Symantec™ Managed PKI®

Integrating Adobe CDS Certificates with Adobe® Reader®

Symantec

Symantec™ Managed PKI® Integration Guide for Adobe® Reader®

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated January 2, 2015

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 Certificates with 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 device they use, no matter if you have provided their devices or if they are using their own mobile devices.

Symantec Managed PKI's digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from a few to thousands of devices, and its in- the-cloud solution provides quick deployment and easy management while also offering Symantec's industry leading security that is unmatched by in-house PKI solutions.

Symantec's digital certificates for Certified Document Services (CDS) 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 certificate with 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	Adobe® Reader®

The procedures in this guide were tested with Adobe Reader X and XI, but may work with other Adobe versions and products as well. Refer to your product documentation to see if your product supports digital signing.

Prerequisites

- The Adobe CDS end-user-certificate must be stored on an Aladdin hardware credential (eToken). The correct drivers or software must be installed with the Aladdin eToken.
- The author of the PDF must have enabled digital signing when creating the PDF in order for you to sign it.

Integration Architecture

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

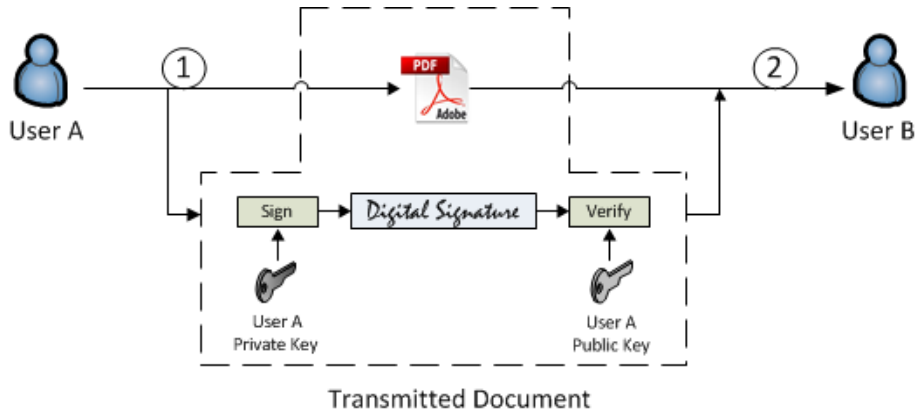

Figure 1-1 Adobe CDS Certificate integration with Adobe Reader

1 User A digitally signs an Adobe PDF document using User A's private key stored on a hardware credential.

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

Integration Workflow

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

Figure 1-2 Managed PKI Integration Workflow

Task 1. Set up your Managed PKI 8.x 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 with 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 Certified Document Services Certificate Profile

Managed PKI uses a certificate profile to define the certificates issued. Certificates issued by Adobe CDS profile support digital signing of PDF documents.

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

1 Log into 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.

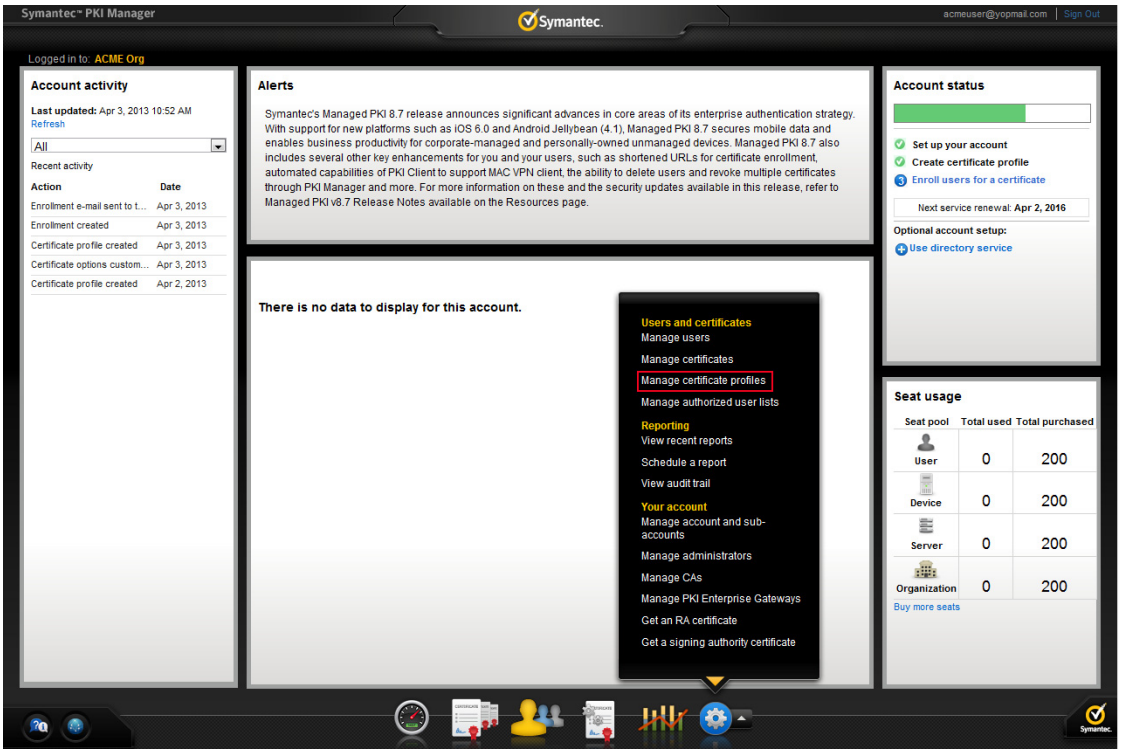

Figure 1-3 Manage Certificate Profile

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** as the certificate template and click **Continue**. The Customize certificate options page appears.

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

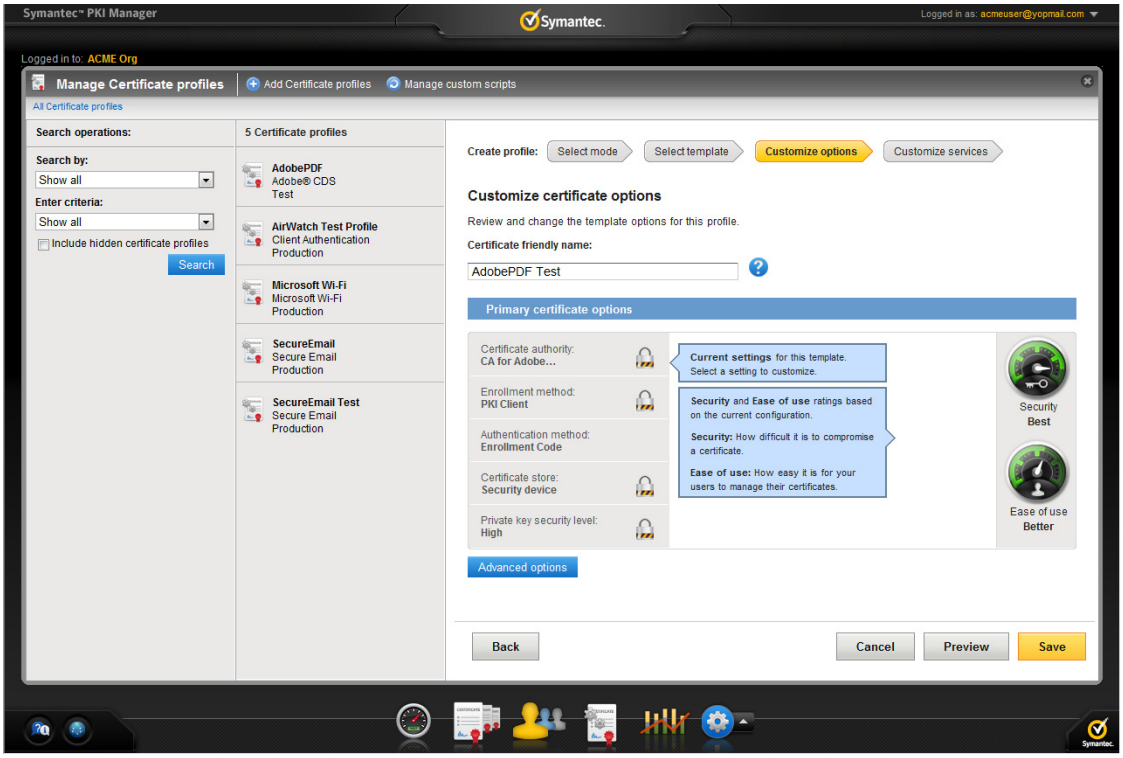

Figure 1-4 Adobe CDS Certificate options

7 Select the appropriate Enrollment method from the following:

- Select **OS/browser** if your user will enroll for certificates using browser.
- Select **PKI Client** if your user will enroll for certificates using PKI Client.
- Select **PKI Web Services** if your user will enroll for certificates using third party applications.

Select the appropriate Authentication method based on your Enrollment method:

- Select **Enrollment Code** to generate a unique enrollment code for each user and to automatically approve certificate requests.
- Select **Active Directory** to automatically approve authorized certificate requests based on data in your enterprise Active Directory.
- Select **Manual approval** to manually approve individual certificate using enrollment pages. After the administrator approves a request, the user is sent an enrollment code for authentication when picking up the certificate.

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

9 Click **Save**.

On the confirmation page, you can view the attribute used for the Seat ID, which is a mandatory attribute for third party configuration or during enrollment process. You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

Task 3. Enroll for an Adobe CDS certificate

You must add the user to PKI Manager before enrolling for a certificate.

1. In PKI Manager, click **Manage users** or select **Manage users** from the Tasks menu on the bottom navigation bar.
2. Click **Add Users** from the top of the resulting Manage users page.
3. Enter the Seat ID (typically the end user's email address) and click **Continue**.
   - Enroll for a single user by entering end user's email address.
   - Enroll for multiple users at one time by uploading a comma-separated value (csv) file with your user data. You can skip step 4 if you are enrolling multiple users using a .csv file.
4. Enter the First Name, Last Name, and select the **I want to enroll this user for a certificate** check box and click **Continue**.
5. Select the Adobe CDS certificate profile and click **Continue**.

   The final enrollment link is displayed to the administrator along with the enrollment code which can be sent to the user for authentication. Symantec recommends that you send the enrollment code separately from the enrollment link, and that you do not send the enrollment code by email.

Task 4. Pick up the Certificate

1. Click the enrollment link in the email.
2. Enter the email address used for enrollment and click **Continue**.
3. Enter the enrollment code provided by the administrator or received in an email and click **Continue**.

   This step authenticates the end user to ensure the correct user is picking up the certificate.
4. Click **Continue**.
5. Insert the Aladdin eToken and click **Install certificate** to install the certificate.
6. Enter the PIN for the certificate store when prompted and click **OK**.

   The certificate is installed on your credential. You must configure Adobe Reader to use this certificate to sign PDF documents. For information on configuring Adobe Reader with Adobe CDS certificate, see "Configuring Adobe Reader" on page 7.

Chapter 2

Configuring Adobe Reader

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

Setting Up Adobe Reader X for Signing

Complete the following steps to set up a digital certificate on Adobe Reader X:

1 Open Adobe Reader X.

2 Choose **Edit → Preferences**.

3 Click **Security** from the Preferences dialog box.

4 Click **Advanced Preferences**.

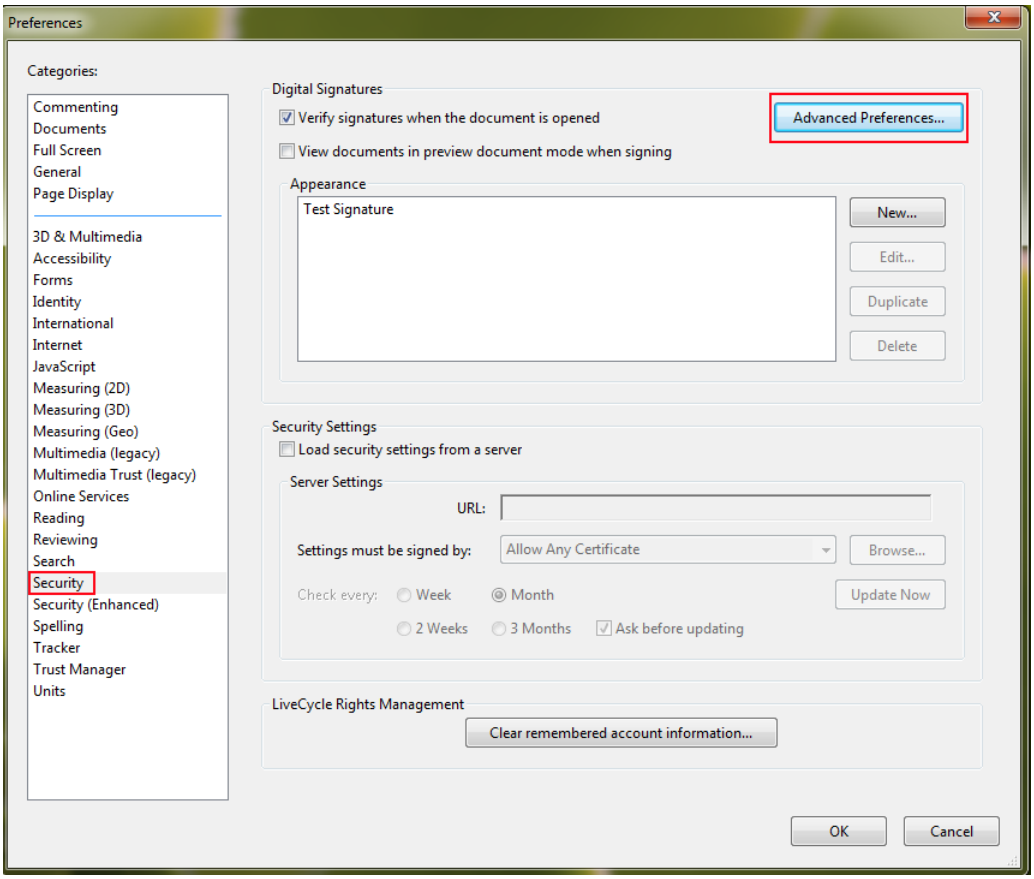

Figure 2-1 Preferences dialog box for Adobe Reader X

5 Click the **Creation** tab from Digital Signatures Advanced Preferences dialog box to view the security options configuration and click **OK**.

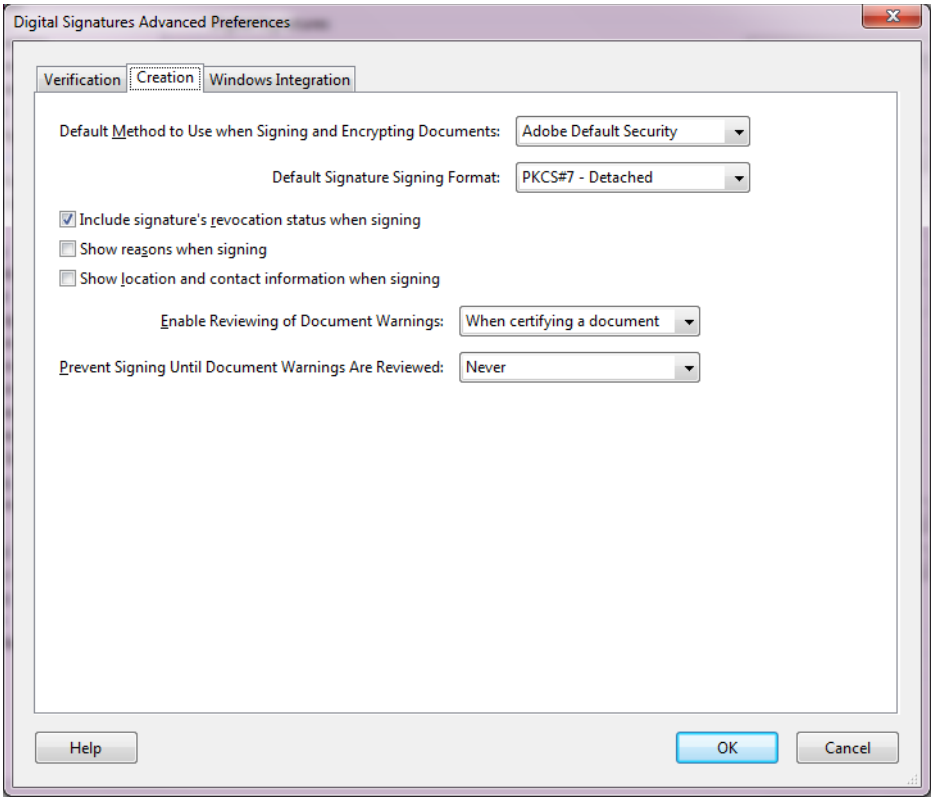

Figure 2-2 Signature Preferences

6 Click **New** in the Digital Signatures Preferences to open the Configure Signature Appearance dialog box.

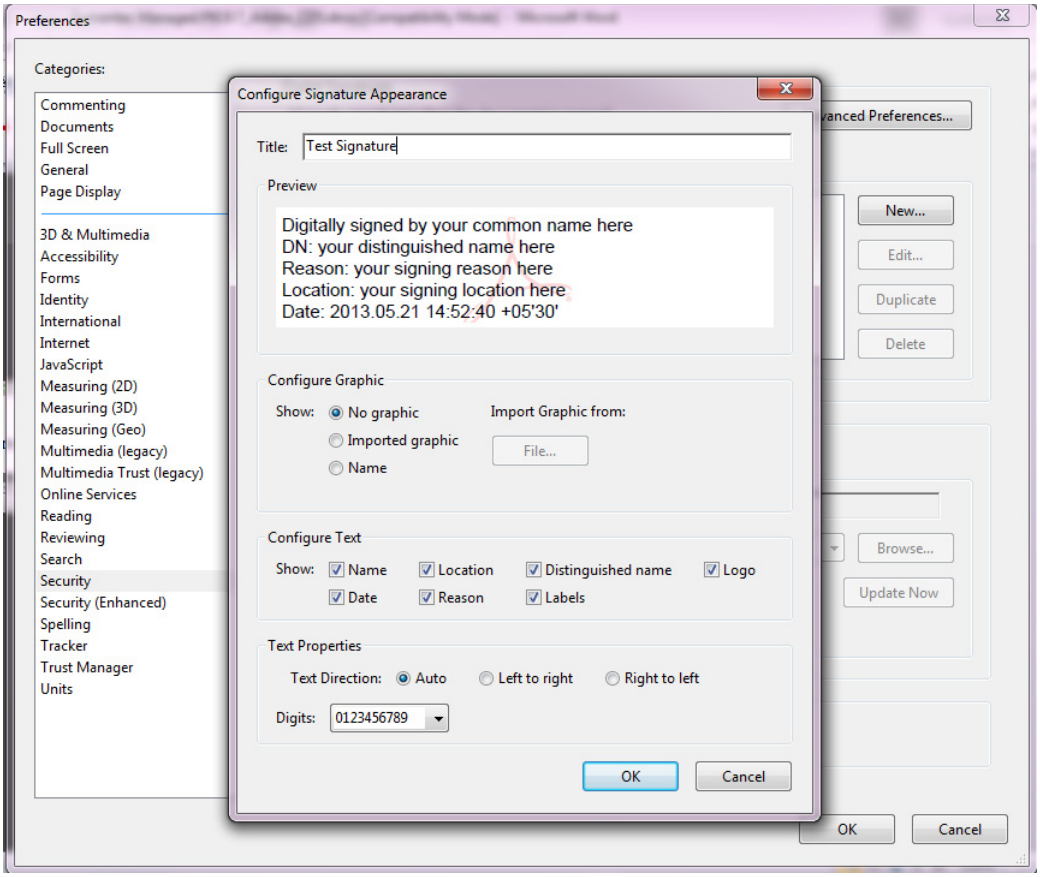

Figure 2-3 Configure Signature Appearance

7 Configure how your signature will appear in the PDF document:

   a Enter a unique name for this signature.

   b Select whether a graphic or your common name will appear next to your signature. You can choose to use no graphic, an image from your file, or the common name from the certificate. To use an image, click **Imported graphic** and click **File** to browse for the image from your machine.

   c In the Configure Text option, specify the text options you want to display. By default, all the text options are selected.

   d In the Text Properties option, specify the text property option you want to display. By default, **Auto** option is selected.

   e Click **OK**.

8 Select **Local security settings from a server** under Security Settings.

9 Select the digital certificate that you received from Managed PKI in the **Settings must be signed by** drop-down list. If the certificate is not displayed in the drop-down list, click **Browse** to choose the certificate from your credential. The selected certificate is used for signing all the documents.

10 Click **OK**.

Setting Up Adobe Reader XI for Signing

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.

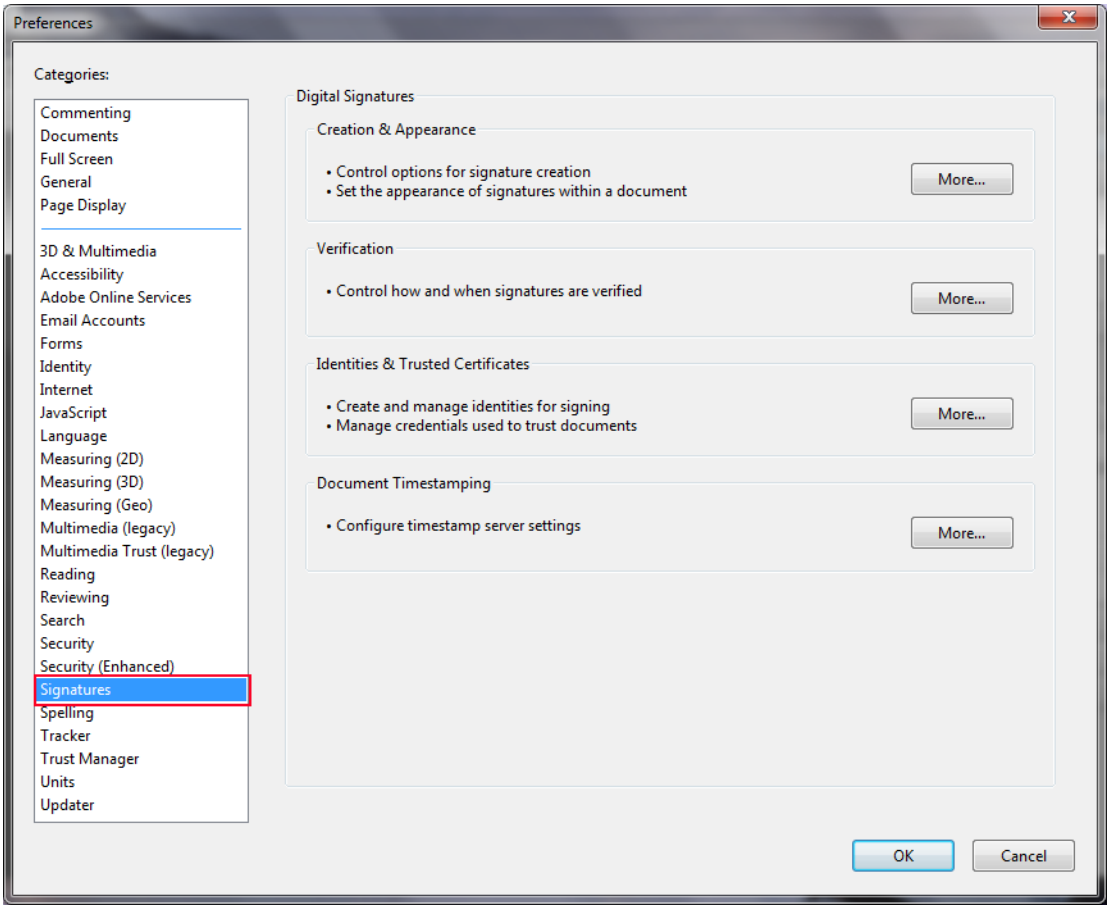

Figure 2-4 Preferences dialog box for Adobe Reader XI

4 Click **More** on the Creation and Appearance menu under Digital Signatures to view the security options configuration.

5 Click **New** in the Creation and Appearance Preferences to open the Configure Signature Appearance dialog box.

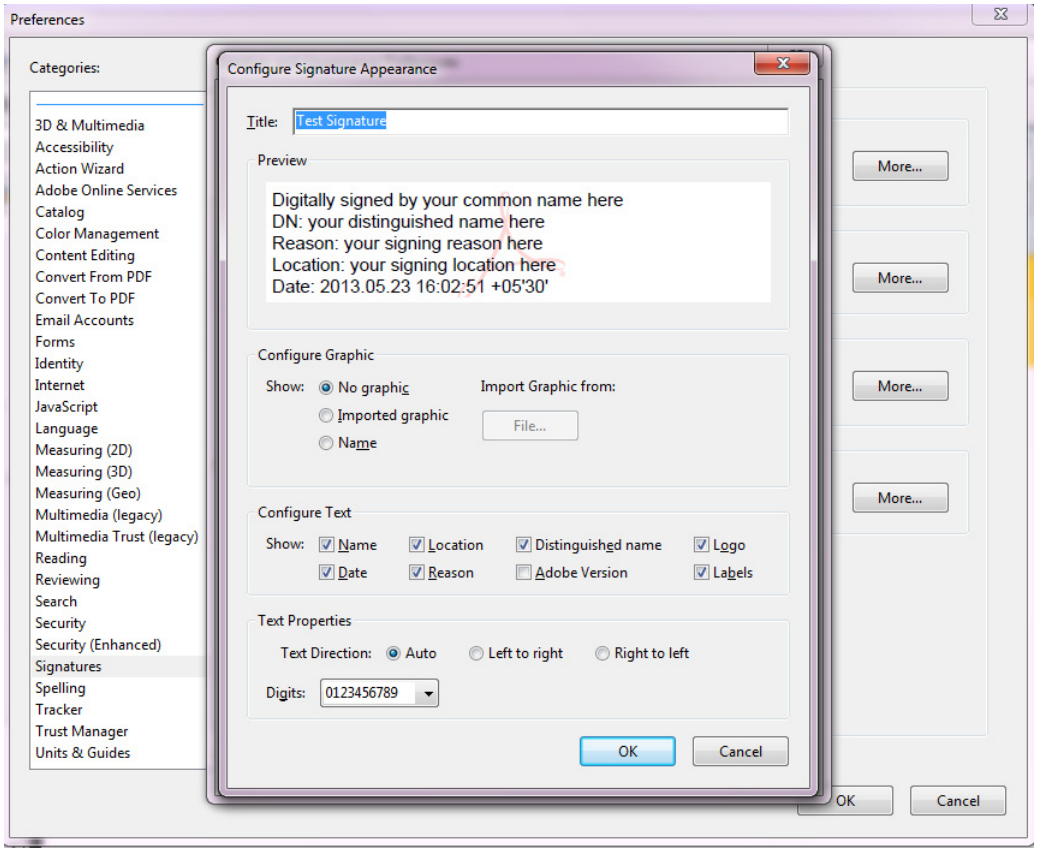

Figure 2-5 Configure Signature Appearance

6 Configure how your signature will appear in the PDF document:

   a Enter a unique name for this signature.

   b Select whether a graphic or your common name will appear next to your signature. You can choose to use no graphic, an image from your file, or the common name from the certificate. To use an image, click **Imported graphic** and click **File** to browse for the image from your machine.

   c In the Configure Text option, specify the text options you want to display. By default, all the text options are selected.

   d In the Text Properties option, specify the text property option you want to display. By default, **Auto** option is selected.

   e Click **OK.**

7 Click **More** on the appropriate menu under Digital Signature to configure when and how a signature is used, how a signature is verified, and whether a timestamp is added.

8 Click **More** on the Identities & Trusted Certificates under Digital Signature to select the certificate that you received from Managed PKI. If the certificate is not displayed, click **Add ID** to choose the certificate from your credential.

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

10 Click **OK**.

Digitally Signing Documents using Adobe Reader

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

1 Open the PDF document you want to sign.

Note: The author of the PDF must have enabled digital signing when creating the PDF in order for you to sign it.

2 Choose **View** → **Sign**.

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

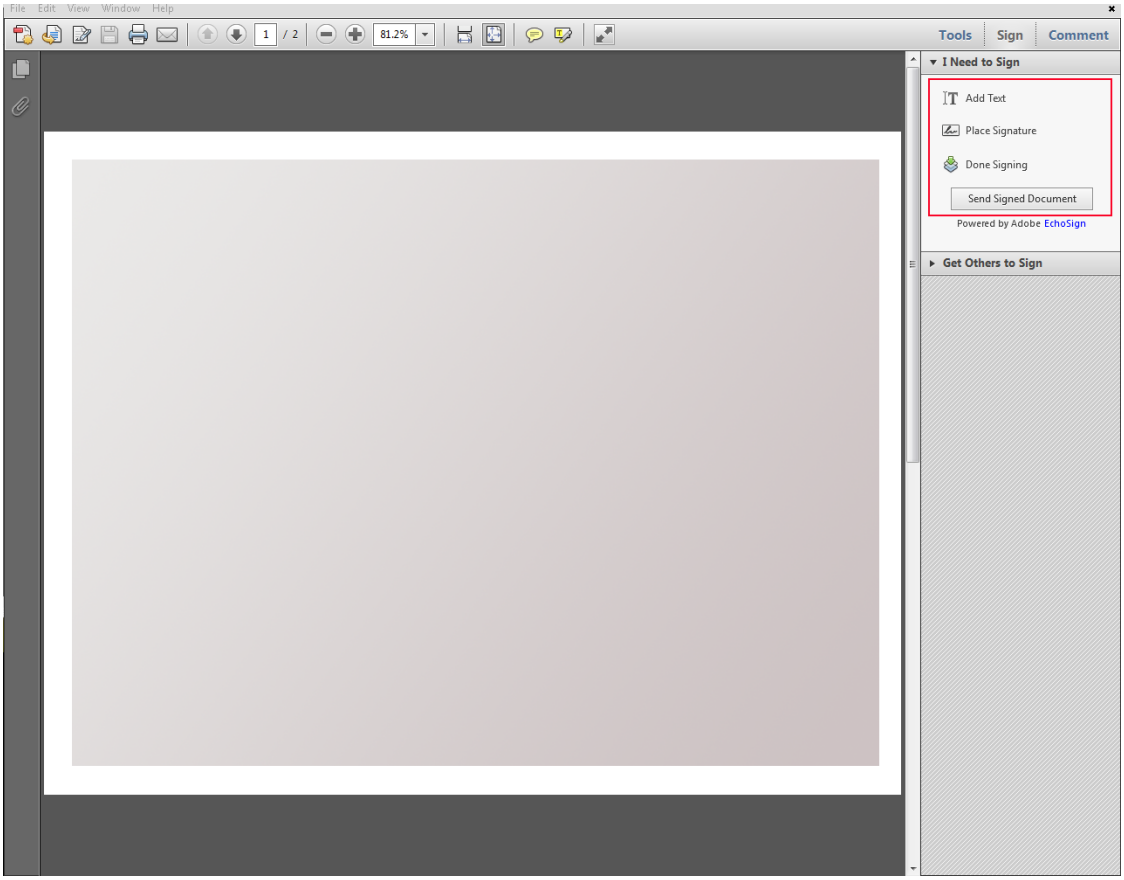

Figure 2-6 Digital Signing

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.

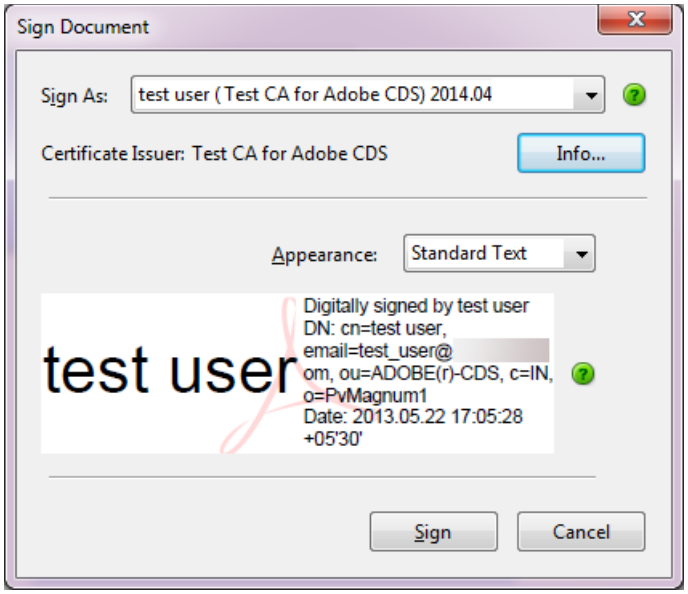

Figure 2-7 Sign Document

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.

8 Enter the PIN for the certificate store (eToken) when prompted and click **OK**. The document is signed with the selected signature.

If you have not specified a timestamp server for the digital signature, Adobe will create a timestamp for the digital signature using your local machine's time and date.

Validate Digital Signature

You can validate a digital signature by verifying the signature properties:

1 Open the PDF that has the signature.

2 Right-click the signature and click **Validate Signature**. The Signature Validation Status displays the validity of the signature.

3 Click **Signature Properties**.

4 If the status is unknown, a validity unknown icon is displayed.

Figure 2-8 Unknown Signature Status

a Click the **Signer** tab, and click **Show Certificate** to view the details of the certificate.

b Click the **Trust** tab, and click to **Add to Trusted Identities** and click **OK**.

5 If the signature is valid, a trusted certificate icon is displayed.

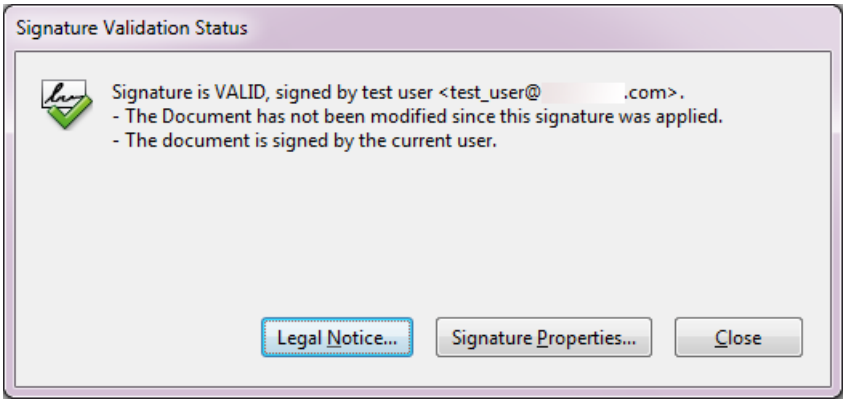

Figure 2-9 Valid Signature Status

Enabling Adobe Reader for Online Certificate Status Protocol

A certificate must be validated when a user or device authenticates using the certificate. Symantec's Managed PKI certificates provide certificate validation tools such as Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL). All Adobe Acrobat and Adobe Reader versions 7.x and higher support OCSP validation.

Certificate validation may occur automatically based on the configuration of your application. Adobe Reader validates OCSP URL that is part of a certificate's Authority Information Access (AIA) extension. During validation, Adobe Reader verifies for CRL and OCSP validation. Adobe Reader also verifies how it scales back if OCSP responder is not reachable. The browsers such as Firefox and Chrome validate the certificate even if OCSP fails for non-EV certificates.

Note: Adobe Acrobat and Adobe Reader versions 9.x and lower cannot process the OCSP validation if the OID value in a certificate is very large in length. No revocation check is performed on these certificates. Adobe Acrobat and Adobe Reader versions 10.x and higher include a fix to handle large OID values for certificate parsing.

Symantec issued certificates does not contain long OID values. Because of the optimal size of Symantec's OID values, the OCSP validation for Symantec issued CDS certificates work with Adobe Acrobat and Adobe Reader versions 7.x and higher.

Adobe Acrobat and Adobe Reader perform revocation locally before it proceeds with OSCP revocation. If the CRL issued by Symantec Shared CA is already in the local cache, then Adobe Acrobat and Adobe Reader uses it before going online to send an OCSP request (and thus wait for the OCSP response).

To verify the certificate's revocation status on Windows Vista/Windows 7 or later, follow these steps:

1. Close the pdf.
2. Go to **C:\Users\<user_name>\AppData\Roaming\Adobe\Acrobat\<latest_version>\Security\CRLCache** and delete the contents.
3. Relaunch Acrobat and verify the revocation status.