सत्यमेव जयते

eOffice

A DIGITAL WORK PLACE SOLUTION

DST

Digital Signing Tool

User Manual

NIC-EOF-DST-UM-001

Prepared by
National Informatics Centre

Amendment History

Date	Document Version	Description	Author
13 June 2018	3.2	User Manual	eOfice Project Division
28 March 2019	4.1	User Guidelines	eOfice Project Division

Table of Contents

Introduction 4

About Digital Signing Tool 4.1 5

Features 6

DST 7

Pre-Requisite for DST Installation 8

Installation Guidelines for DST 9

How the Tool Works 10

- Single PDF Signing 11
- Bulk PDF Signing 18
- View/Verify Signature Detail 19

Configuration 22

Annexure-I 23

Annexure-II 24

- Process to Validate a Signature on a Digitally Signed Document 24

Annexure III 29

- Troubleshooting (For DST) 29

Annexure IV 35

- DSC Pin Management in prevalent dongles today 35
  - ProxKey Token-session Management 35
  - ePass Token Session Management 36
  - Aladin Token-Session Management 38

Annexure V 40

Introduction

Due to recent digital India initiatives, electronic signatures have started gaining acceptability as trustworthy signing mechanism for maintaining identity, authenticity, and security of the electronic documents/transactions.

Digital Signature is the subset of the electronic signatures that use public key infrastructure (PKI) to digitally sign an electronic document and provide assurances of the evidence to the provenance of the identity of signer and integrity of the document. This means that the content of the document cannot be altered after signing and the receiver of a document is assured of the signer authenticity.

The Information Technology Act, 2000 and subsequent amendments provide the required legal sanctity to the digital signatures based on asymmetric cryptosystems.

About Digital Signing Tool 4.1

PDF digital signing tool Version 1.0 was released in the year 2014 and made available through e-Gov App store. Version 3.2 of this open source desktop tool is now being released with enhanced features, improved and intuitive signer interface and built on latest technology using JavaFX. It provides digitally signing of the electronic documents (PDF) by reading digital certificates (X.509) from USB token provided by the CA. In **Version 4.1**, some internal API changes are made.

The digital signing functionality is provided for single or multiple signatures on a single PDF document as well as for bulk signing of PDF documents.

Features

1. Tool Interface supports two languages (English & Hindi).
2. Simple signing of single PDF files
3. Multiple signs on a single PDF.
4. Bulk singing of multiple documents with a single sign.
5. Bulk signing of multiple documents with multiple signs.
6. Enabling/Disabling signature visibility in the PDF based on signer's choice.
7. Coordinates selection to sign on the desired location in single signing.
8. Coordinates selection to sign on the desired location in bulk signing. (In this case, the bulk documents should be same structure so that sign is placed properly uniformly at the chosen location).
9. Password window is provided for signing password protected PDF files.
10. Certificate Revocation List (CRL) check before signing.
11. Configuration to set Maximum number of files can be signed in one go. The default value is 5000 PDF files.
12. Configuration to set the Maximum number of signatures on the same document, for bulk signing also. The default value is 10 signatures.
13. View and verify signature details on Single Signed PDF file(s).
14. View and verify signature details on Bulk Signed PDF files.
15. Quick Help.

DST

The DST is available for following **OS** client's machine:

1. Windows
2. MAC
3. Ubuntu

Minimum client's machine Requirements	
Windows OS	Windows 7 & above.
MAC OS	MAC 10.7 & above.
Ubuntu OS	Ubuntu 18 & above.
JRE	Version 1.8 or above appropriate as per OS.
Internet connectivity	Internet connectivity is required at every client machine.

Pre-Requisite for DST Installation

Pre-requisite required for smooth installation, implementation, and use of DST:

JAVA Download/ Installation:

DST Installation procedures for different Operating Systems are described in **Table 1** below:

OPERATIG SYSTEM		
Windows	**MAC**	**UBUNTU**
Download the latest JRE version available from the Official site at client machine. (Refer website https://www.java.com/en/ for JRE installation). **Note:** 1. User(s) with 32-bit windows OS needs to install 32-bit JRE. 2. User(s) with 64-bit windows OS needs to installs 64-bit JRE.	In case of MAC only tool needs to be installed.	In case of Ubuntu only tool needs to be installed.

Installation Guidelines for DST

OPERATIG SYSTEM		
Windows	**MAC**	**UBUNTU**
• Locate the **Digital_Signing_Tool.exe** file from downloaded bundle. • Double click required **exe** file to start the installation • For a custom installation, click **Browse (** Browse... **)** button, select the directory and click **Next (** Next > **)** button. **OR** • For default installation, click **Next (** Next > **)** button. • **Digital Signing Tool: License Agreement** window appears, read the agreement and click **I Agree** (I Agree) button. • Click **Close (** Close **)** button, the DST is successfully installed. • A shortcut is created on the desktop, named **DST**. • Double click the desktop icon "**DST**" to use the tool.	• Locate the **InstScript** file from downloaded bundle. • Open terminal at the same location of **InstScript** file. • Run the command "***sudo bash InstScript***" on the terminal for MAC OS. • This completes the installation of **DST** for MAC user(s). • After successful installation, a message "**DST**" will be displayed.	• Locate the **InstScript** file from downloaded bundle. • Open terminal at the same location of **InstScript** file. • Run the command "***sudo bash InstScript***" on the terminal for Ubuntu OS. • This completes the installation of **DST** for Ubuntu user(s). • After successful installation, a message "**DST**" will be displayed. • Then, reboot the system

How the Tool Works

The tool interface support two languages (**English and Hindi**), and consist of four tabs (**Fig.1**):

- **Single Signing**
- **Bulk PDF Signing**
- **View/Verify Signature Detail**
- **Configuration**

Fig.1

Note:

By default the interface is in English Language.

Let's learn to use sign the PDF(s) using the above mentioned tabs of DST.

Single PDF Signing

This option allows a signer to sign a new document or a previously signed document.

To sign a document, steps are:

- Click **Single PDF Signing** tab, then click the **Browse** (Browse) button to select the document for signing as shown in **Fig.2**:
- By default, the destination location of the signed document will be the same as the source location.
- To change the destination location, click Browse (Browse) button corresponding to the "**Save To**" option and select the destination folder to save the signed document, as shown in **Fig.2**:
- Add the remarks (if required) in **Remarks** field, as shown in **Fig.2**:

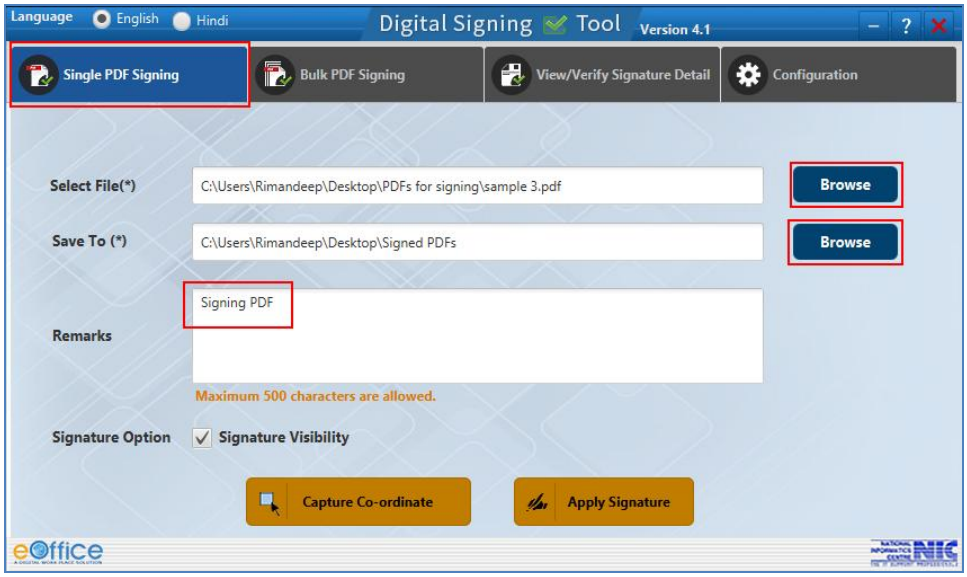

Fig.2

Signature visibility: It is related to the appearance of signature on the document.

To maintain the authenticity and integrity of the document, user can use hide signature visibility. By default, Signature Visibility option remains checked.

- Uncheck the checkbox corresponding to **Signature Visibility** option, depending on the requirement as shown in **Fig.3**:

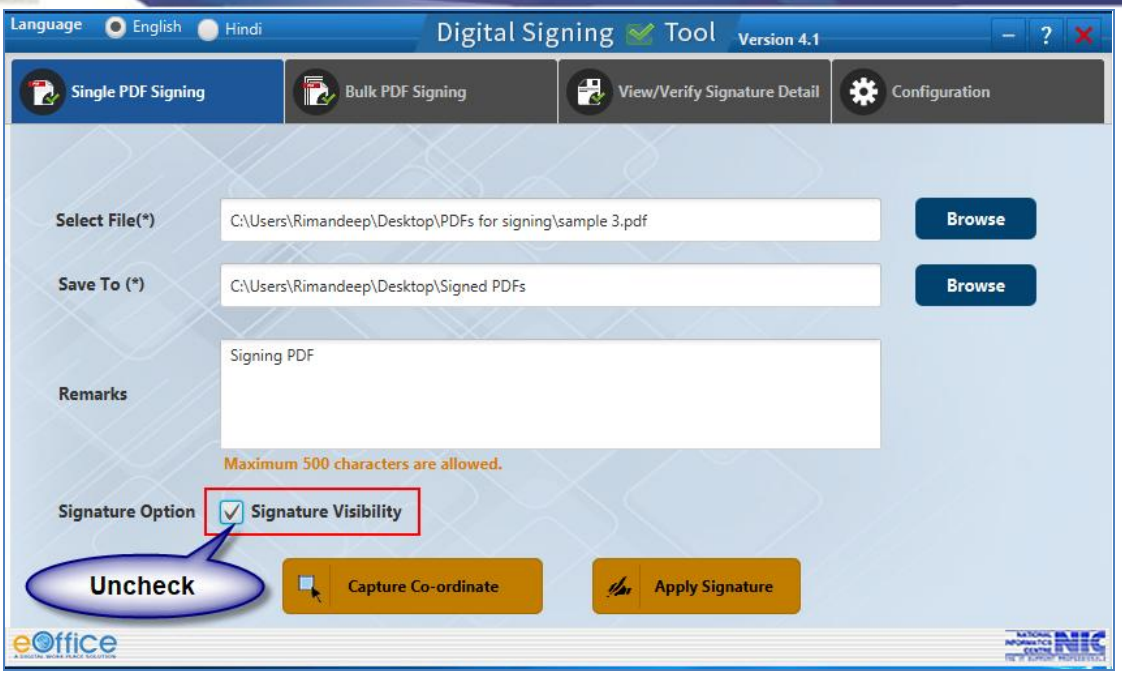

Fig.3

- **Green Check** will be shown at upper left corner of adobe reader and also inside signature panel itself with "**Field: Signature1 (Invisible Signature)**", as shown in **Fig.4**:

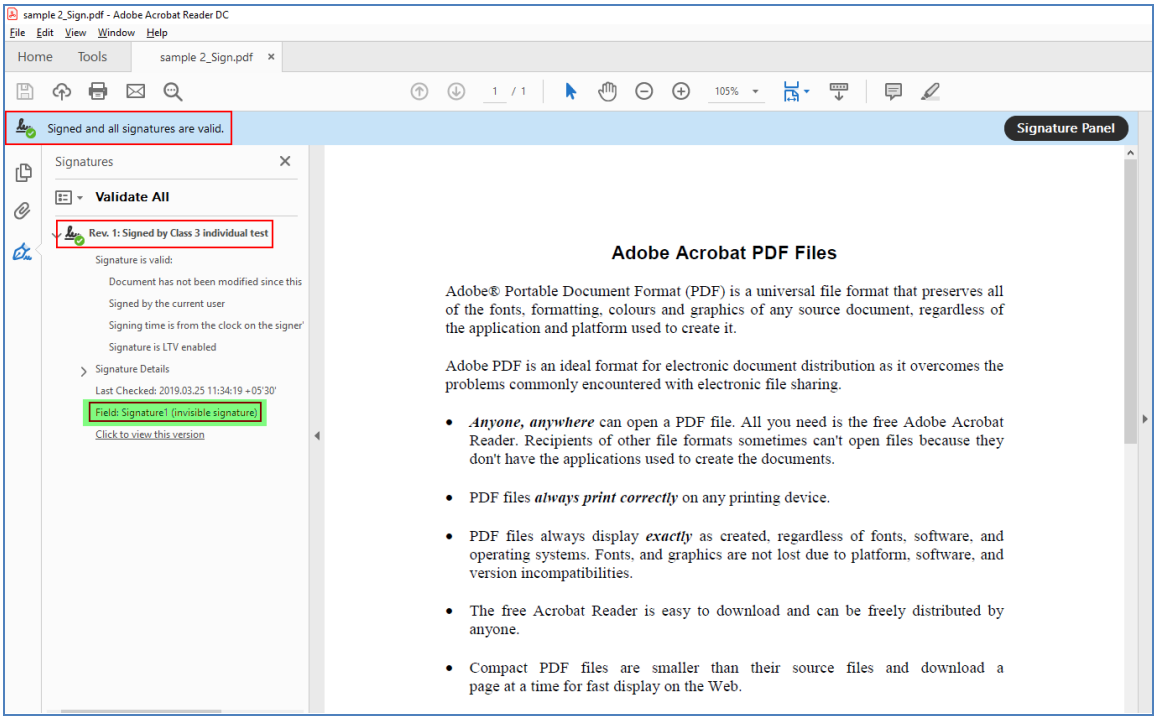

Fig.4

Capture Co-ordinates: This option is to place the signature image at the location selected by the signer.

To capture the sign, steps are:

- Click **Capture Co-ordinate** (Capture Co-ordinate) button, the document with first page will appear, as shown in **Fig.5.**
- Enter the **Page Number** where the user wants to put up the signature **(Fig.5)**.
- Click **Display (Display)** button, the selected page will appear.
- Click **Capture** (Capture) button and place the cursor; draw a virtual **L-shape** at the user preferred location.
- Then, click **Back** (Back) button, as shown in **Fig.5**:

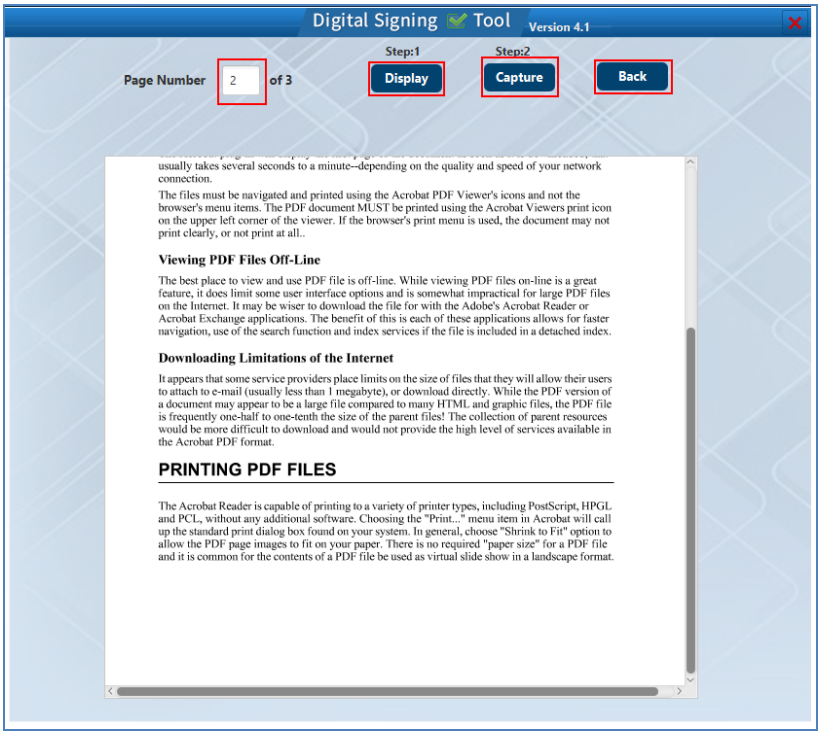

Fig.5

- Click **Apply Signature** (Apply Signature) button as shown in the **Fig.6**:

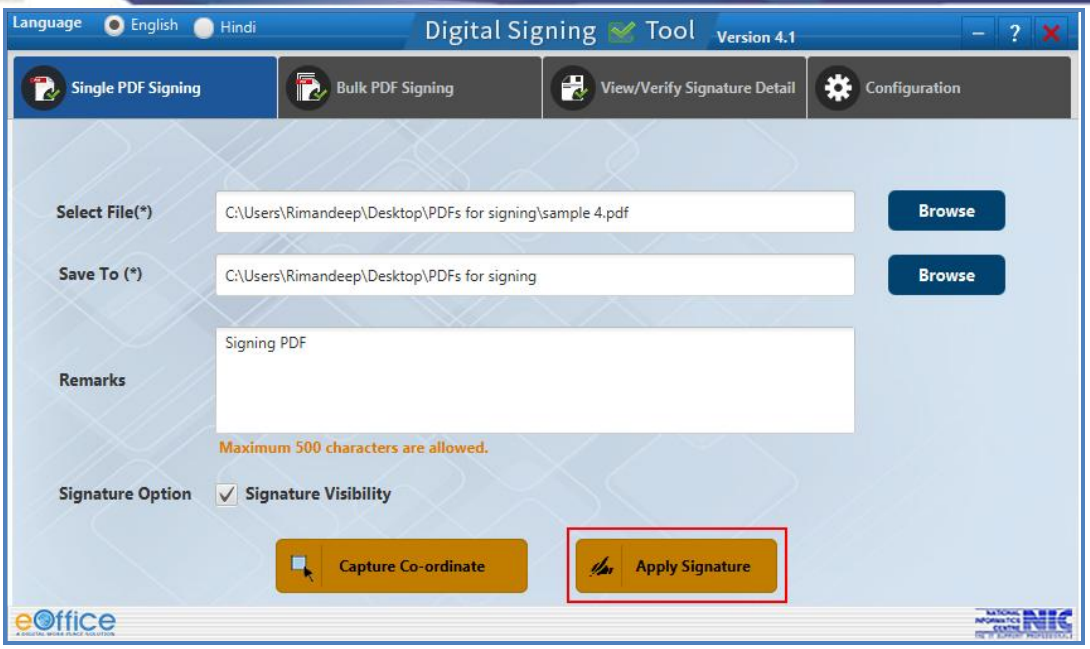

Fig.6

- Select the certificate and click **Ok** (OK) button as shown in **Fig.7.**

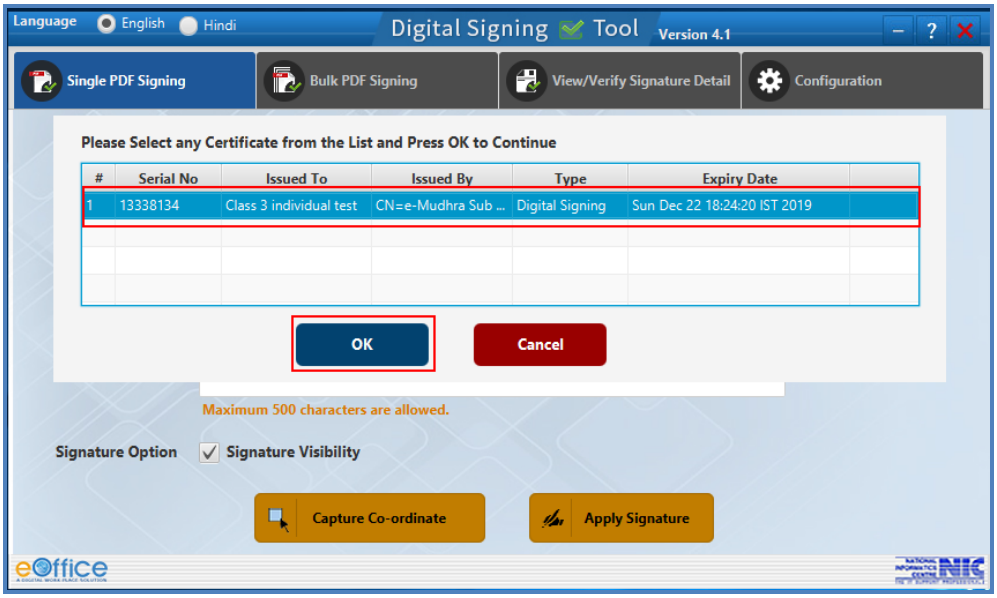

Fig.7

- Verify User PIN window appears, enter the PIN and click **Login** (Login) button as shown in **Fig.8:**

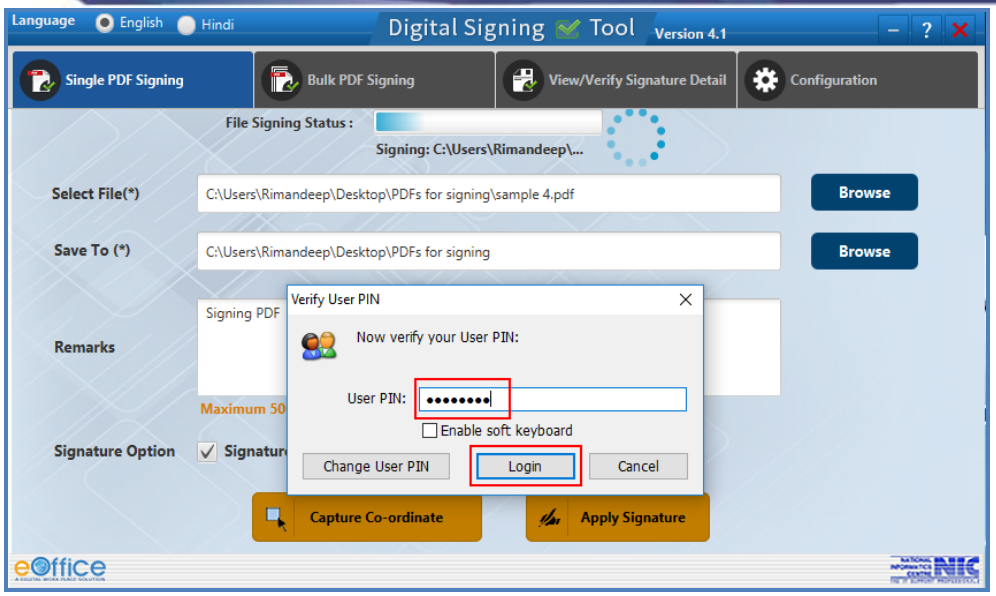

Fig.8

- The document will be signed successfully, provided with the path of the signed file as shown in **Fig.9:**

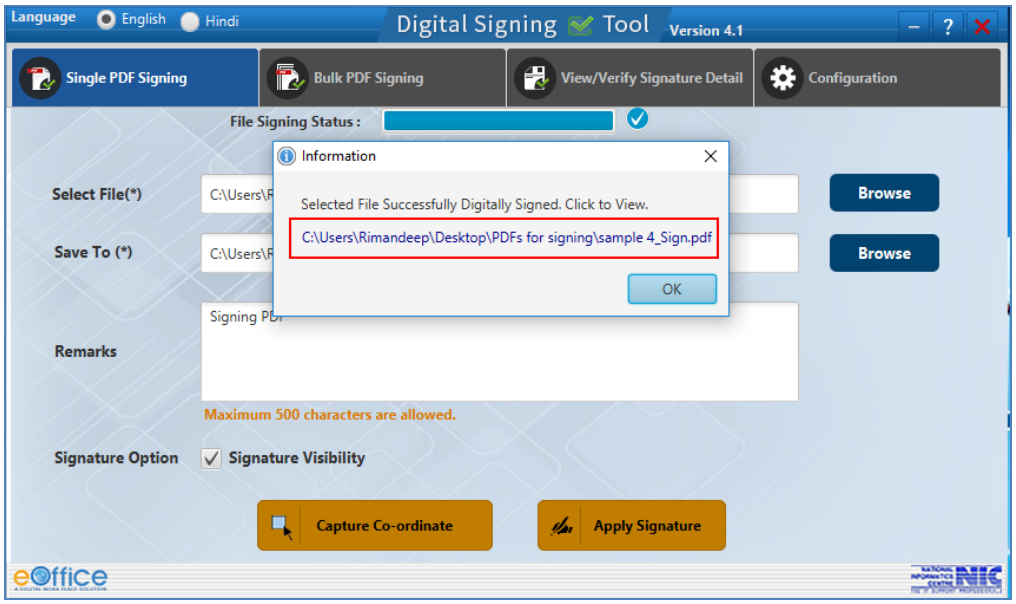

Fig.9

Note:

File names concatenated with "**_Sign**", states that file is successfully signed and saved.

- Click the path (**Fig.9**), the PDF will open with signature at the defined coordinates as shown in **Fig.10:**

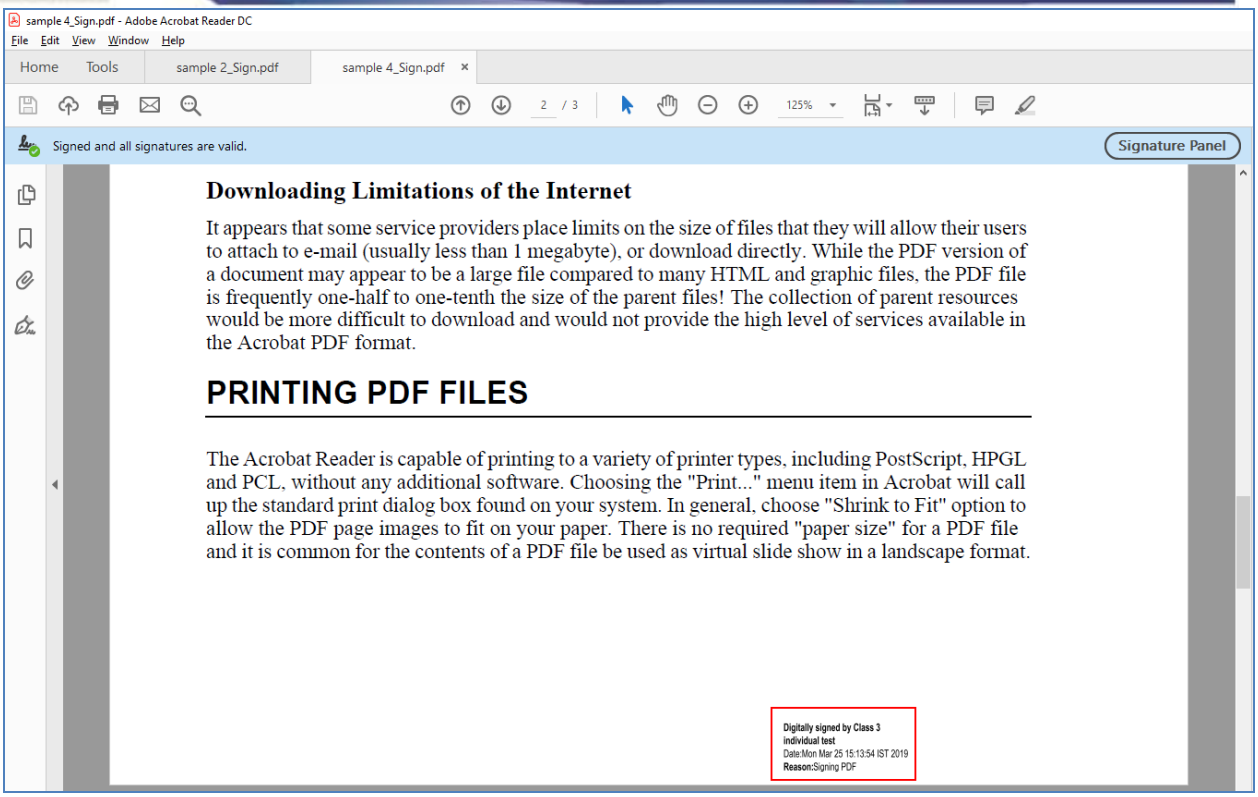

Fig.10

- By default, the signature appears at the bottom right corner of last page of the PDF file.
- The default alignment of the signature can be changed from the configuration tab (Refer **Configuration** section for detail).
- Signature details are being displayed along with the original content of the page, refer to **Fig.11:**

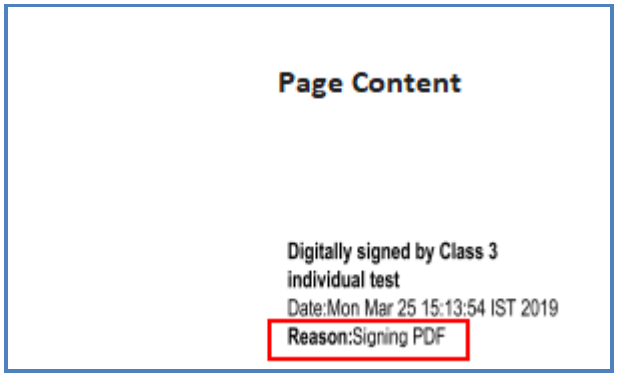

Fig.11

- The given Remarks appear as a **Reason** for the signature **(Fig.11)**.
- 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.12: Valid Signature**:

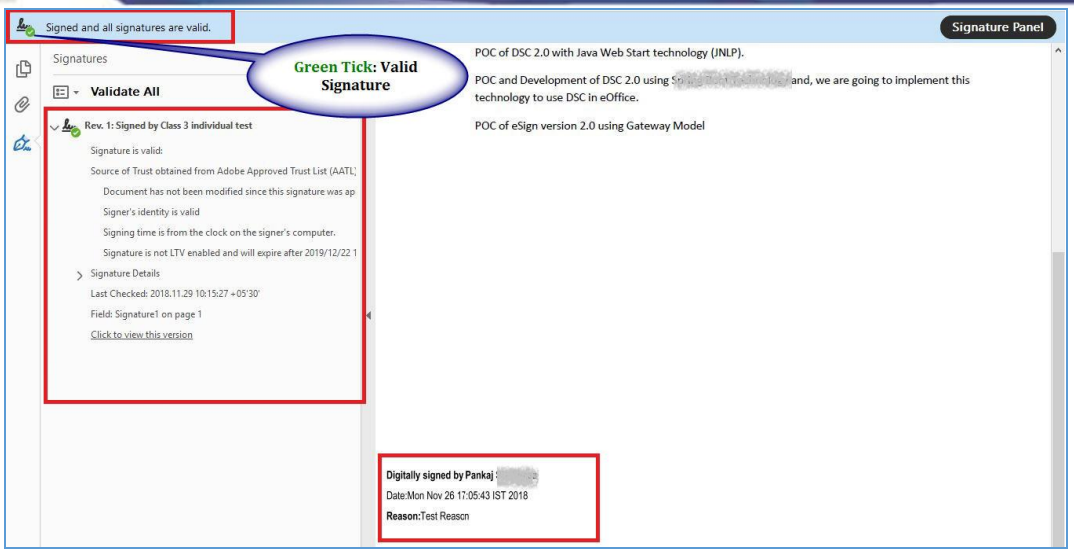

Fig.12: Valid Signature

- In case of **Invalid Signature**, **Red Cross sign** is displayed at upper left corner of adobe reader and inside signature panel itself.

Multiple Signatures on single PDF: More than one signer can put their digital signature on a previously digitally signed paper. Multiple signatures in a single document are shown in **Fig.13:**

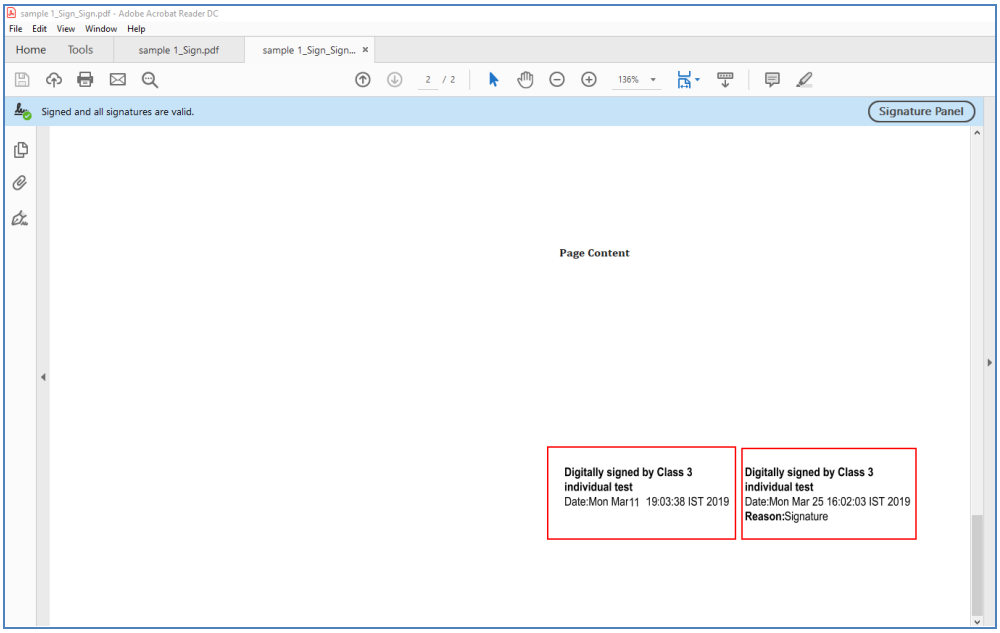

Fig.13

Bulk PDF Signing

This option is to sign more than one PDF in a single click. Further, a user can select the coordinates on single PDF and signatures will appear at the same location in all PDFs.

To sign in the bulk, steps are:

- Click **Bulk PDF Signing** tab, then click the **Browse** (Browse) button to select the folder for bulk signing as shown in **Fig.14.**
- By default, the application creates a folder naming **"BULK"** containing all the signed files. The destination of the signed documents folder will be same as the source location.
- Click **Browse (Browse)** button corresponding to "**Save To**" option to define the destination folder where the signed document will be saved, as shown in **Fig.14**.
- Add the remarks (if required) in **Remarks** field as shown in **Fig.14:**

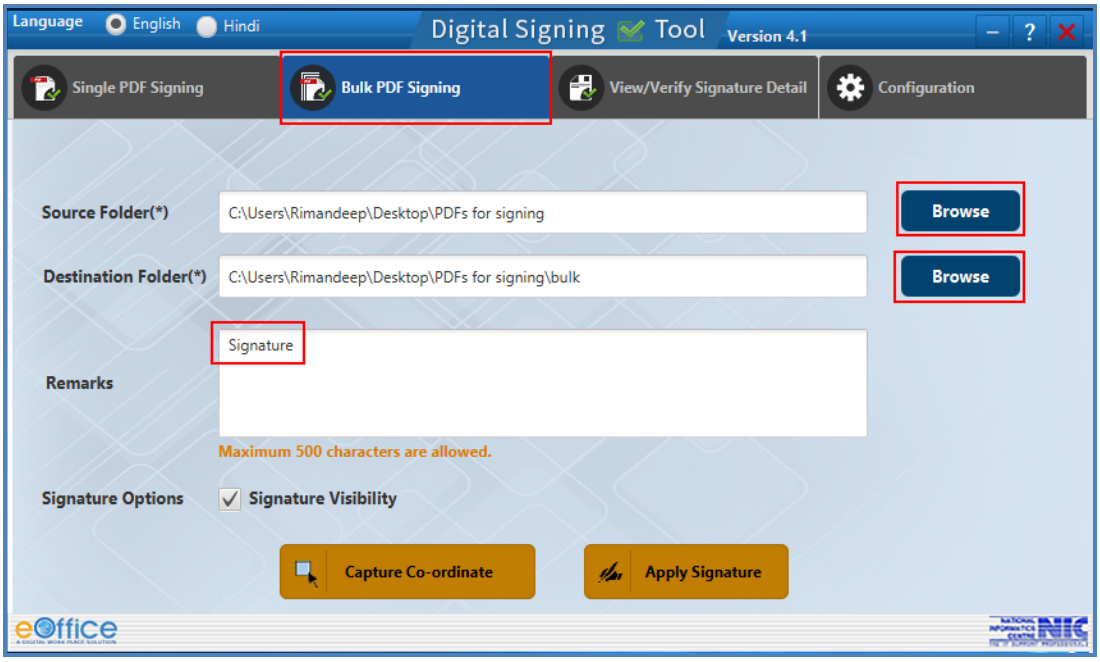

Fig.14

- Further, [Signature Visibility](), [Capture co-ordinate]() **and** [Signing]() steps are same as mentioned in **Single PDF Signing** section.

Note:

For capturing co-ordinates in bulk signing, the folder documents should have same structure/layout to attain uniformity in all documents.

View/Verify Signature Detail

It consists of two sections, the

1. First section allows a user to view the details and verify the signature of a single signed document.
2. Second section is for documents signed in bulk and it only verifies signature available in the bulk folder documents.

To view the details, steps are:

- Click **View/Verify Signature Detail** tab as shown in **Fig.15:**

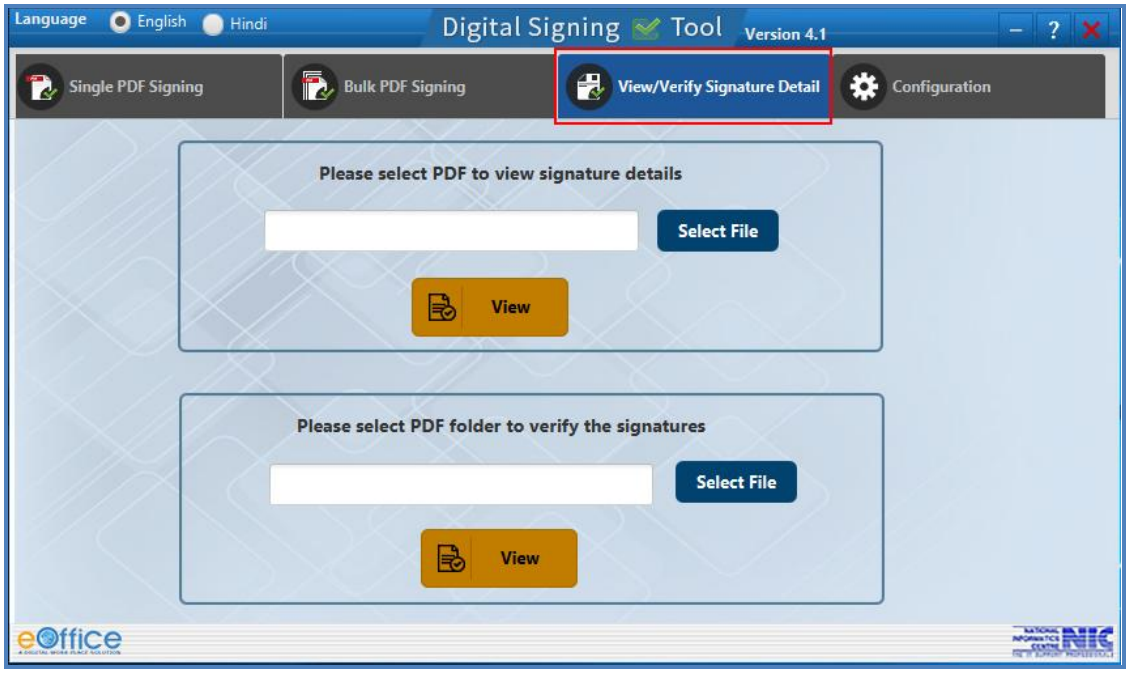

Fig.15

For Single Signed Document

- Click on **Select File (**  **)** button to upload the document.
- Click on **View (**  **)** button to view the details of the signature as shown in **Fig.16:**

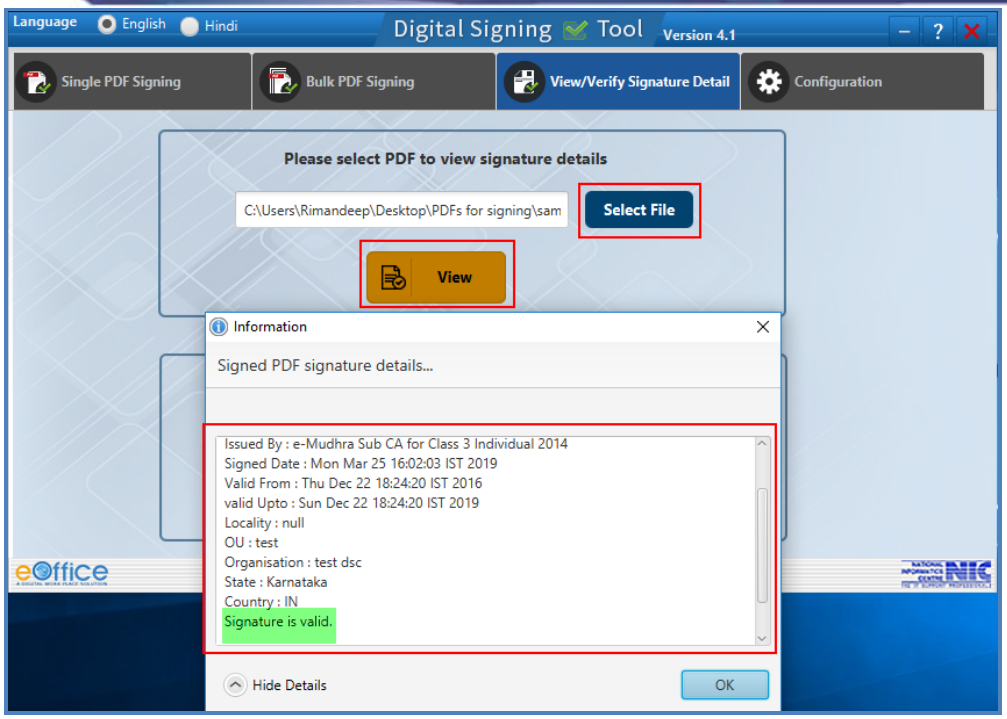

Fig.16

- **Information** screen appears, displaying PDF details and Signature validity **(Fig.16)**.

For Bulk Signed documents

- Click on **Select File (**  **)** button to upload the bulk documents from the folder.
- Click on **View (**  **)** button to verify the signature of the documents as shown in **Fig.17:**

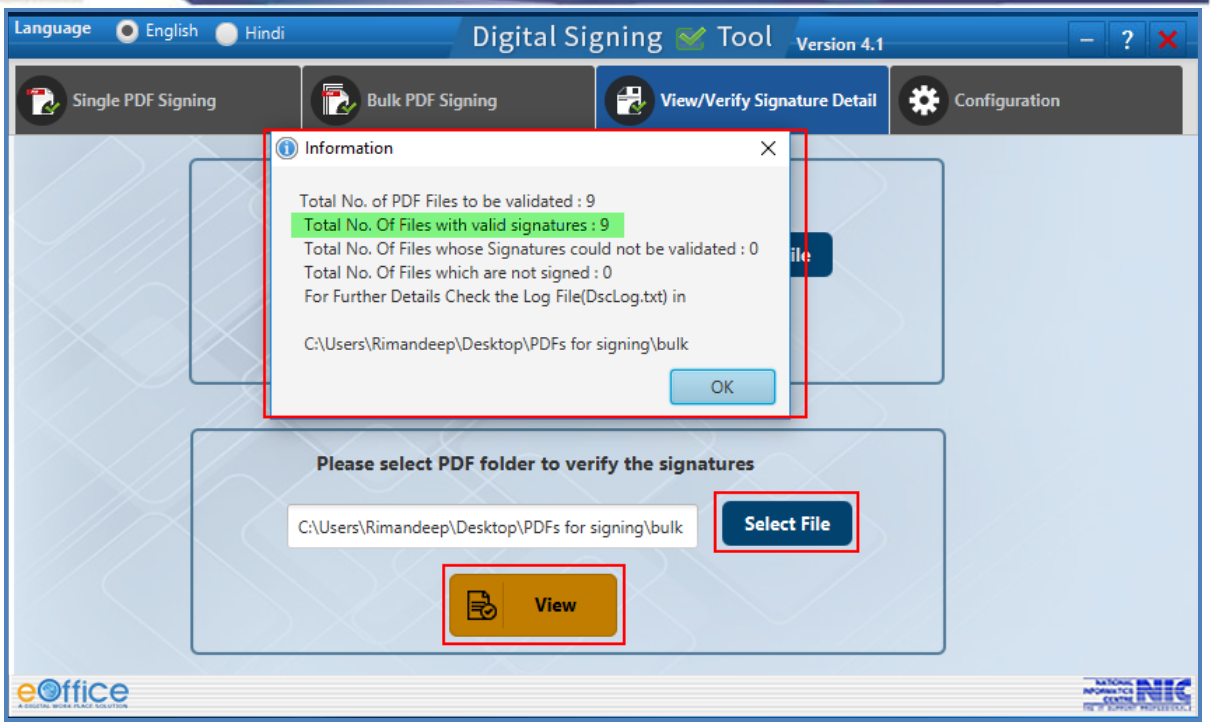

Fig.17

- **Information** screen appears, displaying consolidated detail of the PDF files with valid Signature **(Fig.17)**.
- Also, a file name "**DscLog**" is created inside the selected folder which contains more details.

Configuration

An interface to set a limit on:

1. maximum number of PDF files that can be signed in bulk signing.
2. maximum number of signatures that can be carried on a single PDF.
3. Signature Alignment (Left or Right).

To configure the settings, steps are:

- Enter the count to set the limit for bulk signing (below or equal to 5000), as shown in **Fig.18.**
- Enter the count to set the limit for signature(s) counts allowed on a single document (below or equal to 10), as shown in **Fig.18.**
- Select the radio button for **Left** or **Right** for the positioning of the signature, as shown in **Fig.18**.
- Click **Save (** Save **)** button, as shown in **Fig.18:**

Fig.18

- The application then continues with the settings saved.

Annexure-I

What is Revocation?

When a certificate is issued it is expected to be in use for its entire validity period. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include a change of name, change of association between subject and CA (e.g. an employee terminates employment with an organization), and compromise or suspected compromise of the corresponding private key. Under such circumstances, the CA needs to revoke the certificate.

Certificate revocation list (CRL)

X.509 standard certificates are used in many internet protocols and offline applications, for e.g electronic signatures. X.509 defines one method of certificate revocation. This method involves each Certificate Authority (CA) periodically issuing a signed data structure called certificate revocation list (CRL).

A CRL is a time stamped list identifying revoked certificates which are signed by a CA or CRL issuer and made freely available in a public repository. Each revoked certificate is identified in a CRL by its certificate serial number. When a certificate-using system uses a certificate (e.g. for verifying a remote user's digital signature), that system not only checks the certificate signature and validity but also acquires a suitably-recent CRL and checks that the certificate serial number is not on that CRL. The meaning of "suitably-recent" may vary with local policy, but it usually means the most recently-issued CRL.

A new CRL is issued on a regular periodic basis (e.g., hourly, daily,or weekly). An entry is added to the CRL as part of the next update following notification of revocation. An entry MUST NOT be removed from the CRL until it appears on one regularly scheduled CRL issued beyond the revoked certificate's validity period.

Importance of CRL

Certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore should not be relied upon.

Digital Signing Tool (DST) uses Digital Signature Certificate (DSC) for authentication and signing of the content before sending the file to any other user. The validity of DSC requires to be checked before using it.

The following checks must be done.

a) Validate that the certificate is used by the intended user(registered) only.
b) Validate that the certificate should not be expired.
c) Validate that it must be issued by trusted CA.
d) Validate that the certificate must not have been revoked for any reason.

Annexure-II

Process to Validate a Signature on a Digitally Signed Document

Validating Digital Signatures in Adobe

Every digital certificate is issued by a Root CA (Certification Authority). By default, some of the Root CA's are included in Windows Certificate Store (Trusted Root Certification Authorities) and few are included in Adobe Certificate Store. Microsoft and Adobe use different certificate stores and validation procedures.

If the signing certificate (or the Root CA that issued the signing certificate) is not included in Adobe Store, the digital signature is considered as "not trusted". Sometimes when the user opens a document with Adobe Reader the signature shows "**At least one signature requires validating**" at upper left corner of adobe reader as shown in the **Fig.A.2.1:**

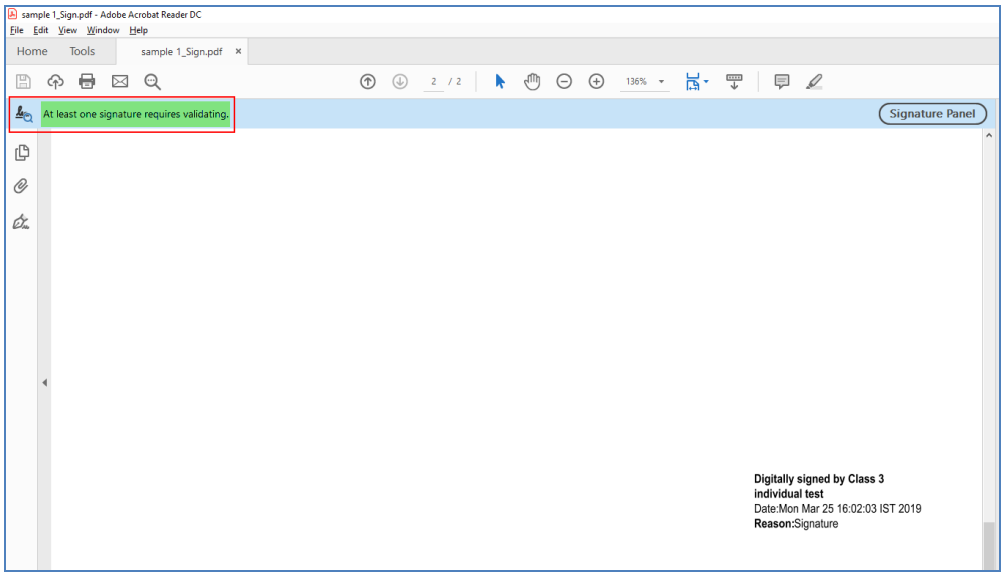

Fig.A.2.1

This behavior has nothing to do with the signing engine but with the Adobe Certification validation procedure.

To trust a signature the user must add the signing certificate on the Adobe certificate store because only a few Root CA's are trusted by default Adobe certificate validation engine.

How to Validate the Signature:

It will be done in the following steps.

1. Install Root Certification (One-time): This is a one-time activity that the user must perform on his computer in which user is validating signed PDF files.

2. Enable Windows Trust for Verification (One-time): This is a one-time activity that the user must perform on his computer to integrate Adobe Reader with Windows Certificate Store.
3. Validate: The viewer will verify all the Digitally Signed PDF's.

Add the certificate manually to the Adobe Trusted Identities

- Click signature rectangle, **Signature Validation Status** window appears.
- Click Signature Properties (Signature Properties...) as shown in **Fig.A.2.2**:

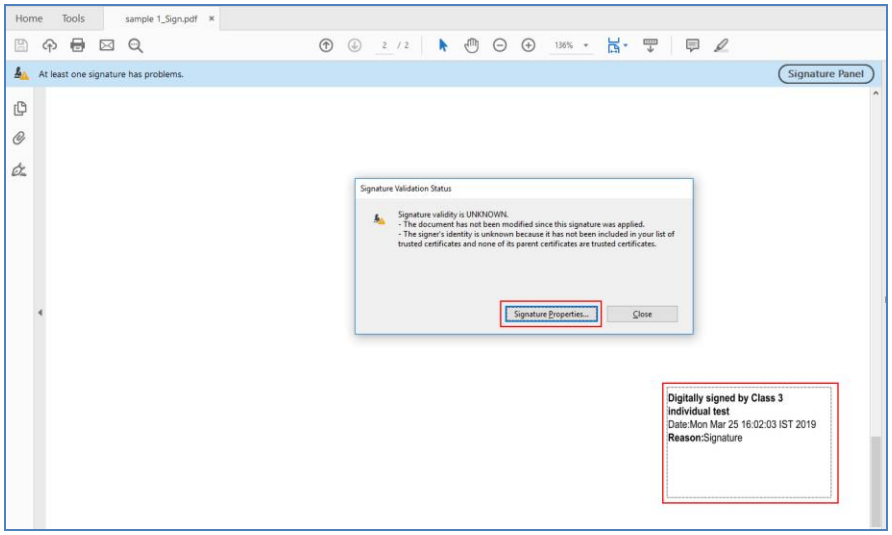

Fig.A.2.2

- Click **Show Signer's Certificate** (Show Signer's Certificate...) button, as shown in **Fig.A.2.3**:

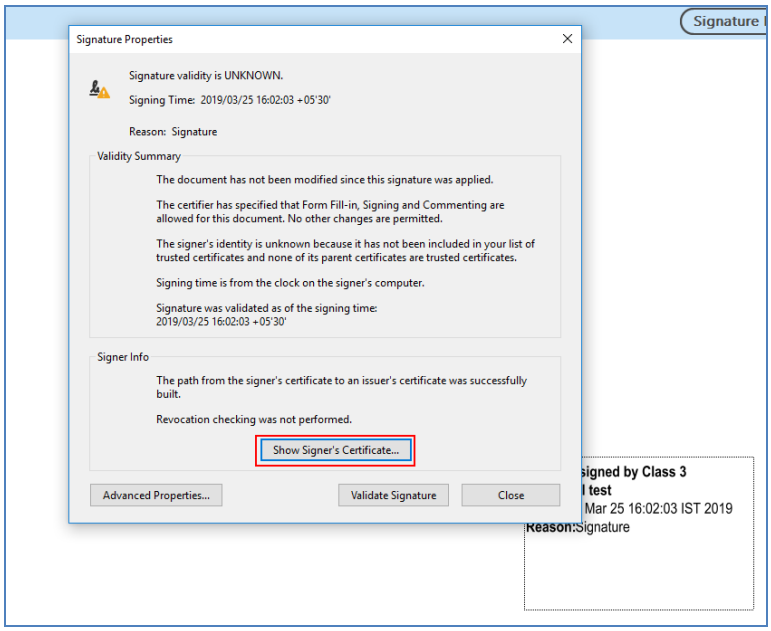

Fig.A.2.3

- Go to the **Trust** tab, click **Add to Trusted Certificates (** Add to Trusted Certificates... **)** button, as shown in **Fig.A.2.4:**

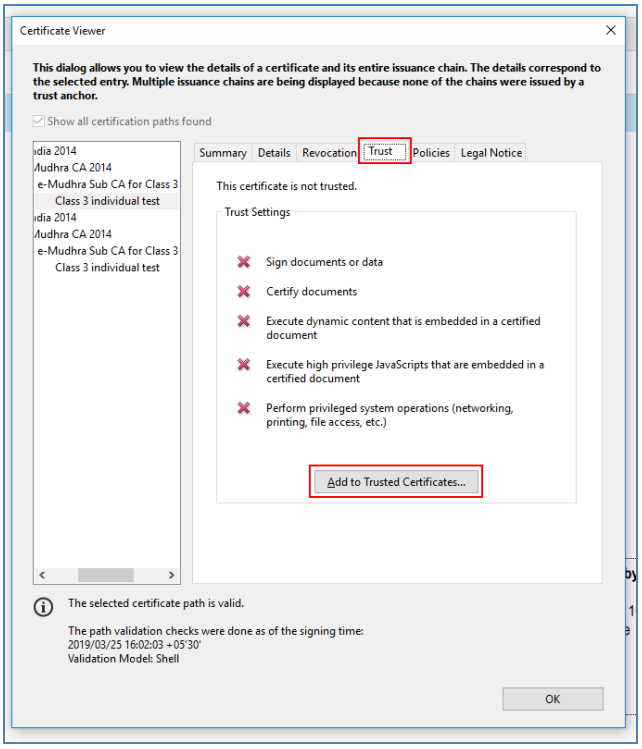

Fig.A.2.4

- **Acrobat Security alert** window appears, click on **OK (** OK **)** button to exit from the window box, as shown in **Fig.A.2.5:**

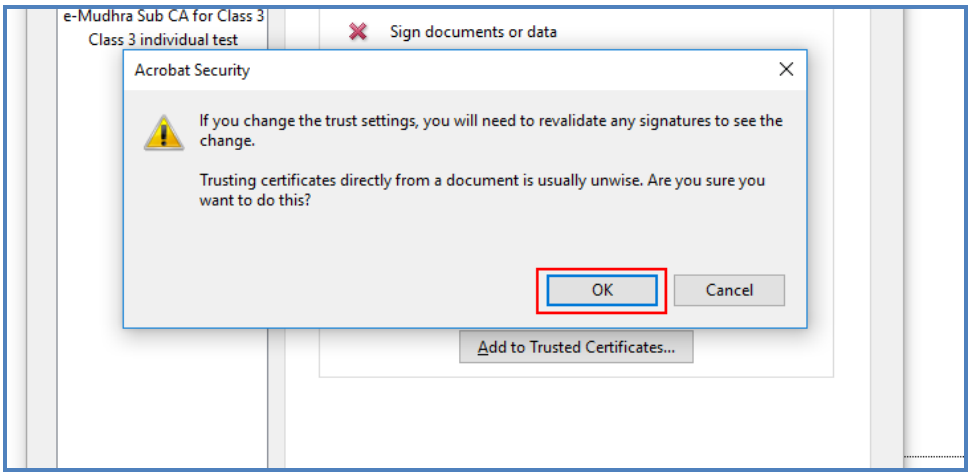

Fig.A.2.5

- **Import Contact Setting** window appears, check all the checkboxes and click on **OK (** OK **)** button to exit from the box, as shown in **Fig.A.2.6:**

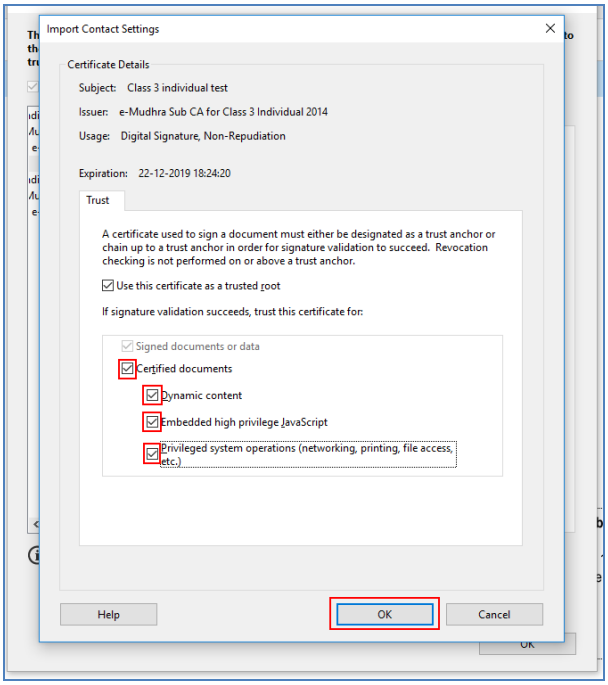

Fig.A.2.6

- Click **Validate Signature (** Validate Signature **)** button and close the window to exit from the box, as shown in **Fig.A.2.7:**

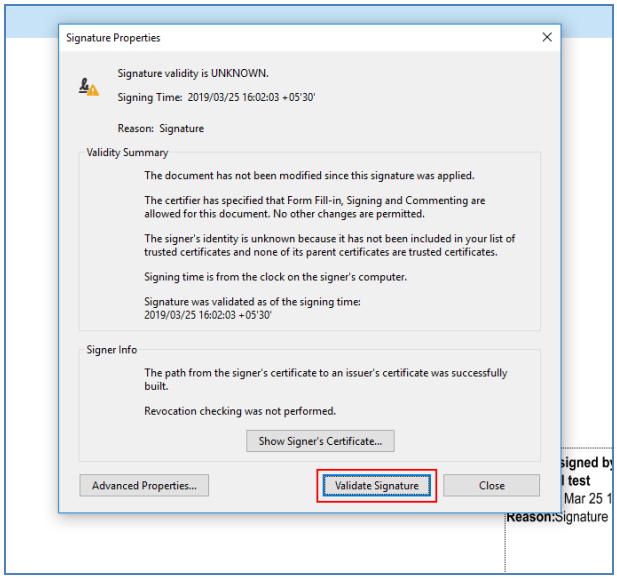

Fig.A.2.7

- The documents signed by this certificate are recognized as trusted.
- **Green Check** will be shown at upper left corner of adobe reader and also inside signature panel itself as shown in **Fig.A.2.8:**

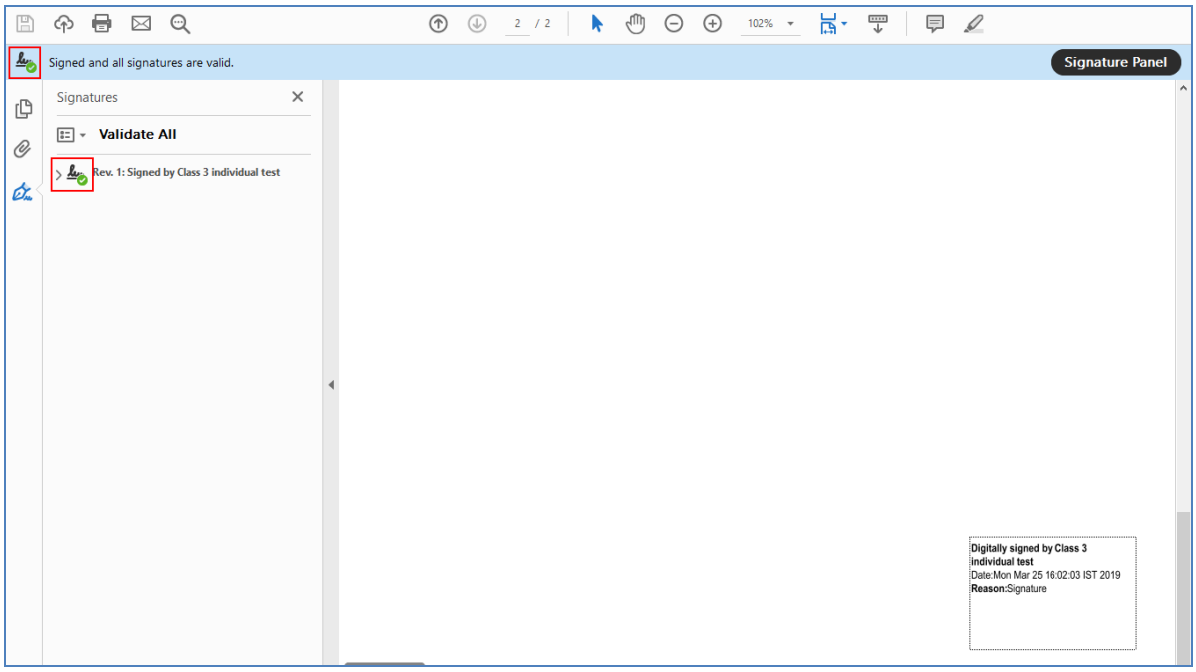

Fig.A.2.8

Annexure III

Troubleshooting (For DST)

Problem 1

Unable to download CRL files due to internet connectivity, CRL file not found at CA CDP location or the CA Site is not working.

Screen-shot

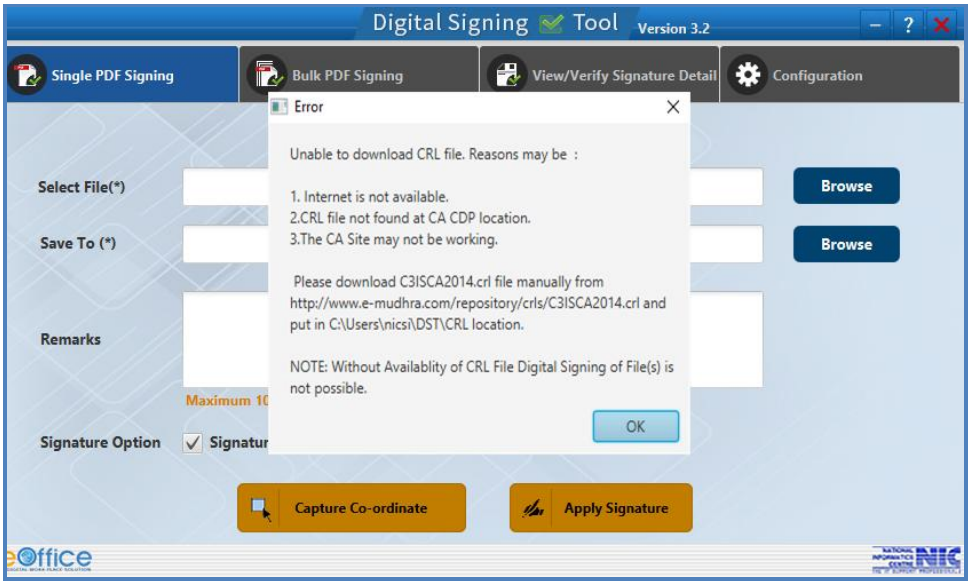

Fig.A.3.1

Solution

Download CRL file manually from the path mentioned in **Error** message and put in path: **\\HOME DIRECTORY \DST\CRL**.

Problem 2

Handshaking error: SSL certificate not found in Java KeyStore.

Solution

For Windows:

User needs to import the SSL certificate manually in java KeyStore and the steps are:

- E.g. Error message: "**https://www.ncodesolutions.com/repository/ncodeca14.crl**"
- Then, user need to import the SSL certificate for CA site: "**https://www.ncode.in/**"
- Click the **Padlock** icon and the, click **Certificate (valid)** link as shown in **Fig.A.3.2**:

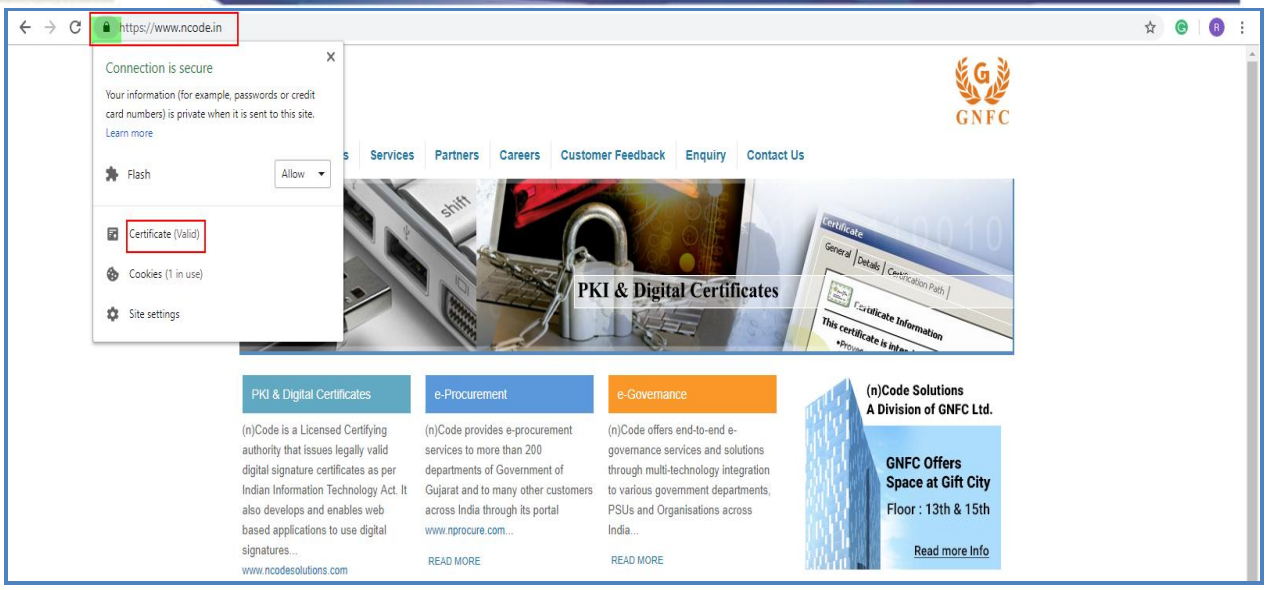

Fig.A.3.2

- Certificate window appears, click **Details** (Details) tab. Click copy to File (Copy to File...) button, as shown in **Fig.A.3.3:**

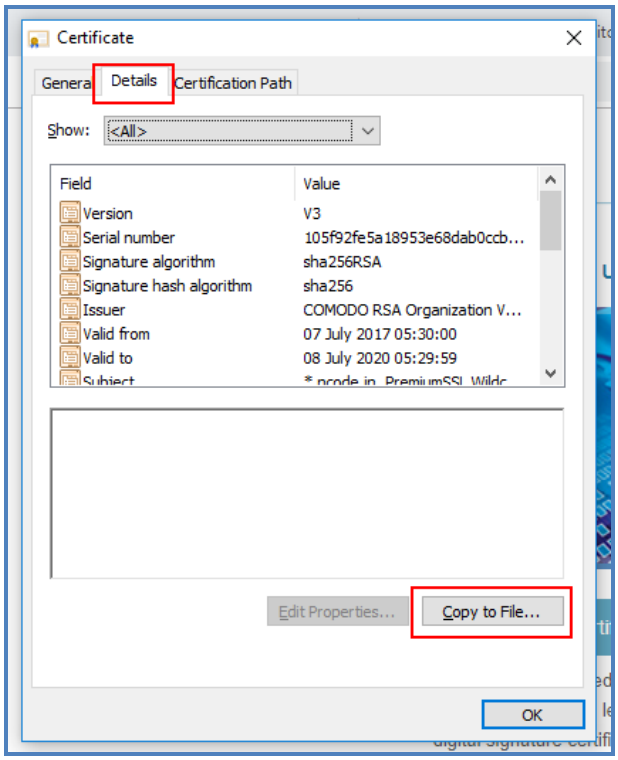

Fig.A.3.3

- **Certificate Export Wizard** window appears, click **Next** (Next) button, **Fig.A.3.4**:

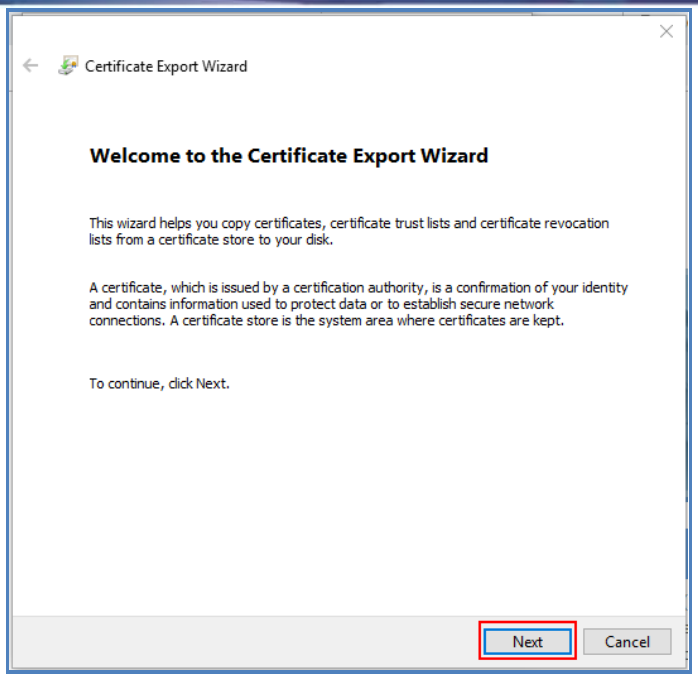

Fig.A.3.4

- Again, click **Next** (Next) button, **Fig.A.3.5:**

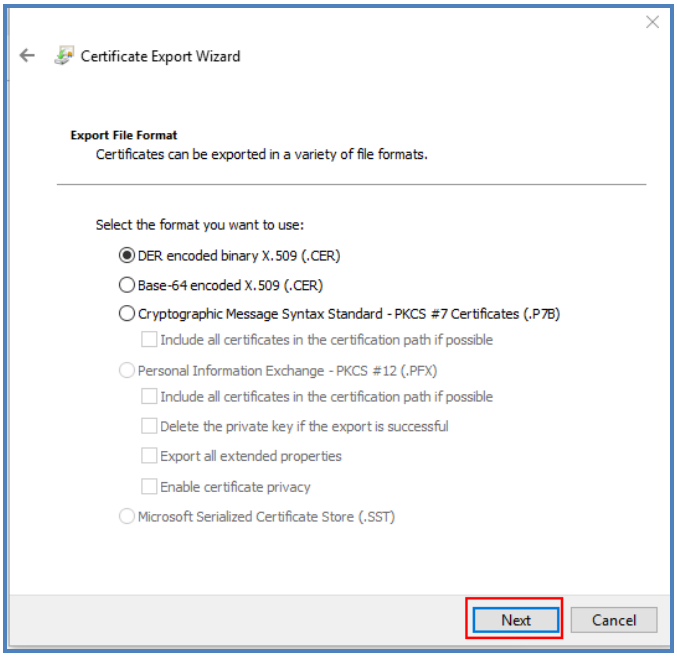

Fig.A.3.5

- Click **Browse (**Browse...**)** button to define the destination to save the certificate and click **Next** (Next) button, as shown in **Fig.A.3.6**:

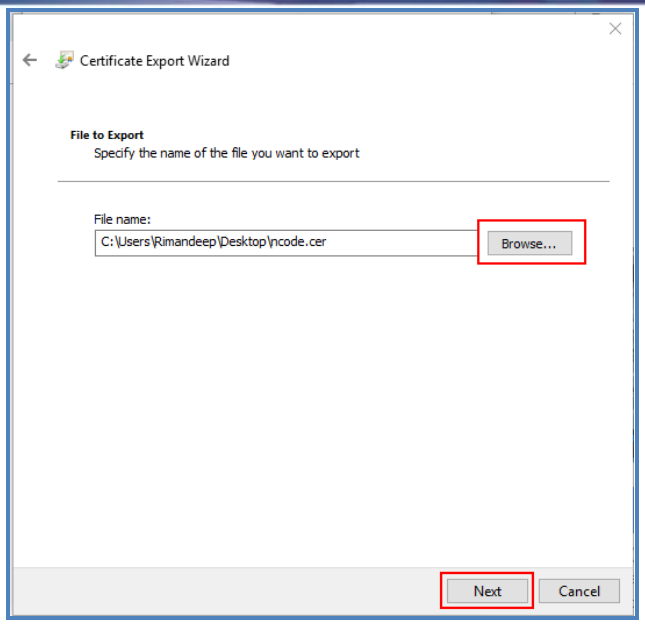

Fig.A.3.6

- Click **Finish** (Finish) button, as shown in **Fig.A.3.7**:

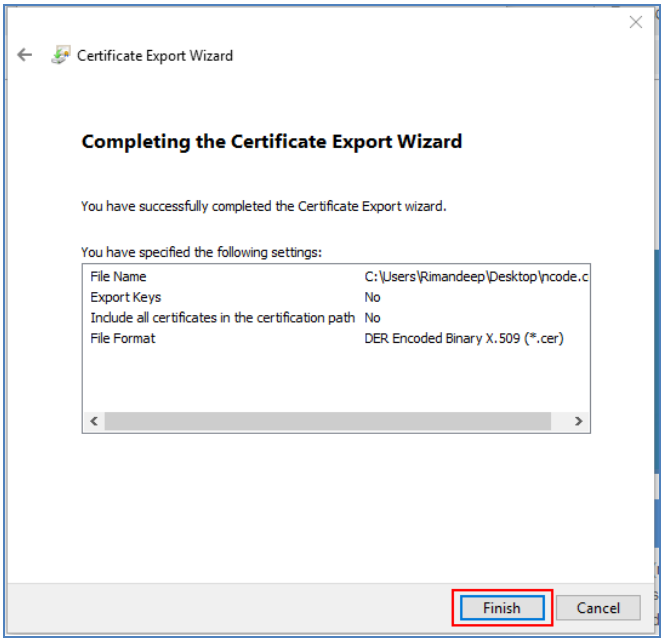

Fig.A.3.7

- A message prompts "**The export was successful**", as shown in **Fig.A.3.8**:

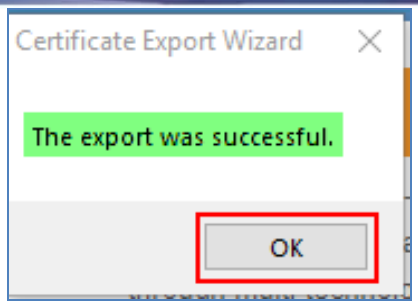

Fig.A.3.8

- Open PowerShell or cmd, enter the command ***<JAVA_HOME>/jre\lib\security> keytool -import -alias alias -keystore cacerts –file <ncode certificate location>,*** as shown in **Fig.A.3.9** and **Password**: ***"changeit"***.

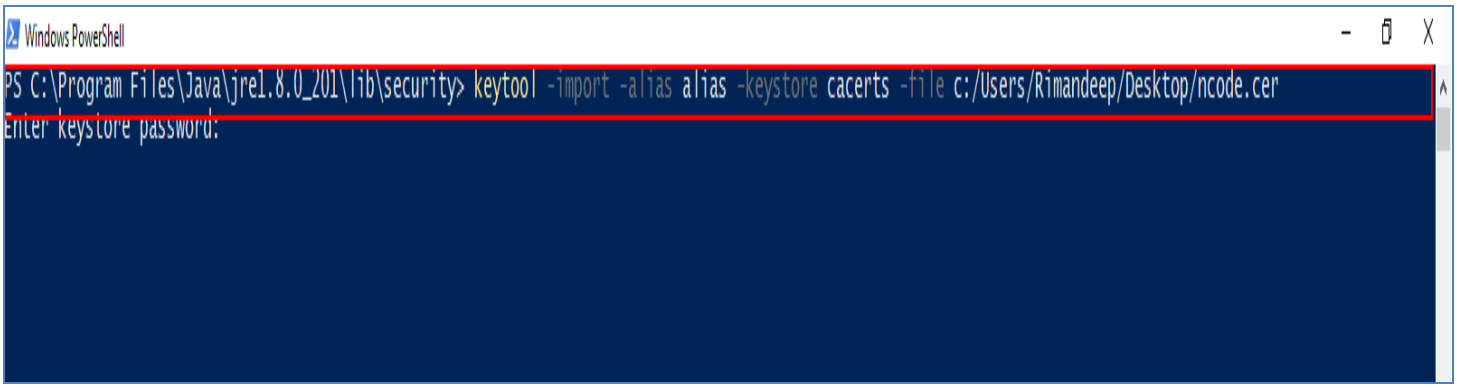

Fig.A.3.9

- Type **'Yes'** to import the SSL certificate, otherwise type **'No'** for terminating the process, as sown in **Fig.A.3.10**:

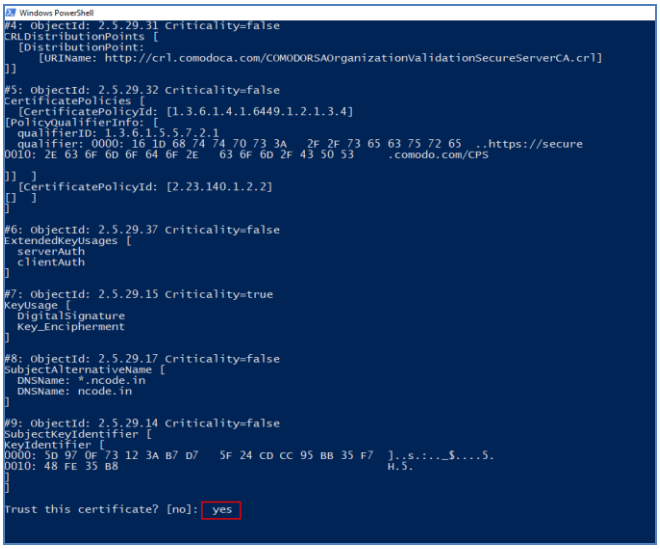

Fig.A.3.10

- A message prompts "**Certificate was added to keystore**", shown in **Fig.A.3.11**:

```
#9: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 5D 97 0F 73 12 3A B7 D7   5F 24 CD CC 95 BB 35 F7  ]..s.:.._$....5.
0010: 48 FE 35 B8                                        H.5.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Fig.A.3.11

Annexure IV

DSC Pin Management in prevalent dongles today

User PIN is the password which the digital signature (DSC application) subscriber uses while doing a digital signature using token. User **PIN** is important to be kept confidential and should not be disclosed to anyone.

For signing a document digitally, user needs to enter the DSC PIN every time. Also, in the case of the multiple files, user has to enter a PIN for each file. To avoid the situation of entering the pin multiple time DSC token driver has a feature to store the User PIN for that particular session, resulting user will enter the PIN once for signing the first file and after that, it will not ask for the PIN.

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

Follow the below instruction to maintain the Pin session:

DISCLAIMER

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

ProxKey Token-session Management

Steps to maintain the Pin session for ProxKey Token:

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

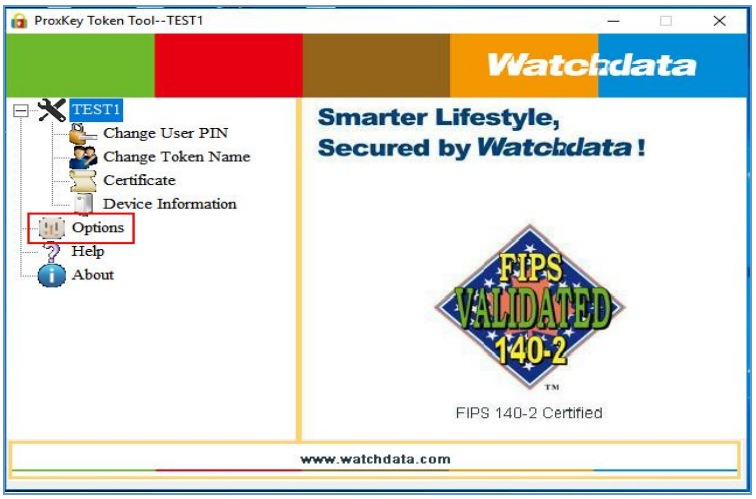

Fig.A.4.1

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

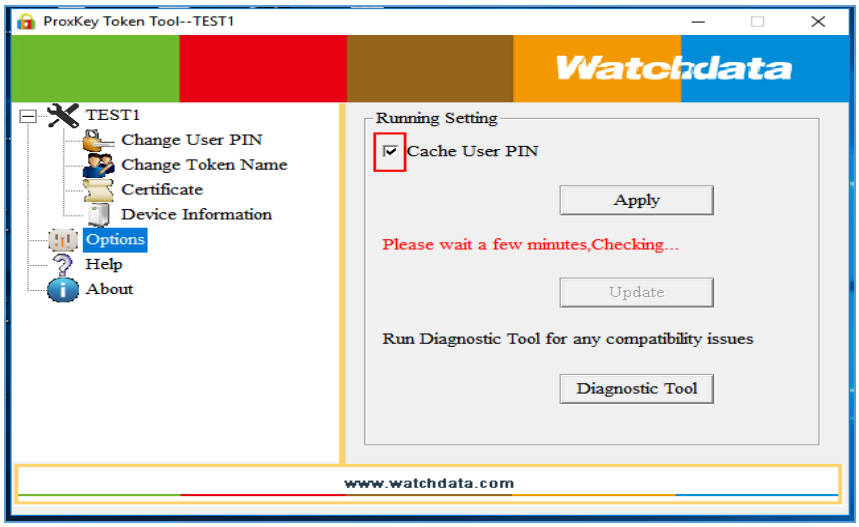

Fig.A.4.2

ePass Token Session Management

Steps to maintain the Pin session for ePass Token:

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

Fig.A.4.3

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

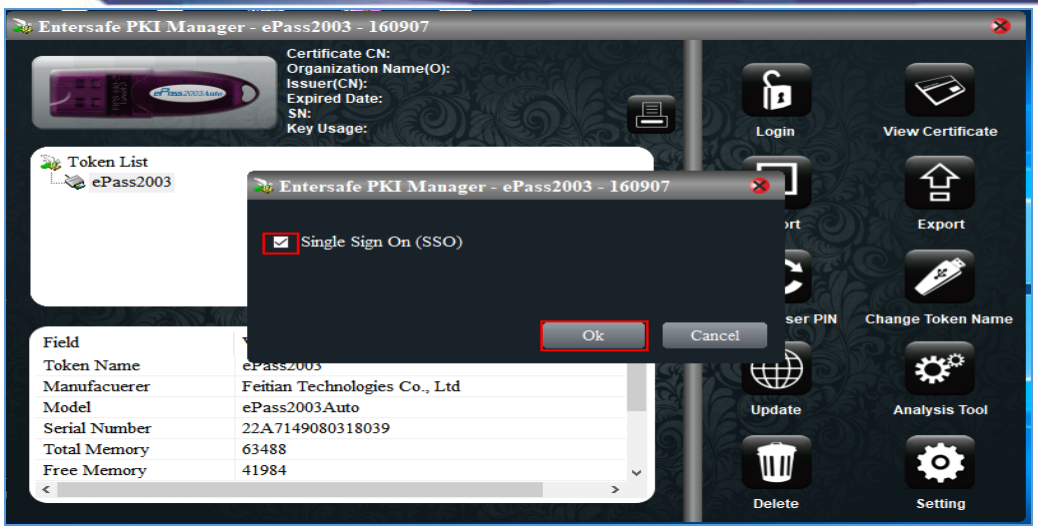

Fig.A.4.4

Session Time limit setting (For ePass Token)

User can also set time out session of DSC 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**

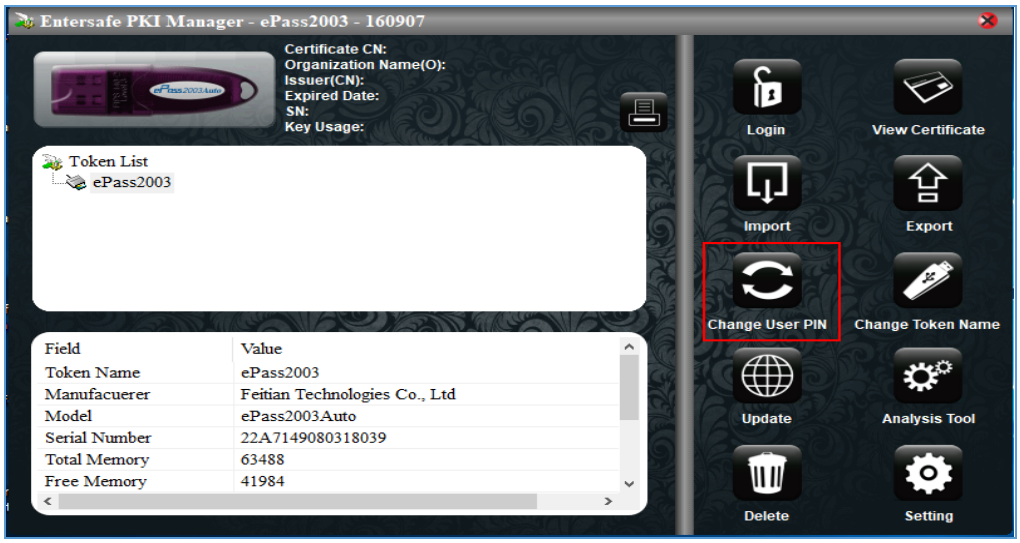

Fig.A.4.5

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

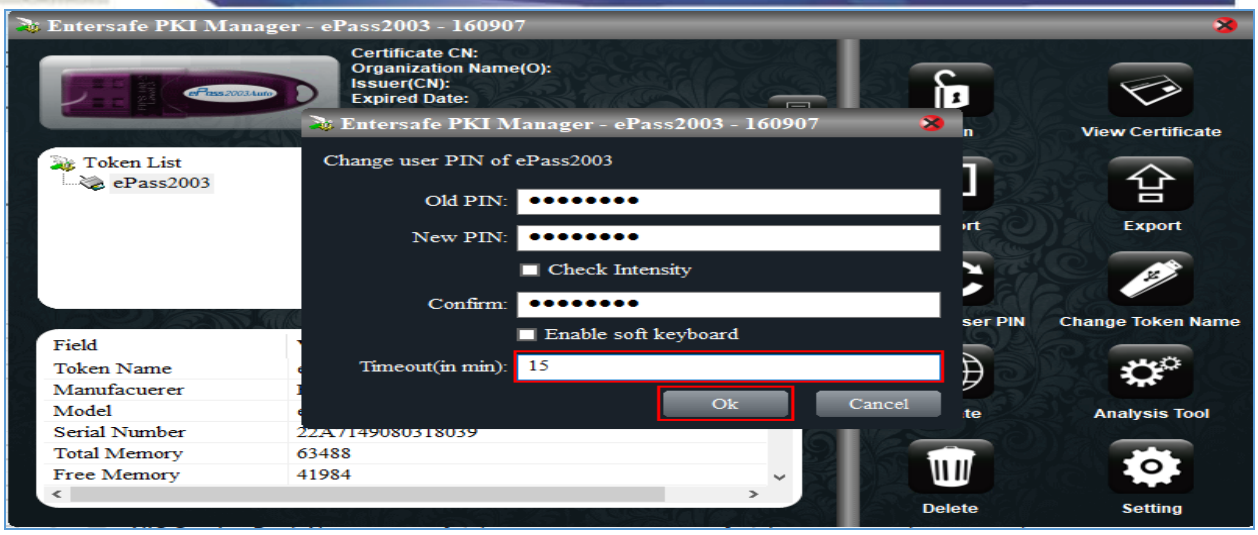

Fig.A.4.6

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**

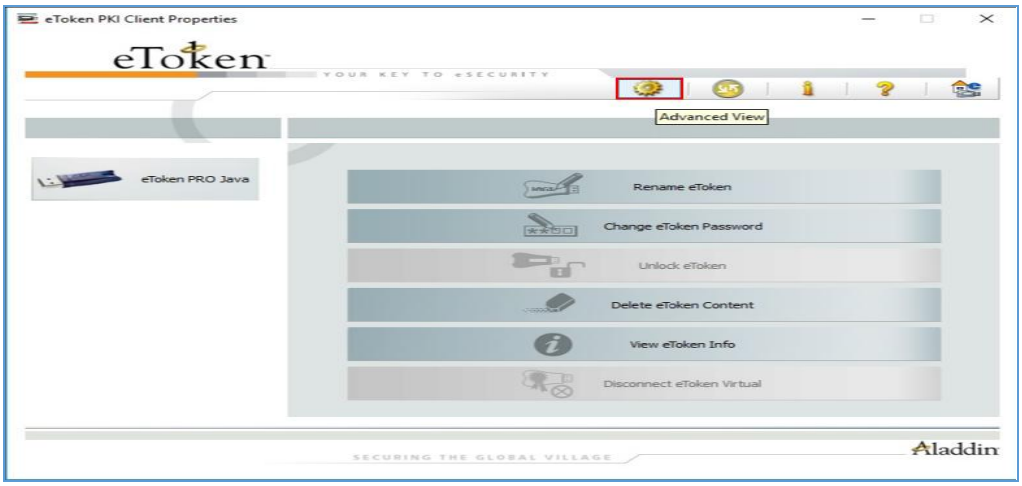

Fig.A.4.7

3. Click eToken PKI client Settings and then click Advanced (Advanced) tab as shown in **Fig.A.4.8:**

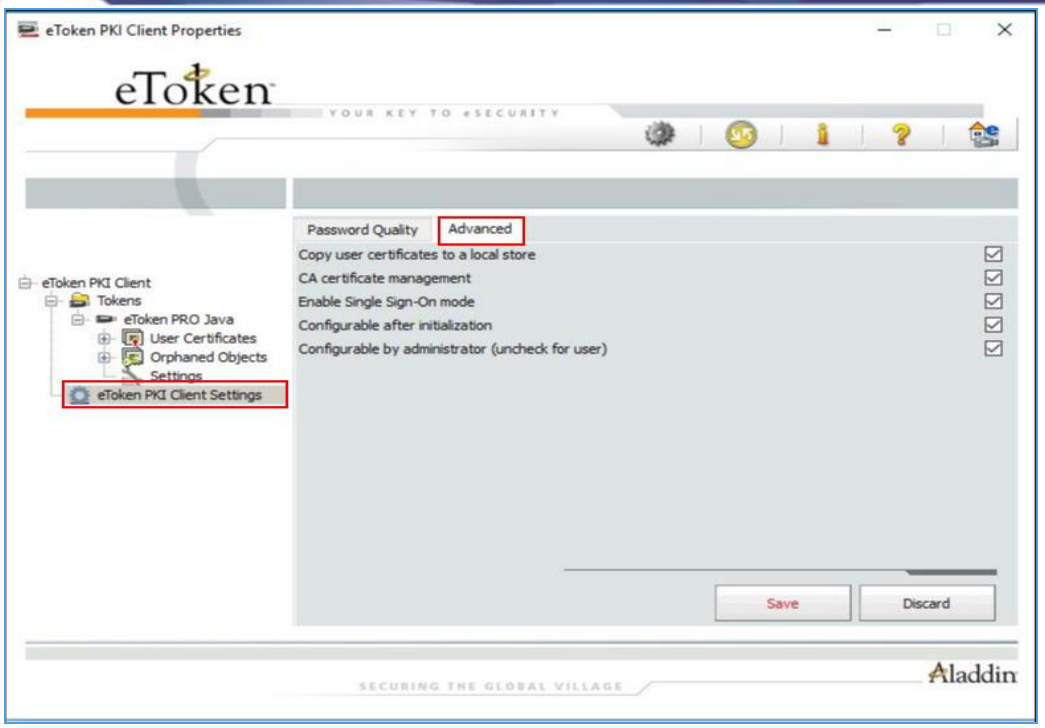

Fig.A.4.8

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

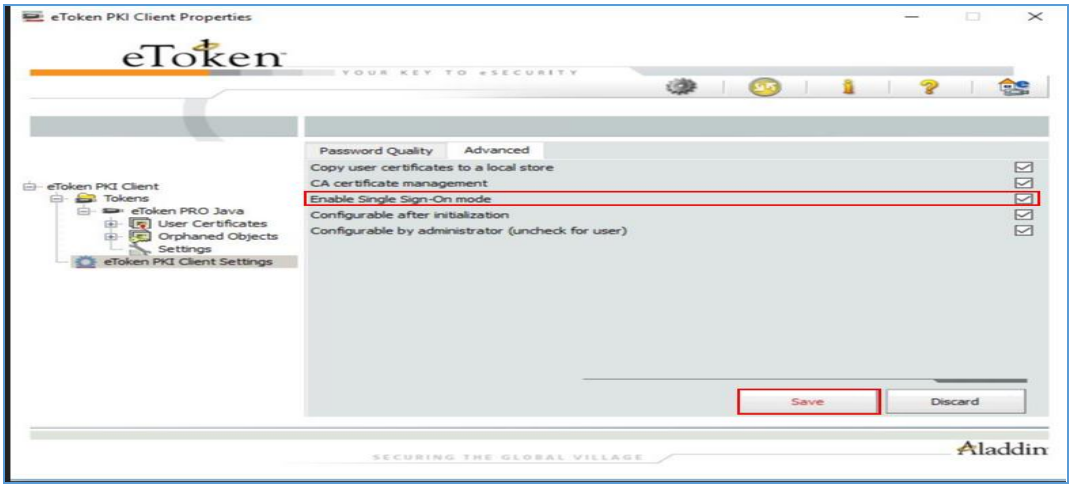

Fig.A.4.9

Annexure V

Brief Technical Description

The tool uses Java FX, JCA and requires Java 8 on the client machines. It will be supported on Windows, Linux and MAC clients that have Java 8.

Created By
Shalini Baluni
Pankaj Shakya
Rohit Kumar Singh
Rimandeep Kaur

Reviewed By
Navneet Kaur

Approved By
Kapil Kumar Sharma

eOffice Project Divison

National Informatics Centre

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