Symantec™ Managed PKI®

Integrating Adobe CDS Organization Certificates with Adobe® LiveCycle® Enterprise Suite and Adobe® Reader®

Symantec

Symantec™ Managed PKI® Integrating Adobe CDS Organization Certificates with Adobe® LiveCycle® Enterprise Suite and Adobe® Reader®

Last updated November 13, 2013

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Chapter 1

Integrating Adobe CDS Organization Certificates with Adobe® LiveCycle® Enterprise Suite and Adobe® Reader®

The enterprise workplace has moved beyond the walls of the organization into a global, mobile environment. To maintain productivity, your end users need to access company resources using a mobile platform. However, you need to be able to trust the end users accessing your systems, and the mobile devices they use, whether you provide their devices or they bring their own.

Symantec's Managed PKI digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from several to thousands of devices, providing an in-the-cloud solution for quick deployment and easy management. It also incorporates features from Symantec's other leading security products.

Symantec's digital certificates for Certified Document Services (CDS) Organization allow you to include digital signatures that let you sign PDF files. By digitally signing a pdf, you apply your unique digital mark to the document and also confirm the document has not been altered in transit.

This document describes how to configure CDS Organization certificate with Adobe® LiveCycle® and Adobe® Reader® to digitally authenticate Adobe® PDF documents.

Partner Information

These procedures have been tested on the following platforms:

Table 1-1 Partner Information

Partner Name	Adobe®
Product Name and Version	Adobe® LiveCycle® Enterprise Suite 4, Adobe® Reader® XI

How the Adobe CDS Organization Certificate Works

The following diagram describes how Managed PKI certificates support CDS Organization certificate and integrates with Adobe Reader for digital authentication.

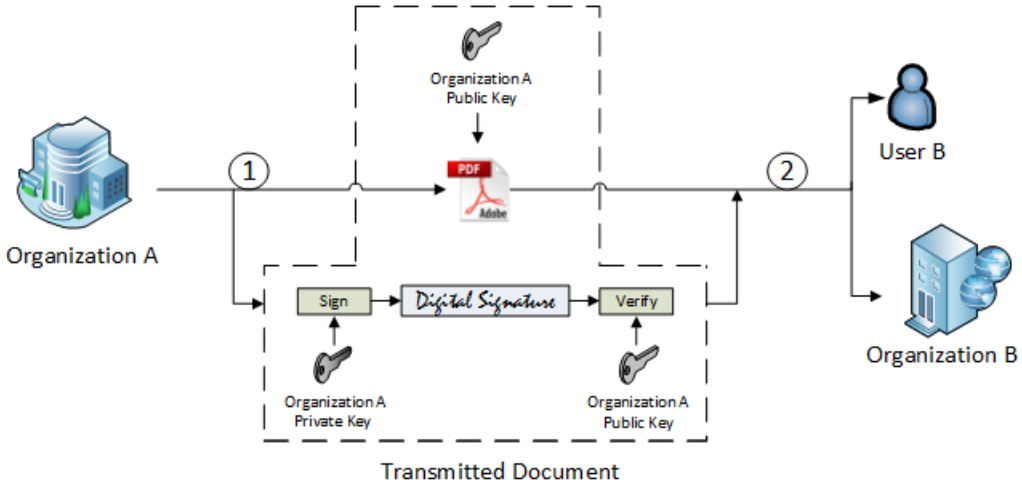

Figure 1-1 Adobe CDS Certificate integration with Adobe Reader

1 Organization A digitally signs an Adobe PDF document using Organization A's private key.

2 Organization B or User B of Organization B receives the document and authenticates it using Organization A's public key.

Integration Workflow

The following diagram describes the general steps required to set up a Symantec Managed PKI account and integrate Managed PKI certificates with Adobe LiveCycle and Adobe Reader.

Figure 1-2 Managed PKI Integration Workflow

Task 1. Set up your Managed PKI 8.9 account

Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

You will need to complete and return the following documents. As needed, your Symantec representative will assist you in obtaining and completing these forms.

- Master Service Agreement
- Issuing Authority Naming Application (also known as the CA Naming Document)
- Symantec Services Order Form
- Purchase Order, credit card, or reference number

You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. For more information on configuring Managed PKI, refer to PKI Manager and its online help.

Task 2. Create a certificate profile

Managed PKI uses a certificate profile to define the certificates issued. Certificate issued by Adobe CDS Organization enables digital authentication of PDF documents.

Complete the following steps to create your Managed PKI Adobe CDS Organization certificate profile:

1 Log on to Managed PKI's PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.

2 On PKI Manager, click **Manage certificate profiles** or select **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.

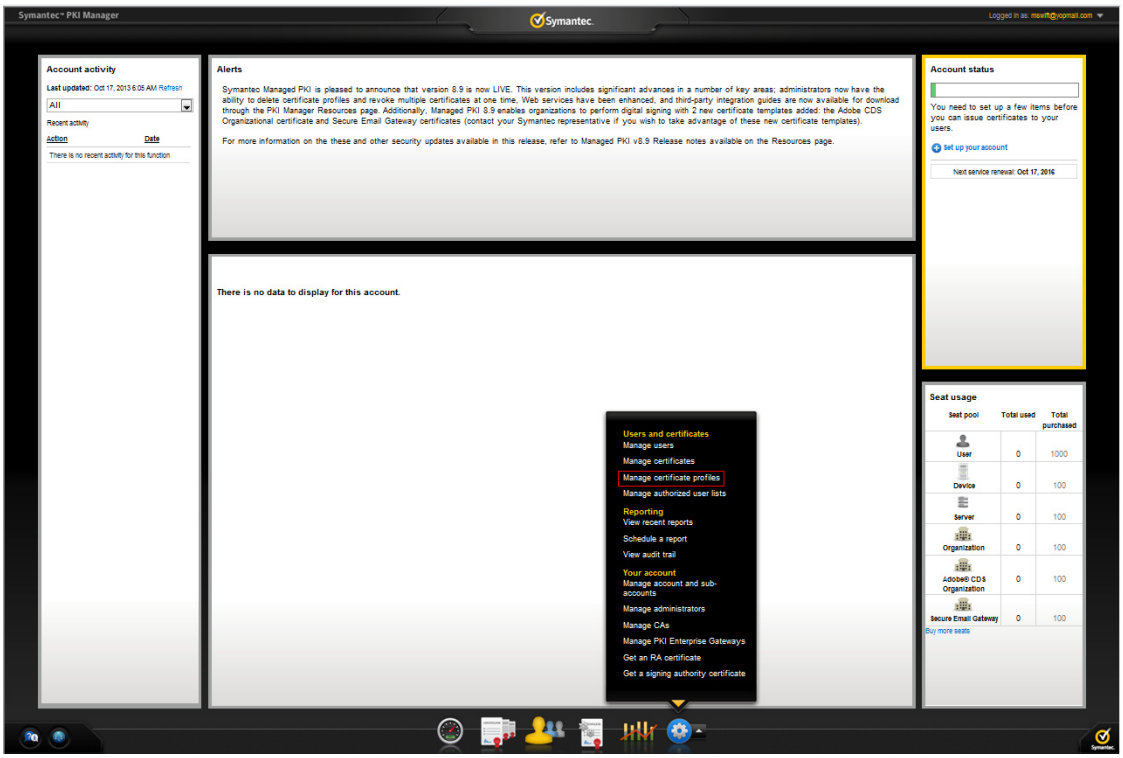

Figure 1-3 Manage Certificate Profile

3 Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The Create profile page appears.

4 Select whether these certificates will be issued in Test mode or Production Mode, and click **Continue**. The Create profile page appears.

5 Select **Adobe® CDS Organization** as the certificate template and click **Continue**. The Customize certificate options page appears.

6 In the Customize certificate options, enter a certificate profile name.

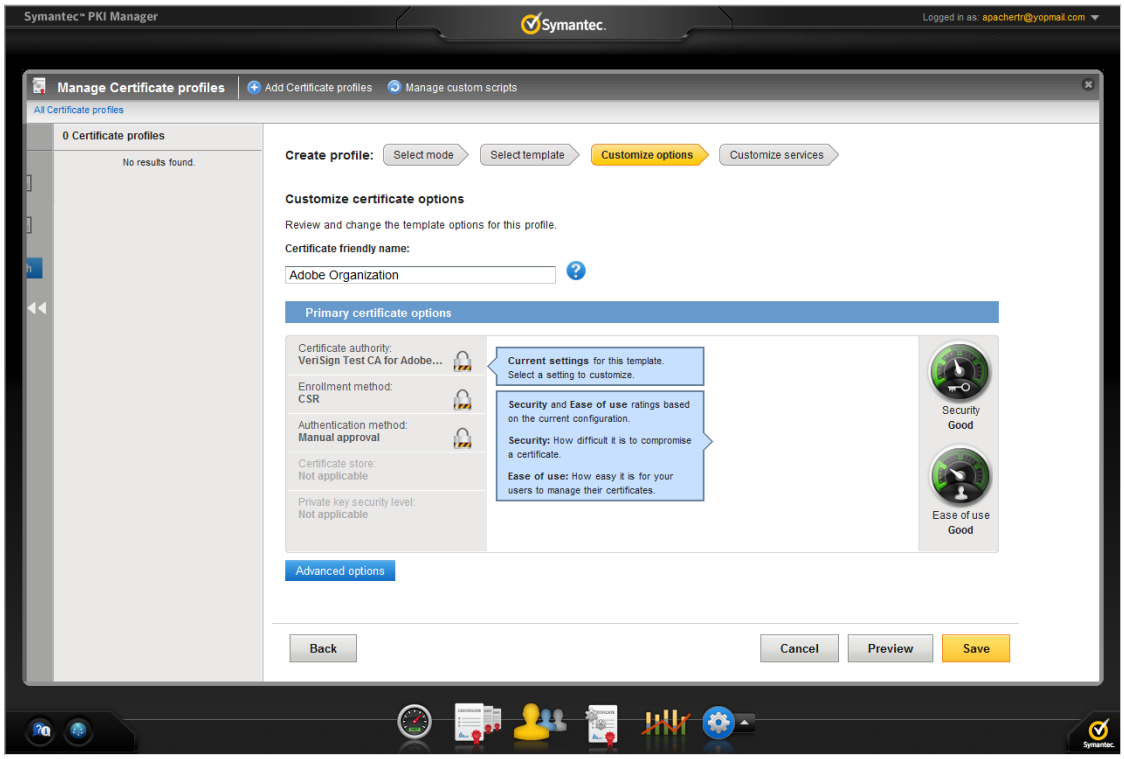

Figure 1-4 Adobe CDS Organization Certificate options

7 Click **Advanced options** to view certificate options and define any additional attributes you may need.

8 Click **Save**.

On the confirmation page, you can view the attribute used for the seat ID, a mandatory attribute that authenticates the user for third-party configurations or during enrollment process. This is typically the user's email address.

You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

Prerequisites

- The Adobe CDS end-user certificate must be stored on a Hardware Security Module (HSM).
- Your administrator must configure the HSM to be partitioned. The Luna SA client must be installed and configured on the partitioned HSM.

Generate CSR on HSM

You must generate Certificate Signing Request (CSR) on Hardware Security Module (HSM) before enrolling for certificates. The certificate along with its private key is stored in HSM.

1 Open the command prompt.

2 Go to the Luna SA client install directory on your system. For example, `C:\Program Files <x86>\LunaSA`.

3 Enter the following commands to generate the CSR on the HSM.

- **Generate key pair** - Use the certificate management utility of Luna SA Client to generate public and private key pair.

  ```
  cmu generatekeypair -modulusbits=2048 -publicexponent=65537 -sign=T -verify=T -
  labelpublic="<public_key_label>" -labelprivate="<private_key_label>"
  ```

  Enter the password for the token slot to generate the key pair.

- **Generate CSR** - After the key pair is generated, you can generate the CSR.

  ```
  cmu requestcertificate -c="<two_letter_country_code>" -o="<organization_name>" -
  cn="<common_name>" -s="<state>" -l="<city/locality>" -publichandle=<public_handle>
  -privatehandle=<private_handle> -outputfile=""
  ```

4 After you generate the CSR, log in to PKI Manager.

5 Click the Certificate Service URL that is displayed on the confirmation of profile creation page.

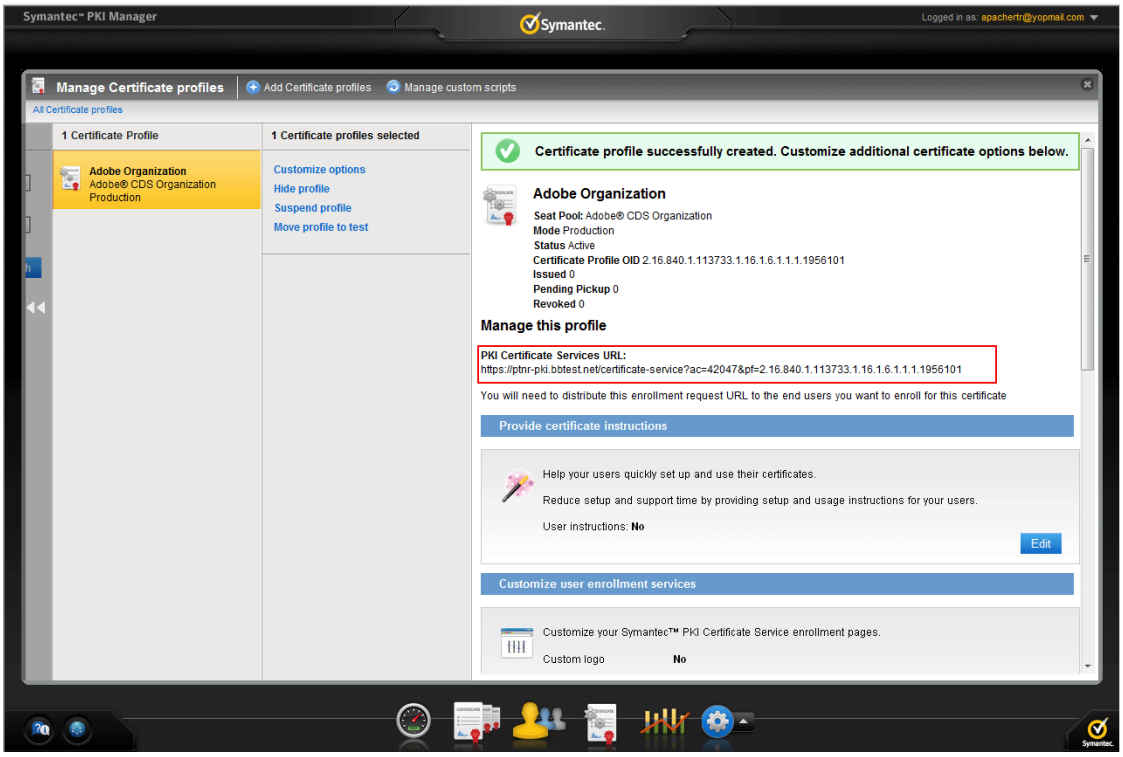

Figure 1-5 PKI Certificate Service URL

6 Enter the required details and paste the CSR that was generated on the HSM.

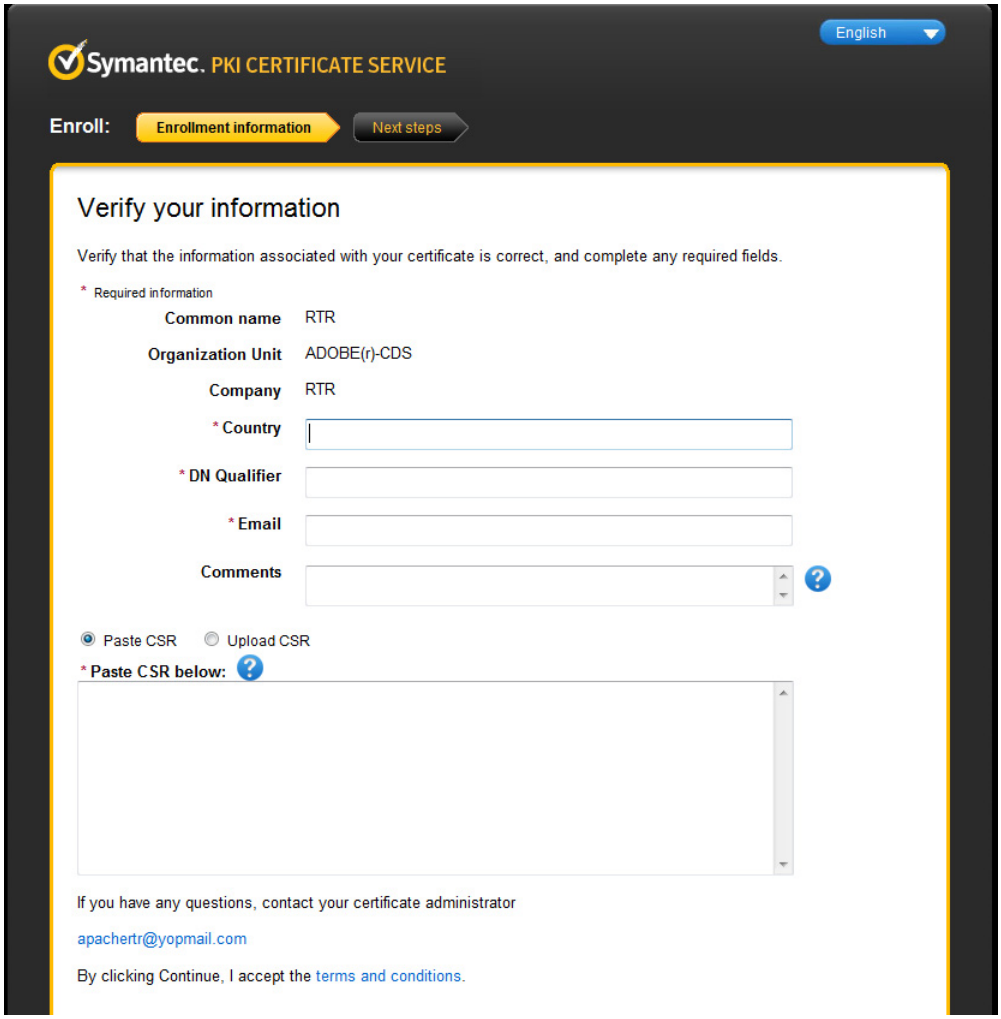

Figure 1-6 Paste CSR

7 Click **Continue**. The request is submitted for approval.

PKI Manager approval

1 Log on to Managed PKI's PKI Manager using your administrator certificate.

2 Click **Manage Users** or select **Managed Users** from the Tasks menu on the bottom navigation bar.

3 Select the pending approval request for Adobe Certificate.

4 Click **Manage this request**.

5 Select **Approved** and click **Save**.

6 Certificate is issued and sent to the registered email ID.

7 Copy the certificate and root in separate files and save them as a `.p7b` extension.

8 After the certificate is saved, import the certificate into the HSM by using the certificate management utility of Luna SA by entering the following command:

```
cmu import -inputFile="<filepath_and_filename_of_cert>" -label="<certificate_label>"
```

9 Verify the imported certificate on the Luna SA by entering the following list command:

```
cmu list
```

The certificate is installed on the HSM. You must configure Adobe LiveCycle Enterprise Suite to use this as a credential to sign the PDF.

Chapter 2

Configuring Partner Products

This chapter discusses how to configure Adobe LiveCycle and Adobe Reader using Managed PKI certificates and sign PDF documents using it.

Setting Up Adobe LiveCycle Enterprise Suite

Adobe LiveCycle can be used to manage the signing process as part of any existing or ongoing workflow in the organization where centralized generation or signing of document content is required and can be easily managed on the server.

Configuring TrustManager on Adobe LiveCycle Enterprise Suite

The following are the steps to configure Adobe LiveCycle Enterprise Suite 4 Server:

1 Log on to the Adobe LiveCycle Administration Console portal using the credentials provided during installation. The Adobe LiveCycle ES4 Home page is displayed.

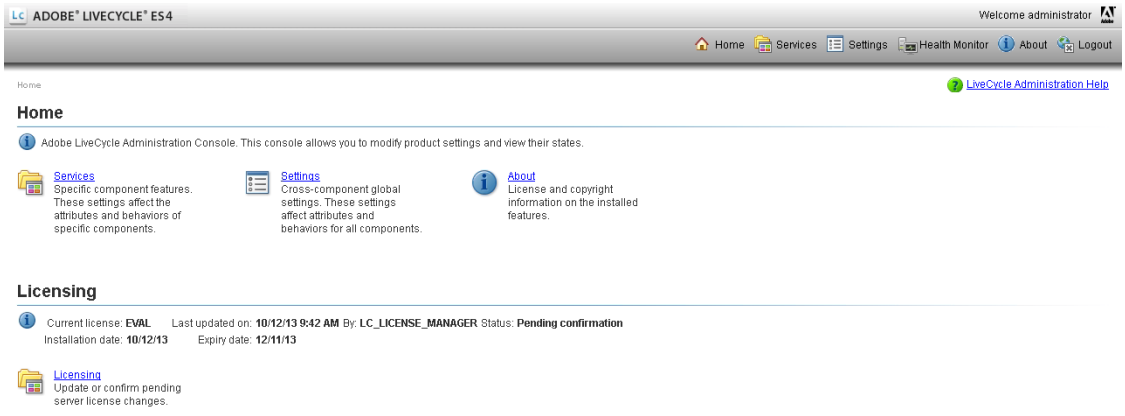

Figure 2-1 Adobe LiveCycle ES4 Home page

2 Click **Settings** and select **Trust Store Management**. The True Store Management page is displayed.

3 Click **HSM Credentials**, then click **Add**. The Add HSM Credential page is displayed.

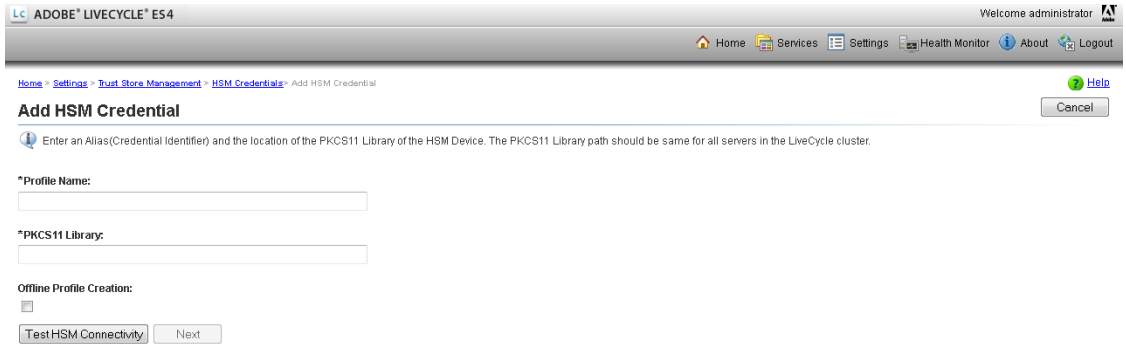

Figure 2-2 Add HSM Credential page

4 Enter the profile name and provide the path for `cryptoki.dll` of LUNA SA client in the PKCS11 Library field.

5 Click **Test HSM Connectivity** to test if HSM is reachable. An acknowledgment message is displayed as confirmation.

The Test HSM Connectivity button is disabled if you select the **Offline Profile Creation** check box.

6 Click **Next**. Select the token name, slot ID, and slot list index and enter the token pin for the slot and click **Next**.

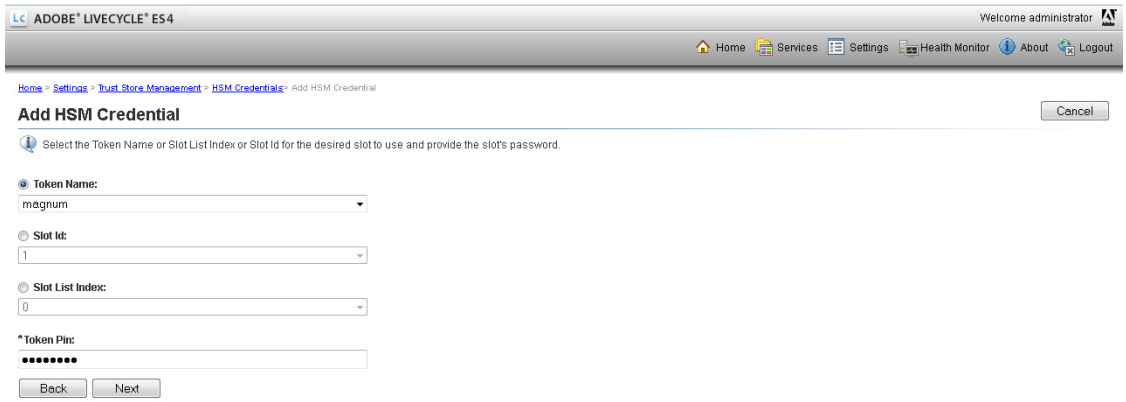

Figure 2-3 Add HSM Credential token details

The HSM connection is established and the available certificates/keys installed on HSM slot are displayed.

7 Select the credential that you want to use while signing the document.

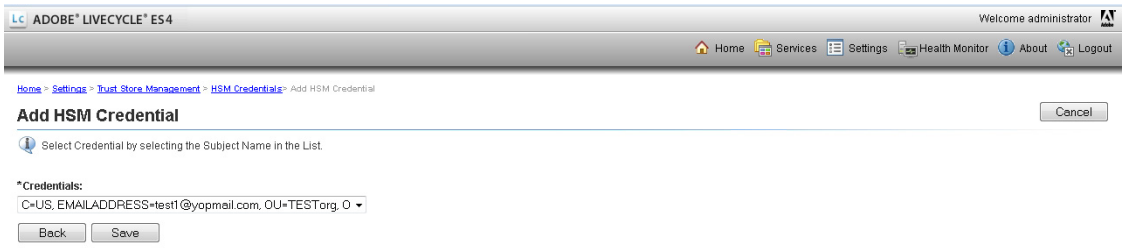

Figure 2-4 Add HSM Credential selection

8 Click **Save**. The HSM Credential page is displayed.

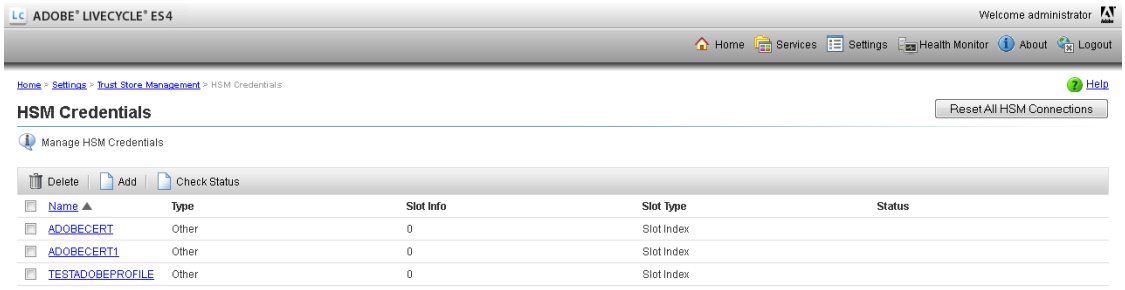

Figure 2-5 Manage HSM Credential

Configuring Adobe LiveCycle Workbench for Signing Process

You must establish a connection with a server (JBoss, WebSphere, WebLogic) while you work on Adobe LiveCycle Workbench. Your administrator must configure your user account and the server so that you can use LiveCycle Workbench. For more information on LiveCycle Workbench, refer to *Adobe documentation*.

Process represents the business processes that you are automating using LiveCycle. Processes are services that run on the LiveCycle server. The following are the steps to create a process:

1 Log on to Adobe LiveCycle Workbench ES4.

2 Click **File** → **New** → **Process** to create an empty process.

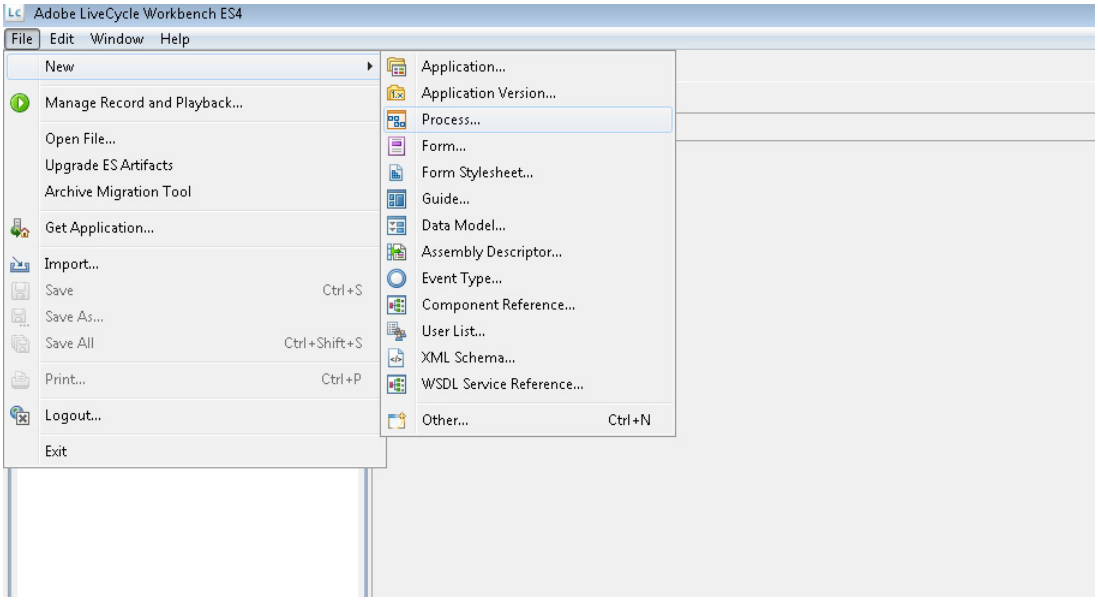

Figure 2-6 New Process

3 Enter a name and description for the process. Enter or select the path to the process location within the application hierarchy and click **Finish**.

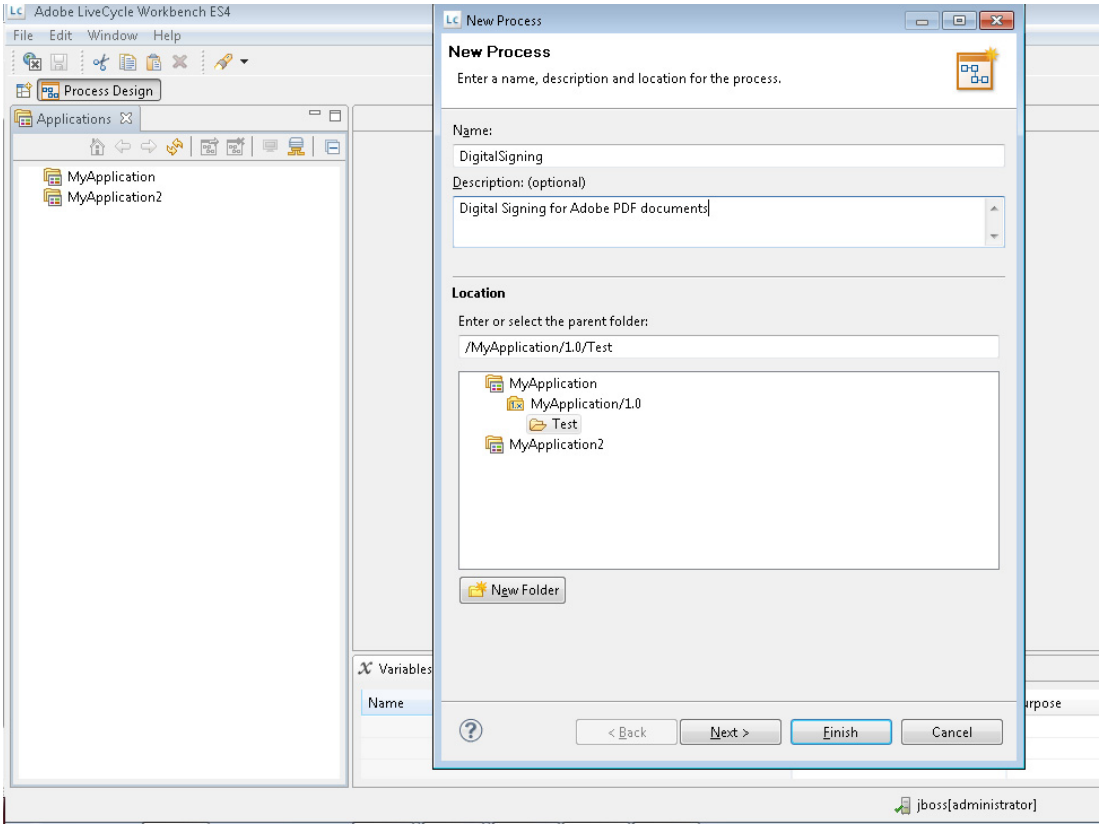

Figure 2-7 New process

4 Select **Activity Picker** from the activity toolbar by dragging and dropping in Default start point.

5 Select **Digital Signatures** and select **Sign Signature Field** and click **OK**.

6 Enter the path for the pdf document in the Input PDF field.

7 Select the credential for signing that was created in "Configuring TrustManager on Adobe LiveCycle Enterprise Suite" on page 9. After the input document is provided, the signature fields are populated.

8 Select the signature field for signing.

9 Complete the required process and click **Save** icon.

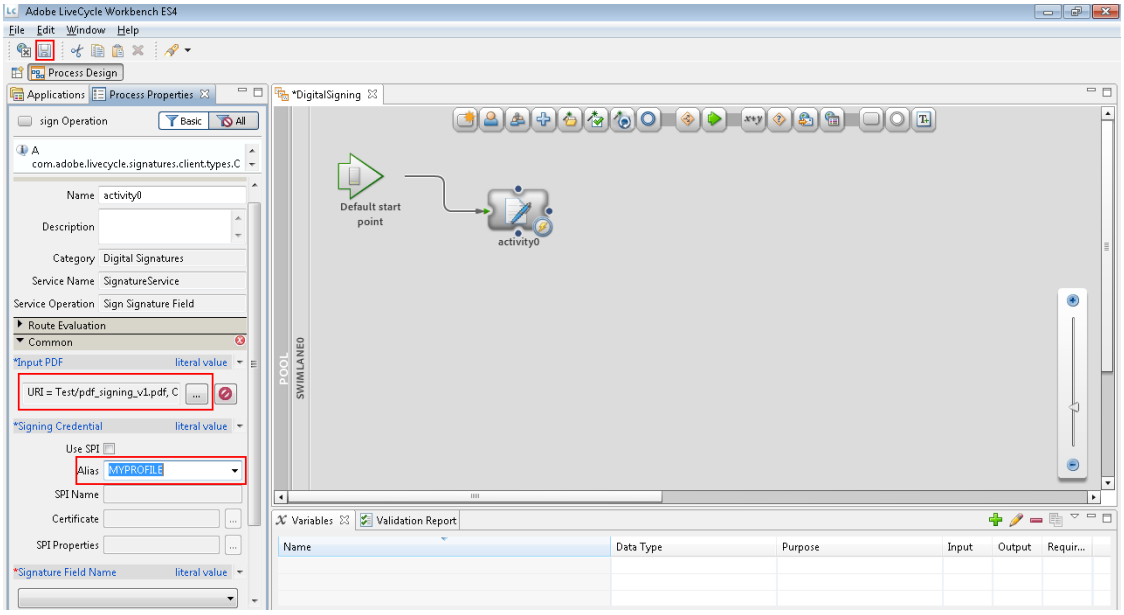

Figure 2-8 Process Design

10 After the process is complete, go to the **Applications** view and select **Deploy** to deploy the application on the server for further usage.

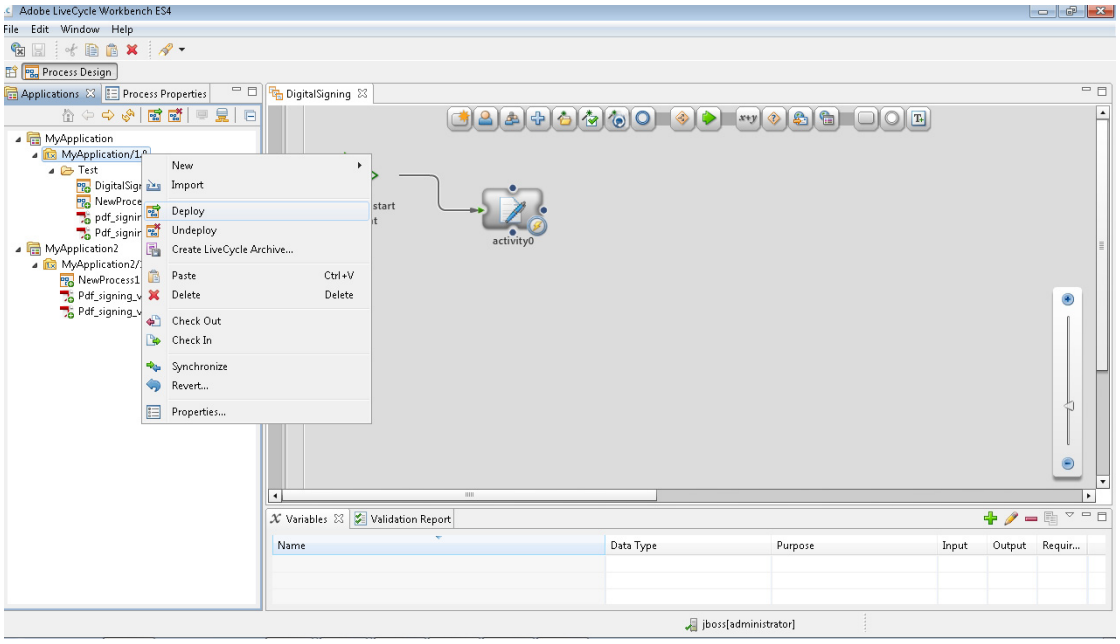

Figure 2-9 Application Deploy

11 Select the files that need to be checked-in and click **OK**. The selected files are deployed.

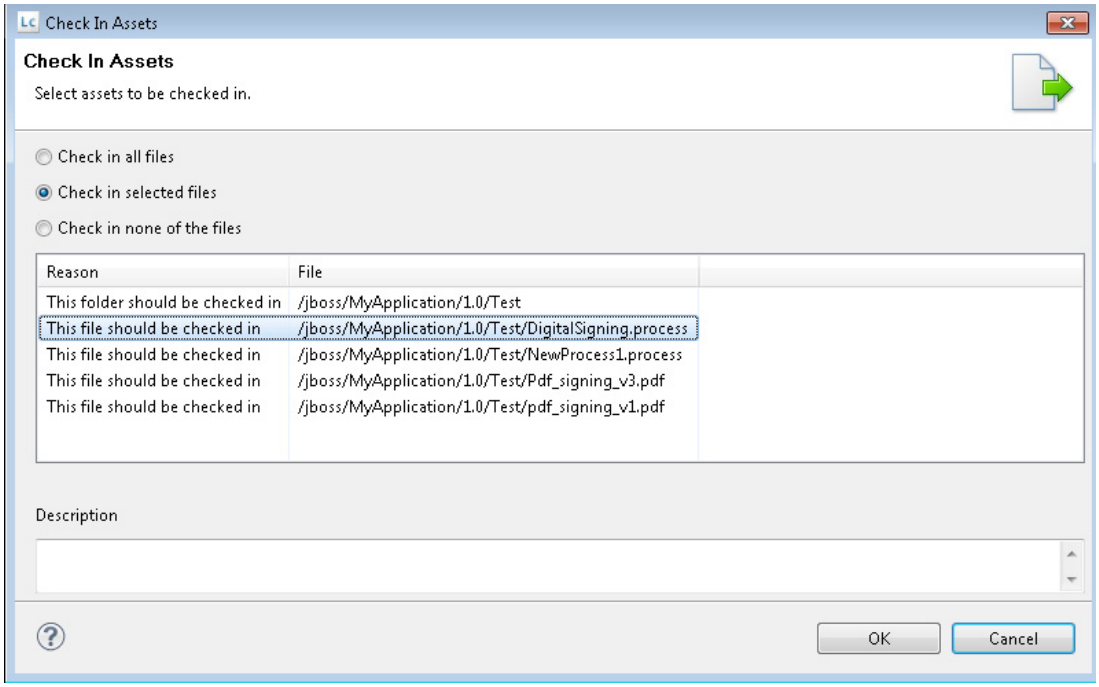

Figure 2-10 Check in files

Setting Up Adobe Reader

Adobe Reader allows you to sign a PDF document based on digital certificates to attest the authenticity and integrity of data exchanged.

Configuring HSM module on the Adobe Reader

Complete the following steps to set up a digital certificate on Adobe Reader XI.

1. Open Adobe Reader XI.
2. Choose **Edit** → **Preferences**.
3. Click **Signatures** from the Preferences dialog box.
4. Click **More** on the Identities & Trusted Certificates under Digital Signature.

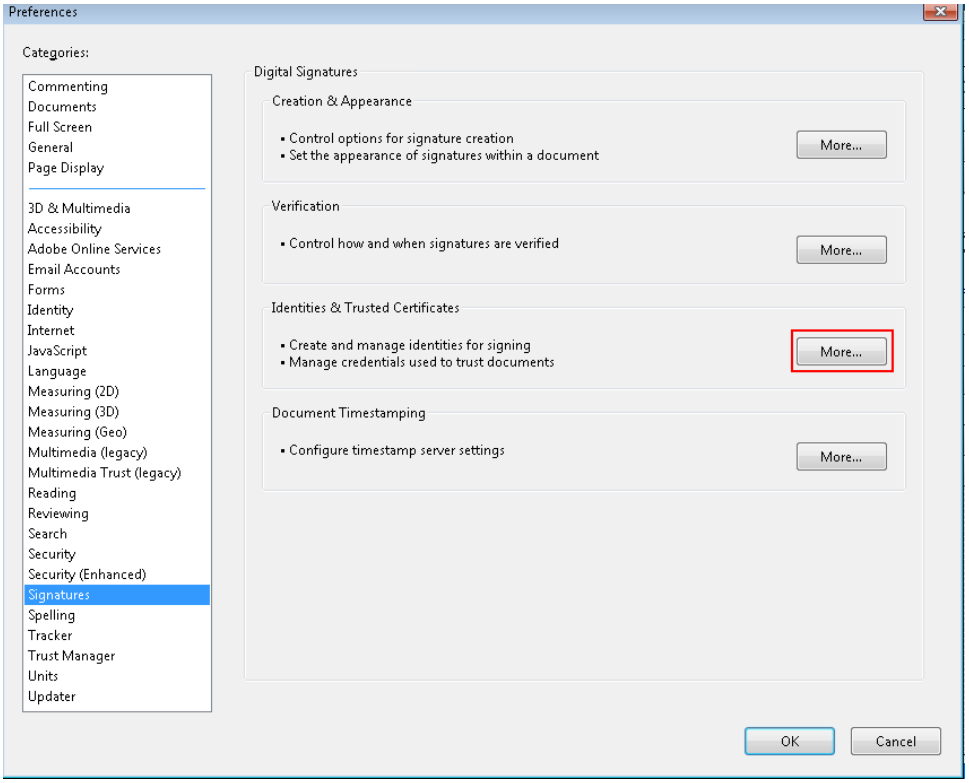

Figure 2-11 Preferences dialog box for Adobe Reader XI

5 Click **PKCS#11 Modules and Tokens** under Digital IDs.

6 Click **Attach Module** to attach a PKCS#11 module (HSM).

7 Browse and select the **cryptoki.dll** of the LUNA SA client. The attached modules are opened.

8 View the list of credentials imported for the module or import from Reader to the module. You can click the partition name to view the details.

9 Select one of the listed IDs for signing or click **Add ID** to choose the certificate from your credential.

10 Click **Usage Options** and select the certificate that you received from Managed PKI and click **Use for Signing**.

11 Click **OK**.

Digitally Signing Documents using Adobe Reader

To digitally sign a PDF document using Adobe Reader XI, follow these steps:

1 Open the PDF document you want to sign.

2 Choose **View** → **Sign**.

3 Select **I Need to Sign** on the Sign panel.

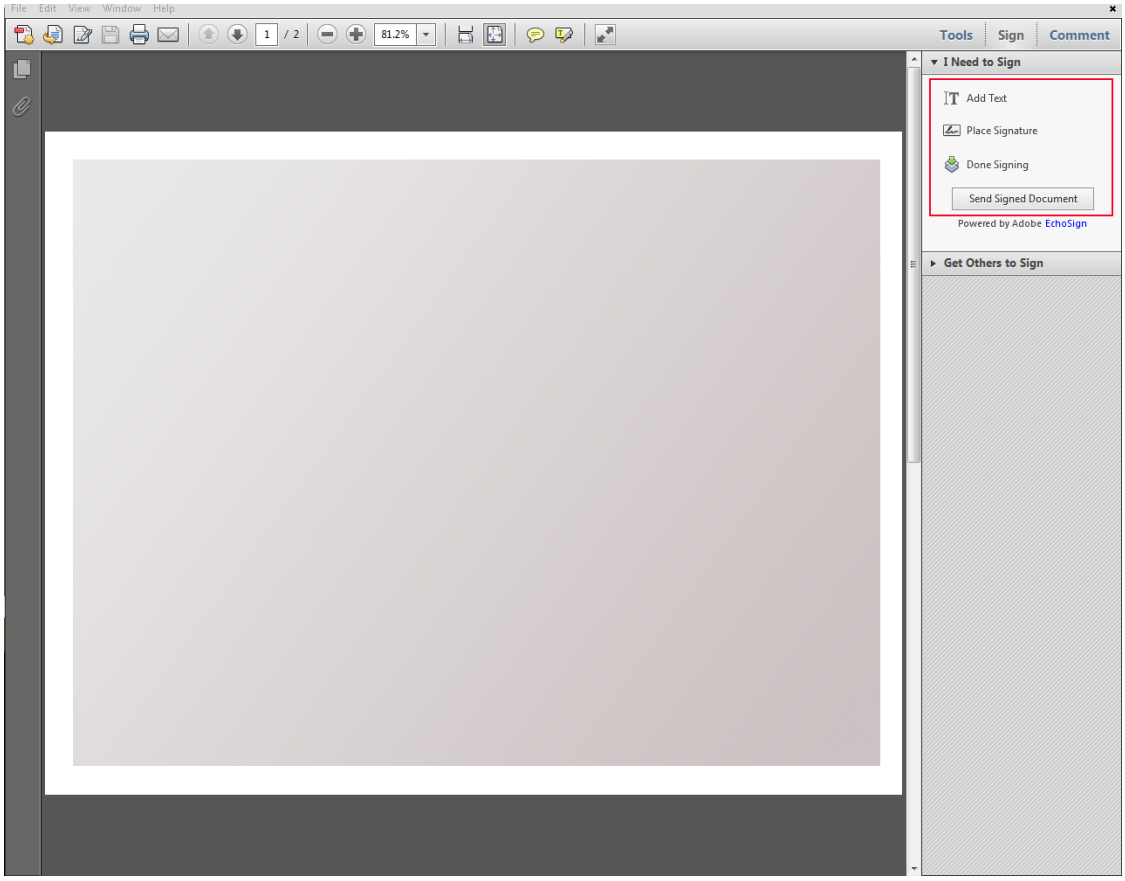

Figure 2-12 Digital Signing

4 Click **Add Text** if you require to add information such as company name, title, date, to name a few.

5 Click **Place Signature**, then click **Drag New Signature Rectangle** to place the signature anywhere in the PDF. Alternatively, you can click on **Sign Here** text box to place the signature.

6 Select the appropriate signature from the **Sign As** field. If you have not configured a default digital signature, Adobe Reader will use the most recently configured digital signature.

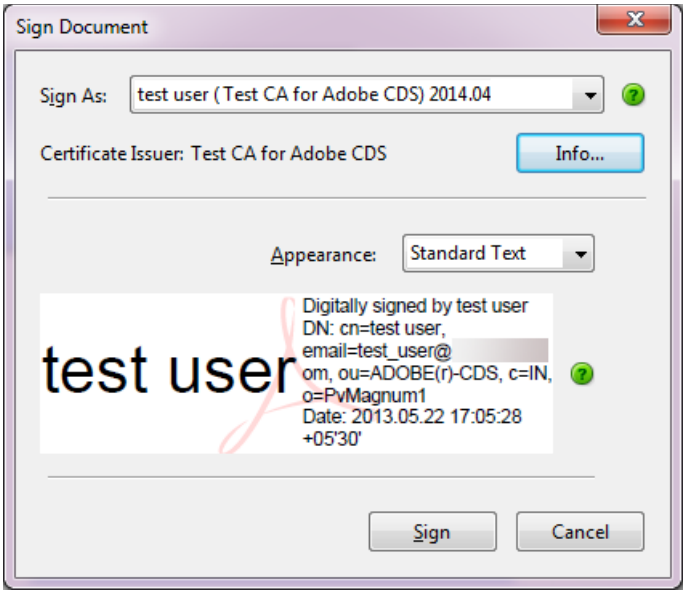

Figure 2-13 Sign Document

You can click **Info** to view the details of a certificate and its entire issuance chain.

7 Click **Sign**. The Adobe Reader will save the document with a different name.