Configuring Outlook's built-in Cryptosystem

October 16, 2017

Contents

1 Prerequisites

- MS Outlook 2013 or later is recommended. Earlier versions officially support S/MIME but users often report difficulties, particularly with Outlook 2010.

- Any of these browsers installed:

Browser	Key storage consistent with Outlook (thus simpler to setup)	Notes
Chrome/Chromium	no	some versions of Chrome have problems with key generation
Firefox	no	
Internet Explorer (OS/X)	?	
Internet Explorer (Windows)	yes	
Safari (OS/X)	yes	some versions of Safari have problems with key generation
Safari (Windows)	?	

The browser is only needed initially to create SSL keys, and will not be used thereafter. Browsers above that are indicated not to share the same key storage as Outlook (e.g. Firefox) may still be used, but there will be some extra configuration steps to copy the user's keys (sections **??** and **??**).

2 Instructional videos (optional)

These videos are optional; not required by this guide.

Link	Outlook ver.	Browser ver.	CA	Scope + Notes
6OxOo-w3Ymo	2007	n/a	n/a	
wGHaB0elkaA	2010	Firefox	Symantec	Demonstrates how to use Firefox and manually copy the key pair into Outlook.
n3rOEpGjrc	2013	Chrome	Comodo	
sfancZGEGjg	2013-2016	IE?	Comodo	This comprehensive video covers every step in this entire document. It demonstrates a case where the browser automatically installs the key where Outlook can find it. The first 9 min. of the video is blather, but the link supplied skips to the relevant part.
4fmBzeq8BVA	2016	IE?	Entrust	Outlook had automatic visibility to the key in this demo on Windows, so IE was likely used.

3 Prep to receive encrypted mail or to send signed mail

3.1 Get an S/MIME certificate

In your browser go to one of these certificate authorities (**Justin recommends Comodo via Secorio**):

certificate authority ("CA")	price (for non-commercial individual use)	validity	notes
CAcert	gratis	6|24 mos.(criteria)	community driven
COMODO direct	gratis	1 yr	
COMODO via InstantSSL	gratis	1 yr	
COMODO via Secorio	gratis	1 yr	recommended; assumed choice by this guide
Entrust	≥$20		
IdenTrust	≥$19		
StartCom	gratis	2 yrs	
wosign	gratis?	2 yrs?	blocks tor?

Warning: the CAs that participate in e-mail certificate verification are constantly changing. Many CAs have discontinued e-mail certification prior to this guide. Those are obviously omitted here, but some of the above listings are likely to become obsolete as this guide ages. Consequently it might be interesting to check out the catalog of certificate authorities listed at http://kb.mozillazine.org/Getting_an_SMIME_certificate).

3.1.1 If you chose "Comodo via Secorio"

1. (secorio.com) If you are using the *noscript* firefox plugin, you must enable javascript for `secorio.com` and `comodo.com`.

2. (secorio.com) In the left frame, select "`S/MIME Class 2`" (even though it's *class 1* that we need), then click "`Order`".

3. (secorio.com) Scroll down to "`S/MIME Certificates`" and choose "1 year" in the pull-down to the right of the *class 1* row.

4. (comodo.com) Fill out the form that appears in a new tab. Setting a revocation password is optional (and it's a good idea).

5. (your inbox) An e-mail will arrive. If your e-mail client renders it graphically, click the button "`Click & Install Comodo Email Certificate`". For text clients, follow the instructions in the e-mail. If your mail client does not automatically use Firefox or IE to open URLs, right-click that button instead, copy the URL, and paste it in the address bar to force it to render in Firefox or IE.

6. Skip to section **??**

3.1.2 If you chose another certificate authority

Simply follow the instructions on the website of the CA. It will generally involve filling out a form and confirming an e-mail.

3.2 Installing your certificate into Outlook

If you created your key using a browser that uses the same key storage as Outlook (as indicated in the "Prerequisites"), skip this section and go to section **??**.

3.2.1 (Chrome only) Export your key from your browser

There are multiple browsers which do not share the same key storage as Outlook, but this section presumes you are using Chrome. Follow YouTube video n3rOEpGjrc (the link of which jumps you to the relevant point in the video), or follow these steps:

1. After creating the certificate (previous section) Chrome presents a status bar under the address bar saying "Successfully stored client certificate..". Click the "`View`" button on that bar.

2. There is a pop-up which showing basic information about your certificate. Switch to the `Details` tab.

3. Click the "`Copy to File`" button to launch an export wizard.

4. Click `Next`.

5. You are asked if you want to export the private key with the certificate. The default answer is no, but you need to click "`yes`", then `Next`.

6. You are asked which format to use. Choose `PKCS#12`, then `Next`.

7. You will be prompted for a password for the backup file. A weak password is fine, because this backup file will not be transmitted or retained for long. You will import it into Outlook locally, and then you will delete the backup file.

Then skip to section **??** for steps to import the key into Outlook.

3.2.2 (Firefox only) Export your key from your browser

There are multiple browsers which do not share the same key storage as Outlook, but this section presumes you are using Firefox. Watch YouTube video wGHaB0elkaA or follow the steps below to export the key from the Firefox and then import it into Outlook.

The video demonstrates using Outlook 2010 for the mail client and Firefox (a pre-2012 version) for the browser. The first few minutes start by walking through key creation on Symantec's website, which is useless because Symantec no longer offers the service. So the YouTube link skips that portion of the video automatically.

If not following the above-mentioned video, these are the steps to export from a more recent version of Firefox:

1. Go to: menu (≡) ≫ Options/Preferences ≫ Advanced ≫ Certificates ≫ View Certificates ≫ Your Certificates.
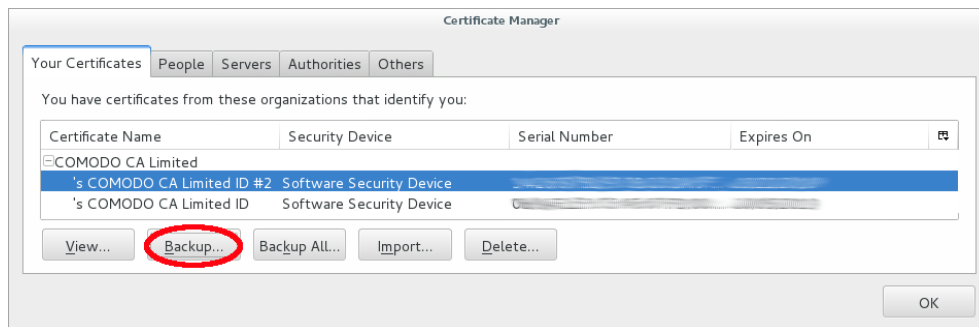
2. Highlight the line showing your new key. It will be under the name of the CA you chose (e.g. the line under "COMODO CA Limited" if you chose Comodo).

3. Click "`Backup...`" to export the key.

4. Save the file somewhere with a filename of your choice. It will likely be given a `.p12` extension.

5. You will be prompted for a password for the backup file. A weak password is fine, because this backup file will not be transmitted or retained for long. You will import it into Outlook locally, and then you will delete the backup file.

3.2.3 Import your key into Outlook

Watch YouTube video n3rOEpGjrc (the link of which jumps you to the relevant point in the video) or follow the steps below to import your key into Outlook 2013.

1. Go to File ≫ Options ≫ Trust Center (left pane) ≫ Trust Center Settings..

2. Go to Email Security (left pane) ≫ Digital IDs (Certificates) ≫ "`Import/Export`" (button)

3. Click "`Browse..`" (button)

4. Select the backup file that was produced in section ?? or ??.

5. In the "`Password`" field enter the password that was chosen at the end of section ?? or ??.

6. Click "`OK`" in the pop-up dialog and the next window.

7. After the key is imported into Outlook, you should delete the backup file. (You can always create a new backup file from Firefox if needed).

3.3 Configuring Outlook

Follow this document. That link skips the top portion and takes you straight to "How to set up your e-mail certificate in Outlook" because you already have a "digital ID". That will configure Outlook for using your certificate.

3.4 Distribute your S/MIME certificate (aka public key)

In short: simply send an e-mail to the recipient using Outlook, and sign the message.

Detailed explanation: You have a pair of keys (these were created in section **??**). One is a public key and the other is a private key. The public key must be sent to those who will send you encrypted e-mail. They will use your public key to encrypt messages to you. Your public key is automatically contained in the signature of all messages you sign.

So to distribute your public key, simply send the other party an signed e-mail from Outlook. Encrypting this key distribution message is optional, but it must be signed. They can then extract your public key from your signature.

4 Prep to send encrypted mail

Before you can send someone an encrypted message, you need the recipients S/MIME certificate (public key). This will normally come to you when they send you a signed message, at which point you can extract the certificate. The certificate must then be associated to that person in your address book.