

Crypto setup on Outlook

October 12, 2017

Contents

1 Prerequisites

- Workstation with a Mozilla-based browser installed (e.g. Firefox). Chrome/Chromium will not work because it cannot handle key generation (as of the time of this composition). Alternatively, IE may work as well, and in fact may even be better because it's more likely to store the key where Outlook needs it.
- MS Outlook 2013 or later (earlier versions officially support S/MIME but users often report difficulties, particularly with Outlook 2010)








2 Prep to receive encrypted mail or to send signed mail

2.1 YouTube video (alternative to this document)

There is a YouTube video that gives an excellent demonstration of the whole process using Comodo for the certificate authority. The demo is suitable for Outlook 2013 and 2016 users. It video starts with some blather, but this link skips straight to the relevant part. That video is thorough enough to replace this entire document.

2.2 Get an S/MIME certificate

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

certificate authority ("CA")	price <small>(for non-commercial individual use)</small>	validity	notes
	gratis	6 24 mos.(criteria)	community driven
	gratis	1 yr	
	gratis	1 yr	
	gratis	1 yr	recommended; assumed choice by this guide
	≥\$20		
	≥\$19		
	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).

2.2.1 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 ??

2.2.2 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.

2.3 Installing your certificate into Outlook

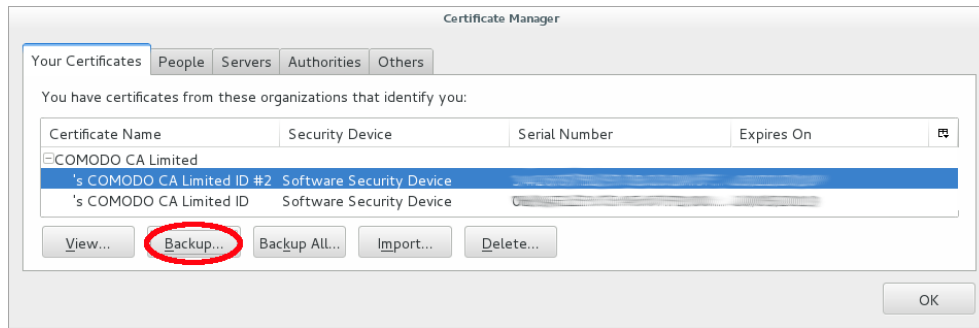
According to this document, Outlook already has your key at this point and no export/import are needed. Follow that document but ignore the top portion because you already have a “digital ID”, and scroll down to “How to set up your e-mail certificate in Outlook”. That will configure Outlook for using your certificate. If there are no issues with the key assignment step (that is, you were able to find your Comodo key), then you can skip the rest of the section.

2.3.1 If the key was not in the Trust Center..

Some Outlook users have reported that in their environment (Windows and Outlook versions) the key is not automatically visible in Outlook. **If your Comodo key was not found** in the Outlook “Trust Center”, then watch this YouTube video or follow the steps below to export the key from the browser and then import it into Outlook. That video demonstrates using Outlook 2010 for the mail client and Firefox for the browser. Ignore the beginning segment about using Symantec to create a key (Symantec no longer offers the service; Comodo is recommended).

These steps assume Firefox was used for the key creation:

1. (Firefox) 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.
6. Now your private key must be imported into Outlook. I’m not entirely sure how to do it, but this document gives the steps for configuring Outlook as needed. Ignore the top of the document because you already have a “digital ID”, and scroll down to “How to set up your e-mail certificate in Outlook”. This will take you to the “Trust Center”, the place in the settings where you can import the key from the backup file.
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).

2.4 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.

3 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.