



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

SEP 19 2008

MEMORANDUM FOR DIRECTORS, TRICARE MANAGEMENT ACTIVITY

SUBJECT: Updated Guidelines on Protection of Sensitive Information in Electronic Mail

This memorandum provides updated guidelines in accordance with TRICARE Management Activity (TMA) memo "Guidelines on Protection of Sensitive Information in Electronic Mail" of 25 June 2008. The attachment updates procedures to include the use of Microsoft Office 2007 to encrypt a file containing sensitive information that can then be sent attached to electronic mail (e-mail).

Per federal law and DoD policy (references attached), all users of the TMA/Health Affairs (HA) network must ensure that sensitive information is protected when transmitted via an e-mail whether in the text or in an attachment. Use of DoD Public Key Infrastructure (PKI) to encrypt an e-mail shall always be the primary means when sending sensitive information beyond the TMA/HA network with e-mail.

TMA policy requires that any e-mail that contains or has an attachment with sensitive information and is sent outside the TMA network must be encrypted and digitally signed. All TMA network users are cautioned to review addressees when replying or forwarding an e-mail to determine if it should be encrypted because an addressee is outside the TMA network.

Questions regarding use of PKI or these guidelines should be directed to Mr Daniel Brooks, [daniel.brooks@tma.osd.mil](mailto:daniel.brooks@tma.osd.mil), (703) 681-6867 in the Information Assurance Division..

A handwritten signature in black ink, appearing to read "Charles Campbell".

Charles Campbell  
Chief Information Officer  
Military Health System

Attachments:  
As stated

Attachment 1 to TMA memorandum "Updated Guidelines on Protection of Sensitive Information in Electronic Mail"

- (a) The Privacy Act of 1974, (Public Law 93-579), Title 5 U.S. Code, Section 552a, 2000
- (b) Health Insurance Portability and Accountability Act (HIPAA), Security Standards, Title 42 U.S. Code, Section 1306, February 20, 2003
- (c) Federal Information Security Management Act of 2002 (FISMA), TITLE III— Information Security, December 2002
- (d) DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004
- (e) DOD 5200.1-R, "Information Security Program," January 1997
- (f) DOD Directive 5400.11 "DoD Privacy Program," May 8, 2007
- (g) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (h) TRICARE Management Activity Memorandum, "Protection of Sensitive Information in Electronic Mail," 13 Aug 2007

**Guidelines for  
Sending Sensitive Information in E-mail  
When the use of DoD-approved Public Key Infrastructure (PKI)  
Is not possible with the Business Partner**

Follow these three steps when PKI cannot be used.

1) **FIRST** – Verify that PKI or other secure means (e.g. access to system or web server) is not possible for the business partner. Always discuss the security of the recipient's e-mail system and network with the recipient before sending to determine the best approach.

- If the business partner is a federal agency, ask when they will be getting their Personal Identity Verification (PIV) card and using PKI with their e-mail system. Also, ask if that can be expedited for them. Use an approved alternative in the interim.
- If the business partner is a state or local government, verify that they do not have or are not getting PKI within their organization. If they can't use PKI, use an approved alternative.
- If the business partner is on contract to TMA, there must be a plan to implement PKI on the contract. In the interim, an approved alternative can be used.
- If the business partner is a non-government organization that is not on contract to TMA and the transmissions are going to be routine (continuous and frequent over a long period of time), ask if they would voluntarily use a DoD-approved PKI. If not, use an approved alternative.
- If the business partner is a non-government organization that is not on contract to TMA and this is a one (or few) time transmission, use an approved alternative.

Please be aware that how often and how sensitive the information is that is being sent determines the risk of compromise. (routine transmissions of PII/PHI create a pattern that is more likely to be compromised and more likely to have a serious impact than infrequent transmissions of non-PII/PHI).

2) **SECOND** - Place the information in a file, encrypt the file using a TMA approved product and procedures (see enclosure (1)), attach the file to an e-mail addressed to the recipient, and digitally sign the e-mail (see enclosure (2)).

3) **THIRD** - Separately from the e-mail that has the encrypted file attached, provide the recipient the password to use to decrypt the file.

The preferable method is to call on the telephone and personally tell the recipient the password. Do not leave it on a voicemail system.

As an alternative if a telephone call is not possible is to send the password via a e-mail

- Send a separate, unrelated, and digitally signed e-mail.
- Use a different Subject line.
- Do not use Reply or Forward with the original e-mail that has the encrypted file.
- Do not state in the message text that the password is a password.
- Do not state in the message text what file the password is for

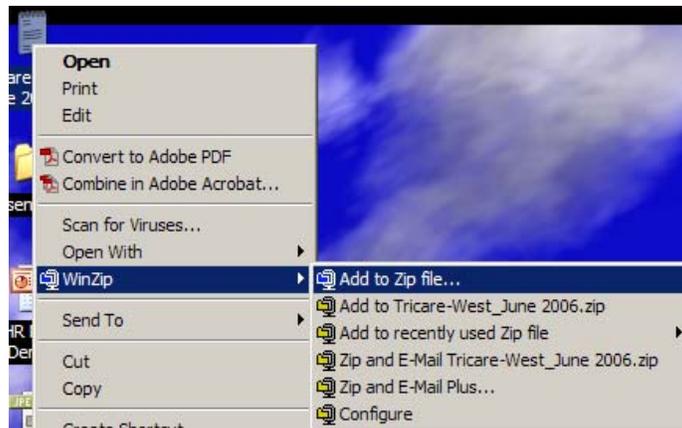
## **TMA Approved Products and Procedures For encrypting a file in an e-mail when the recipient cannot use PKI**

There are two approved products for encrypting a file when using Microsoft Office 2003 or Windows XP: WinZip version 9 and Adobe Acrobat version 7. The first two procedures below must be followed when using those products. Product 1 refers to WinZip version 9 and Product 2 refers to Adobe Acrobat version 7.

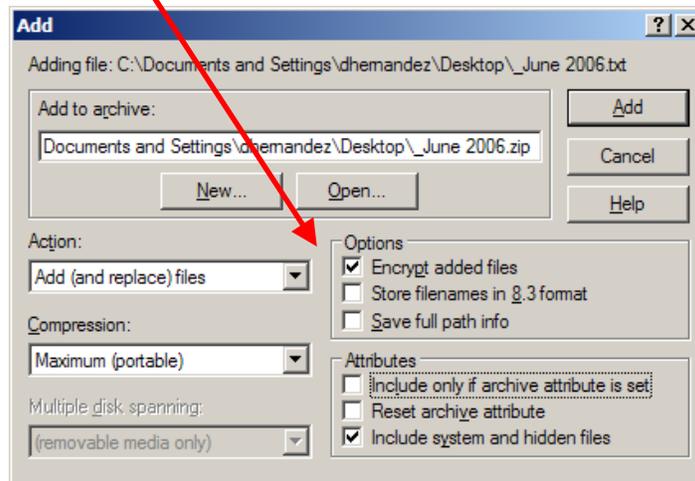
Microsoft Office 2007 employs a different process for encrypting a file. The third product listed below illustrates the procedure that must be followed when using Microsoft Office 2007.

Product 1 - WinZip version 9 is part of the standard TRICARE Management Activity (TMA) office automation suite. The recipient must also have WinZip. WinZip is publicly available to recipients. Evaluation versions of WinZip can be obtained and used without cost (<http://www.winzip.com/dprob.htm>). It is recommended that version 10 only be used if upgraded with Build 7245.

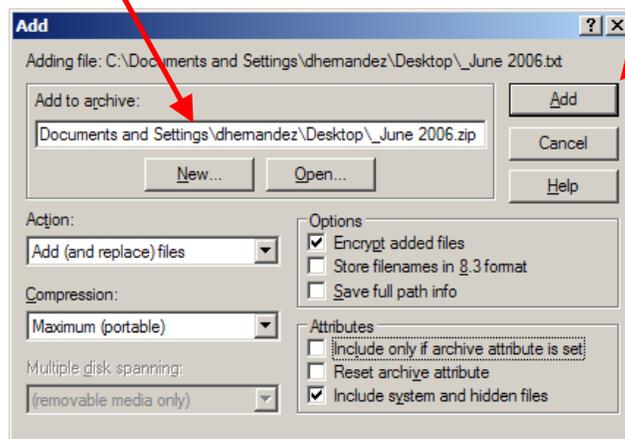
- Browse to file(s) you want to encrypt. Then RIGHT-click on the file(s), select 'WinZip', and LEFT-click on **Add to Zip file...**



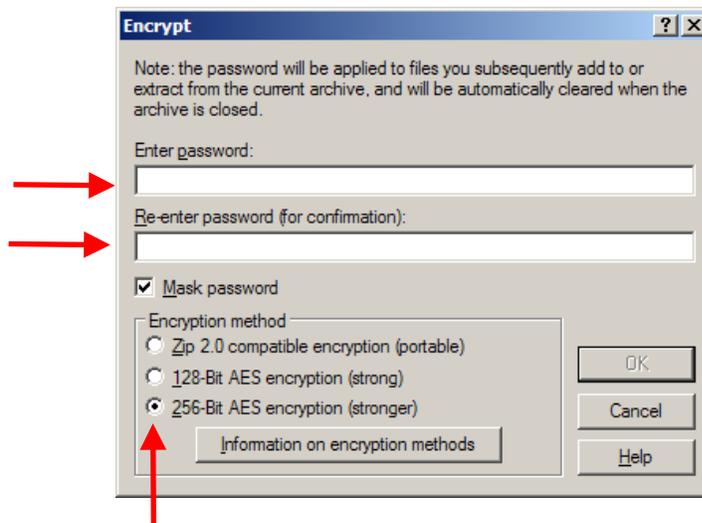
- Choose the **Encrypt added files** under Options



Make a note of the location where the file will be placed, then select the **Add** button.



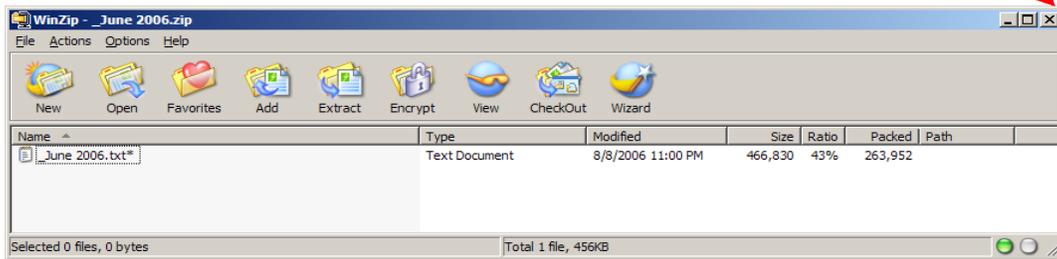
- Create a password when the Encrypt dialog box opens. Passwords must:
  - be at least 9 characters in length
  - contain at least 2 numeric characters
  - contain at least 2 upper and 2 lower case alphabetic characters
  - contain at least 2 special characters (special characters are located above the numeric keys on a standard keyboard)
  - not use common words or phrases



- Select **256-Bit AES encryption (stronger)** under Encryption method. Then click **OK** button.

Attachment 2 to TMA memorandum “Updated Guidelines on Protection of Sensitive Information in Electronic Mail”

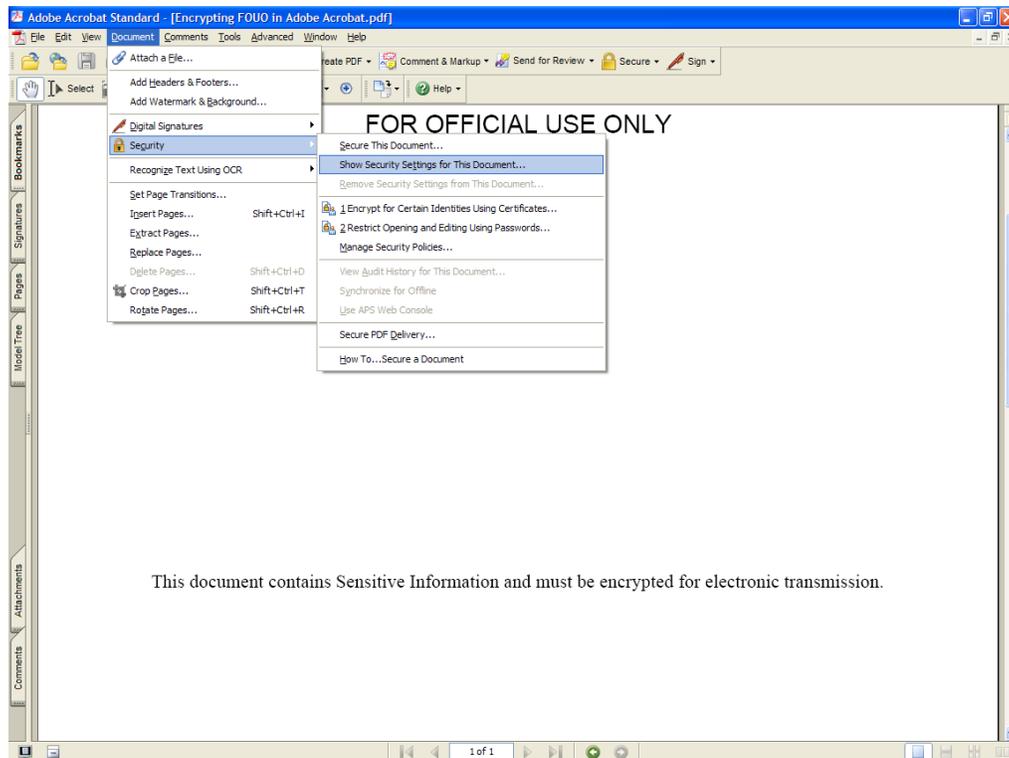
The file(s) will be added to the WinZip main screen. Exit by clicking the **X**.



**NOTE:** Because many e-mail systems block files with the ‘.zip’ extension, one may need to change the file extension before attaching and sending. The recipient(s) will then be required to change the file BACK to a ‘.zip’ file to open. To do this, browse to the location of the file, Right click on the file and choose ‘Rename’. Change the last three characters to something such as ‘txt’ or ‘piz’.

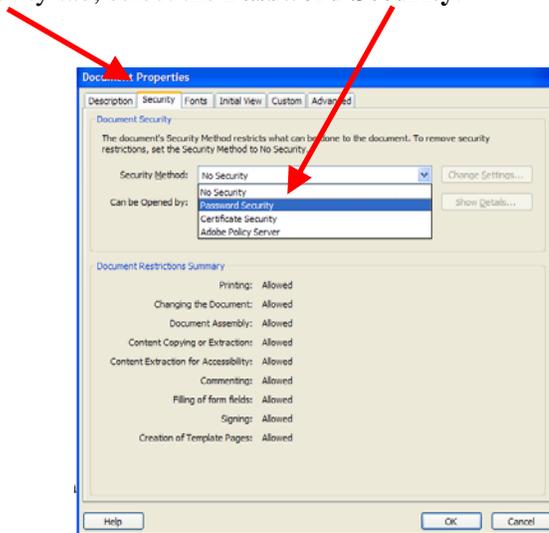
Product 2 – Adobe Acrobat version 7 or greater may be used to encrypt files. Previous versions do not have the required encryption algorithm and are not to be used. Both sender and recipient must have a copy of Adobe Acrobat. Individual TMA offices must coordinate with network operations to procure and install the proper version of Adobe Acrobat.

- Open the Adobe .pdf file. Click on **Document/Security/Show Security Settings for This Document...**

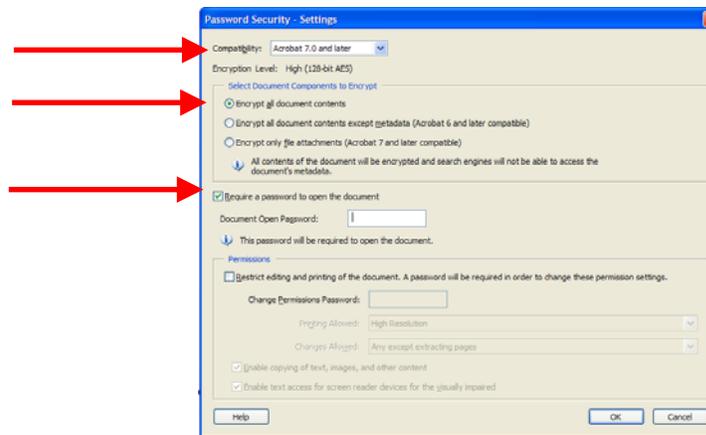


Attachment 2 to TMA memorandum “Updated Guidelines on Protection of Sensitive Information in Electronic Mail”

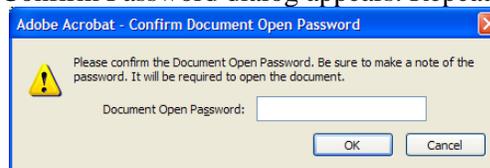
- From the Security tab, select the **Password Security**.



- Choose **Acrobat 7.0 or Higher** in the **Compatibility** drop-down menu, then select **Encrypt all document contents**, and **Require a Password**.

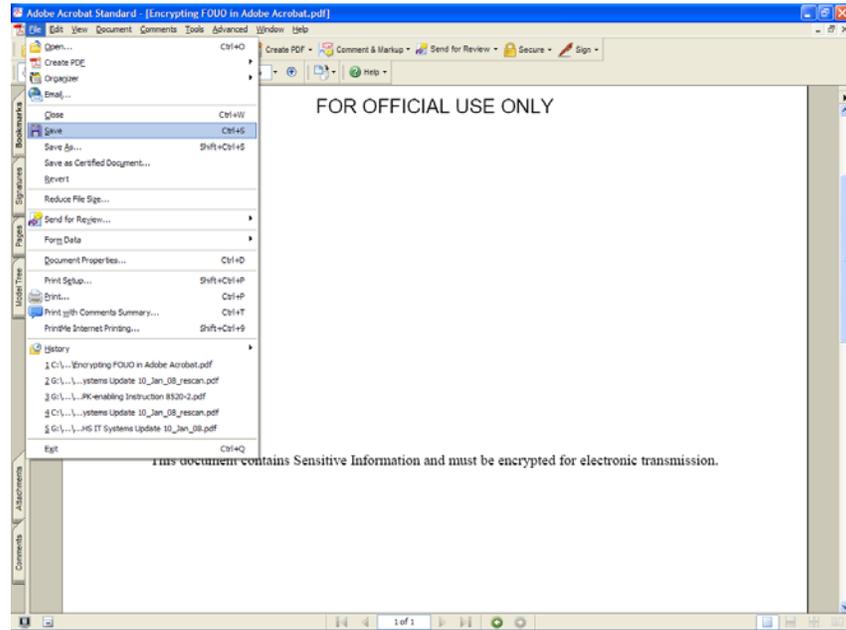


- Type in a password beside **Document Open Password:** Passwords must:
  - be at least 9 characters in length
  - contain at least 2 numeric characters
  - contain at least 2 upper and 2 lower case alphabetic characters
  - contain at least 2 special characters (special characters are located above the numeric keys on a standard keyboard)
  - not use common words or phrases
- Click the **OK** button. A Confirm Password dialog appears. Repeat the password & click **OK**.

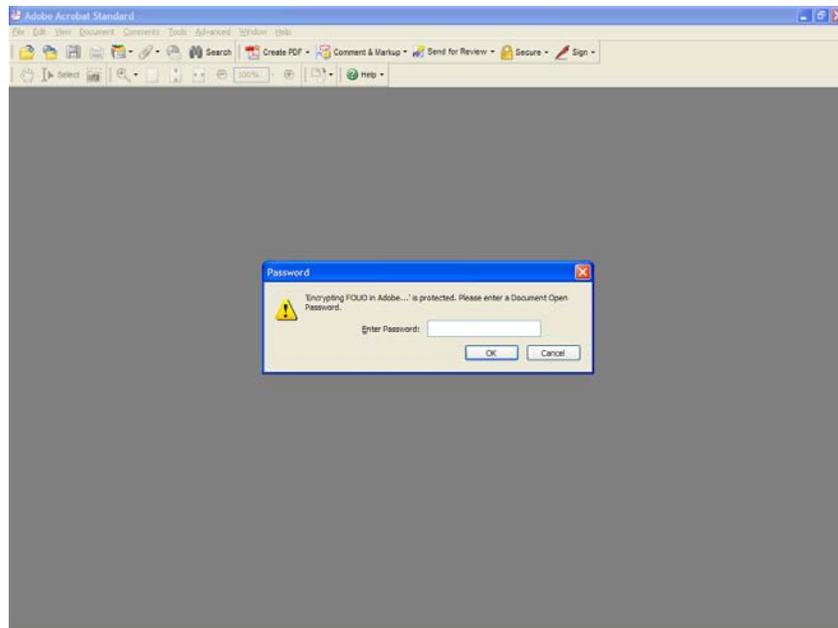


Attachment 2 to TMA memorandum “Updated Guidelines on Protection of Sensitive Information in Electronic Mail”

- Save the document for the security settings to be applied to the document.



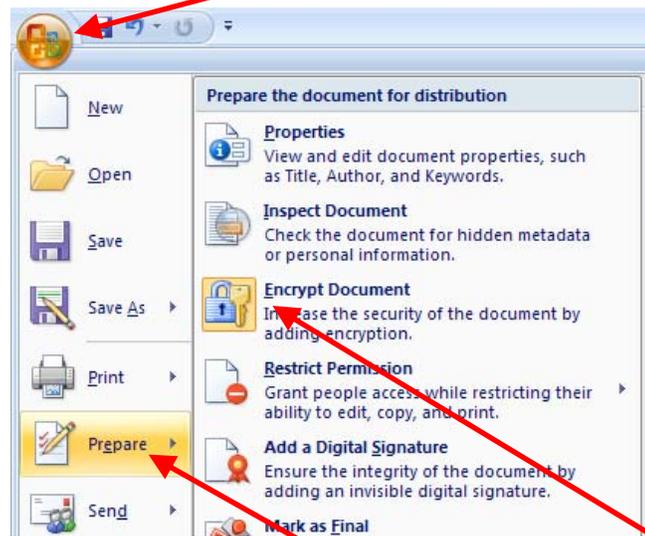
- When the document is opened it will ask for the password.



Product 3 – Use this procedure when employing Microsoft Office 2007. The following steps are applicable to the 2007 versions of Microsoft Word, Excel and PowerPoint.

*NOTE:* To decrypt the file, the recipient will either need the 2007 version of the product used to place the sensitive information (Word, Excel, or PowerPoint 2007), or the XP or 2003 version *plus* the free download Compatibility Upgrade from Microsoft (<http://www.microsoft.com/downloads/details.aspx?FamilyId=941B3470-3AE9-4AEE-8F43-C6BB74CD1466&displaylang=en>).

- Step 1: Before saving the file, first click on the **Office Button** in the upper left corner of the window.



- Step 2: To encrypt the document, click on **Prepare** and then on **Encrypt Document**
- Step 3: Type the password in the Password box. Passwords must:
  - be at least 9 characters in length
  - contain at least 2 numeric character
  - contain at least 2 upper and 2 lower case alphabetic characters
  - contain at least 2 special character
  - not use common words or phrases



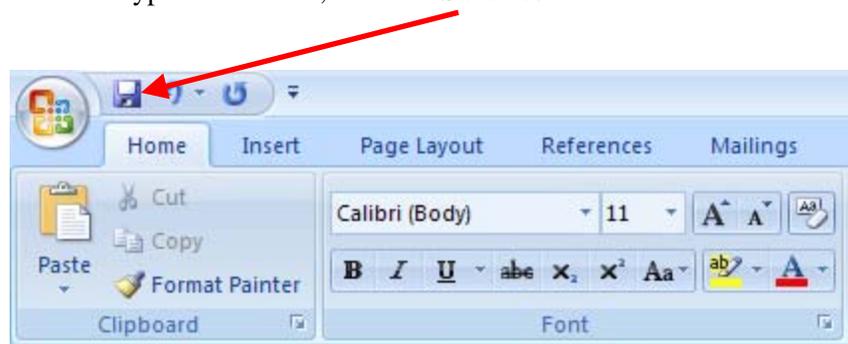
- Click **OK** to set the security for the document

Attachment 2 to TMA memorandum “Updated Guidelines on Protection of Sensitive Information in Electronic Mail”

- Reenter the **password** and click **OK** to confirm



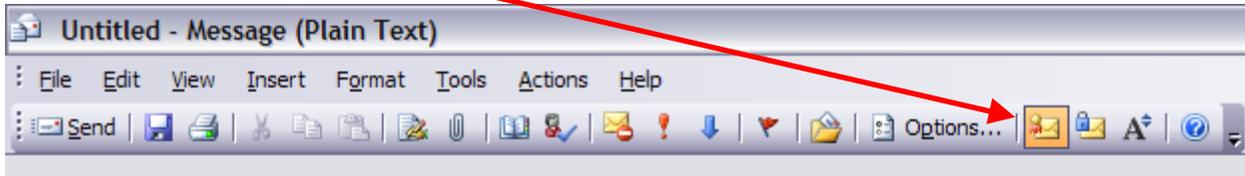
- To save the encrypted document, click the **Save Icon**



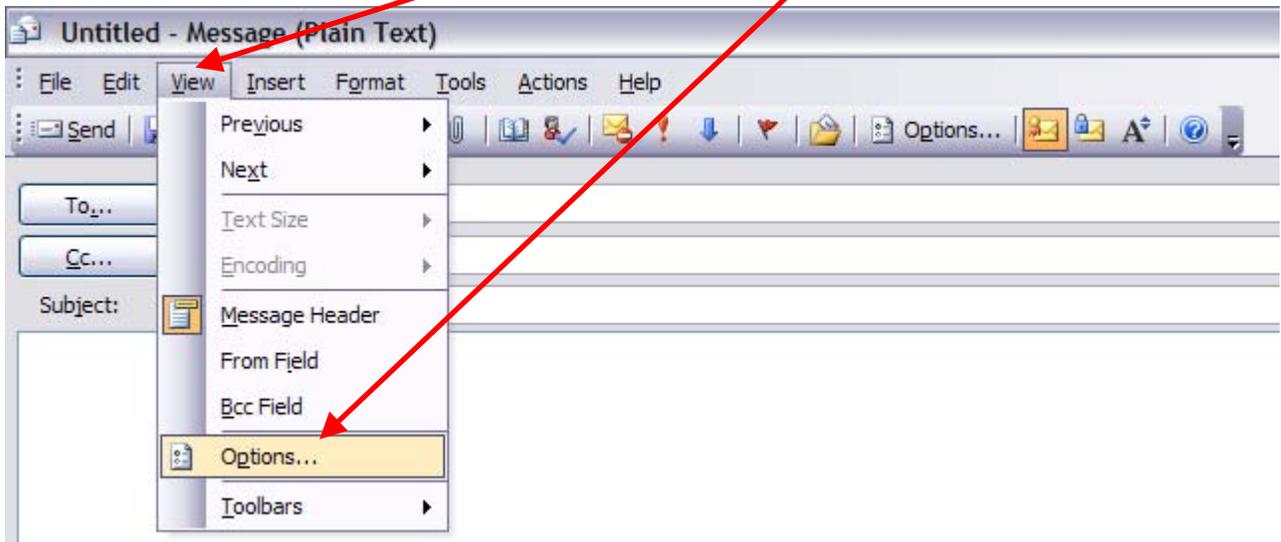
## Procedures for Digitally Signing E-mails Using Microsoft Outlook

Microsoft Office 2003 or Windows XP - Once a file is encrypted using Product 1 or Product 2, the user can create an e-mail message with the encrypted file attached, and a separate e-mail containing the password for the file. The following steps are applicable to digitally sign an e-mail using the 2003 version of Microsoft Outlook. or Windows XP.

- Step 1: Click on the **Sign** icon on the tool bar and go to Step 6.



- Step 2: If the icon is unavailable, click on the **View** and then **Options** in the upper left corner of the window.

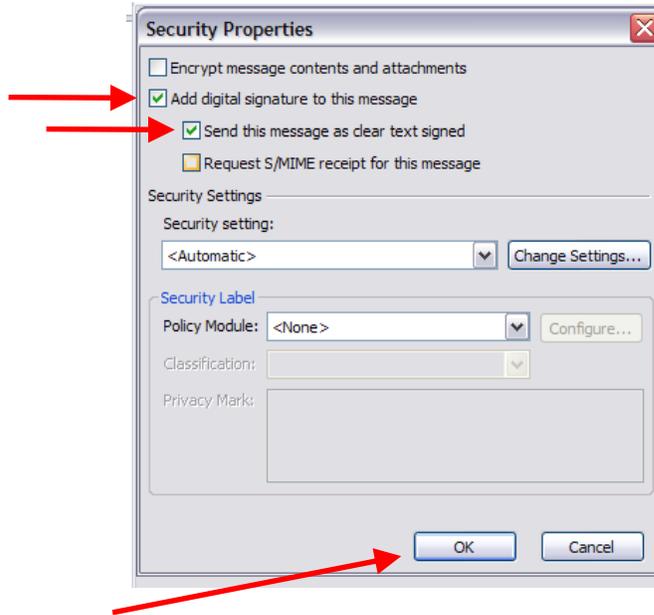


- Step 3: When the “Message Options” Box appears Click on **Security Settings**



Attachment 2 to TMA memorandum “Updated Guidelines on Protection of Sensitive Information in Electronic Mail”

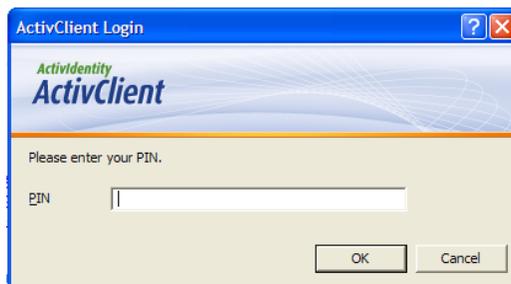
- Step 4: Select **Add Digital Signature to this message** and **Send this message as clear text signed**



- Step 5: Click on **OK** and then close the Message Options window
- Step 6: Send the message by pressing the **Send** button



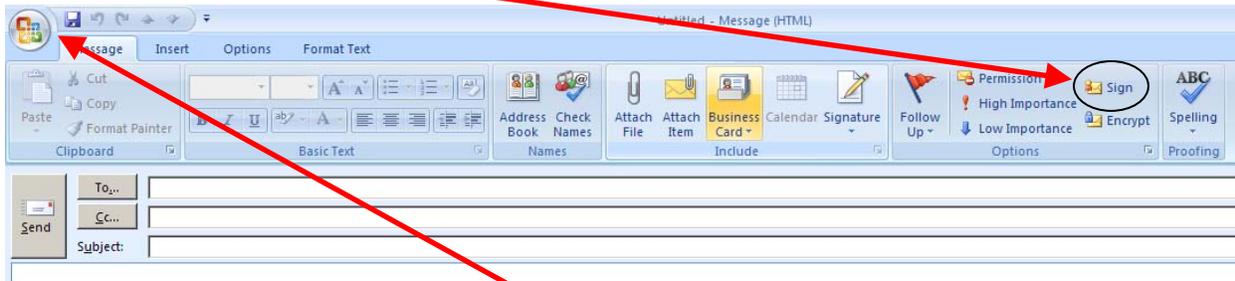
- The user will be prompted to enter their **PIN**



Attachment 2 to TMA memorandum “Updated Guidelines on Protection of Sensitive Information in Electronic Mail”

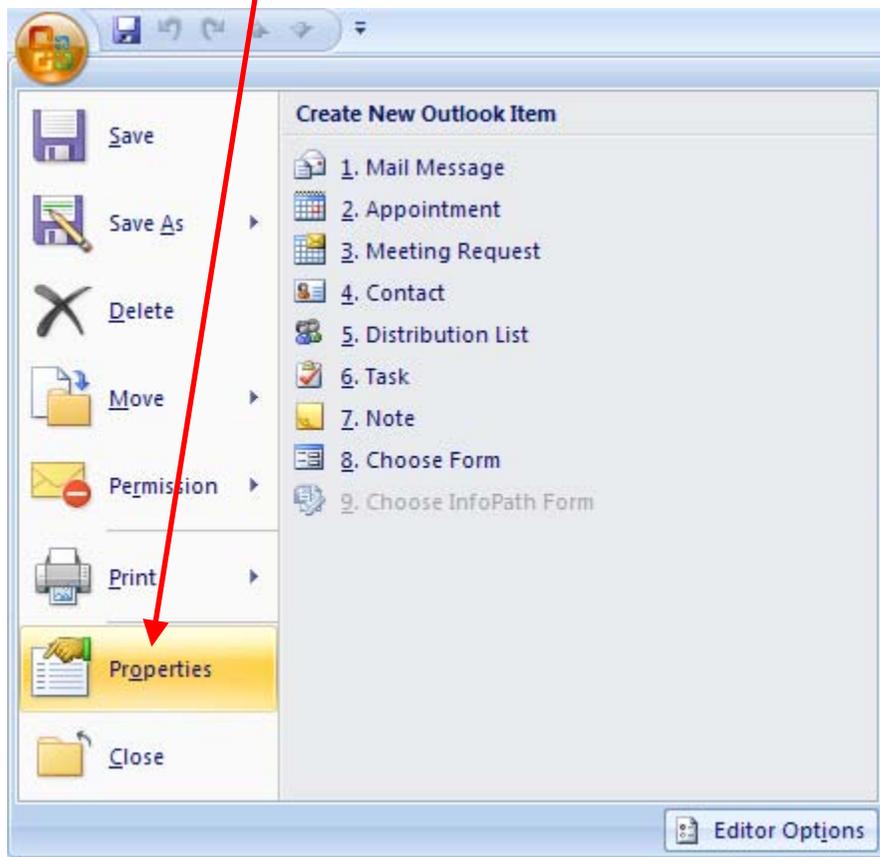
Microsoft Office 2007 – Once a file is encrypted, the user can create an e-mail message with the encrypted file attached, and a separate e-mail containing the password for the file. The following steps are applicable to digitally sign an e-mail using the 2007 version of Microsoft Outlook.

- Step 1: Click on the **Sign** icon on the tool bar and go to Step 5.



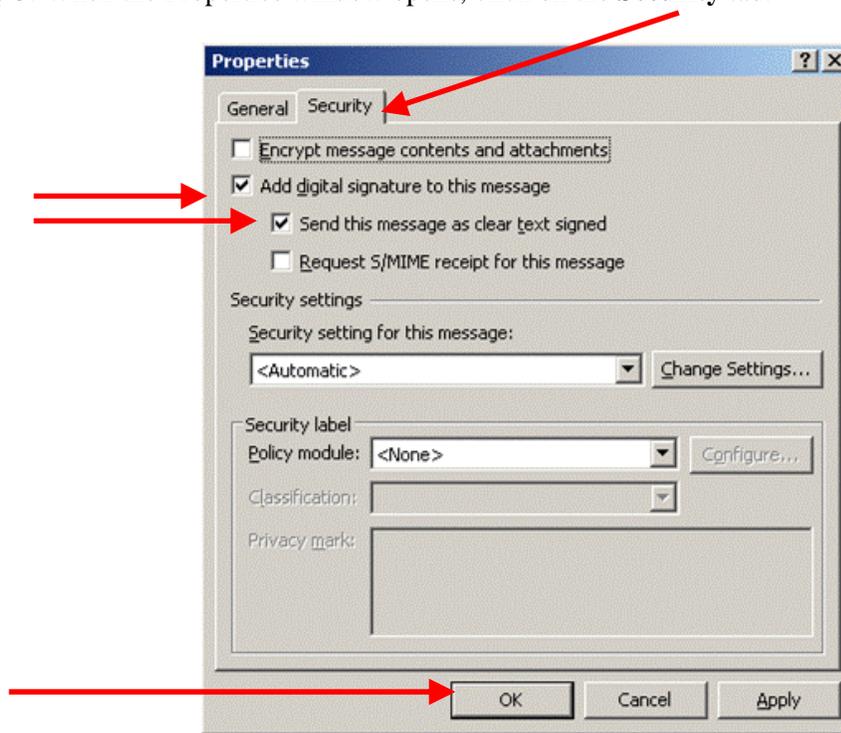
If the icon is unavailable, click on the **Office Button** in the upper left corner of the window.

- Step 2: Click on the **Properties** tab.

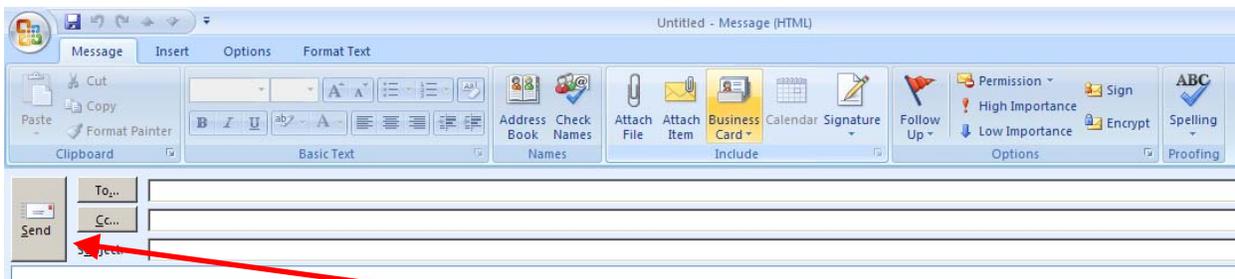


Attachment 2 to TMA memorandum “Updated Guidelines on Protection of Sensitive Information in Electronic Mail”

- Step 3: When the Properties window opens, click on the **Security** tab.



- Step 4: Select **Add digital signature to this message** and **Send this message as clear text signed** then click **OK**.



- Step 5: Send the message by pressing the **Send** button.
- The user will be prompted to enter their **PIN**.

