Digital Signature Certificate (DSC) Signer Service
Implementation Guidelines

NIC-EOF-DSC-IG-001

Prepared by National Informatics Centre
# 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></td>
<td></td>
</tr>
<tr>
<td>03 October 2018</td>
<td>3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 November 2018</td>
<td>3.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05 March 2019</td>
<td>4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 August 2019</td>
<td>6.0 (NG)</td>
<td>Implementation 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></td>
<td></td>
</tr>
<tr>
<td>27 March 2020</td>
<td>6.0.1 (NG)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26 June 2020</td>
<td>6.1.1 (NG)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

Abbreviations ............................................................................................................. 5

Introduction .................................................................................................................. 6

- New Features and Enhancements ................................................................................. 6

**Section1: Digital Signer Service** .................................................................................. 7

- Procedure to download Digital Signer Service ......................................................... 7
- Client’s Machine Requirement: .................................................................................. 8
- Minimum client’s machine Requirements .................................................................... 8

**Section2: Windows OS** ................................................................................................. 9

- Identifying Your System ............................................................................................... 9
- Pre-requisites for Digital Signer Service Installer for Windows ............................... 10
- Installation Guidelines for Windows OS ....................................................................... 11
  - For Bulk User: ............................................................................................................ 11
  - For Single User: ........................................................................................................ 11

**Section3: MAC** ........................................................................................................ 16

- Pre-requisites for Digital Signer Service Installer ..................................................... 16
- Installation Guidelines for MAC OS ............................................................................ 17
- Add Token(s) in Digital Signer Service (MAC OS): ................................................ 24
- Register Token in Digital Signer Service (MAC OS): ............................................... 27

**Section4: Ubuntu** ..................................................................................................... 29

- Pre-requisites for Digital Signer Service Installer for Ubuntu OS ........................... 29
- Installation Guidelines for Ubuntu OS ......................................................................... 30
- Add Token(s) in Digital Signer Service (Ubuntu OS): ............................................... 33
- Register Token in Digital Signer Service (Ubuntu OS): ........................................... 36

**Section 5: Checking the Service Status** .................................................................... 38

- For Windows/MAC/Ubuntu ......................................................................................... 38

**Annexure I** .............................................................................................................. 40

- Add/Import SSL Certificate to the Browsers ............................................................. 40
  - For Mozilla Firefox .................................................................................................. 40
  - For Chrome ............................................................................................................... 43
  - For Internet Explorer ............................................................................................... 45

**Annexure II** ............................................................................................................ 50

- Troubleshooting (For Digital Signer Service). .......................................................... 50
Annexure III ........................................................................................................................................55
  Signature Validity Checkmark Visibility ..........................................................................................55
  The visual representation of signature verification ...........................................................................55
  Display of Valid Signature in previous version of Digital Signature ..................................................55
  Display of Valid Signature in Current Version of Digital Signature ................................................56
  How to verify signature in current scenario .......................................................................................57

Annexure IV .........................................................................................................................................59
  DSC token Pin Management in prevalent tokens today.................................................................59
  ProxKey Token-session Management .............................................................................................59
  ePass Token Session Management ..................................................................................................60
    Session Time limit setting (For ePass Token) ..................................................................................61
  Aladin Token-Session Management ..................................................................................................62

Annexure V .........................................................................................................................................64

Identifying Your System ......................................................................................................................64
  Windows OS .....................................................................................................................................64
    Check Windows version: .....................................................................................................................64
    Check availability of Java Version in windows: ...............................................................................64
  MAC OS ...........................................................................................................................................66
    Checking MAC version: ....................................................................................................................66
    Check availability of Java Version in MAC OS: ..............................................................................66
  Ubuntu OS .......................................................................................................................................67
    Checking Ubuntu version: ..............................................................................................................67
    Check availability of Java Version in Ubuntu OS: .........................................................................67

Annexure VI .........................................................................................................................................68
  DSC –Error Codes .............................................................................................................................68
## 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.

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

In the previous version, multiple URLs were used for signing/authentication/registration purposes, and this was quite complex for consuming applications. To make it simple, in the current version of Digital Signer Service 6.1.1 (.msi installer) a single URL is provided for signing/authentication/registration purposes. A new functionality is provided for single or multiple signatures on a single PDF document as well as for bulk signing of PDF documents. Also, user(s) can add multiple token drivers in MAC/Ubuntu machines. It is essentially a service that would require to be installed one time in the individual windows/MAC/Ubuntu client’s machines of the user.

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

New Features and Enhancements

1. Multiple signatures on a single PDF.
2. An enhanced & modified Digital Signer Service 6.1.1 interface is created for all platforms (Windows/Mac/Ubuntu) and additionally, the user(s) can add /configure new token(s) to work with MAC/Ubuntu clients’ machines.
3. Improved messages & exception handling.
4. Users can remove the signature from pdf files(s) and can also get details of previously signed pdf file(s).
5. In a single go, Digital Signer Service 6.1.1 can be installed silently on multiple machines.
6. Updates can now install automatically.
7. Windows users can remove/uninstall Digital Signer Service 6.1.1 from Control Panel.
8. Quick Help.
Section 1: Digital Signer Service

Procedure to download Digital Signer Service
The Digital Signer Service 6.1.1 can be downloaded from (as per client’s machine OS):

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

OR

https://eoffice.gov.in, shown in Fig.1.1 & Fig.1.2:
1. Windows (For installation steps refer Section 2 Windows)
2. MAC (For installation steps refer Section 3 MAC)
3. Ubuntu (For installation steps refer Section 4 Ubuntu)

**Client’s Machine Requirement:**
The Digital Signer Service is available for following OS client’s machine:

<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 appropriate as per OS</td>
</tr>
<tr>
<td><strong>Availability of port 55103</strong></td>
<td></td>
</tr>
</tbody>
</table>

Note:
For Digital Signer Service 4.1 the available ports are 55100 and 55101.
Section 2: Windows OS

Download the Digital Signer Service 6.1.1 and related utilities (available as a single bundled zip file) from one of the URLs mentioned previously.

Identifying Your System

- Unzip the downloaded folder, locate and run `Check_System_Details.bat` file from downloaded bundle (`Digital Signer Service 6.1.1 windows Installer folder, Fig.2.1`) to check if user machine has java installed or not.

  ![Fig.2.1](image)

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

    ![Fig.2.2](image)

Note:

1. In case .bat file does not run, refer to Annexure V for manually identifying the JAVA, OS and Digital Signer Service status details.
# Pre-requisites for Digital Signer Service Installer for Windows

## Following four activities to be completed by User(s).

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Java Version 1.8 appropriate as per OS.</td>
<td>Needs to be downloaded at client machine by Individual User. (Refer website <a href="https://www.oracle.com/java/technologies/javase-jre8-downloads.html">https://www.oracle.com/java/technologies/javase-jre8-downloads.html</a> for JRE installation).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note:</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 needs to installs 64-bit JRE.</td>
</tr>
<tr>
<td>2.</td>
<td>Add/ Import SSL certificate to the browsers.</td>
<td>To Add/ Import SSL certificate to the browsers (Refer Annexure I for steps).</td>
</tr>
<tr>
<td>3.</td>
<td>Re-register DSC (*only applicable for users previously using applet based signing service)</td>
<td>For user(s) who have already DSC registered in eOffice application, then to use new Digital Signer Service, they have to de-activate already registered certificate and register again one time. (*only applicable for users previously using applet based signing service).</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(s)

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

For Single User:
• Locate and select the Digital Signer Service 6.1.1_x64.msi / Digital Signer Service 6.1.1_x86.msi file from the downloaded bundle as per the system configuration (32 bit or 64 bit respectively).
• Double click required msi file to start the installation as shown in Fig.2.3:

Fig.2.3

• A welcome page appears, click Next button to continue as shown in Fig.2.4:

Fig.2.4
- **End-User License Agreement** window appears, read the agreement. Click **I Accept** radio button and then click **Next (Next >)** button as shown in Fig.2.5:

![End-User License Agreement](image)

**Fig.2.5**

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

**OR**

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

![Select Installation Folder](image)

**Fig.2.6**
- **Install SSL Certificate** (for first time installation at clients' machine) screen appears, select **Yes** radio button and then click **Install** button as shown in **Fig.2.7 (a):**

![Fig.2.7 (a)](image)

OR

- **Upgrade Older Version & Install SSL Certificate** (previous version exists in clients' machine) window appears asking for **SSL certificate**, now, to remove the older version or for side by side installation select the respective option.

- Also, to add **SSL certificate** in Internet Explorer browser, select **Yes** radio button and then click **Install** button as shown in **Fig.2.7 (b):**

![Fig.2.7 (b)](image)
Note:
SSL certificate is mandatory for signing purpose, if user clicks on No option while installing the Digital Signer Service, then they have to install the certificate manually in Internet Explorer as well (To Add/ Import SSL certificate to the browsers refer Annexure I).

- **Side by Side installation:** Process will take some moments to complete the installation and click **Finish** button as shown in Fig.2.8.

- **Upgrade to new version:** Process will take some moments to uninstall the Digital Signer Service 4.1 and complete the installation of Digital Signer Service 6.1.1 and click **Finish** button as shown in Fig.2.8:

![Fig.2.8](image)

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

- This completes the installation of Digital Signer Service 6.1.1 for Windows user(s).
- A shortcut will be created on the desktop, named Digital Signer Service 6.1.1.
- Also, a Digital Signer Service icon will appear in the system tray (in the bottom-right corner of monitor) which indicates that Digital Signer Service is running in the system, as shown in Fig.2.9:

![Fig.2.9](image)

- Now, whenever the system is turned on the Digital Signer Service will start automatically.
Steps to manually START/STOP the Digital Signer Service 6.1.1 are:

- To start the service, double click the desktop icon “Digital Signer Service 6.1.1”.
- The service will take a few seconds to start and once it is started it will appear in system tray.

- Right click on the Digital Signer Service Icon ( ) from the system tray & select Open/Stop button as per requirement, as shown in Fig. 2.10:

![Fig.2.10](image)

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

![Fig.2.11](image)

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

![Fig.2.12](image)

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

Note:
1. To import the SSL certificate refer Annexure I (Add/Import SSL certificate to the Browsers).
Section 3: MAC

Download the Digital Signer Service 6.1.1 and related utilities (available as a single bundled zip file) from one of the URLs mentioned previously.

Pre-requisites for Digital Signer Service Installer

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add/ Import SSL certificate to the browsers.</td>
<td>To Add/ Import SSL certificate to the browsers (Refer Annexure I for steps).</td>
</tr>
<tr>
<td>2.</td>
<td>Re-register DSC (*only applicable for users previously using applet based signing service)</td>
<td>For user(s) who have already DSC registered in eOffice application, then to use new Digital Signer Service, they have to de-activate already registered certificate and register again one time. (*only applicable for users previously using applet based signing service)</td>
</tr>
<tr>
<td>3.</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(s)

<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 Digital_Signer_Service-6.1.1.sh file from the downloaded bundle (Digital Signer Service v6.1.1 MAC Installer folder, Fig.3.1).

  ![Fig.3.1](image1)

- Go to the downloaded location of Digital_Signer_Service-6.1.1.sh file and open the terminal.
- Run the command "sudo bash Digital_Signer_Service-6.1.1.sh" on the terminal for MAC OS.
- Then, provide account password (if required) and press Enter.
- In case any other process is using port 55103, system will ask user for YES/NO, as shown in Fig.3.2:
- Type 'Y' for terminating that process and continue installation of Digital Signer Service otherwise type 'N' for terminating the Digital Signer Service installation.

  ![Fig.3.2](image2)

- This completes the installation of Digital Signer Service for MAC user(s).
After successful installation, a message “Digital Signer Service 6.1.1 installed successfully” will be displayed as shown in Fig.3.3

- Press ‘Y’ to restart the system (Fig.3.3) or manually reboot the system.

- Restart is mandatory to run Digital Signer Service 6.1.1 effectively.

- For the first time installation in Mac OS, a confirmation window appears asking for allowing the installation of Digital Signer Service, as shown in Fig.3.4:
For allowing the installation of Digital Signer Service, steps are:

- Go to System Preferences and click Security & Privacy, as shown in Fig.3.5:

![Fig.3.5](image)

- Allow installation access by clicking Open Anyway button as shown in Fig.3.6:

![Fig.3.6](image)
A prompt window appears, click **Open** button as shown in **Fig.3.7**:

![Fig.3.7]

- A shortcut will be created on the desktop, named **Digital Signer Service 6.1.1**.
- Also, a Digital Signer Service icon ( ) will appear in the menu bar (in the upper-right corner of monitor) which indicates that Digital Signer Service 6.1.1 is running in the system, as shown in **Fig.3.8**:

![Fig.3.8]

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

**In case the Digital Signer Service does not start automatically, follow the below steps:**
- Go to **System Preferences** and click **Users & Group**, as shown in **Fig.3.9**:

![Fig.3.9]
• Select **Current Login User**, click **Login Items** tab and then click + icon, as shown in **Fig.3.10**:

![Fig.3.10](image)

• **Browse the Digital Signer Service and click the Add ( ) button**, as shown in **Fig.3.11**:

![Fig.3.11](image)

• **Now, the Digital Signer Service will appear under Users & Group screen (Fig.3.12) and whenever the system is turned on the Digital Signer Service will start automatically.**

![Fig.3.12](image)
Steps to manually START / STOP the Digital Signer Service 6.1.1 are:

- To start the service, double click the desktop icon "Digital Signer Service 6.1.1".
- The service will take a few seconds to start and once it is started it will appear in menu bar.
- Left click on the Digital Signer Service icon from the menu bar & select Configure / Stop button as per requirement, as shown in Fig. 3.13:

![Fig. 3.13](image)

- Digital Signer Service application window appears, to stop the service click Stop Service button, as shown in Fig. 3.14:

![Fig. 3.14](image)

- Warning pop-up window appears, click Yes button to stop the Digital Signer Service, as shown in Fig. 3.15:

![Fig. 3.15](image)
- The Digital Signer Service gets stopped and icon will disappear from the menu bar.

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

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

Steps to add new token in Digital Signer Service are:

- Open Digital Signer service app and click Add New Token ( ) button, as shown in Fig.3.16:

Fig.3.16

Note:

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

Fig.3.17

Home ( ): To go back to Home screen of Digital Signer Service
- Provide Token Name, Token Path and click **Save** button, as shown in **Fig.3.18**:

![Fig.3.18](image)

**Note:**

1. Token Name & Token Path is mandatory.
2. User can also copy & paste the Token path in the Digital Signer Service (**Fig.3.18**).
3. The token name should be relevant like if a user is adding token of epass then the token name must include “epass” in its name e.g. epass-new, new-epass, etc.

- Login window appears, enter the **Token Pin** and click **OK** button as shown in **Fig.3.19**:

![Fig.3.19](image)
• The certificate list appears, if valid certificate is displayed, click **Confirm** button, else click **Reject** button, as shown in Fig.3.20:

![Fig.3.20](image)

• Token details get added successfully, click **OK** button as shown in Fig.3.21:

![Fig.3.21](image)

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

Steps to register the token with Digital Signer Service are:

- Left click the menu bar icon "Configure", click Configure option, as shown in Fig.3.22:

![Fig.3.22](image)

- The digital Signer Service window appears, select token from the drop-down list, as shown in Fig.3.23:

![Fig.3.23](image)

- Token path for the selected token gets populated in the Token Path Field.

- Select checkbox for setting the token as default token, as shown in Fig.3.24:

![Fig.3.24](image)
- Confirmation window appears, click **Yes** button as shown in **Fig.3.25**:

![Digital Signer Service](image)

**Fig.3.25**

**Note:**

1. It is mandatory for singing purpose to set the selected token as default.
2. In case the Token is not available in Token Name dropdown list, then Add the token (refer [Steps to add new token in Digital Signer Service](#))
## Section 4: Ubuntu

Download the Digital Signer Service 6.1.1 and related utilities (available as a single bundled zip file) from one of the URLs mentioned previously.

### Pre-requisites for Digital Signer Service Installer for Ubuntu OS

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Activities</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add/ Import SSL certificate to the browsers.</td>
<td>To Add/ Import SSL certificate to the browsers (Refer <a href="#">Annexure I</a> for steps).</td>
</tr>
<tr>
<td>2.</td>
<td>Re-register DSC (*only applicable for users previously using applet based signing service)</td>
<td>For user(s) who have already DSC registered in eOffice application, then to use new Digital Signer Service, they have to de-activate already registered certificate and register again one time. (*only applicable for users previously using applet based signing service).</td>
</tr>
<tr>
<td>3.</td>
<td>Internet connectivity is required to check for certificate revocation status</td>
<td>Check the Internet connectivity at every client machine.</td>
</tr>
<tr>
<td>4.</td>
<td>Account password setting.</td>
<td>Account password is required for installing DSC signer service.</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 Digital_Signer_Service-6.1.1.sh file from the downloaded bundle (Digital Signer Service 6.1.1 Ubuntu Installer folder, Fig.4.1).

![Fig.4.1]

- Go to the downloaded location of Digital_Signer_Service-6.1.1.sh file and open the terminal.

- Run the command “sudo bash Digital_Signer_Service-6.1.1.sh” on the terminal for Ubuntu OS.

- Then, provide account password (if required) and press Enter.

- In case other process is using port 55103, system will ask user for YES/NO as shown in Fig.4.2:

- Type ‘Y’ for terminating that process and continue installation of Digital Signer Service otherwise type ‘N’ for terminating the Digital Signer Service installation.

![Fig.4.2]

- This completes the installation of Digital Signer Service for Ubuntu user(s).
• After successful installation, a message “Digital Signer Service 6.1.1 installed successfully” will be displayed as shown in Fig.4.3:

![Fig.4.3](image)

• Press 'Y' to restart the system (Fig.4.3) or manually reboot the system.

• Restart is mandatory to run Digital Signer Service 6.1.1 effectively.

Steps to manually START/STOP the Digital Signer Service 6.1.1 are:

• Double click the desktop icon (辋) “Digital Signer Service 6.1.1”.

• The Digital Signer Service pop-up window appears and the service gets started, as shown in Fig.4.4:

![Fig.4.4](image)
• Now, click **Hide Service** or **Stop Service** button to hide the screen.

• To Stop the service, click **Stop Service** button.

• Warning window appears, click **Yes** button to stop the Digital Signer Service, as shown in **Fig.4.5**:

![Digital Signer Service](image)

**Fig.4.5**

• The Digital Signer Service gets stopped.

Note:

1. While using the Digital Signer Service application if a token is plugged-out or not properly plugged-in before signing, then, occasionally user has to manually restart the Digital Signer Service. This issue is tokens specific, so to avoid this ensure that token is properly plugged-in before proceeding for Signing/Authentication/Registration process. For restarting the Digital Signer Service manually, refer Annexure II (Troubleshooting→**Problem 1**).

2. There are many providers for DSC tokens and sometimes issue(s) specific to DSC token hardware may come, for which the respective vendor may be approached.

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

4. Refer to **Annexure V** for manually identifying the JAVA, OS and Digital Signer Service status details.
Add Token(s) in Digital Signer Service (Ubuntu OS):

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

Steps to add new token in Digital Signer Service are:

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

![Fig.4.6](image)

Note:

Help (Help): Click help icon for “About and How to add token?” steps.

![Fig.4.7](image)

Home (Home): To go back to Home screen of Digital Signer Service
• Provide Token Name, Token Path and click **Save** button, as shown in **Fig.4.8**:

![Fig.4.8](image)

**Note:**

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

• Login window appears, enter the **Token Pin** number and click **OK** button as shown in **Fig.4.9**:
The certificate list appears, if valid certificate is displayed, click **Confirm** button, else click **Reject** button, as shown in Fig.4.10:

![Certificate List](image1)

Fig.4.10

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

![Token Added](image2)

Fig.4.11

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

Steps to register the token with Digital Signer Service are:

- Double click the desktop icon “Digital Signer Service 6.1.1”.

- The digital Signer Service window appears, select token from the drop-down list, as shown in Fig.4.12:

![Fig.4.12](image)

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

![Fig.4.13](image)
• Confirmation window appears, click Yes (Yes) button as shown in Fig.4.14:

![Digital Signer Service v6.1](image)

Fig.4.14

**Note:**
1. It is mandatory for signing purpose to set the selected token as default.
2. In case the Token is not available in Token Name dropdown list, then Add the token (refer Add new token in Digital Signer Service)
Section 5: Checking the Service Status

For Windows/MAC/Ubuntu

Digital Signer Service uses 55103 port.

https port: 55103

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

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

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

![Fig.5.1]

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

![Fig.5.2]
4. To check for service status manually use [https://127.0.0.1:portNumber/check/isLive](https://127.0.0.1:portNumber/check/isLive)
   For Ex. [https://127.0.0.1:55103/check/isLive](https://127.0.0.1:55103/check/isLive)

“Success” message on the screen states that the service is running successfully otherwise may refer to the [Annexure II (Troubleshooting)](https://example.com).

**Note:**

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

Add/Import SSL Certificate to the Browsers

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

Note:
SSL certificate gets automatically imported in Internet Explorer browser only in the case when the user selects the YES option for adding the SSL certificate during the installation process.

- Download the Digital Signer Service Installer folder (For windows/ For MAC/ For Ubuntu), go to the “Pre-Requisites” folder and locate the Self Signed 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://127.0.0.1:55103/check/isLive as shown in Fig.A.1.1:
• Then, the browser will notify the user to add the exception to the list (Fig.A.1.1).

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

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

![Fig.A.1.2](image)

• 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:

![Fig.A.1.3](image)
• The browser will confirm and displays the message “Success” as shown in Fig.A.1.4:

![Image of browser displaying success message]

**Fig.A.1.4**

**Note:**
Kindly use updated version of Mozilla Firefox browser.
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://127.0.0.1:55103/check/isLive as shown in Fig.A.1.5:

![Fig.A.1.5](image)

- The browser will notify the user to add the exception to the list (Fig.A.1.5).
- Click 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:
- Additionally, go to browser and type “chrome://flags/#allow-insecure-localhost” in address bar.

- Searched flags screen appears, select **Enabled** to allows requests to local host 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-url)
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://127.0.0.1:55103/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** tab and select the **Certificates** button as shown in **Fig.A.1.11**:

![Internet Options window](image)

**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**:

![Certificates window](image)

**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 (Yes) button, as shown in Fig.A.1.17:

![Security Warning Window](image1)

Fig.A.1.17

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

![Certificate Import Wizard](image2)

Fig.A.1.18
Annexure II

Troubleshooting (For Digital Signer Service)

Problem 1
Service is not running after successful installation.

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

For Windows

- Double click the desktop icon “Digital Signer Service 6.1.1”.
- Digital signer Service icon will appear in the system tray (in the bottom-right corner of monitor) which indicates that Digital Signer Service is running in the system, as shown in Fig.A.2.1:

![Fig.A.2.1](image)

For MAC

- Restart the Digital Signer Service by clicking desktop icon “Digital Signer Service 6.1.1”.
- Digital Signer Service icon will appear in the menu bar (in the upper-right corner of monitor) which indicates that Digital Signer Service 6.1.1 is running in the system, as shown in Fig.A.2.2:

![Fig.A.2.2](image)

For Ubuntu

- Restart the Digital Signer Service by clicking desktop icon “Digital Signer Service 6.1.1”.

Note:
1. While using DSC application in MAC OS and Ubuntu OS, if a token is plugged-out, then, occasionally user has to manually restart the Digital Signer Service.
Problem 2
Service is not running even after starting manually.

Solution
Check availability of port HTTPs
https port: 55103

Commands to check for availability of port are mentioned below:

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

Screen-shot

```
C:\Users\DELL> netstat -ano | find "55103"
TCP 0.0.0.0:55103 0:0:0:0:0:0:0:0 LISTENING 12008
TCP [::]:55103 [::]:0 LISTENING 12008
```

Fig.A.2.3

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

Screen-shot

```
pankaj@PS:~$ netstat -tunlp | grep 55103
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp6 0 0 :::55103 ::::
1940/java
pankaj@PS:~$ 
```

Fig.A.2.4
For MAC
For MAC use Terminal.
**Command:** `netstat -tanptcp | grep port` (Fig.A.2.5).

**Screen-shot**

![Screen-shot](image)

**Fig.A.2.5**

If no service is running on port, manually start the service. If still it does not start, contact the administrator.
Problem 3
If the port 55103 is in use with some other service.

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

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

Screen-shot

![Fig.A.2.6](image)

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

Screen-shot

![Fig.A.2.7](image)
Problem 4
If the certificate is not displaying while adding a new token in MAC/Ubuntu machine.

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

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

Screen-shot

![Screen-shot](image)

**Fig.A.2.8**
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](image)

![Fig.A.3.2: Invalid Signature](image)
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:
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:
Red Cross: Invalid Signature

Fig.A.3.5: Invalid Signature
Annexure IV

DSC token Pin Management in prevalent tokens today

User PIN is the password which the digital signature (Digital Signer Service 6.1.1 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 token 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 tokens are given below; same steps will be followed in case of other token(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
```

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

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

Steps to set the DSC token 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
```
3. Enter DSC token PIN, Timeout time and click **Ok** button, as shown in **Fig.A.4.6**

![Fig.A.4.6]

**Note:**
It is not mandatory to change the DSC token 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]
3. Click **eToken PKI client Settings** and then click **Advanced** tab as shown in Fig.A.4.8

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

![Fig.A.4.1](image)

Check availability of Java Version in windows:
- Click Start button and go to Control Panel.
- Click Java link as shown in Fig.A.4.2:

![Fig.A.4.2](image)
• A screen appears is shown in Fig.A.4.3, select Java (Java) tab and then click View (View...) button.

![Fig.A.4.3](image)

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

![Fig.A.4.4](image)
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

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: \DigitalSignerService-6.1.1\Logs for current day logs and Home directory: \DigitalSignerService-6.1.1\Logs\archives 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>DSC-01</td>
<td>No Certificate Found.</td>
</tr>
<tr>
<td>2</td>
<td>DSC-02</td>
<td>Purpose is not defined in request.</td>
</tr>
<tr>
<td>3</td>
<td>DSC-03</td>
<td>Serial number not found in request.</td>
</tr>
<tr>
<td>4</td>
<td>DSC-04</td>
<td>Server Date not found in request.</td>
</tr>
<tr>
<td>5</td>
<td>DSC-05</td>
<td>System date is not valid. Kindly check system date.</td>
</tr>
</tbody>
</table>
| 6     | DSC-06     | Purpose (Signing/Authentication/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. |
| 7     | DSC-07     | Selected certificate chain is not found. |
| 8     | DSC-08     | The selected certificate is not valid any more. Check your system date and certificate validity. |
| 9     | DSC-09     | The certificate inserted is not valid for purpose.
1. One of the certificate keys are missing. |
<p>| 10    | DSC-10     | No input found to check if certificate is valid for registration. |
| 11    | DSC-11     | No content found to sign. |
| 12    | DSC-12     | No login seed found to authenticate. |
| 13    | DSC-13     | The selected certificate is not valid for signing. |
| 14    | DSC-14     | CRL validation failed. The selected certificate is revoked by the CA. |
| 15    | DSC-15     | OCSP validation failed. The selected certificate is revoked by the CA. |
| 16    | DSC-16     | OCSP validation failed. Responder does not know the status of the certificate. |
| 17    | DSC-17     | The action was cancelled by the user. |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>DSC-18</td>
<td>No provider configuration found on this OS.</td>
</tr>
<tr>
<td>19</td>
<td>DSC-19</td>
<td>Invalid or no library definition found for the provider in this OS.</td>
</tr>
<tr>
<td>20</td>
<td>DSC-20</td>
<td>Either device driver is to be installed or Digital Signer Service requires restart.</td>
</tr>
<tr>
<td>21</td>
<td>DSC-21</td>
<td>Incorrect password provided.</td>
</tr>
<tr>
<td>22</td>
<td>DSC-22</td>
<td>No driver found for this path in this OS.</td>
</tr>
<tr>
<td>23</td>
<td>DSC-23</td>
<td>Either device driver is to be installed or Token is not plugged in.</td>
</tr>
<tr>
<td>24</td>
<td>DSC-24</td>
<td>Error in retrieving the certificate chain.</td>
</tr>
<tr>
<td>25</td>
<td>DSC-25</td>
<td>Either action was cancelled by the user or some internal error occurred.</td>
</tr>
<tr>
<td>26</td>
<td>DSC-26</td>
<td>Signing failed due to internal application error.</td>
</tr>
<tr>
<td>27</td>
<td>DSC-27</td>
<td>Invalid signature/the object has not been signed.</td>
</tr>
<tr>
<td>28</td>
<td>DSC-28</td>
<td>Signing failed due to the certificate chain not found in the system. Please contact the administrator.</td>
</tr>
<tr>
<td>29</td>
<td>DSC-29</td>
<td>Signing failed. Please check if the Digital token has been inserted properly in the system.</td>
</tr>
<tr>
<td>30</td>
<td>DSC-30</td>
<td>Signing failed due to unexpected internal application error while signing the document.</td>
</tr>
<tr>
<td>31</td>
<td>DSC-31</td>
<td>Client machine date has been changed during process.</td>
</tr>
<tr>
<td>32</td>
<td>DSC-32</td>
<td>Certificate not found. It may be due to faulty USB Port/Token or token has been plugged-out.</td>
</tr>
<tr>
<td>33</td>
<td>DSC-33</td>
<td>Error while signing xml response.</td>
</tr>
<tr>
<td>34</td>
<td>DSC-34</td>
<td>Error while validating XML signature.</td>
</tr>
<tr>
<td>35</td>
<td>DSC-35</td>
<td>Error while initializing keystore to verifying/signing request/response xml.</td>
</tr>
<tr>
<td>36</td>
<td>DSC-36</td>
<td>Some error occurred while getting OCSP response.</td>
</tr>
<tr>
<td>37</td>
<td>DSC-37</td>
<td>Chain certificate not found for certificate serial no <strong>Serial Number</strong> while getting OCSP response</td>
</tr>
<tr>
<td>38</td>
<td>DSC-38</td>
<td>Unable to check OCSP response due to network error. Kindly contact your system administrator.</td>
</tr>
<tr>
<td>39</td>
<td>DSC-39</td>
<td>Some unknown error occurred.</td>
</tr>
<tr>
<td>Created By</td>
<td>Reviewed By</td>
<td>Approved By</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Rimandeep Kaur</td>
<td>Navdeep Singh Nagi</td>
<td>Navneet Kaur</td>
</tr>
<tr>
<td>Maheep Singh</td>
<td>Pankaj Shakya</td>
<td>Scientist- C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eOffice Project Division</td>
</tr>
</tbody>
</table>
eOffice Project Division
National Informatics Centre

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