Entrust Certificate Services

Using Certificates for Adobe CDS

Getting Started Guide

Date of issue: November 2010

Entrust®
Securing Digital Identities
& Information

Copyright © 2009-2010 Entrust. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.

TOC

About this guide 5

Documentation conventions 6
Note and Attention text 6
Related documentation 7
Obtaining documentation 8
Documentation feedback 8
Obtaining technical assistance 9
Technical support 9
Professional Services 10

Installing and using your Entrust certificate on a token 11

Before you start 12
Installing and initializing your token 13
Installing the token drivers 13
Installing the token software 17
Initializing the token 21
Logging in to your token 25
Changing your token passphrase 28
Storing the Entrust certificate on your token 30
Recovering a certificate 32

Signing and certifying PDF documents with your certificate 33

Signing and certifying a PDF document 34
Adding a signer to the trusted list 44
Setting signature verification preferences 49

About this guide

This guide describes how to store an Entrust certificate on an iKey 4000 or 2032 token. This includes:

- installing your token (drivers and software)
- enrolling your token
- accessing the Entrust Certificate Retrieval Web pages to store the certificate on your token

This guide also provides basic instructions on how to sign and/or certify a PDF file or form and how to set signature validation preferences. For more advanced features, see the Adobe documentation.

Note: To navigate through this PDF, you can use the arrow buttons in the menu bar of Adobe Reader.

Documentation conventions

The following documentation conventions are used in Entrust guides:

Table 1: Typographic conventions

Convention	Purpose	Example
Bold text (other than headings)	Indicates graphical user interface elements and wizards.	Click **Next**.
Italicized text	Used for book or document titles.	*Entrust Certificate Services Enrollment Guide*
Blue text	Used for hyperlinks to other sections in the document.	Entrust TruePass supports the use of many types of digital ID.
Underlined blue text	Used for Web links.	For more information, visit our Web site at www.entrust.net.
`Courier` type	Indicates installation paths, file names, Windows registry keys, commands, and text you must enter.	Use the `entrust-configuration.xml` file to change certain options for Verification Server.
Angle brackets < >	Indicates variables (text you must replace with your organization's correct values).	By default, the `entrust.ini` file is located in `<install_path>/conf/security/entrust.ini`.

Note and Attention text

Throughout this guide, there are paragraphs set off by ruled lines above and below the text. These paragraphs provide key information with two levels of importance, as shown below.

Note: Information to help you maximize the benefits of your Entrust product.

Attention: Issues that, if ignored, may seriously affect performance, security, or the operation of your Entrust product.

Obtaining technical assistance

Entrust recognizes the importance of providing quick and easy access to our support resources. The following subsections provide details about the technical support and information available to you.

Technical support

For Entrust technical support services, visit our Web site at:

http://www.entrust.net/ssl-technical/index.htm

For technical resources including a comprehensive Knowledge Base visit:

http://www.entrust.net/knowledge-base/index.cfm

Telephone numbers

For support assistance by telephone call one of the numbers below:

- 1 (866) 267-9297 (toll free within North America)
- 1 (613) 270-2680 (outside North America)

Email address

The email address for Customer Support is:

ssl@entrust.com

Related documentation

This section describes related reading material that may be used in conjunction with this guide.

- Entrust Certificate Services Adobe CDS Individual Enrollment Guide
- Entrust Certificate Services Adobe CDS Group Enrollment Guide
- Token software information (http://www.safenet-inc.com)

Documentation feedback

You can rate and provide feedback about Entrust product documentation by completing the online feedback form. Any information that you provide goes directly to the documentation team and is used to improve and correct the information in our guides. You can access this form by:

- clicking the *Report any errors or omissions* link located in the footer of Entrust's PDF documents (see bottom of this page).
- following this link: http://www.entrust.com/products/feedback/index.cfm

1

Installing and using your Entrust certificate on a token

This chapter describes how to enroll your token and install your Entrust certificate on your token. This guide assumes that you have already purchased a CDS signing certificate.

This chapter includes the following sections:

- "Before you start" on page 10
- "Installing token software and enrolling a token" on page 11
- "Changing the password for your token" on page 21
- "Picking up your Entrust certificate" on page 23
- "Recovering a certificate" on page 27

Before you start

In order to securely sign or sign and certify a PDF document using a certificate stored on a token, you require the following:

- A supported browser with Internet access
- An iKey 4000 or 2032 token
- The email message that was sent to you after you purchased the certificate, containing the link to the Entrust Certificate Retrieval Web pages

Report any errors or omissions

Installing token software and enrolling a token

Topics in this section include:

- "Downloading and installing the token software" on page 11
- "Enrolling a token" on page 17

Downloading and installing the token software

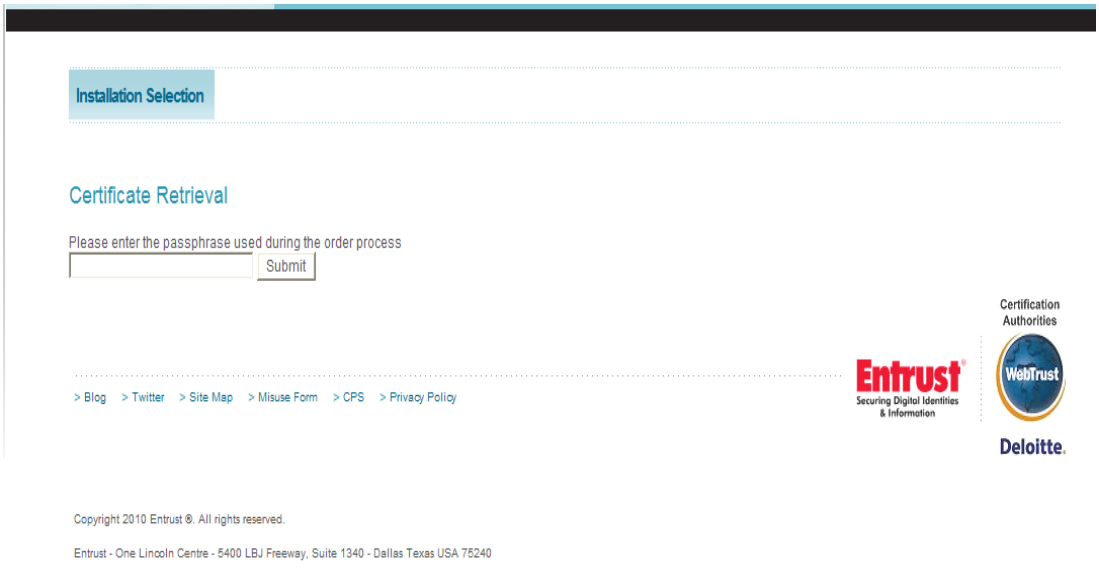
In order to manage your token, including tasks such as logging in, initializing, and resetting your password, you must download and install the token software provided by Entrust.

Complete the following procedure to obtain and install the token software.

To obtain and install the token software

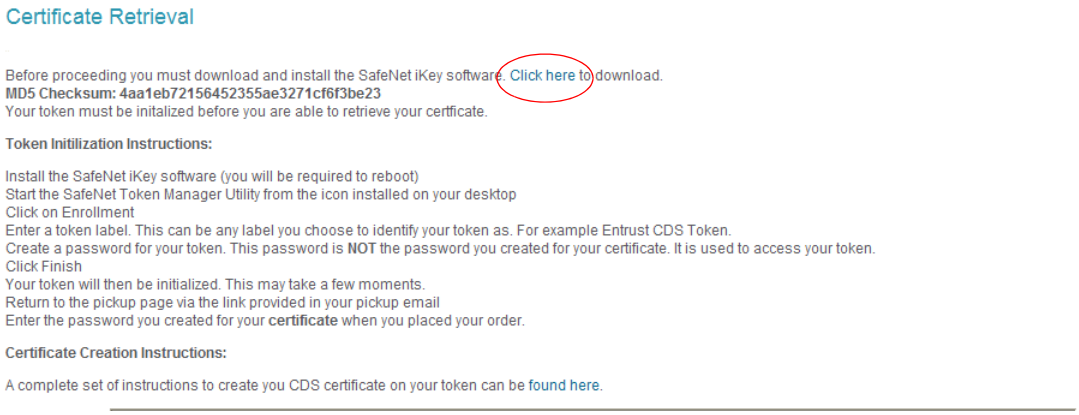
1. Click the link to the Entrust Certificate Retrieval Web pages in the notification email sent to you by Entrust.

   The Entrust Certificate Retrieval log-in page appears.



2. Log in to the page using the passphrase issued to you by Entrust and click **Submit.**
3. In the **Certificate Retrieval** page, use the **click here** link to begin downloading the token software.

Note: The software available on the retrieval Web site is works with Microsoft Windows 2000, 2003, XP and Vista. Contact Entrust Certificate Services support to obtain software compatible with Windows 7.



Certificate Retrieval

Before proceeding you must download and install the SafeNet iKey software. Click here to download.
MD5 Checksum: 4aa1eb72156452355ae3271cf6f3be23
Your token must be initalized before you are able to retrieve your certficate.

Token Initilization Instructions:

Install the SafeNet iKey software (you will be required to reboot)
Start the SafeNet Token Manager Utility from the icon installed on your desktop
Click on Enrollment
Enter a token label. This can be any label you choose to identify your token as. For example Entrust CDS Token.
Create a password for your token. This password is **NOT** the password you created for your certificate. It is used to access your token.
Click Finish
Your token will then be initialized. This may take a few moments.
Return to the pickup page via the link provided in your pickup email
Enter the password you created for your **certificate** when you placed your order.

Certificate Creation Instructions:

A complete set of instructions to create you CDS certificate on your token can be found here.

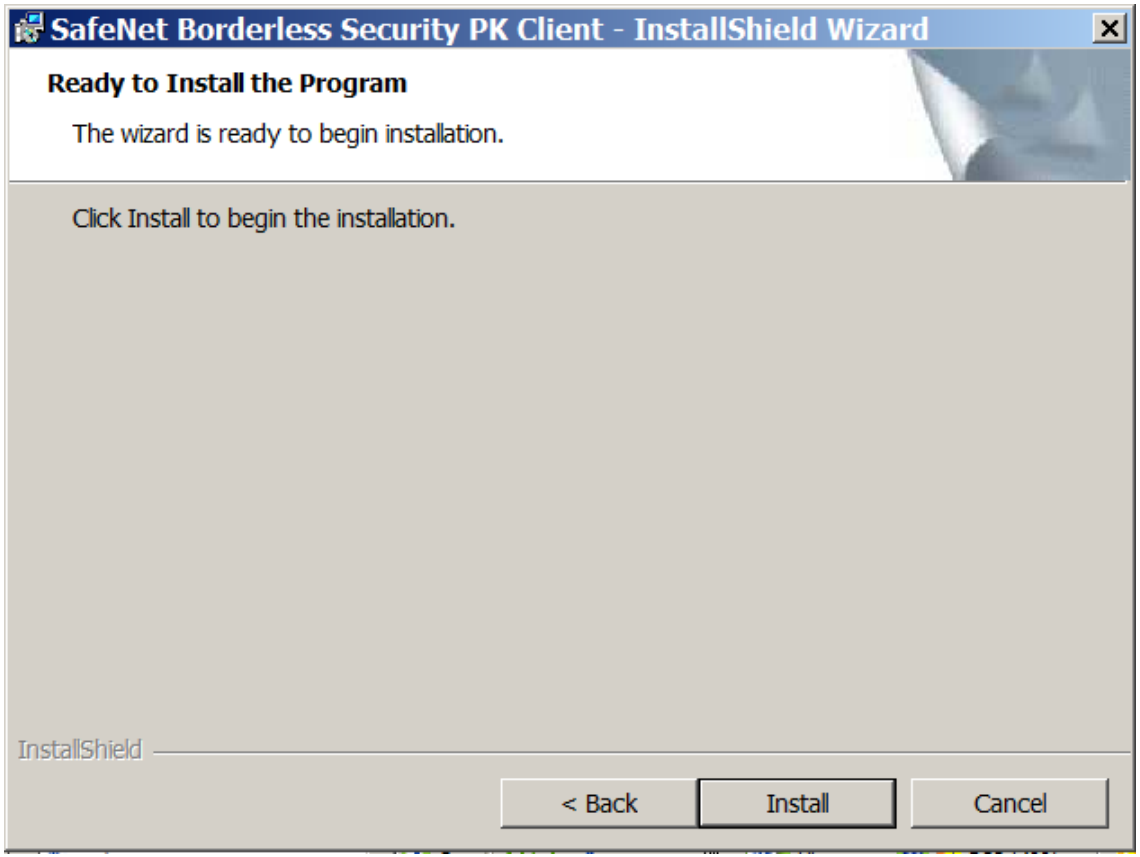
4. Save the software to your machine.
5. Click the `EntrustCDSikeyInstaller-<number>.msi` file from the Web site.

   The **InstallShield Wizard** appears.

Report any errors or omissions

6 Click **Next**.

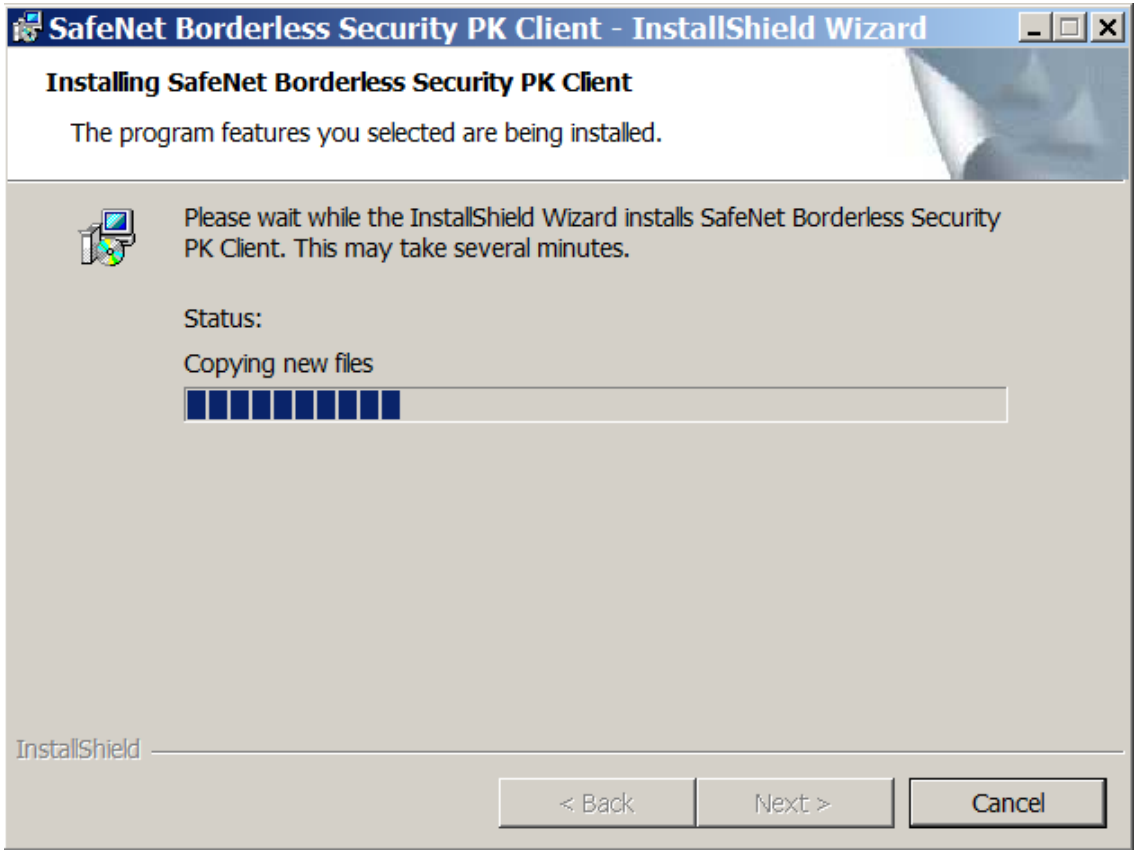
The **Ready to Install the Program** screen appears.



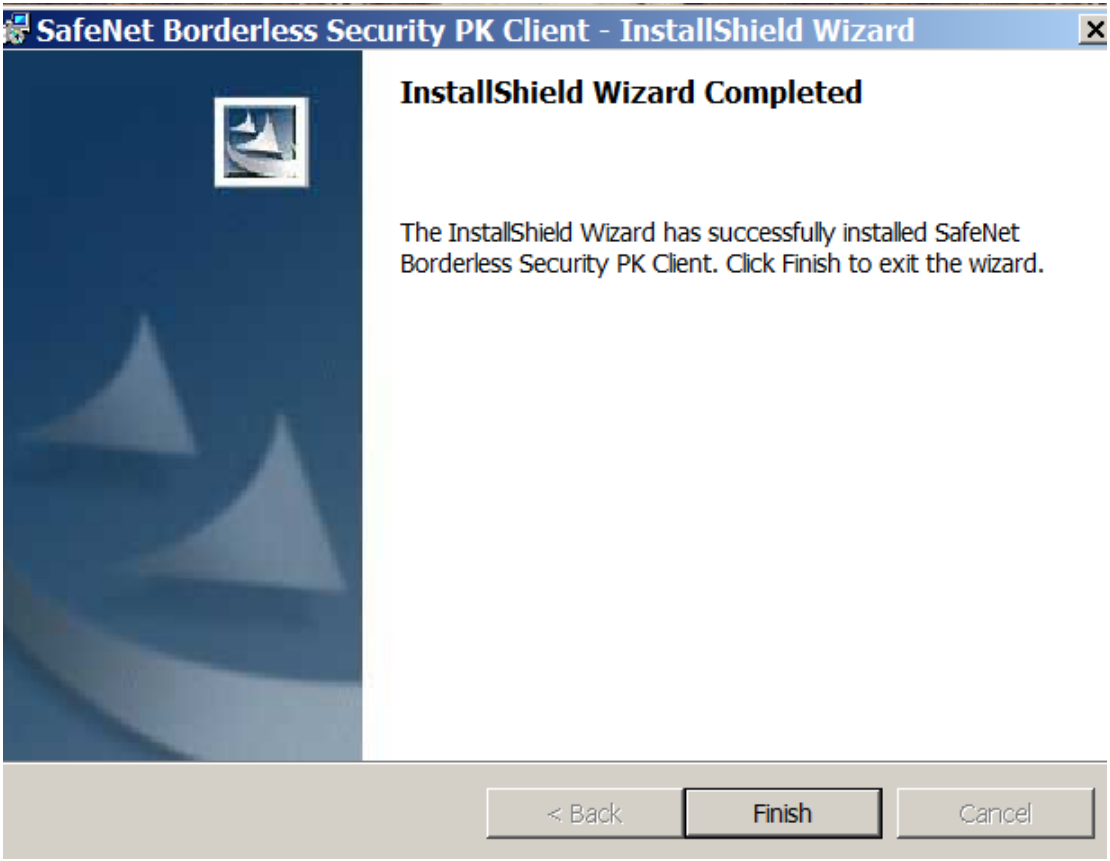
7 Click **Install**.

Report any errors or omissions

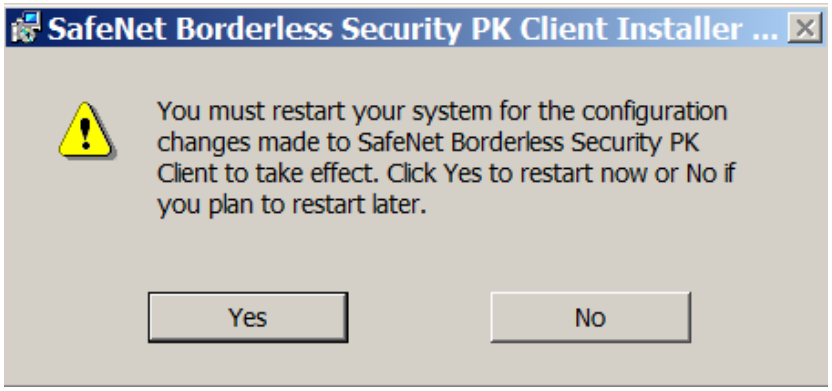
The wizard begins to configure your software installation. This may take a few moments.



8 Once configured, a success message appears. Click **Finish**.



9 A message appears prompting you to restart your system. Click **Yes** to reboot now.



Report any errors or omissions

Your system reboots.

You have successfully installed the token software. You must enroll the token before picking up your certificate.

Enrolling a token

You must enroll a new token before it can store your Adobe signing certificate.

Note: If your token is not new, or you have already personalized it, enrollment is not required.

Complete the following procedure to enroll your token.

To enroll your token

1. Insert your token into a USB slot on your machine.
2. Open the **Token Manager Utility** application. Click **Start** > **All Programs** > **SafeNet** > **Borderless Security PK** > **SafeNet Token Manager Utility**.

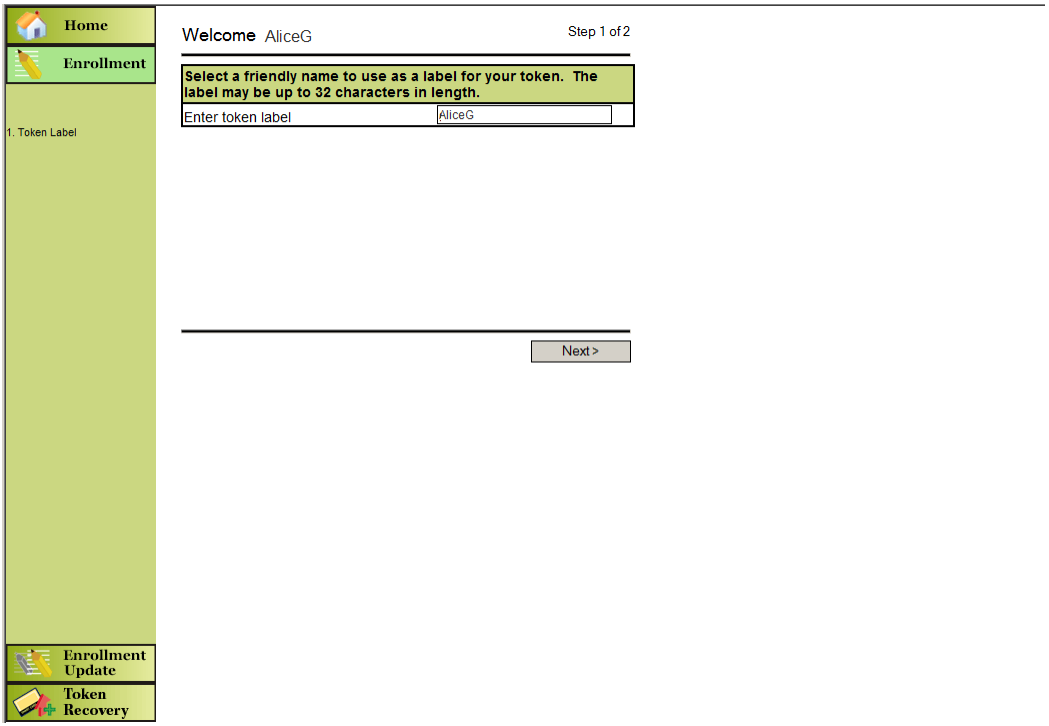
The **Token Manager Utility** application appears.

3 Click **Enrollment**.

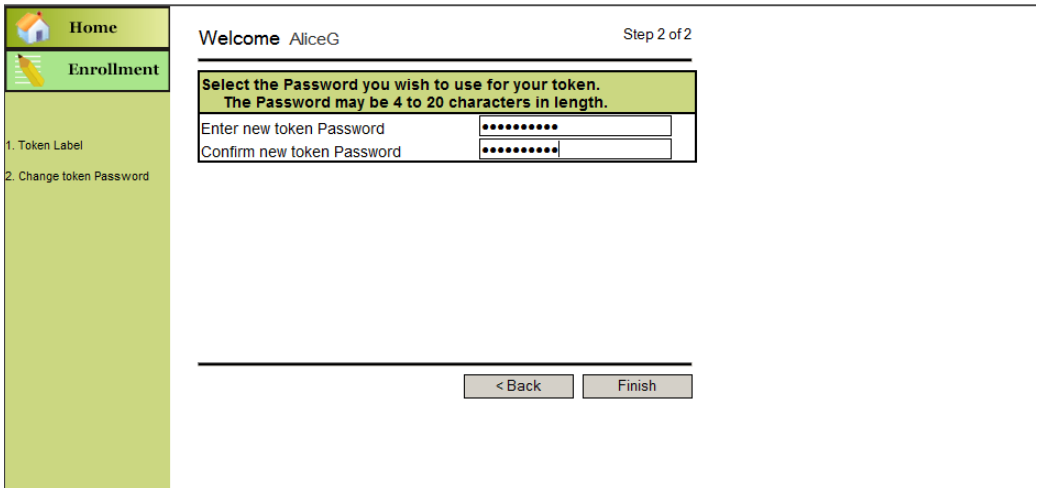
Depending on your browser configuration, you may get a warning massage. Allow the Active X control to run.

Report any errors or omissions

4 In the **Welcome** page, select a friendly name for your token or accept the default. Click **Next**.



5 Enter and confirm a password for the token. It is important to to use a password that you will remember. Do not use a password that is easily guessed or broken.

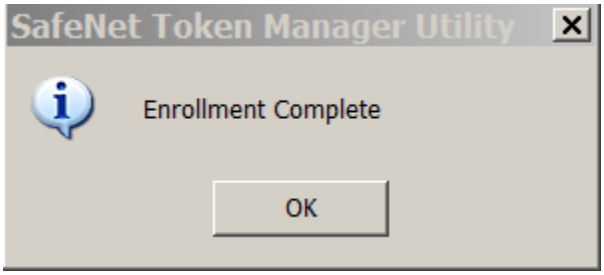


6 Click **Finish**.

The enrollment process begins.

When the enrollment is complete, the software displays a success message.

7 Click **OK**.



The **Login** dialog box appears.

You successfully enrolled your token.

Report any errors or omissions

Changing the password for your token

Complete the following procedure to change the password for your token.

Attention: If you forget your password, you must initialize your token. Initializing your token deletes its contents including certificates and keys.

To change your token password

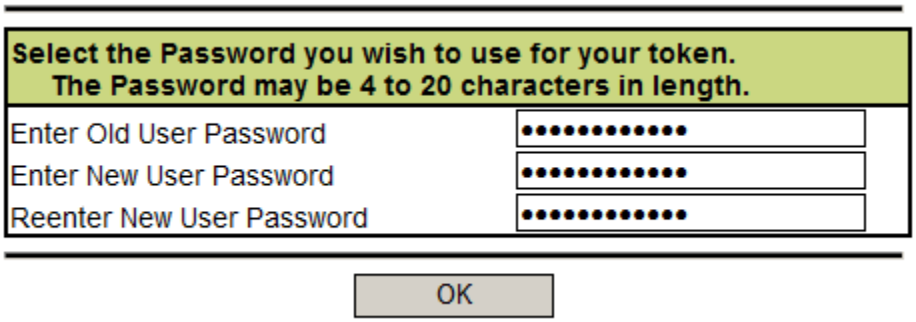
1. Insert your token into a USB slot on your machine.
2. Open the **Token Manager Utility** application. Click **Start** > **All Programs** > **Safenet** > **Borderless PKI Security** > **Token Manager Utility**.

   The **Token Manager Utility** application appears.

3. Click **Enrollment Update**.

4 In the left menu column select **Change token Password**.

5 Complete the following and click **OK**:



a Enter your current password in the **Enter Old User Password** field.

b Enter a new password in the **Enter New User Password** field.

c Reenter your new password in the **Reenter New User Password** field.

You have successfully changed your password.

Report any errors or omissions

Picking up your Entrust certificate

When your certificate is ready, Entrust sends you an email containing a link to the Certificate Retrieval Web pages. You are also provided with a passphrase that allows you to log into the Entrust Certificate Retrieval Web pages and obtain the Entrust certificate.

When you pick up the certificate, the page is able to store it directly on your token.

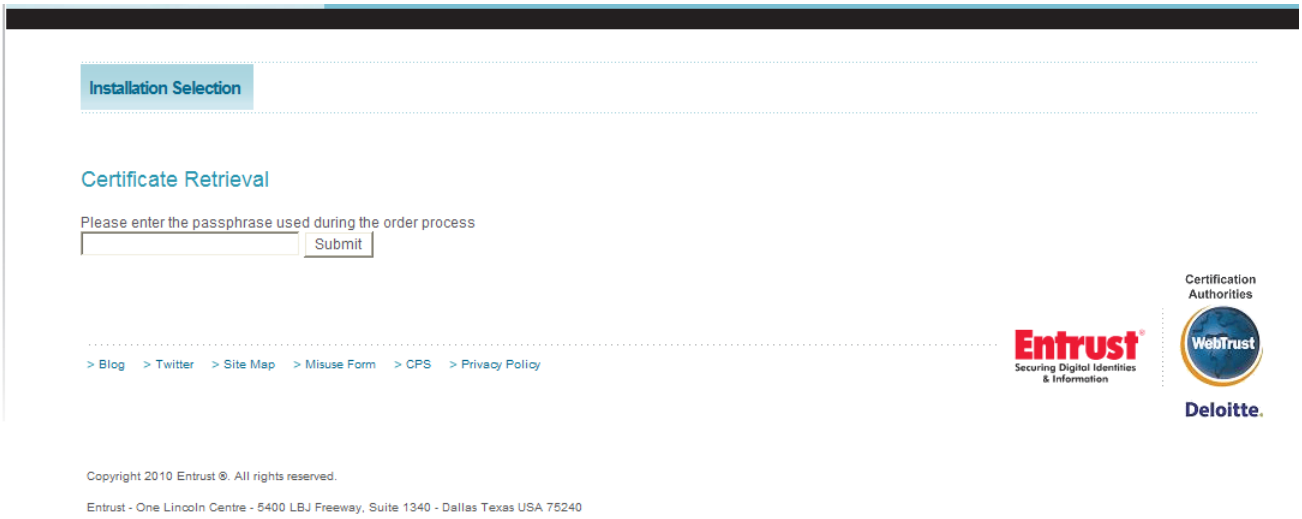
If you are picking up a PDF signing certificate for the first time, be sure that you have completed the procedures in "Installing token software and enrolling a token" on page 11.

Complete the following procedure to obtain your Entrust certificate.

To obtain your Entrust certificate

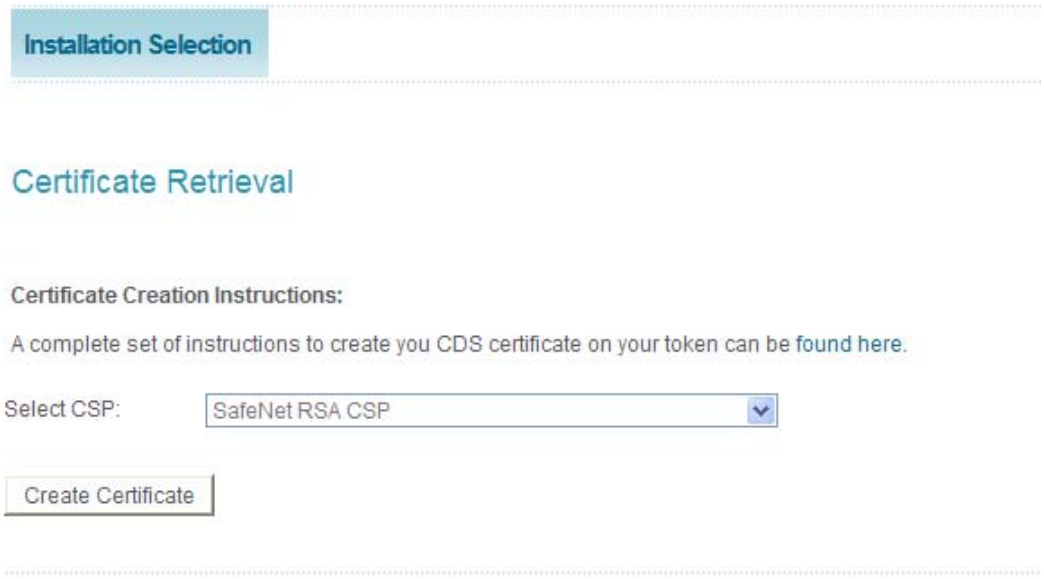
1. Insert your token into a USB port.
2. Open a browser and enter the URL for Entrust Certificate Retrieval Web pages provided in the notification email.

   The **Certificate Retrieval** log in page appears.

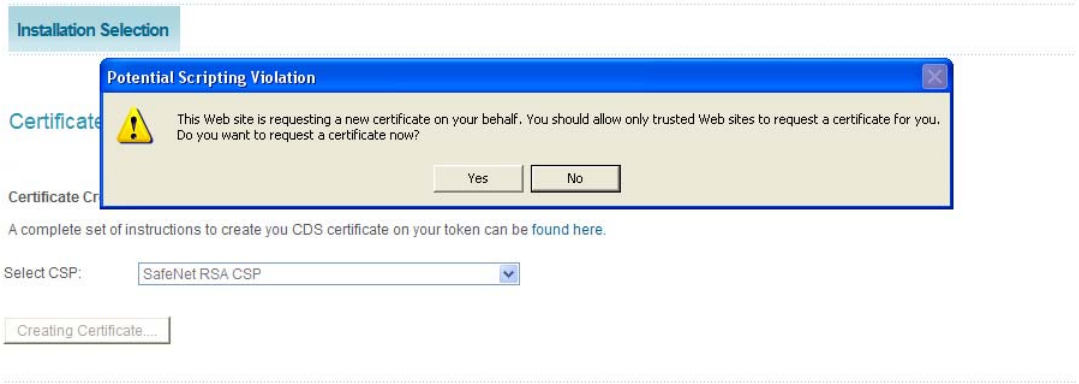


3. Log in to the **Certificate Retrieval** Web pages using the passphrase provided by Entrust.
4. If you have not already done so, download and install the token software as outlined in "Downloading and installing the token software" on page 11.
5. Read the software subscription agreement. By clicking **Accept**, you agree to all of the terms and conditions of the subscription agreement.

6 Select the Cryptographic Service Provider from the pull down menu and click **Create certificate**.



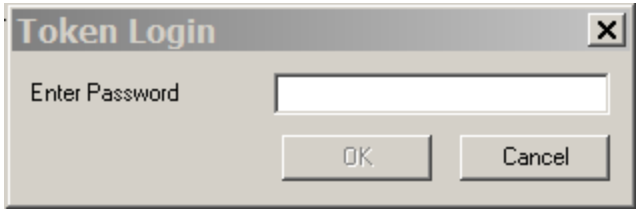
7 In the warning dialog, click **Yes** to proceed.



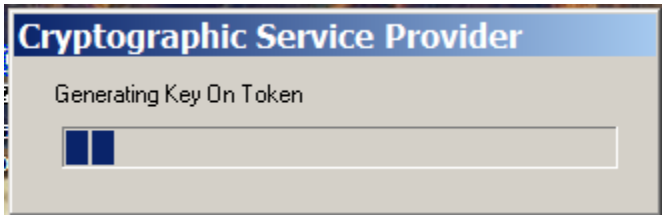
Report any errors or omissions

8 In the **Alert** dialog, click **OK** to proceed.

9 Enter the password that you created for your token (see "Changing the password for your token" on page 21). This is the password that was created specifically for the token not the passphrase used to log in to the Entrust Web site.



10 The Web site generates the certificate on your token. This will take a few moments..



11 At the potential scripting violation alert, click **Yes** to continue adding the certificate to the token. Because two certificates are added, click **Yes** a second time to continue.

12 Click **Yes** and store the certificate chain on the token.

13 A status message is displayed when the certificate has been downloaded onto your token.

You have successfully picked up your Entrust certificate and loaded it onto your token.

The certificate is also added to the Windows Certificate Store. This allows Adobe Acrobat to recognize (not validate) the signature so you can select it for signing, certification, or signing and certification.

Report any errors or omissions

Recovering a certificate

If you need to recover your certificate, for example, because you forgot the password you have several options:

- If you need to recover your certificate within 30 days of purchasing it, Entrust Certificate Services will reissue it once for free. After the 30 day period or if you need to recover the certificate more than once you must purchase a new certificate.
- If the certificate is from a single certificate order and you forget the password before the certificate is generated, Entrust Certificate Services support will reset the password for you.
- If your certificates are managed using Entrust Certificate Management Service (CMS), the Administrator can reset your token's password.

The token recovery button in the Token Manager Utility will not recover the certificate. One of the methods listed above must be used.

Report any errors or omissions

2

Signing and certifying PDF documents with your certificate

This chapter provides basic information on how to sign and certify a PDF file, how to add a signer to the trusted list, and how to set signature preferences.

For more advanced tasks, see the Adobe documentation.

Note: Procedures in this chapter are based on the 9.0 versions of Adobe Reader and Adobe Acrobat Pro. While previous versions are similar, the procedures are not identical. For instructions involving older product versions, see the Adobe documentation.

Note: You may need to register your digital ID with Adobe Acrobat before you can sign a PDF. See the Adobe documentation for more information on registering your digital ID.

This chapter includes:

- "Signing and certifying a PDF document" on page 30
- "Setting signature verification preferences" on page 39

Signing and certifying a PDF document

You can add one or more digital signatures to a PDF file or form using Adobe Acrobat Professional or LiveCycle. A digital signature enables recipients to verify that the document came from you.

The signature displays one or more signature fields directly on the PDF for easy viewing. The field contains details about the certificate and the signature name.

Note: Adobe Reader 9.0 users can sign PDF files and forms provided the PDF includes the correct permissions. In Abode Acrobat Pro 9.0, this is accomplished by selecting **Advanced** > **Extend Features in Adobe Reader** from the toolbar. Adobe Reader users cannot certify files or forms. For more information, see the Adobe documentation.

You can certify a PDF document as well as adding your signature. Certify a document to let recipients know that you approve of the contents of the PDF. This prevents content tampering, since any modification of the document after certification causes the PDF to lose its certified status.

To allow the recipient to make modifications to specific areas of the document (such as adding values to a form), the certification process allows you to specify which permitted modifications. You can certify a document with a visible signature or an invisible signature.

Complete the following procedures as required:

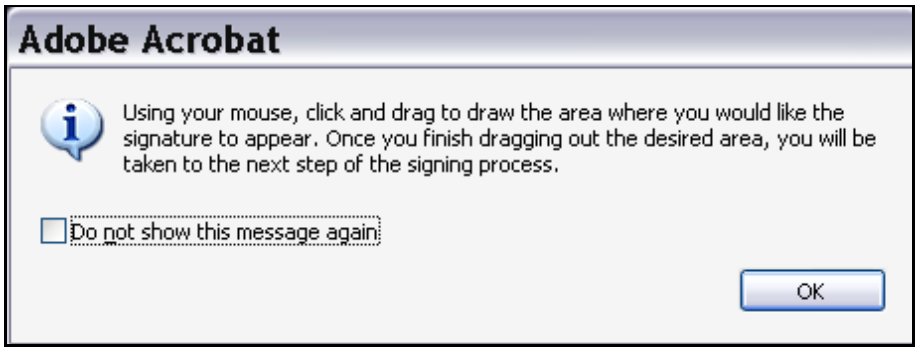
- "To add a signature to a PDF document" on page 30
- "To sign and certify a PDF document with a visible signature" on page 33
- "To sign and certify a PDF file without a visible signature" on page 36

To add a signature to a PDF document

1 From the tasks toolbar of Adobe Professional or Adobe Reader, click **Sign** and select **Sign Document**.

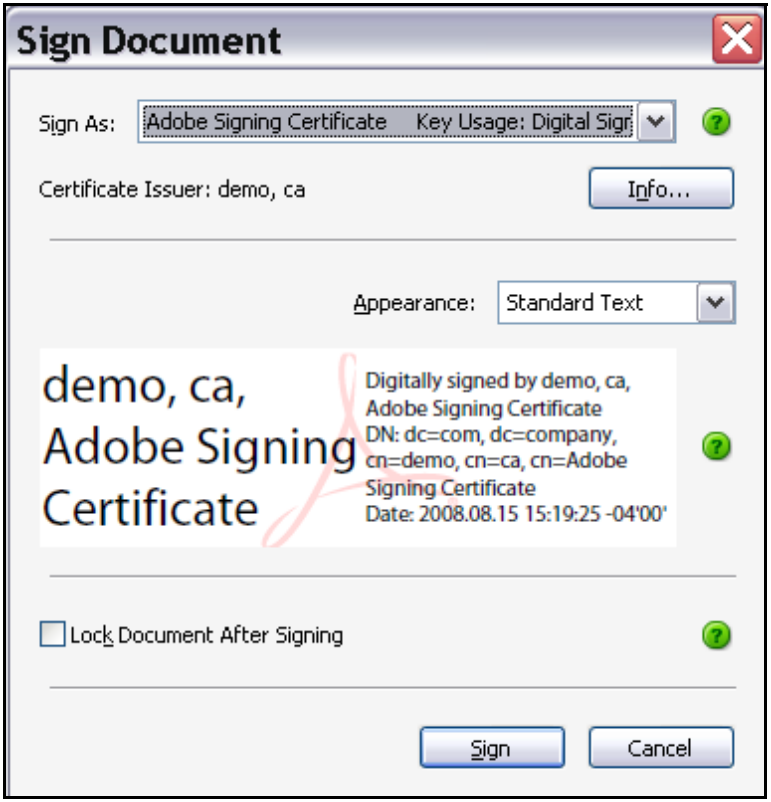
Note: A dialog box may appear describing how to apply the signature to your document. Read the instructions and click **OK**.

Report any errors or omissions



2 In your PDF, click and drag your mouse to create a signature field.

The **Sign Document** dialog box appears.



3 Select your Entrust certificate used for signing PDFs from the **Sign As** drop-down list and click **Sign**.

Note: If your digital ID is unrecognized, remove your token from the USB port, reinsert, and log back in.

Note: You can also view your digital ID, change or create a new appearance for your digital signature, and lock your document after signing (PDF file only). For more information, see the Adobe documentation.

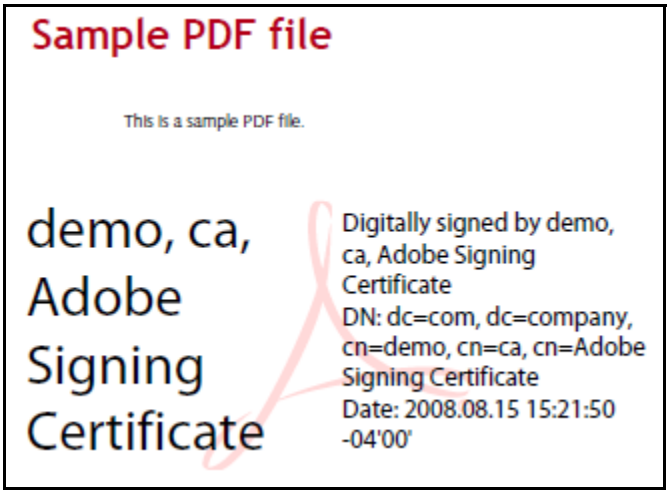
The **Save As** dialog box appears.

4 Save your signed PDF document and click **Save**. If you want to keep the original, unsigned version, save the PDF document under a new file name.

The token login dialog box appears.

5 Enter your token passphrase and click **OK**.

Your signature appears in the field.



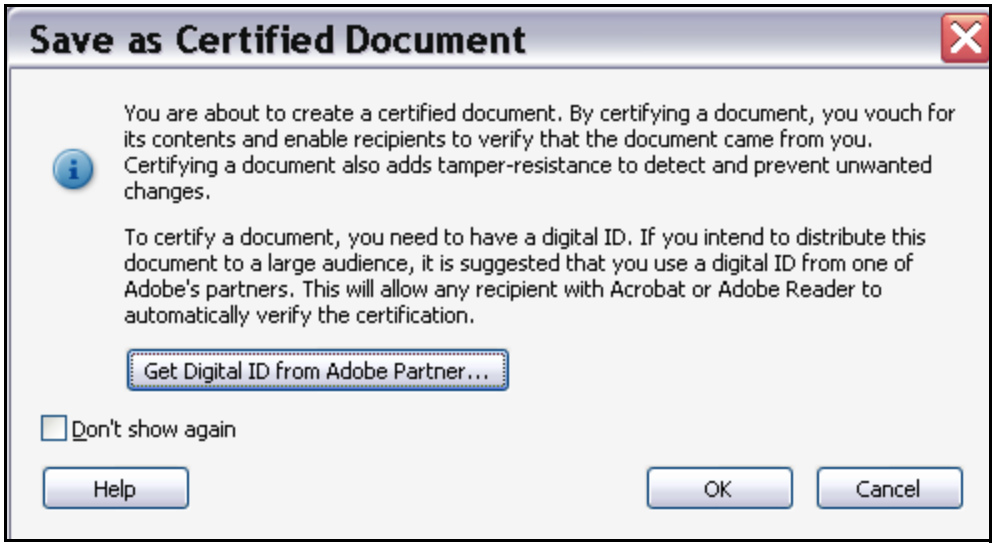
Report any errors or omissions

You successfully signed a PDF document.

To sign and certify a PDF document with a visible signature

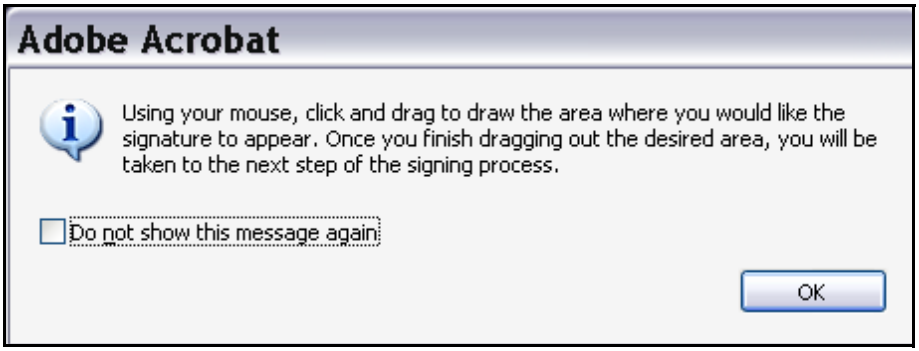
1 From the tasks toolbar, click **Sign** and select **Certify with Visible Signature**.

The **Save as Certified Document** appears.

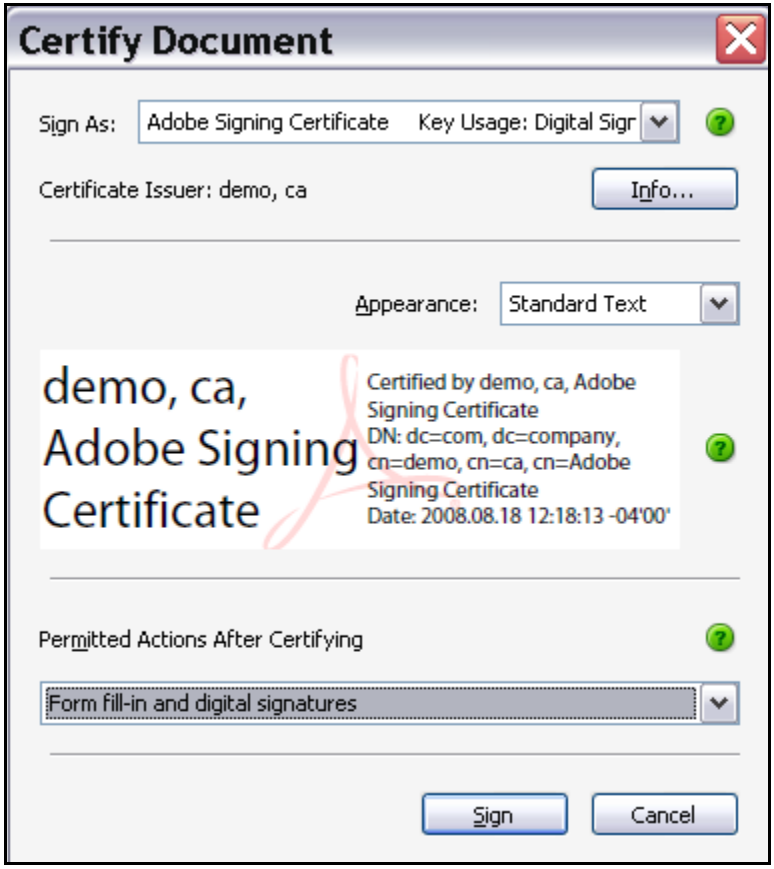


2 Click **OK**.

Note: A dialog box may appear describing how to apply the signature to your document. Read the instructions and click **OK**.



The **Certify Document** dialog box appears.



Report any errors or omissions

3 Select your Entrust certificate used for signing PDFs from the **Sign As** drop-down list and click **Sign**.

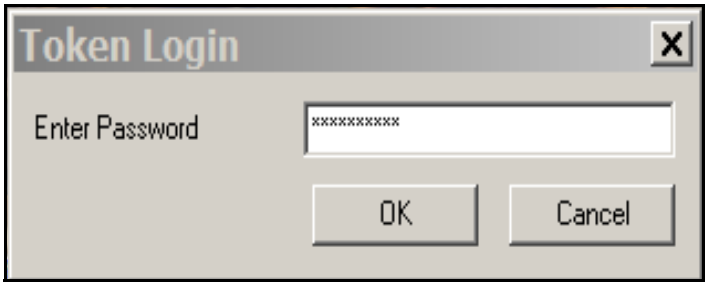
Note: If your digital ID is unrecognized, remove your token from the USB port and reinsert.

Note: You can also view your digital ID, change or create a new appearance for your digital signature, and permit specific actions after certifying. For more information, see the Adobe documentation.

The **Save As** dialog box appears.

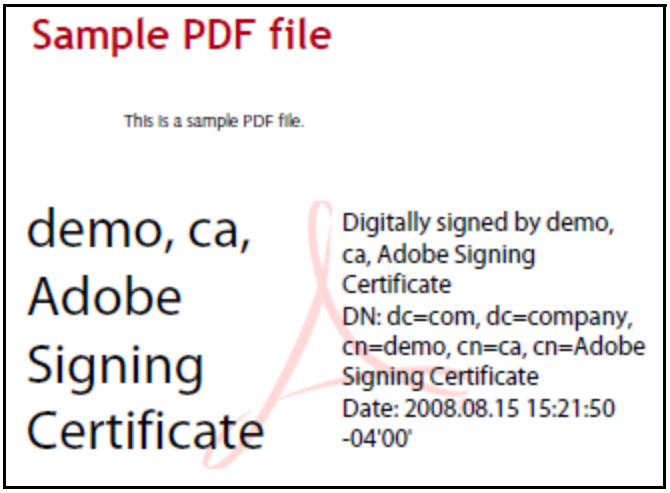
4 Save your signed and certified PDF document and click **Save**. If you want to keep the original, unsigned and uncertified version, save the PDF document under a new file name.

The token login dialog box appears.



5 Enter your token passphrase and click **OK**.

Your signature appears in the field.



If the signer identity is on your list of Trusted Identities, a blue ribbon in the document message bar indicates the file's certified status.

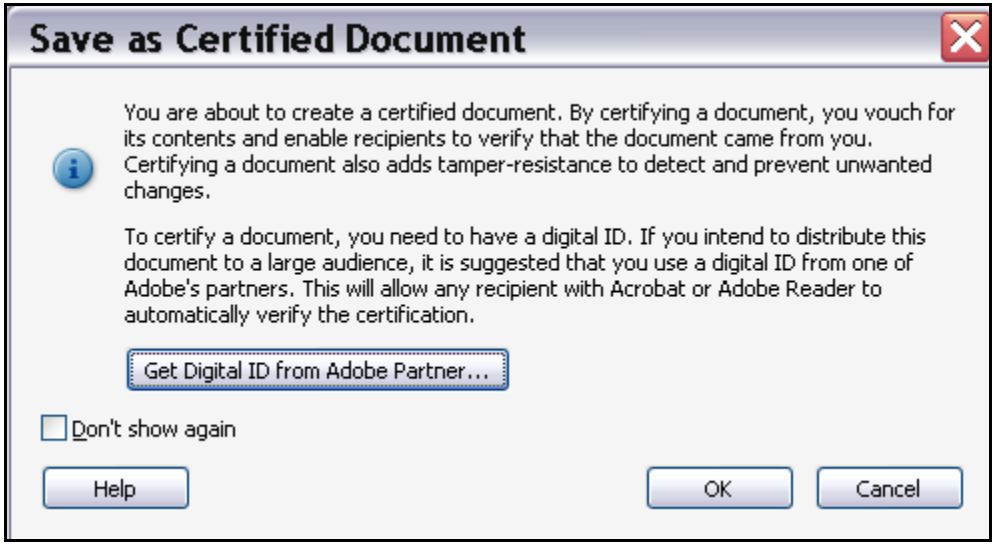
You have successfully signed and certified a PDF document.

To sign and certify a PDF file without a visible signature

1 From the tasks toolbar, click **Sign** and select **Certify without Visible Signature**.

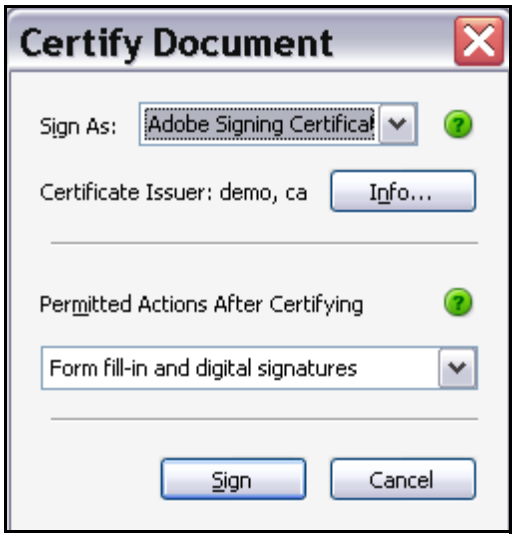
Report any errors or omissions

The **Save as Certified Document** dialog box appears.



2 Click **OK**.

The **Certify Document** dialog box appears.



3 Select your Entrust certificate used for signing PDFs from the **Sign As** drop-down list and click **Sign**.

Note: If your digital ID is unrecognized, remove your token from the USB port, and reinsert.

Note: You can also view your digital ID and permit specific actions after certifying. For more information, see the Adobe documentation.

The **Save As** dialog box appears.

4 Save your invisibly signed and certified PDF document and click **Save**. If you want to keep the original, unsigned and uncertified version, save the PDF document under a new file name.

If the signer identity is on your list of Trusted Identities, a blue ribbon in the document message bar indicates the file's certified status.

You successfully invisibly signed and certified a PDF document.

Report any errors or omissions

Setting signature verification preferences

Both Adobe Acrobat and Adobe Reader allow you set specific signature preferences to verify digital signatures and document certifications.

Complete the following procedure.

To set signature verification preferences

1. Select **Edit > Preferences** and click **Security**.
2. Select **Verify signatures when the document is opened**.
3. Click **OK**.

Report any errors or omissions