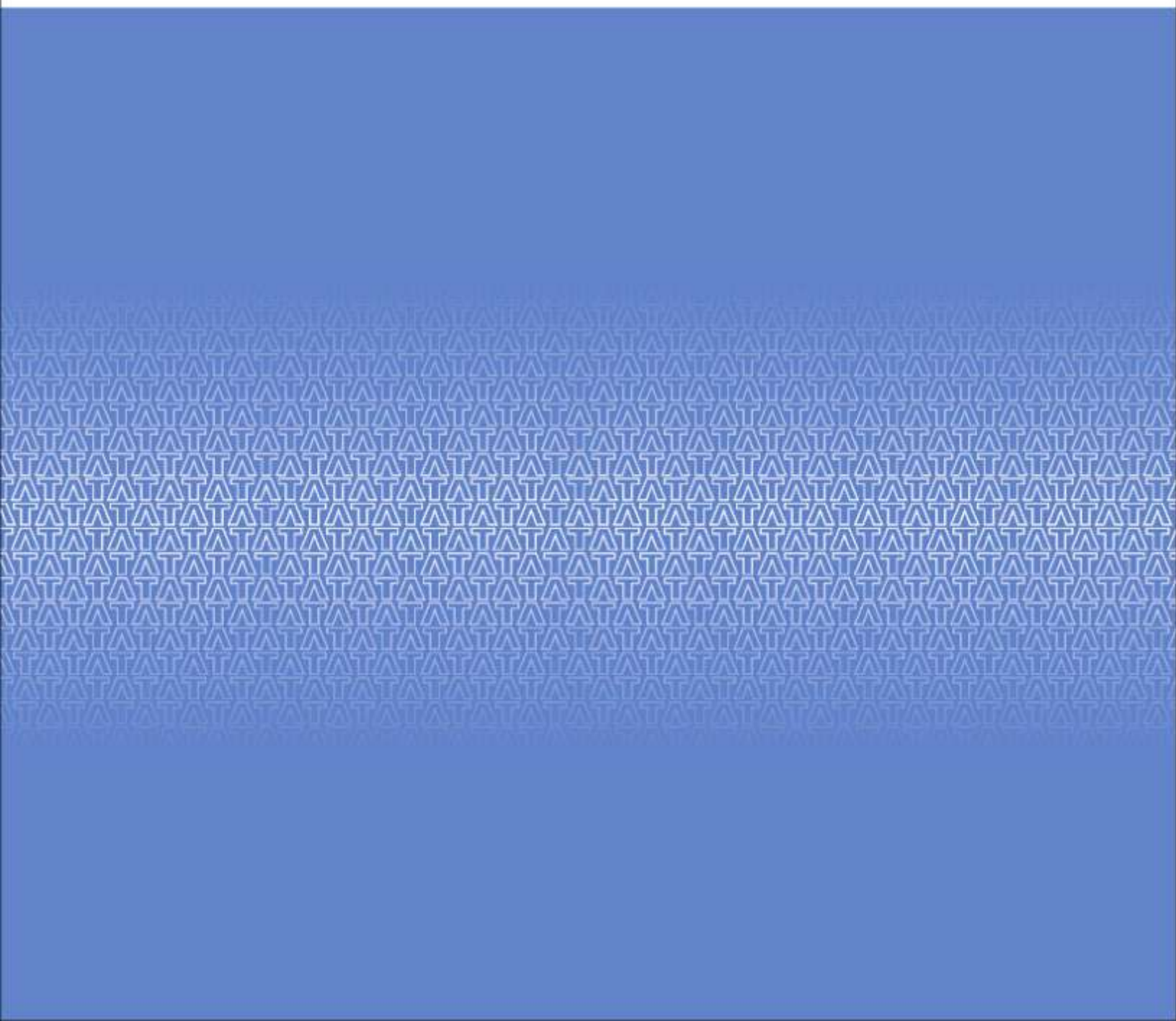
TATA CONSULTANCY SERVICES

Experience certainty. IT Services
Business Solutions
Outsourcing

TATA

FILESIGNER® PLUS V7.3.1

USER GUIDE



CONTENTS

1 GETTING STARTED

1.1 INSTALLING FILESIGNER® PLUS

The installation procedure for FileSigner® Plus is straightforward:

- Double click FileSigner® Plus Setup.
- Click on Next to install the software.
- By default, software will be installed under "C:\Program Files". It is the user wish to install the software under any drive by creating a folder with the folder name "FileSigner Plus".

1.2 SYSTEM REQUIREMENTS

To install and use FileSigner® Plus, the following are the system requirements:

- Processor: Pentium IV (recommended)
- Memory: 1GB RAM (recommended)
- Browser: IE 7.x or above
- Operating System: Windows XP SP3 or above
- 32-bit JRE 1.6.0 update 29 or above
- Admin Rights

For signing files, you will need a Digital Certificate issued by a licensed certifying authority such as Tata Consultancy Services – Certifying Authority (TCS-CA).

Visit http://www.tcs-ca.tcs.co.in to learn more about TCS-CA Digital Certificates.

2 ABOUT FILESIGNER® PLUS

2.1 ABOUT FILESIGNER® PLUS

FileSigner® Plus is a desktop utility designed to provide a simple interface for digital signing/verification of electronic documents. It includes:

- Configuration Manager
- FileSigner® Plus Wizard
- FileVerifier™ Plus Wizard

2.2 CONFIGURATION MANAGER

The Configuration Manager module allows you to configure FileSigner® Plus according to your specific needs and preferences. Using this, you can:

- Set a default location for source file(s) on which security operations are to be performed.
- Set a default location for the file(s) produced as a result of performing security operations.
- Enable/Disable the wizard introduction screens.
- Select signature formats.

2.3 PROFILE MANAGER

The Profile Manager can be used for creating profiles for Sign operation. These profiles contain the settings required for the sign operation. Once a Profile is created the necessity of repeating certain inputs like certificate location, etc. is eliminated.

2.3.1 Features

Profile Manager can be used to perform the following operations:

Operation	Purpose
Add	Create a new profile
Modify	Modify an existing profile

Delete	Delete an existing profile

2.4 FILESIGNER® PLUS WIZARD

The FileSigner® Plus wizard guides you through a simple, step-by-step procedure to sign file(s). It may be used to perform the following operations:

Operation	Result
Sign	Signed File(s)

2.4.1 Sign

Using FileSigner® Plus, you can sign files of any format.

PKI-based Digital Signatures provide assurance over the source and validity (*Authenticity*) of electronic files and the information contained within. They provide persistent approvals on documents, ensuring that information is tamper-proof (*Integrity*). Digital Signatures also make it impossible for signing parties to dissociate themselves from documents signed by them (*Non-Repudiation*).

FileSigner® Plus allows you to sign multiple files at one go. This saves time when a large number of files are to be signed.

2.5 FILEVERIFIER™ PLUS WIZARD

The FileVerifier™ Plus wizard helps you to verify file(s). It may be used for the following operations

File Type	Operation
Signed File	Verify

2.5.1 Verify

When you receive digitally signed documents, you can use FileVerifier™ Plus to verify the signature(s) on them. FileVerifier™ Plus also provides settings/options for flexible checking of the revocation status of signer certificate(s) depending on the level of security required.

Verification of signatures ensures that:

- The identity of the sender is irrefutably established.
- You are alerted if the information in the signed file has been tampered with.
- The sender cannot deny involvement at a later date.

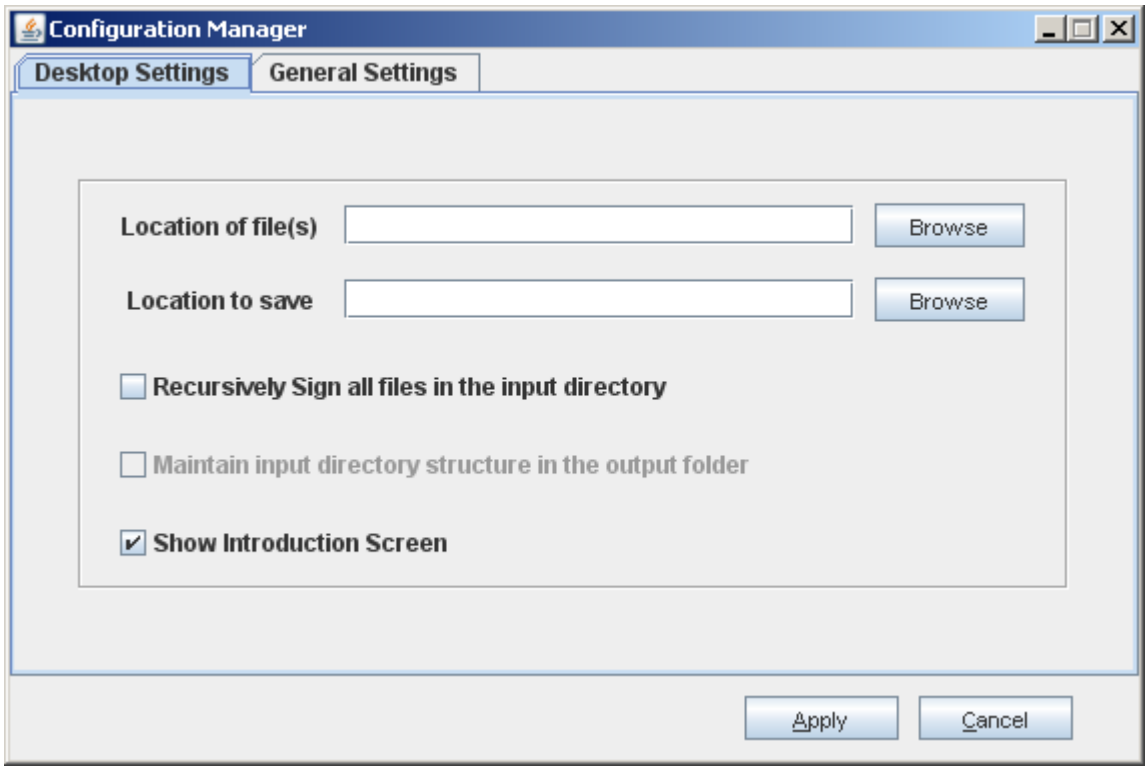
3 CONFIGURING FILESIGNER® PLUS

3.1 INVOKING CONFIGURATION MANAGER

The Configuration Manager can be accessed from the FileSigner® Plus menu in Windows' Program Files as follows:

- Start → Program Files → TCS FileSigner Plus → Configuration Manager

3.2 USING CONFIGURATION MANAGER



Once Configuration Manager is invoked, the above screen is displayed.

3.2.1 Desktop Settings

3.2.1.1 Setting location of source file(s)

- Click [Browse] to select a default folder for the source file(s) for signing. Each time the FileSigner® Plus wizard is invoked, it will automatically list the file(s) contained in the selected folder.

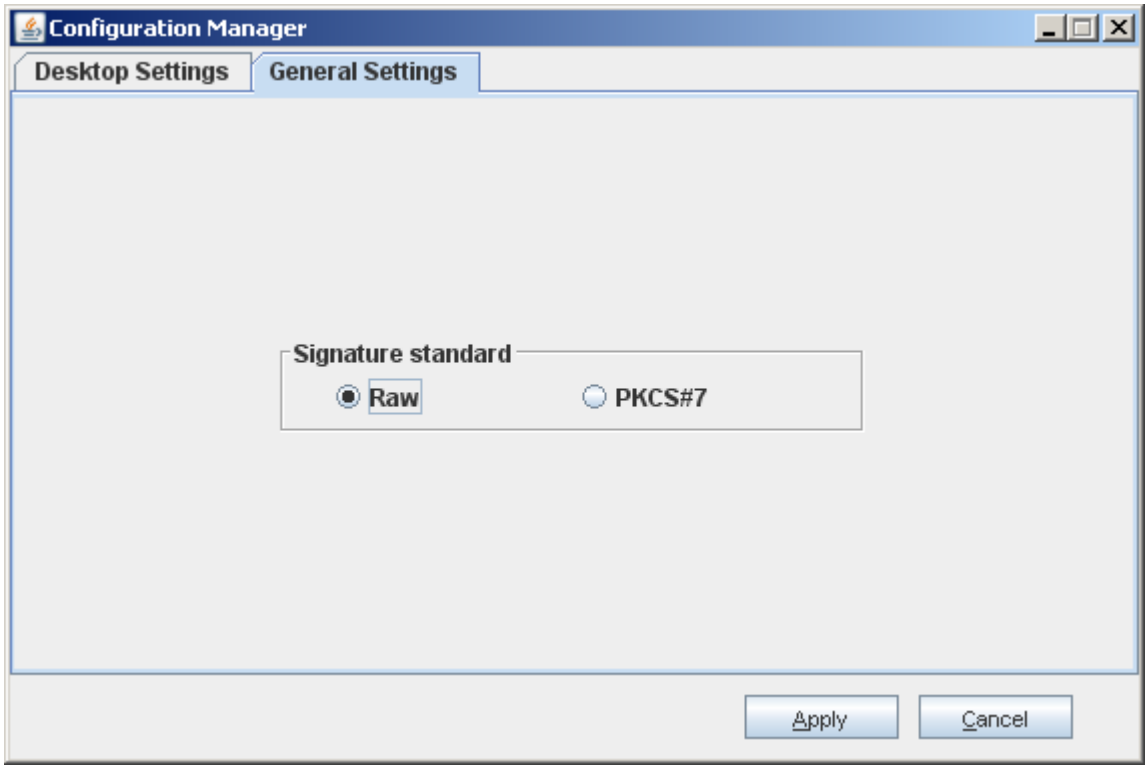
3.2.1.2 Setting location to save result file(s)

- Click [Browse] to select a default folder for signed files. When the FileSigner Plus wizard is invoked, it will automatically use this as the destination folder for processed files.

3.2.1.3 Show Introduction Screen

Check/Uncheck the [Show Introduction Screen] box to enable/disable the introduction screen for the FileSigner® Plus and FileVerifier™ Plus Wizards. If the introduction screen is disabled, you will be taken directly to the first step that needs to be performed in the selected wizard.

3.2.2 General Settings



3.2.2.1 Signature standard

FileSigner® Plus allows you to generate two types of signature standards. You can choose between:

- Raw
- PKCS#7

3.2.3 Apply Configuration Settings

Once you complete configuring FileSigner® Plus according to your preferences, click [Apply] to apply the settings and close the Configuration Manager.

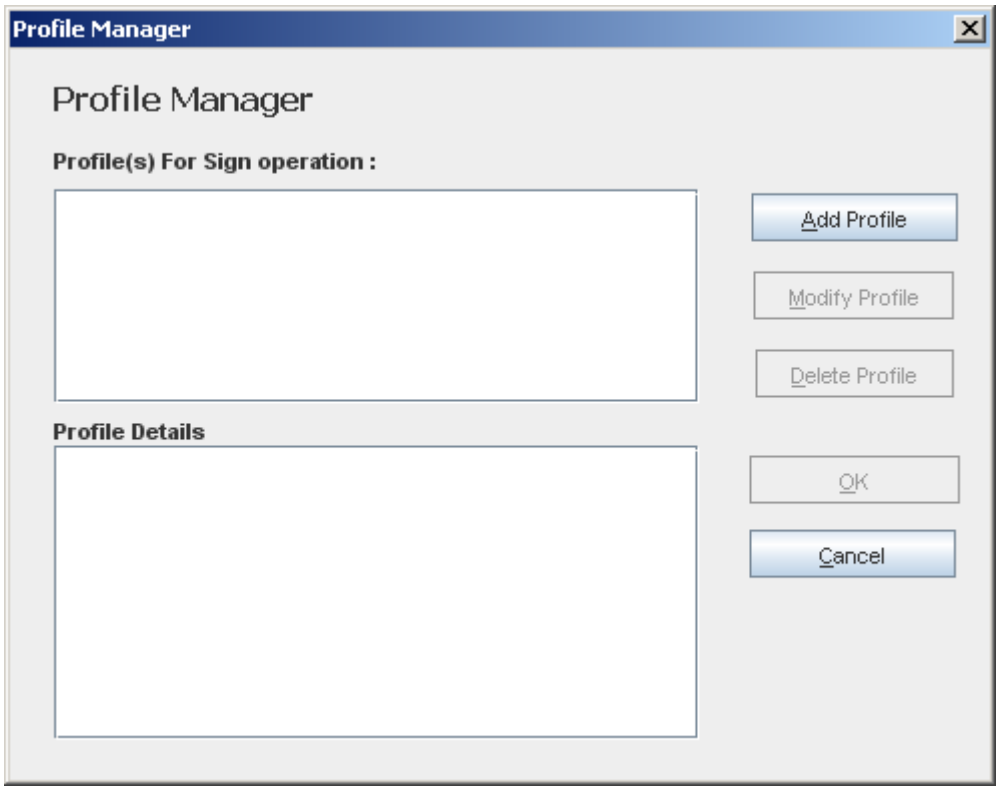
4 PROFILE MANAGER

4.1 USING PROFILE MANAGER

The following sections outline the procedure for creating, modifying and deleting a profile for Sign operation:

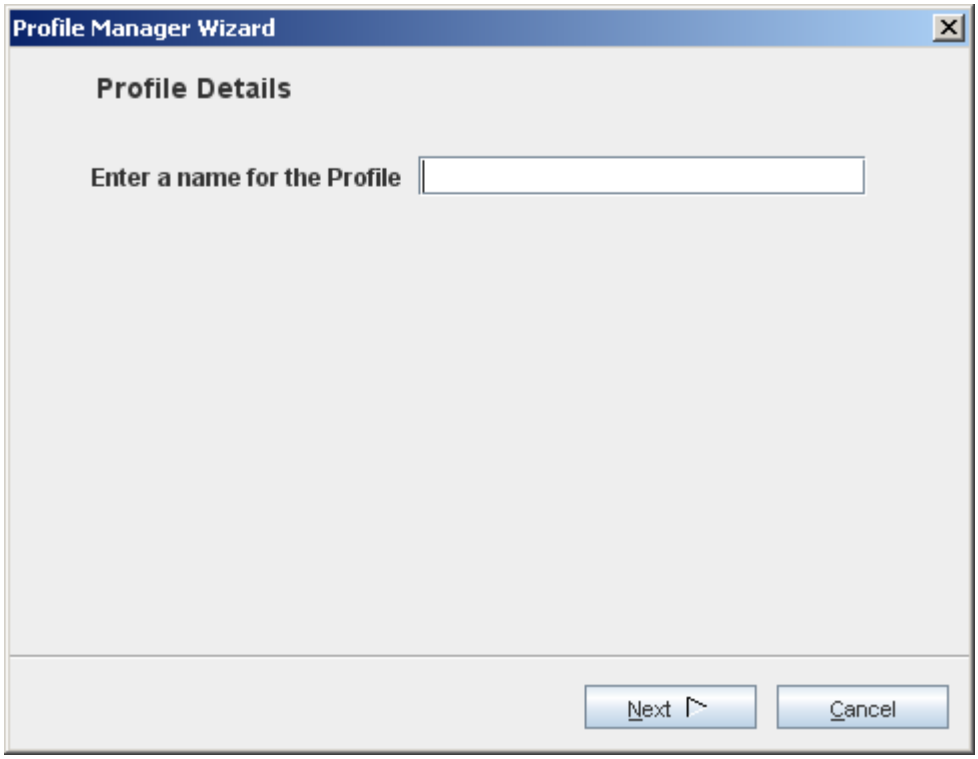
4.1.1 Add a Profile

STEP 1 » SELECT OPERATION TO BE PERFORMED



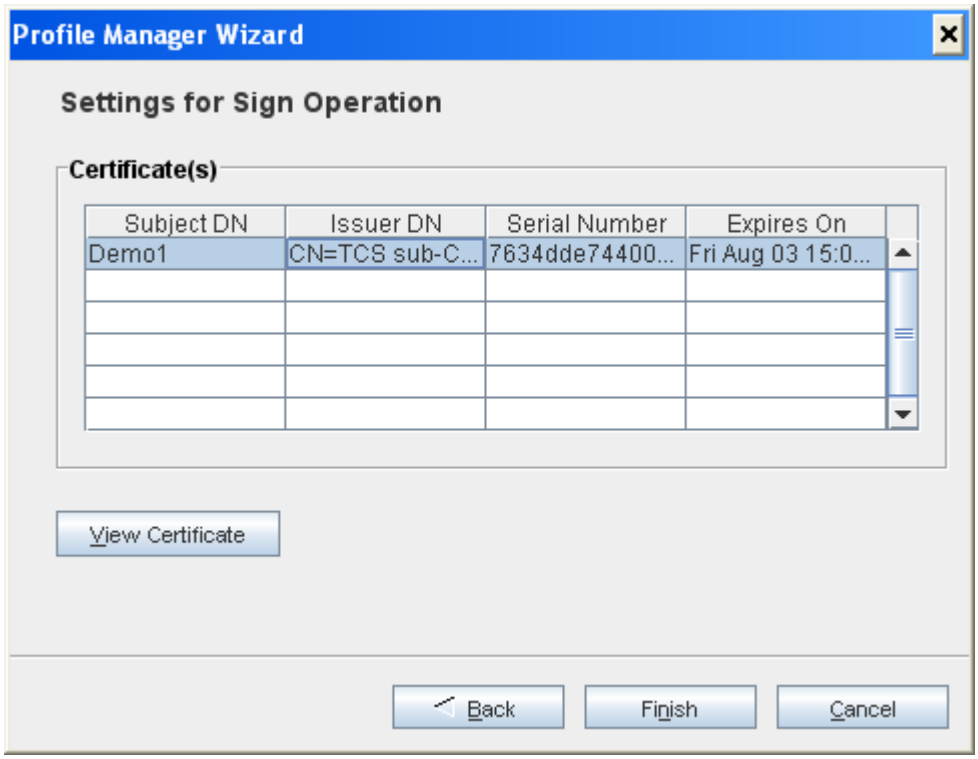
- Select [Add Profile] from the Profile Manager Start-up screen.

STEP 2 » PROVIDE PROFILE DETAILS



- Enter the name of the profile to be added.

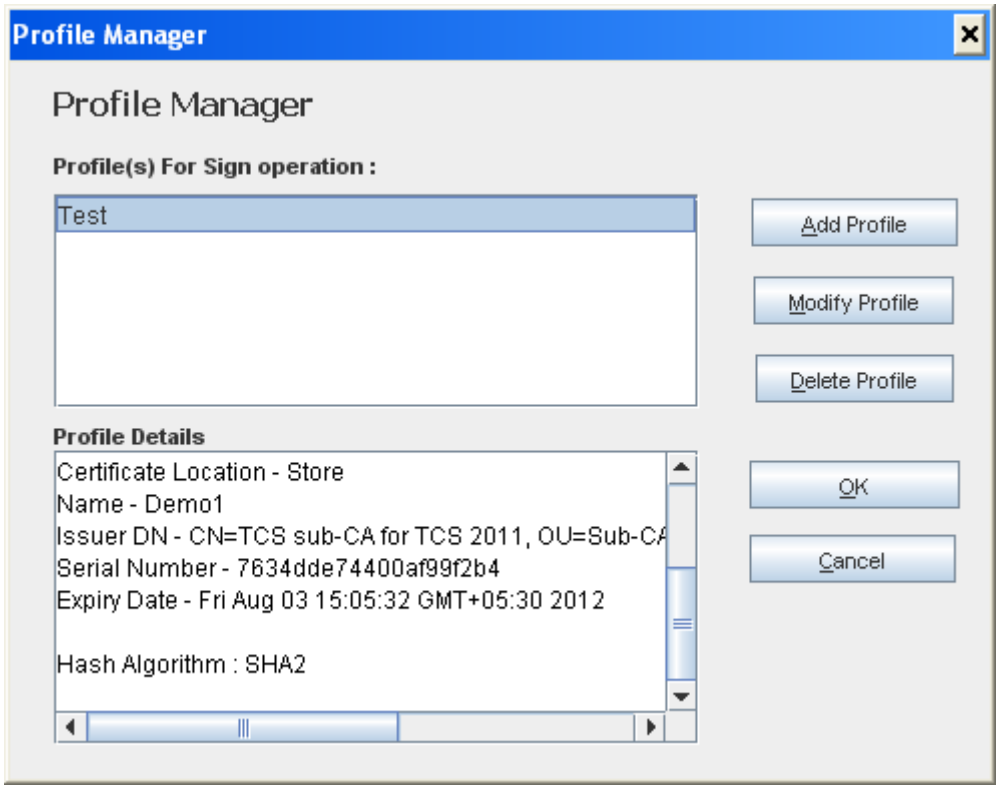
STEP 3 » SELECT CERTIFICATE FOR SIGNING



- Select the certificate to be used for signing from the list displayed.

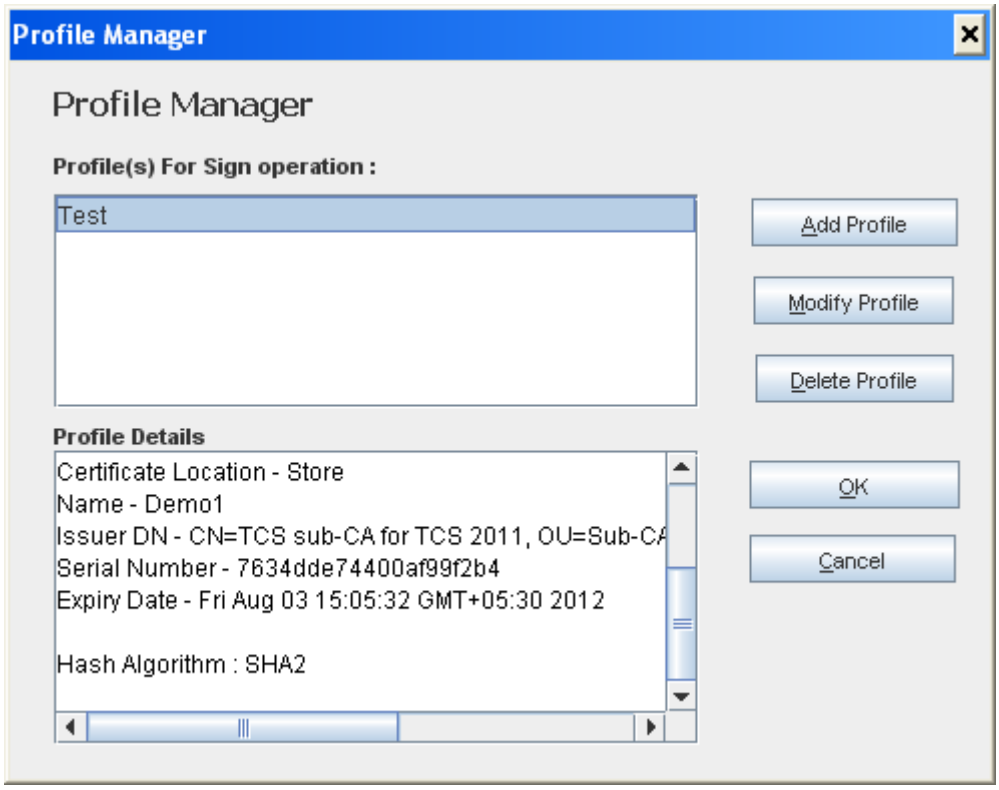
This completes the settings for the signing operation.

4.1.2 Modify a Profile



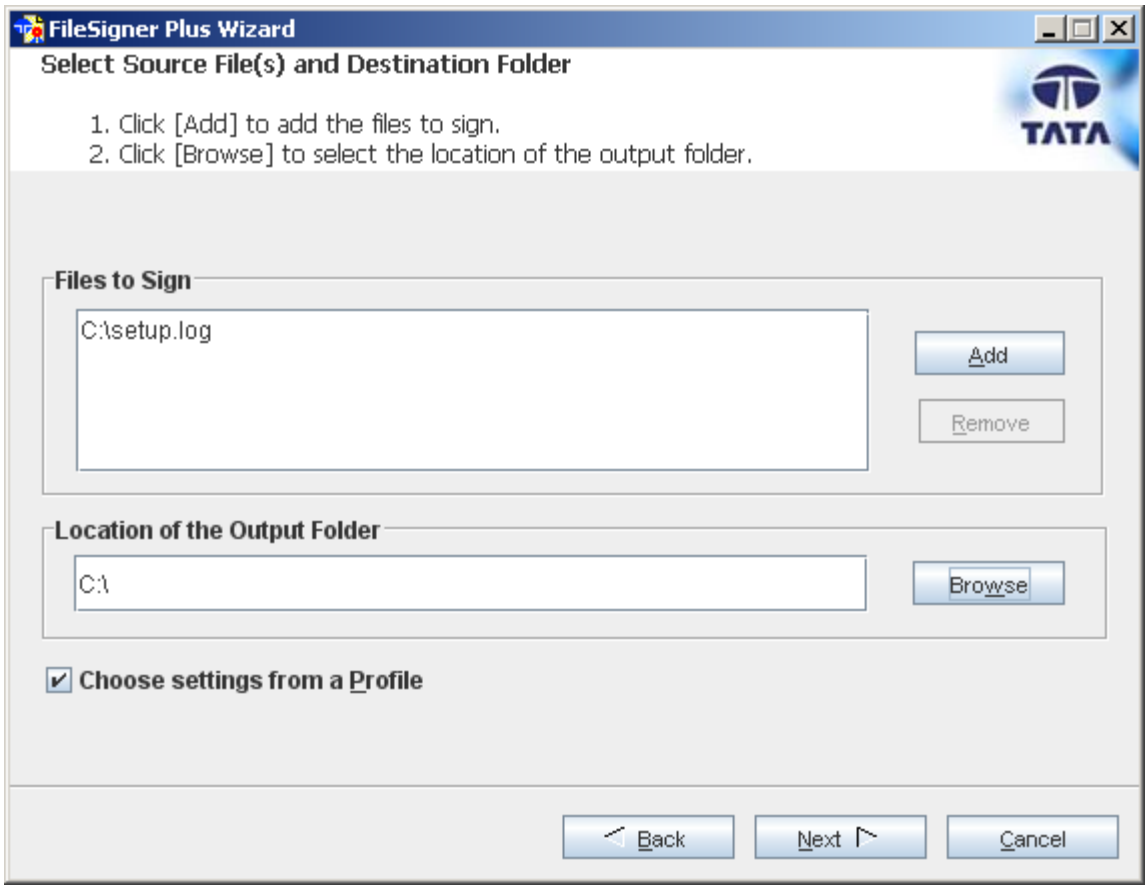
Existing profiles can be modified using Profile Manager. To modify a profile, select it from the list of available profiles and click [Modify Profile].

4.1.3 Delete a Profile



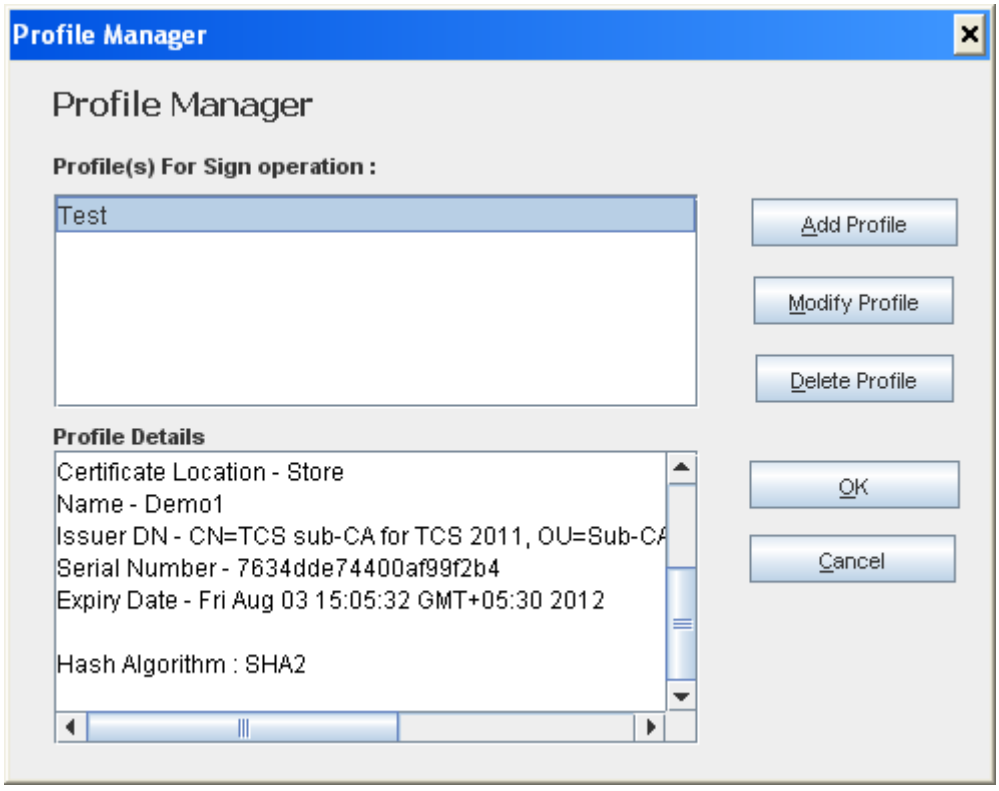
Existing profiles can be deleted using Profile Manager. To delete a profile, select it from the list of available profiles and click [Delete Profile].

4.2 USING PROFILE MANAGER FROM FILESIGNER® PLUS

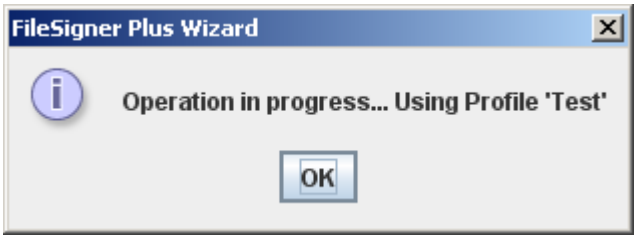


- Profiles created using Profile Manager can be used while performing security operations using FileSigner® Plus. In order to use profiles, select 'Choose Settings from a Profile' in the FileSigner® Plus wizard.

- On clicking [Next], the created Profiles (viz., Sign) are displayed for selection as shown below.



- Select the desired Profile and click [OK]. A message will be displayed, as shown below, confirming that the selected profile will be used for the current operation.



- Click [OK] to continue with the operation.

5 PERFORMING SECURITY OPERATIONS

5.1 FILESIGNER® PLUS WIZARD

5.1.1 Invoking FileSigner® Plus Wizard

5.1.1.1 From the Start Menu

- Start → Program Files → TCS FileSigner Plus → FileSigner Plus

5.1.1.2 From the Desktop

- Double click the FileSigner Plus icon on your desktop.

Introduction Screen for Raw signature standard

Introduction Screen for PKCS#7 signature standard

N

7

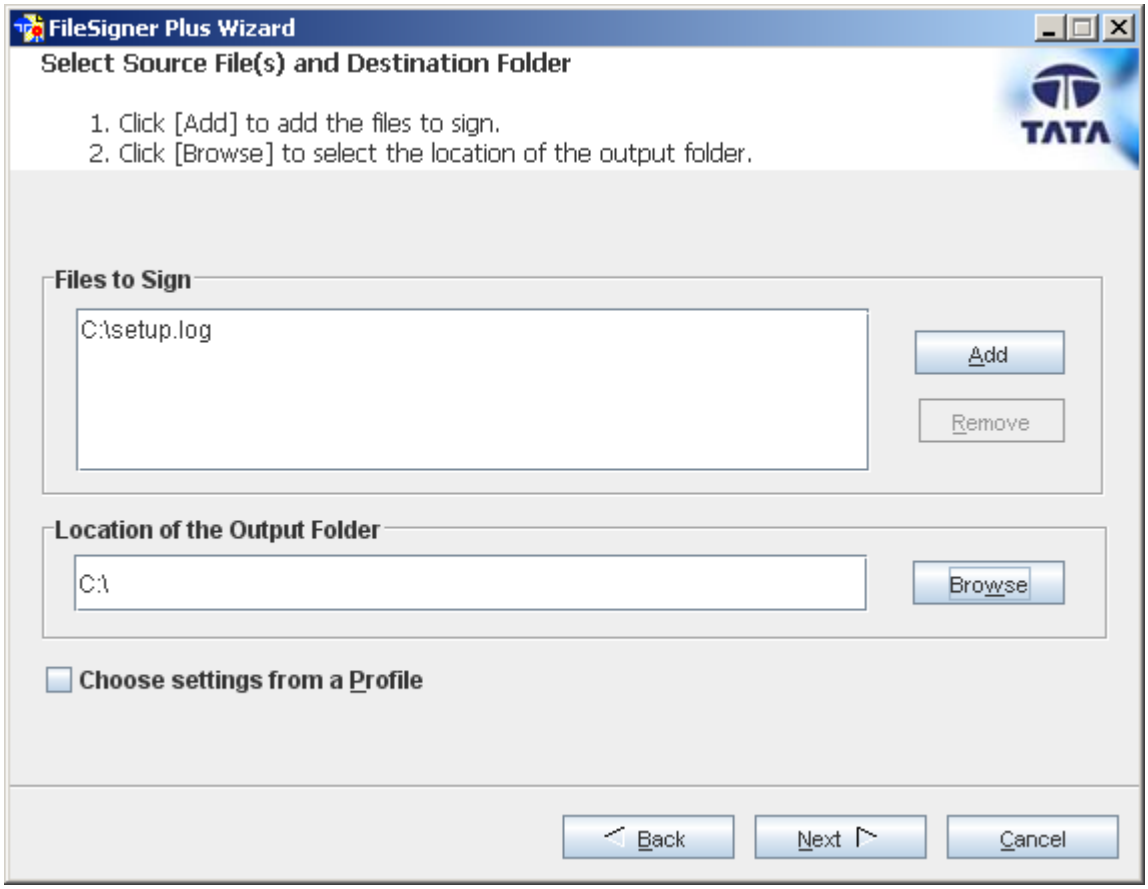
Once the FileSigner® Plus wizard is invoked, you will see the above introduction screen.

The introduction screen can be disabled using the Configuration Manager.

- Click [Next] to perform signing operations.

5.1.2 Sign

STEP 1 » SELECT OPERATION, SOURCE FILE(S) AND DESTINATION FOLDER



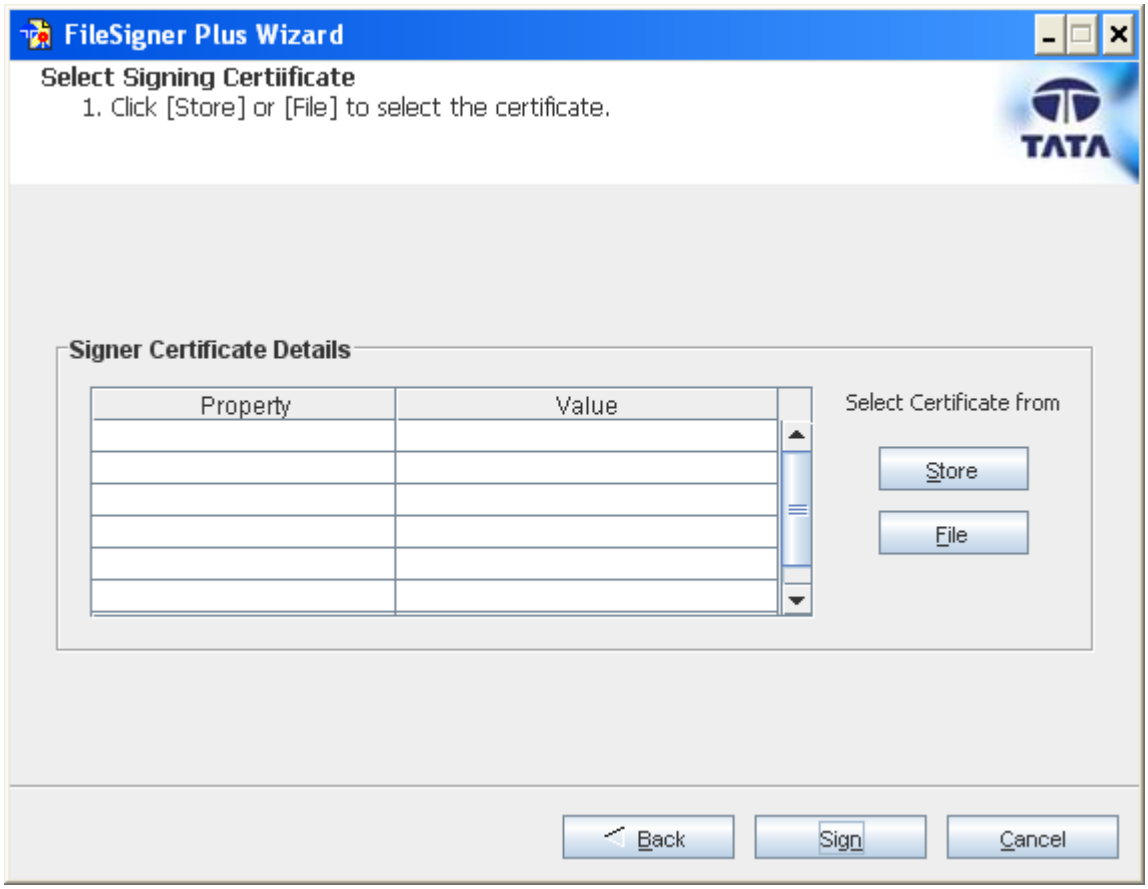
- Select the file(s) to be signed. FileSigner® Plus supports batch signing, hence, you can choose multiple files to sign at one go.

While selecting a file to sign, ensure that:

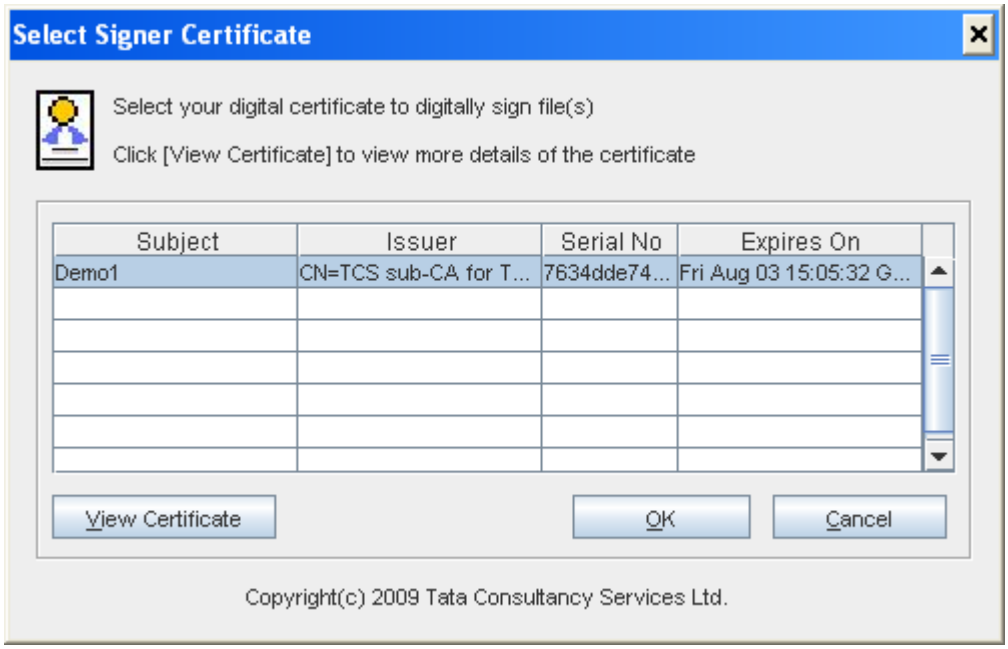
- The file is not open.
- The file is not empty.

- Select the destination folder for the signed file.
- Click [Next] to continue.

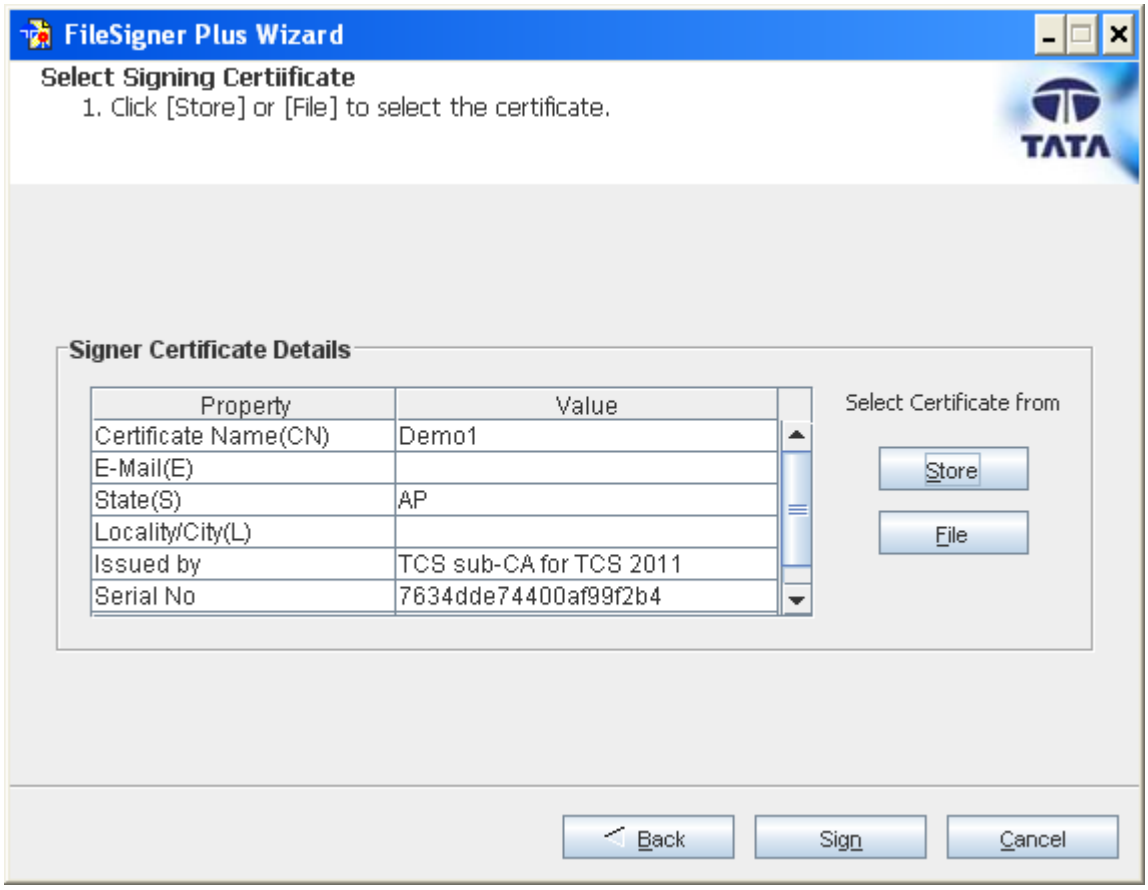
STEP 2 » SELECT SIGNING CERTIFICATE



- Click the [Store] button to select the digital certificate from certificate store, to be used for signing the file(s) selected in the previous section. Only those certificates whose key usage enables them to be used for signing will be displayed.
- Click the [File] button to select the digital certificate from a file



- You can view the details of any certificate by clicking the [View Certificate] button.
- Click [OK] to select a certificate for signing.



- Now click [Sign] to continue.

OPERATION STATUS » VIEW STATUS OF SIGNING OPERATION

Once the signing is complete, you will be able to view the final status of the operation.

Files signed by FileSigner® Plus have the same extension as input file.

5.2 FILEVERIFIER™ PLUS WIZARD

5.2.1 Invoking FileVerifier™ Plus Wizard

5.2.1.1 From the Start Menu

- Start → Program Files → TCS FileSigner Plus → FileVerifier Plus.

5.2.1.2 From the Desktop

- Double click the FileVerifier™ Plus icon on your desktop.

5.2.2 Introduction Screen

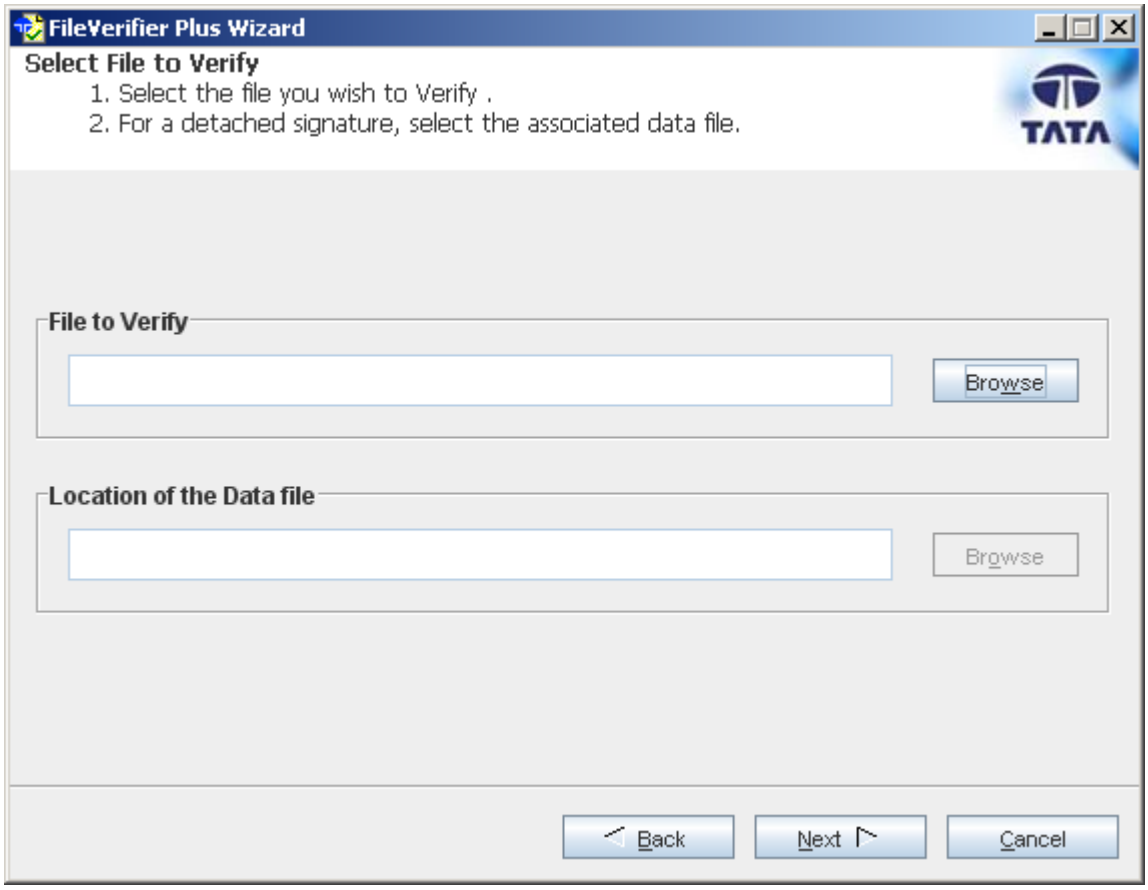
Once the FileVerifier™ Plus wizard is invoked, you will see the above introduction screen.

The introduction screen can be disabled using the Configuration Manager.

- Click [Next] to perform verification operations.

5.2.3 Verify

STEP 1 » SELECT SOURCE FILE

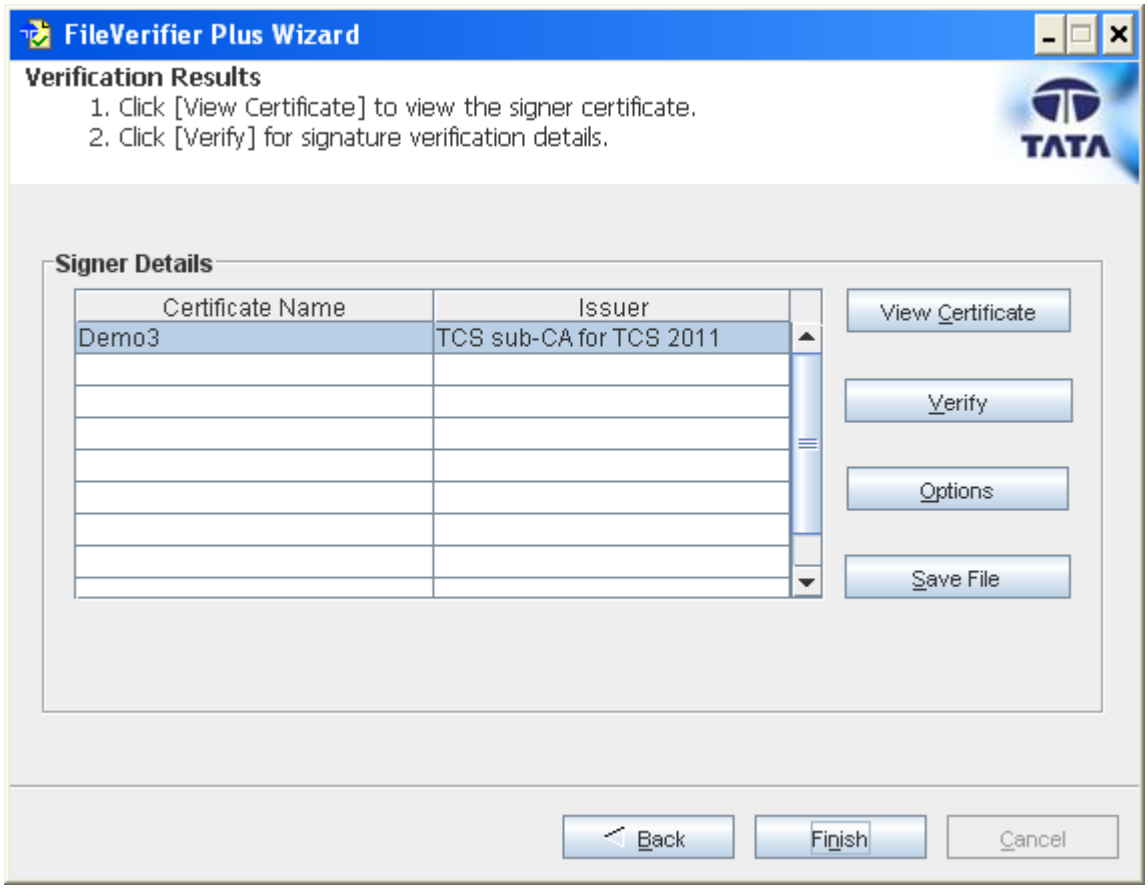


- Click [Browse] to select the file to be verified.
- Click [Next] to view the signature details.

Only **one** file may be verified at a time.

STEP 2 » VERIFY SIGNATURE(S)

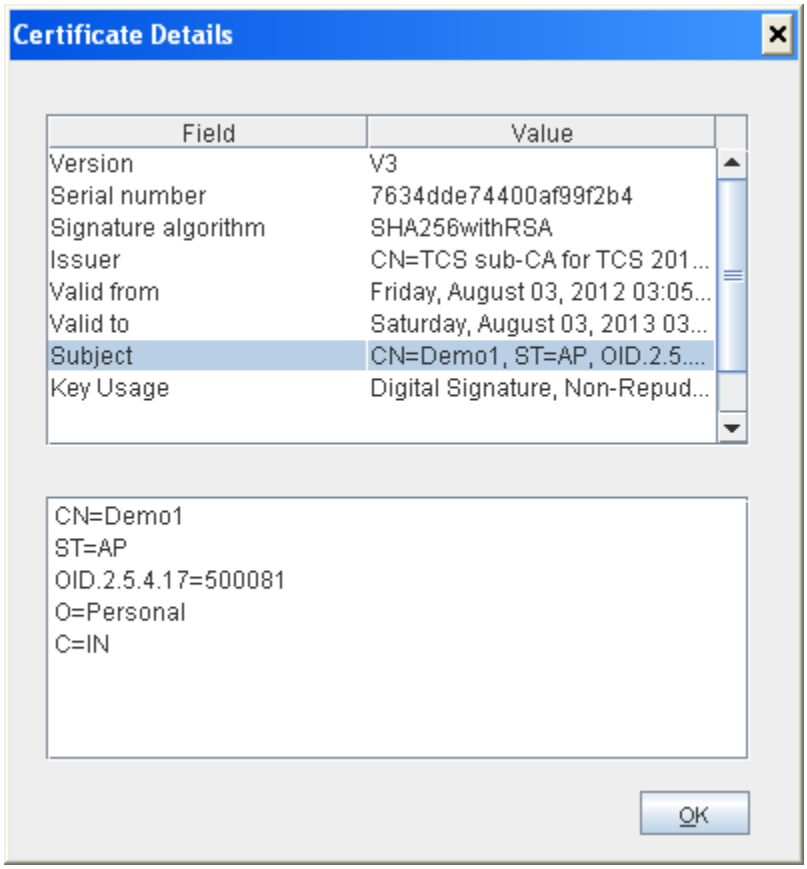
On successful extraction of signatures from the signed file, FileVerifier™ Plus displays the following screen:



The details of certificate(s) used to sign the file being verified are displayed in the Signer Certificate(s) list. In order to verify a signature, you need to perform the following steps:

- Select a certificate from the list of signer certificates displayed.

- Click [View Certificate] to view the certificate details. [Check to see if the signer's information is as expected.]



- Click [Verify] to verify the signature. You will see the following summary screen.

- You can customize the verification process depending on your requirements. Click [Options] to view the Certificate Revocation List (CRL) options available.

OPTIONS » SELECT CERTIFICATE REVOCATION LIST (CRL) OPTIONS

» Revocation Check Required

To ensure that the revocation status of the signer's certificate is verified, you can check the [Revocation Check Required] box.

The CRL Verification is done offline here, i.e. you need to manually place the corresponding CRLS in the CRLs folder present in the installed directory of FileSigner Plus → ".fsp" folder.

» Certificate Validation Options

For certificate validation, the issuer certificates which are the public key certificates of Issuers like TCS-CA (CA certificate) and CCA (Root CA certificate), have to be placed in the "IssuerCerts" folder which is present in ".fsp" folder after the software installation.

If the installation directory is "C:\FileSigner Plus" then a folder ".fsp" is automatically created during installation of FileSigner® Plus software. Under ".fsp" folder a folder "IssuerCerts" is created in which the issuer certificates have to be placed.

For example, to verify a digital signature, which is signed using a TCS-CA issued digital certificate, you will need to place the TCS-CA and CCA certificate in the "IssuerCerts" folder to trust the signer's digital certificate.

While verifying the signature, there is no need of providing public key certificate as the signature created out of FileSigner® Plus software includes the signer's public key certificate as part of digital signature. If a signature without public key certificate

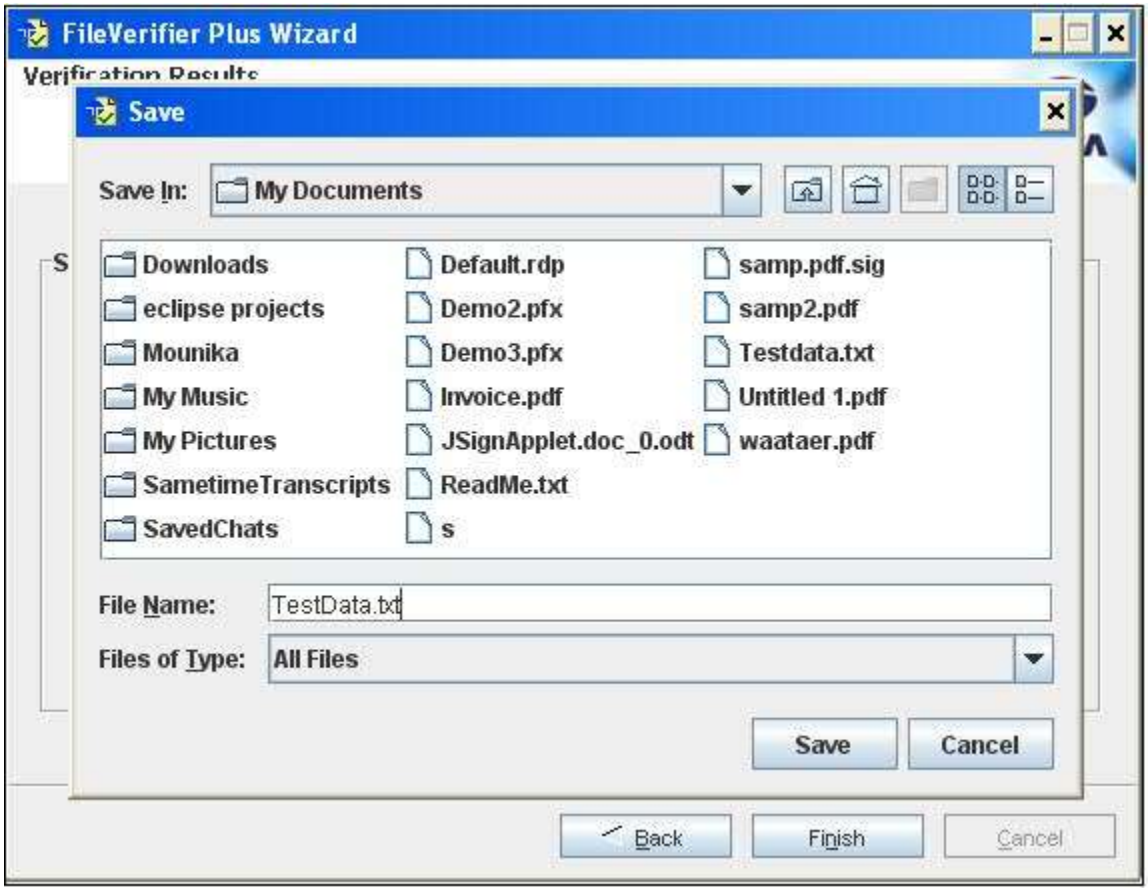
needs to be verified using FileSigner® Plus software, verifier should place the signer's public key certificate in "SignerCerts" folder present in ".fsp" folder.

For Verifying the revocation status, two options are available. You can check the revocation status for:

- The signer certificate only – In this case only the signer's certificate is checked for revocation.
- The entire trust chain – In this case, in addition to the signer's certificate, all the certificates in the trust chain are checked for revocation. This is the more secure option for verification.

Once the options are set, you can click [Verify] to verify the signer certificates with the new options.

SAVE FILE » TO SAVE THE CONTENT FROM THE SIGNATURE



To save the Original data file Save File button is used. When the button is clicked the above screen is displayed. The location and name of the data file can be specified to save the data file at required location and then click on Save button.

Click [Finish] to exit the Wizard.

6 SMART CARDS & HARDWARE TOKENS

FileSigner® Plus supports Smart Cards and Hardware Tokens. Certificates stored on these devices are automatically made available for selection to the user during signing.

7 UNINSTALLING FILESIGNER® PLUS

To uninstall FileSigner® Plus, you can do the following:

- Start → Program Files → TCS FileSigner Plus → Uninstall

8 APPENDIX

The following table shows the signer certificate validation results.

Signer certificate validation results will be based on the

- Revocation check level that is selected in the CRL Options dialog
- Validity of the signer certificate
- Signer certificate trust chain
- Revocation status of the signer certificate

Revocation check level (Not requested / Signer Certificate only / Entire trust chain)	**Validity of the certificate (Valid / Invalid - Expired or Not yet valid)**	**Certificate Trust Chain (Complete/ Incomplete)**	**Revocation status (Not Requested/ Revoked / Not Revoked / Not available)**	**Result**
Not Requested	Valid	Complete	Not Requested	Signer certificate is valid Signer certificate is trusted Revocation status is not requested
Not Requested	Invalid	Complete	Not Requested	Signer certificate is not valid Signer certificate is not trusted Revocation status is not requested
Not Requested	Valid	Incomplete	Not Requested	Signer certificate is valid Signer certificate is not trusted Revocation status is

				not requested
Not Requested	Invalid	Incomplete	Not Requested	Signer certificate is not valid Signer certificate is not trusted Revocation status in not requested
Signer Certificate only	Valid	Complete	Not Revoked	Signer certificate is valid Signer certificate is trusted Signer certificate is not revoked
Signer Certificate only	Invalid	Complete	Not Revoked	Signer certificate is not valid Signer certificate is not trusted Signer certificate is not revoked
Signer Certificate only	Valid	Incomplete	Not Revoked	Signer certificate is valid Signer certificate is not trusted Signer certificate revocation status is not available
Signer Certificate only	Valid	Complete	Revoked	Signer certificate is valid Signer certificate is not trusted Signer certificate is revoked

Signer Certificate only	Invalid	Incomplete	Not Revoked	Signer certificate is not valid Signer certificate is not trusted Signer certificate revocation status is not available
Signer Certificate only	Invalid	Complete	Revoked	Signer certificate is not valid Signer certificate is not trusted Signer certificate is revoked
Signer Certificate only	Valid	Incomplete	Revoked	Signer certificate is valid Signer certificate is not trusted Signer certificate revocation status is not available
Signer Certificate only	Invalid	Incomplete	Revoked	Signer certificate is not valid Signer certificate is not trusted Signer certificate revocation status is not available
Signer Certificate only	Valid	Complete	Not available	Signer certificate is valid Signer certificate chain status is unknown Signer certificate revocation status is not available

Signer Certificate only	Valid	Incomplete	Not available	Signer certificate is valid Signer certificate is not trusted Signer certificate revocation status is not available
Signer Certificate only	Invalid	Complete	Not available	Signer certificate is not valid Signer certificate chain status is unknown Signer certificate revocation status is not available
Signer Certificate only	Invalid	Incomplete	Not available	Signer certificate is not valid Signer certificate is not trusted Signer certificate revocation status is not available
Entire trust chain	Valid	Complete	*Not Revoked	Signer certificate is valid Signer certificate is trusted Signer certificate is not revoked
Entire trust chain	Invalid	Complete	*Not Revoked	Signer certificate is not valid Signer certificate is not trusted Signer certificate is not revoked

Entire trust chain	Valid	Incomplete	*Not Revoked	Signer certificate is valid Signer certificate is not trusted Signer certificate revocation status is not available
Entire trust chain	Valid	Complete	**Revoked	Signer certificate is valid Signer certificate is not trusted One of the certificates in the chain is revoked
Entire trust chain	Invalid	Incomplete	*Not Revoked	Signer certificate is not valid Signer certificate is not trusted Signer certificate revocation status is not available
Entire trust chain	Invalid	Complete	**Revoked	Signer certificate is not valid Signer certificate is not trusted One of the certificates in the chain is revoked
Entire trust chain	Valid	Incomplete	**Revoked	Signer certificate is valid Signer certificate is not trusted One of the certificates in the chain is revoked

Entire trust chain	Invalid	Incomplete	**Revoked	Signer certificate is not valid Signer certificate is not trusted One of the certificates in the chain is revoked
Entire trust chain	Valid	Complete	Not available	Signer certificate is valid Signer certificate chain status is unknown Signer certificate revocation status is not available
Entire trust chain	Valid	Incomplete	Not available	Signer certificate is valid Signer certificate is not trusted Signer certificate revocation status is not available
Entire trust chain	Invalid	Complete	Not available	Signer certificate is not valid Signer certificate is not trusted Signer certificate revocation status is not available
Entire trust chain	Invalid	Incomplete	Not available	Signer certificate is not valid Signer certificate is not trusted Signer certificate revocation status is not available

Note: * - Revocation status is checked for all the certificates in the chain
** - Any one of the certificates in the chain may be revoked

Contact Us

http://www.tcs-ca.tcs.co.in

TATA CONSULTANCY SERVICES

www.tcs.com