Report Number: I33-002R-2005

Guide to Using DoD PKI Certificates in Outlook

Security Evaluation Group

Authors:
Margaret Salter
Mike Boyle

Updated: June 9, 2005
Version 4.0

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

SNAC.Guides@nsa.gov

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 and XP systems and should not be applied to any other Windows versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of Sep. 1, 2004. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows operating system.

This Page Intentionally Left Blank

Trademark Information

This Page Intentionally Left Blank

Table of Contents

Table of Figures

Introduction

The purpose of this guide is to provide detailed information on the configuration of Outlook 2000, 2002 or 2003 for Windows 2000 or XP in order to allow the use of DoD PKI Certificates that do not contain the email address, or contain an incorrect email address. It will also provide detailed information on enabling the checking of Certificate Revocation Lists (CRLs) in Outlook. The instructions in this guide are meant to be applied to Windows 2000 or XP and may not work with Outlook installed on Windows NT.

Currently, DoD PKI issues three certificates: two for signing and one for encryption. One of the signing certficates contains the user's email address; the other one doesn't. Once most applications can accept the authentication certificate without the email address DoD PKI plans to discontinue issuance of the signing certificate containing the email address. At that time, they will also stop including the email address in the encryption certificate. In this guide, detailed instructions are given that will allow a user to use these certificates in Outlook when DoD PKI no longer issues certificates containing the email address. These instructions also allow a user to use his DoD PKI Certificate with an email account that has a different address than that specified in his email certificate.

In addition, this guide describes how to enable CRL checking in Outlook. This allows users to check the revocation status of certificates received in emails.

Getting the Most from this Guide

The following list contains suggestions to successfully use the *Guide to Using DoD PKI Certificates in Outlook:*:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
  - Perform a complete backup of your system before implementing any of the recommendations in this guide.
  - Ensure that the latest Windows 2000 or XP service pack and hotfixes have been installed. For further information on critical Windows updates, see the Windows Update web page.

Follow the security settings that are appropriate for your environment.

About the Guide to Using DoD PKI Certificates in Outlook

This document consists of the following chapters:

Chapter 1, "Outlook Certificate Configuration," contains information on configuring Outlook to use DoD PKI certificates, suppressing name checking to use certificates without email addresses, enabling service release features, and checking Certificate Revocation Lists (CRLs).

Appendix A, "References," contains a list of resources cited.

Chapter 1

Outlook Certificate Configuration

Previous versions of Outlook are compatible with S/MIME version 2. In S/MIME version 2, certificates for email are required to have the correct email address in the certificate. In S/MIME version 3, the email address is not required to be in the certificate. Microsoft Outlook 2000, 2002 and 2003 can be configured to conform to S/MIME version 3 and use any valid certificate for email. In addition, Outlook 2000 and above can be configured to check Certificate Revocation Lists (CRLs) for the entire certificate chain of an email certificate. This paper shows the changes that need to be made to the configuration of Outlook to permit the use of future DoD PKI Certificates without the email address (or with an incorrect email address). It also explains how to enable checking of CRLs. Throughout this guide we assume that the operating system is Windows 2000 or XP.

DoD PKI Certificates

The DoD PKI intends in the future to issue two certificates to all users - one certificate to be used for encryption and one to be used for signing. These certificates will not contain any user information that changes frequently. The email address of the user, for instance, will not be in the certificate. Both of these certificates are used for email, one to sign outgoing messages and one to decrypt incoming encrypted email. The certificates will contain an extension called the Certificate Revocation List Distribution Point (CDP). This extension should contain a URL that is used to obtain the latest CRLs from the DoD. Below are the instructions for enabling this feature in different versions of Outlook.

Suppress Name Checking In Outlook 2000

To use a certificate without an email address in Outlook 2000, you need to have your system administrator create the following registry key:

`HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Office/9.0/Outlook/Security`

Then add a new DWORD value called `SupressNameChecks` and set it to `0x1`. The conscientious spellers out there will want to note the misspelling of the word `Supress` in this key. Make sure that it is spelled exactly as above (with only one p in `Supress`). This will allow the use of certificates without the email address check being applied.

Suppress Name Checking In Outlook 2002

To use a certificate without an email address in Outlook 2002, you need to create the following registry key if it is not already present on your system (this can be done by the user, since it only affects the currently logged on user's registry settings).

`HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/10.0/Outlook/Security`

Then add a new DWORD value called `SupressNameChecks` and set it to `0x1`. The conscientious spellers out there will want to note the misspelling of the word `Supress` in this key. Make sure that it is spelled exactly as above (with only one p in `Supress`). This will allow the use of certificates without the email address check being applied.

Suppress Name Checking In Outlook 2003

To use a certificate without an email address in Outlook 2003, you need to create the following registry key if it is not already present on your system (this can be done by the user, since it only affects the currently logged on user's registry settings).

`HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/11.0/Outlook/Security`

Then add a new DWORD value called `SupressNameChecks` and set it to `0x1`. The conscientious spellers out there will want to note the misspelling of the word `Supress` in this key. Make sure that it is spelled exactly as above (with only one p in `Supress`). This will allow the use of certificates without the email address check being applied.

Choose the DoD PKI Certificates

To use your DoD PKI Certificates to sign and receive encrypted email.

- Open Outlook
- Click on the **Tools** menu and select **Options**.
- Select the **Security** tab
- Click on the **Settings** button.
- Click on the **New** button to create a new set of security settings. Give the setting a name. If you wish to use this setting as default for all email messages, check the default buttons.
- Use the **Choose** button to select the certificates to be used for signing and encryption. Since currently the DoD PKI issues two certificates that can be used for signing, you will be presented with a choice of two DoD issued certificates for signing.

Figure 1 – Choosing a Signing Certificate

To tell the difference between the two certificates, expand the *Issued by* field by dragging the separator bar to the right.

Figure 2 – Expanding the Issued by Field

The certificate issued by the EMAIL CA contains the email address, the other does not. Choose the certificate that does not contain the email address. Click OK to finish choosing a signing certificate. Next choose the encryption certificate. Since the DoD PKI only issues one certificate for encryption, you should only have one choice. Select that certificate and click OK.

- Now you are back in the Security Settings Preferences window. You should also select SHA1 as the hash and 3DES for encryption. These certificates will now be used to sign and encrypt your email.

Figure 3 – Changing the Security Settings Dialog Box

For any given message that you are sending, you can check that these settings are the ones being applied to the message. The instructions are slightly different for different versions of Outlook.

For Outlook 2000:

- In the message composition window under the **File** menu, choose **Properties**.
- Select the **Security** tab. Choose the **Security Setting** that you created using the window above. Make sure that you have chosen to encrypt and/or sign the message. (See **Figure 4**)

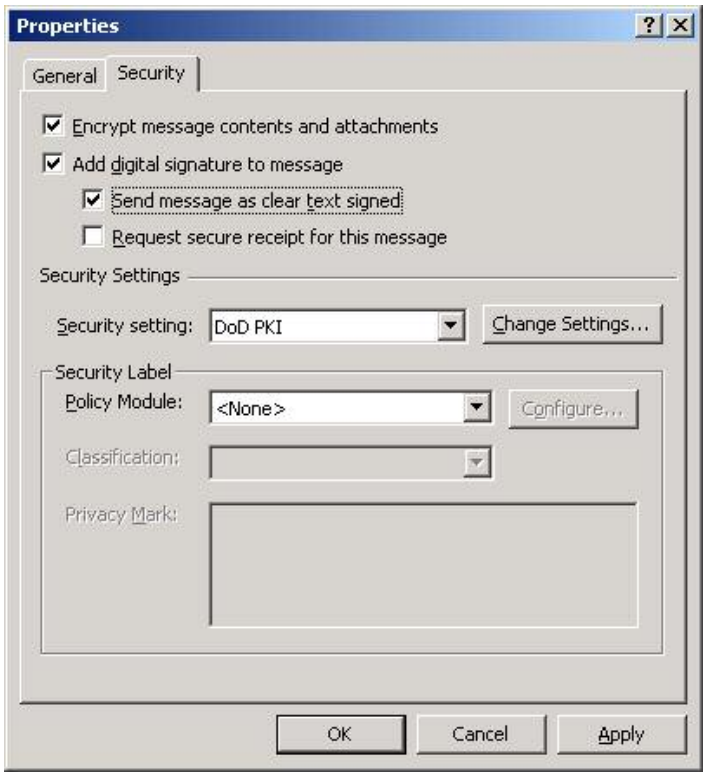

Figure 4 – Checking Security Setting Dialog Box

For Outlook 2002 and 2003:

- In the message composition window select options. Then click the Security Settings button. Choose the **Security Setting** that you created earlier (shown in **Figure 3**). Make sure that you have chosen to encrypt and/or sign the message. (See **Figure 5**)

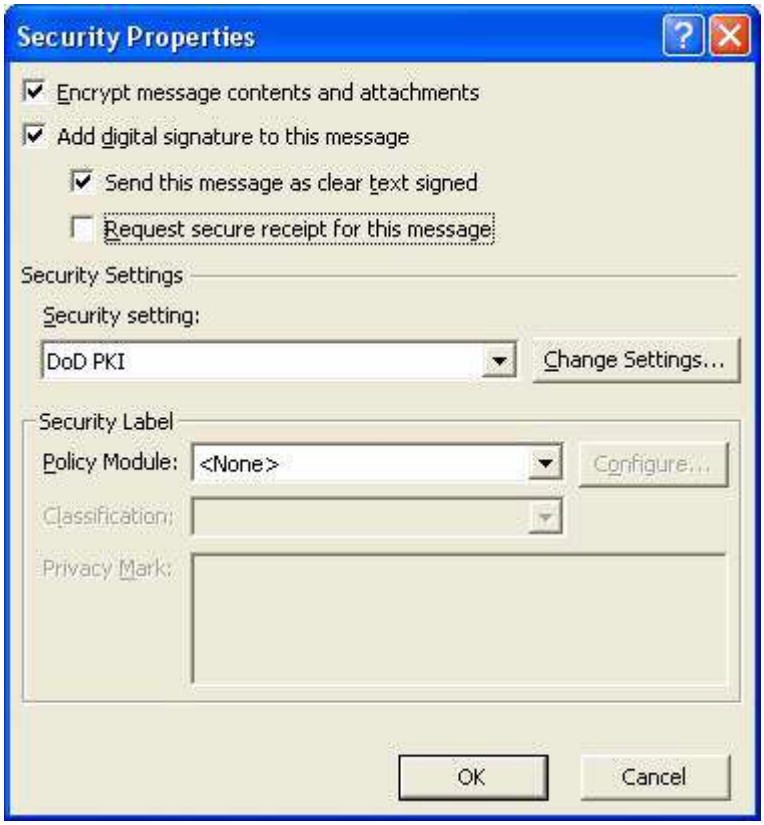

Figure 5 – Checking Security Setting Dialog Box

Enable Service Release Features in Outlook 2000

Outlook 2000 can be configured to display more information about the certificates being used in the email tool. Specifically, the status of the CRLs for the certificates can be displayed. To enable these extra security displays, you need to have your system administrator edit the following registry key:

`HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Office/9.0/Outlook/Security`

Then add a new DWORD value called `EnableSRFeatures`, and set it to `0x1`. Once this setting is added, you will see that the displays of information are different when you click on either the certificate icon or the lock icon on any signed or encrypted email. Outlook 2002 and 2003 have this enabled by default.

Get and Check the CRL for Outlook 2000

Outlook 2000 does not currently download the CRL without some modification to the registry. The system administrator needs to add the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\{7801ebd0-cf4b-11d0-851f-0060979387ea}`

Then add a new DWORD value called `PolicyFlags` and set it to `0x00010000`. This causes Outlook to download the CRL the next time it processes a certificate. To verify that the CRL was downloaded, open Internet Explorer and perform the following steps:

- In the Internet Explorer menu, select **Tools → Options**
- Click the **General** tab
- Click **Settings**. This will present you with another dialog box.
- Select **View Files** and you should see the CRLs in the Temporary Internet Files.

Unfortunately, the Outlook 2000 display still indicates that the CRLs were not checked. To get the results of the CRL checking displayed by the Outlook software, you must have installed Service Pack 3 or greater for Windows 2000.

CRL Checking and Reporting for Outlook 2002 and 2003

By default, when a CRL Distribution Point Field (CDP) is present in a certificate, Outlook 2002 and 2003 attempt to retrieve the CRL from the URL in the CDP. Errors that occur in checking the certificates or verifying the email message will be displayed to the user by default.

In Outlook 2002 and 2003, you will notice that a Signed By field is also displayed so that you can easily check the signer of the message. Notice that in **Figure 6,** the email was sent by Joe User, but it was signed by User.Joe.3010002571. This is how a message sent using SupressNameChecks will appear to the recipient. The message was actually sent by Joe User using his email account user@lemon.dod but he used a certificate that contained no email address. In this case the Common Name of the sender will appear in the Signed By field. If there actually was an email address in the certificate, that is what would appear in the Signed By field. To encrypt a reply to this message, the recipient would need to *Suppress Name Checking* on his machine. Otherwise Outlook will pop up an error message.

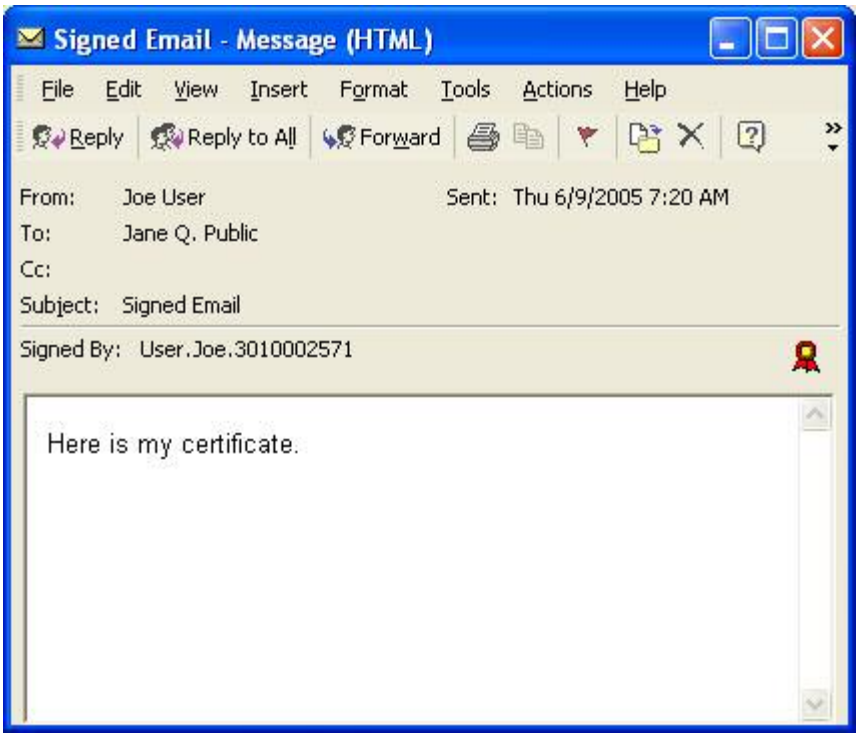

Figure 6 – Outlook Pane

Adding User Certificates to the List of Contacts

To encrypt a message to another person, you must have a copy of their encryption certificate located in a place where Outlook can find it. The simplest way to do this is to have the person send you a signed email. View the signed message in the Message pane. Then highlight the sender's address and right click. Select Add to Contacts.

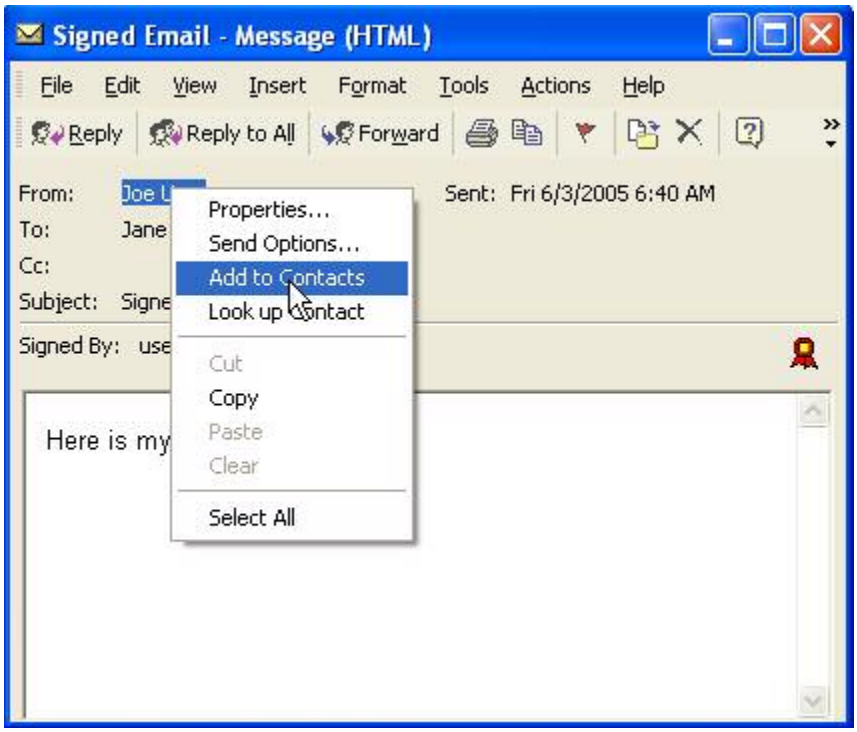

Figure 7 – Adding a Person to Contacts

If the person that you are adding to the contacts list has a different email address in the certificate than the address that they used to send the email, you will see the following message.

Figure 8 – Address Mismatch Warning

As long as the signature is valid and the Common Name of the sender matches the name that you expect to see, it is ok to ignore this warning and click yes. What you are doing is adding the certificate of the sender to his contact information. In our example, the certificate issued to User.Joe.3010002571 will be put in the Contact information for Joe User with the email address user@lemon.dod.

After you click yes, the user's contact information will be displayed. Choose the Certificate tab and verify that the appropriate certificate is in the user's information.

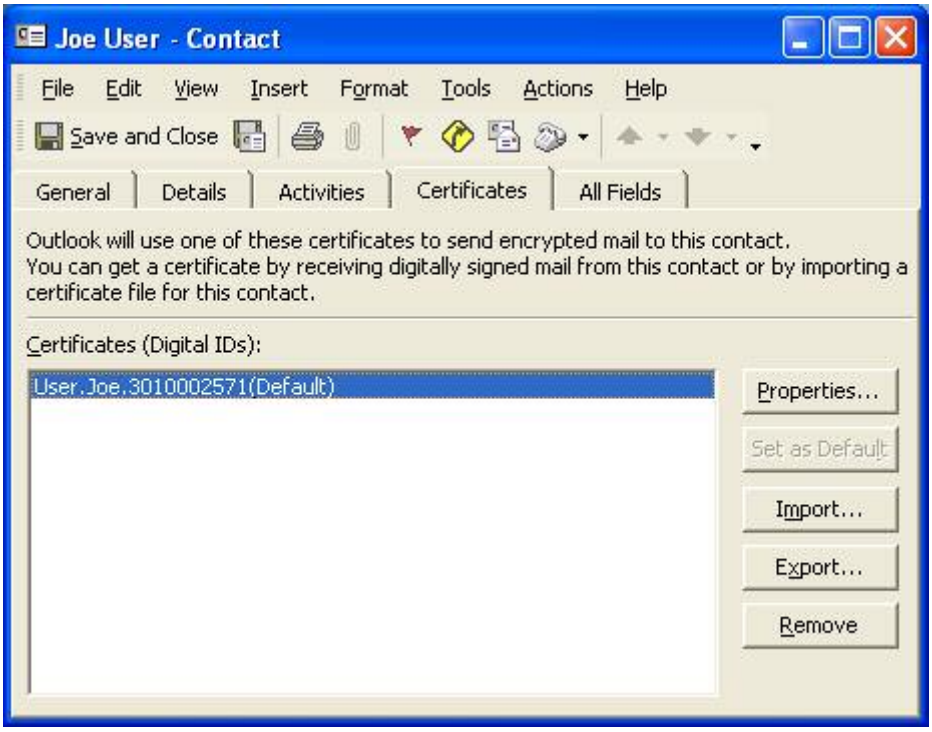

Figure 9 – Contact Information

You can further examine the certificate by selecting the Properties button. If the certificate isn't there, something is wrong with the user's certificate. This issue will need to be resolved before you can encrypt to this user.

Assuming the certificate is present in the user's contact information, you have everything you need to encrypt email to them. However, there is one further issue. When you send an encrypted email to somebody, the first place Outlook goes to look for a certificate may not be the Contacts. By default, Outlook first goes to the Global Catalog. If the recipient has an entry in the Global Catalog, but no certificate is present, Outlook will claim that it can't find a certificate for that user. To fix this, you need to make sure that Outlook is looking in the Contacts for the user's certificate. There are two ways to accomplish this. One way is to set the default place for Outlook to look for users' certificates to Contacts and the other is to overtly use the Contacts list to send email to the user every time you send an encrypted email. We will show how to do both.

Setting the Default to the Contacts List

To set Contacts as the default location for Outlook to find people, go to the Tools menu of the main Outlook window (not a Message pane) and select Address Book, which displays the Address Book window as shown below.

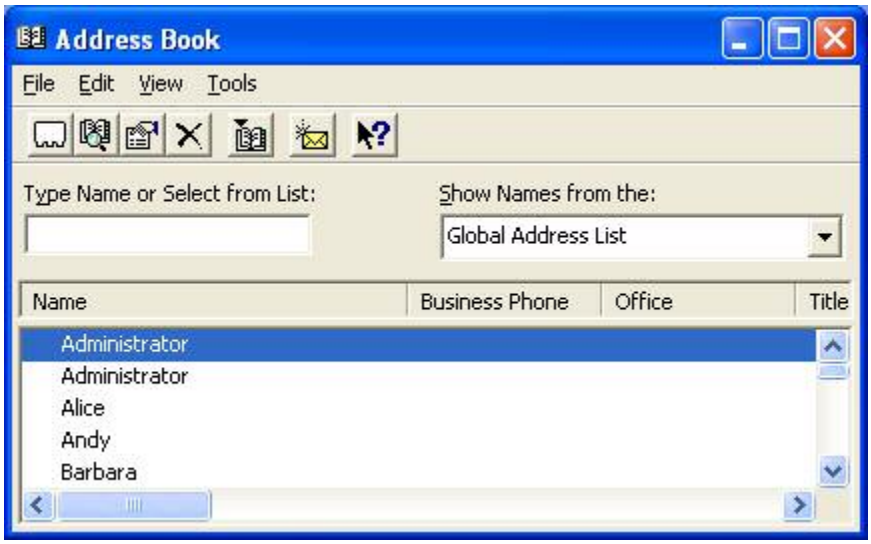

Figure 10 – Address Book Window

Under the Tools menu, choose Options to display the Addressing window.

Figure 11 – The Addressing Window

Change the order of the Address lists in the third listbox from the top so that Contacts is the first choice.

Figure 12 – The Addressing Window with Contacts First

Overtly Using Contacts to Send the Email

When you are selecting the recipients for a given email, click the To button next to the Recipients field.

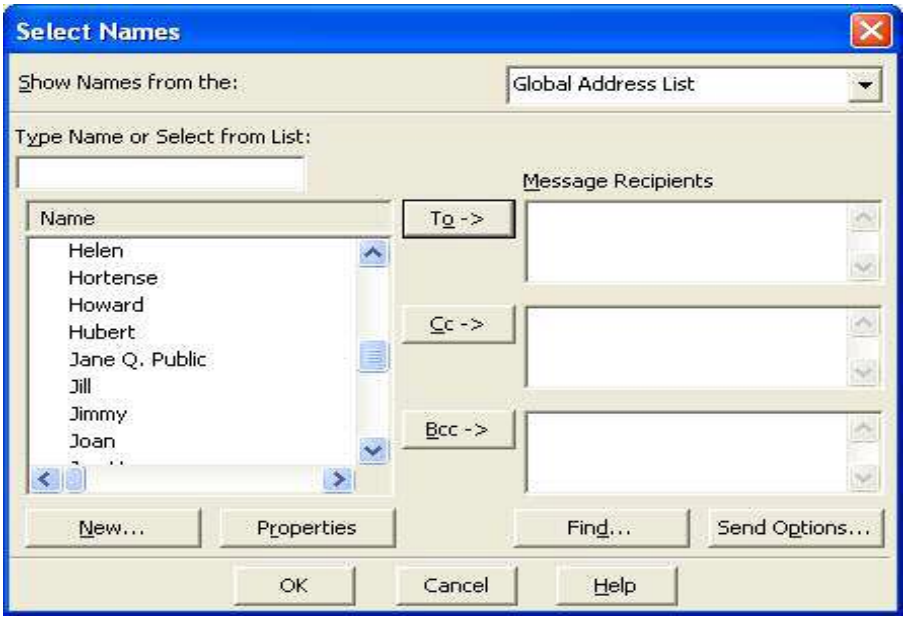

Figure 13 – Selecting Recipients for Email

Select the Contacts List in the Drop down ListBox in the upper right hand corner.

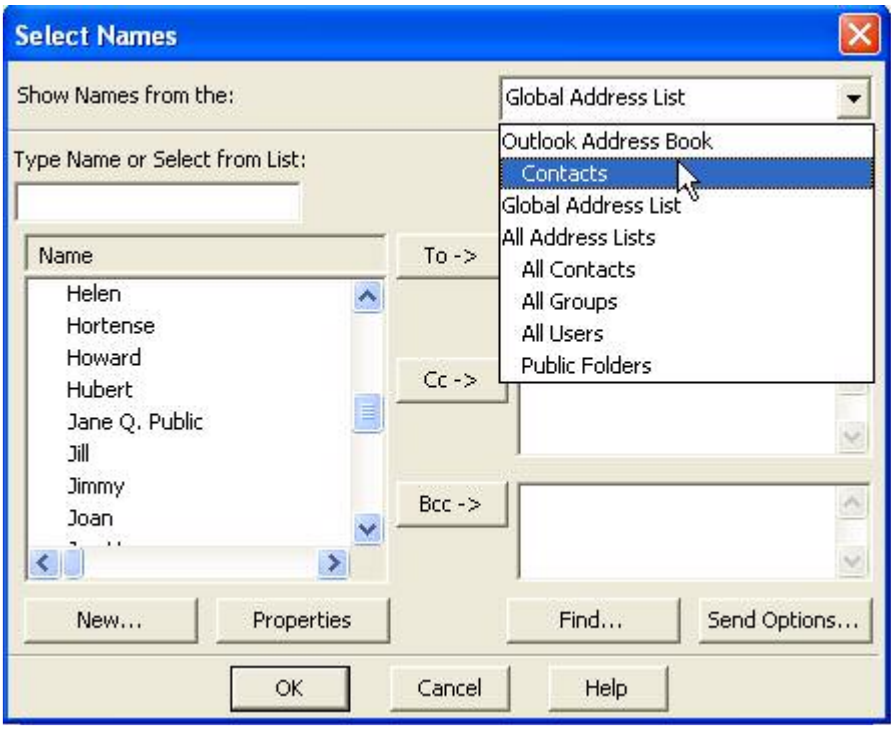

Figure 14 – Viewing Contacts

The intended recipient should appear in the list of Names. Move that name to the right side using the To-> button and select ok.

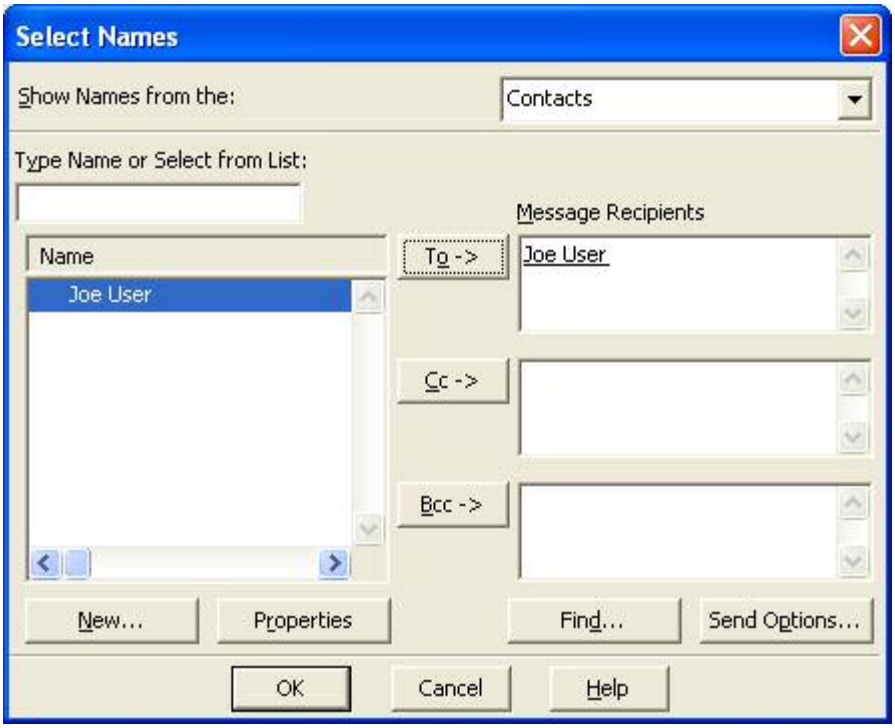

Figure 15 – Adding a Recipient from Contacts

Checking the Encryption in a Received Email

To check the encryption in a received email, click on the blue lock that is shown in the upper right hand corner of the message pane as shown below.

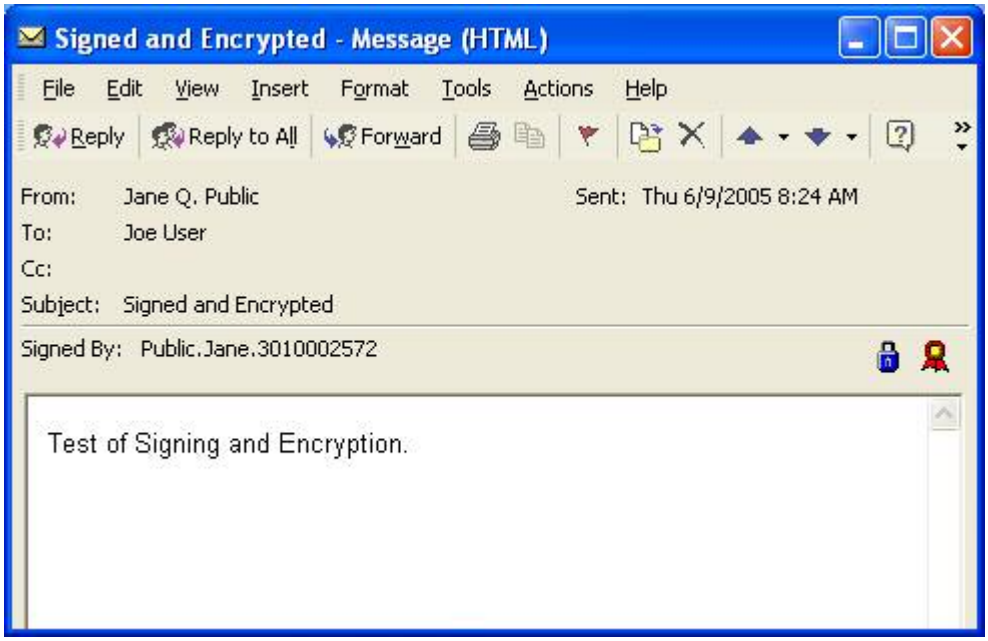

Figure 16 – An Encrypted Message

When you click on the blue lock, you will see the Message Security Properties Window.

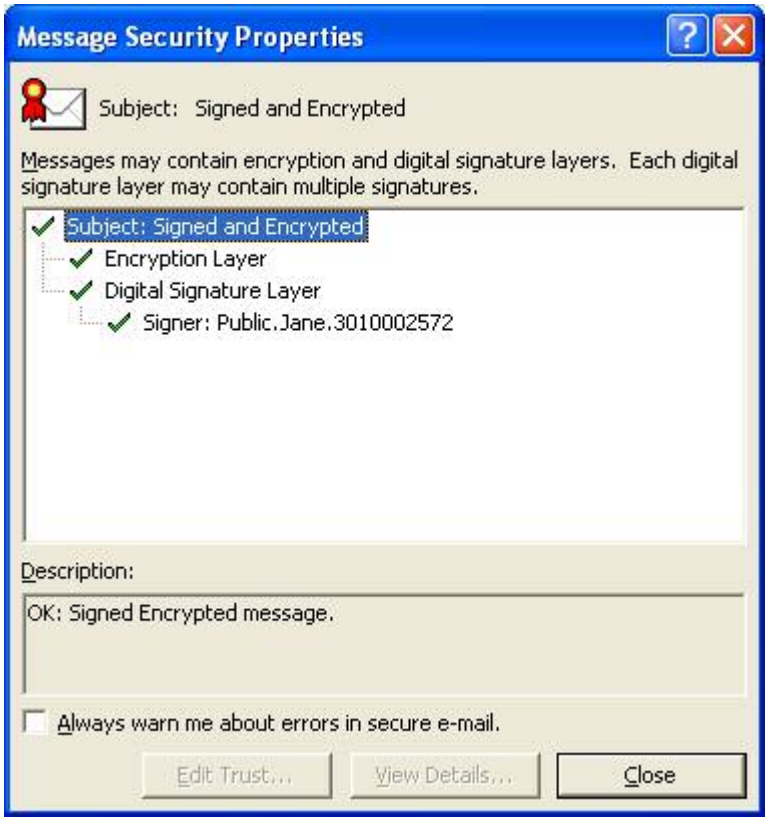

Figure 17 – Message Security Properties

If you highlight a topic, more information will be displayed in the Description box. Shown below is what you should see if you highlight the Encryption Layer.

Figure 18 – Encryption Properties

If you see an algorithm different than 168 bit 3DES, you should take steps to correct this. Make sure that both you and your intended recipient have chosen 3DES in the Security Settings Dialog Box (see page **6**).

Appendix
A

References

Microsoft's Web Site,
http://www.microsoft.com/

About Certificates and Cryptographic E-mail Messaging in Outlook,
http://office.microsoft.com/en-us/assistance/HP010461711033.aspx

About Microsoft Exchange Server 2000,
http://nsa2.www.conxion.com/win2k/guides/w2k-21.pdf

Windows Update for Windows 2000 Web Page,
http://www.microsoft.com/windows2000/downloads/default.asp