Signing and Encryption: Configuring Apple Mail

As long as you have imported your certificate into the OS X Keychain, Apple Mail detects the certificates and uses them.

1. When you open the Mail application after importing your certificate, a prompt will appear:

![Mail wants to use your confidential information stored in “privateKey” in your keychain. Do you want to allow access to this item?](image)

By selecting “Always Allow” you are permitting Mail to use your personal signature to sign your emails.

2. By selecting “Always Allow” you are permitting Mail to use your personal signature to sign your emails.

3. Under Options you can select the desired signing and encryption settings:

![Options for signing and encryption settings in Apple Mail](image)

4. When composing a new message, the Mail client will notify you that the message will be signed:

![Message will be digitally signed and encrypted](image)
You can send an encrypted message only if you have the recipient’s public key. If you do not, Mail displays the following message: “This message cannot be encrypted because you do not have the public key for destination email address. Do you want to send the message without encryption?”