Secure Encrypted and Signed Email, FREE!

© Chuck Hauge - CPH Solutions
chaz@cphsolutions.com

If you use the Apple Mail client application in OS 10.3 or higher and would prefer to have a more secure and trusted way to send email, this is for you! Before I begin, however, I should give you a brief description of what it means to have *signed* or *encrypted* email.

Digitally *signed* email is a more secure way to send email to any email recipient from your email application. *Signed* email does not encrypt your email, but puts your public certificate on your outgoing email telling the recipient they can *trust* you, the sender. Public/Private email certificates (a.k.a. Digital ID, secure certificate, Certificate Authority key, Personal Certificates, X.509, …) are obtained through a trusted third party, such as Thawte Communications or VeriSign, and are part of the reason they are more secure. Spammers *never* use signed email.

Encrypted email is as it sounds, encrypted, so anyone other than the sender, or any of the recipient's can not read the email. *Encrypted* email is more secure than just *signed* email. But in order to send an *encrypted* email, the sender must first have the recipient's public key. In order for the recipient get a public key, they must also go through this process. There are technically other ways to send *encrypted* email than what I will describe here, but the Personal Certificate process is by far the easiest and most common method.

Here's how to setup your own Personal Certificate using Thawte Communications free Personal Certificate process. It is important to read all instructions carefully, but you can ignore references to the Web of Trust (WOT),and Certificate Bearers Name, these are more advanced subjects, and not required. You will receive email as part of the process, so you will need to open your email application to follow some instructions.

1. Go to http://www.thawte.com/secure-email/personal-email-certificates/index.html, click the Join button in the upper right corner. You need only one account for all your email addresses.

2. Go through the process of obtaining a Personal Certificate, make sure you follow al the steps, it can be a bit tedious. You need one Certificate for each email address you want to send signed/encrypted email. Use the Mozilla/Netscape key for Apple Mail, and the High Grade-2048 bit options.

3. The Certificate may take several minutes or hours to obtain via email. Once you have the Certificate, it should have a name like "deliver.exe.p7s". Depending upon your version of Mac OS and settings, the certificate may be automatically embedded in your keychain. However, if not, and if the name is truncated, add the .p7s filename

extension. Stick the original Certificate in a safe place, because it is the key to protecting your digital email identity.

4. Double-click on it; Keychain Access will launch; embed it in your personal keychain.

5. The next time you launch Mail and create a new message, two new icons should appear to the right of the Signature popup menu - a padlock  , and an “X” inside a starburst  . Click on the “X” and you should see a check mark inside a starburst  , this is digitally *signing* your email. The padlock icon should be grayed out at this point.

6. Once you've corresponded with someone using a Mac, your personal certificate (the "public key" portion) gets automatically embedded in the recipient's Keychain (for an explanation of operations on different email clients, go to http://www.thawte.com/ssl-digital-certificates/technical-support/email/sign.html and follow the link in the line starting with "To sign email on various email clients"). If interested take a look inside your Keychain; you'll find *at minimum* my own Personal Certificate, and possibly others from people who use Personal Certificates. You can send encrypted email to anyone whose Personal Certificate "public key" is in your Keychain. (Your Personal Certificate public key is actually a special kind of attachment to every email you send; it's all automatic.)

7. When you address a message to someone who’s own Personal Certificate is in your Keychain, the padlock option becomes available (it is no longer grayed out). When selected, the entire content of your message is securely encrypted, and can only be decrypted by recipients who have your Personal Certificate public key.

8. Any message sent can be verified by your recipient as having truly come from you by verifying the presence of the "digitally signed" icon and checkmark/starburst (in Apple Mail, it shows up in just below the From/Subject/Date/To: lines 

). Entourage and other email applications have their own way of noting signed emails. Any messages not actually sent by you will not bear this digital signature icon. Also, if a message is somehow tampered with in transit, the recipient will be told so because the message's checksums won't match.

There are different instructions for installing a Personal Certificate on other email applications, see the government web site in sources, below.

Sources:

http://security.fnal.gov/pki/email_with_dig_sig.html
http://docs.info.apple.com/article.html?artnum=25555
http://www.thawte.com/secure-email/personal-email-certificates/index.html