

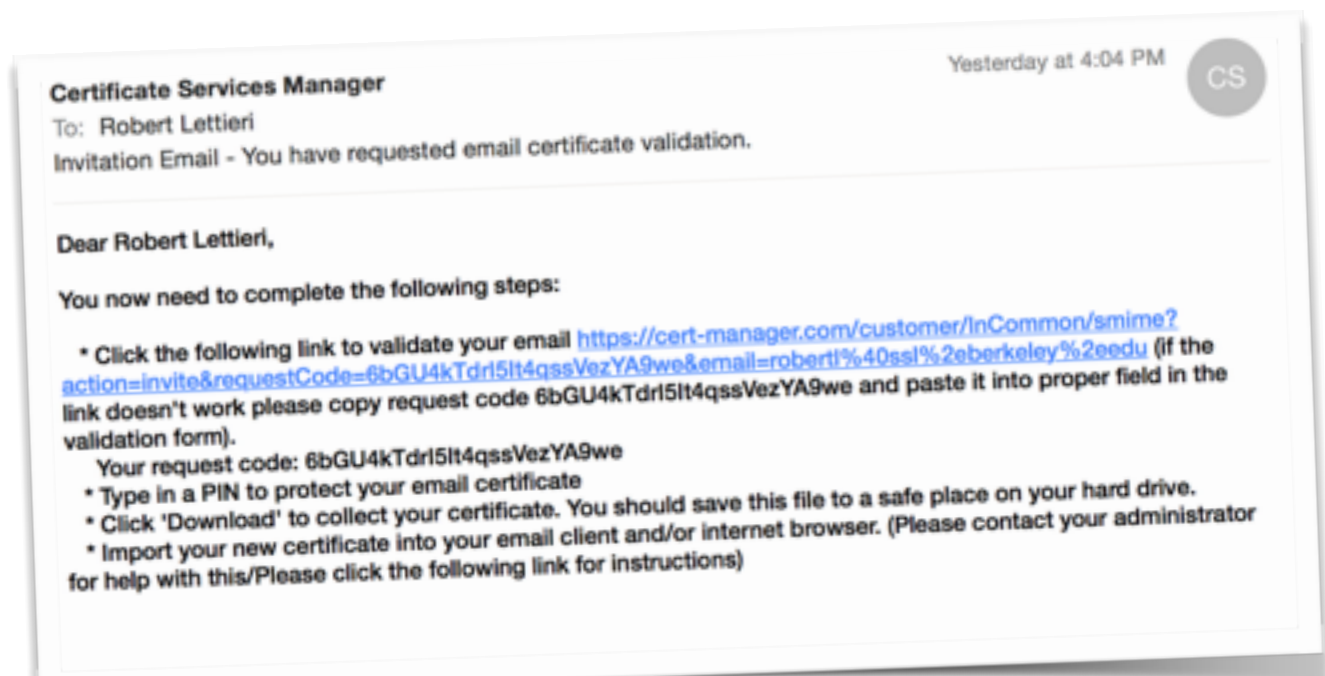
Setting up to digitally sign e-mail (Mail.app Mac OS X)

Part 1 - Getting a Certificate

What you need to know before you start:

- To request a certificate, send email to ssl-sysadmin@ssl.berkeley.edu with the title "Request Signature Certificate". Also send email to this address if you have any questions.
- You must have an @ssl.berkeley.edu email address to proceed. We don't handle Signature certificates for @berkeley.edu or other email addresses.
- Signature certificates are only available to active (i.e. paid) SSL employees. Volunteers and affiliates are not eligible.
- These certificates can be used to sign and/or encrypt emails or other documents. However, there is no "key escrow" (i.e. password recovery) available for them. If you lose your password, there is no way for us to recover it for you, hence there will be no way to decrypt the document anymore.
- In most cases you'll be "signing" PDF documents, make sure you **Acrobat XI (11)** installed. If you don't ask for it.

Once the certificate is generated you will get an email. If it asks for a pin or password, make absolutely sure you never forget it. Once you forget it, there is no way of unlocking signed documents.



Follow the link in the e-mail

The screenshot shows the 'User Registration' page of the InCommon Certificate Manager. The page has a header with the InCommon logo and the text 'Certificate Manager'. Below the header is a red bar with the text 'User Registration'. The form contains several fields: 'Code' (6bGU4kTdr15It4qssVezYA9we), 'Email' (roberti@ssl.berkeley.edu), 'PIN', 'Re-type PIN', 'Pass-phrase', and 'Re-type pass-phrase'. A purple box highlights the PIN, Re-type PIN, Pass-phrase, and Re-type pass-phrase fields. Below these fields is a section titled 'Select address fields to remove from the certificate.' with a table of address fields and 'Remove' checkboxes. The fields are: 'Address1' (200 California Hall #1500), 'Address2', 'Address3', 'City' (Berkeley), 'State or province' (California), and 'Postal Code' (947201500). At the bottom of the form are 'Submit' and 'Cancel' buttons.

You'll need to fill this info out. DON'T forget this we can not recover it for you. The PIN will be your Password. The Pass-Phrase is used to delete your Cert if lost.

Do not change any of this info

The screenshot shows a 'Digital Certificate download' dialog box. It has a red header with the text 'Digital Certificate download'. Below the header is a red line of text: 'Please save your digital certificate in safe place.' At the bottom of the dialog box are 'Download' and 'Cancel' buttons.

Remember the location of the downloaded certs.

Part 2 — Setting up Mail.app (Mac OS X)

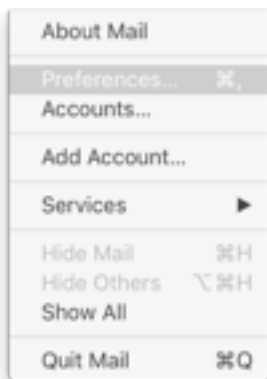
Once you get your certificate, you can digitally sign your e-mails. Locate the file you download. It should have a file extension of .p12 and icon like this:



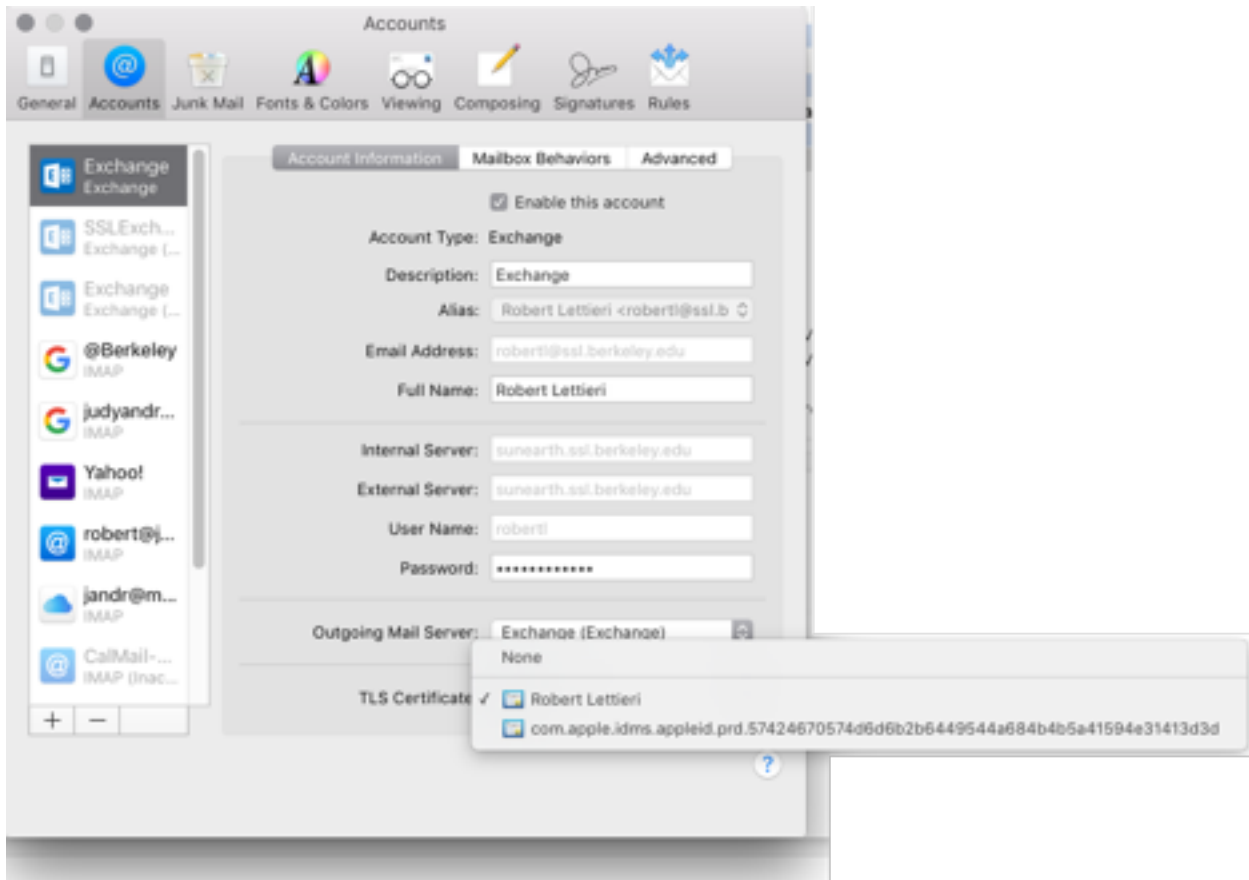
Double-click the certificate file, this will open KeyChain Access and ask you for the PIN (password) for the Certificate that you set in Step 1.

This will install the Certificate at the OS level and be available to other applications. Because the certificate is based on your e-mail address mail.app will just use it. If it doesn't automatically pick it up you'll need to set it.

From the Mail Menu choose Preferences:




Choose Your Name from TLS Certificate pop-up:





To Send Encrypted E-Mail



If you have added your personal certificate you should see this icon  this means your are sending encrypted e-mail.

If you see this icon  you either are not sending from your @ssl.berkeley.edu account or you didn't install the certificate.

The second icon on the bar is a lock. If the lock is closed, locked  this means that you have the persons public certificate and this e-mail will be encrypted.

If the lock icon is unlocked , your e-mail will NOT be encrypted.