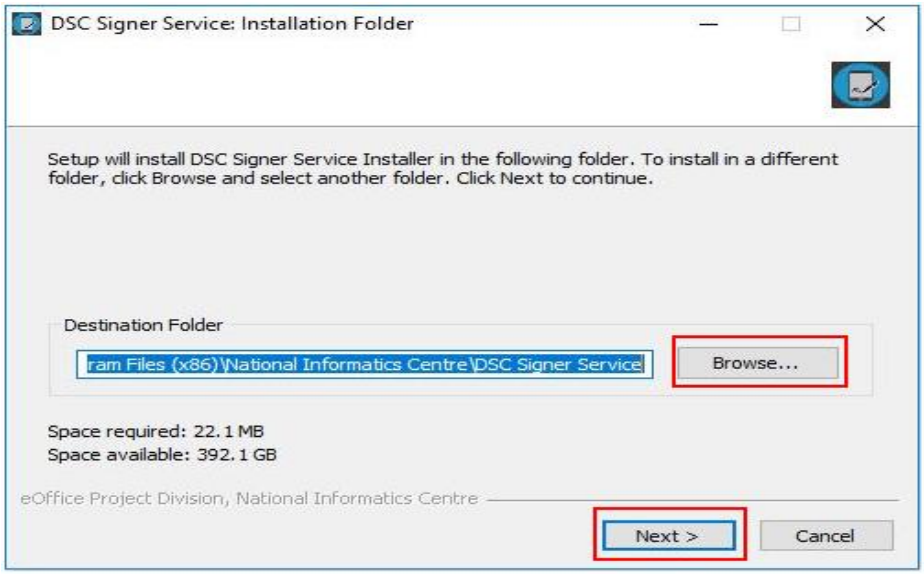


Fig.2.5

OR

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

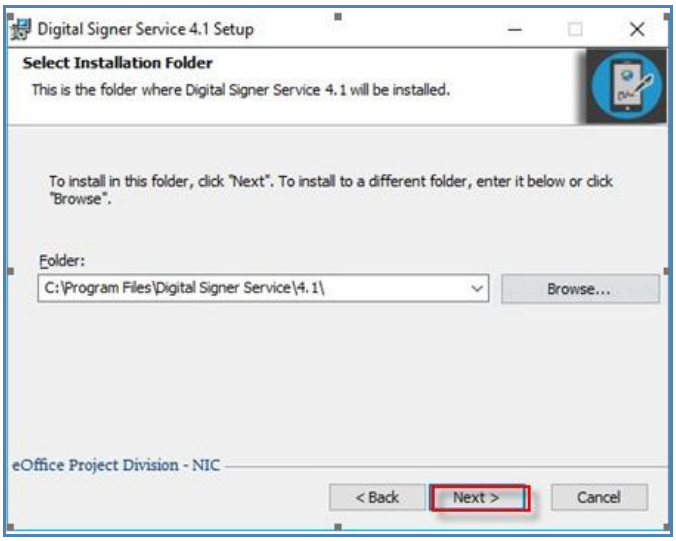


Fig.2.6

Note:

If Digital Signer Service already exists in the system, click on **Uninstall** button as shown in the **Fig.2.7**:

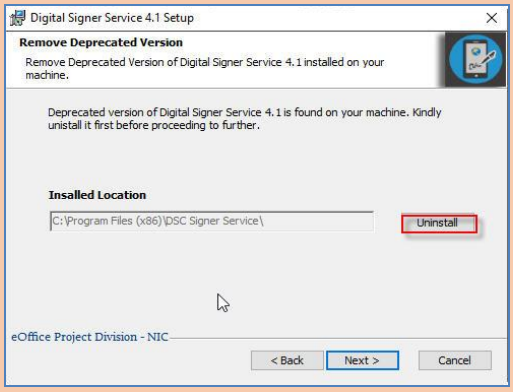


Fig.2.7

A confirmation window will appear, click on **Uninstall** button to start the uninstallation as shown in **Fig.2.8:**

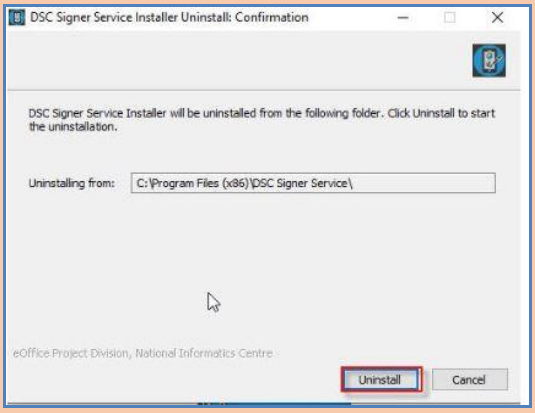


Fig.2.8

- Ready to Install window appears asking for SSL certificate, click the **Yes** radio button and then click **Install** (Install) button as shown in **Fig.2.9:**

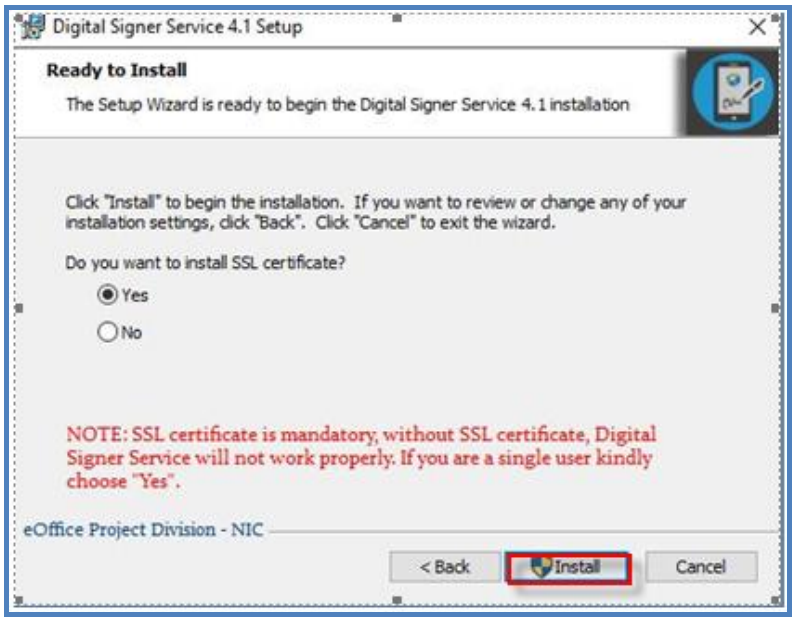


Fig.2.9

Note: single certificates are mandatory for siging purpose, if user clicks on **No** option while installing the Digital signer service, then they have to install the certificate manually.

- Process will take some moments to complete the installation as shown in **Fig.2.10:**

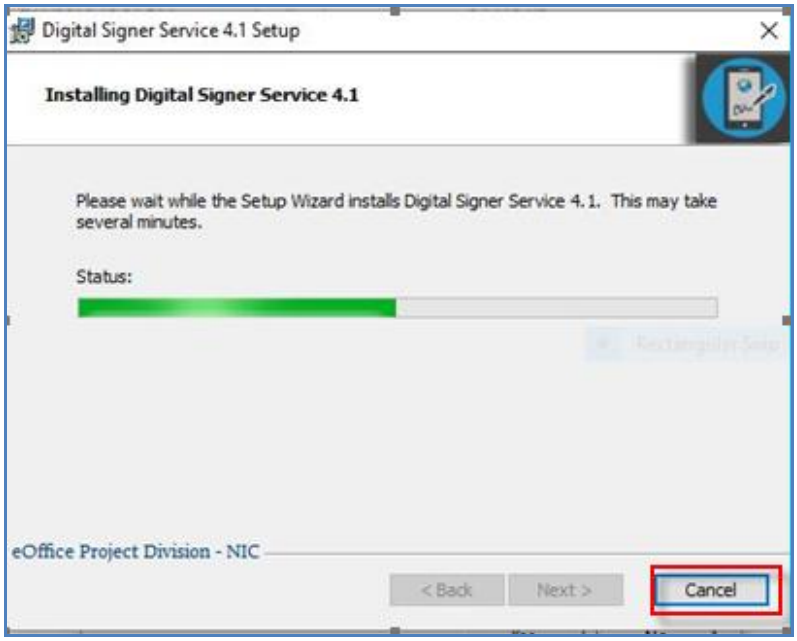


Fig.2.10

- This completes the installation of **Digital Signer Service** for Windows user(s).
- A shortcut will be created on the desktop, named **Digital Signer Service 4.1**.
- After completion of installation it is required to either run the **Digital Signer Service** manually or reboot the system for the first time.

Steps to manually START the Digital Signer Service Installer are:

- Double click the desktop icon **"Digital Signer Service 4.1"**.
- The service will take few seconds to start.
- A message prompts **"DCS Signer Service started successfully"**, as shown in **Fig.2.11**:

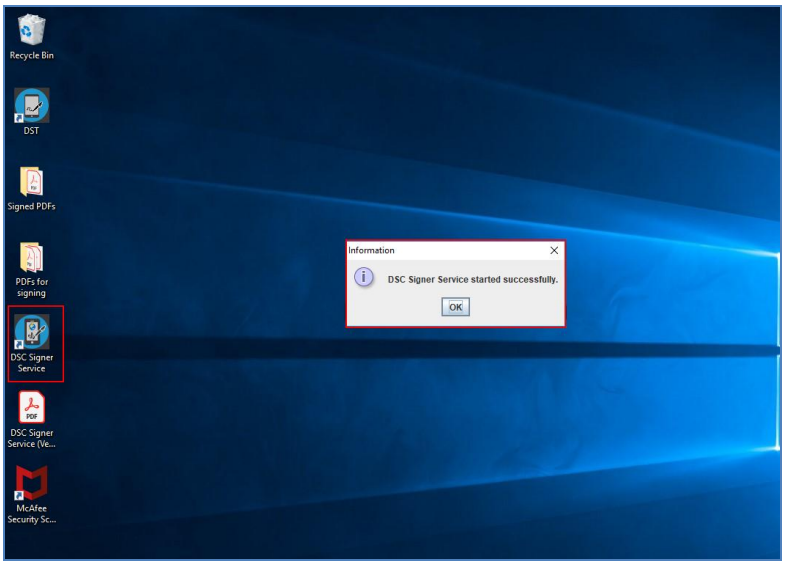


Fig.2.11

Steps to manually STOP the Digital Signer Service Installer are:

- Double click the desktop icon **"Digital Signer Service 4.1"**.
- DSC Signer Service pop-up window appears, click **Stop DSC Signer Service** (

), as shown in **Fig.2.12**:

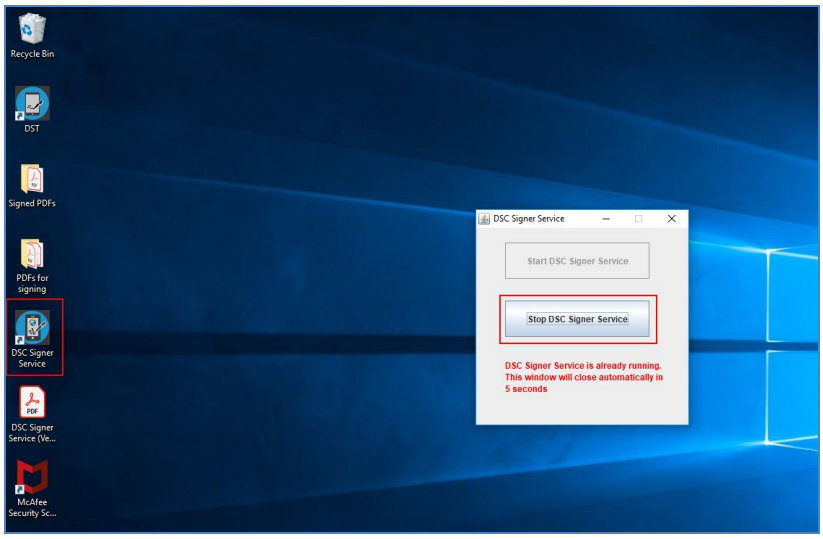


Fig.2.12

Note:

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

2. While service is running and user double clicks the Digital Signer Service 4.1 desktop icon and does not take any action, the Digital Signer Service remains running and the window will get disappear automatically after 10 seconds.

Section 3: MAC

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

Pre-requisites for DSC Signer Service Installer

Following four activities to be completed by User(s).		
S. No.	**Activities**	**Remarks**
1.	Version 1.8 or above appropriate as per OS	In case of MAC only installer needs to be downloaded.
2.	Add/ Import SSL certificates to the browsers.	To Add/ Import SSL certificates to the browsers (Refer **Annexure I** for steps).
3.	Re-register DSC certificate.	For user(s) who have already DSC registered in the eOffice application, then to use new DSC Signer Service, they have to de-activate already registered certificate and register again one time. (Refer **Annexure V** for steps).
4.	Internet connectivity is required to check for certificate revocation status.	Check the Internet connectivity at every client machine.

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 MAC OS

- Locate the **Dsc_Signer_Service.sh** file from downloaded bundle.
- Open terminal at the same location of Dsc_Signer_Service.sh file.
- Run the command "***sudo bash Dsc_Signer_Service.sh***" on the terminal for MAC OS.
- In case other process is using port 55100 and 55101, system will ask user for YES/NO as shown in **Fig.3.1**:

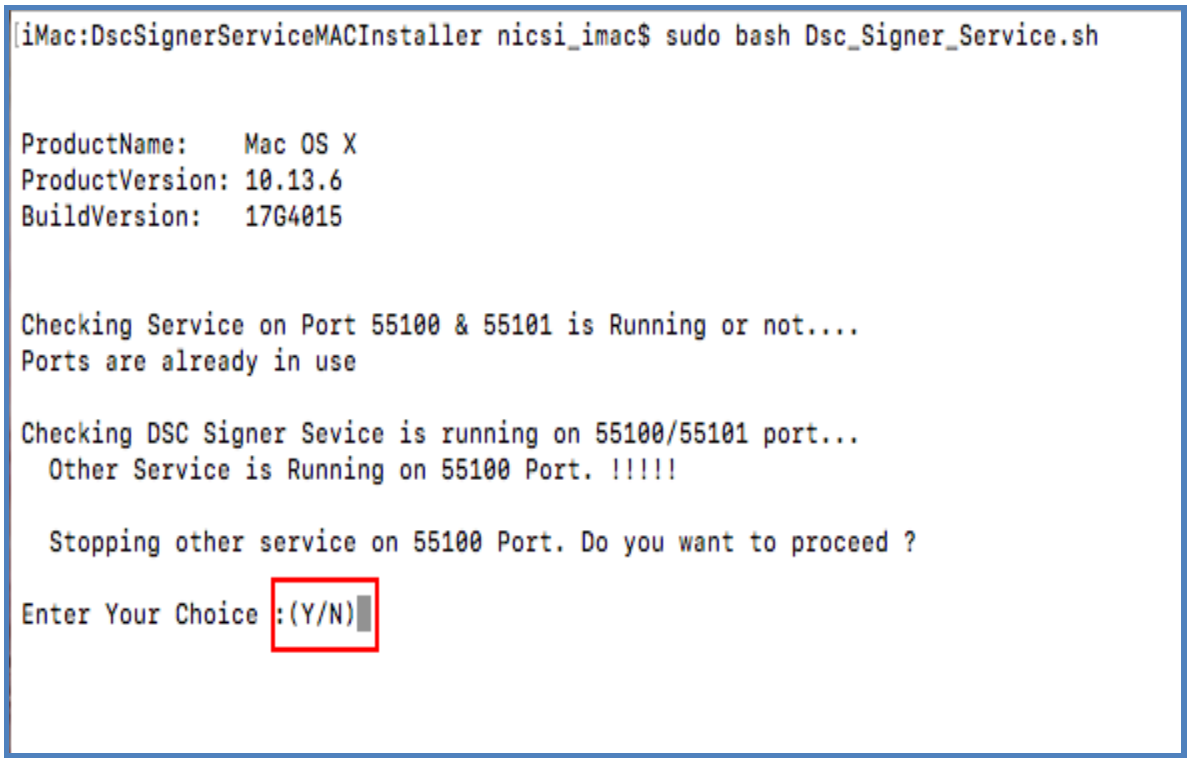


Fig.3.1

- Type '**Y**' for terminating that process and continue installation of DSC Signer Service otherwise type '**N**' for terminating the DSC Signer Service installation.
- This completes the installation of **DSC Signer Service** for MAC user(s).
- After successful installation, a message "**DSC Signer Service started successfully**" will be displayed and is shown in **Fig.3.2:**

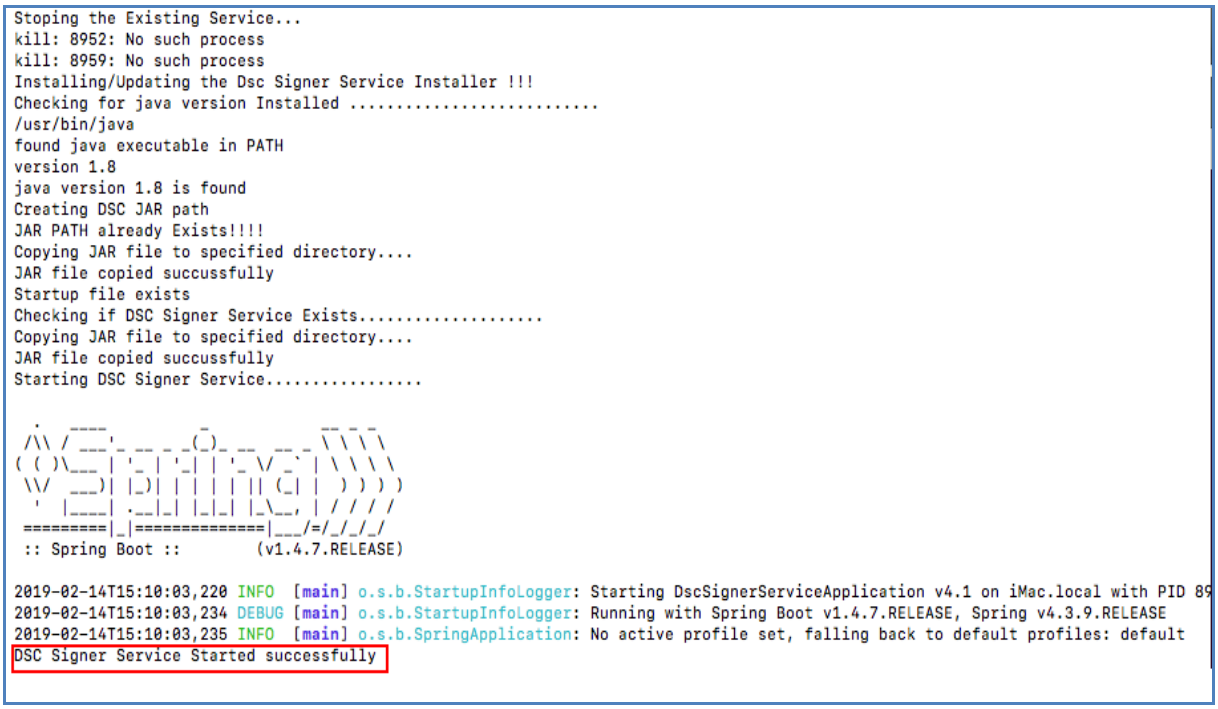


Fig.3.2

Note:

1. While using DSC application if a dongle is plugged-out, then, occasionally user has to manually restart the DSC signer service. For restaring the DSC Signer Service manually refer **Annexure II (Troubleshooting →Problem 1)**.
2. There are many providers for DSC dongles and sometimes issue specific to DSC dongle hardware may come, for which the respective vendor may be approached.
3. To import the certificates refer **Annexure I** (Add/ Import SSL certificates to the Browser).
4. Refer to **Annexure IV** for manually identifying the **JAVA**, **OS** and **DSC Signer Service status** details.

Section 4: Ubuntu

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

Pre-requisites for DSC Signer Service Installer for Ubuntu OS

Following four activities to be completed by User(s).		
S. No.	**Activities**	**Remarks**
1.	Version 1.8 or above appropriate as per OS	In case of Ubuntu only installer needs to be downloaded.
2.	Add/ Import SSL certificates to the browsers.	To Add/ Import SSL certificates to the browsers (Refer **Annexure I** for steps).
3.	Re-register DSC certificate.	For user(s) who have already DSC registered in the eOffice application, then to use new DSC Signer Service, they have to de-activate already registered certificate and register again one time. (Refer **Annexure V** for steps).
4.	Internet connectivity is required to check for certificate revocation status.	Check the Internet connectivity at every client machine.

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 **Dsc_Signer_Service.sh** file from downloaded bundle.
- Open terminal at the same location of DscSignerService.sh file.
- Run the command "***sudo bash Dsc_Signer_Service.sh***" on the terminal for Ubuntu OS.
- In case other process is using port 55100 and 55101, system will ask user for YES/NO as shown in **Fig.4.1**:

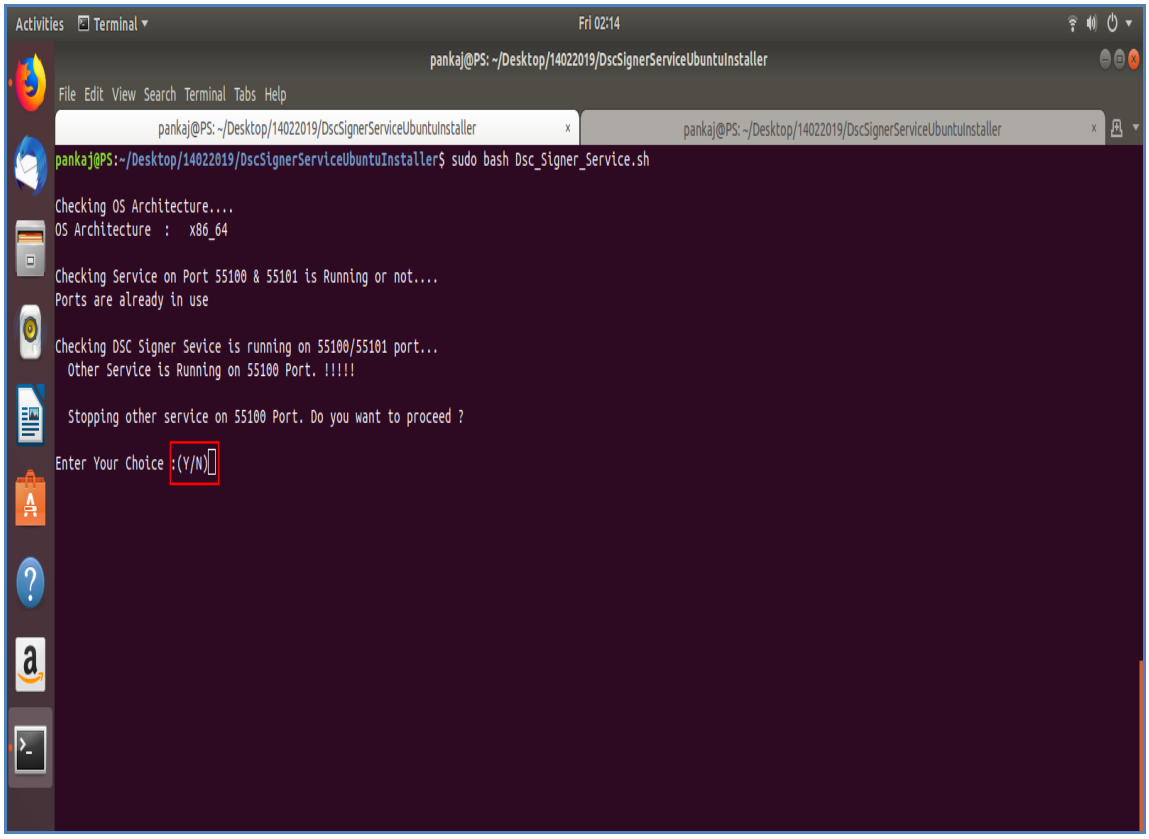


Fig.4.1

- Type '**Y**' for terminating that process and continue installation of DSC Signer Service otherwise type '**N**' for terminating the DSC Signer Service installation.
- This completes the installation of **DSC Signer Service** for Ubuntu user(s).
- After successful installation, a message "**DSC Signer Service started successfully**" will be displayed and is shown in **Fig.4.2:**

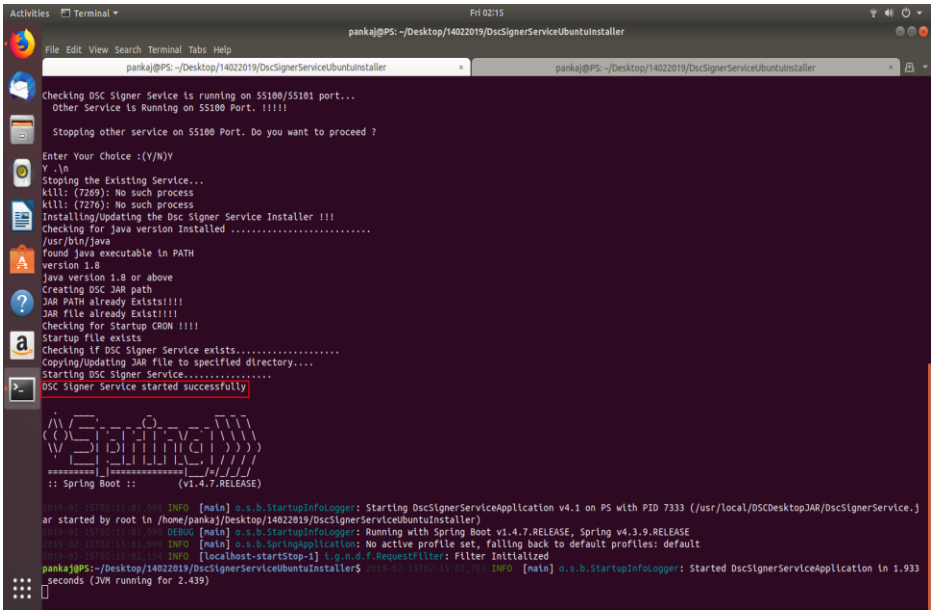


Fig.4.2

- Then, reboot the system.

Steps to manually START the DSC Signer Service Installer are:

- Double click the desktop icon **"DSC Signer Service"**.
- The service will take few seconds to start.
- A message prompts **"DCS Signer Service started successfully".**

Steps to manually STOP the DSC Signer Service Installer are:

- Double click the desktop icon "**DSC_Signer_Service**".
- DSC Signer Service pop-up window appears, click **Stop DSC Signer Service** (

) button.
- While service is running and user double clicks the **DSC_Signer_Service** desktop icon and does not take any action, the DSC Signer Service remains running and the window will get disappear automatically after 10 seconds.

Note:

1. While using DSC application if a dongle is plugged-out, then, occasionally user has to manually restart the DSC signer service. For restaring the DSC Signer Service manually refer **Annexure II (Troubleshooting→Problem 1)**.
2. There are many providers for DSC dongles and sometimes issue specific to DSC dongle hardware may come, for which the respective vendor may be approached.
3. To import the certificates refer **Annexure I** (Add/ Import SSL certificates to the Browser).
4. Refer to **Annexure IV** for manually identifying the **JAVA**, **OS** and **DSC Signer Service status** details.

Section 5: Checking the Service Status

For Windows/MAC/ Ubuntu

DSC Signer Service uses 55100 & 55101ports.

http port: 55100
https port: 55101

The user should check for availability of both ports. :

1. To check service running status, go to the "**Pre-requisites**" folder inside **DscSignerServiceInstaller** folder and then, locate the **DscSignerserviceTest.html file**.
2. Open **DscSignerserviceTest.html** file in preferred browser and then click **Check for HTTP Port** (Check for HTTP Port) button or **Check for HTTPS Port** (Check for HTTPS Port) button as shown in **Fig.5.1**:

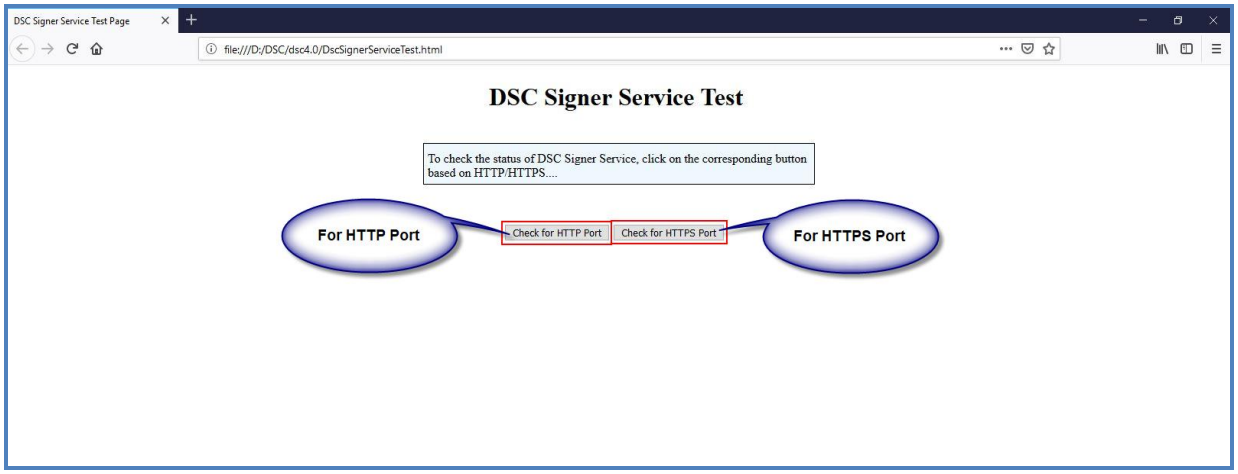


Fig.5.1

3. The running statuses for HTTP or for HTTPS are shown in **Fig.5.2** & **Fig.5.3**:

Fig.5.2

Fig.5.3

OR

4. To check for service status manually use https://127.0.0.1:portNumber/check/isLive
   For Ex. https://127.0.0.1:55101/check/isLive
   For HTTP check the port 55100.

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

Note :

1. HTTPS will work where the consuming application(s) are running on HTTPs protocol only.
2. HTTP is for eOffice hosted in a closed environment (i.e. where internet connectivity is not available). But, it is always recommended to use HTTPS over HTTP for security reason.
3. The DSC 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 the **DscSignerServiceInstaller** folder (For windows/ For MAC/ For Ubuntu), go to the "**Pre-Requisites**" folder and locate the **DSC Self sign Certificate → 127.0.0.1.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 Mozilla Firefox

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

- Open the Mozilla browser and enter the URL https://127.0.0.1:55101/check/isLive as shown in **Fig.A.1.1:**

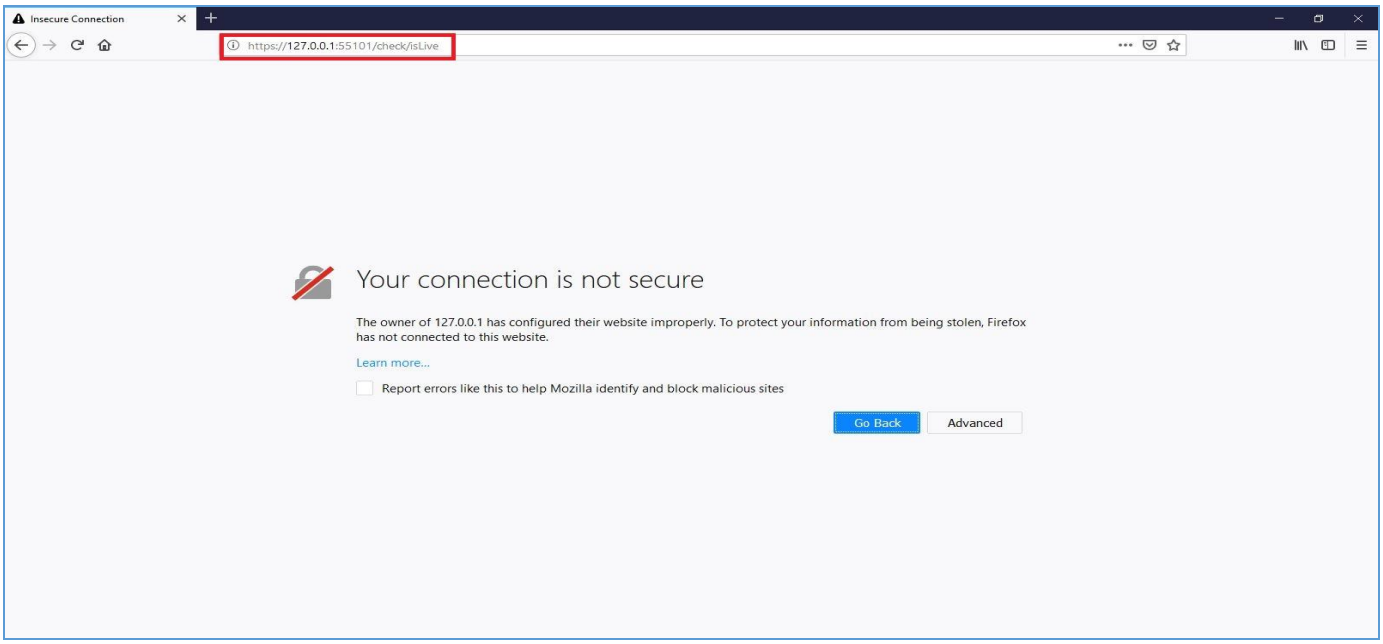


Fig.A.1.1

- Then, the browser will notify the user to add the exception into the list **(Fig.A.1.1)**.

- Click **Advance** (Advanced) button to add an exception **(Fig.A.1.1).**

- A message box appears, click **Add Exception** (Add Exception...) button as shown in **Fig.A.1.2:**

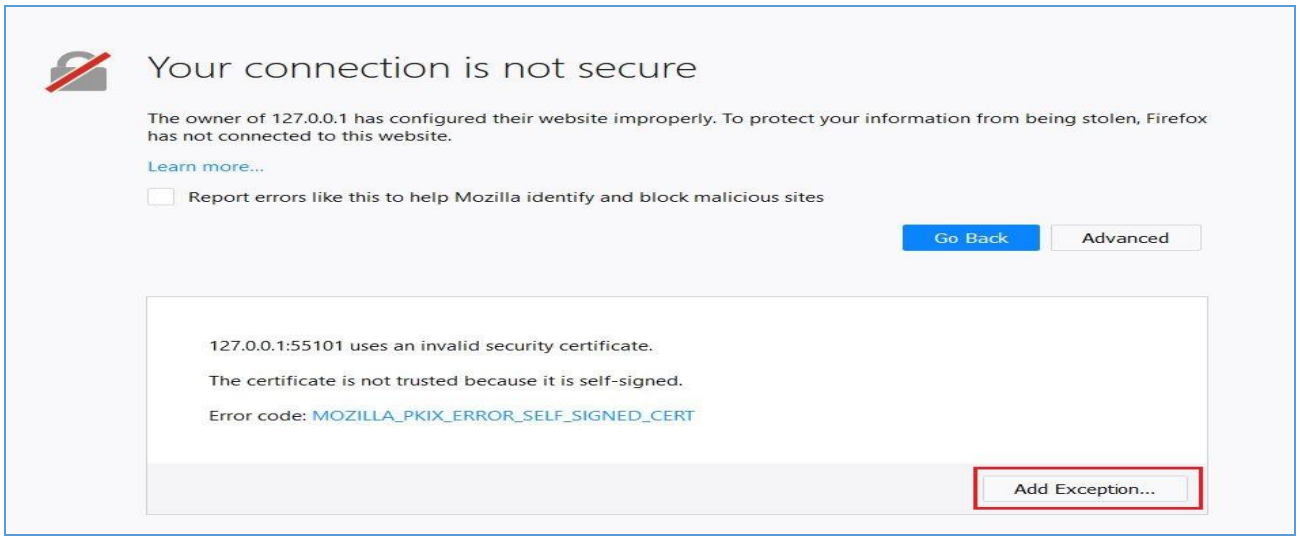


Fig.A.1.2

- The browser will open a window to get the certificate. Click **Confirm Security Exception** (Confirm Security Exception) button to add the exception as shown in **Fig. A.1.3:**

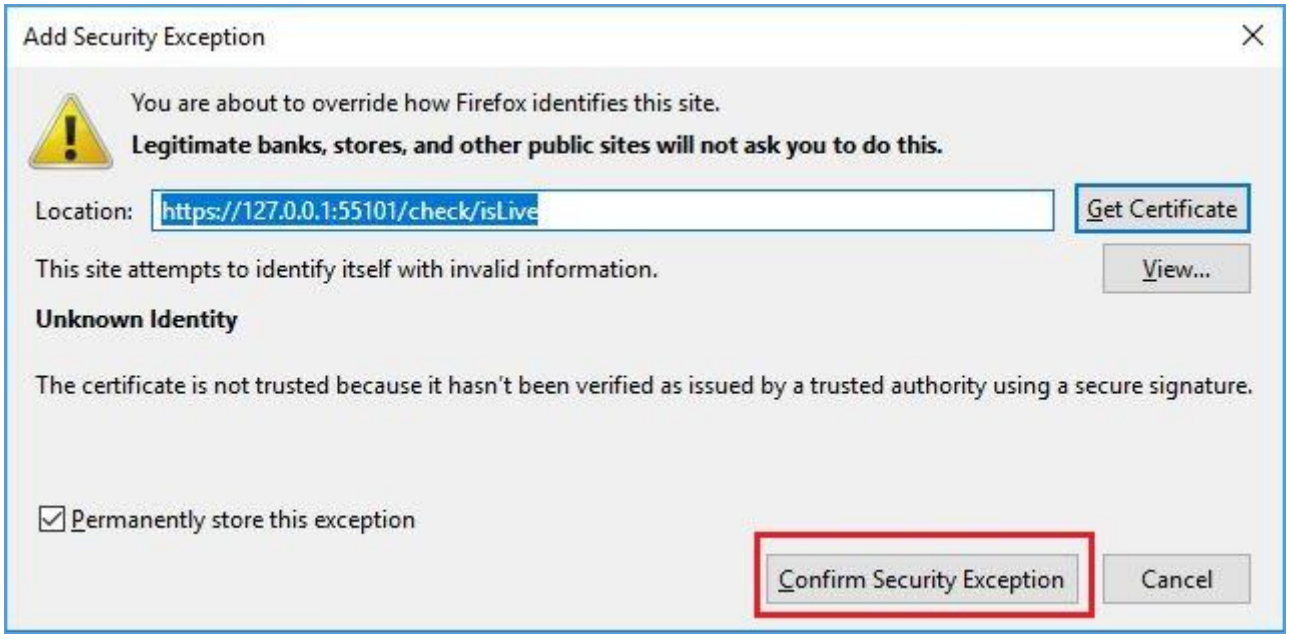


Fig.A.1.3

- The browser will confirm and displays the message "**Success"** as shown in **Fig.A.1.4:**

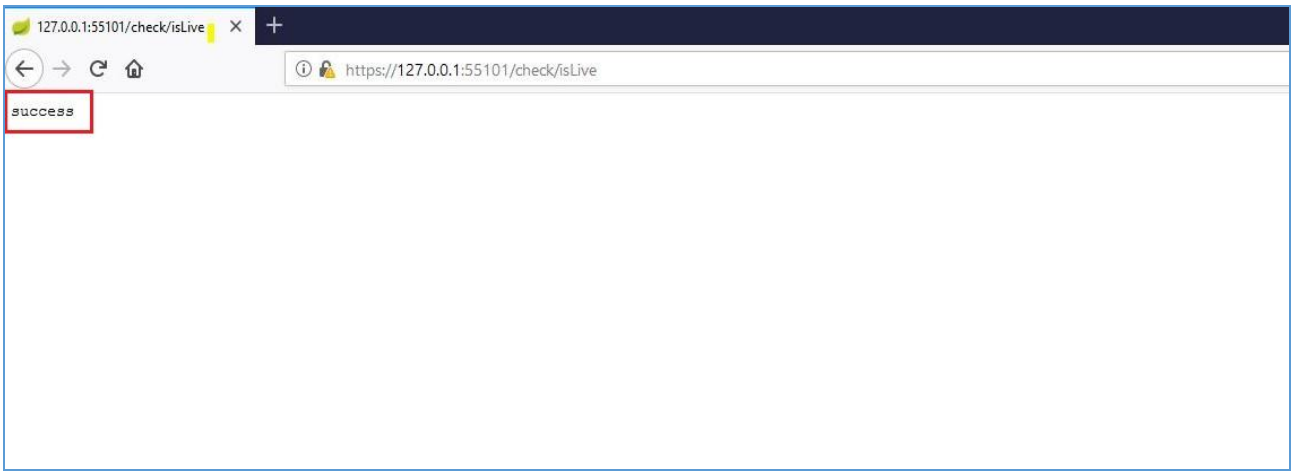

127.0.0.1:55101/check/isLive
https://127.0.0.1:55101/check/isLive
success

Fig.A.1.4

For Chrome

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

- Open the Chrome browser and enter the URL https://127.0.0.1:55101/check/isLive as shown in **Fig.A.1.5:**

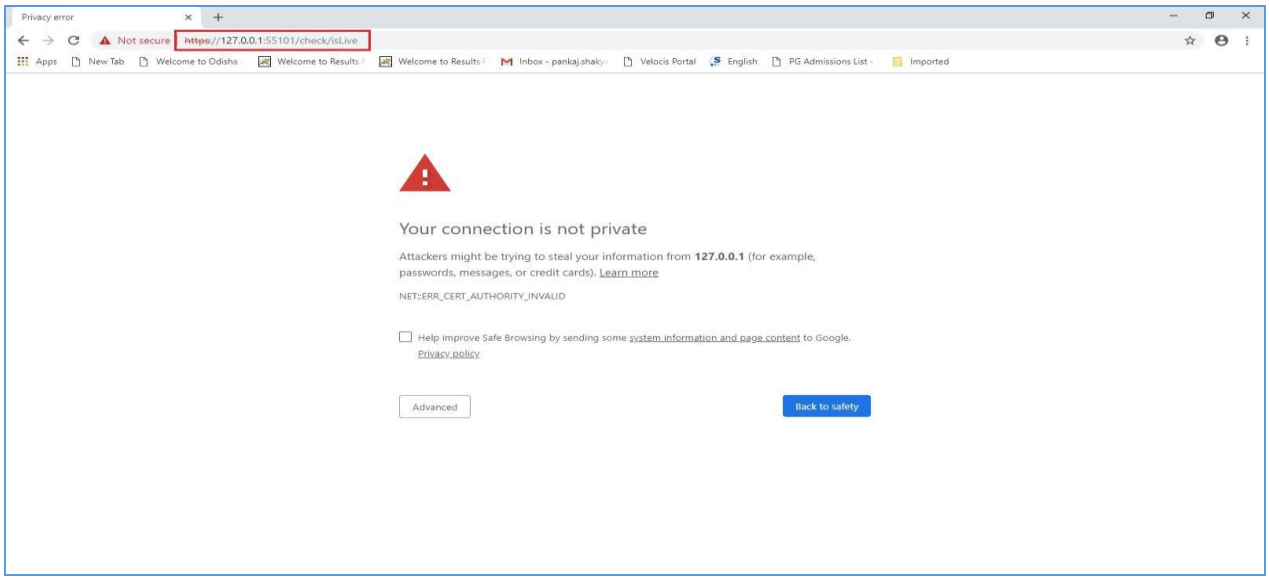


Fig.A.1.5

- The browser will notify the user to add the exception into the list **(Fig.A.1.5)**.
- Click **Advance** (Advanced) button to add an exception **(Fig.A.1.5).**
- A message box appears, click **Proceed to 127.0.0.1 (Unsafe) (** Proceed to 127.0.0.1 (unsafe) **)** button as shown in **Fig.A.1.6:**

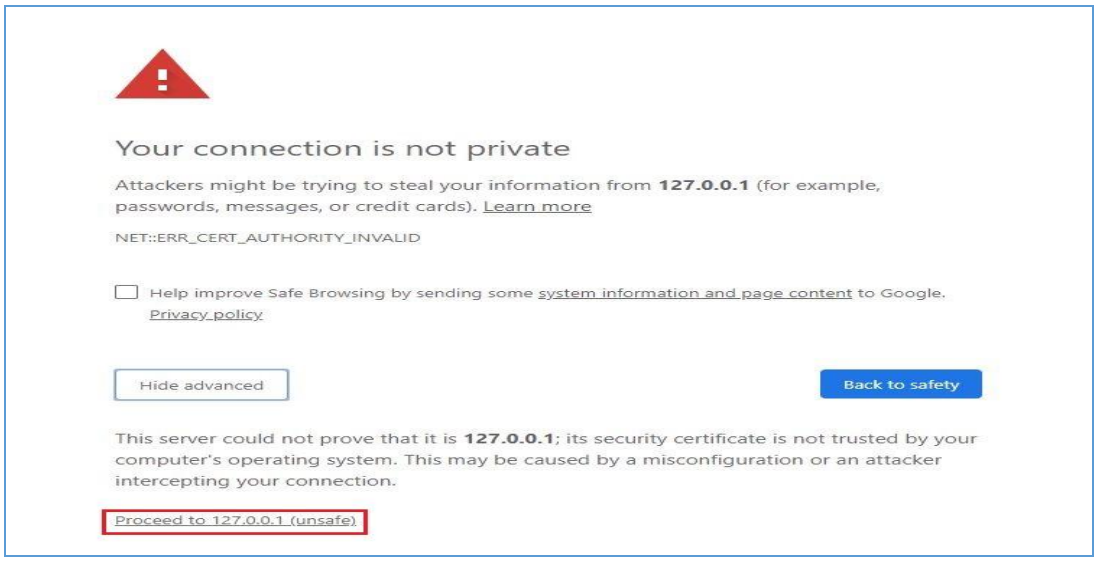


Fig.A.1.6

- The browser will confirm and displays the message "**Success**" as shown in **Fig.A.1.7:**

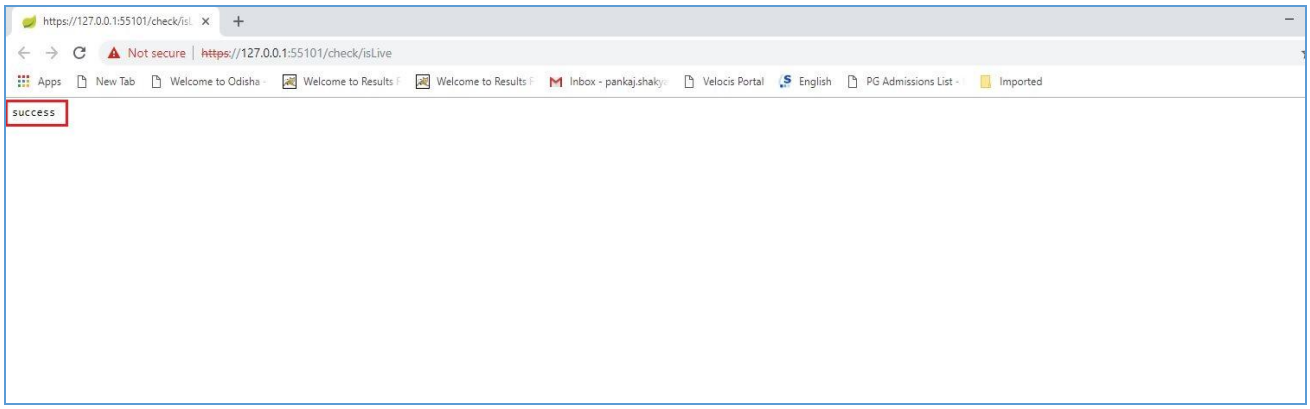


Fig.A.1.7

- Additionally, go to browser and type **"chrome://flags/#allow-insecure-localhost"** in address bar.

- Searched flags screen appears, select **Enabled** to allows requests to localhost over HTTPS even when an self-signed certificate is presented – Mac, Windows, Linux, Chrome OS, as shown in **Fig.A.1.8**:

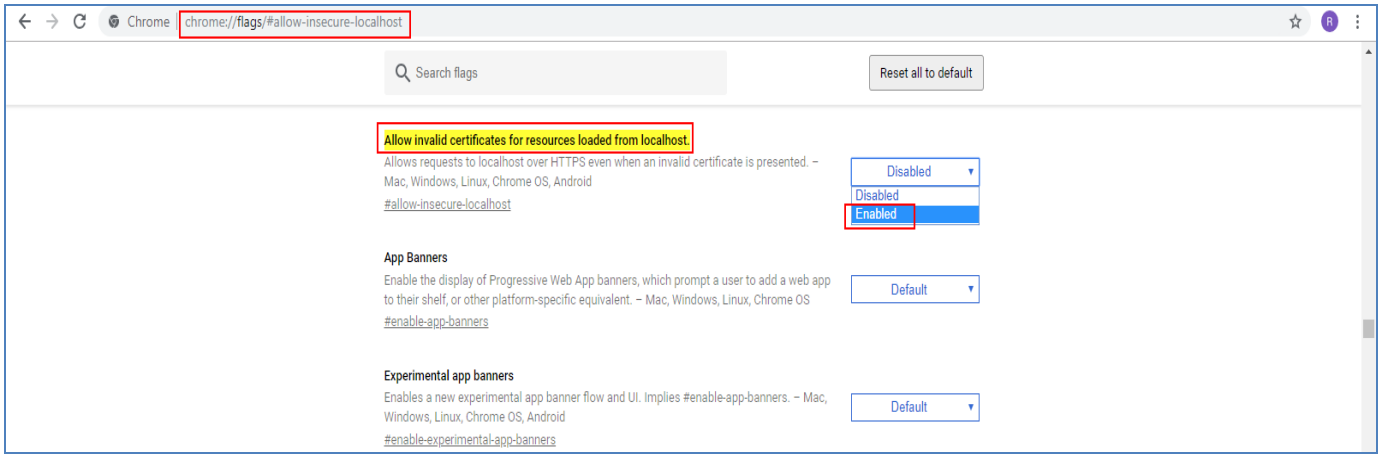


Fig.A.1.8

For Internet Explorer

In case of Internet Explorer, SSL certificate gets automatically imported by the installer.
Steps to check SSL certificate are:

- Open the Internet Explorer and enter the URL https://127.0.0.1:55101/check/isLive.
- The "**Success**"' message will appears, as shown in **Fig.A.1.9**

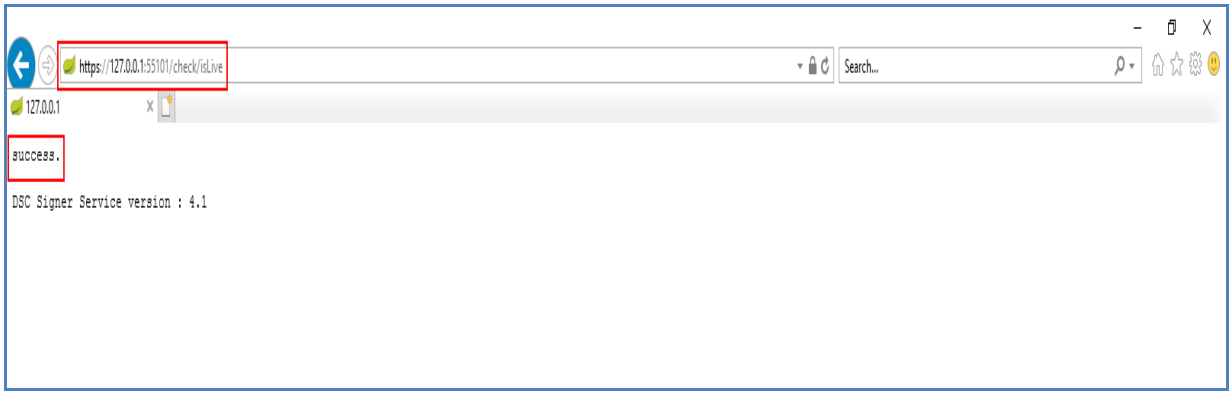


Fig.A.1.9

In case success message does not appear, or certificate is not available, then follow below steps to import the SSL certificate.
Steps to manually update SSL certificate are:

- Open Internet Explorer browser window.
- Go to the **Setting** icon and select the **Internet options**, as shown in **Fig.A.1.10:**

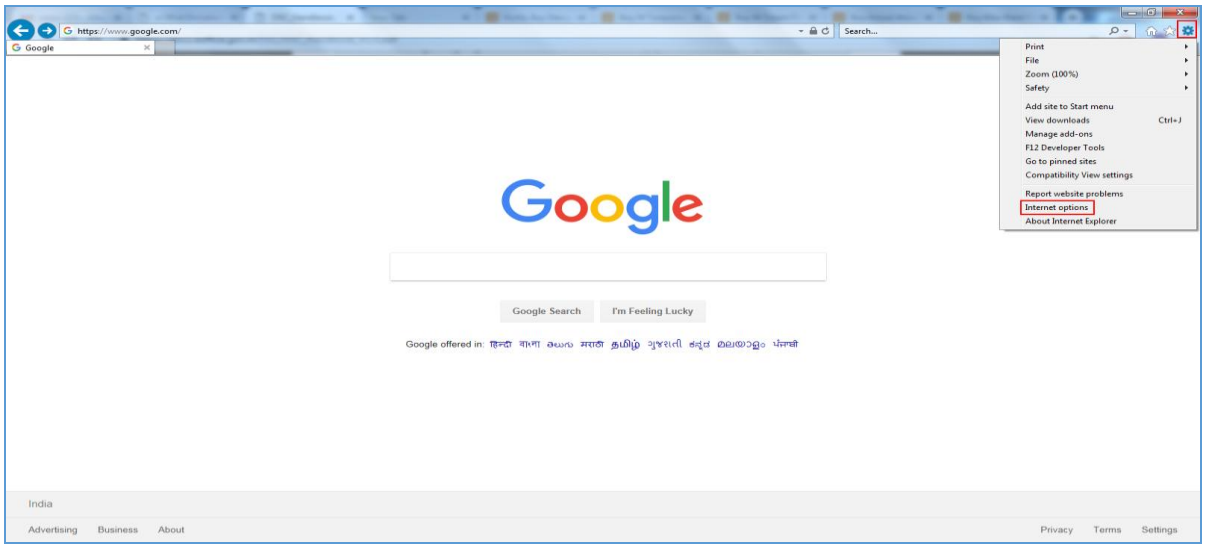


Fig.A.1.10

- Internet Options window will appear, click **Content** (Content) tab and select the **Certificates** (Certificates) button as shown in **Fig.A.1.11:**

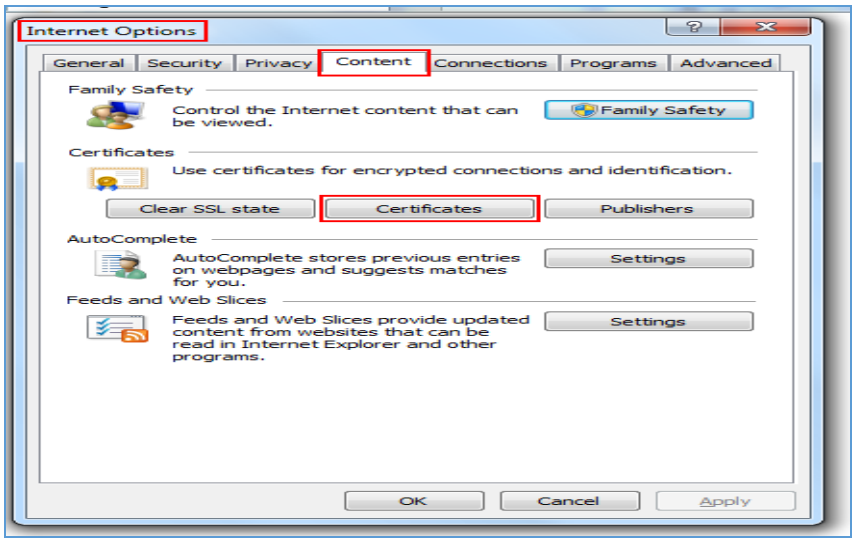


Fig.A.1.11

- Under certificates window go to the **Trusted Root Certification Authorities** (Trusted Root Certification Authorities) tab and click **Import** (Import...) button, as shown in **Fig.A.1.12:**

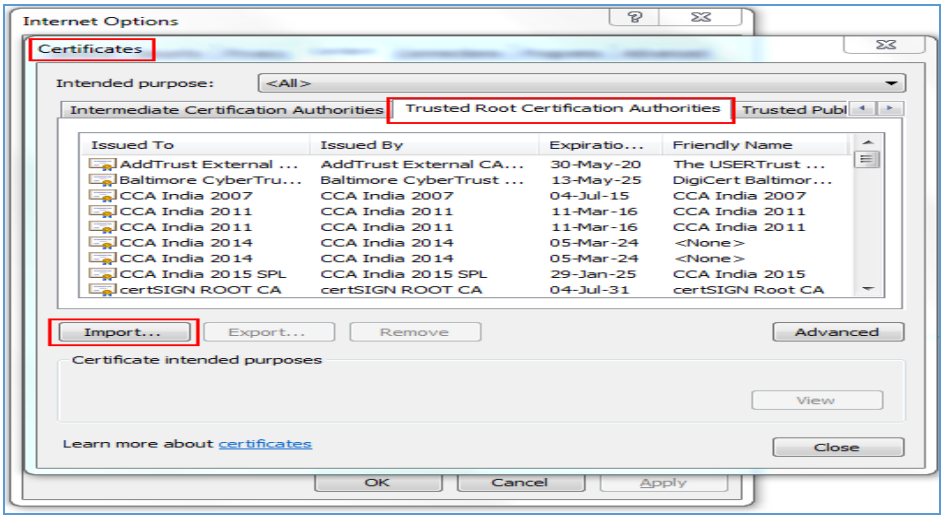


Fig.A.1.12

- The Certificate Import Wizard window appears and click **Next** (Next) button, as shown in **Fig.A.1.13:**

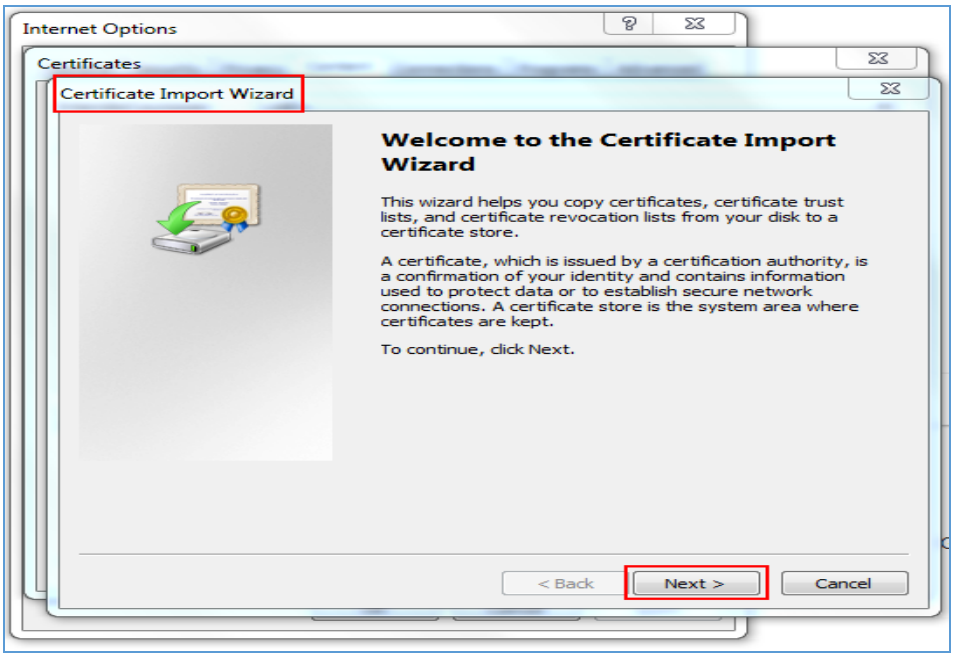
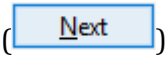


Fig.A.1.13

- Browse the certificate from the saved location and click **Next** (

) button as shown in **Fig.A.1.14** and **Fig.A.1.15:**

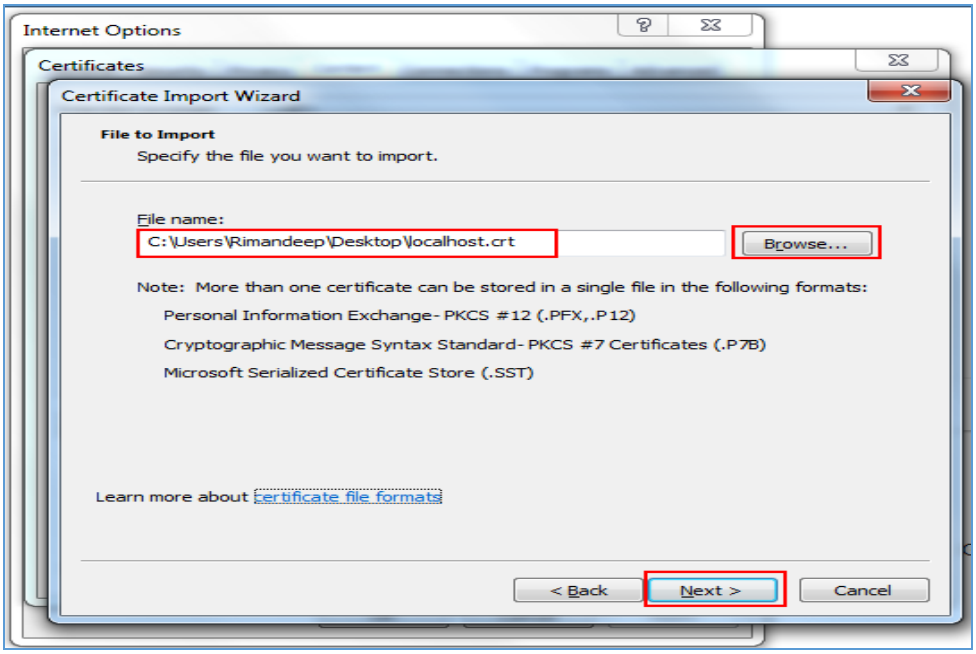


Fig.A.1.14

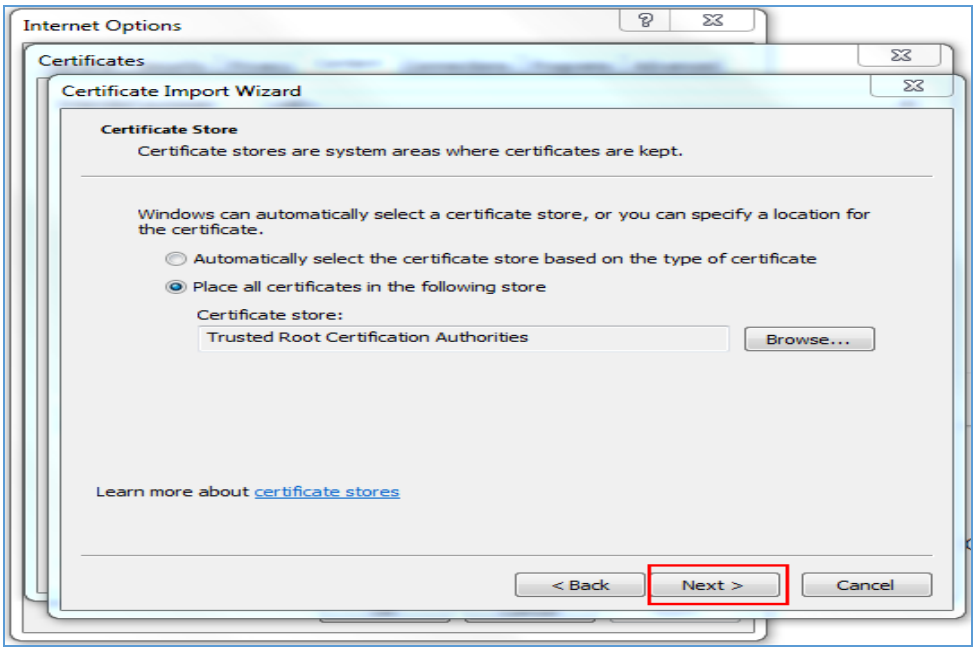


Fig.A.1.15

- Click **Finish** (Finish) button to close the process as shown in **Fig.A.1.16:**

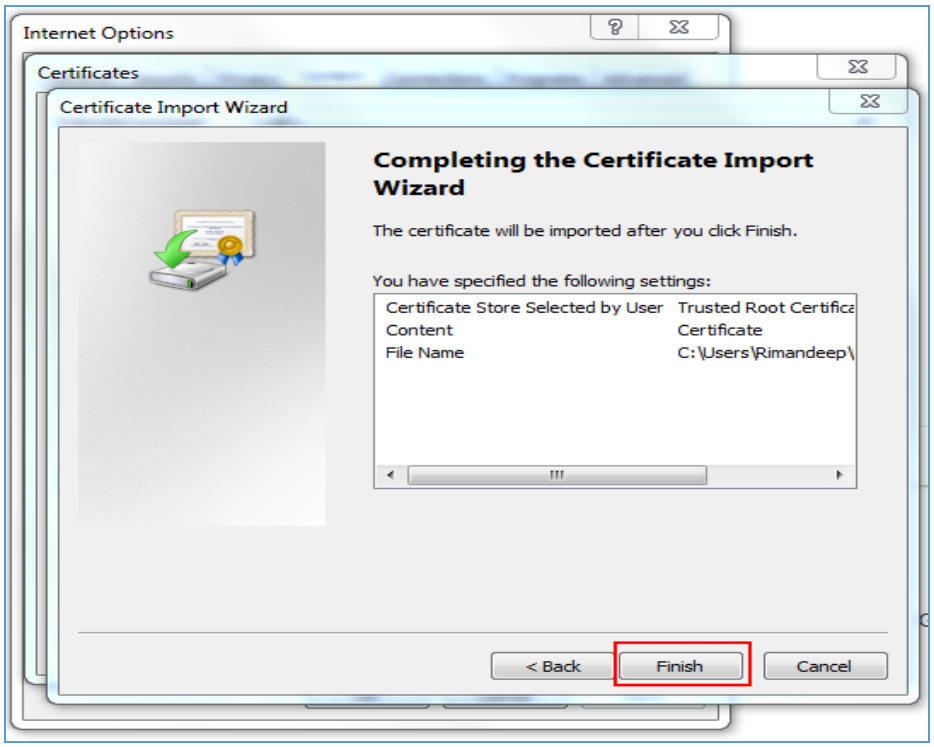


Fig.A.1.16

- Security warning window appears, click **Yes** (Yes) button, as shown in **Fig.A.1.17:**

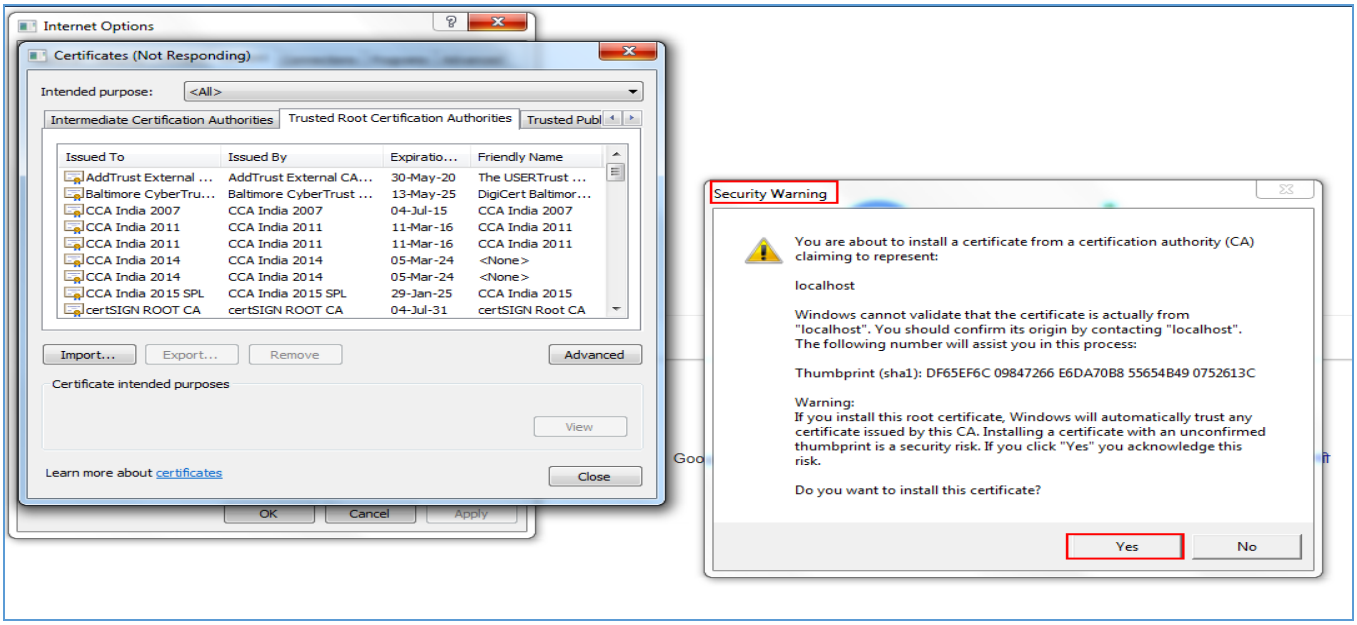


Fig.A.1.17

- The message box prompt "**The import was successful**", click **Ok** (OK) button as shown in **Fig.A.1.18:**

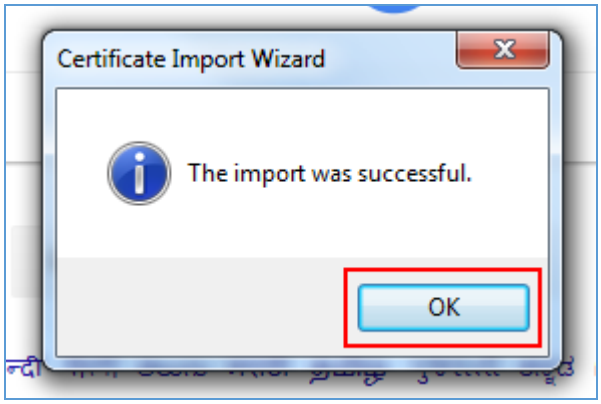


Fig.A.1.18

Annexure –II

Troubleshooting (For DSC Signer Service)

Problem 1

Service is not running after successful installation.

Solution

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

For Windows

Double click the desktop icon **"DSC Signer Service"**.

Screen-shot

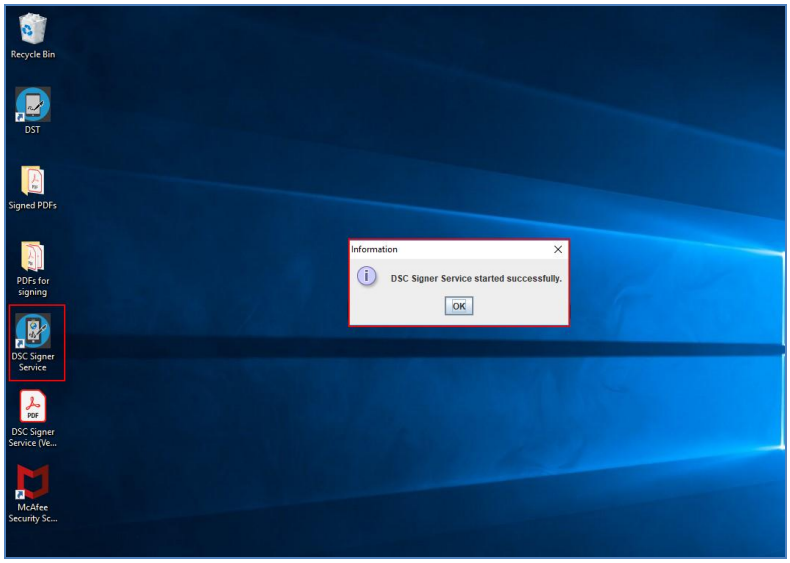


Fig.A.2.1

For MAC

Restart the **DSC Signer Service** by clicking desktop icon **"DSC_Signer_Service"**.

For Ubuntu

Restart the **DSC Signer Service** by clicking desktop icon **"DSC_Signer_Service"**.

Note:

1. While using DSC application in MAC OS and Ubuntu OS, if a dongle is plugged-out, then, occasionally user has to manually restart the DSC signer service.

Problem 2

Service is not running even after starting manually.

Solution

Check availability of ports for HTTP and HTTPs

http port: 55100

https port: 55101

Commands to check for availability of both ports (For example, we are using port 55101 in each screenshot; user can choose any other port to test) are mentioned below:

For Windows

Use cmd/powerShell to run following commands in windows.

Command: netstat –ano | find "port" (**Fig.A.2.2**).

Screen-shot

Fig.A.2.2

For Ubuntu

For Ubuntu use Terminal.

Command: netstat -tunlp | grep port (**Fig.A.2.3**).

Screen-shot

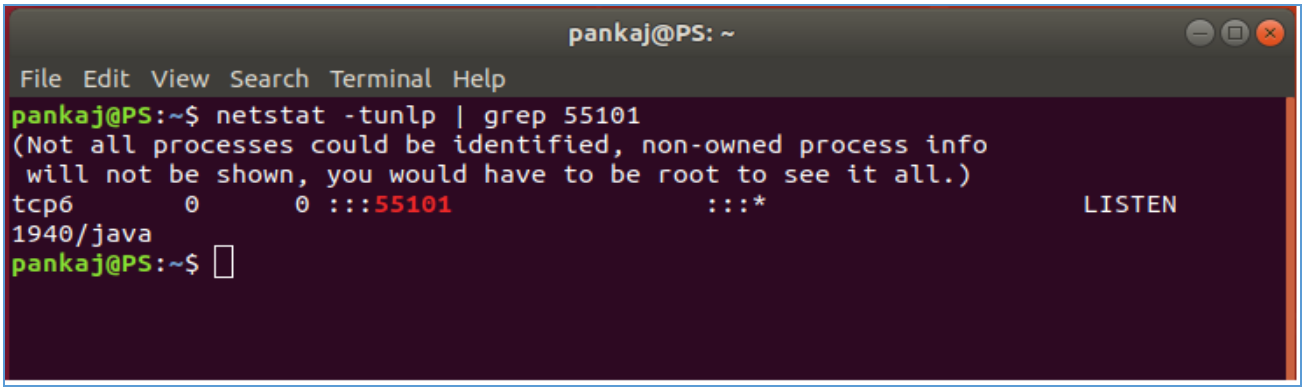


Fig.A.2.3

For MAC

For MAC use Terminal.

Command: netstat –vanptcp | grep port **(Fig.A.2.4).**

Screen-shot

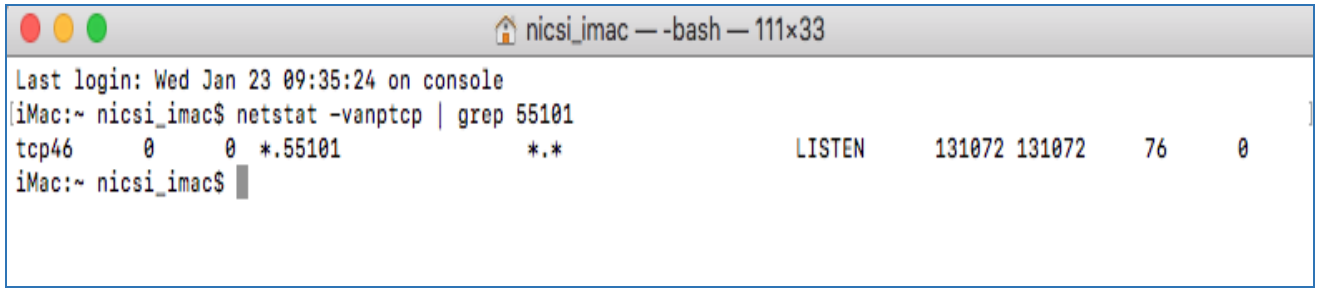


Fig.A.2.4

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

Problem 3

If both the ports or any one of the ports are in use with some other services

Solution

Kill the service running at specified port.
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.2.5**).

Screen-shot

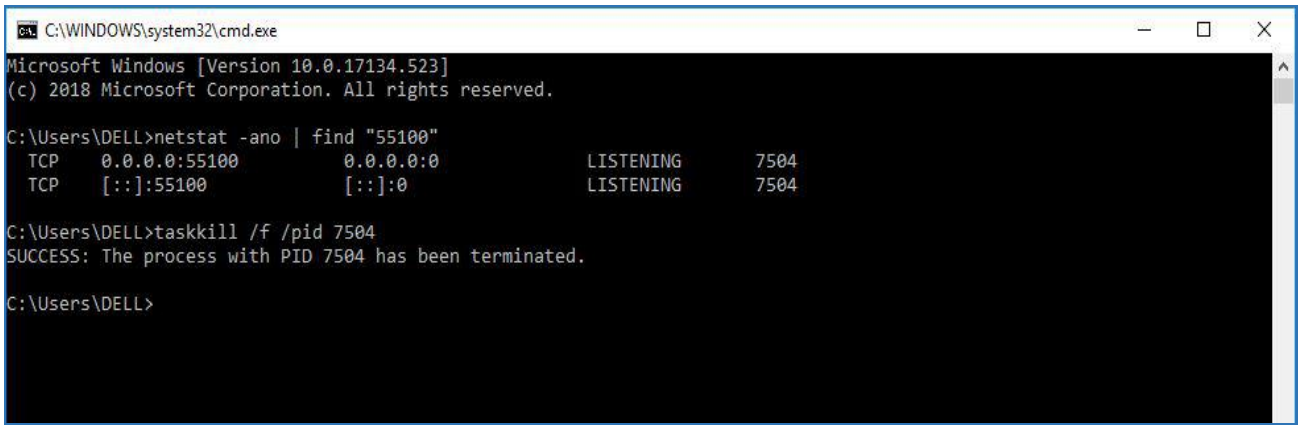


Fig.A.2.5

For Ubuntu

For Ubuntu use Terminal.
Command: Sudo kill -9 [PID] (**Fig.A.2.6**).

Screen-shot

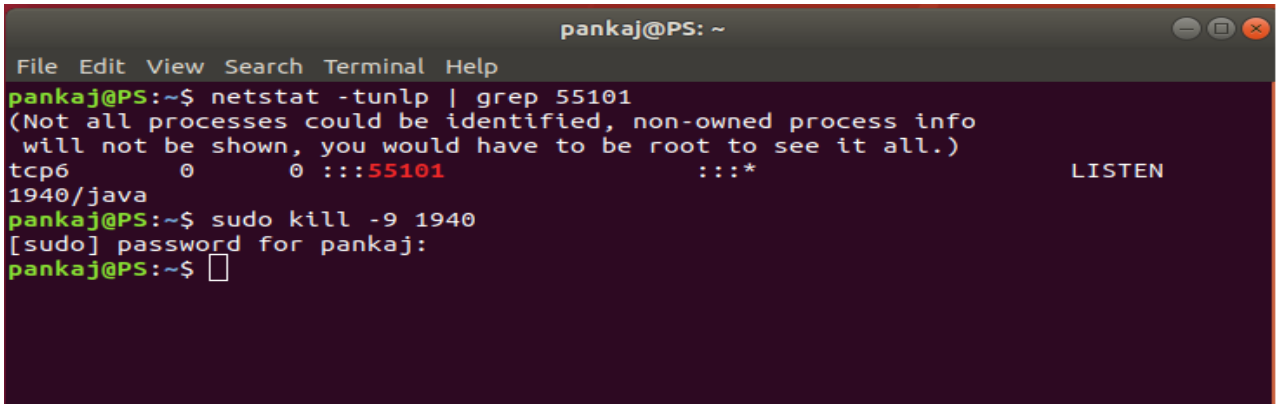


Fig.A.2.6

For Mac

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

Screen-shot

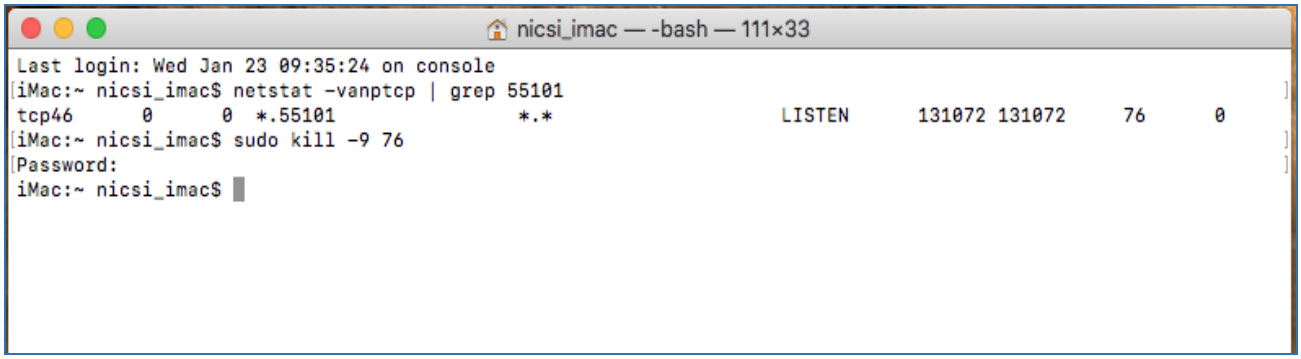


Fig.A.2.7

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

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**:

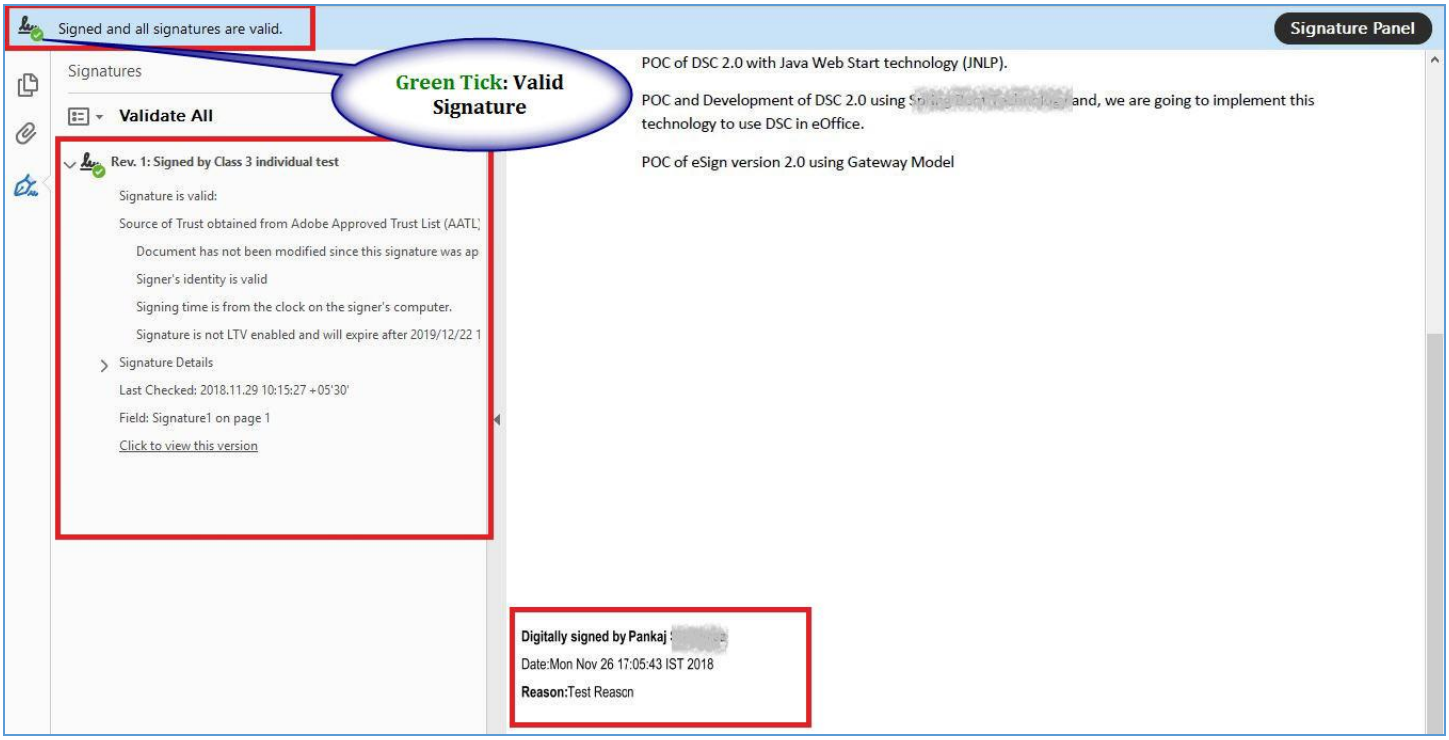


Fig.A.3.4: Valid Signature

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:**

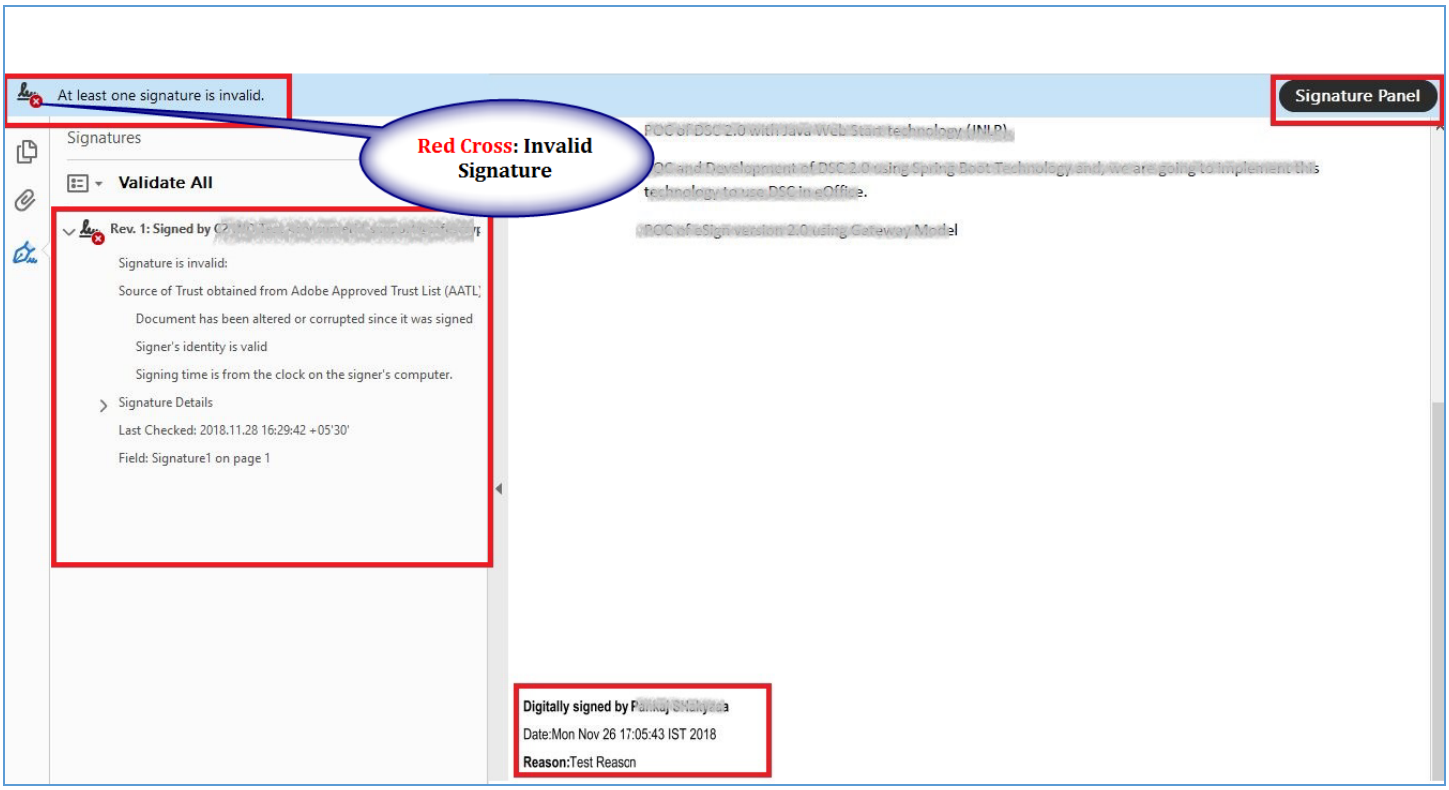


Fig.A.3.5: Invalid Signature

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:**

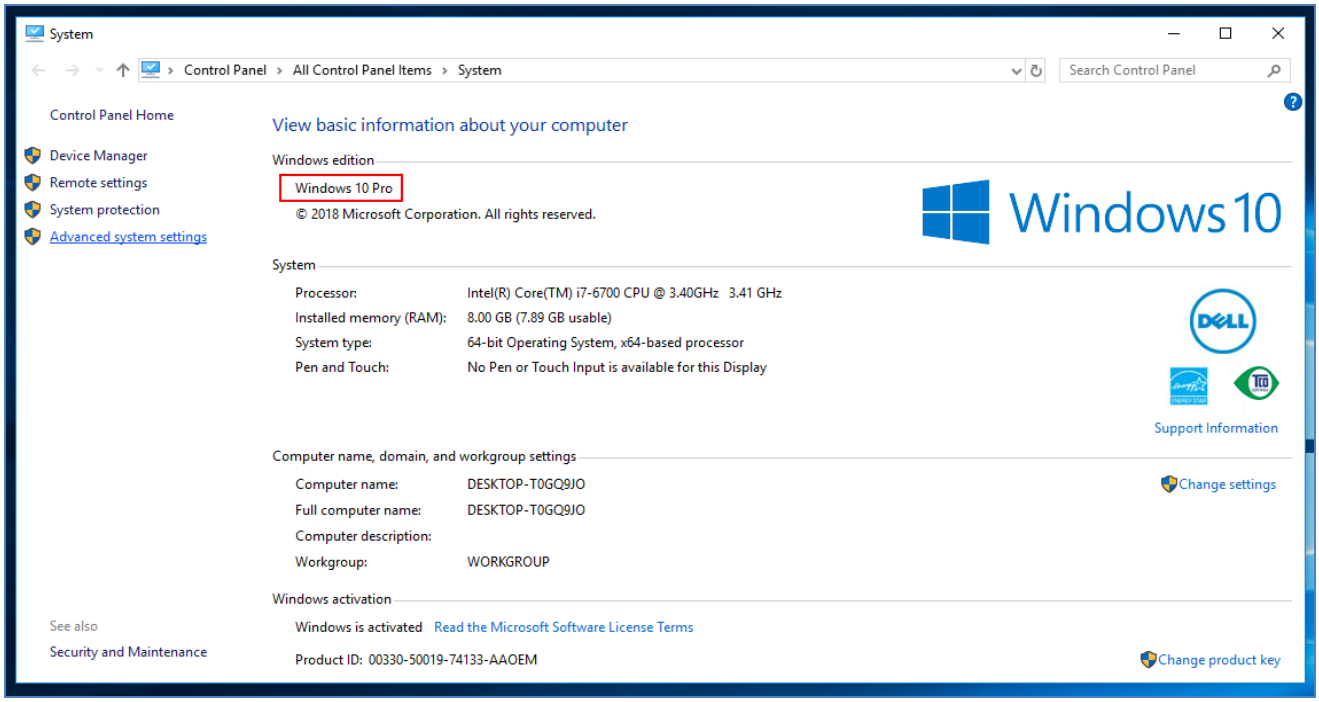


Fig.A.4.1

Check availability of Java Version in windows:

- Click **Start** button and go to **Control Panel**.
- Click **Java** link as shown in **Fig.A.4.2:**

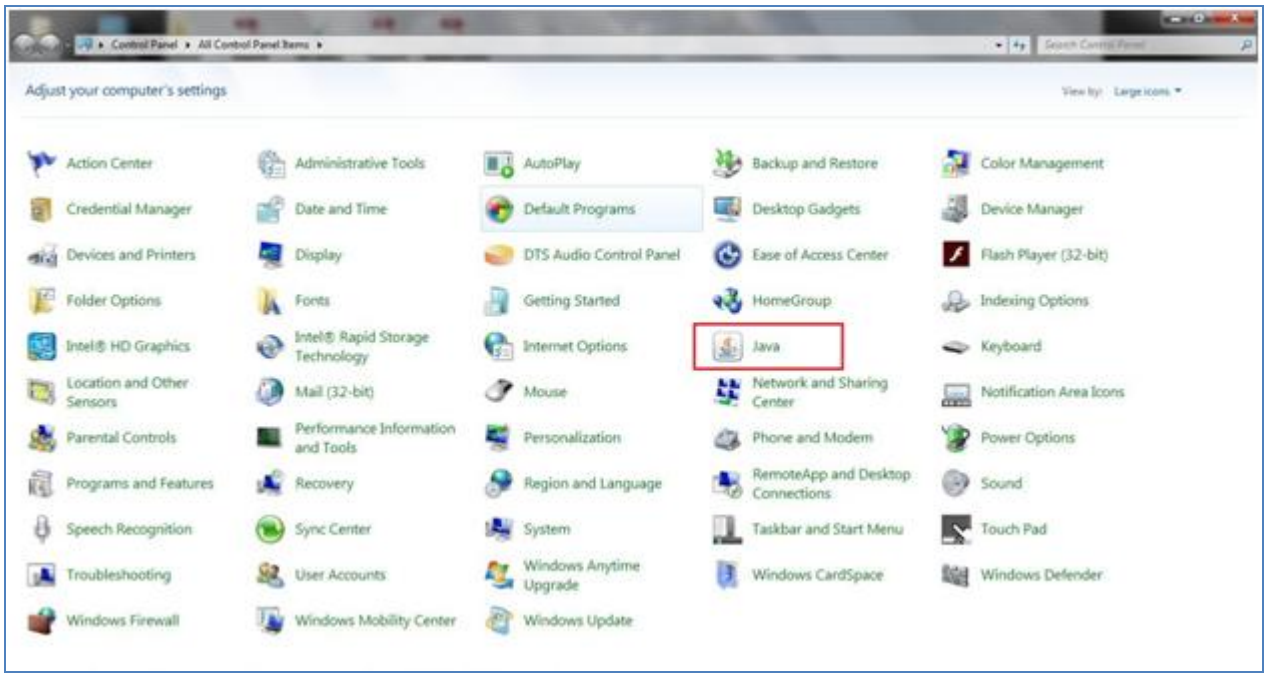
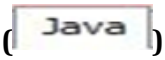


Fig.A.4.2

- A screen appears is shown in **Fig.A.4.3**, select **Java (** 

) tab and then click **View** (

) button.

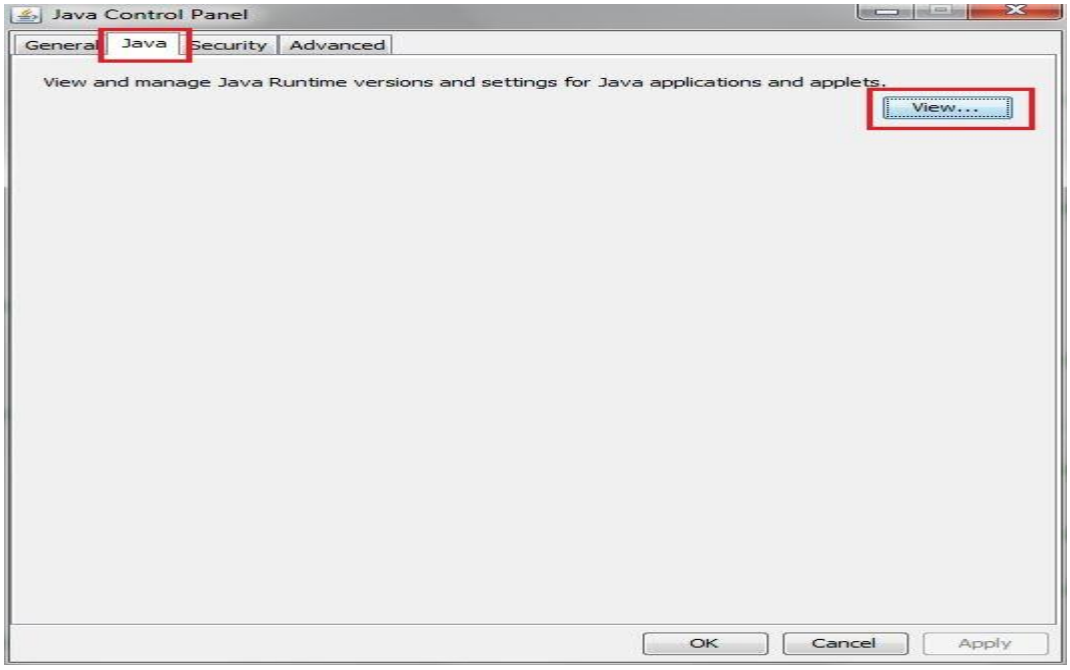


Fig.A.4.3

- The version of Java will appear under **User** Tab as shown in **Fig.A.4.4**.

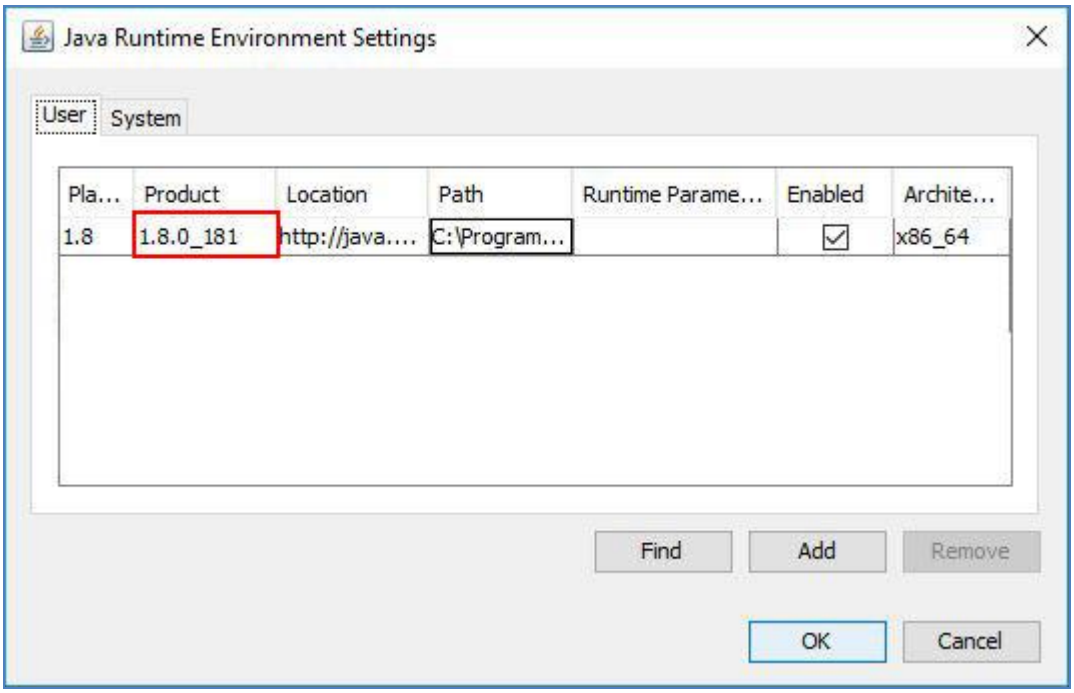

Java Runtime Environment Settings
User
System
Pla...
Product
Location
Path
Runtime Parame...
Enabled
Archite...
1.8
1.8.0_181
http://java....
C:\Program...
x86_64
Find
Add
Remove
OK
Cancel

Fig.A.4.4

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).

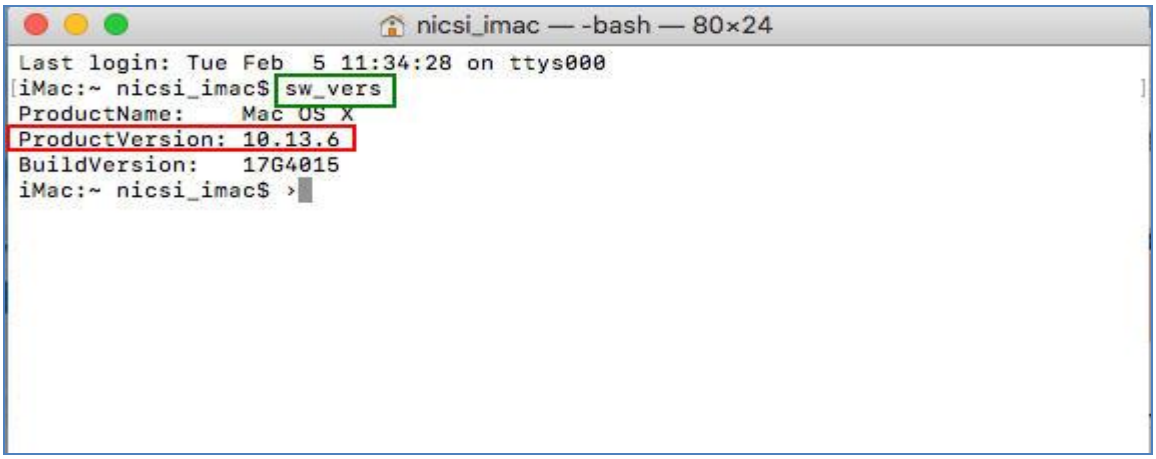


Fig.A.4.5

Check availability of Java Version in MAC OS:

- Open the **Terminal**
- Type the command **"java -version",** press enter.
- If java is not installed in system, then the output will be **"Command java -version not found**".
- If java is installed then the java version will be displayed as shown in **Fig.A.4.6**:

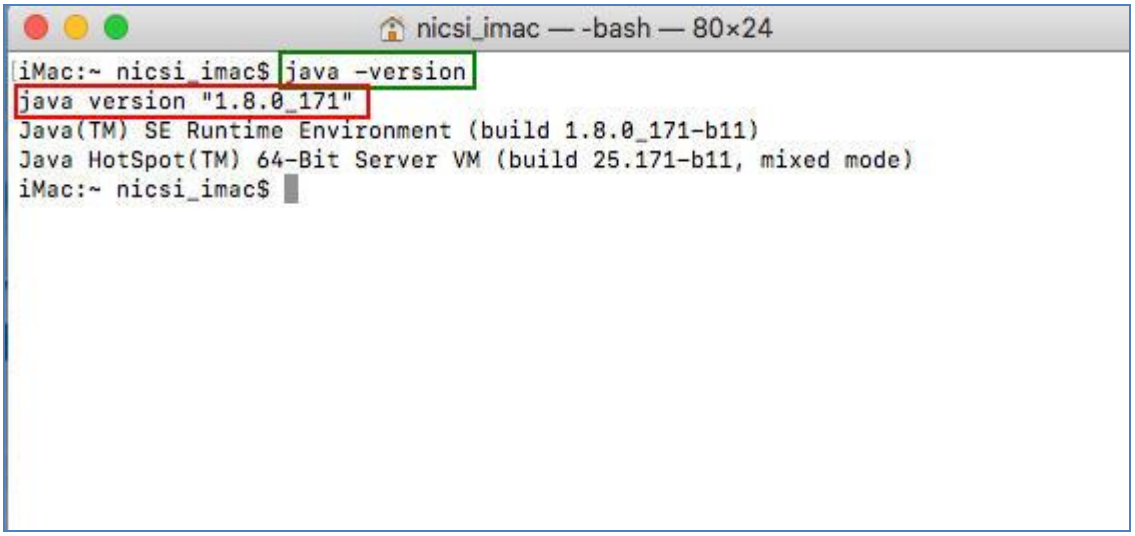


Fig.A.4.6

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).

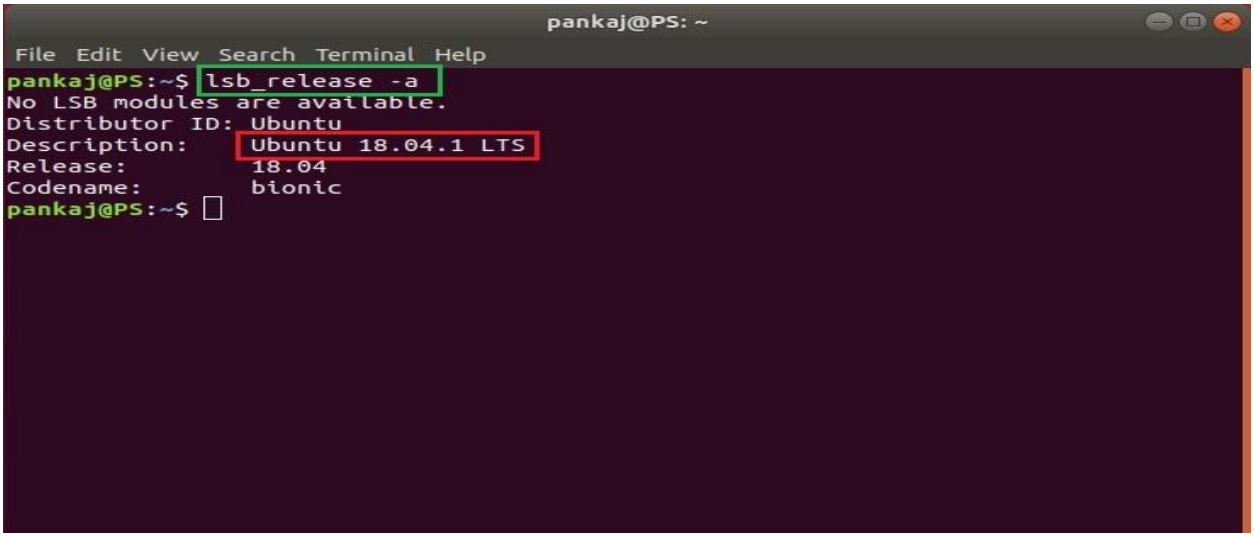


Fig.A.4.7

Check availability of Java Version in Ubuntu OS:

- Open the **Terminal**
- Type the command **"java -version",** press enter.
- If java is not installed in system, then the output will be **"Command java -version not found**"**.**,
- If java is installed then the java version will be displayed as shown in **Fig.A.4.8:**

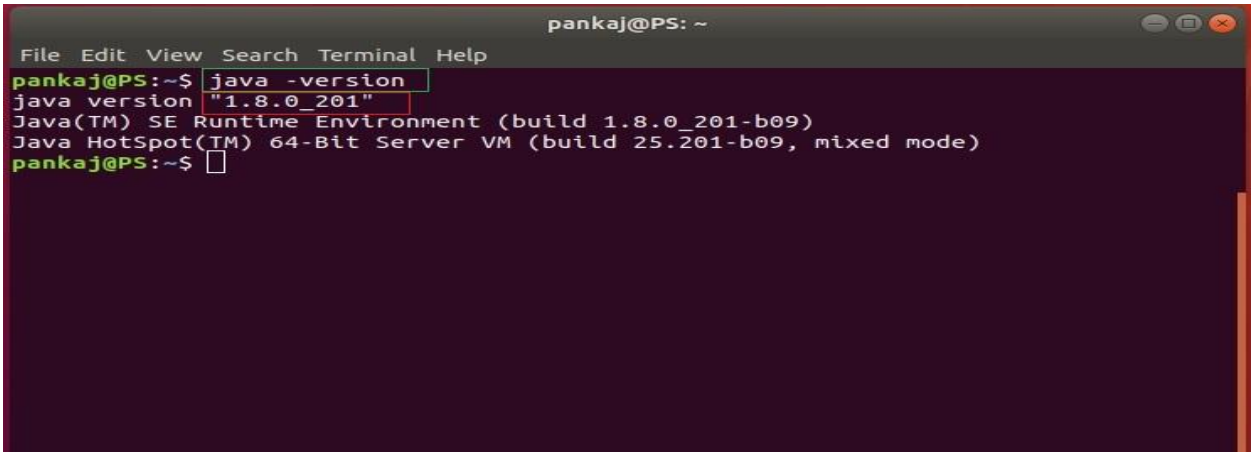


Fig.A.4.8

Annexure V

Re-register DSC certificate in eFile:

For re-registration of DSC certificate in eFile, perform the below mentioned steps:

- Login to the eFile application, the **eFile application** screen appears, as shown in **Fig.A.5.1.**
- Click **Re-register** (Re-register) link as shown in **Fig.A.5.1**:

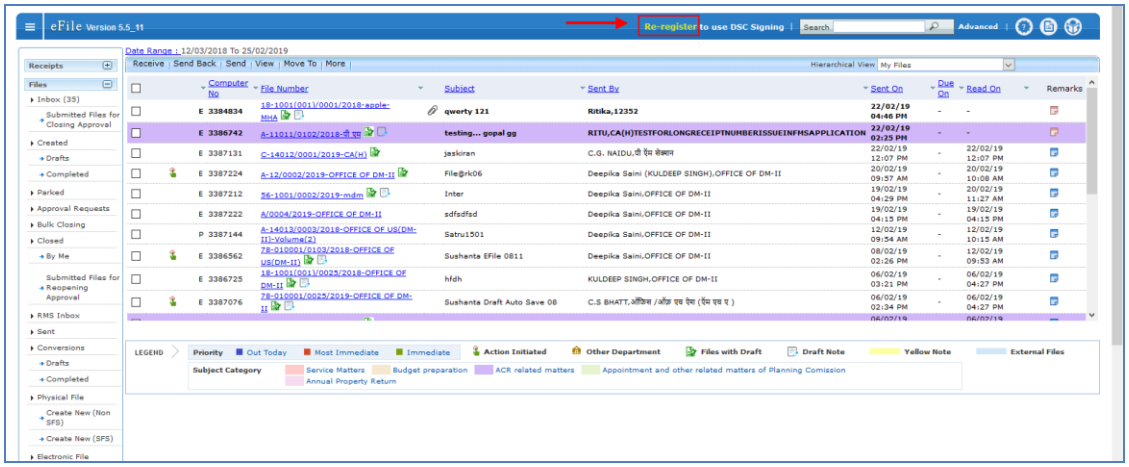


Fig.A.5.1

- The **Certificate Information** screen appears, click **Register DSC** (Register DSC) link, as shown in **Fig.A.5.2**:

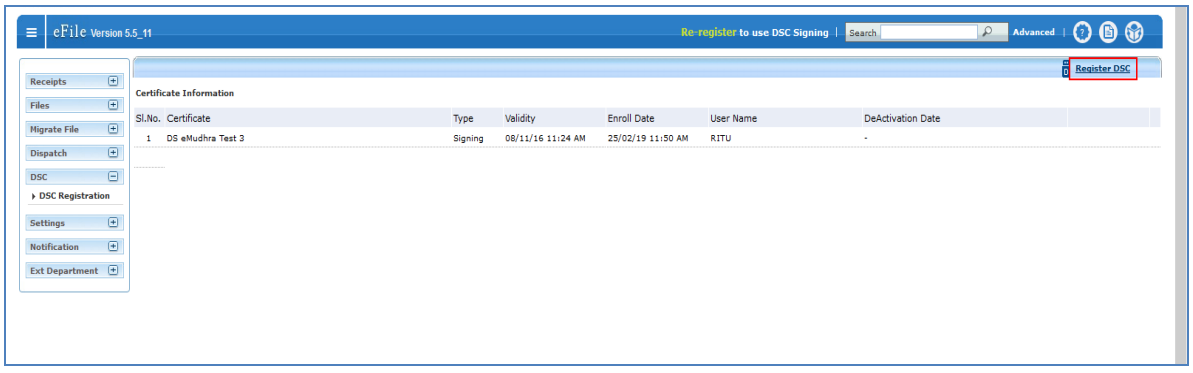


Fig.A.5.2

- The **DSC Registration** screen appears, click **Register** (Register) button, as shown in **Fig.A.5.3:**

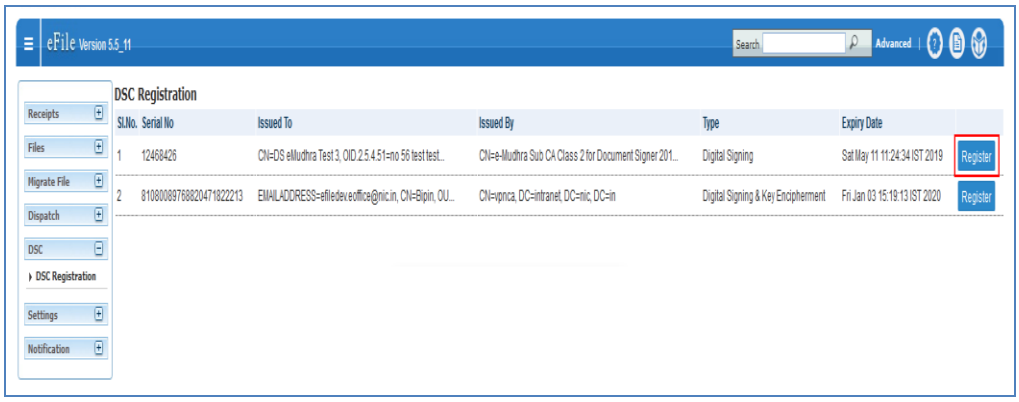


Fig.A.5.3

- The **Verify User PIN** pop-up appears, enter the User PIN and click **Login** (Login) button, as shown in **Fig.A.5.4**:

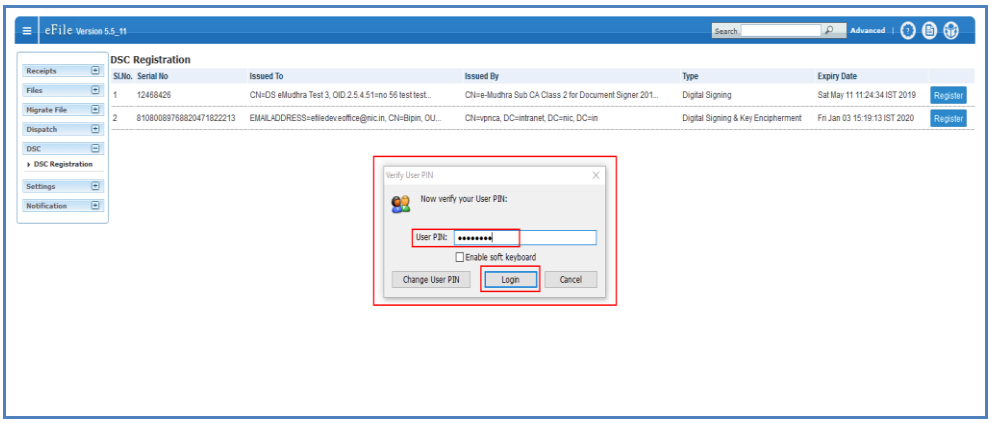


Fig.A.5.4

- The **Alert** box appears, displaying message **"DSC Registered successfully",** click **OK** (OK) button as shown in **Fig.A.5.5**:

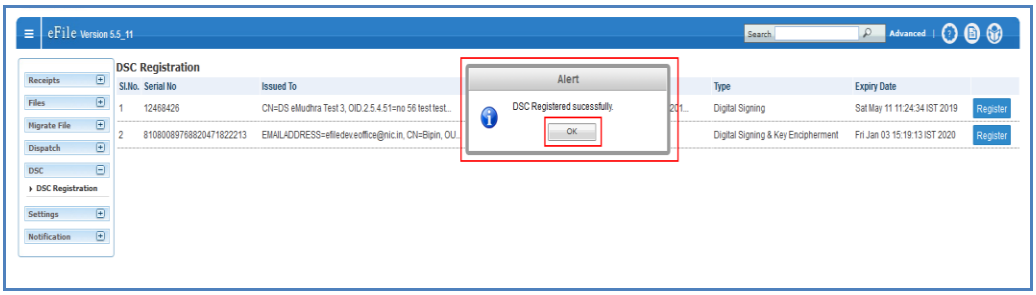


Fig.A.6.5

Created By:

Rohit Kumar Singh
Pankaj Shakya
Heena Kaushar
Rimandeep Kaur

Reviewed By:

Navdeep Singh Nagi

Approved By:

Navneet Kaur

eOffice Project Divison

National Informatics Centre

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