## Amendment History

<table>
<thead>
<tr>
<th>Date</th>
<th>Document Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 June 2018</td>
<td>2.0</td>
<td>User Guidelines</td>
<td>eOffice Project Division</td>
</tr>
<tr>
<td>03 October 2018</td>
<td>3.0</td>
<td>User Guidelines</td>
<td>eOffice Project Division</td>
</tr>
<tr>
<td>29 November 2018</td>
<td>3.5</td>
<td>User Guidelines</td>
<td>eOffice Project Division</td>
</tr>
<tr>
<td>05 March 2019</td>
<td>4.1</td>
<td>User Guidelines</td>
<td>eOffice Project Division</td>
</tr>
<tr>
<td>26 February 2020</td>
<td>4.1.01 (change in installation steps for windows)</td>
<td>User Guidelines</td>
<td>eOffice Project Division</td>
</tr>
</tbody>
</table>
Table of Contents

Abbreviations .............................................................................................................................................. 5
Introduction .................................................................................................................................................. 6
Section 1: DSC Signer Service .................................................................................................................... 7
Client’s Machine Requirements: ................................................................................................................ 8
Minimum client’s machine Requirements ................................................................................................ 8
Section 2: Windows OS .................................................................................................................................. 9
Identifying Your System ............................................................................................................................. 9
Pre-requisites for DSC Signer Service Installer for Windows..................................................................... 10
Installation Guidelines for Windows OS .................................................................................................. 11
  For Bulk User: .................................................................................................................................. 11
  For Single User: ................................................................................................................................. 11
Section 3: MAC ........................................................................................................................................... 17
Pre-requisites for DSC Signer Service Installer ...................................................................................... 17
Installation Guidelines for MAC OS .................................................................................................... 18
Section 4: Ubuntu ....................................................................................................................................... 20
Pre-requisites for DSC Signer Service Installer for Ubuntu OS .............................................................. 20
Installation Guidelines for Ubuntu OS ................................................................................................ 21
Section 5: Checking the Service Status .................................................................................................. 23
For Windows/MAC/ Ubuntu .................................................................................................................... 23
Annexure I ................................................................................................................................................ 26
  Add/Import SSL Certificate to the Browsers .......................................................................................... 26
  For Mozilla Firefox ............................................................................................................................. 26
  For Chrome........................................................................................................................................ 29
  For Internet Explorer .......................................................................................................................... 31
Annexure –II .............................................................................................................................................. 36
  Troubleshooting (For DSC Signer Service)........................................................................................ 36
Annexure III .............................................................................................................................................. 41
  Signature Validity Checkmark Visibility ............................................................................................... 41
  The visual representation of signature verification.......................................................................... 41
  Display of Valid Signature in previous version of Digital Signature ............................................. 41
  Display of Valid Signature in Current Version of Digital Signature ............................................. 42
How to verify signature in current scenario ..........................................................................................43

Annexure IV ..........................................................................................................................................45
DSC Pin Management in prevalent dongles today ..................................................................................45
ProxKey Token-session Management ..................................................................................................45
ePass Token Session Management ......................................................................................................46
Session Time limit setting (For ePass Token) .........................................................................................47
Aladin Token-Session Management ......................................................................................................48

Annexure V .............................................................................................................................................50
Identifying Your System .........................................................................................................................50
Windows OS ...........................................................................................................................................50
Check Windows version: .........................................................................................................................50
Check availability of Java Version in windows: .........................................................................................50
MAC OS ..................................................................................................................................................53
Checking MAC version: ..........................................................................................................................53
Check availability of Java Version in MAC OS: .......................................................................................53
Ubuntu OS ..............................................................................................................................................54
Checking Ubuntu version: .......................................................................................................................54
Check availability of Java Version in Ubuntu OS: ......................................................................................54

Annexure VI .............................................................................................................................................55
Re-register DSC certificate in eFile: .........................................................................................................55
# Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSC</td>
<td>Digital Signature Certificate</td>
</tr>
<tr>
<td>NPAPI</td>
<td>Netscape Plug-in Application Programming Interface</td>
</tr>
<tr>
<td>NICNET</td>
<td>National Informatics Center Network</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>LTV</td>
<td>Long Term Validation</td>
</tr>
</tbody>
</table>
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:
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:

<table>
<thead>
<tr>
<th>Minimum client’s machine Requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows OS</td>
<td>Windows 7 &amp; above.</td>
</tr>
<tr>
<td>MAC OS</td>
<td>MAC 10.7 &amp; above.</td>
</tr>
<tr>
<td>Ubuntu OS</td>
<td>Ubuntu 18 &amp; above.</td>
</tr>
<tr>
<td>JRE</td>
<td>Version 1.8 or above appropriate as per OS</td>
</tr>
</tbody>
</table>

**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](image)

Note:
1. In case .bat file does not run, refer to Annexure V 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).

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Version 1.8 or above appropriate as per OS.</td>
<td>To be Downloaded by Individual User at client machine. (Refer website <a href="https://www.java.com/en/">https://www.java.com/en/</a> for JRE installation).&lt;br&gt;&lt;br&gt;Note:&lt;br&gt;1. User(s) with 32-bit windows OS needs to install 32-bit JRE.&lt;br&gt;2. User(s) with 64-bit windows OS needs to install 64-bit JRE.</td>
</tr>
<tr>
<td>2.</td>
<td>Add/ Import SSL certificates to the browsers.</td>
<td>To Add/ Import SSL certificates to the browsers (Refer Annexure I for steps).</td>
</tr>
<tr>
<td>3.</td>
<td>Re-register DSC certificate.</td>
<td>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 VI for steps).</td>
</tr>
<tr>
<td>4.</td>
<td>Internet connectivity is required to check for certificate revocation status.</td>
<td>Check the Internet connectivity at every client machine.</td>
</tr>
</tbody>
</table>

### Note for System Administrator

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>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.</td>
<td>CRL should be downloaded manually by the System Administrator.</td>
</tr>
</tbody>
</table>
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](image)

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

![Fig.2.3](image)

- 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:
• 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**.
Note:

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

A confirmation window will appear, click on **Uninstall** button to start the uninstallation as shown in **Fig.2.8**:
• Ready to Install window appears asking for SSL certificate, click the **Yes** radio button and then click **Install** button as shown in **Fig.2.9:**

![Fig.2.9](image)

**Note:** single certificates are mandatory for signing 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](image)
• 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](image)

**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:
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**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Version 1.8 or above appropriate as per OS</td>
<td>In case of MAC only installer needs to be downloaded.</td>
</tr>
<tr>
<td>2.</td>
<td>Add/ Import SSL certificates to the browsers.</td>
<td>To Add/ Import SSL certificates to the browsers (Refer Annexure I for steps).</td>
</tr>
<tr>
<td>3.</td>
<td>Re-register DSC certificate.</td>
<td>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).</td>
</tr>
<tr>
<td>4.</td>
<td>Internet connectivity is required to check for certificate revocation status.</td>
<td>Check the Internet connectivity at every client machine.</td>
</tr>
</tbody>
</table>

**Note for System Administrator**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>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.</td>
<td>CRL should be downloaded manually by the System Administrator.</td>
</tr>
</tbody>
</table>
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](image)

- 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**:
Note:

1. While using DSC application if a dongle is plugged-out, then, occasionally user has to manually restart the DSC signer service. For restarting 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 V 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

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Version 1.8 or above appropriate as per OS</td>
<td>In case of Ubuntu only installer needs to be downloaded.</td>
</tr>
<tr>
<td>2.</td>
<td>Add/ Import SSL certificates to the browsers.</td>
<td>To Add/ Import SSL certificates to the browsers (Refer Annexure I for steps).</td>
</tr>
<tr>
<td>3.</td>
<td>Re-register DSC certificate.</td>
<td>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 VI for steps).</td>
</tr>
<tr>
<td>4.</td>
<td>Internet connectivity is required to check for certificate revocation status.</td>
<td>Check the Internet connectivity at every client machine.</td>
</tr>
</tbody>
</table>

Note for System Administrator

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>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.</td>
<td>CRL should be downloaded manually by the System Administrator.</td>
</tr>
</tbody>
</table>
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](image_url)

- 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**:
• 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 restarting 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 V 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 & 55101 ports.

  - **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** button or **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**:
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:

  ![Fig.A.1](https://example.com/figA1.png)

  **Fig.A.1**

- Then, the browser will notify the user to add the exception into the list (Fig.A.1).

- Click Advanced button to add an exception (Fig.A.1).
A message box appears, click **Add Exception** button as shown in Fig.A.1.2:

![Your connection is not secure](image)

**Fig.A.1.2**

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

![Add Security Exception](image)

**Fig.A.1.3**

The browser will confirm and displays the message “**Success**” as shown in 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](https://127.0.0.1:55101/check/isLive) as shown in Fig.A.1.5:

![Fig.A.1.5](image)

- 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)** button as shown in Fig.A.1.6:

![Fig.A.1.6](image)
• The browser will confirm and displays the message “Success” as shown in Fig.A.1.7:

![Fig.A.1.7](image)

• 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](image)
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 appear, as shown in Fig.A.1.9

![Fig.A.1.9](image)

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

![Internet Options window](image1)

**Fig.A.1.11**

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

![Internet Options window](image2)

**Fig.A.1.12**

- The Certificate Import Wizard window appears and click **Next** button, as shown in **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:
• Click Finish button to close the process as shown in Fig.A.1.16:
Security warning window appears, click Yes button, as shown in Fig.A.1.17:

- The message box prompt “The import was successful”, click Ok button as shown in 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

![Screen-shot Fig.A.2.1](image)

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](image)

For Ubuntu
For Ubuntu use Terminal.
  **Command**: netstat -tunlp | grep port *(Fig.A.2.3)*.

Screen-shot

![Fig.A.2.3](image)
For MAC
For MAC use Terminal.
**Command:** `netstat -vnptcp | grep port` (Fig.A.2.4).

**Screen-shot**

![Image of terminal output](image)

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](image1.png)

For Ubuntu
For Ubuntu use Terminal.

Command: Sudo kill -9 [PID]  (Fig.A.2.6).

Screen-shot

![Fig.A.2.6](image2.png)
For Mac
For MAC use Terminal.
**Command:** `sudo kill -9 [PID]` *(Fig.A.2.7)*.

**Screen-shot**

![Screen-shot](image)

**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:

Digitally signed by ABC
Date: Mon Nov 26 17:05:43 IST 2018
Reason: Test Reason

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:

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

DSC Pin Management in prevalent dongles today

User PIN is the password which the digital signature (DSC application) subscriber uses while doing a digital signature using token. User PIN is important to be kept confidential and should not be disclosed to anyone. For signing a document digitally, user needs to enter the DSC PIN every time. Also, in the case of the multiple files, user has to enter a PIN for each file. To avoid the situation of entering the pin multiple time DSC token driver has a feature to store the User PIN for that particular session, resulting user will enter the PIN once for signing the first file and after that, it will not ask for the PIN.

Storing and caching of PIN completely depends on the dongle used by the user.

Follow the below instruction to maintain the Pin session:

![DISCLAIMER]

Steps for few known dongles are given below; same steps will be followed in case of other dongle(s).

ProxKey Token-session Management

Steps to maintain the Pin session for ProxKey Token:

1. Open token driver of Proxkey.
2. Select Options from left panel as shown in Fig.A.4.1.

![Fig.A.4.1]
3. Select the checkbox corresponding to **Cache User Pin** and click **Apply** button as shown in **Fig.A.4.2**:

![Image of Fig.A.4.2](image)

**Fig.A.4.2**

**ePass Token Session Management**

Steps to maintain the Pin session for ePass Token:

1. Open **ePass** token driver.

2. Select **Setting** from the options available at right side panel as shown in **Fig.A.4.3**:

![Image of Fig.A.4.3](image)

**Fig.A.4.3**
3. Select the checkbox corresponding to **Single Sign on** and click **Ok** button as shown in **Fig.A.4.4**:

![Fig.A.4.4](image)

**Session Time limit setting (For ePass Token)**

User can also set time out session of DSC PIN for signing multiple files.

Steps to set the DSC PIN session time out are as follows:

1. Open **epass** token driver.

2. Click **Change User Pin** option as shown in **Fig.A.4.5**

![Fig.A.4.5](image)
3. Enter **DSC PIN, Timeout** time and click **Ok** button, as shown in **Fig.A.4.6**

![Fig.A.4.6](image1)

**Note:**
It is not mandatory to change the DSC PIN, existing DSC PIN can also be provided in **Old Pin** and **New PIN** column.

**Aladin Token-Session Management**

Steps to maintain the Pin session for Aladin Token:

1. Open **Aladin** Token Driver.
2. Click **Advanced View** icon as shown in **Fig.A.4.7**

![Fig.A.4.7](image2)
3. Click eToken PKI client Settings and then click Advanced ( ) tab as shown in Fig.A.4.8.

![Fig.A.4.8](image)

4. Select the checkbox corresponding to Enable Single Sign-On Mode and click Save ( ) button as shown in Fig.A.4.9:

![Fig.A.4.9](image)
Annexure V

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:

![Windows 10 screenshot](image)

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.
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](image)

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](image)
**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 get displayed (marked in red color box).

![Fig.A.4.7](image)

**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](image)
Annexure VI

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](image1)

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

![Fig.A.5.2](image2)
- The DSC Registration screen appears, click Register button, as shown in Fig.A.5.3:

![Fig.A.5.3](image)

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

![Fig.A.5.4](image)

- The Alert box appears, displaying message “DSC Registered successfully”, click OK button as shown in Fig.A.5.5:

![Fig.A.5.5](image)