

Outlook 2003: Digital Signatures and Message Encryption

Definitions:

Digital Signature: An electronic, encryption-based, secure stamp of authentication on a message. This signature confirms that the message originated from the signer and has not been altered.

Encrypting a message protects the privacy of the message by converting it from plain, readable text into cipher (scrambled) text. Only the recipient who has the private key that matches the public key you used to encrypt the message can decipher the message. This is a separate process from digitally signing a message.

Certificate: A digital means of proving your identity, using a public and private key pair. The private key is the secret part kept on the sender's computer that the sender uses to digitally sign messages to recipients and to decrypt (unlock) messages from recipients. Private keys should be password protected. The public key is sent to others or published in a directory, so that others can use it to send you encrypted messages.

To Use Secure Messaging:

There are four main steps to get your Outlook 2003 e-mail client set up for secure messaging:

1. Set up an account at Thawte (Thawte is a certificate authority who offers free personal e-mail certificates.)
2. Request a personal e-mail certificate
3. Install your personal e-mail certificate in Outlook 2003
4. Use your e-mail certificate in Outlook 2003

Detailed, step-by-step instructions for each of the main steps are listed below.

Setting Up A Thawte Account:

1. Go to the website: <http://www.thawte.com/email/>
2. Click on the red “**join**” button
3. Read the Terms and Conditions and then click “**next**”
4. Fill out the requested information on this page
Leave the character set as default
5. Click “**Next**”
6. Fill in your USA National Identification Number
Select the Type of number you entered

Enter your email address. This should be first-last@uiowa.edu NOT the abcdef@iowa.uiowa.edu

7. Click **"Next"**
8. Use the defaults for Language and Charset
9. Click **"Next"**
10. Enter a password twice
11. Click **"Next"**
12. Enter a Contact Number
13. Choose 5 Questions and answer them
14. Click **"Next"**
15. Confirm your Information
16. Click **"Next"**

17. Wait for the Confirmation Email
18. Click on the website link in the confirmation email
19. Enter the Probe and Ping Information from the Email
20. Click **"Next"**
21. Your Account should now be active
22. Click **"Next"**

Request A Personal E-mail Certificate:

1. Enter your account information. (This will be your email and password for accessing your account at Thawte.)
2. Click on "Request a Certificate" on the left menu
3. Click on "Request" under the title bar X.509 Format Certificates
4. Select "Microsoft Internet Explorer, Outlook and Outlook Express"
5. Click **"Request"**
6. Don't modify the Employment Information
7. Click **"Next"**
8. Select your address
9. Click **"Next"**
10. Click **"Next"**
11. Click **"Accept"**
12. Don't modify the CSP. It should say "Microsoft Enhanced Cryptographic Provider v1.0"
13. Click **"Next"**
14. Click **"Yes"** to allow the site to create a key
15. Click **"OK"** to create the new key
16. Click **"Finish"** and your certificate will be generated.

Install Your Personal E-mail Certificate in Outlook 2003:

1. Go to this URL: <https://www.thawte.com/cgi/personal/cert/status.exe> This will list your generated certificates

2. Click on "**MSIE**" on the first certificate.
3. Click on "**Fetch**"
4. Click on "**Install Your Cert**"
5. Click on "**Yes**" to allow the cert to be installed
6. Click "**Yes**" again
7. Your Certificate is now installed.
8. Click **OK**

Using Your E-mail Certificate In Outlook 2003:

1. In Outlook 2003 go to **Tools | Options | Security**
2. Check "*Add Digital Signature to Outgoing Messages*" (Note: Use this option if you want all messages to be digitally signed. Otherwise leave it unchecked, and press the "Digitally Sign Message" icon only in those individual messages you wish to sign.)
3. Check "*Send Clear Text Signed messages when sending signed messages*".
4. Click the "**Settings**" button next to the Default Settings Dropdown
5. Click "**New**"
6. Enter a Name
7. Click "**Choose**" across from Signing Certificate
8. Select your Cert
9. Click "**OK**"
10. Click "**OK**"
11. Make sure the Setting you just made is in the Default Settings Box
12. Click "**OK**"

Notes:

Message Digital Signatures: You can send a Message Digital Signature to anyone. By default your Message Digital Signature will be turned on if you selected that option in number 48 above. Otherwise, sign a message by pressing the "Digitally Sign Message" icon when composing the message.

Message Digital Encryption: In order to use the Message Digital Encryption feature, (e.g., to exchange encrypted messages between yourself and someone else), you will need to first send a Digitally Signed message to the person, thus sending him your Public key. Next, the recipient will have to reply to your message, thus sending you their Public Key. Once you both have each other's Public Keys you will be able to begin sending encrypted messages to one another. Both parties must have a personal certificate, and both parties must have an e-mail client which supports S/MIME.

To send an encrypted message, just type your message and press the "Encrypt message content and attachment" icon, then press the Send button. This option will encrypt both the message text and the attachment included with the message

into one “package”. When the recipient opens the received message, they will see that the message was encrypted, and can also check the certificate and encryption details.

NOTE: Encrypting a file and then attaching it to a regular, clear-text message for sending will FAIL. The University’s Anti-Virus/Anti-Spam system will drop any message with an attachment that it can’t scan for viruses.

NOTE: If you don’t have the recipient’s Public Key, you will get a warning message telling you that the message cannot be encrypted.