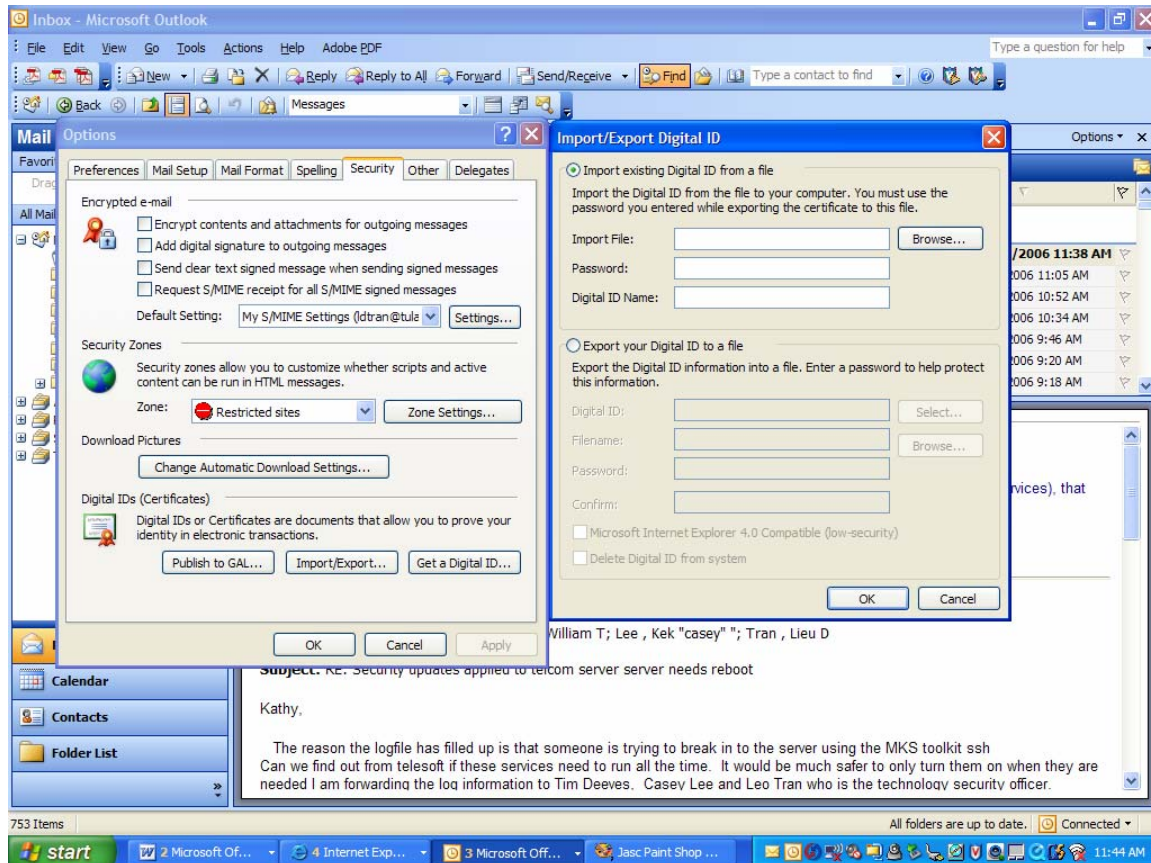


# Configure e-mail and message security in Microsoft Outlook 2003

After installing the Digital Certificate you will now need to configure Microsoft Outlook to use the new message security features.

## Import your Digital Certificate to Outlook

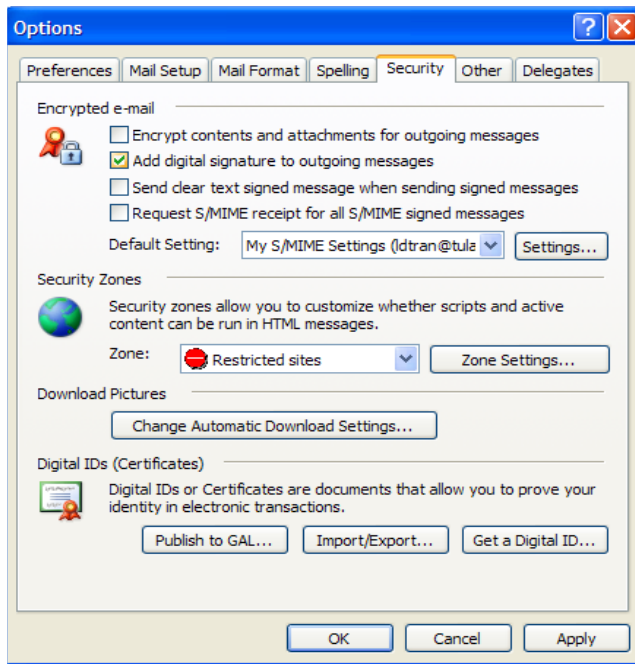


Enter the **Import File** and **password**. This is the file you saved when exporting the Digital Certificate. Enter your name for **Digital ID name** then click OK

**Digital signing an e-mail message:** Digitally signing a message applies your signature to the message. This includes your digital certificate and public key.

Your digital signature proves to the recipient that the contents of the message were signed by you and not an imposter, and that the contents have not been altered in transit.

- In the message, click Options.
- Click Security Settings.
- Select the Add digital signature to this message check box.



d. If available, you can select one of the following options:

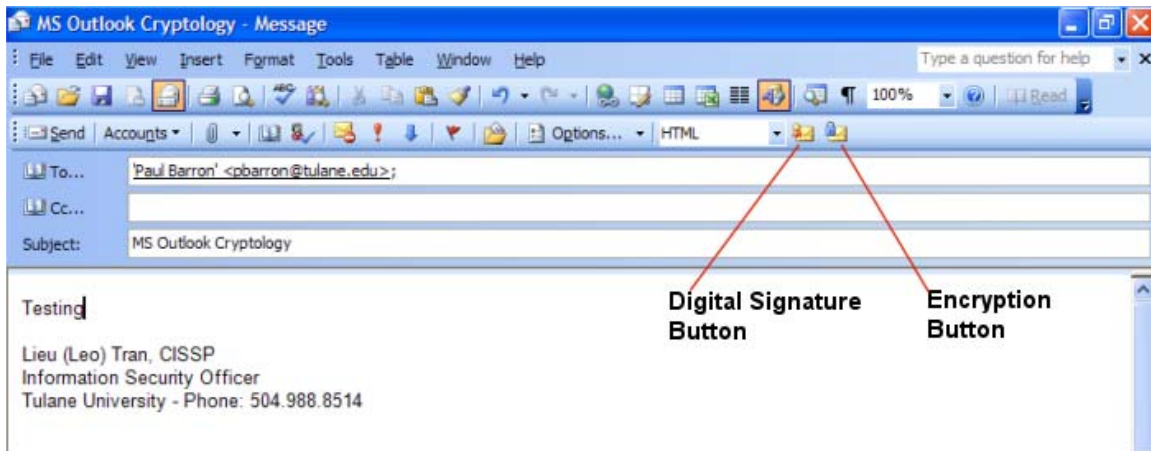
- If you want recipients who don't have S/MIME security to be able to read the message, select the Send this message as clear text signed check box. By default, the check box is selected.
- To verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered, as well as notification telling you who opened the message and when it was opened, select the Request S/MIME receipt for all S/MIME signed messages check box. When you send a message with an S/MIME return receipt request, this verification information is returned as a message sent to your Inbox.

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

f. Click OK three times.

g. Compose your message and then send it.

Alternatively, you can click on the **Digital Signature Button** to digitally sign the message.



**Encrypt an e-mail message.** 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 can decipher the message. This is a separate process from digitally signing a message.

- a. In the message, click Options.
- b. Click Security Settings.
- c. Select the Encrypt message contents and attachments check box.
- d. To change additional settings, such as choosing a specific certificate to use, click Change Settings.
- e. Click OK three times.

Or alternatively, you can click on the **Encryption Button** to encrypt the message.



### **Importance information about Encryption**

In order to send encrypted message, you need to swap the public key with the recipient.

#### **For recipient outside of Tulane Exchange Server**

- a. Send a digitally signed message. The recipient adds your e-mail name to Contacts and in doing so also adds your public key.
- b. Send a message with your .cer file attached or give a floppy disk with the .cer file. The recipient can import the .cer file into your contact card.
- c. Create a contact card with your .cer file, and then send the contact card.
- d. Post your public key to a Public Key Infrastructure (PKI) database.

#### **For recipient with an Exchange Mailbox**

Publish your public key to the Exchange Global Access List

- a. In the message, click Options.
- b. Click Security Settings.
- c. Under the Digital Certificate Section, Click Publish to GAL.