



TRICARE
MANAGEMENT
ACTIVITY

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

JUN 25 2008

MEMORANDUM FOR DIRECTORS, TRICARE MANAGEMENT ACTIVITY

SUBJECT: Guidelines on Protection of Sensitive Information in Electronic Mail

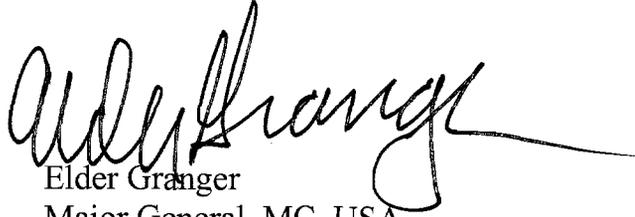
This memorandum provides specific guidelines to implement the TRICARE Management Activity (TMA) memorandum "Protection of Sensitive Information in Electronic Mail (e-mail)" of August 13, 2007. Ensuring the proper protection in accordance with Department of Defense (DoD) policy and federal direction is essential to safeguarding beneficiary as well as TRICARE business information.

TMA personnel communicating with TMA business partners; including federal, state, and local government organizations, as well as private businesses that currently cannot accept e-mail with Public Key Infrastructure (PKI) encryption, shall follow the attached guidelines to send sensitive information. Each TMA office sending sensitive information in e-mail without using PKI must keep a record of what was sent and the recipient. If a business partner acquires PKI capability, e-mails with sensitive information shall then use PKI.

Each program manager of a TMA contract shall include, or have a plan to include, the requirement to accept e-mail with sensitive information encrypted by DoD PKI. TMA Procurement Support's Task Order templates, available on the TMA Web site at http://www.tricare.mil/tps/Acquisition_Tools_Guides.cfm, include PKI in the information assurance section which must be enforced by program managers.

Only by using approved methods can we protect against threats to e-mail and the information or files in them. When additional products are approved for use, the Military Health System Chief Information Officer (CIO) will update and distribute the attachment. This memorandum will be posted on the TMA Web site with all other TMA network policies and guidance.

If a business partner cannot use PKI and has reason not to use an approved alternative, managers should coordinate with Mr. Daniel Brooks, who may be reached at (703) 681-6867 or Daniel.Brooks@tma.osd.mil in the CIO's Information Assurance Division.

A handwritten signature in black ink, appearing to read 'Elder Granger', with a long horizontal flourish extending to the right.

Elder Granger
Major General, MC, USA
Deputy Director

Attachments:
As stated

Guidelines for Sending Sensitive Information in E-mail When the use of Department of Defense-approved Public Key Infrastructure Is not possible with the Business Partner

Follow these three steps when Public Key Infrastructure (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. Before sending an e-mail, always discuss with the recipient the security of the recipient's e-mail system and network to determine the best approach.

- If the business partner is a federal agency, ask when they will be getting their Personal Identification Verification 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 TRICARE Management Activity (TMA), there must be a plan to implement 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 Department of Defense (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 the sensitivity of information and how often it is sent to the same user affects the risk of compromise (routine transmissions of Personally Identifiable Information/Protected Health Information (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 an approved product and procedures for the TMA network (see enclosure (1)), attach the file to an e-mail to the recipient, and digitally sign the e-mail (see enclosure (2)).

3) **THIRD** - Separately from the e-mail with the encrypted file, 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 the password on a voicemail system.

Alternatively, if a telephone call is not possible, then send the password via an e-mail.

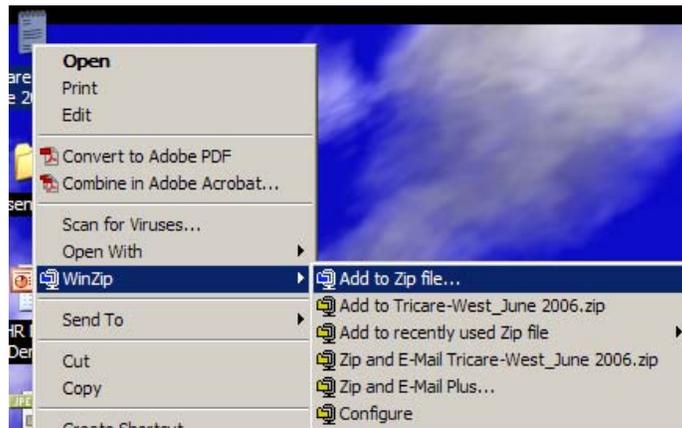
- Send a separate, unrelated, and digitally signed e-mail.
- Use a different Subject line.
- Do not use Reply or Forward with the original e-mail that has the encrypted file.
- Do not state in the message text that the password is a password.
- Do not state in the message text what file the password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

TRICARE Management Activity Approved Products and Procedures For encrypting a file in an e-mail when the recipient cannot use Public Key Infrastructure

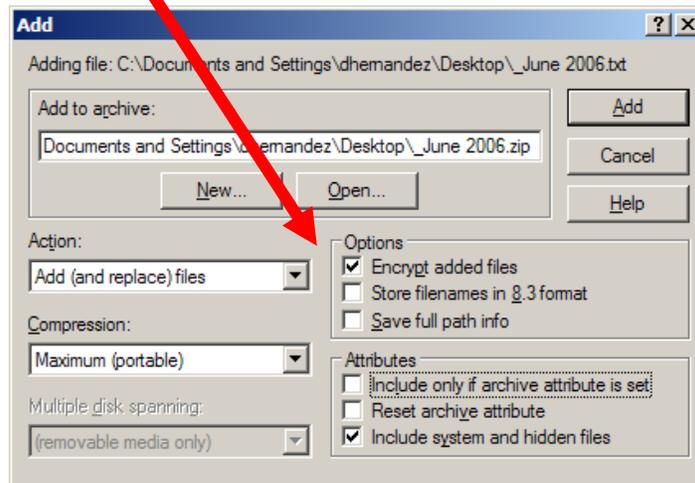
There are two approved products. The procedures below must be followed when using the product.

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. Evaluations 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.

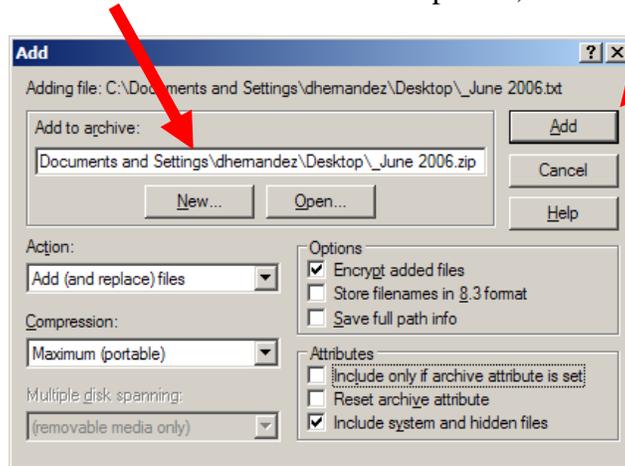
- o Browse to file(s) you want to encrypt. Then RIGHT-click on the file(s), select 'WinZip', and LEFT-click on **Add to Zip file...**



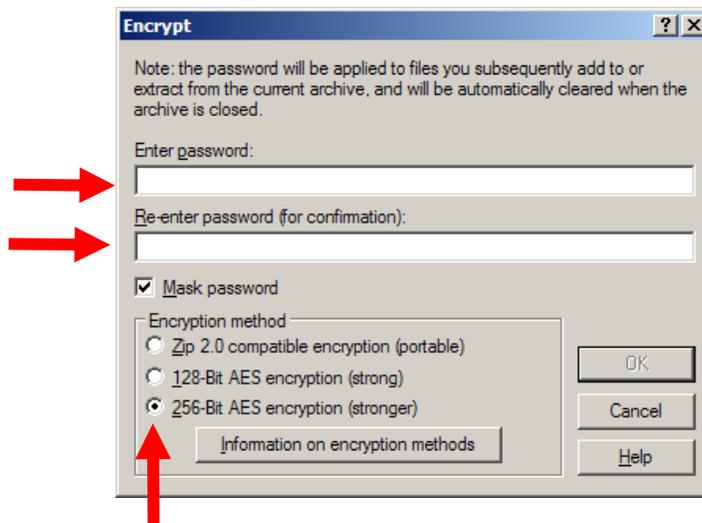
- o Choose the **Encrypt added files** under Options



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



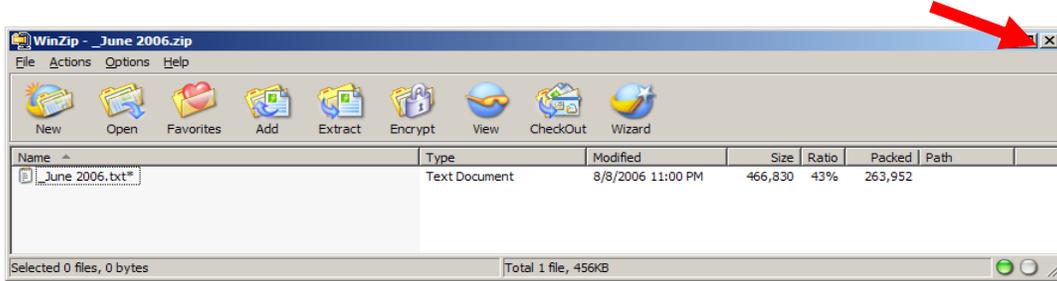
- Create a password when the Encrypt dialog box opens. Passwords must:
 - be at least 9 characters in length
 - contain at least 2 numeric characters
 - contain at least 2 upper and 2 lower case alphabetic characters
 - contain at least 2 special characters (special characters are located above the numeric 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 1 to TMA memorandum “Guidelines on Protection of Sensitive Information in Electronic Mail (e-mail)”

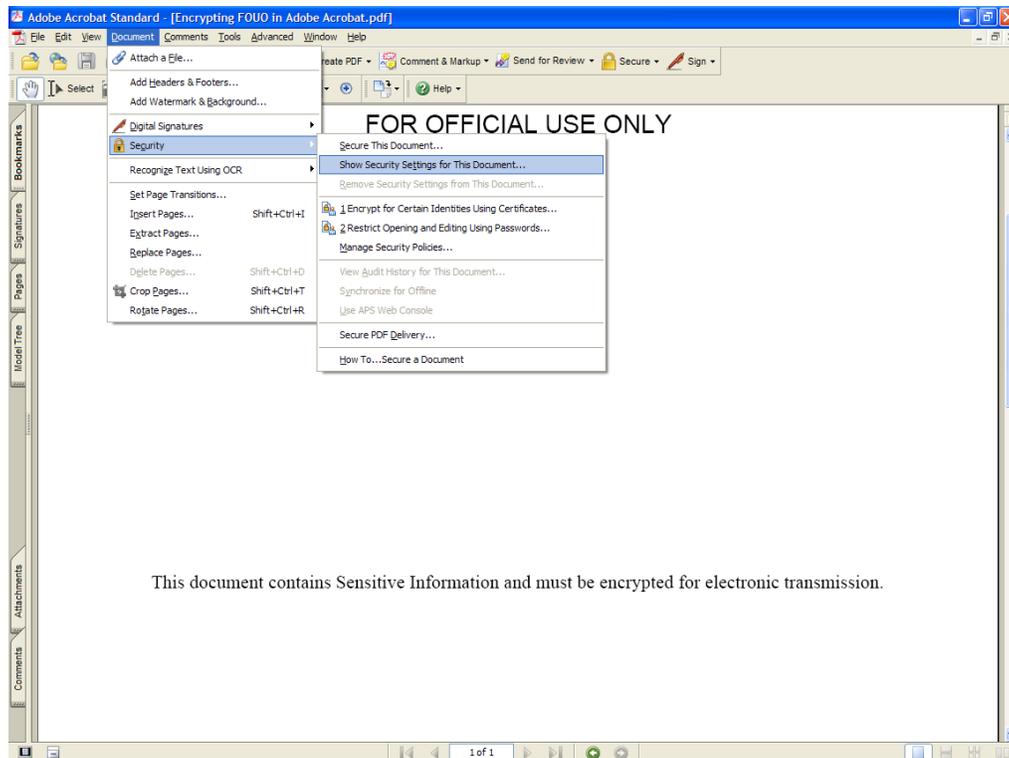
The file(s) will be added to the WinZip main screen. Exit by clicking the **X**.



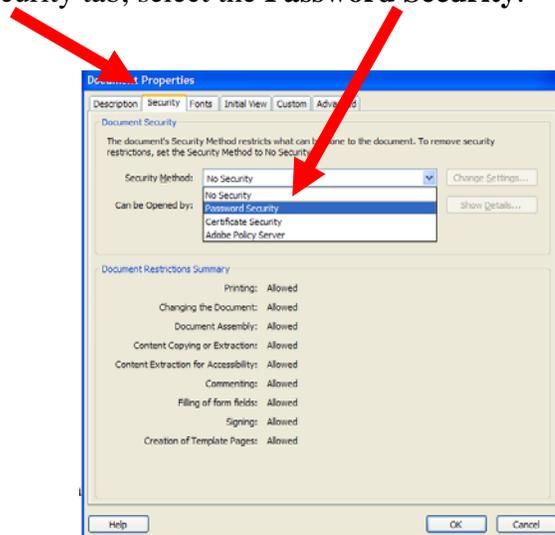
NOTE: Because many e-mail systems block files with the ‘.zip’ extension, one may need to change the file extension before attaching and sending. The recipient(s) will then be required to change the file BACK to a ‘.zip’ file to open. To do this, browse to the location of the file, Right click on the 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.

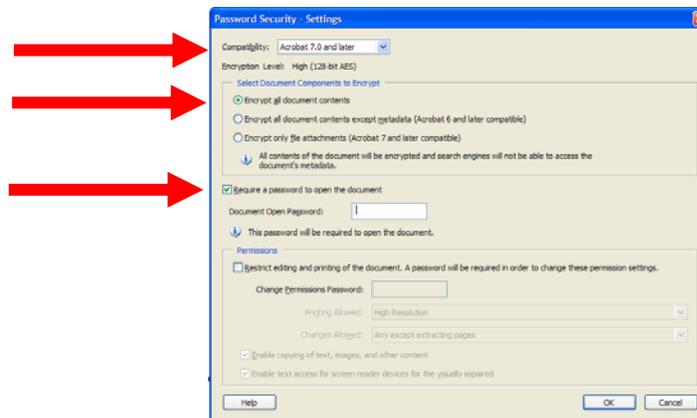
- Open the Adobe .pdf file. Click on **Document/Security/Show Security Settings for This Document...**



- 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**.

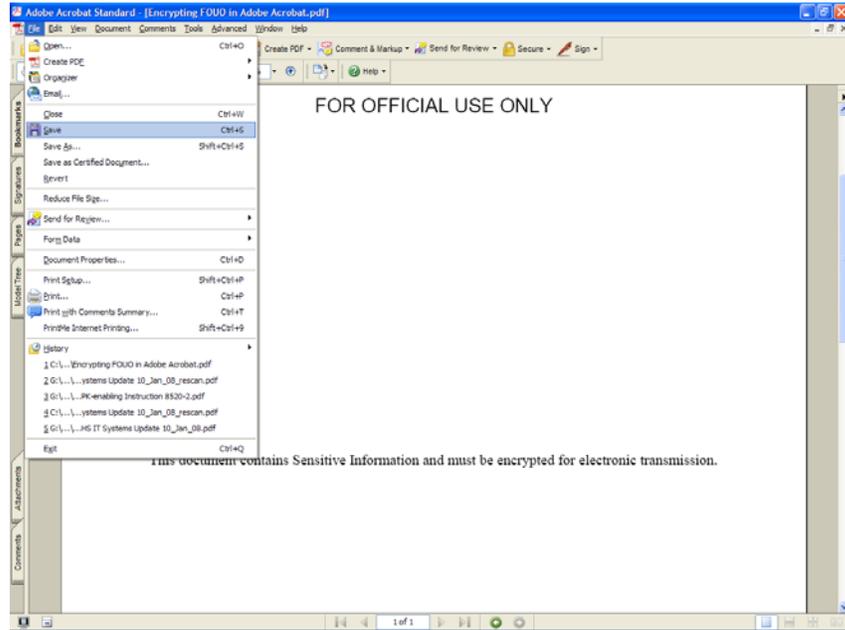


- Type in a password beside **Document Open Password**: Passwords must:
 - be at least 9 characters in length
 - contain at least 2 numeric characters
 - contain at least 2 upper and 2 lower case alphabetic characters
 - contain at least 2 special characters (special characters are located above the 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**.

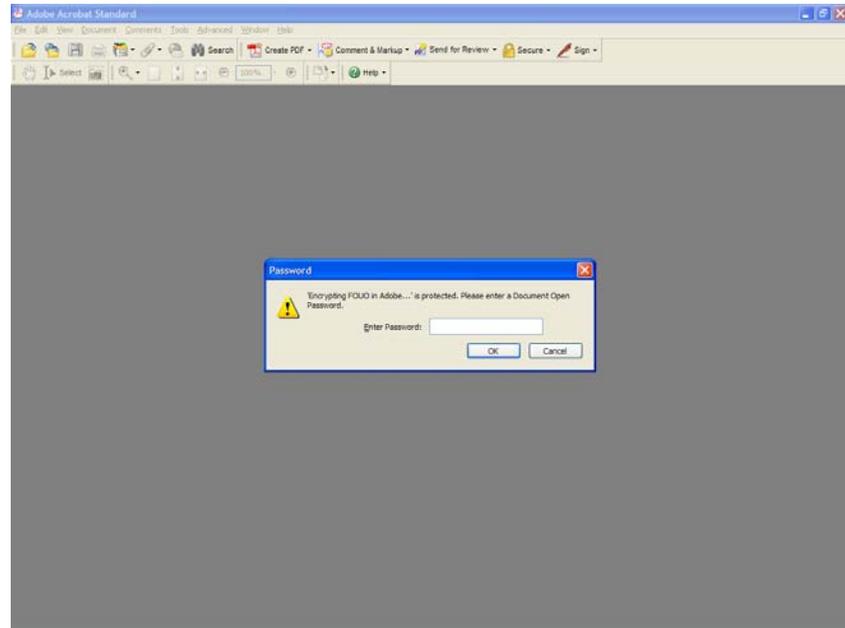


Attachment 1 to TMA memorandum “Guidelines on Protection of Sensitive Information in Electronic Mail (e-mail)”

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



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



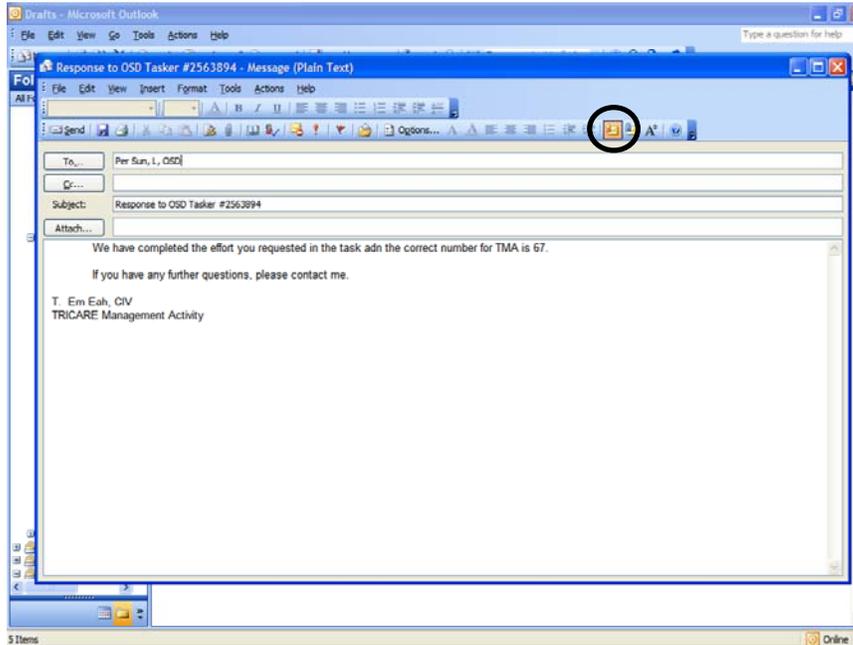


HEALTH AFFAIRS

Outlook Digital Signature



TRICARE
Management
Activity



Click on the "Digitally Sign Message" button on the toolbar so it either appears orange or is outlined.

Make sure your CAC is in the reader.

Click "Send" as usual.

Enter your PIN when requested.