## 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 Oct 2018</td>
<td>3.0</td>
<td>User Guidelines</td>
<td>eOffice Project Division</td>
</tr>
<tr>
<td>29 Nov 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>
</tbody>
</table>
Table of Contents

Abbreviations .............................................................................................................................. 5
Introduction .................................................................................................................................. 6
Section 1: DSC Signer Service ..................................................................................................... 7
  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
Section 3: MAC ............................................................................................................................. 15
  Pre-requisites for DSC Signer Service Installer ............................................................................. 15
  Installation Guidelines for MAC OS ............................................................................................... 16
Section 4: Ubuntu .......................................................................................................................... 18
  Pre-requisites for DSC Signer Service Installer for Ubuntu OS ....................................................... 18
  Installation Guidelines for Ubuntu OS ............................................................................................ 19
Section 5: Checking the Service Status .......................................................................................... 21
  For Windows/MAC/ Ubuntu ........................................................................................................... 21
Annexure I ..................................................................................................................................... 23
  Add/Import SSL Certificate to the Browsers ................................................................................... 23
    For Mozilla Firefox ....................................................................................................................... 23
    For Chrome ................................................................................................................................. 26
    For Internet Explorer ................................................................................................................... 28
Annexure –II .................................................................................................................................... 33
  Troubleshooting (For DSC Signer Service) .................................................................................... 33
Annexure III .................................................................................................................................... 38
  Signature Validity Checkmark Visibility .......................................................................................... 38
    The visual representation of signature verification ....................................................................... 38
    Display of Valid Signature in previous version of Digital Signature ............................................. 38
    Display of Valid Signature in Current Version of Digital Signature .............................................. 39
    How to verify signature in current scenario .................................................................................. 40
Annexure IV ..................................................................................................................................... 42
  DSC Pin Management in prevalent dongles today ........................................................................... 42
ProxKey Token Session Management .......................................................... 42
ePass Token Session Management ............................................................ 43
Session Time limit setting (For ePass Token) ............................................ 44
Aladin Token Session Management ............................................................ 45

Annexure V ................................................................................................. 47

Identifying your System ........................................................................... 47
Windows OS ............................................................................................... 47
Check Windows version: ........................................................................ 47
Check availability of Java Version in windows: ...................................... 47
MAC OS ..................................................................................................... 50
Checking MAC version: .......................................................................... 50
Check availability of Java Version in MAC OS: ...................................... 50
Ubuntu OS ................................................................................................ 51
Checking Ubuntu version: ...................................................................... 51
Check availability of Java Version in Ubuntu OS: .................................. 51

Annexure VI ............................................................................................... 52
Re-register DSC certificate in eFile: ......................................................... 52

Annexure VII ............................................................................................. 55
DSC – Error Codes ................................................................................... 55
**Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</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 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. A new signer has been developed and released that would work with latest browsers and does not require applet to run. 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.
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 & Fig.1.2:
The DSC Signer Service is available for following OS client’s machine:

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

Availability of ports 55100 and 55101

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](#))
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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. User(s) with 32-bit windows OS needs to install 32-bit JRE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. User(s) 64-bit windows OS installs, 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

- Locate the DSC_Signer_Service.exe file from downloaded bundle.
- Double click required exe file to start the installation as shown in Fig.2.2:

![Fig.2.2](image)

- For a custom installation, click Browse button, select the directory as shown in Fig.2.3 and click Next button.

OR

- For default installation, click Next button, as shown in Fig.2.3:

![Fig.2.3](image)
• **DSC Signer Service: License Agreement** window appears, read the agreement and click **I Agree** button as shown in Fig.2.4:

![Fig.2.4](image)

• The process may take some time for the complete installation as shown in Fig.2.5:

![Fig.2.5](image)
• Click Close button (Fig.2.6), the DSC Signer Service is successfully installed.

Fig.2.6

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

**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 “**DSC Signer Service started successfully**”, as shown in Fig.2.7:

Fig.2.7
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** ( ), as shown in Fig.2.8:

![DSC Signer Service](image)

Fig.2.8

- 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. To import the SSL certificates refer **Annexure I** (Add/ Import SSL certificates to the Browser).
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>Following four activities to be completed by User(s).</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>S. No.</strong></td>
<td><strong>Activities</strong></td>
</tr>
<tr>
<td>1.</td>
<td>Version 1.8 or above appropriate as per OS</td>
</tr>
<tr>
<td>2.</td>
<td>Add/ Import SSL certificates to the browsers.</td>
</tr>
<tr>
<td>3.</td>
<td>Re-register DSC certificate.</td>
</tr>
<tr>
<td>4.</td>
<td>Internet connectivity is required to check for certificate revocation status.</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**:

```
ProductName: Mac OS X
ProductVersion: 10.13.6
BuildVersion: 1704015

Checking Service on Port 55100 & 55101 is Running or not....
Ports are already in use

Checking DSC Signer Service is running on 55100/55101 port...
Other Service is Running on 55100 Port. !!!!!

Stopping other service on 55100 Port. Do you want to proceed ?
Enter Your Choice : [Y/N]
```

**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**:
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 \(\Rightarrow\) 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>Following four activities to be completed by User(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. No.</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>4.</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]

- 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.
- Service will automatically start after 5 seconds in case no action is taken while the service is not running.
- 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 (Check for HTTP Port) button or Check for HTTPS Port (Check for HTTPS Port) button as shown in Fig.5.1:

![Fig.5.1](image)

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](https://127.0.0.1:portNumber/check/isLive)
   For Ex. [https://127.0.0.1:55101/check/isLive](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

DSC Signer Service runs as https which is 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](image)

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

- Click **Advance** 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:
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:

![Fig.A.1](image1)

- 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](image2)
• The browser will confirm and displays the message “Success” as shown in Fig.A.1.7:

![Image of a browser displaying success message]

**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**:

![Image of the flags screen with Enabled selected]

**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](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, 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:

![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:

![Fig.A.1.12]
The Certificate Import Wizard window appears and click **Next** button, as shown in **Fig.A.1.13**:

![Fig.A.1.13](image1)

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](image2)
Click Finish (Finish) button to close the process as shown in Fig.A.1.16:
Security warning window appears, click Yes (Yes) button, as shown in Fig.A.1.17:

![Fig.A.1.17](image1)

The message box prompt “The import was successful”, click Ok (Ok) button as shown in Fig.A.1.18:

![Fig.A.1.18](image2)
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”.

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 -vanptcp | grep port *(Fig.A.2.4).*

**Screen-shot**

![Screen-shot](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**

![Screen-shot](image1)

Fig.A.2.5

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

**Screen-shot**

![Screen-shot](image2)

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

Screen-shot

![Screen-shot](image_url)

Fig.A.2.7
After killing the service, manually start the service. If still it does not start, contact the administrator.

Note:
1) If user is facing some unidentified issue in that case, kindly provide DSC Signer Service logs from user machine.
   (Refer Annexure VII to get logs.)
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](image1)

![Fig.A.3.2: Invalid Signature](image2)
**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:

![Signature Details](image)

**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:

![Green Tick: Valid Signature](image)

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

![Fig.A.4.2](image)

**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:**

![Fig.A.4.3](image)
3. Select the checkbox corresponding to **Single Sign on** and click **Ok** button as shown in **Fig.A.4.4**:

![Fig.A.4.4](image1)

**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](image2)
3. Enter **DSC PIN, Timeout** time and click **Ok** button, as shown in Fig.A.4.6

![Fig.A.4.6](image)

**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](image)
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.5.1:

![Fig.A.5.1](image)

Check availability of Java Version in windows:
- Click Start button and go to Control Panel.
- Click Java link as shown in Fig.A.5.2:
- A screen appears as shown in Fig.A.5.3, select Java tab and then click View button.

- The version of Java will appear under User Tab as shown in Fig.A.5.4.
Fig.A.5.4
MAC OS

Checking MAC version:
- Open the Terminal.
- Type the command “sw_vers”, and press enter (Fig.A.5.5), and the version of MAC will gets displayed (marked in red color box).

![Fig.A.5.5]

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.5.6:

![Fig.A.5.6]
Ubuntu OS

Checking Ubuntu version:

- Open the Terminal.
- Type the command “lsb_release -a”, press enter (Fig.A.5.7), and the version of Ubuntu will gets displayed (marked in red color box).

![Fig.A.5.7]

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.5.8:

![Fig.A.5.8]
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.6.1.
- Click Re-register (Re-register) link as shown in Fig.A.6.1:

![Fig.A.6.1](image1)

- The Certificate Information screen appears, click Register DSC (Register DSC) link, as shown in Fig.A.6.2:

![Fig.A.6.2](image2)
The **DSC Registration** screen appears, click **Register** button, as shown in **Fig.A.6.3**:

![Fig.A.6.3](image)

The **Verify User PIN** pop-up appears, enter the User PIN and click **Login** button, as shown in **Fig.A.6.4**:

![Fig.A.6.4](image)
The **Alert** box appears, displaying message "**DSC Registered successfully**", click **OK** button as shown in **Fig.A.6.5**:
Annexure VII

DSC – Error Codes

When the user experiences issue/error in the application, in that case, user can check the logs and understand the issue.

To check for the logs, user needs to go to the location i.e. **Home directory:** `\DscSignerAppLogs` for current day logs and **Home directory:** `\DscSignerApp` for previous day logs.

Below table elaborates the type of errors occurs in DSC web service:

<table>
<thead>
<tr>
<th>S. No</th>
<th>Error Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DSCR01</td>
<td>The certificate without serial number cannot be registered.</td>
</tr>
<tr>
<td>2</td>
<td>DSCR02</td>
<td>Server Date not found in request.</td>
</tr>
<tr>
<td>3</td>
<td>DSCR03</td>
<td>Some Error has been occurred while getting certificate.</td>
</tr>
</tbody>
</table>
| 4     | DSCR04     | DSCR04: Registration failed due to client certificate initialization error due to one of the following reasons: 
1. No DSC is plugged in the system.
2. The plugged DSC is not matching with the registered DSC.
3. The plugged DSC already has been revoked.
4. The system has been restarted after installation of DSC driver. |
<p>| 5     | DSCR05     | The certificate inserted is not valid for registration. One of the certificate keys are missing. |
| 6     | DSCR06     | The selected certificate is not valid for signing. |
| 7     | DSCR07     | System is unable to identify certificate due to one of the following reasons. 1. Verify whether eToken or Smartcard is inserted. 2. Check you have selected a correct certificate. |
| 8     | DSCR08     | The selected certificate is not valid anymore. Check your server date and certificate validity. |
| 9     | DSCR09     | CRL validation failed. The selected certificate is revoked by the CA. |
| 10    | DSCR10     | CRL validation failed. Responder does not know the status of the certificate. |
| 11    | DSCR11     | The DSC has been registered successfully. |
| 12    | DSCR12     | Xml Signature Verification Failed. |
| 13    | DSCR13     | The action was cancelled by the user. |
| 14    | DSCR14     | In case of unknown error/exception while registering. (It is not defined message, it is based on exception/error occurred.) |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>DS CA01</td>
<td>Serial number not found in request.</td>
</tr>
<tr>
<td>17</td>
<td>DS CA02</td>
<td>Server date not found in request.</td>
</tr>
<tr>
<td>18</td>
<td>DS CA03</td>
<td>Some Error has been occurred while getting certificate.</td>
</tr>
<tr>
<td>19</td>
<td>DS CA04</td>
<td>Authentication failed due to client certificate initialization error due to one of the following reasons: 1. No DSC is plugged in the system. 2. The plugged DSC is not matching with the registered DSC. 3. The plugged DSC already has been revoked. 4. The system has been restarted after installation of DSC driver.</td>
</tr>
<tr>
<td>20</td>
<td>DS CA05</td>
<td>The selected certificate is not valid any more. Check your system date and certificate validity.</td>
</tr>
<tr>
<td>21</td>
<td>DS CA06</td>
<td>CRL validation failed. The selected certificate is revoked by the CA.</td>
</tr>
<tr>
<td>22</td>
<td>DS CA07</td>
<td>CRL validation failed. Responder does not know the status of the certificate.</td>
</tr>
<tr>
<td>23</td>
<td>DS CA08</td>
<td>In case of unknown error/exception while signing login seed. (It is not defined message, it is based on exception/error occurred.)</td>
</tr>
<tr>
<td>24</td>
<td>DS CA09</td>
<td>Login seed not found in the request.</td>
</tr>
<tr>
<td>25</td>
<td>DS CA10</td>
<td>XML Signature Verification Failed.</td>
</tr>
<tr>
<td>26</td>
<td>DS CA11</td>
<td>The action was cancelled by the user.</td>
</tr>
<tr>
<td>27</td>
<td>DS CA12</td>
<td>In case of unknown error/exception while authenticating. (It is not defined message, it is based on exception/error occurred.)</td>
</tr>
<tr>
<td>28</td>
<td>DS CAV01</td>
<td>Login seed to verify is not found in request.</td>
</tr>
<tr>
<td>29</td>
<td>DS CAV02</td>
<td>Signed response with respect to Login seed is not found in request.</td>
</tr>
<tr>
<td>30</td>
<td>DS CAV03</td>
<td>Authenticated.</td>
</tr>
<tr>
<td>31</td>
<td>DS CAV04</td>
<td>Authentication Failed.</td>
</tr>
<tr>
<td>32</td>
<td>DS CAV05</td>
<td>XML Signature Verification Failed.</td>
</tr>
<tr>
<td>33</td>
<td>DS CAV06</td>
<td>In case of unknown error/exception while authentication verification. (It is not defined message, it is based on exception/error occurred.)</td>
</tr>
<tr>
<td>34</td>
<td>DS CSF01</td>
<td>No certificate found/registered at the server side.</td>
</tr>
<tr>
<td>35</td>
<td>DS CSF02</td>
<td>No content found to sign.</td>
</tr>
<tr>
<td>36</td>
<td>DS CSF03</td>
<td>Server date not found in request.</td>
</tr>
<tr>
<td>37</td>
<td>DS CSF04</td>
<td>Some Error has been occurred while getting certificate.</td>
</tr>
<tr>
<td>38</td>
<td>DS CSF05</td>
<td>Signing failed due to client certificate initialization error due to one of the following reasons: 1. No DSC is plugged in the system. 2. The plugged DSC is not matching with the registered DSC. 3. The plugged DSC already has been revoked.</td>
</tr>
<tr>
<td>No.</td>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>39</td>
<td>DSCSF06</td>
<td>The selected certificate is not valid any more. Check your server date and certificate validity.</td>
</tr>
<tr>
<td>40</td>
<td>DSCSF07</td>
<td>CRL validation failed. The selected certificate is revoked by the CA.</td>
</tr>
<tr>
<td>41</td>
<td>DSCSF08</td>
<td>CRL validation failed. Responder does not know the status of the certificate.</td>
</tr>
<tr>
<td>42</td>
<td>DSCSF09</td>
<td>In case of unknown error/exception while signing pdf hash. (It is not defined message, it is based on exception/error occurred.)</td>
</tr>
<tr>
<td>43</td>
<td>DSCSF10</td>
<td>Xml Signature Verification Failed.</td>
</tr>
<tr>
<td>44</td>
<td>DSCSF11</td>
<td>The action was cancelled by the user.</td>
</tr>
<tr>
<td>45</td>
<td>DSCSF12</td>
<td>In case of unknown error/exception while signing file. (It is not defined message, it is based on exception/error occurred.)</td>
</tr>
<tr>
<td>46</td>
<td>DSCSN01</td>
<td>No certificate found/registered at the server side.</td>
</tr>
<tr>
<td>47</td>
<td>DSCSN02</td>
<td>No contents found to sign.</td>
</tr>
<tr>
<td>48</td>
<td>DSCSN03</td>
<td>Server date not found in request.</td>
</tr>
<tr>
<td>49</td>
<td>DSCSN04</td>
<td>Some Error has been occurred while getting certificate.</td>
</tr>
<tr>
<td>50</td>
<td>DSCSN05</td>
<td>Signing failed due to client certificate initialization error due to one of the following reasons: 1. No DSC is plugged in the system. 2. The plugged DSC is not matching with the registered DSC. 3. The plugged DSC already has been revoked. 4. The system has been restarted after installation of DSC driver.</td>
</tr>
<tr>
<td>51</td>
<td>DSCSN06</td>
<td>The selected certificate is not valid anymore. Check your server date and certificate validity.</td>
</tr>
<tr>
<td>52</td>
<td>DSCSN07</td>
<td>CRL validation failed. The selected certificate is revoked by the CA.</td>
</tr>
<tr>
<td>53</td>
<td>DSCSN08</td>
<td>CRL validation failed. Responder does not know the status of the certificate.</td>
</tr>
<tr>
<td>54</td>
<td>DSCSN09</td>
<td>In case of unknown error/exception while signing text hash. (It is not defined message, it is based on exception/error occurred.)</td>
</tr>
<tr>
<td>55</td>
<td>DSCSN10</td>
<td>Xml Signature Verification Failed.</td>
</tr>
<tr>
<td>56</td>
<td>DSCSN11</td>
<td>The action was cancelled by the user.</td>
</tr>
<tr>
<td>57</td>
<td>DSCSN12</td>
<td>In case of unknown error/exception while signing text content/note. (It is not defined message, it is based on exception/error occurred.)</td>
</tr>
<tr>
<td>58</td>
<td>DSCR_WS</td>
<td>CRL validation failed. The selected certificate is revoked by the CA.</td>
</tr>
<tr>
<td>59</td>
<td>DSCU06</td>
<td>The certificate inserted is not valid for registration. Signature verification failed. Please contact the issuer organization or the administrator.</td>
</tr>
</tbody>
</table>