

Use a Digital Certificate to Encrypt Your Personal E-mail

Michael Chesbro

January 29, 2011

Most people recognize that e-mail is not a secure means of communication, and we are frequently warned about the dangers of sending personal or financial information via e-mail. The Federal Trade Commission (2006) states: "Don't e-mail personal or financial information. E-mail is not a secure method of transmitting personal information." The Social Security Administration (2010) similarly states: "Electronic mail is not secure. Therefore, we suggest that you don't send personal information to us via e-mail." And the government's cyber-security web-site OnGuard Online (2008) says: "Don't e-mail your financial information. E-mail is not a secure method of transmitting financial information like your credit card, checking account, or Social Security number."

However e-mail is quick and convenient, and too often this convenience outweighs the need for security. Information that should be encrypted is often sent as plaintext because encryption is just too hard, or too inconvenient, or too time consuming. Fortunately there is a simple and convenient method of encrypting e-mail between people with whom we regularly communicate - that method is a personal digital certificate.

Digital Certificates

Digital certificates are data files issued by certification authorities (CA). These digital certificates contain the data necessary to allow the user to digitally sign and encrypt e-mail messages, and add digital signatures to Microsoft Office documents (i.e. MS Word document MS Excel workbooks, and MS PowerPoint presentations).

Personal digital certificates are available from a number of CA. Three of the most popular and widely accepted are: VeriSign⁽¹⁾, Comodo⁽²⁾, and GlobalSign⁽³⁾. These digital certificates can be used with most any e-mail client that supports S/MIME (Secure/Multipurpose Internet Mail Extensions); such as Thunderbird, Netscape, Outlook, Mac Mail, and Eudora.

To obtain a personal digital certificate simply visit one of the CA web-sites, fill out the application and download your certificate. Installation varies slightly from one e-mail client to the next, but is pretty simple regardless of which e-mail client you are using. Digital certificates are valid for between 1 to 3 years, after which you must renew your digital certificate. The cost is about \$20 per year, although at the time this article was written Comodo offered a free digital certificate for personal use.

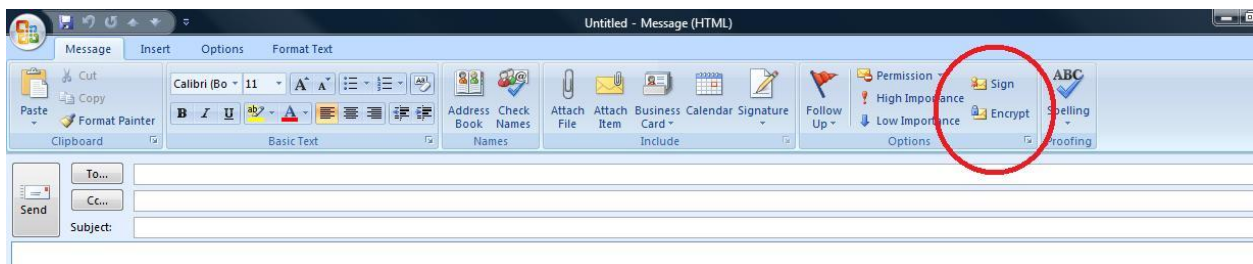
Once you have your personal digital certificate associated with your e-mail address and installed on your computer you must exchange digital certificate public keys with those individuals with whom you plan to send encrypted e-mail. There are various ways to exchange

digital certificate public keys, but perhaps the easiest is to send a digitally signed message to the person with whom you wish to communicate. That person should likewise send you a digitally signed message. Once you receive the digitally signed message you will need to add the person's certificate to your contacts. To do this (using Microsoft Office Outlook) simply open the digitally signed e-mail, right-click on the "From" address, and then click on "Add to Outlook Contacts". You are now able to send digitally signed and encrypted messages to the person you just added to your contacts list.

Encrypting E-mail Messages

Sending an encrypted message is now literally as simple as a click of your mouse. The Microsoft (2011) on-line help file explains how to encrypt a message using Microsoft Office Outlook 2007:

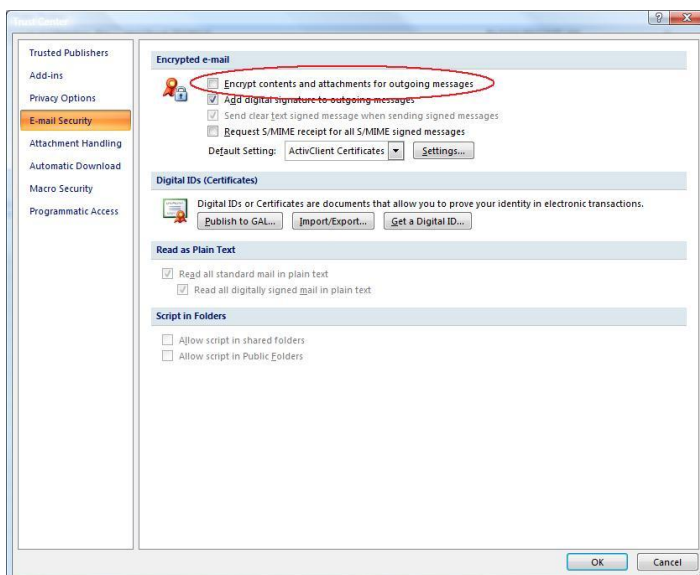
Encrypt a single message



1. In the message, on the Message tab, in the Options group, click the Encrypt Message Contents and Attachments button.

2. Compose your message and send it.

Encrypt all messages



1. On the Tools menu, click Trust Center, and then click E-mail Security.

2. Under Encrypted e-mail, select the Encrypt contents and attachments for outgoing messages check box.

3. To change additional settings, such as choosing a specific certificate to use, click Settings.

4. Click OK twice.

With your digital certificate you are now able to increase the security of your e-mail communications by encrypting any message that contains personal or sensitive information. Of course you must obtain a copy of the digital certificate of the person to whom you are sending this type of information, but as we have seen it's a simple matter to obtain and install a digital certificate. Any person who is trustworthy enough for you to exchange sensitive information with, should be responsible enough to provide a digital certificate to ensure that this information can be exchanged securely.

Encrypting your personal e-mail is a relatively simple act which returns a significant security benefit. A digitally signed and encrypted e-mail confirms that the message actually came from you, that it has not been altered during transmission, and because it's encrypted it can only be read by the intended recipient (i.e. the person whose digital certificate you used to encrypt the message).

Where to Obtain a Digital Certificate:

- (1) VeriSign - <http://www.verisign.com/authentication/digital-id/index.html>
- (2) Comodo - <http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html>
- (3) GlobalSign - <http://www.globalsign.com/authentication-secure-email/digital-id/>

References

- Federal Trade Commission (FTC). (2006). *How Not to Get Hooked by a 'Phishing' Scam*. Retrieved from <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf>
- Microsoft. (2011). *Support / Outlook / Outlook 2007 Help and How-to Encrypt e-mail messages*. Retrieved from <http://office.microsoft.com/en-us/outlook-help/encrypt-e-mail-messages-HP001230536.aspx>
- OnGuard Online. (2008). *Online Shopping Quick Facts*. Retrieved from <http://www.onguardonline.gov/topics/online-shopping.aspx>
- Social Security Administration. (2010). *Protecting my privacy on the web*. Retrieved from http://ssa-custhelp.ssa.gov/app/answers/detail/a_id/223/~/protecting-my-privacy-on-the-web.