User Guide

Symantec Managed PKI AATL Certificate for PDF Impress

Securing PDF/Digital Signature Documents

The portable document format file format (PDF) has drastically improved business communications. Various applications can uniformly convert files into PDF format with a reasonable expectation that the remote side will render it correctly.

In business, PDF documents are created for a variety of reasons, including contracts, purchase orders, invoices, receipts, and for many more documents that require signatures. It is so convenient that many business partners never need to physically meet in person. However, this versatility is also exploited by attackers, who use the PDF format to produce fraudulent financial and/or legal documents that create liability on the part of recipients.

For this reason, digital document signing is gaining attention in business communications for one or both parties to ensure documents are not altered in transit and to establish the originator of the document. Core to this issue is how to establish trust between business partners. Adobe introduced the certified document services program and invited certificate authorities (CAs) to participate. An updated version of the program is called Adobe Approved Trust List (AATL), and includes many entities that need the efficiency of digital commerce but also require the reliability of a paper document.

With public key infrastructure (PKI) technology and digital signatures, document integrity is ensured in transit, but this transfers the problem to whether or not the certificate is trusted. In a CA model, the relying applications trust that the CA will issue certificates only to trusted parties. This is governed by a formal document about how certificates are handled called a certificate practices statement. PDF software, such as Acrobat Reader and PDF Impress, need to trust the certificates that make up this CA. Signatures created by certificates issued under this CA are then trusted without extra effort by the business parties.

Symantec Adobe Approved Trust List (AATL) certificates can solve the issue of fraudulent documents because all Adobe products automatically obtain this trust list” CA as member of AATL; there is no need to install certificates for every business partner.

Another issue with the CA model is the signing process. There are not many applications that can sign several documents in a single operation. One that can do this is PDF Impress from BinaryNow, Inc.

Symantec AATL certificates are available through Symantec Managed PKI service. Managed PKI service can issue digital certificates that provide trusted document signatures. Adobe also requires hardware-level security: each user needs an additional hardware token (or hardware security module, HSM) that Symantec can provide.

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™

Architecture

Figure 1, below, illustrates how PDF documents are signed by the sender, verified by the receiver, and how Symantec AATL certificates are used during this process.

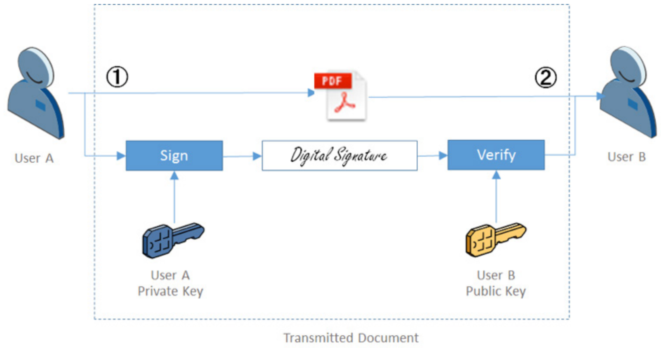
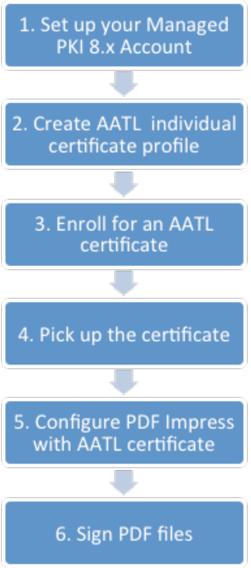


Figure 1. User A digitally signs an Adobe PDF document using User A's private key stored on a hardware credential. User B receives the document and authenticates with User A's public key, which is embedded in the Symantec AATL certificate.

Tasks

Figure 2, below, describes the general steps required to set up the Symantec Managed PKI account and integrate Symantec AATL certificates with related software.



1. Set up your Managed PKI 8.x Account

2. Create AATL individual certificate profile

3. Enroll for an AATL certificate

4. Pick up the certificate

5. Configure PDF Impress with AATL certificate

6. Sign PDF files

Figure 2. In this case, we apply user seats for Symantec AATL individual certificate issuance. For an organizational AATL certificate, you need an Adobe organizational certificate and a physical HSM appliance.

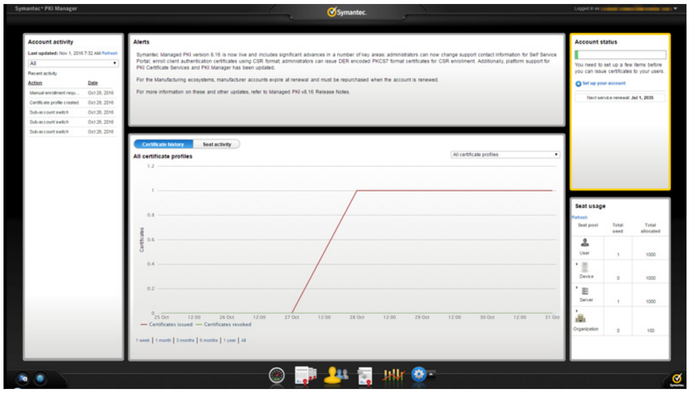
Task 1. Set Up Your Managed PKI 8.x Account

Contact your Symantec Sales representative to set up a Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile. You must complete and return the following documents. Your Symantec representative can 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 also need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative can 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.

Figure 3, shows a screen shot of Managed PKI 8.x, PKI Manager



Logged in as: [redacted]

Account activity

Last updated: Nov 1, 2016 7:32 AM Refresh

All

Recent activity

Action	Date
Manual enrollment requ...	Oct 28, 2016
Certificate profile created	Oct 28, 2016
Sub-account switch	Oct 26, 2016
Sub-account switch	Oct 26, 2016
Sub-account switch	Oct 26, 2016

Alerts

Symantec Managed PKI version 8.16 is now live and includes significant advances in a number of key areas: administrators can now change support contact information for Self Service Portal; enroll client authentication certificates using CSR format; administrators can issue DER encoded PKCS7 format certificates for CSR enrollment. Additionally, platform support for PKI Certificate Services and PKI Manager has been updated.

For the Manufacturing ecosystems, manufacturer accounts expire at renewal and must be repurchased when the account is renewed.

For more information on these and other updates, refer to Managed PKI v8.16 Release Notes.

Account status

You need to set up a few items before you can issue certificates to your users.

Set up your account

Next service renewal: Jul 1, 2035

Seat usage

Refresh

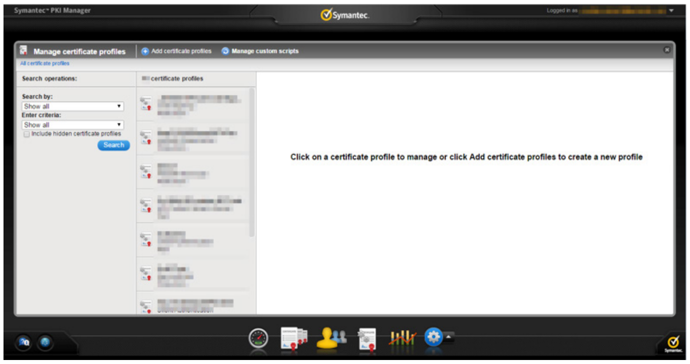
Seat pool	Total used	Total allocated
User	1	1000
Device	0	1000
Server	1	1000
Organization	0	100

Figure 3. Managed PKI 8.x, PKI Manager screen view.

Task 2. Create an AATL Individual Certificate Profile

Managed PKI uses a certificate profile to define the certificates issued. Certificates issued by the AATL individual profile support digital signing of PDF documents. Complete the following steps to create your Managed PKI AATL certificate profile:

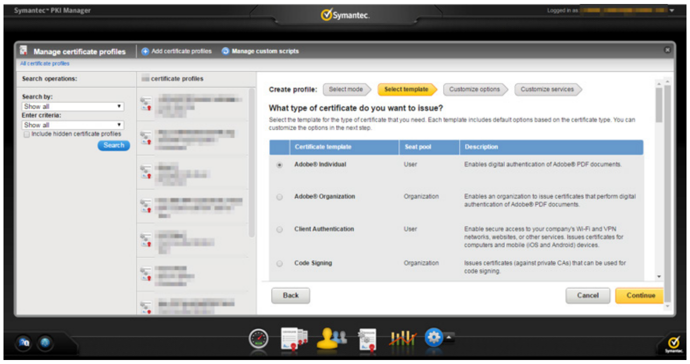
1. Log into Managed PKI 8.x, PKI Manager using your administrator certificate. You will be prompted for your PKI client PIN.
2. In PKI Manager, click Manage certificate profiles or select Manage certificate profiles from the Tasks menu on the bottom navigation bar.



Click on a certificate profile to manage or click Add certificate profiles to create a new profile

Figure 4. Manage certificate profile view.

3. Click Add certificate profiles from the top of the resulting Manage certificate profiles page. The Create profile page will appear.
4. Select whether the certificates will be issued in test mode or production mode, and click Continue. The Create profile page will appear.
5. Select AATL Individual as the certificate template and click Continue. The Customize certificate options will appear.



What type of certificate do you want to issue?

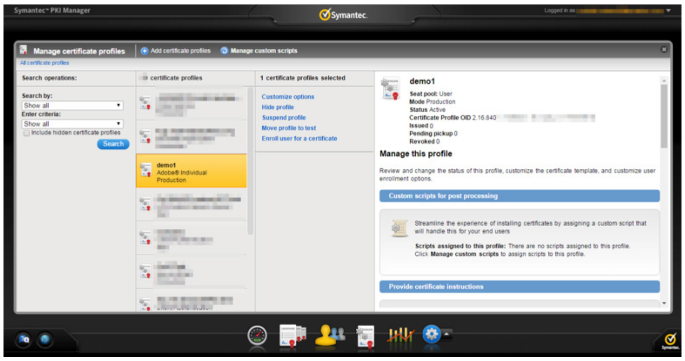
Select the template for the type of certificate that you need. Each template includes default options based on the certificate type. You can customize the options in the next step.

	Certificate template	Seat pool	Description
●	Adobe® Individual	User	Enables digital authentication of Adobe® PDF documents.
○	Adobe® Organization	Organization	Enables an organization to issue certificates that perform digital authentication of Adobe® PDF documents.
○	Client Authentication	User	Enable secure access to your company's Wi-Fi and VPN networks, websites, or other services. Issues certificates for computers and mobile (iOS and Android) devices.
○	Code Signing	Organization	Issues certificates (against private CAs) that can be used for code signing.

Figure 5. AATL individual certificate template view.

6. In the Customize certificate options, enter a certificate profile name.
7. Select the appropriate Enrollment type:
   - Select PKI Client if your user will enroll for certificates using PKI Client. PKI Client would typically be chosen in larger deployments and involves additional infrastructure.
   - Select CSR (certificate signing request) if your user will enroll using CSR. CSR is typically selected in smaller deployments.
   - Select PKI Web Services if your user will enroll for certificates using third-party applications. API-based enrollment is also supported.
8. Select the appropriate Authentication method based on your Enrollment type:
   - Select Enrollment Code to generate a unique enrollment code for each user and to automatically approve certificate requests.
   - Select Manual approval to manually approve individual certificates using enrollment pages. After the administrator approves a request, the user is sent an enrollment code for authentication when picking up the certificate.
9. Click Advanced options to view certificate options and define any additional attributes.
10. 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. On this page you can also customize the profile further, such as adding custom scripts, and additional languages, or email notifications.



demo1

Seat pool: User
Mode Production
Status Active
Certificate Profile OID 2.16.840 [redacted]
Issued 0
Pending pickup 0
Revoked 0

Manage this profile

Review and change the status of this profile, customize the certificate template, and customize user enrollment options.

Streamline the experience of installing certificates by assigning a custom script that will handle this for your end users

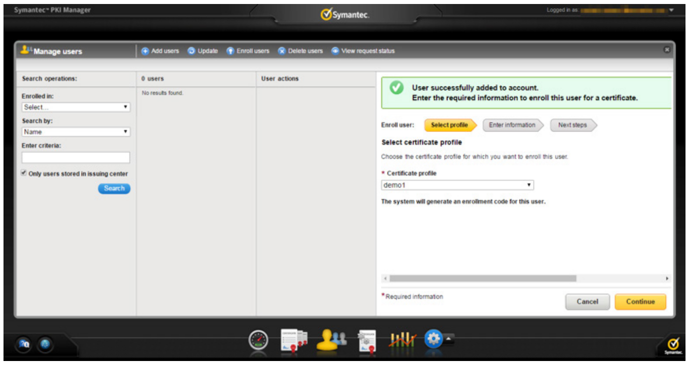
Scripts assigned to this profile: There are no scripts assigned to this profile. Click **Manage custom scripts** to assign scripts to this profile.

Figure 6. Confirmation page view.

Task 3. Add User and Enroll for an AATL certificate

In the following scenario, a certificate profile is created (see Task 2), with PKI Client selected as the enrollment type and Enroll code selected for the authentication method. However, you must first add the user to PKI Manager before enrolling the user 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 below if you are enrolling multiple users using a csv file.
4. Enter the first name, last name, and select 'I want to enroll this user for a certificate.' Then click Continue.
5. Select the Adobe individual certificate profile and click Continue.
6. The final enrollment link is displayed to the administrator, along with the enrollment code that can be sent to the user for authentication. Symantec recommends sending the enrollment code separately from the enrollment link, and that you do not send the enrollment code by email.



Search operations:

Enrolled in: Select...

Search by: Name

Enter criteria:

☑ Only users stored in issuing center

0 users

No results found.

User actions

User successfully added to account.
Enter the required information to enroll this user for a certificate.

Enroll user: Select profile > Enter information > Next steps

Select certificate profile

Choose the certificate profile for which you want to enroll this user.

* Certificate profile: demo1

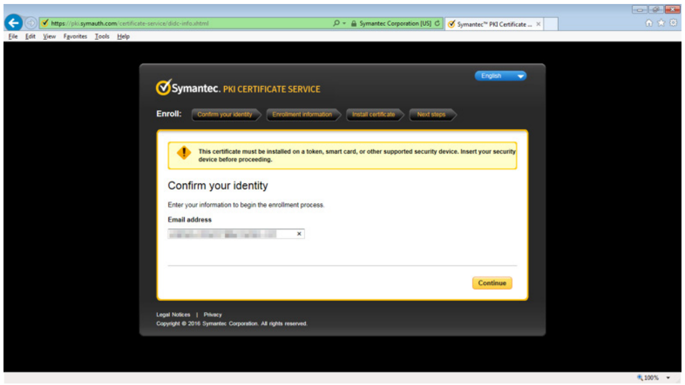
The system will generate an enrollment code for this user.

*Required information

Figure 7. Manage users view

Task 4. Pick Up the Certificate

1. The user will click the enrollment link sent by the administrator.
2. Enter the email address used for enrollment and click Continue.


File
Edit
View
Favorites
Tools
Help
Symantec Corporation [US]
Symantec™ PKI Certificate ...
Symantec. PKI CERTIFICATE SERVICE
English
Continue
100%

https://pki.symauth.com/certificate-service/didc-info.xhtml

Enroll: Confirm your identity > Enrollment information > Install certificate > Next steps

This certificate must be installed on a token, smart card, or other supported security device. Insert your security device before proceeding.

Confirm your identity

Enter your information to begin the enrollment process.

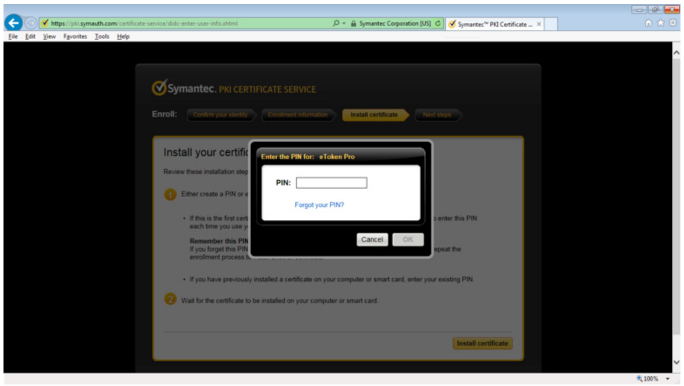
Email address: [redacted]

Legal Notices | Privacy

Copyright © 2016 Symantec Corporation. All rights reserved.

Figure 8. Enter email address as user identity.

3. Enter the enrollment code provided by the administrator and click Continue. This step authenticates the end user to ensure that the correct user is picking up the certificate.
4. Click Continue.
5. Insert the Gemalto/SafeNet eToken and click Install your certificate.


File
Edit
View
Favorites
Tools
Help
Symantec Corporation [US]
Symantec™ PKI Certificate ...
Symantec. PKI CERTIFICATE SERVICE
Cancel
OK
Install certificate
100%

https://pki.symauth.com/certificate-service/didc-enter-user-info.xhtml

Enroll: Confirm your identity > Enrollment information > Install certificate > Next steps

Install your certific

Review these installation step

1 Either create a PIN or e

- If this is the first cert ... enter this PIN each time you use y

Remember this PIN
If you forget this PIN ... epeat the enrollment process t

- If you have previously installed a certificate on your computer or smart card, enter your existing PIN.

2 Wait for the certificate to be installed on your computer or smart card.

Enter the PIN for: eToken Pro

PIN:

Forgot your PIN?

Figure 9. Entering the PIN for the security token allows the certificate to be installed.

6. Enter the PIN for the security token when prompted and click OK.
7. The certificate is now installed on your credential.

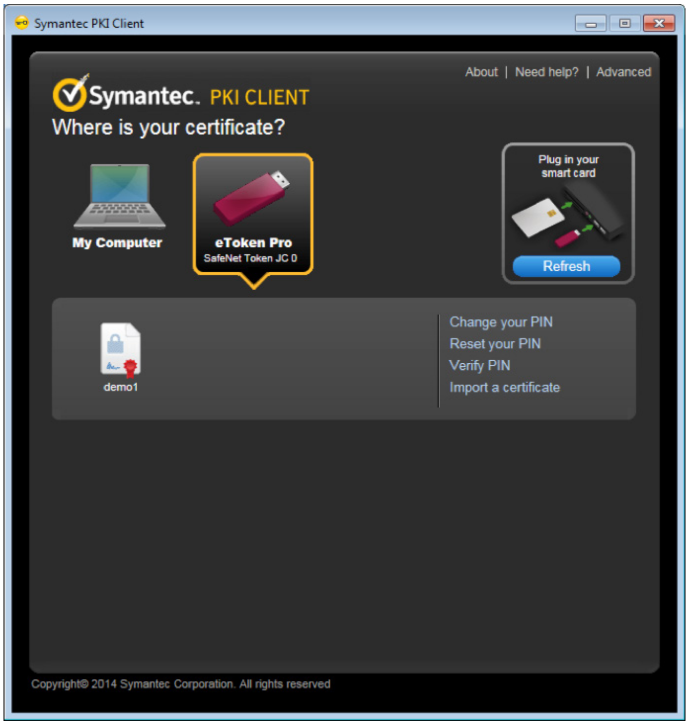


Figure 10. Certificate installed using eToken.

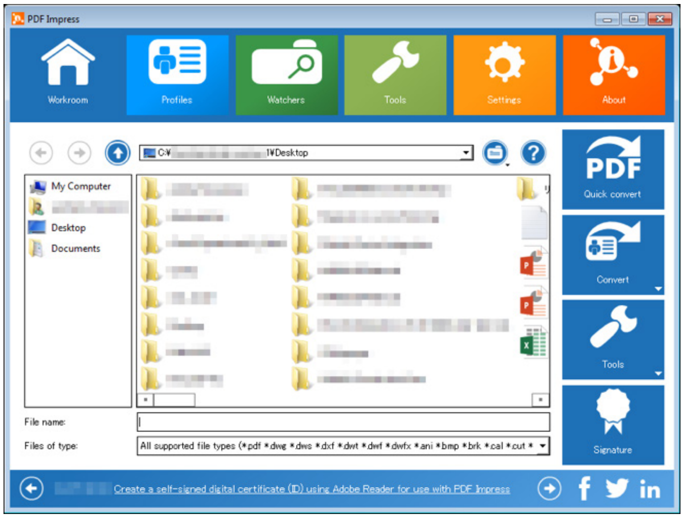
Configure and Sign Using PDF Impress

You must first configure PDF Impress to use the certificate to sign PDF documents. This section describes how to configure PDF Impress using Symantec Managed PKI AATL certificates and then use it to sign PDF documents.

There are many ways to sign using an installed digital certificate, such as signing a document without pre-configuration or using virtual printer with preconfiguration. In this section, we describe how to configure and sign by batch process for multiple documents.

Configure PDF Impress with AATL Certificate

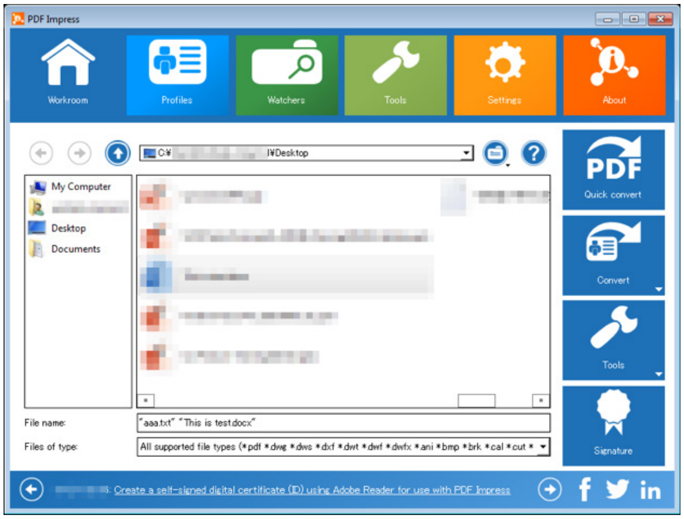
1. Launch PDF Impress from the Start menu.



Files of type: All supported file types (*.pdf *.dwg *.dws *.dxf *.dwt *.dwf *.dwfx *.ani *.bmp *.brk *.cal *.cut *

Figure 11. Workroom menu of PDF Impress.

2. Select the files to be converted to PDF and signed. Note that you can select multiple files by pressing the CTRL key. If PDF files are selected, PDF Impress will digitally sign the original documents without recreating them.

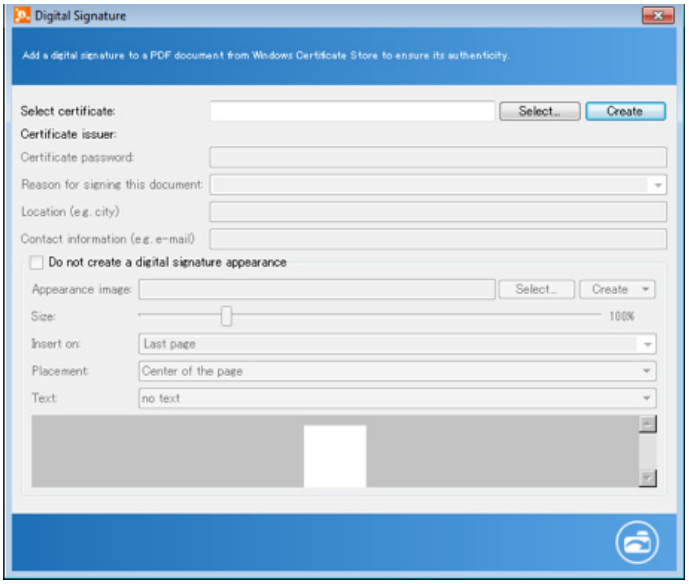


File name: "aaa.txt" "This is test.docx"

Files of type: All supported file types (*.pdf *.dwg *.dws *.dxf *.dwt *.dwf *.dwfx *.ani *.bmp *.brk *.cal *.cut *

Figure 12. In this example, 'aaa.txt' and 'This is test.docx' files are selected.

3. Click the Signature icon in the lower right corner.



Digital Signature

Add a digital signature to a PDF document from Windows Certificate Store to ensure its authenticity.

Select certificate: [Select...] [Create]

Certificate issuer:

Certificate password:

Reason for signing this document:

Location (e.g. city)

Contact information (e.g. e-mail)

□ Do not create a digital signature appearance

Appearance image: [Select...] [Create]

Size: 100%

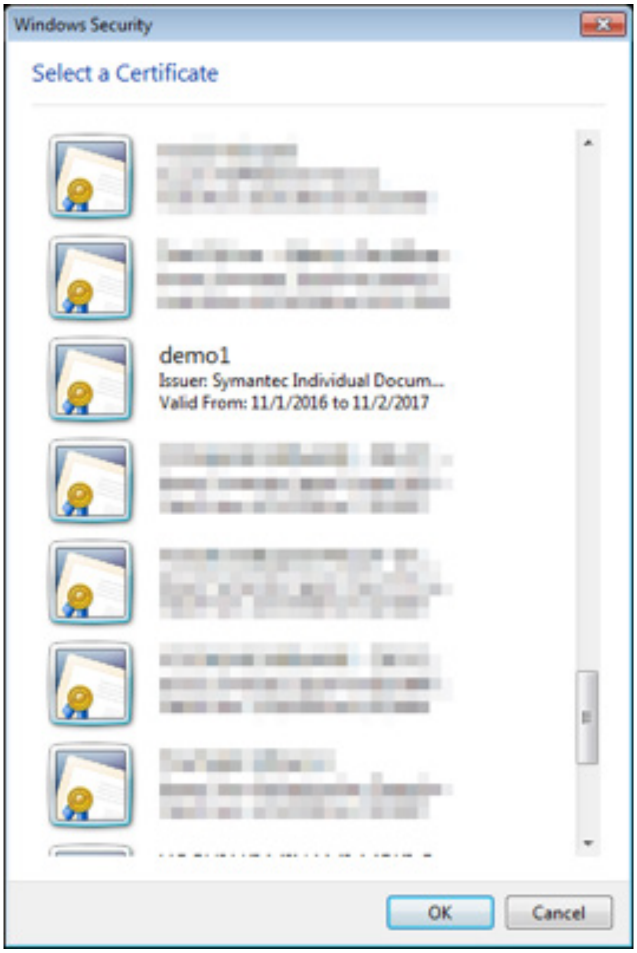
Insert on: Last page

Placement: Center of the page

Text: no text

Figure 13. Signature icon appears in the lower right corner.

4. Insert the USB security token and select the appropriate certificate from the list. Note that there is typically a small delay if many certificates are on this token.



Windows Security

Select a Certificate

[redacted]

[redacted]

demo1
Issuer: Symantec Individual Docum...
Valid From: 11/1/2016 to 11/2/2017

[redacted]

[redacted]

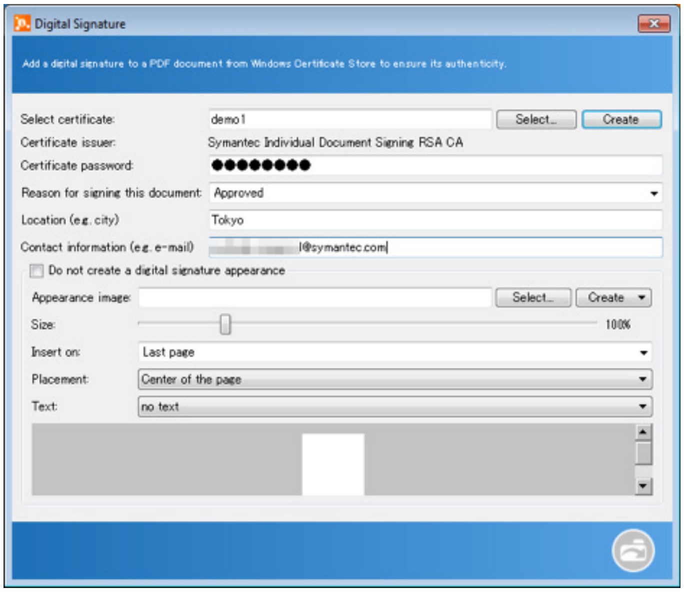
[redacted]

[redacted]

[OK] [Cancel]

Figure 14. Select your certificate from the list and click OK.

5. Select the AATL individual certificate and other items to be digitally signed. Note that the password will protect access to the Windows certificate store and should not be confused with the PIN required by Symantec PKI Client during signing.



Digital Signature

Add a digital signature to a PDF document from Windows Certificate Store to ensure its authenticity.

Select certificate: demo1 [Select...] [Create]

Certificate issuer: Symantec Individual Document Signing RSA CA

Certificate password: ●●●●●●●●●

Reason for signing this document: Approved

Location (e.g. city) Tokyo

Contact information (e.g. e-mail) [redacted]l@symantec.com

□ Do not create a digital signature appearance

Appearance image: [Select...] [Create]

Size: 100%

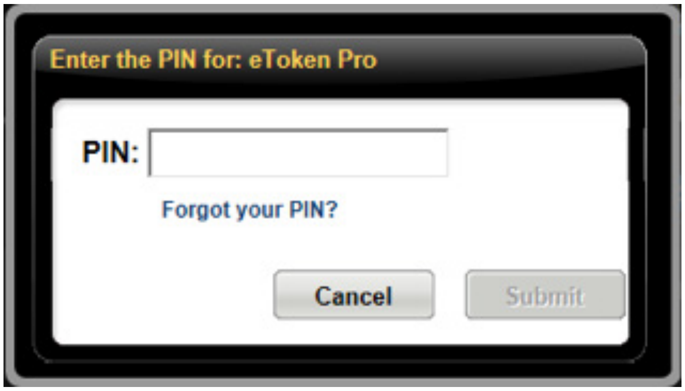
Insert on: Last page

Placement: Center of the page

Text: no text

Figure 16. Click on the Apply task and save document icon in the lower tight corner to start the process.

6. Click the Apply task and save document icon in the lower right corner. Then start the PDF conversion. When prompted, enter your PIN into the Symantec PKI client. Only one PIN entry is needed to sign multiple documents at once.



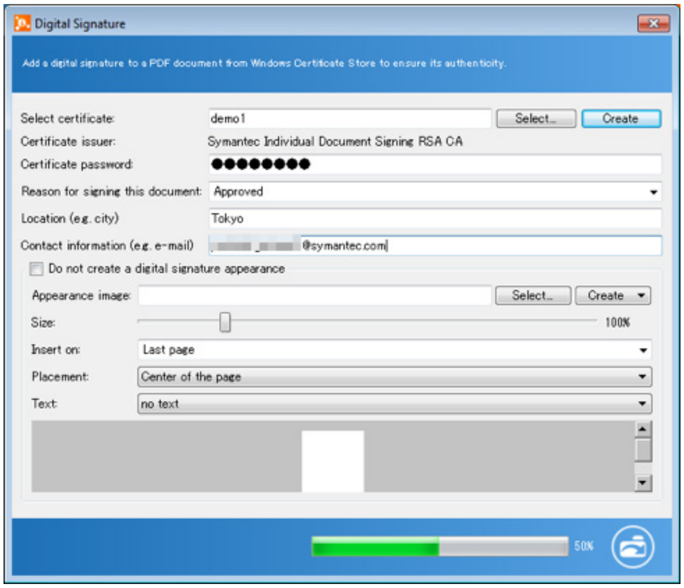
Enter the PIN for: eToken Pro

PIN:

Forgot your PIN?

[Cancel] [Submit]

Figure 17. Enter the PIN to complete the signature/s.



Add a digital signature to a PDF document from Windows Certificate Store to ensure its authenticity.

Select certificate: demo1 [Select...] [Create]

Certificate issuer: Symantec Individual Document Signing RSA CA

Certificate password: ●●●●●●●●●

Reason for signing this document: Approved

Location (e.g. city): Tokyo

Contact information (e.g. e-mail): [redacted]@symantec.com

□ Do not create a digital signature appearance

Appearance image: [Select...] [Create]

Size: 100%

Insert on: Last page

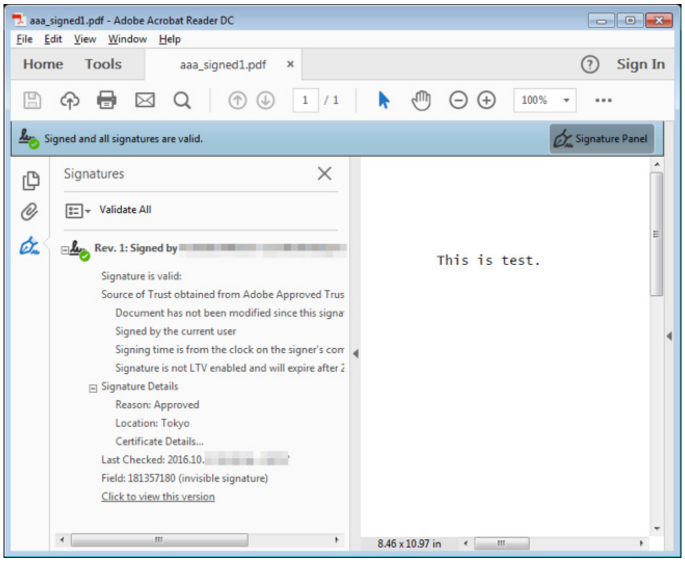
Placement: Center of the page

Text: no text

50%

Figure 18. The digital signature in progress.

7. On the desktop, you may see two types of PDF files; one is a conversion of the original PDF file and the other is the PDF with the digital signature. The figure below shows how this appears in Adobe Acrobat Reader DC.



aaa_signed1.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools aaa_signed1.pdf
Sign In
1 / 1
100%
Signature Panel
Signatures
Validate All

Signed and all signatures are valid.

Rev. 1: Signed by [redacted]

Signature is valid:

Source of Trust obtained from Adobe Approved Trus

Document has not been modified since this signa

Signed by the current user

Signing time is from the clock on the signer's com

Signature is not LTV enabled and will expire after 2

Signature Details

Reason: Approved

Location: Tokyo

Certificate Details...

Last Checked: 2016.10.[redacted]

Field: 181357180 (invisible signature)

Click to view this version

This is test.

8.46 x 10.97 in

Figure 19. Adobe Acrobat Reader view of PDF files.

Automate PDF Signing With PDF Impress

PDF Impress allows ad-hoc addition of a digital signature during a conversion process. For example, a user can simply print from Microsoft Word (or any application) into PDF Impress virtual printer and add digital signature in the Extended Save As dialog box. This process is straightforward and allows creation of digitally signed PDF documents from any application that can print a file. Users can also add a visual appearance of a hand written signature, stamp, or watermark; merge, split, extract, insert, remove, or rotate PDF pages; or encrypt a whole document before a final PDF version is signed. Single PDF document signing is also possible in the PDF Impress workroom or straight from the desktop via a right-click menu.

Significant productivity improvement comes with PDF profiles and batch conversion/signing. PDF Impress profiles allow adding digital signature tasks into PDF profiles, which limits the need for adding signatures with each conversion. Once a signature task is added to the profile, every PDF document created will be automatically signed. In addition, multiple PDF profiles can be created for various PDF workflows and different signatures used on one system.

Batch PDF signing is also available on demand or can be scheduled with watched folders. On-demand batch conversion works by selecting multiple files (in different formats) in PDF the Impress workroom or Windows Explorer and then selecting signature from the workroom toolbar or right-click menu. All files are converted into PDF and digitally signed. A user is prompted only once to insert a PIN into the Symantec PKI client to authorize access to digitally sign; the authorization is then used for all files in a batch.

PDF Impress watchers is used to automate conversion and signing through watched folders--set source, destination and archive folders, and folders for journal and conversion log. Watchers can run continuously, periodically at certain times, or on demand, and are controlled through a system tray application.

PDF Impress can be also integrated into third-party applications using an API described in the PDF Impress Developer Guide.

PDF Impress is Windows productivity software created by BinaryNow, Inc.—a 30-day, fully functional trial. For additional information, go to PDF Impress online

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934

www.symantec.com

Symantec Support for Authentication Services

03/17

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software -Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec® product.