Symantec™ Managed PKI®

Integrating S/MIME Certificates with Microsoft Outlook®

Symantec™ Managed PKI® Integration Guide for S/MIME

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 May 15, 2013

Legal Notice

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.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/contact/index.html#support4

Contents

Chapter 1

Integrating S/MIME Certificates with Microsoft Outlook

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 Secure Email allow you to digitally sign and encrypt your digital communications using a certificate. By digitally signing and encrypting an email message, you apply your unique digital mark to the message and protect the privacy of the message by converting readable plain text into scrambled cipher text.

This document describes how to configure Secure/Multipurpose Internet Mail Extensions (S/MIME) certificate with Microsoft Outlook to digitally sign and encrypt digital communication.

Partner Information

These procedures have been tested on the following platforms:

Table 1-1 Partner Information

Partner Name	Microsoft®
Product Name	Microsoft Outlook Client® 2007, 2010

The procedures in this guide are written for a system running Microsoft Outlook 2010. The screens and procedures for Outlook 2007 may differ slightly. However, the process for integrating Managed PKI certificates with Outlook 2007 is essentially the same.

Integration Architecture

The following diagram describes how Managed PKI certificates support S/MIME certificate and integrates with Microsoft Outlook to digitally sign and encrypt emails.

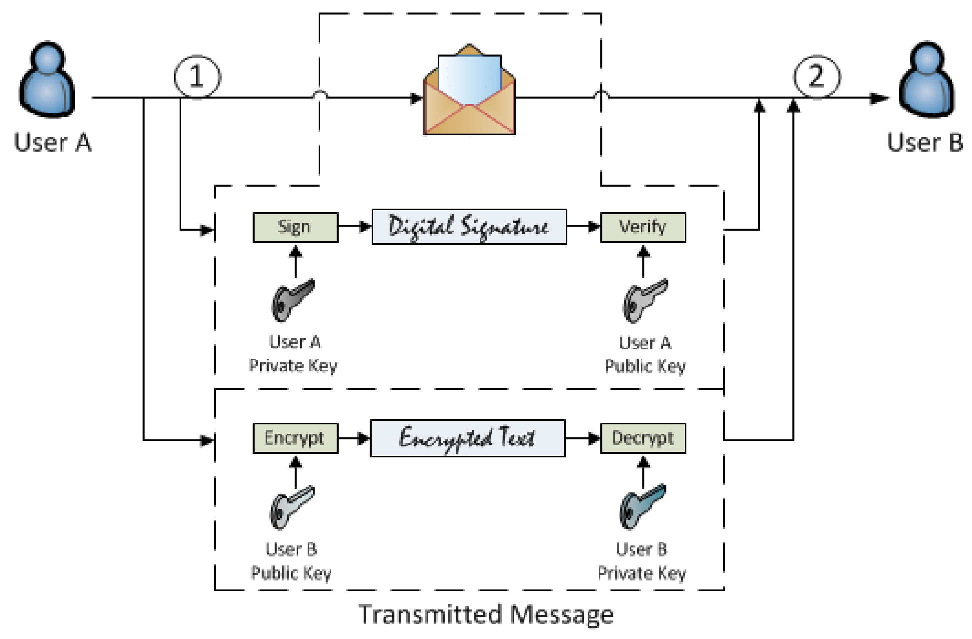


Figure 1-1 S/MIME Certificate integration with Microsoft Outlook

1. User A digitally signs an email message using User A's private key and encrypts using User B's public key.
2. User B receives the email message and authenticate it using User A's public key and decrypts it using User B's private 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 Microsoft Outlook.

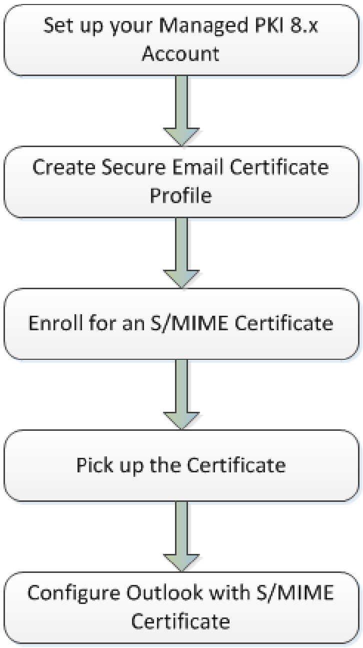

Set up your Managed PKI 8.x Account
Create Secure Email Certificate Profile
Enroll for an S/MIME Certificate
Pick up the Certificate
Configure Outlook with S/MIME Certificate

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.

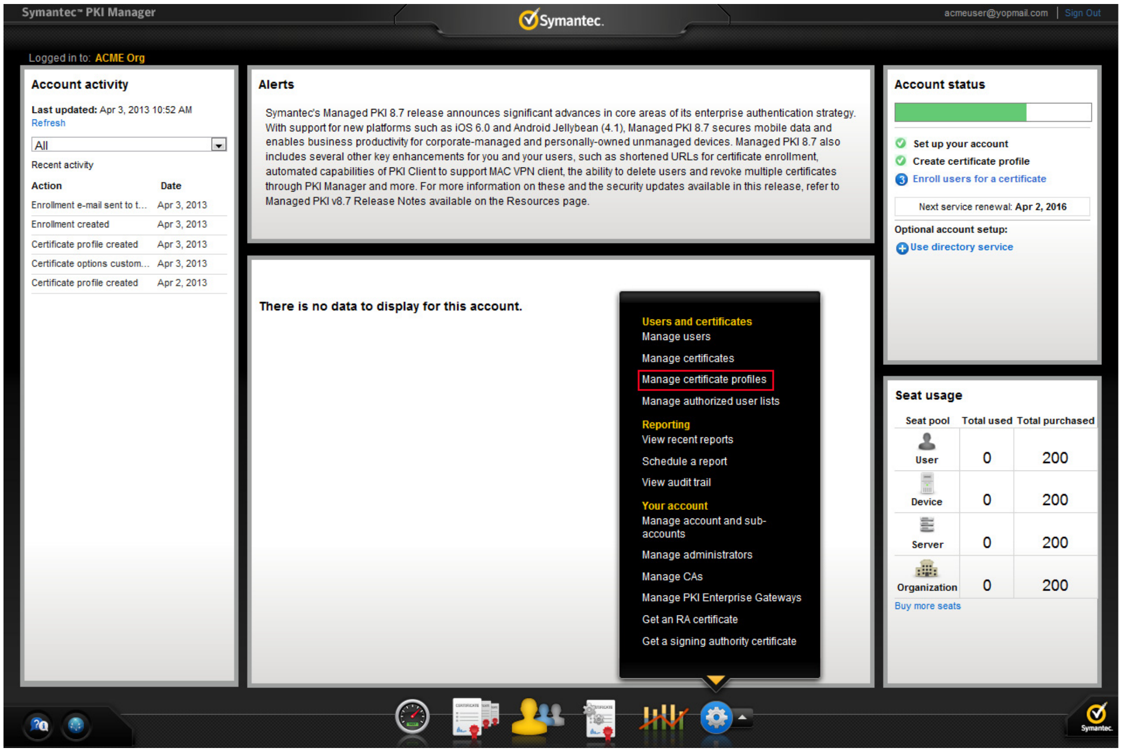
Task 2. Create a Secure Email Certificate Profile

Managed PKI uses a certificate profile to define the certificates issued. Certificates issued by the Secured Email profile support the S/MIME protocol. These certificates can be used for digital signing and/or authentication of emails through S/MIME.

Complete the following steps to create your Managed PKI Secure Email 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.



Account activity

Last updated: Apr 3, 2013 10:52 AM

Refresh

All

Recent activity

Action	Date
Enrollment e-mail sent to t...	Apr 3, 2013
Enrollment created	Apr 3, 2013
Certificate profile created	Apr 3, 2013
Certificate options custom...	Apr 3, 2013
Certificate profile created	Apr 2, 2013

Alerts

Symantec's Managed PKI 8.7 release announces significant advances in core areas of its enterprise authentication strategy. With support for new platforms such as iOS 6.0 and Android Jellybean (4.1), Managed PKI 8.7 secures mobile data and enables business productivity for corporate-managed and personally-owned unmanaged devices. Managed PKI 8.7 also includes several other key enhancements for you and your users, such as shortened URLs for certificate enrollment, automated capabilities of PKI Client to support MAC VPN client, the ability to delete users and revoke multiple certificates through PKI Manager and more. For more information on these and the security updates available in this release, refer to Managed PKI v8.7 Release Notes available on the Resources page.

There is no data to display for this account.

Account status

✓ Set up your account
✓ Create certificate profile
3 Enroll users for a certificate

Next service renewal: **Apr 2, 2016**

Optional account setup:

Use directory service

Seat usage

Seat pool	Total used	Total purchased
User	0	200
Device	0	200
Server	0	200
Organization	0	200

Buy more seats

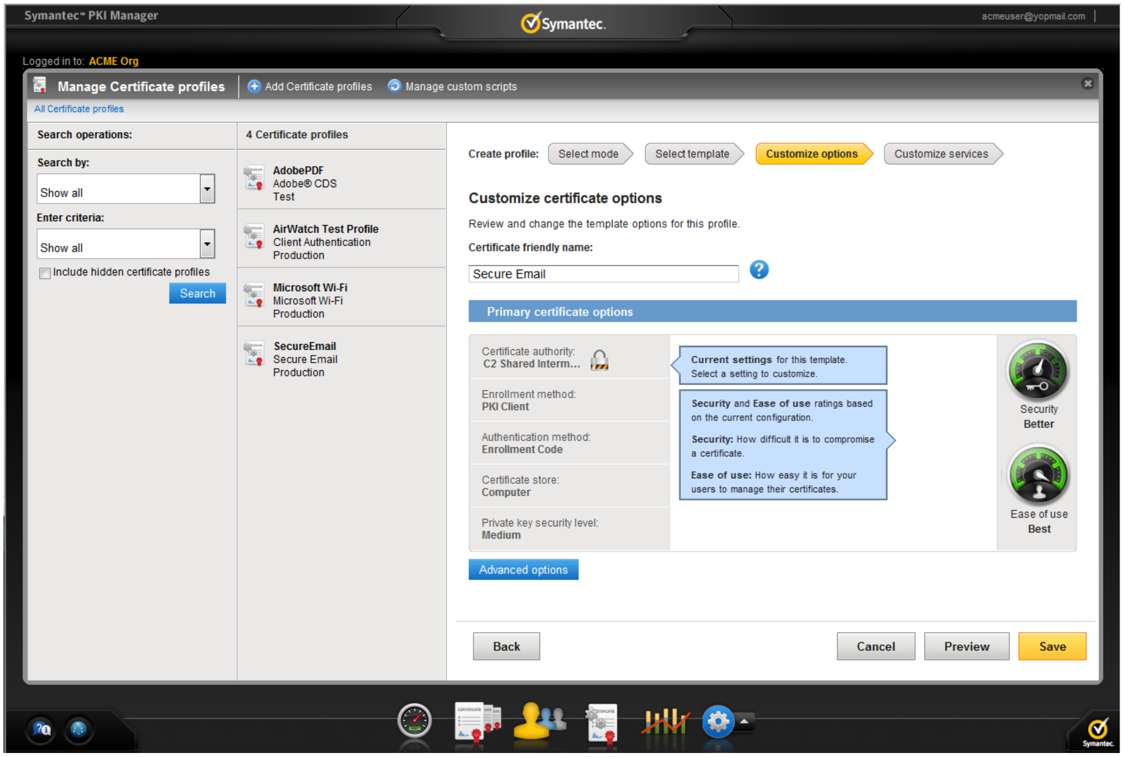
Figure 1-3 Manage Certificate Profile

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

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



Customize certificate options

Review and change the template options for this profile.

Certificate friendly name: Secure Email

Primary certificate options

Certificate authority: C2 Shared Interm...

Enrollment method: PKI Client

Authentication method: Enrollment Code

Certificate store: Computer

Private key security level: Medium

Current settings for this template. Select a setting to customize.

Security and **Ease of use** ratings based on the current configuration.

Security: How difficult it is to compromise a certificate.

Ease of use: How easy it is for your users to manage their certificates.

Figure 1-4 S/MIME 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.

The Authentication method is pre-configured based on your Enrollment method:

- For the PKI Web Services Enrollment method, the Authentication method is **3rd party application.**
- For the PKI Client or OS/browser Enrollment method, the Authentication method is **Active Directory.**

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

Note: Select **Publish to public directory** in the Secure Email certificate option to allow customers and others outside your company to download the public key to quickly enable secure communication. For information on importing the public key, see “Obtaining a Sender’s Public Key Manually” on page 10.

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 S/MIME 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 S/MIME 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 completing the enrollment process. 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 the certificate.
4. Click **Continue**.
5. Click **Install certificate** to install the certificate.
6. Enter the PIN for the certificate store (PKI Client) when prompted and click **OK**.
7. The certificate is installed on your machine. You must configure Microsoft Outlook to use this certificate to encrypt and sign the email messages. For information on configuring Microsoft Outlook with S/MIME certificate, see "Configuring Microsoft Outlook" on page 7.

Chapter 2

Configuring Microsoft Outlook

This chapter discusses how to configure Microsoft Outlook and digitally sign and encrypt email messages using Managed PKI certificates.

Import your Certificate into Outlook

Complete the following steps to import the S/MIME certificate to Microsoft Outlook:

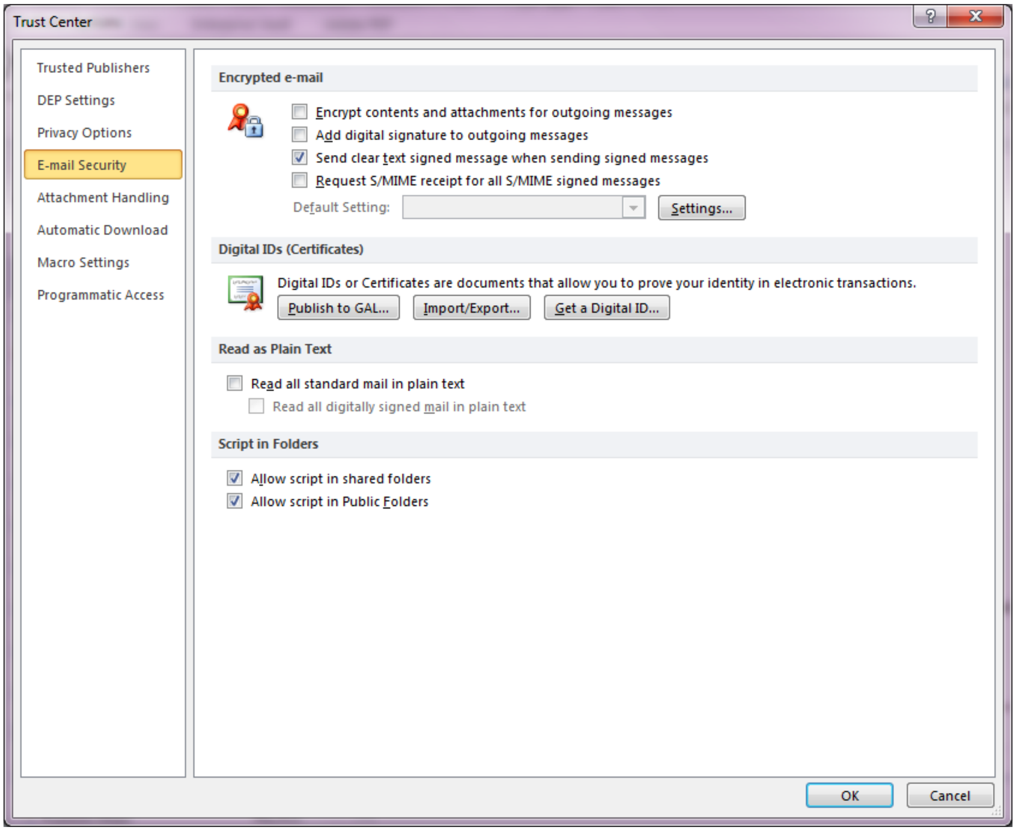
1 Open Microsoft Outlook.

2 Click the **File** tab.

3 Click **Options**.

4 Click **Trust Center** from the Outlook options menu and click **Trust Center Settings**.

5 On the **E-mail Security** tab, click **Import/Export**.



Trust Center

- Trusted Publishers
- DEP Settings
- Privacy Options
- E-mail Security
- Attachment Handling
- Automatic Download
- Macro Settings
- Programmatic Access

Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages

□ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: [Settings...]

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

[Publish to GAL...] [Import/Export...] [Get a Digital ID...]

Read as Plain Text

□ Read all standard mail in plain text

□ Read all digitally signed mail in plain text

Script in Folders

☑ Allow script in shared folders

☑ Allow script in Public Folders

[OK] [Cancel]

Figure 2-1 Email Security tab

6 Click **Browse** to locate your S/MIME certificate on your local machine and provide the password (PIN) for the certificate.

7 Click **OK**.

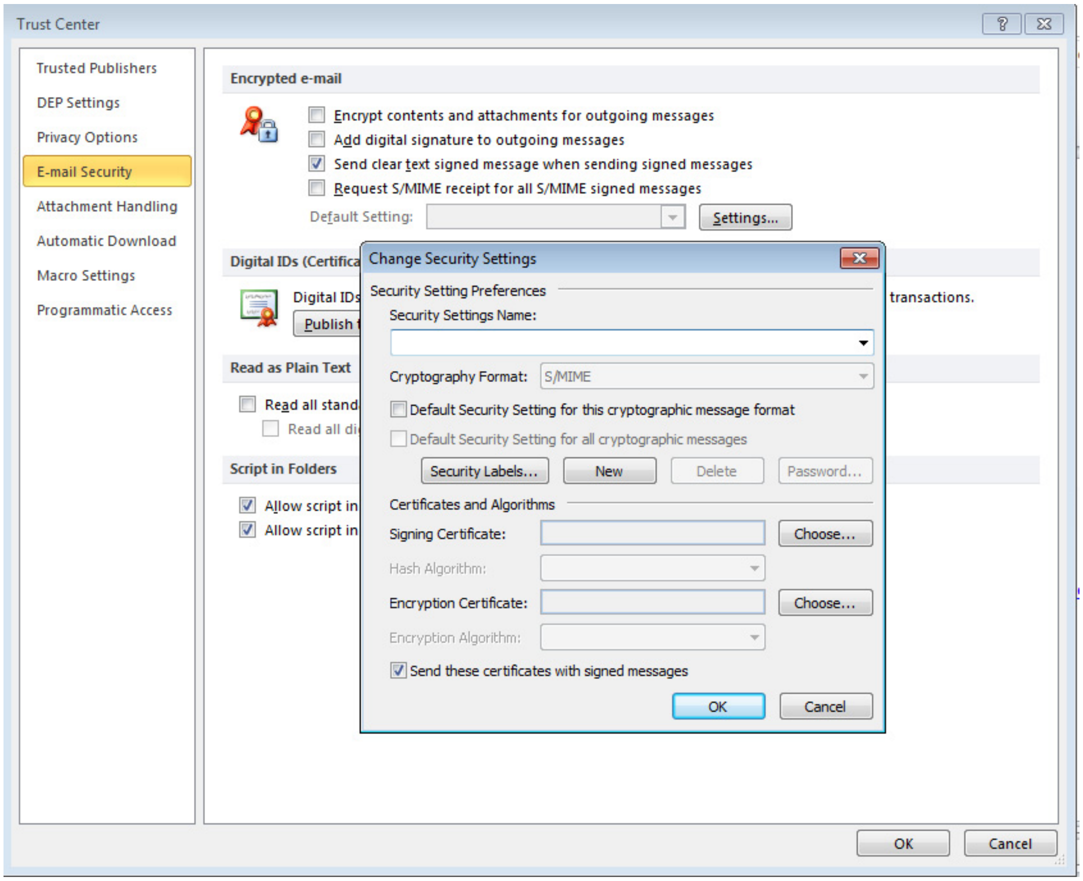
Digitally Signing Messages

1 In Outlook, click **File > Options > Trust Center > Trust Center Settings**.

2 On the **Email Security** tab, under **Encrypted e-mail**, select the **Add digital signature to outgoing messages** check box. You can also select the following options:

- To allow recipients who do not have S/MIME security settings to read your messages, select the **Send clear text signed message when sending signed messages** check box.
- To verify that your digitally signed message was received unaltered and to request a notification on who opened the message, select the **Request S/MIME receipt for all S/MIME signed messages** check box.

3 Click **Settings** to choose which certificate to use to encrypt messages, or to configure additional security settings.



Trust Center

Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages
□ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Change Security Settings

Security Setting Preferences

Security Settings Name:

Cryptography Format: S/MIME

□ Default Security Setting for this cryptographic message format
□ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate:

Hash Algorithm:

Encryption Certificate:

Encryption Algorithm:

☑ Send these certificates with signed messages

Figure 2-2 Security Settings

4 Click **OK**.

Encrypt Messages

1. In Outlook, click **File > Options > Trust Center > Trust Center Settings**.
2. On the **Email Security** tab, under **Encrypted e-mail**, select the **Encrypt contents and attachments for outgoing messages** check box.
3. Click **Settings** to choose which certificate to use to encrypt messages, or to configure additional security settings.

   To read an encrypted email, the recipient must have access to the public key of the sender's certificate. There are several ways for a recipient to obtain the sender's public key:

   - The sender can send a digitally-signed message to the recipient so that the recipient can add you to the Outlook contact. The digital certificate is also added to the contact details.
   - The sender can send a `.cer` file to a recipient which the recipient can add to the Outlook contact manually. For more information, see "Adding a Sender's Public Key to Your Outlook Contacts" on page 9.
   - The sender or PKI administrator can provide a public key to a recipient directly. Symantec offers public LDAP search portal (Certificate search portal) at https://pki-search.symauth.com/pki-search/index.html through which the recipient can download the public certificate. For instructions on importing the public key, see "Obtaining a Sender's Public Key Manually" on page 10.
4. Click **OK**.

Importing a Sender's Public Key

If the recipient is in the same CA hierarchy as the sender, and Publish to a public directory was configured for this profile, the recipient will automatically have access to the sender's public key. Otherwise, the recipient must obtain the public key before being able to verify digital signatures or read encrypted messages from the sender.

Adding a Sender's Public Key to Your Outlook Contacts

You can add a sender's public key to your Outlook Contacts in one of two ways:

- If you received a digitally-signed email, add the sender to your Outlook Contacts. The public key is added to the contact.
- If you receive a `.cer` file from a sender, you can import the certificate to a contact manually (you may need to create the contact first).

The following steps describe how to create a contact and public key from a digitally-signed email:

1. In the email message you receive, right-click the name of the sender, and click **Add to Outlook Contacts**.

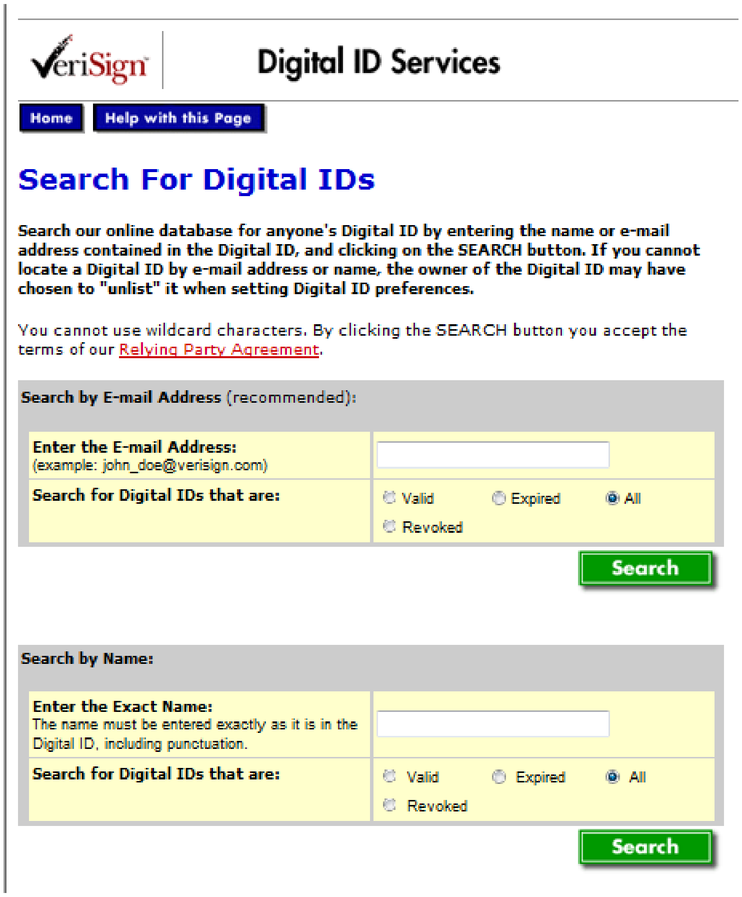
   A contact form with sender's name and email address already filled in appears.
2. Click **Save & Close**. The contact name and public key is added to the Outlook Contact folder.

The following steps describe how to create a new contact and add the public key.

1. On the **Home** tab, click **Contacts**.
2. Click **New Contact**.
3. Enter a contact name, email address, and any other information that you want to include.
4. Click **Certificates**.
5. Click **Import**.
6. Select the `.cer` file that you downloaded.
7. Click **Save & Close.**

Obtaining a Sender's Public Key Manually

1 Click the Certificate search portal at https://pki-search.symauth.com/pki-search/index.html.



Search For Digital IDs

Search our online database for anyone's Digital ID by entering the name or e-mail address contained in the Digital ID, and clicking on the SEARCH button. If you cannot locate a Digital ID by e-mail address or name, the owner of the Digital ID may have chosen to "unlist" it when setting Digital ID preferences.

You cannot use wildcard characters. By clicking the SEARCH button you accept the terms of our Relying Party Agreement.

Search by E-mail Address (recommended):

Enter the E-mail Address: (example: john_doe@verisign.com)	
Search for Digital IDs that are:	○ Valid ○ Expired ● All ○ Revoked

Search

Search by Name:

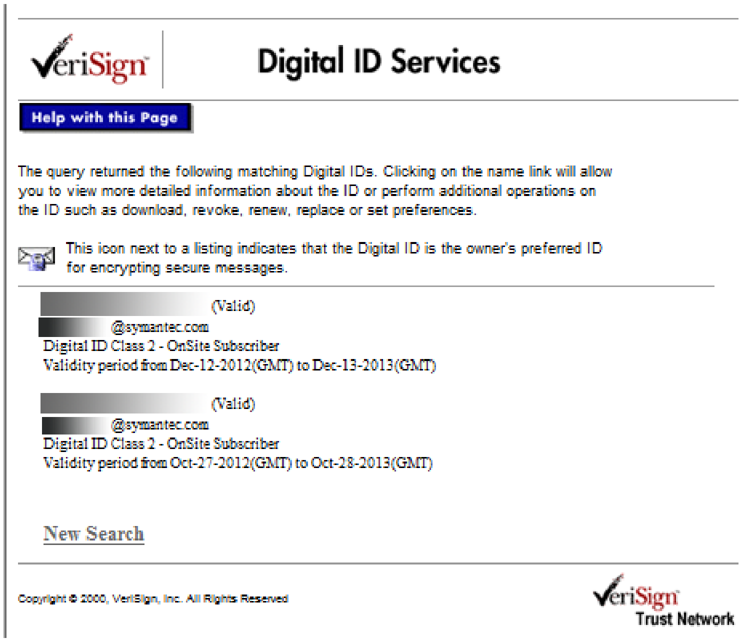
Enter the Exact Name: The name must be entered exactly as it is in the Digital ID, including punctuation.	
Search for Digital IDs that are:	○ Valid ○ Expired ● All ○ Revoked

Search

Figure 2-3 Digital ID Services

2 Enter the email address or the exact name and click **Search**.

3 From the list of certificates, click on the link to view the details.



The query returned the following matching Digital IDs. Clicking on the name link will allow you to view more detailed information about the ID or perform additional operations on the ID such as download, revoke, renew, replace or set preferences.

This icon next to a listing indicates that the Digital ID is the owner's preferred ID for encrypting secure messages.

[redacted] (Valid)
[redacted]@symantec.com
Digital ID Class 2 - OnSite Subscriber
Validity period from Dec-12-2012(GMT) to Dec-13-2013(GMT)

[redacted] (Valid)
[redacted]@symantec.com
Digital ID Class 2 - OnSite Subscriber
Validity period from Oct-27-2012(GMT) to Oct-28-2013(GMT)

New Search

Copyright © 2000, VeriSign, Inc. All Rights Reserved

Figure 2-4 Digital ID Services download

4 Click **Download** to download the certificate.

5 Select Outlook as the type of client.

6 Click **Download This Digital ID**.

7 Click **Install**.

Verify the Digital Signature on an Email Message

1 Open the digitally-signed email message.

2 To verify if the signature is valid, click the **Digital Signature** icon at the Signed By status line.

3 Click **Details** to view the digital certificate details.

4 Select the certificate signer and click **View Details** to view the signature details.