SECURITY BEST PRACTICES FOR
USING S/MIME WITH PERSONAL CERTS IN THUNDERBIRD AND FIREFOX ON A MAC

S/MIME (RFC5751) is a technology that will let you cryptographically sign and/or encrypt your email using a personal certificate. This document is for S/MIME using Mozilla Thunderbird on an Apple Mac.

PART 1. GETTING READY TO USE S/MIME (YOU'LL ONLY NEED TO DO THIS ONCE)

1. Install Firefox and Thunderbird If You Don't Already Have Them Installed.

You can get them online from:
http://www.mozilla.com/en-US/firefox/new/
http://www.mozillamessaging.com/en-US/thunderbird/

2. Configure Thunderbird to use your email account.

In Thunderbird, go to Thunderbird --> File --> New --> Mail Account... You'll need to know:

- Your email address and password
- The name of your outgoing mail server (this is often known as the SMTP server)
- The name of your incoming mail server (this is often known as your IMAP server).

Caution: do not use POP (instead of IMAP) unless specifically advised by local support staff to do so. POP will download your email onto your local workstation, and may delete it from the server unless you tell Thunderbird to "leave mail on server." If you need help, check with your IT help desk folks.

2. Obtain A Comodo Personal Certificate. For test/trial use, individuals can obtain a free personal certificate at http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html
Use Firefox to collect your certificate by following the instructions that will be sent to your email address.

When you collect your certificate from that vendor, it will automatically be installed in Firefox on the system you're using at that time. **NOTE:** *Do NOT accidentally collect and install your personal certificate on a shared system (such as a machine in a computer lab)!*

3. Export A Copy of Your S/MIME Private Key From Firefox. In Firefox, go to Firefox --> Preferences --> Advanced --> Encryption --> View Certificates --> Your Certificates. Highlight your certificate by clicking on it, then click Backup. Save the file as a PKCS12 file with a name of your choice, such as myprivatekey.p12 You will need to provide a strong password for this file. (Never share that file! Save a copy of that file on a CD or thumb drive somewhere safe, such as in your personal safety deposit box. Don't forget to also save a copy of the password you'll need to access the contents of that file!)

4. Import Your S/MIME Private Key Into Thunderbird. In Thunderbird, go to Thunderbird --> Preferences --> Advanced --> Certificates --> View Certificates --> Your Certificates. Click Import. Select the S/MIME private key exported in Step 3. You'll need to provide the password you used when saving that file.

5. Select That Private Key For Your Email. In Thunderbird, go to Thunderbird --> Tools --> Account Settings. In the left hand column, click on the account you set up in step 1. Click View Settings For This Account. Click Security. In the Digital Signing pane, click Select. Select the certificate you imported. You will also be asked if you would like to use the same certificate for encrypting and decrypting messages sent to you. Click Yes. Click Okay to close the window.

Disclaimer: All opinions expressed in this document are those of the author and do not necessarily represent the opinion of any other entity.

PART 2. S/MIME SIGNING A MESSAGE YOU'RE SENDING IN THUNDERBIRD.

1. Begin Writing a Message As You Normally Would in Thunderbird. In Thunderbird, go to Thunderbird --> File --> New Message, and create a new test email message to a friend or colleague. Once you've finished writing it, do NOT send it yet -- you still need to cryptographically sign it.

2. Digitally Sign The Message. In Thunderbird, go to Thunderbird --> Options --> Digitally Sign This Message.

3. [Optional] Confirm That This Message Will Be Sent Digitally Signed. In Thunderbird, in the window where you're composing your message, click on the yellow security padlock and confirm that "The contents of your message will be sent as digitally signed" says "Yes." Click Okay.

4. Go Ahead And Send the Message As You Normally Would. In Thunderbird, in the window where you're composing your message, click Send.

Note #1: When your friend or colleague receives your cryptographically signed message, they will get the body of the message as they normally would, but they will also receive an additional S/MIME signature. If they are S/MIME enabled, their email client will automatically validate (or check and confirm) your messasge's cryptographic signature. If they're not S/MIME enabled, they can simply ignore the S/MIME signature (it will be an attachment called smime.p7s).

Note #2: When your correspondent receives your S/MIME signed message, they will automatically fetch your S/MIME public key. At that point, if they are S/MIME enabled, they will be able to send encrypted mail to you. If you would like to send encrypted mail to them, have them begin by sending you a signed email so you'll automatically get their S/MIME public key.

PART 3. ENCRYPTING A MESSAGE YOU'RE SENDING TO SOMEONE WITH THUNDERBIRD

Note: In order to be able to send an S/MIME encrypted message to someone, they first need to send you a signed message, as described in Part 2, above. By doing so, they'll automatically share their public key with you. Once you've received at least one signed message from them, you'll then be able to send them an encrypted message…

1. Begin Writing a Message As You Normally Would In Thunderbird. In Thunderbird, go to Thunderbird --> File --> New Message, and create a new test email message to a friend or colleague. Once you've finished writing it, do NOT send it yet -- you still need to encrypt it.

2. Encrypt The Message. In Thunderbird, go to Thunderbird --> Options --> Encrypt This Message. (If you like, you can also optionally click Digitally Sign This Message).

3. [Optional] Confirm That This Message Will Be Sent Encrypted. In Thunderbird, in the window where you're composing your message, click on the yellow security padlock and confirm that "The contents of your message will be sent encrypted" says "Yes." Click Okay.

4. Go Ahead And Send the Message As You Normally Would. In Thunderbird, in the window where you're composing your message, click Send.

Two Potentially Important Caveats: the subject field of your message will **NOT** be encrypted! Any malware scanning your site might normally do, will NOT be done to S/MIME encrypted message traffic!