OFFICE OF THE CHIEF INFORMATION OFFICER
INNOVATIONS & OPERATIONAL ARCHITECTURE

Digital Signatures
Microsoft Outlook – 2003 & 2007
User Guide

21 March 2011

United States Department of Agriculture

Table 1. Document Revision & Version Information

Version No.	Date	Description	Author/Approval
1.0	3/21/2011	Version 1.0 Final	Todd Kaywood, Carol Van Natta

Digital Signatures Microsoft Outlook– 2003 and 2007.docm

Table of Contents

1. Introduction 4
1.1 What is a Digital Signature? 4
1.2 When Should I Use a Digital Signature? 4
1.3 Definitions and Acronyms 5

2. Adding a Digital Signature to an Outlook Email 6
2.1 How to Digitally Sign an Outlook 2003 Email 6
2.1.1 Digitally Sign an Individual Message 6
2.1.2 Digitally Sign All Messages by Default 14
2.2 How to Digitally Sign an Outlook 2007 Email 20
2.2.1 Digitally Sign an Individual Message 20
2.2.2 Digitally Sign All Messages by Default 27

3. How to Verify a Signature is Valid (Outlook 2003 & 2007) 30

4. Help Desk and Troubleshooting for Digital Signature 32

5. References 32

-- -- --

1. Introduction

This document provides instructions on how to add digital signatures to Microsoft Outlook 2003 or 2007 emails. You must have an activated LincPass + PIN, the ActivIdentity ActivClient software installed, and a card reader to digitally sign a document. You must also have Microsoft Outlook 2003 or 2007 installed.

> **NOTE:** These instructions are based on the FDCC-approved installation of Microsoft Office on computers with the Windows XP operating system. As other agencies may have implemented options, settings, and limitations during installation, you may see slight variations in behavior and screenshots than those shown in this document. Check with your agency's IT help desk if you have questions or problems.

User guides like this one are also available for:

- Microsoft Office 2003
- Microsoft Office 2007
- Adobe Acrobat versions 8 and 9

1.1 What is a Digital Signature?

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document. Besides being easily transportable, it can also add assurance that the content of the message or document that has been sent is unchanged. When time-stamped, the ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Digital signatures provide a high form of signature and content integrity. Digital signatures are based on public key infrastructure (PKI), and are a result of a cryptographic operation that guarantees signer authenticity, data integrity, and non-repudiation of signed documents. The digital signature cannot be copied, tampered, or altered, and therefore non-repudiable. In addition, because they are based on standard PKI technology, digital signatures made within one application (such as Microsoft Word or Adobe Acrobat) can be validated by others using the same application.

1.2 When Should I Use a Digital Signature?

USDA is developing policy or directives that will officially address the technology of digital signature and its application in USDA. Check with your agency for interim guidance on when to use digital signatures for business purposes. Here are some general guidelines on when you might want to use them:

- Placing a "seal" on the document. Digitally signing using the USDA LincPass card is assurance of document integrity and its legal standing as an official document.
- Multiple signatures. Documents can be digitally signed by more than one person, indicating an approval or agreement with the (unaltered) content.
- Compliance. A digital signature may be required for compliance purposes when a legal signature is required. For example, the System Security Plan for a major system must be signed by the system owner and by the responsible security officer.

- Leadership Memorandums and Policy Issuance. Digital signatures on such documents are assurance that the document was reviewed and approved by the signer, and the recipient can be assured the content is as the signer intended.
- Verification of the signer's digital identity. Digital signatures can be traced to a known electronic identity, which in turn represents a specific individual in USDA. For example, although email headers can be spoofed or forged, the digital signature associated with it cannot.

This is by no means an exhaustive list, and Agencies may well find other uses for digital signatures that meet a specific business need.

1.3 Definitions and Acronyms

- **PIV card**: FIPS 201-compliant personal identity verification (PIV) card
- **LincPass:** USDA's name for the PIV cards it issues to employees, contractors, partners, affiliates, et al.
- **HSPD-12**: Homeland Security Presidential Directive 12, signed 27 August 2004. HSPD-12 requires all federal agencies to conduct background investigations and issue personal identity verification (PIV) credentials to all employees and contractors, and integrate those credentials with logical and physical access control systems.
- **Microsoft Office file types**:
  - DOC file: Microsoft Word 2003 file
  - DOCX file: Microsoft Word 2007 file *(not backward compatible with Word 2003)*
  - DOCM file: Microsoft Word 2007 file *(not backward compatible with Word 2003)*
  - XLS file: Microsoft Excel 2003 file
  - XLSX file: Microsoft Excel 2007 file *(not backward compatible with Excel 2003)*
  - PPT file: Microsoft PowerPoint 2003 file
  - PPTX file: Microsoft PowerPoint 2007 file *(not backward compatible with PowerPoint 2003)*
  - PDF file: Adobe Acrobat version 8 & 9
  - Microsoft Outlook 2003
  - Microsoft Outlook 2007
- **User:** Employee, contractor, affiliate, partner, et al. with an activated LincPass card.
- **Public key infrastructure (PKI):** Standards-based system that creates a hierarchy of "certification authorities" to allow individuals and organizations to identify each other for the purpose (principally) of doing business electronically.
- **Non-repudiation:** A method to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. In reference to digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.

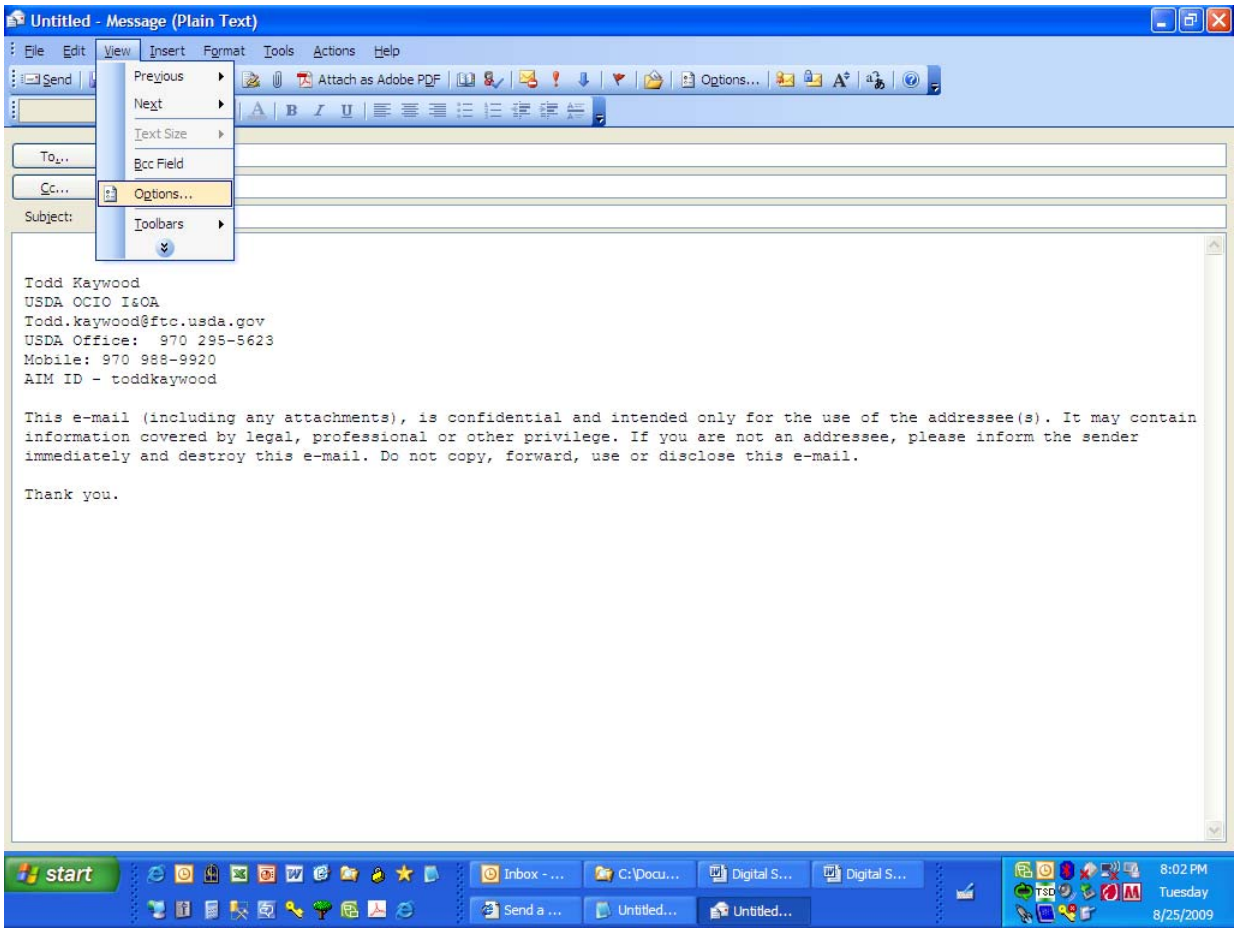
2. Adding a Digital Signature to an Outlook Email

In Microsoft Outlook 2003 and 2007, you can choose to either digitally sign individual messages, or digitally sign all messages you send. The following sections cover how to do both in Outlook 2003 and Outlook 2007.

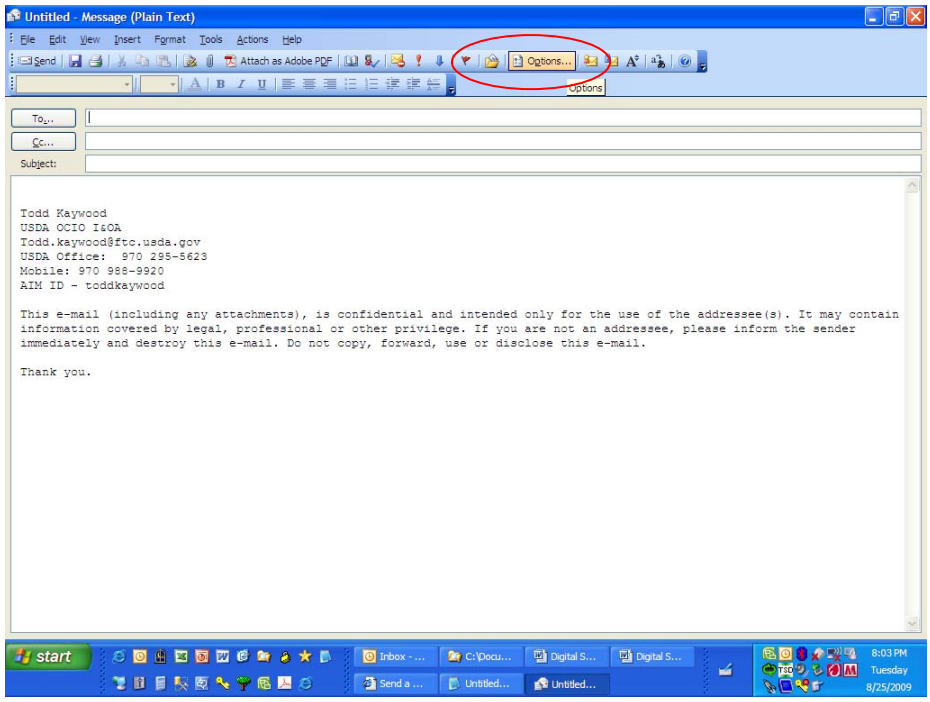
2.1 How to Digitally Sign an Outlook 2003 Email

2.1.1 Digitally Sign an Individual Message

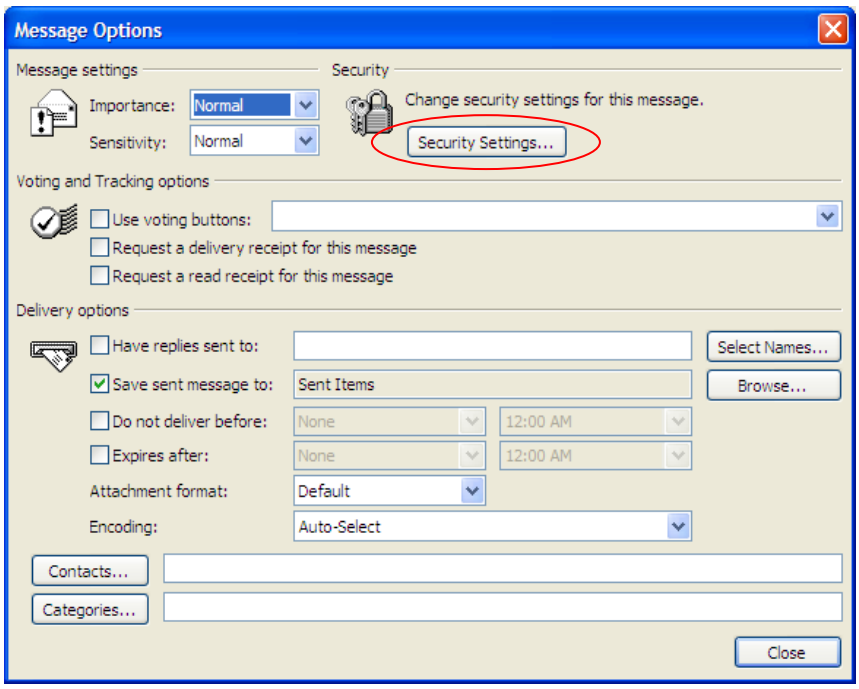
1. Open Outlook and, if it isn't already there, insert your LincPass in the card reader.
2. Start a new message in Outlook. Address it to yourself so you can see what it looks like when you receive a digitally signed email (described later in step 9).
3. From the menu, select **View**, then **Options**.



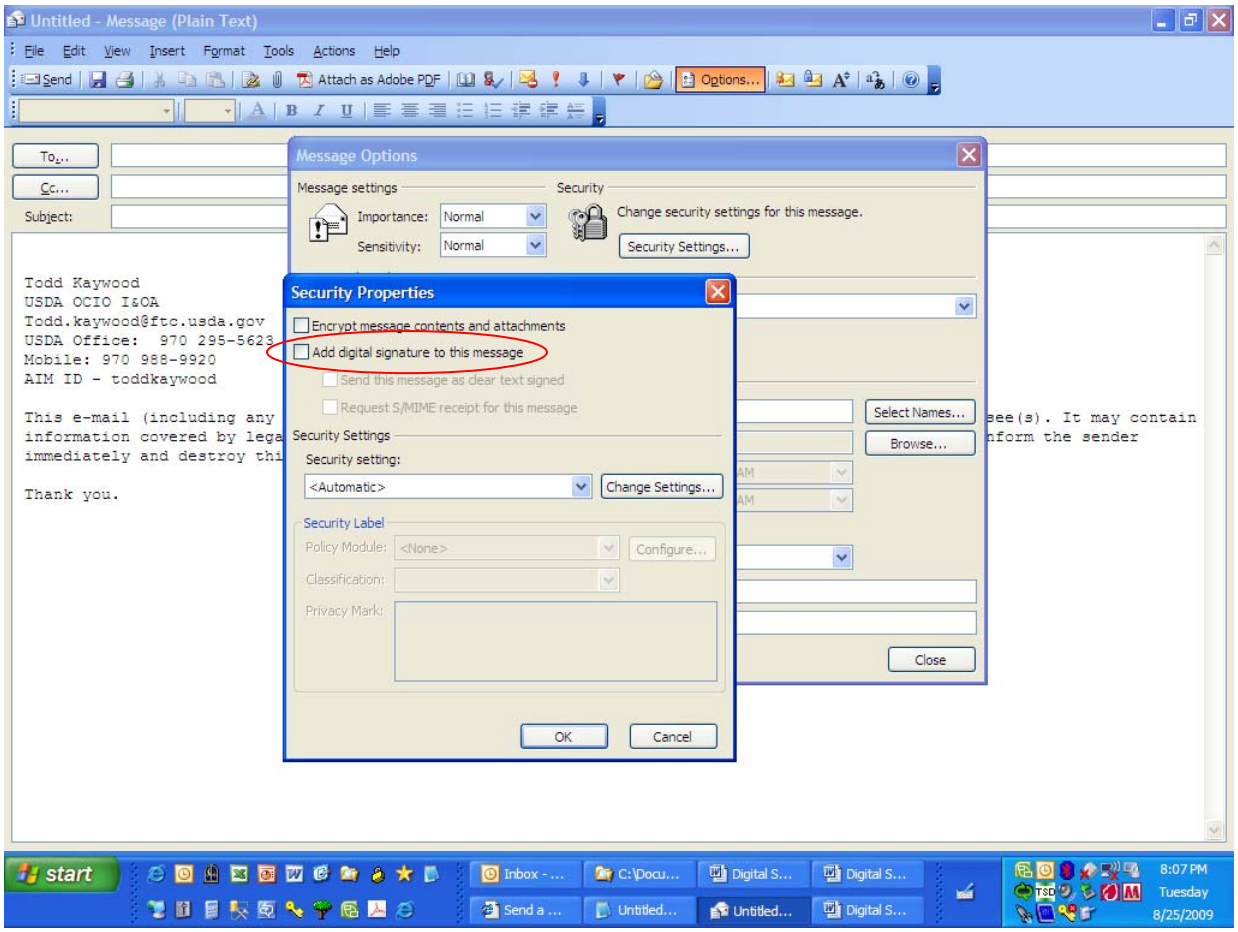
Alternatively, if it's available on your toolbar, click the Options button.



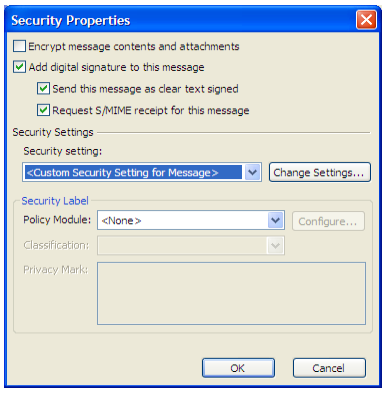
4. In the *Message Options* window, click the **Security Settings** button.



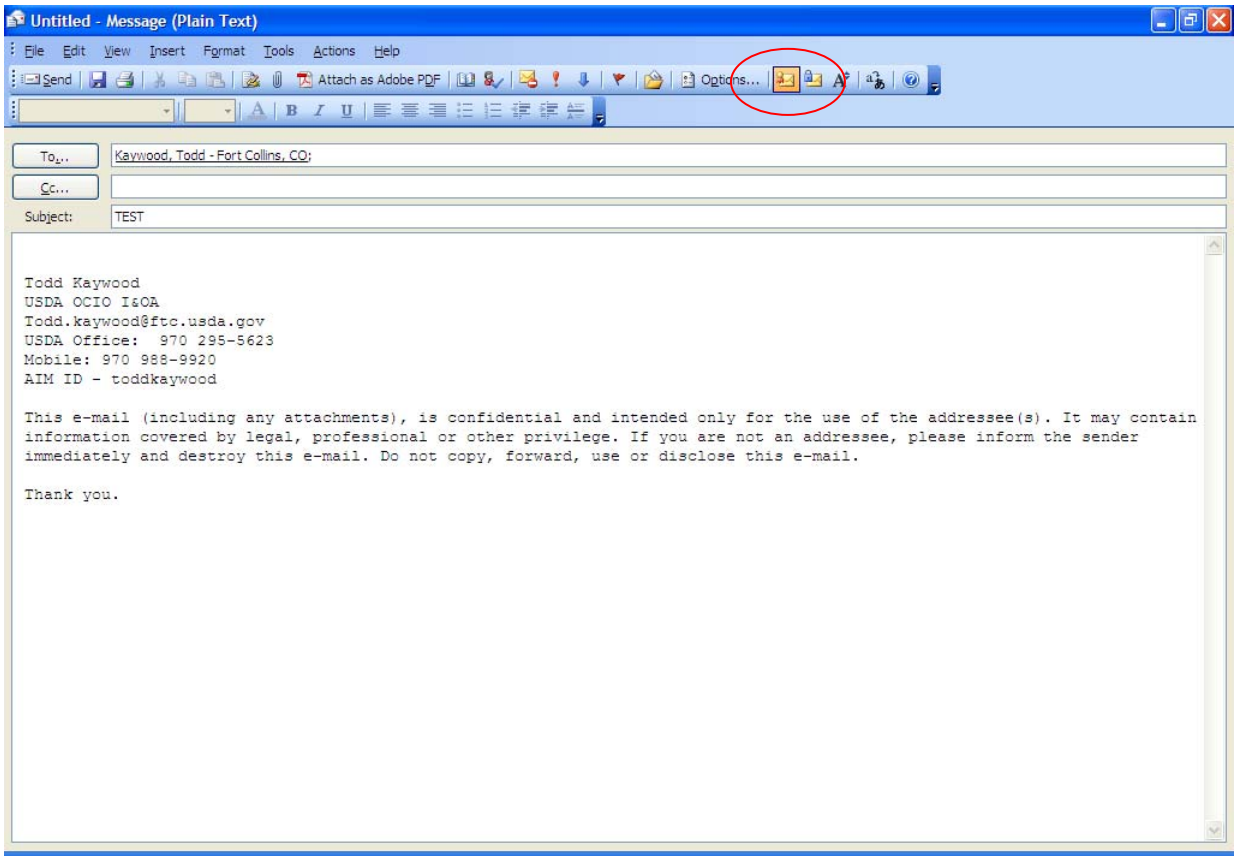
5. In the *Security Properties* window, select the "Add digital signature to this message" option.



6. Click none, one, or both of the two new options that become available:
   - Select **"Send this message as clear text signed"** if you want to allow others who may be using a lesser technology with Outlook to read your message. Recipients who don't have S/MIME security will be able to read the message.
   - Select **"Request S/MIME receipt for all S/MIME signed messages"** if you want to be able 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.

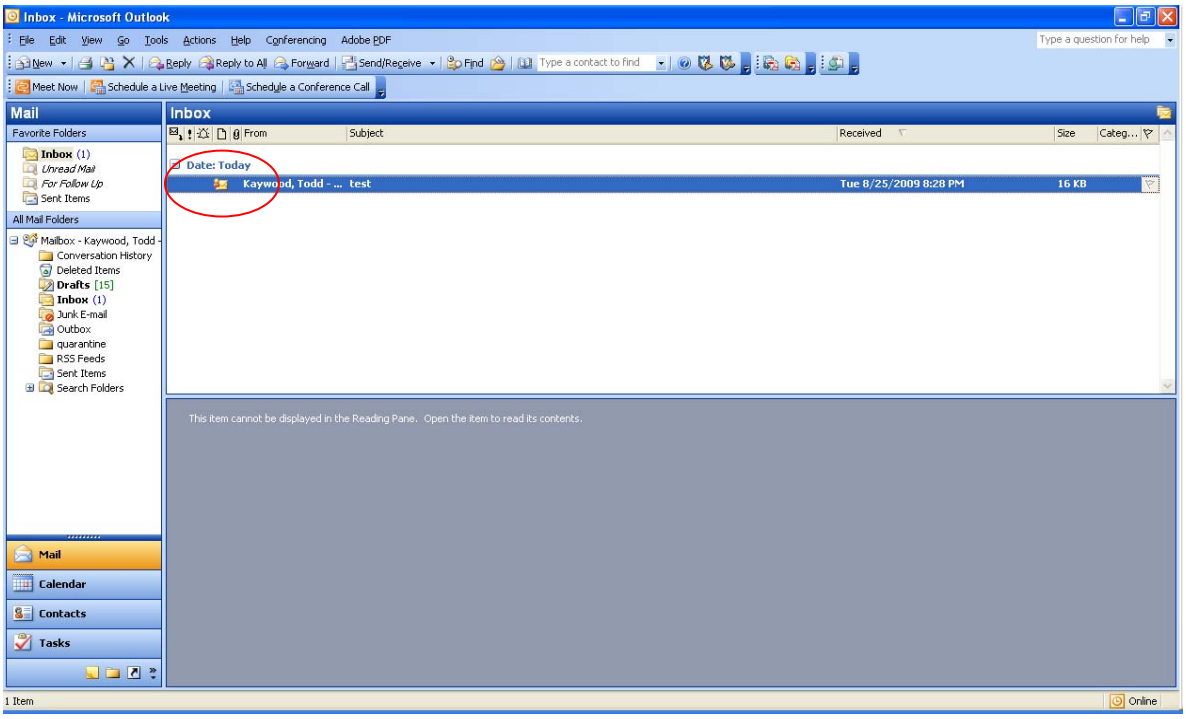


7. Click the **OK** button, then the **Close** button to close all the windows. Your email is now ready for signature. In the toolbar, the envelope icon with a small red ribbon on it indicates the signed message.



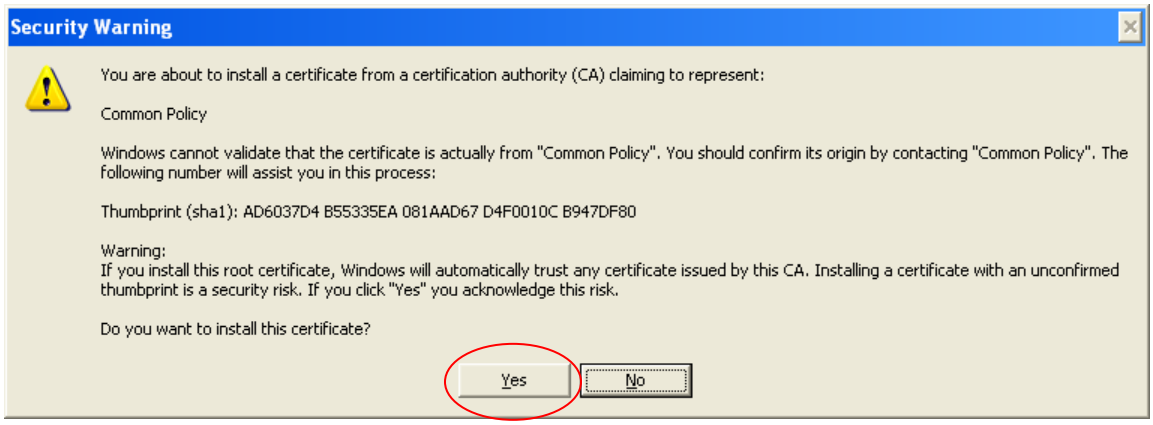
8. Type the content of your message and add other recipients, if any. When you click the **Send** button, you'll be challenged to enter your PIN.

9. Messages that have been digitally signed show up in your Outlook Inbox with the icon that indicates the signature (the envelope with a red ribbon). If you followed the instructions in step 2 and addressed the email to yourself, you'll see what this looks like in your Inbox. Note that the contents won't be displayed in the preview window.

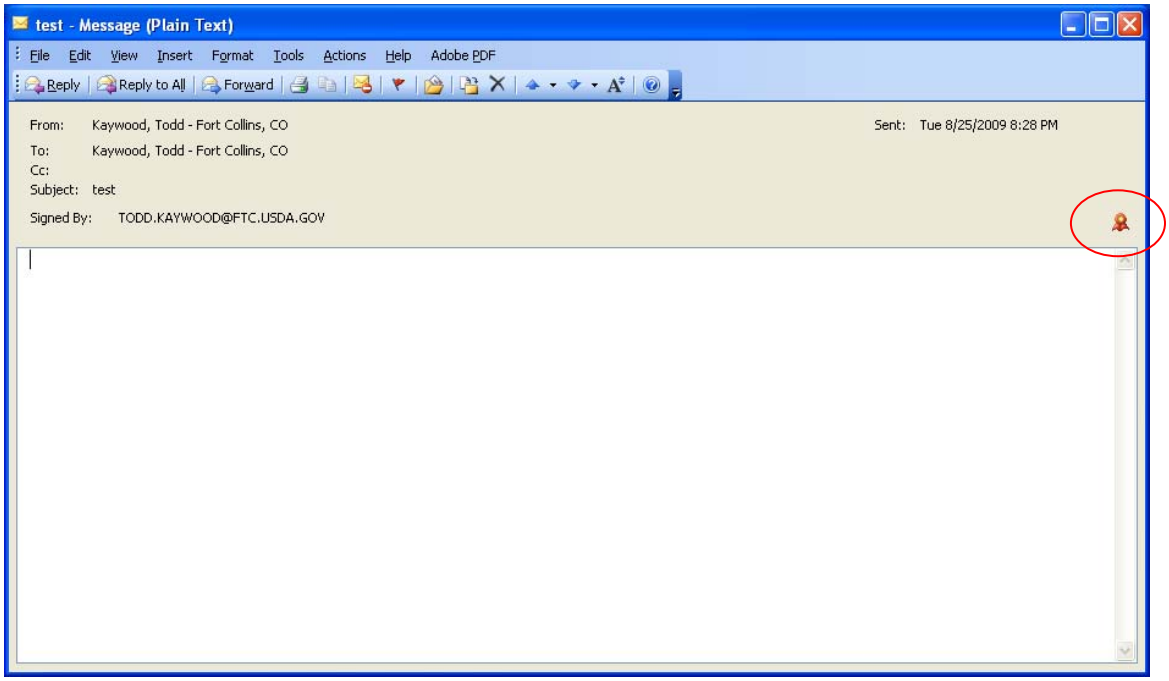


10. When you open the message, you may be prompted to enter your PIN again.

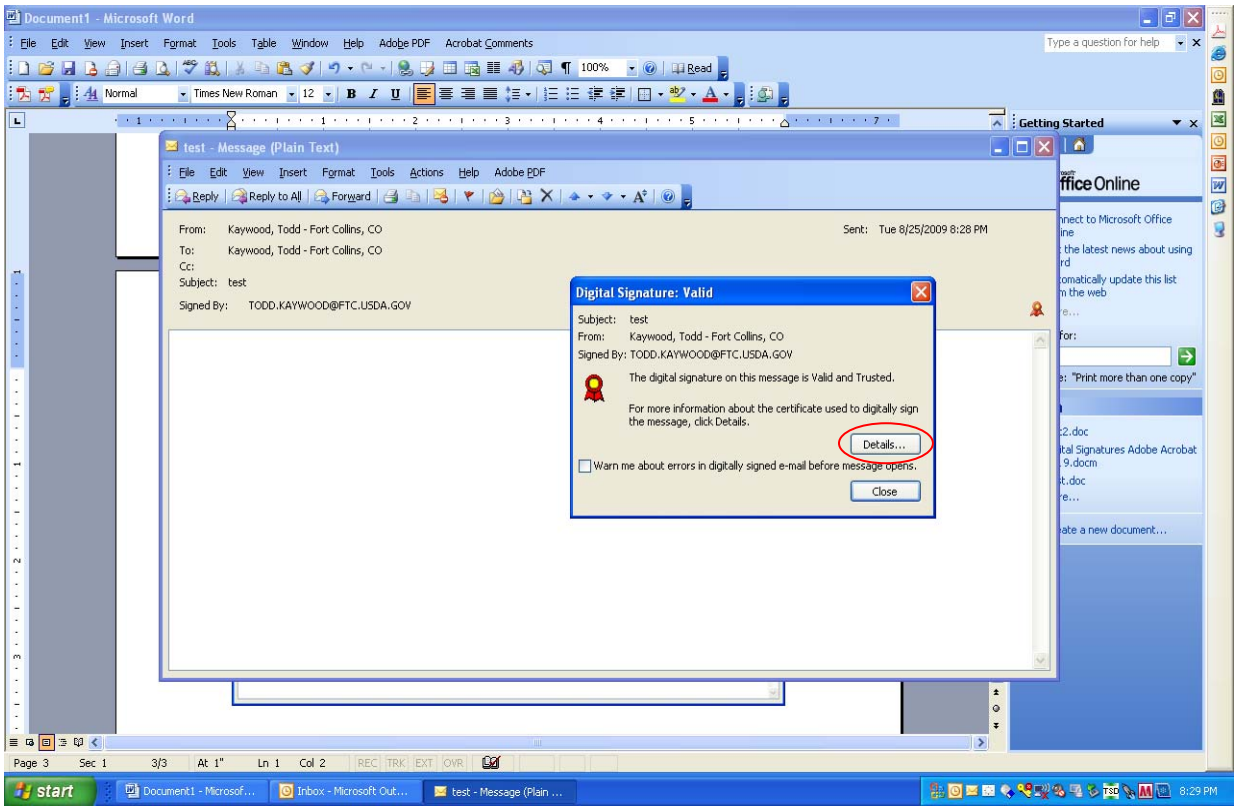
11. If this is the first time through the process, you will probably see a security warning telling you that you're about to install a certificate. Click the **Yes** button. You won't see this message again for future signed messages sent to you by anyone who used their LincPass certificate to sign the message.



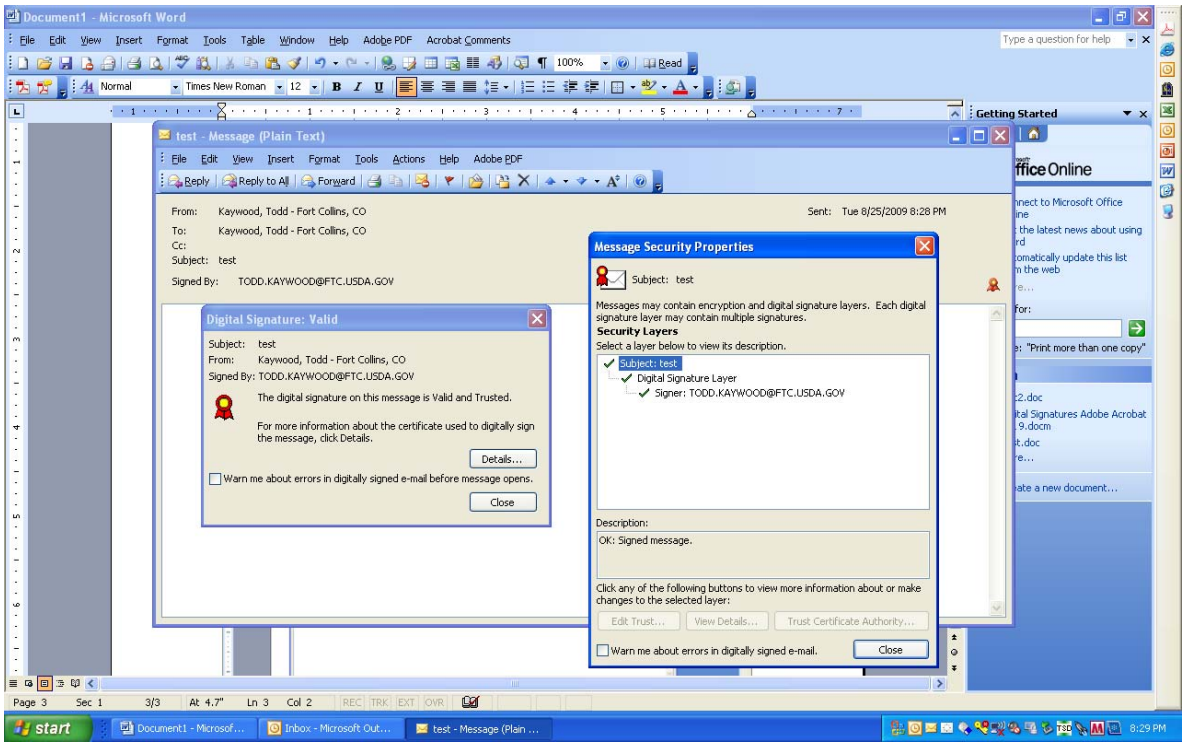
12. When the message opens, the red ribbon in the lower right of the header indicates the message is digitally signed.



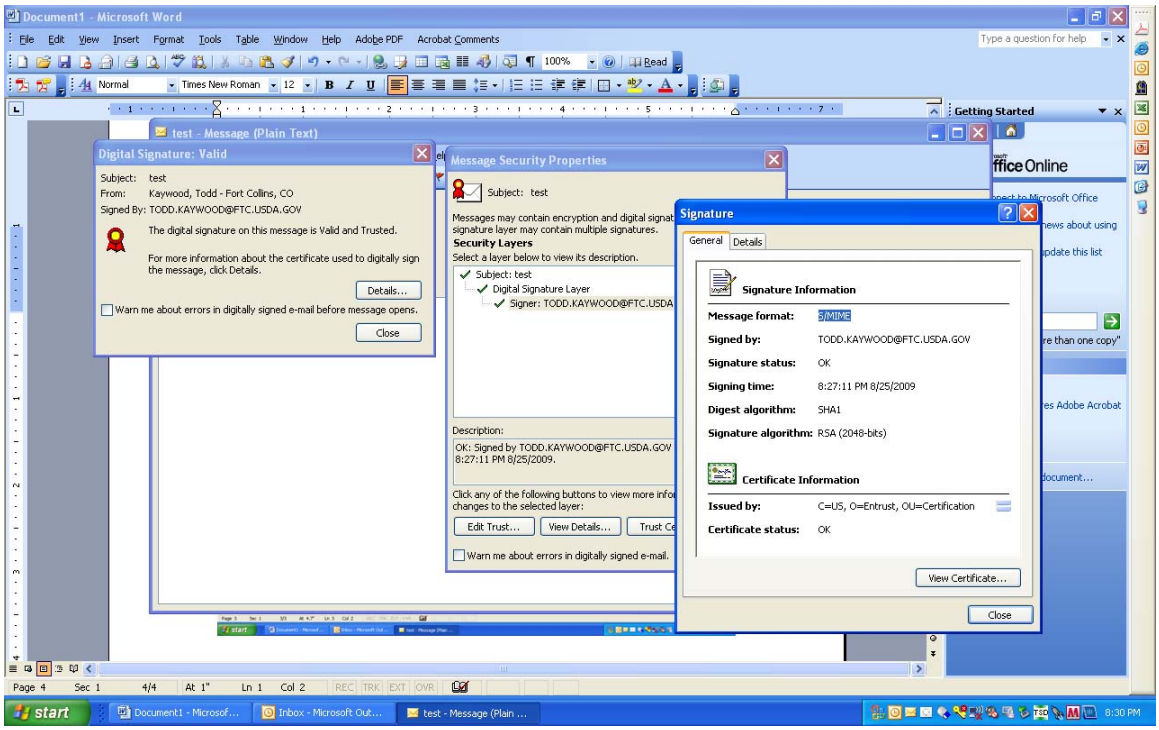
13. To verify the signature and certificate, double-click the red-ribbon icon. If you want to see more information about the signature, click the **Details** button…



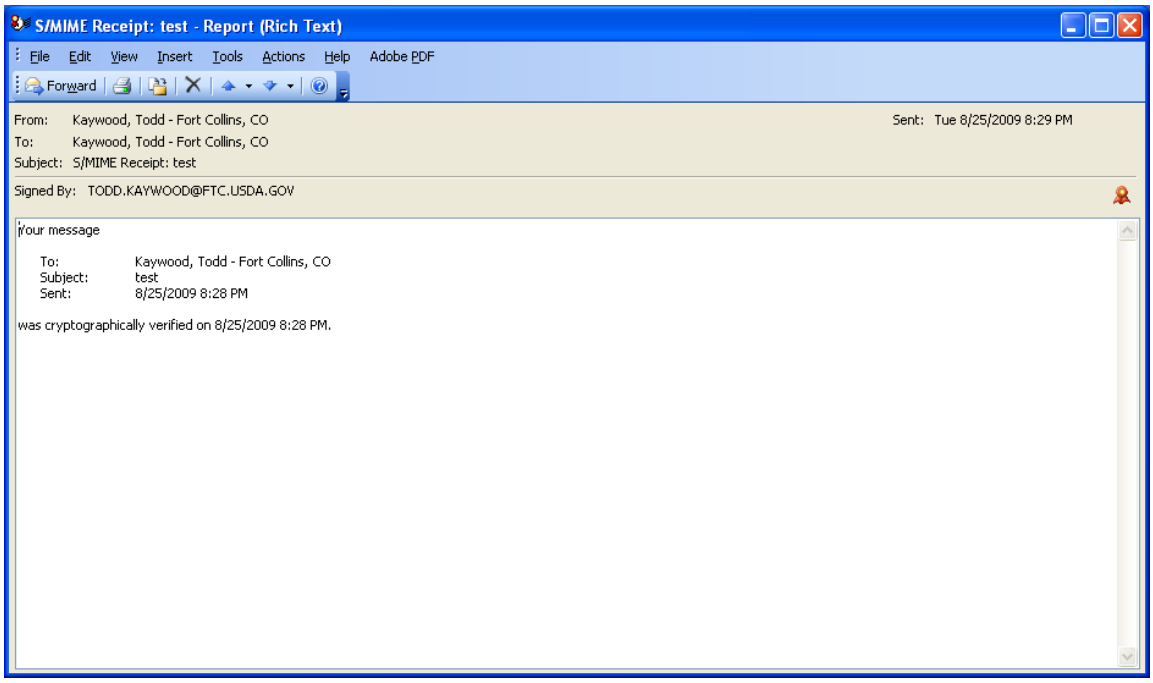
…then highlight the "Signer" line and click the **View Details** button.



The *Signature* window shows the details about the signer's certificate.

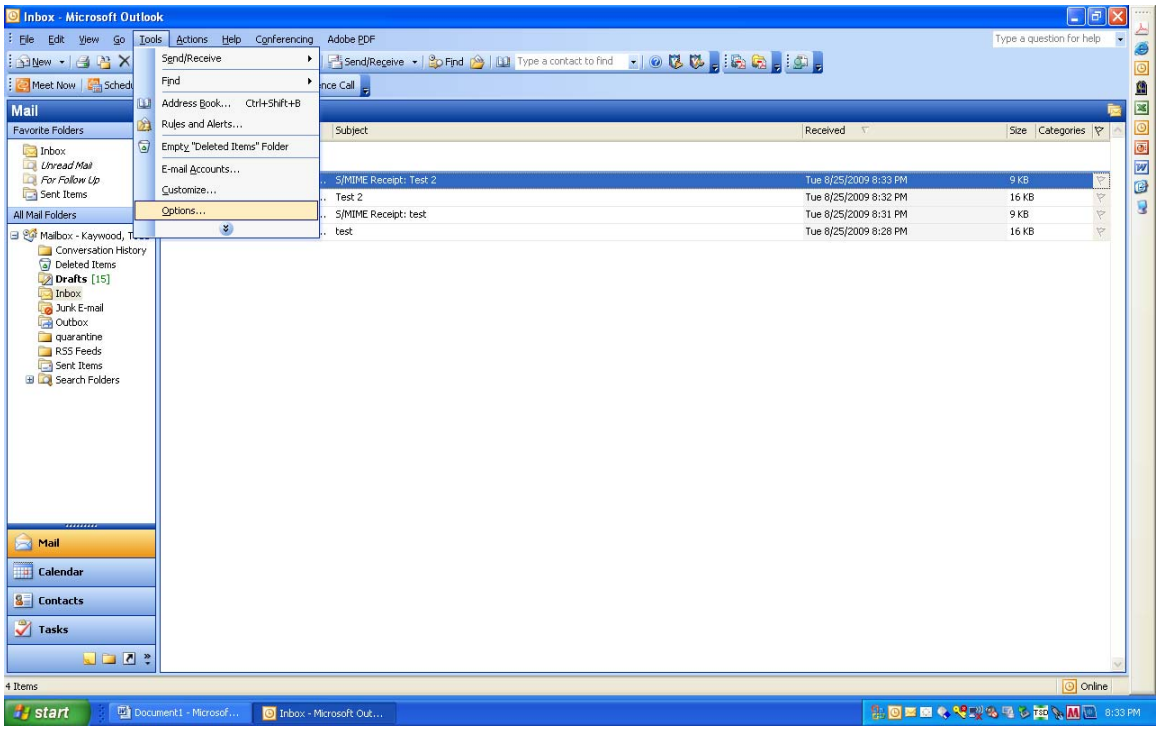


14. If you selected the "Request S/MIME receipt" option in step 6, you'll receive a new message that will require you to enter your LincPass PIN again before you can open it.

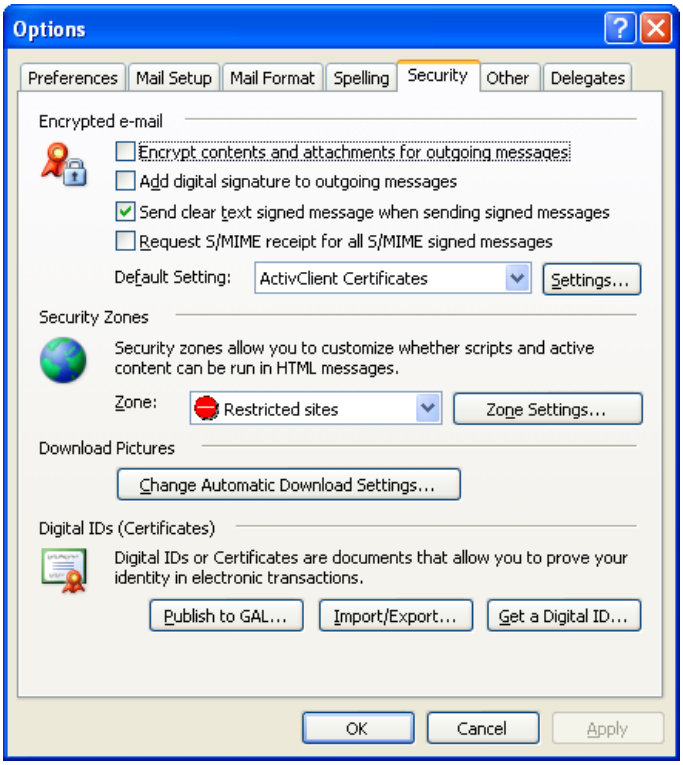


2.1.2 Digitally Sign All Messages by Default

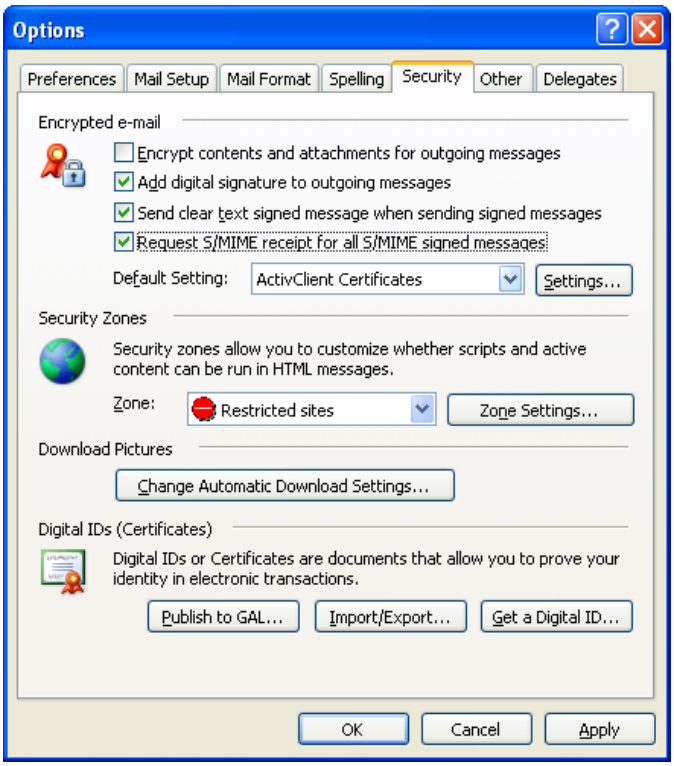
1. Open Outlook and, if it isn't already there, insert your LincPass in the card reader.
2. From the top menu, select **Tools**, then **Options**.



3. In the ***Options*** window, select the "Security" tab.



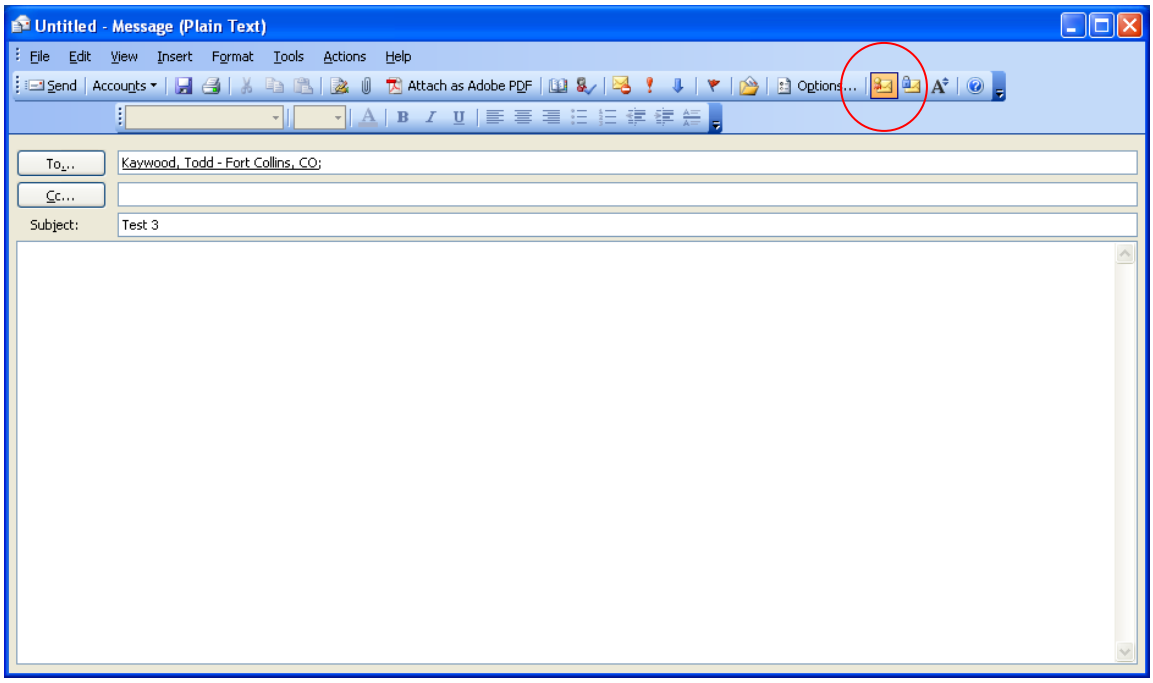
4. In the "Encrypted email" section, select the "Add digital signature to outgoing messages" option. See below for a description of the other two options.



- Select **"Send this message as clear text signed"** if you want to allow others who may be using a lesser technology with Outlook to read your messages. Recipients who don't have S/MIME security will be able to read the messages.
- Select **"Request S/MIME receipt for all S/MIME signed messages"** if you want to be able to verify that your digital signature is being validated by recipients and to request confirmation that each message was received unaltered, as well as notification telling you who opened the message and when it was opened.

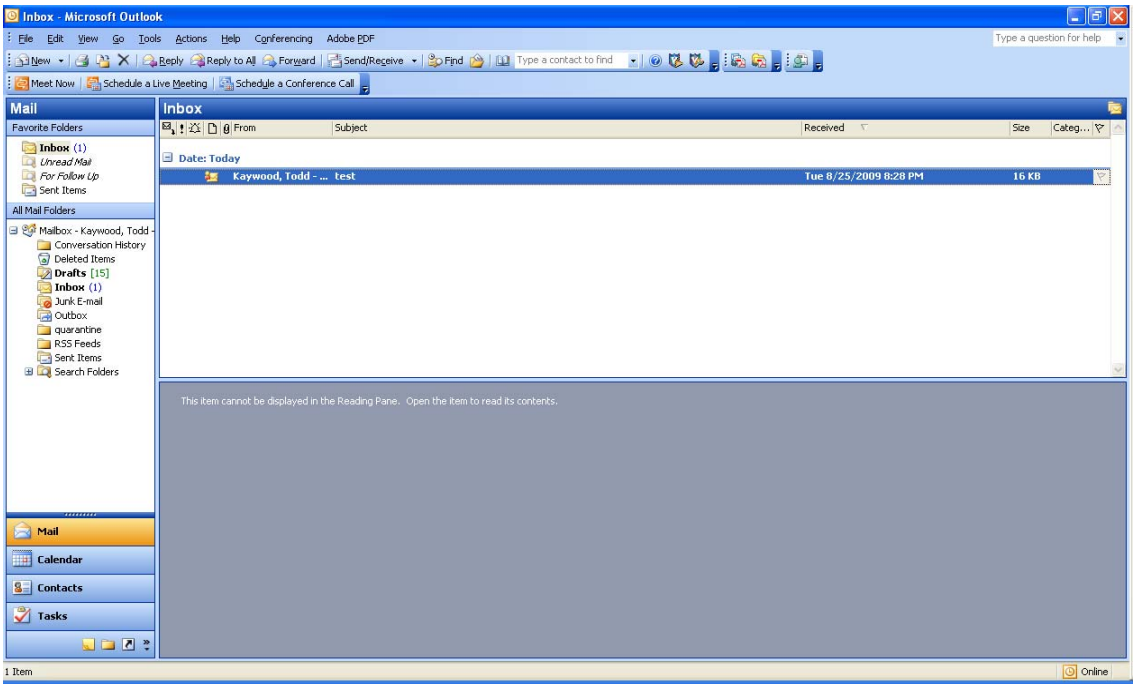
NOTE: It is recommended that you don't select the "Request S/MIME receipt" option unless you have a strong business need, as it doubles the number of emails in your Inbox and adds network traffic.

5. Click the **OK** button to close the Options window. When you start a new message, your toolbar will show the envelope with a small red ribbon already selected, indicating the message will be digitally signed. (You can choose not to sign an individual email by clicking the envelope icon.)



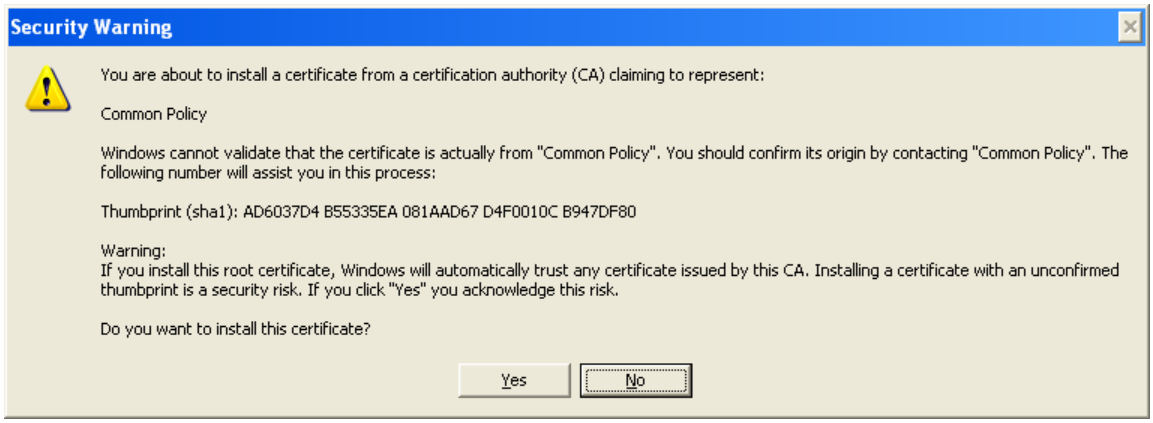
6. After adding recipients and content, click the **Send** button. You will be prompted for your LincPass PIN.

7. The message will appear in the recipient's Inbox with an envelope with a red ribbon on it indicating the message is digitally signed.

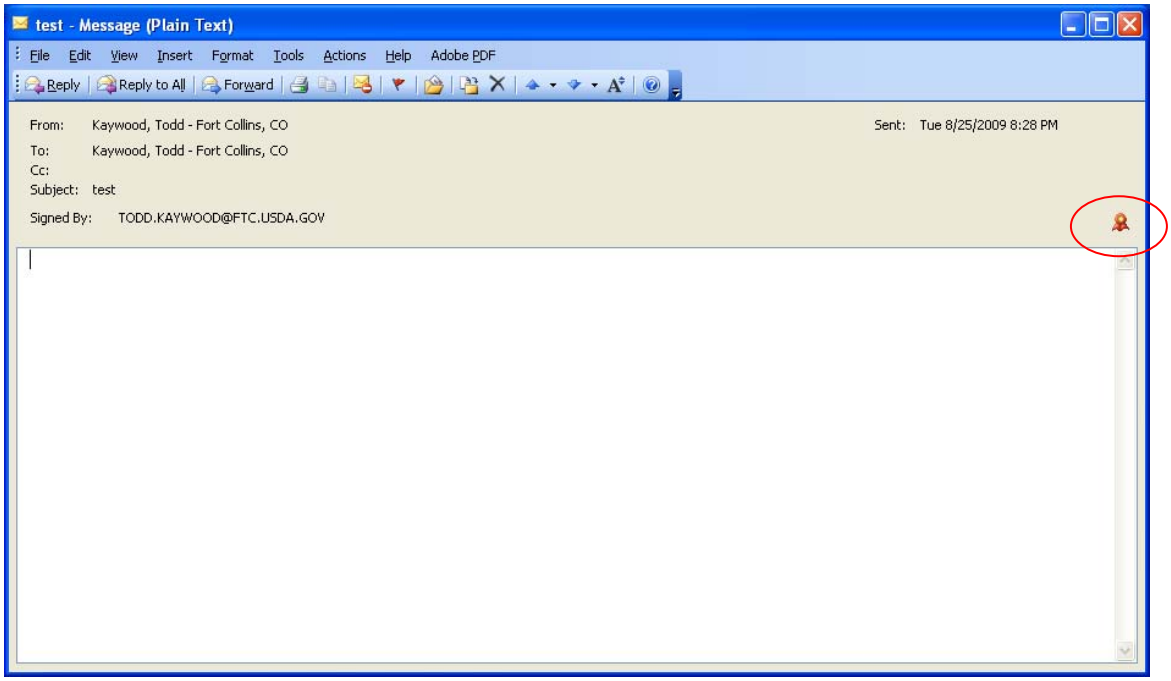


8. If you open a digitally signed email, you may be prompted for your PIN before the message will open.

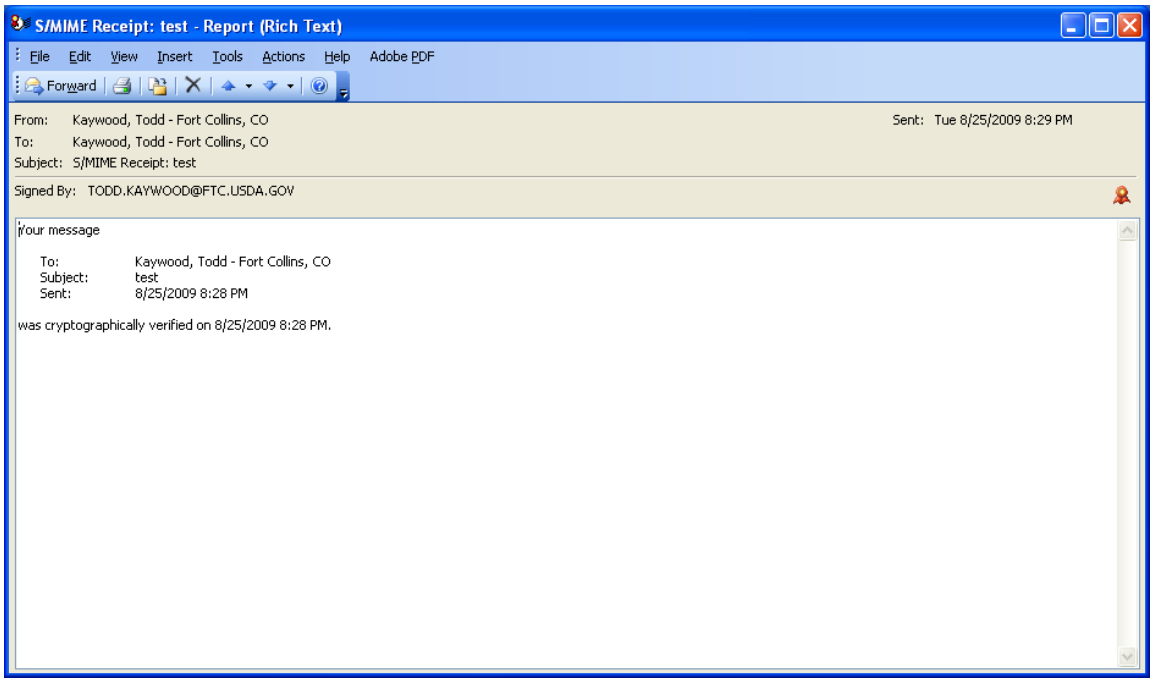
9. If this is the first time through the process, you will probably get a security warning telling you that you're about to install a certificate. Click the **Yes** button. You won't see this message again for future signed messages sent to you by anyone who used their LincPass certificate to sign the message.



10. When the message opens, the red ribbon in the lower right of the header indicates the message is digitally signed.



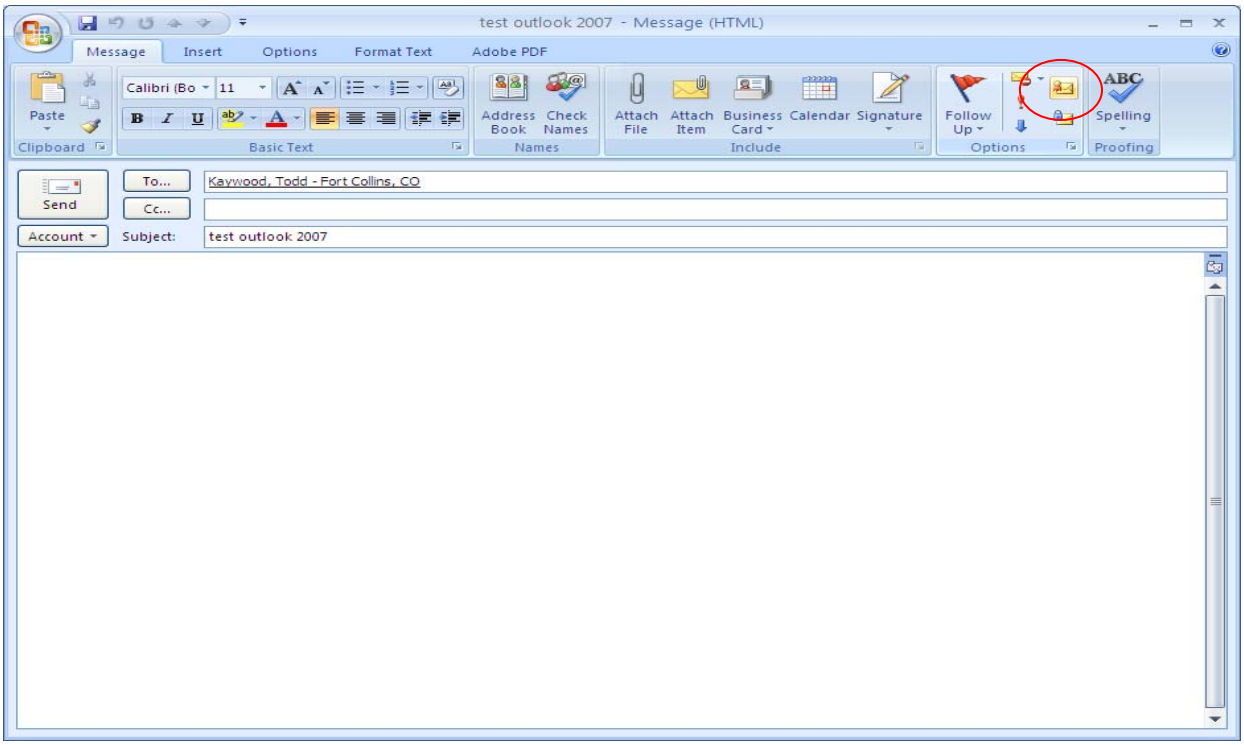
11. If you chose to request S/MIME receipts for all digitally signed emails you send, you will receive a separate email stating that the message was cryptographically verified on the given date and time.



2.2 How to Digitally Sign an Outlook 2007 Email

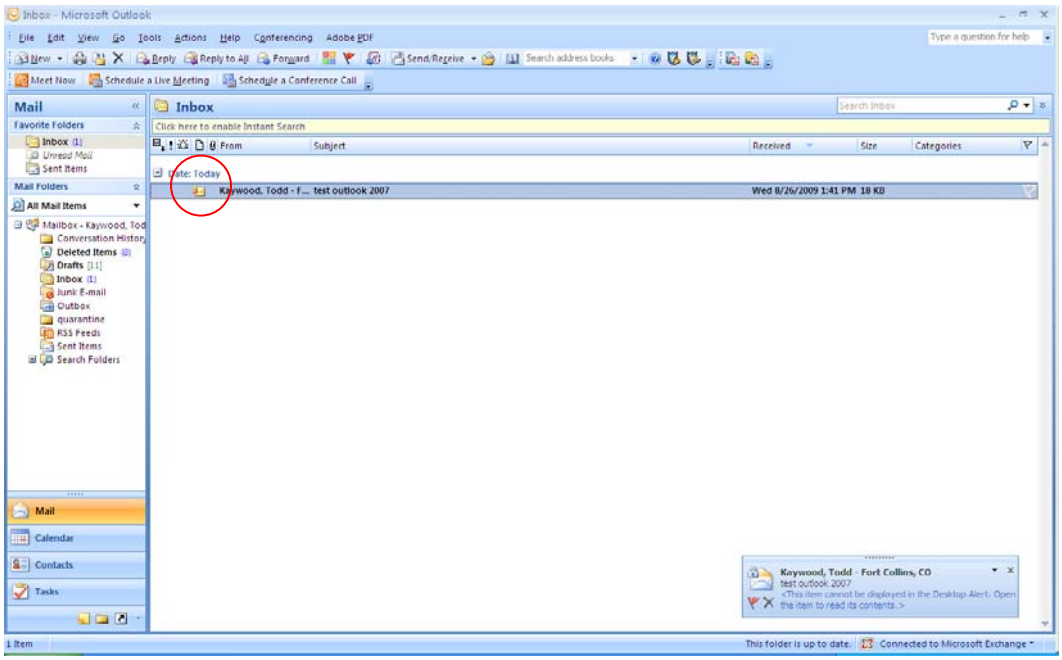
2.2.1 Digitally Sign an Individual Message

1. Open Outlook and, if it isn't already there, insert your LincPass in the card reader.
2. Start a new message in Outlook. Address it to yourself so you can see what it looks like when you receive a digitally signed email (described later in step 5).
3. In the message, with the Message tab selected, look for the digital signature icon (envelope with a red ribbon). Click the digital signature icon to turn it on. Select recipients and compose the message as usual, then click the **Send** button.

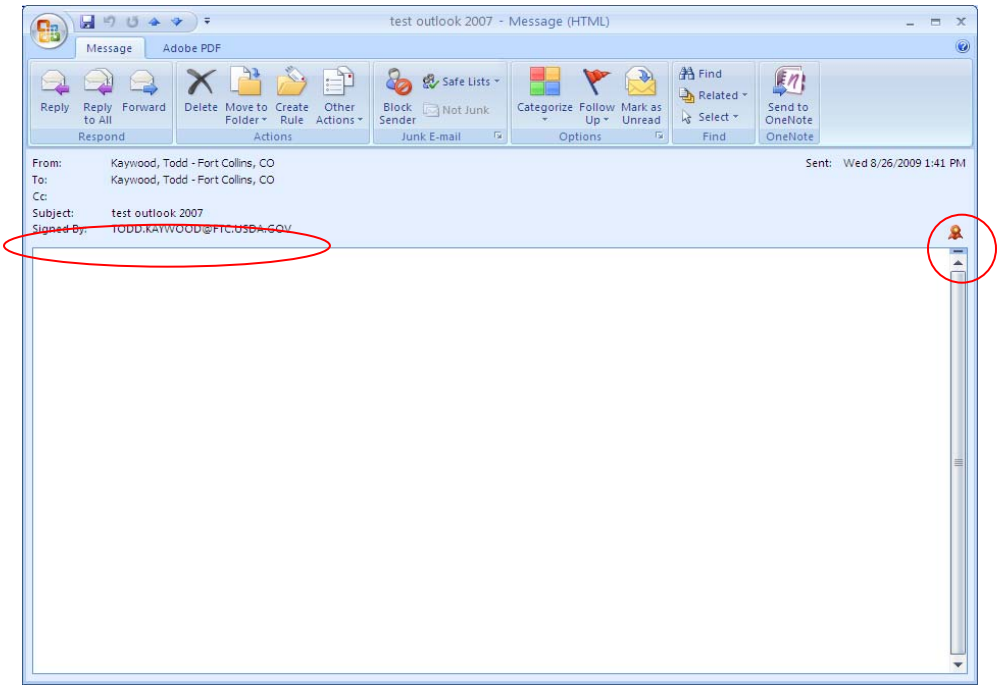


4. At the ActivClient prompt, enter your LincPass PIN, then press ENTER or click the **OK** button. Outlook will automatically verify your certificates on your LincPass and send the message.

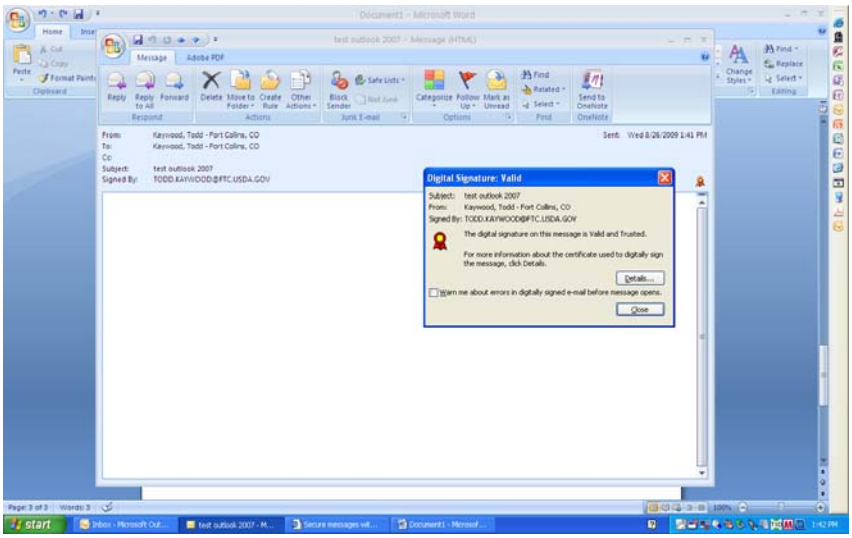
5. The message will appear in the recipient's Inbox with an envelope with a red ribbon on it, indicating the message is digitally signed.



6. Open the message and look for the "Signed By" information below the subject, and the red ribbon icon on the right. This indicates the message has been digitally signed.

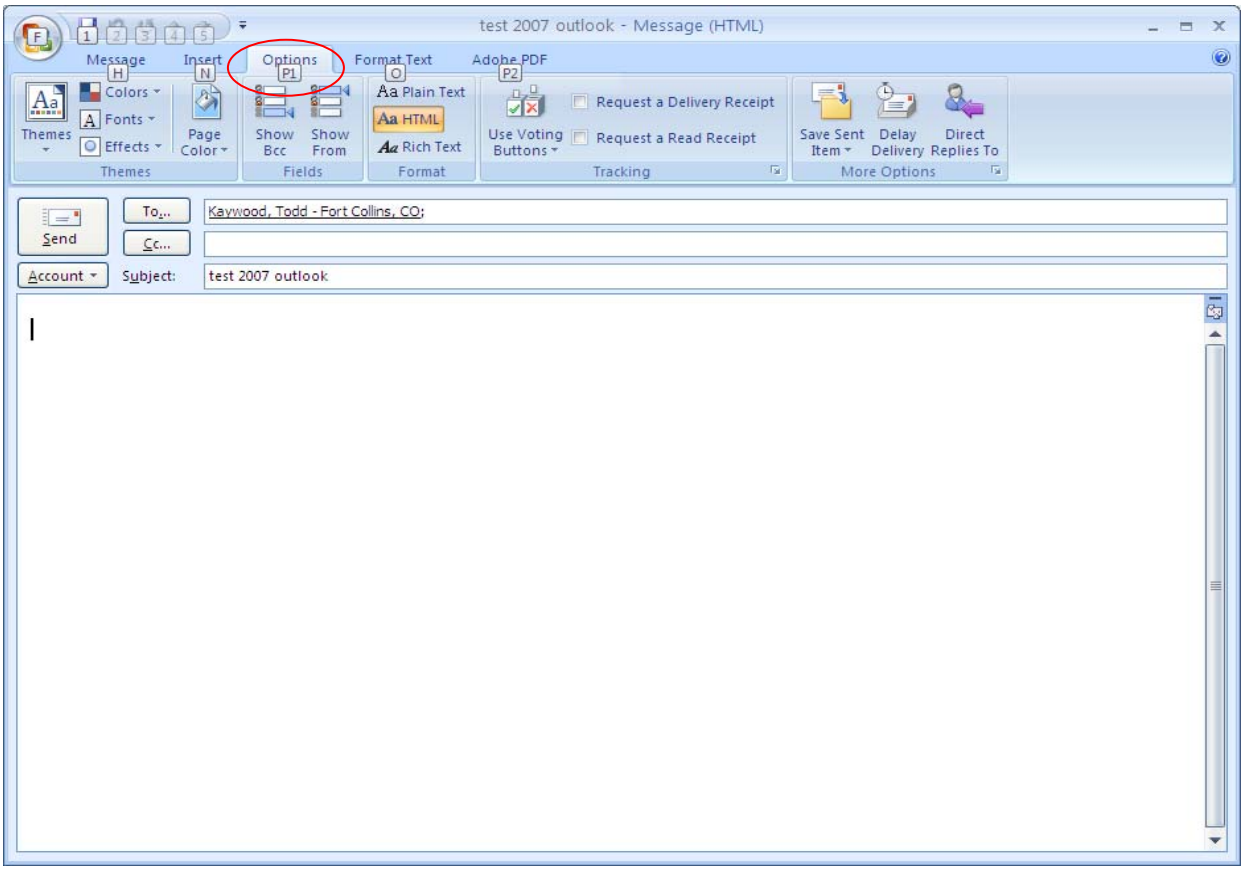


7. Click the red ribbon icon, then the **Details** button to see details of the digital signature.

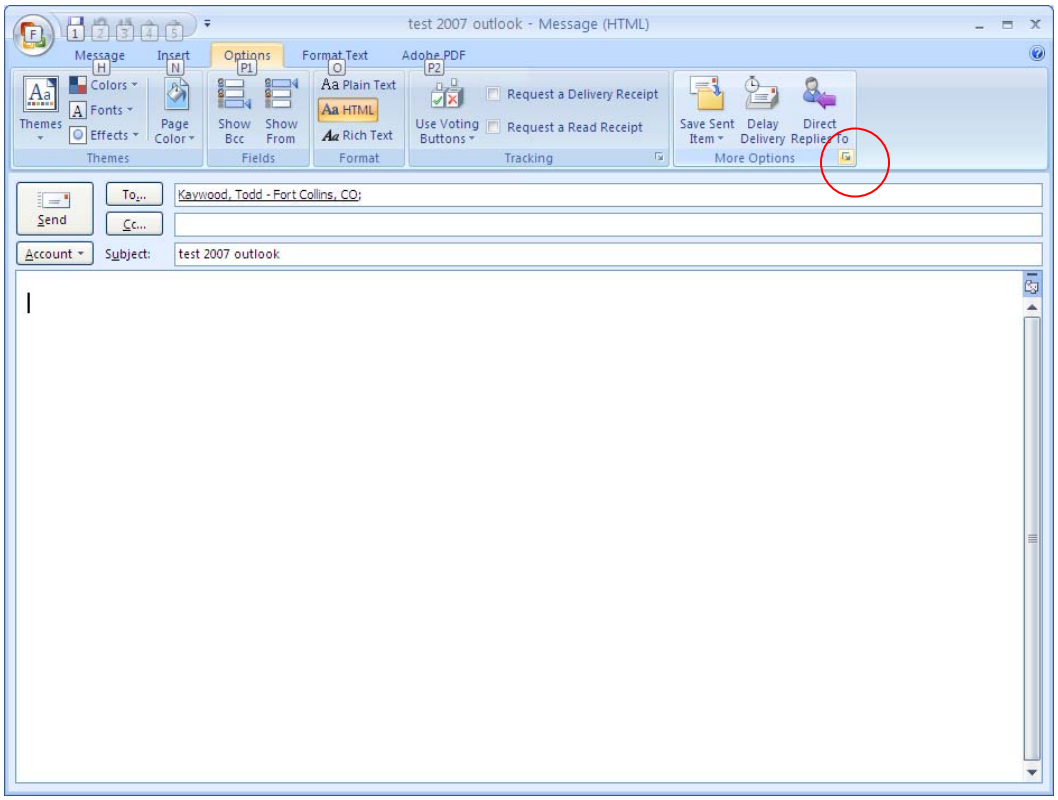


If you want to send the message in clear text signed and/or request an S/MIME receipt the email you're sending, continue on to step 8.

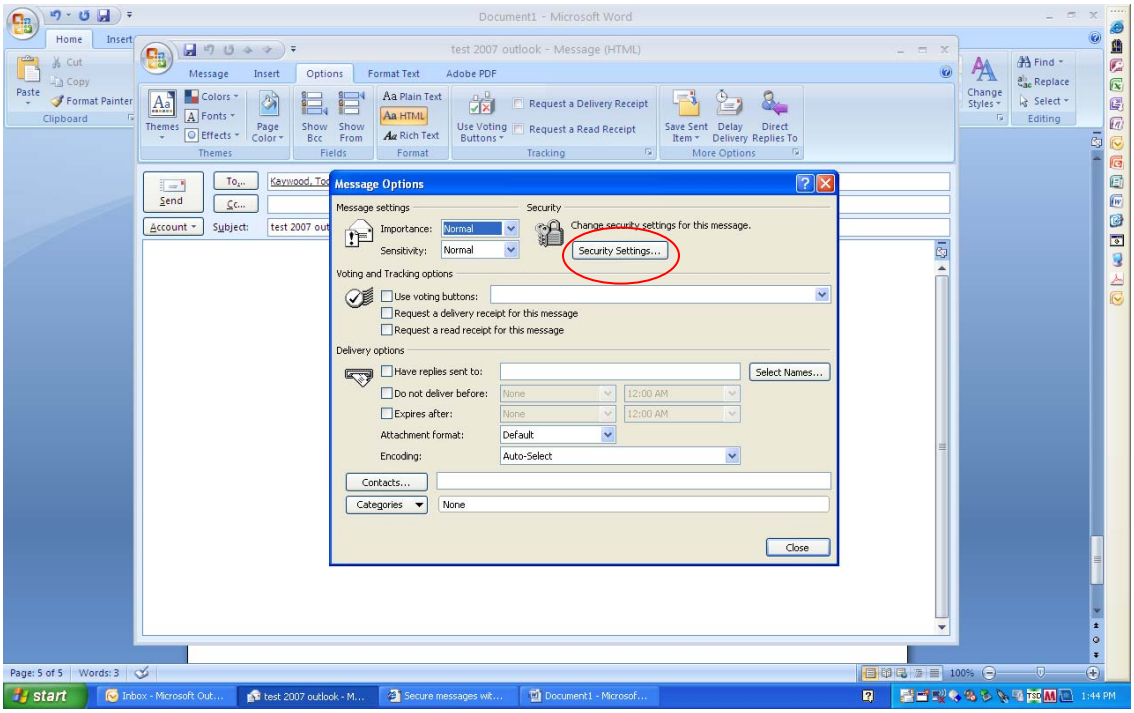
8. Start a new message in Outlook. In the top menu bar, select the Options tab.



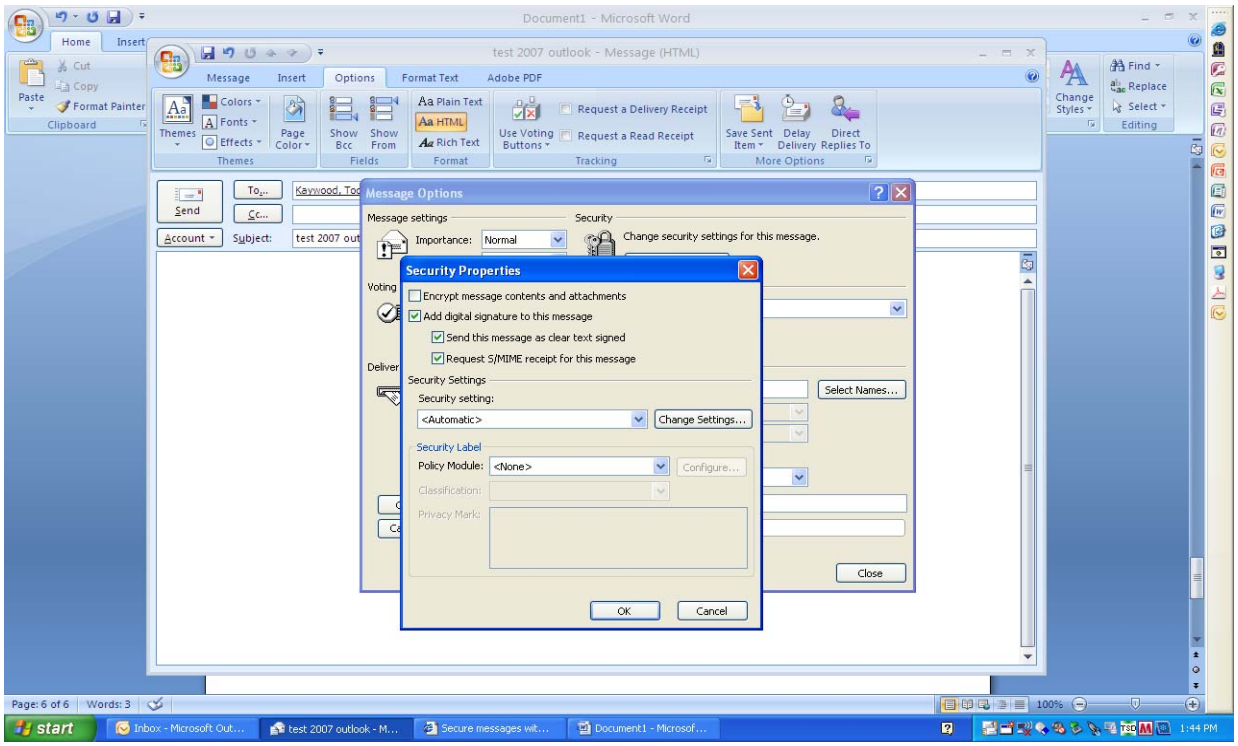
9. In the "More Options" group, click the small arrow in the lower right corner of the group title.



10. In the ***Message Options*** window, click the **Security Settings** button.

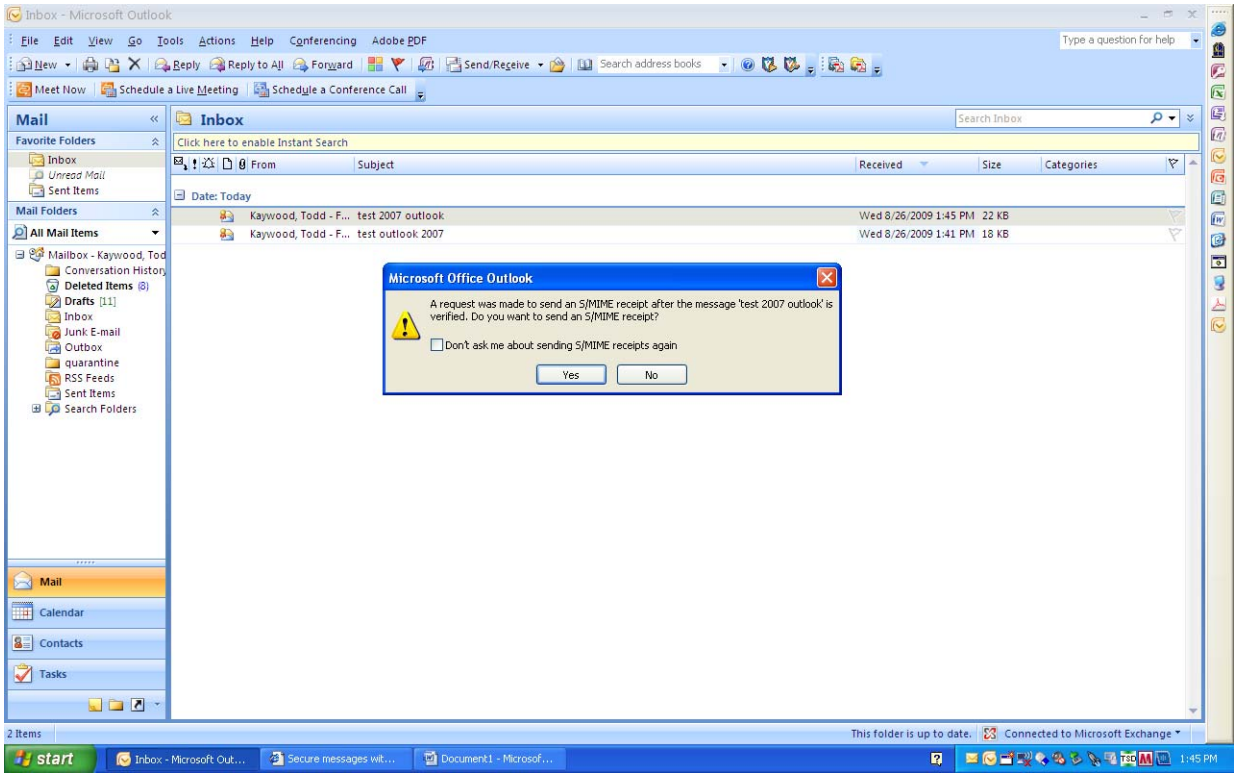


11. In the ***Security Properties*** window, check the "Add digital signature to the message" (if it isn't already checked) and, optionally, the "Send the message as clear text signed" and/or the "Request S/MIME receipt for this message" options.



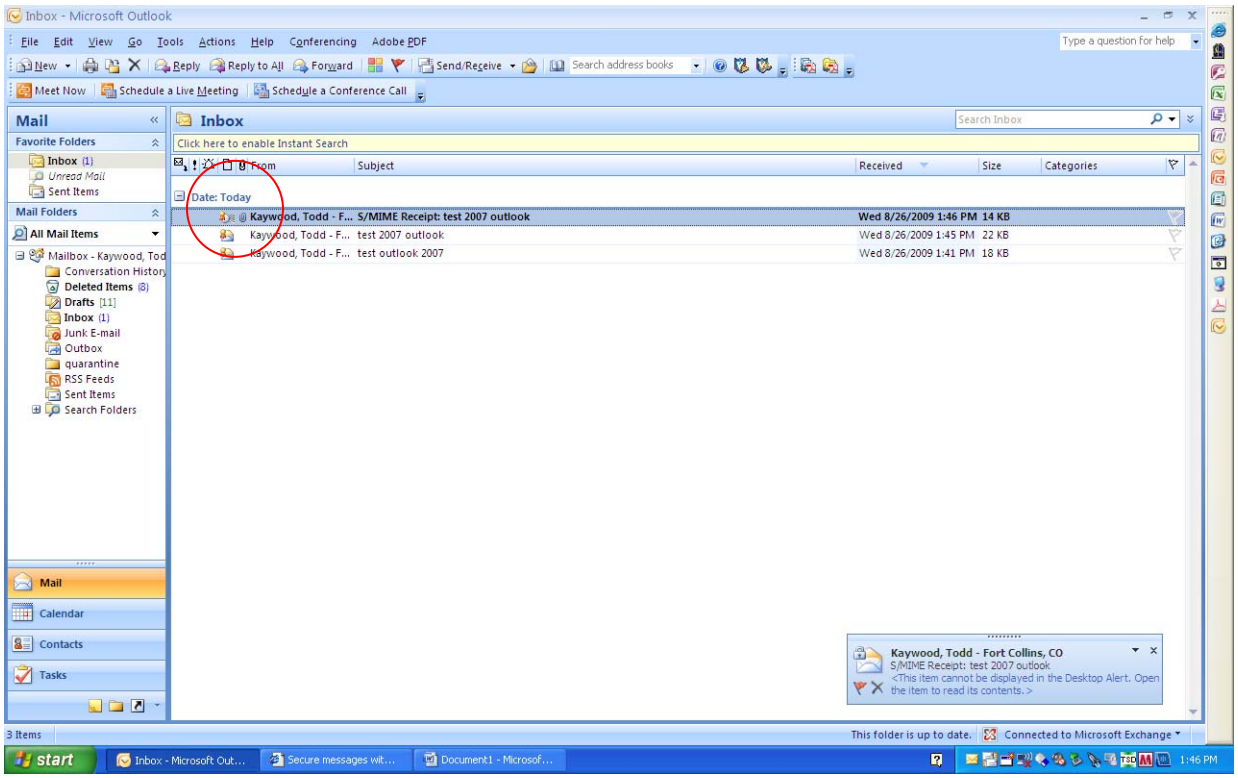
- Select **"Send this message as clear text signed"** if you want to allow others who may be using a lesser technology with Outlook to read your message. Recipients who don't have S/MIME security will be able to read the message.
- Select **"Request S/MIME receipt for all S/MIME signed messages"** if you want to be able 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.

12. Click the **OK** button to close the ***Security Properties*** window, and the **Close** button to close the ***Message Options*** window. Add recipients and content as usual, then click the **Send** button. If you selected the "Request S/MIME receipt" option, Outlook will ask you to confirm that you want to send an S/MIME receipt. If you do, click the **Yes** button; if you don't, click the **No** button. (If you want Outlook to always request the receipt when you've selected the option in step 11, first click the "Don't ask me about sending S/MIME receipts again" option, then click the **Yes** button.)

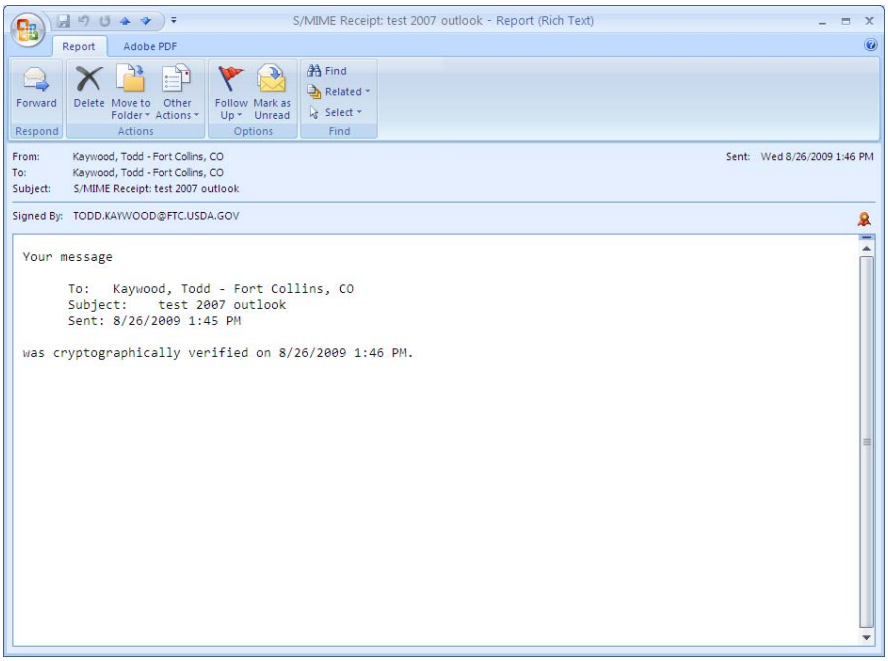


13. At the ActivClient prompt, enter your LincPass PIN, then press ENTER or click the **OK** button.

14. The message will appear in the recipient's Inbox with an envelope with a red ribbon on it, indicating the message is digitally signed. If you want to check the signature, follow steps 6 and 7 above.

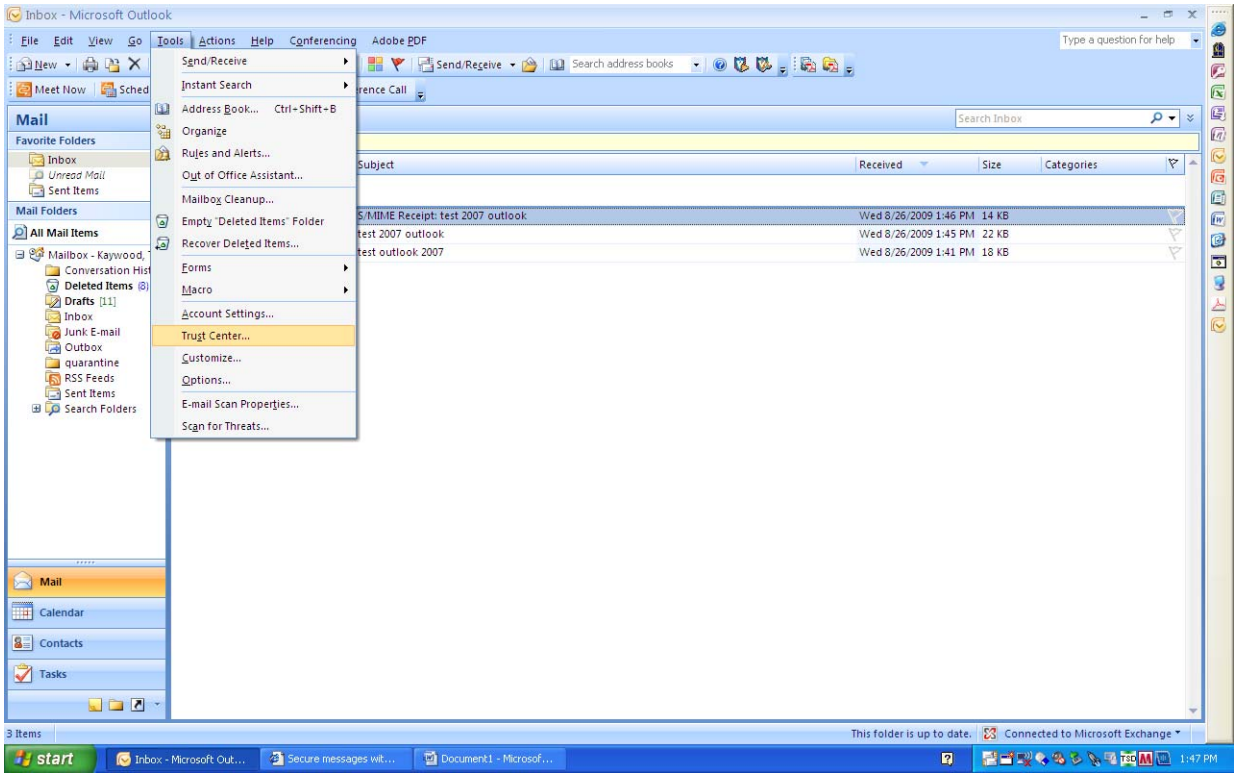


15. If you selected the "Request S/MIME receipt" option, you'll receive a new message that will require you to enter your LincPass PIN again before you can open it.

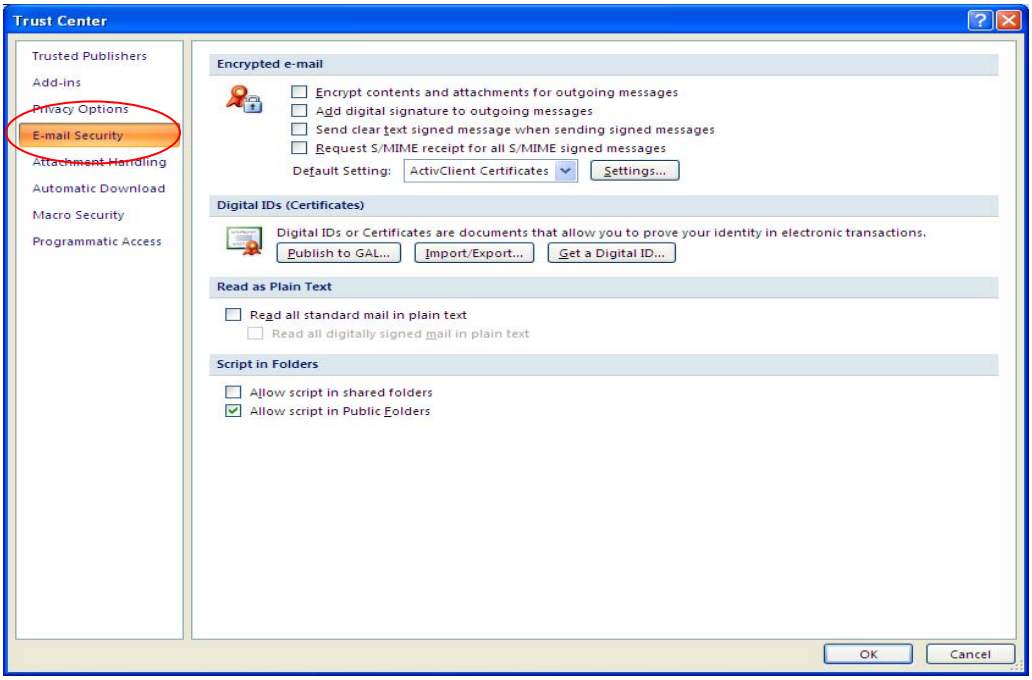


2.2.2 Digitally Sign All Messages by Default

1. Open Outlook and, if it isn't already there, insert your LincPass in the card reader.
2. From the top menu bar, select **Tools**, then **Trust Center**.

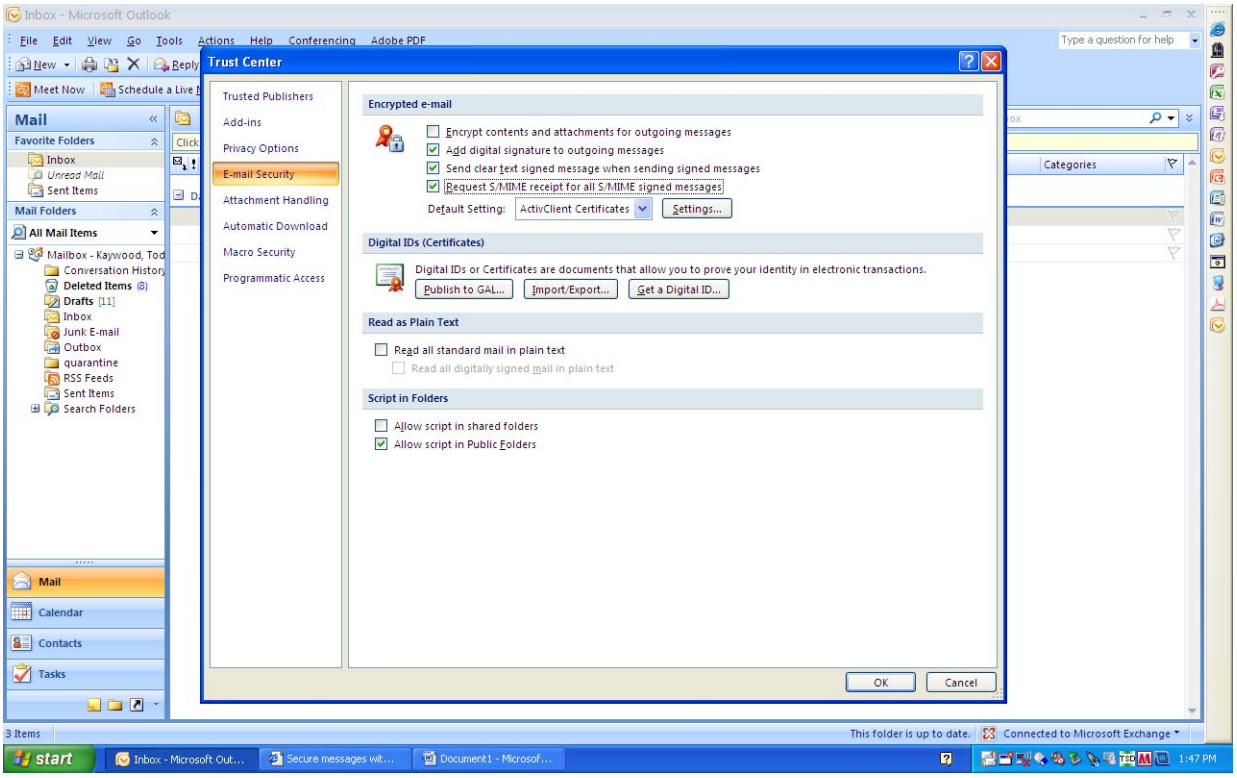


3. In the Trust Center window, select Email Security from the left menu.

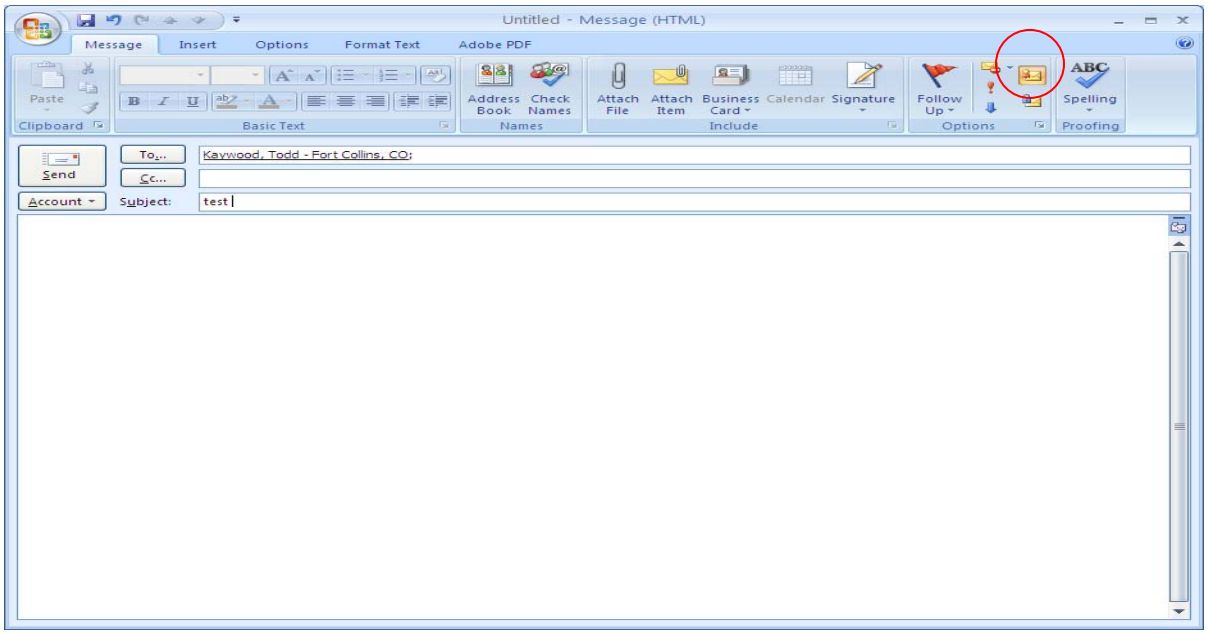


- Select **"Add ditigal signature to outgoing messages"** to automatically send digitally signed emails unless you choose not to for an individual message.
- Select **"Send clear text signed message when sending signed messages"** if you always want to allow others who may be using a lesser technology with Outlook to read your message. Recipients who don't have S/MIME security will be able to read the message.
- Select **"Request S/MIME receipt for all S/MIME signed messages"** if you want to be able 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.

NOTE: It is recommended that you don't select the "Request S/MIME receipt" option unless you have a strong business need, as it doubles the number of emails in your Inbox and adds network traffic.



4. Click the **OK** button to close the Options window. When you start a new message, your toolbar will show the envelope with a small red ribbon already selected, indicating the message will be digitally signed. (You can choose not to sign an individual email by clicking the envelope icon.)

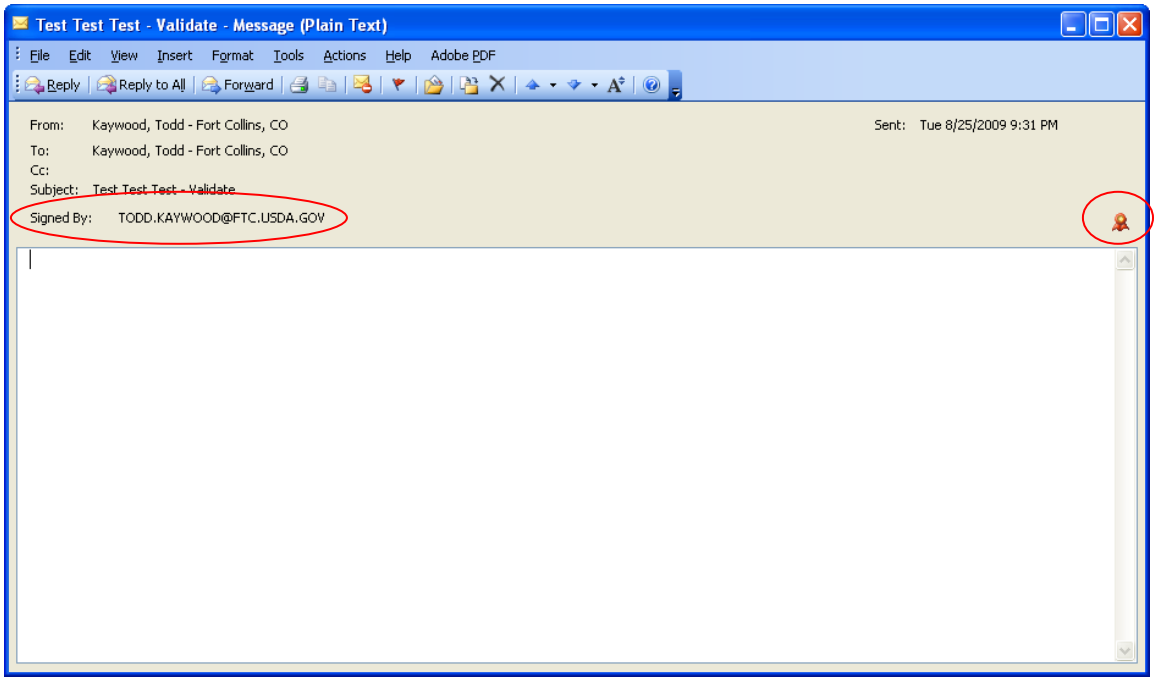


If you selected the "Request S/MIME receipt" option in step 3, you will receive a separate message with the receipt information, as described above in section 2.2.1, steps 12-15.

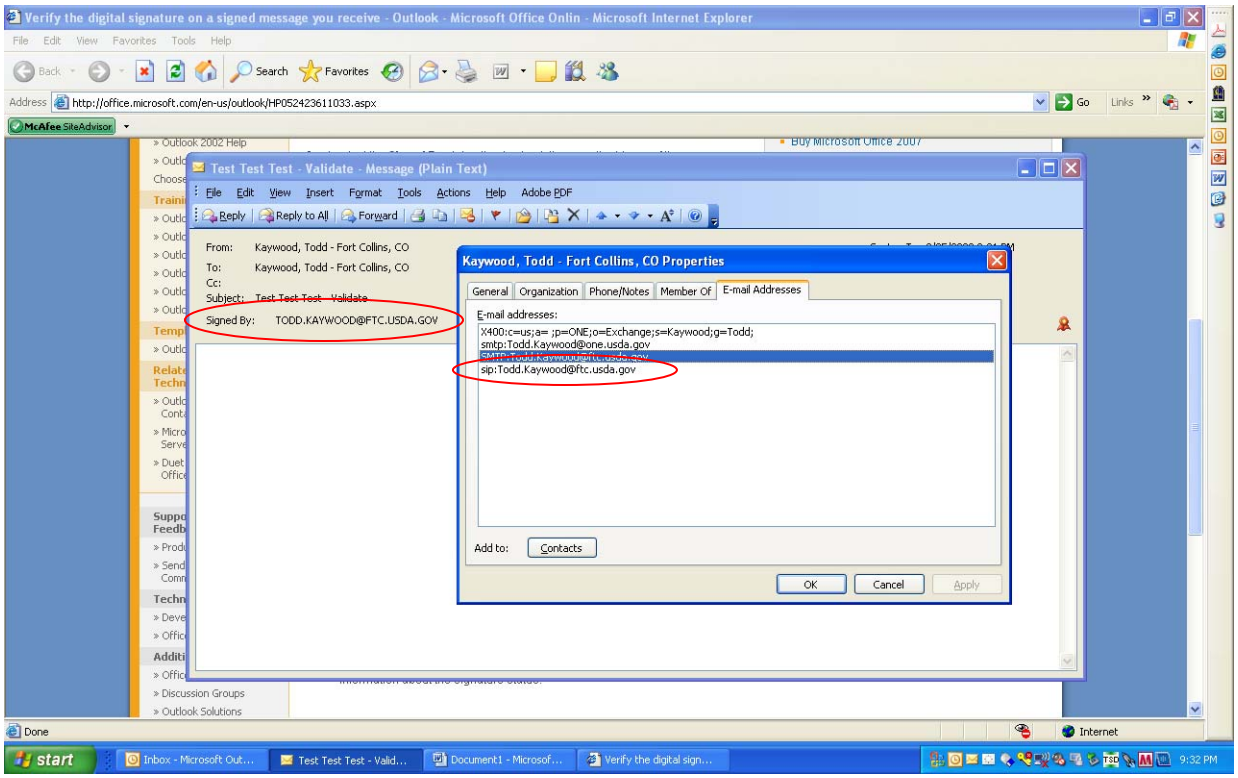
3. How to Verify a Signature is Valid (Outlook 2003 & 2007)

NOTE: The screenshots shown in this section are from Outlook 2003, but they look very similar in Outlook 2007.

1. Open the message that has been digitally signed. Outlook will show you that the email has a digital signature by showing the "Signed By" information and the red ribbon icon.



2. To verify the person who sent the email is the person who signed it, compare the "From" properties (right click the name, select Outlook Properties, then click the "Email Addresses" tab) with the email address in the "Signed By" field.



You can also click the red ribbon icon, then click the Details button to look at the signature details (see section 2.1.1, step 13 above).

NOTE: If the Signed By information is underlined in red and the red ribbon icon has a red exclamation point, the signature is invalid. Click the red ribbon icon for more information about the signature status.

4. Help Desk and Troubleshooting for Digital Signature

Problems with digitally signing documents may actually be due to problems with your LincPass. Contact the HSPD-12 help desk for assistance in resolving LincPass issues:

USDA HSPD-12 Help Desk
Toll Free: 1-888-212-9309
Local: 703-245-7888
Email: hspd12@ftc.usda.gov

If you are new to using your LincPass, consider taking the USDA AgLearn course on Two-Factor Authentication for end users (look for course ID "USDA-TwoFactorAuthEndUsers-01").

The Two-Factor Authentication Web site also has information on how to use your LincPass:
http://hspd12.usda.gov/twofactor.html
In the middle of the page is a section called "Two-Factor Authentication References," which has instructions on using your LincPass, and will help you confirm you are using your card correctly for digital signature.

If you are still having problems digitally signing documents and you know your LincPass is working correctly, contact your agency's IT help desk or IT system administrator to review your operating system, hardware (computer and card reader), and application software for correct setup and functionality.

You may be able to find answers on digital signature issues at the following vendor Web sites:

Microsoft
Microsoft Digital Signature Support Content:
http://office.microsoft.com/en-us/outlook/CH010045641033.aspx
Microsoft General Support:
http://support.microsoft.com/

Adobe
Adobe Digital Signature Support Content:
http://www.adobe.com/security/digsig.html
Adobe General Support:
http://www.adobe.com/support/

5. References

The IOA Digital Signature Web site has information on the project, user guides, technical documents, and policy guidance for digitally signing documents and emails.

IOA Digital Signature Web site:
http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digitial_signature/

Digital Signature User Guides:
http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digitial_signature/

- Digital Signatures Microsoft Office – 2003 *(this document)*
- Digital Signatures Microsoft Office – 2007
- Digital Signatures Microsoft Outlook– 2003 and 2007
- Digital Signatures Adobe Acrobat 8 & 9

Technical Configuration Guide Change
http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digitial_signature/

- Digital Signatures Adobe Configuration Change To Registry setting for Certificates

Policy Guidance
http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digitial_signature/

- OCIO I&OA Digital Signatures Policy Guidance

Vendor Web sites have information on how to apply digital signatures in their products:

Microsoft Office
Location: Microsoft Support Site
http://www.microsoft.com/downloads/details.aspx?FamilyId=79d06e72-4b45-4669-9eac-0eca5821e8ff&displaylang=en

Microsoft Outlook
Location: Microsoft Support Site
http://www.microsoft.com/downloads/details.aspx?FamilyId=CC37CC1E-028D-4D30-9093-96CC6513ECA1&displaylang=en

Adobe Acrobat 8 & 9
Location: Adobe support site
http://learn.adobe.com/wiki/display/security/Document+Library
http://www.adobe.com/security/digsig.html

USDA Web sites have general information on the issuance, activation, and use of the LincPass card:

HSPD12
http://hspd12.usda.gov/index.html
http://hspd12.usda.gov/faq.html

Two-Factor Authentication
http://hspd12.usda.gov/twofactor.html

-- -- --