Configuring mail.app's built-in S/MIME Cryptosystem (iOS)

December 4, 2017

Contents

1 Prerequisites

- iOS device (e.g. iPhone or iPad).

- A desktop browser is only needed initially to create SSL keys, and only if you are going to use a Certificate Authority ("CA"). The browser will not be used thereafter. Any of these browsers will work:

Browser	Key storage consistent with Apple Mail on OS/X	Notes
Chrome/Chromium (OS/X)	yes	Some versions of Chrome may have problems with key generation.
Chrome/Chromium (Windows)	not applicable	
Firefox (all platforms)	no (browser uses its own internal key store)	
~~Internet Explorer~~ (OS/X)	–	Don't use IE on Mac; latest version (4.0) is discontinued.
Internet Explorer (Windows)	not applicable	
Safari (OS/X)	yes	Some versions of Safari may have problems with key generation.
Safari (Windows)	not applicable	

If you have a Mac and intend Apple Mail to also handle encrypted messages, browsers above that are indicated "yes" for sharing the same key storage as Apple Mail are more convenient. If you only need to setup an iOS device then it doesn't matter what browser you use.

2 Prep to receive encrypted mail or to send signed mail

2.1 Get an S/MIME certificate

You have a choice in whether you want to subscribe to a Certificate Authority ("CA") or whether you want to be your own CA and generate your keys manually. The advantage of using a CA is that the recipient has less key management effort (this doesn't matter if Justin is your recipient). But CA subscriptions cost money in some situations and also limit the validity period of the key.

If you want to create your own key using Windows, install OpenSSL for Windows. Mac users will already have openssl installed. Then follow "Create a Certificate Authority to Sign A Certificate" to create your own CA and personal key pairs.

If you're opting to use a CA, then browse to one of these certificate authorities (Justin recommends Comodo via Secorio):

CA	price (for non-commercial individual use)	validity	notes
CAcert	gratis	6|24 mos. (criteria)	community driven; getting a 2yr cert requires meeting w/someone and showing state-issued proof of id
COMODO direct	gratis	1 yr	
COMODO via InstantSSL	gratis	1 yr	
COMODO via Secorio	gratis	1 yr	simple; assumed choice by this guide
Entrust	≥$20		
IdenTrust	≥$19		
StartCom	gratis	2 yrs	distrusted by Mozilla and others, thus signed msgs will likely be seen as invalid unless recipients manually add Startcom's CA key to their keystore
WoSign	~~gratis~~ n/a	~~2 yrs~~ n/a	recently **discontinued** but still maintained in this list because they intend to return to business

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 with no intent to return to service are 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).

2.1.1 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 2.2

2.1.2 If you chose "StartCom"

1. (startcomca.com)
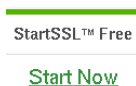
2. (startcomca.com)

3. (startcomca.com) Fill out the form.

4. (your e-mail account) A verification code will arrive.

5. (startcomca.com) Enter the verification code, click "sign up".

   The system could not install the login certificate automatically, you should install it manually. Create a "Private key password" Please click here to install the issuing CA certificate into your browser first. save a *.p7b file

6. Skip to section 2.2

2.1.3 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.

2.2 Transferring your certificate from the browser to Mail.app

If you generated your key pair manually, skip to subsubsection 2.2.4 Importing your key. Otherwise, follow the steps below to first export your key from your browser.

2.2.1 (Chrome only) Export your key from your browser

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 strong password is important because the next step will expose the file to entities who could attack it. Since this password is temporary (will only need to be typed on one occasion), a strong password will not be a burden.

2.2.2 (Firefox only) Export your key from your browser

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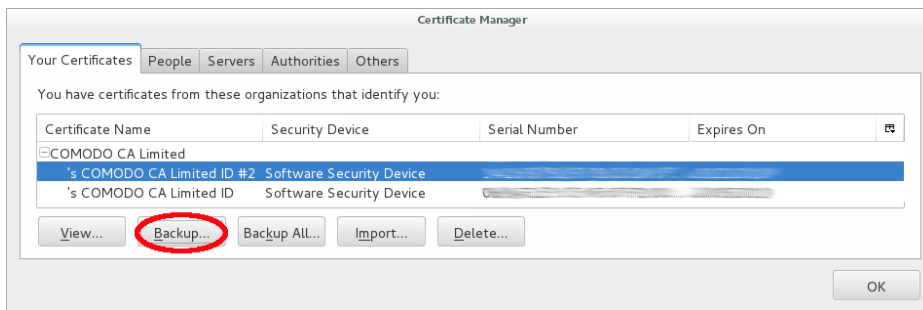
2. Highlight the line showing your new key. It will be under the name of the CA you chose (e.g. the line under "COMODO CA Limited" if you chose Comodo).

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.

2.2.3 Export your key from browsers other than Chrome or Firefox

¯_(ツ)_/¯ Try to mirror the approaches above in your browser.

2.2.4 Importing your key

1. Find the `.p12` file you either created manually or exported from a browser in previous steps. E-mail it to yourself.

Either follow the illustrated steps under "Importing your certificate into iPhone/iPad" in `https://www.comodo.com/pdf/Comodo-CPAC-iPhone-iPad.pdf`, **OR** continue with the following steps:

2. (on your iOS device, in mail.app) open the above-composed e-mail. Do this on all your iOS devices.

3. Open the file attachment by tapping it.

4. Tap "`install`" at the top right.

5. Ignore the unsigned profile warning, and tap "`install`" two more times (or as needed).

6. At the password prompt, enter the *backup* password created in step 5.

7. Tap "`Next`" at the top right.

8. Tap "`Done`" at the top right.

9. (optional) The key backup file and e-mail carrying it may be deleted and the password may be forgotten at this point. There is no further use for them. The backup file can always be re-created from Firefox if the key must be imported to other iOS devices later.

The new certificate will expire (see "validity" in section 2.1).

2.3 Enabling S/MIME functionality in mail.app

Either follow the illustrated steps under "Enable S/MIME for your mail account" and "Enable signing and encryption" in `https://www.comodo.com/pdf/Comodo-CPAC-iPhone-iPad.pdf`, or continue with the following steps:

1. (iOS device) go to: Settings ≫ Mail, Contacts, Calendars ≫ Accounts: (e-mail service provider for the address you created a key for) ≫ IMAP: Account... ≫ Advanced ≫ S/MIME.

2. enable it

3. go to: "`Sign`" and enable it. There will be an address under "Certificates" if the certificate installation worked earlier.

4. repeat the above step for "`Encrypt`"

5. go back: **Account** ≪ Advanced

6. tap "`Done`" in the top right corner.
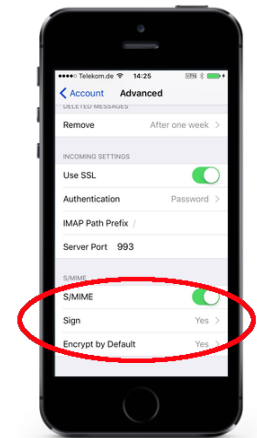
2.4 Distribute your S/MIME certificate (aka public key)

In short: simply send an e-mail to the recipient using mail.app. If you created your own CA and key pair manually instead of using your browser to subscribe to a CA, then you must also send the `ca.crt` file that you created.

Detailed explanation: You have a pair of keys (these were created in section 2.1). 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 send using mail.app (because you enabled S/MIME signing in section 2.3).

So to distribute your public key, simply send the other party an e-mail from mail.app, which need not be encrypted. They can then extract your public key from your signature (which is composed as an attached file named "`smime.p7s`").

3 Prep to send encrypted mail

Before you can send someone an encrypted message, you need their S/MIME certificate (public key). Follow section 2.3 if you haven't already done so, but instead of configuring the e-mail service provider for your own key, choose the e-mail service provider you will send the encrypted messages from (if different). Then follow the next section (3.1):

3.1 Importing the S/MIME certificate of another party

1. Ask the other party to send you a signed message.

2. Open the signed message in mail.app. Successfully signed messages have a blue ten-point star with a check in the center, which appears to the right of the senders address. E.g.
   From: **Bruce W. Moore...** ✪ ›
   To: Kristin Moore ›

3. Tap the *From* address.

4. Tap "`View Certificate`".

5. Tap the "`Install`" button.

6. Tap "`Done`" on the top right corner.

Now you can send encrypted messages to the sender.