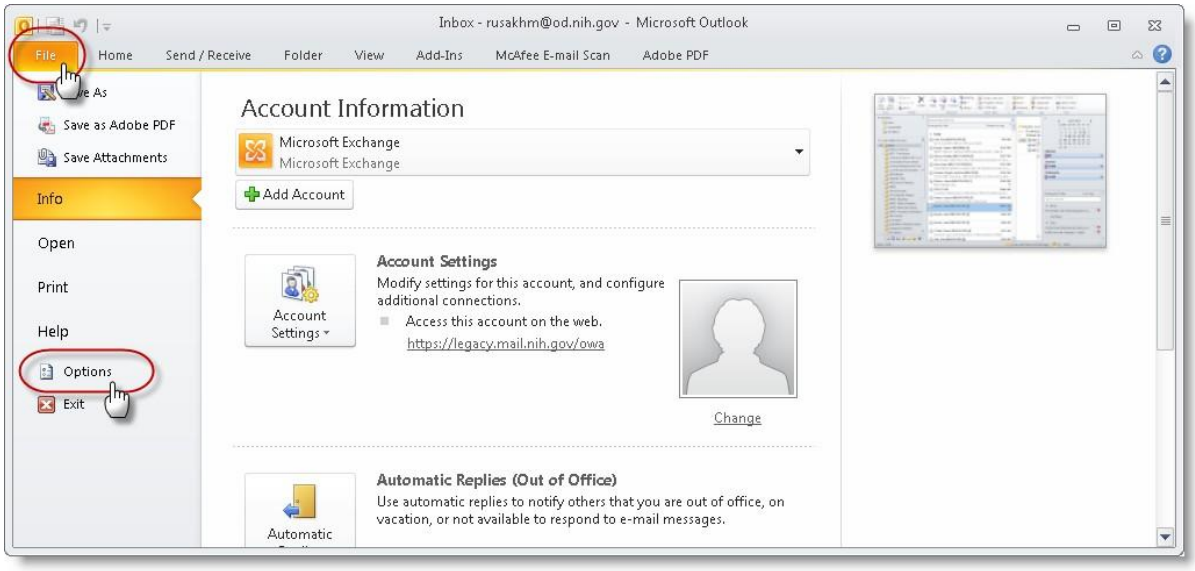
How to Publish Your Smart Card Certificates Using Outlook 2010

To send or receive (and read) digitally signed or encrypted email messages with colleagues at NIH, you must first publish your PIV certificate (a part of PKI, or Public Key Infrastructure) to the Global Address List (GAL). Certificates are stored on your PIV smart card's chip. Digitally signing your email tells your recipient that a message is verifiably from you. Encrypting your email ensures that only the intended recipient can read your message. Publishing your certificate to the GAL allows the recipient's Outlook to verify the digital signature, or allows the recipient to read email you have encrypted, and vice versa.

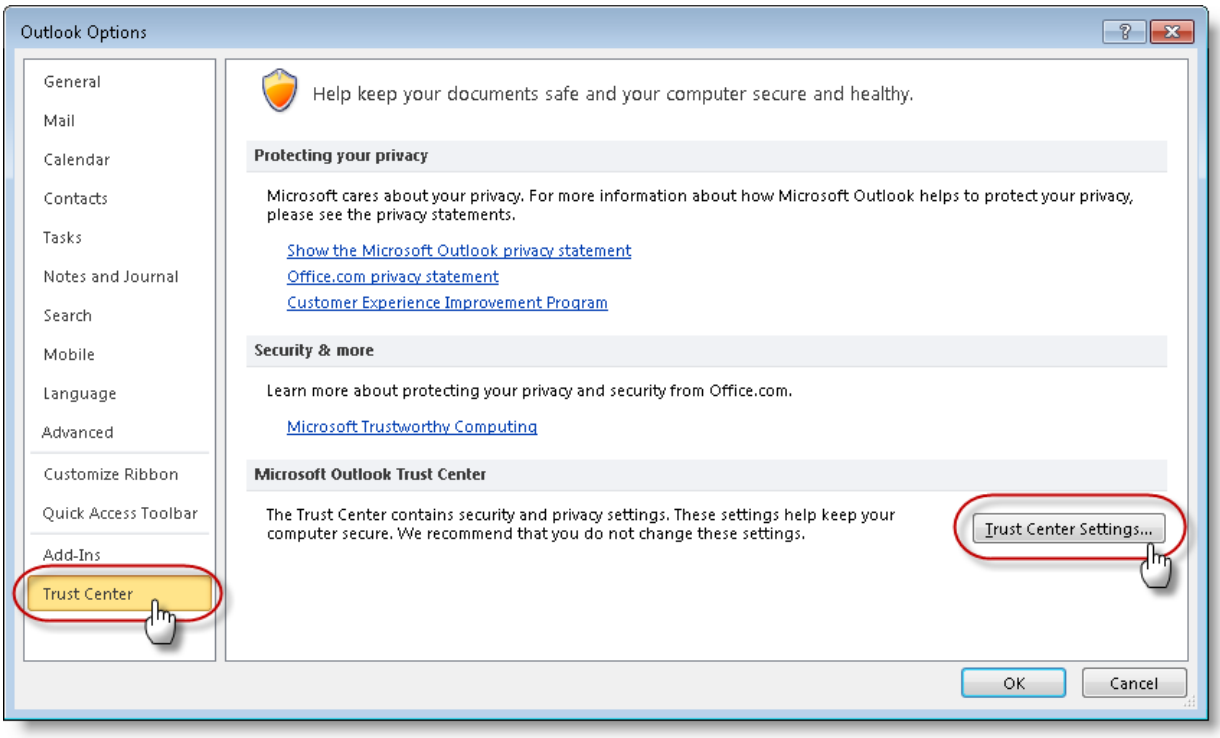
If you send sensitive or personally identifiable information (PII), you *must* encrypt your email.

You only need to publish your valid certificate once (or when you renew a certificate). You will use your NIH PIV smart card and PIN to do this.

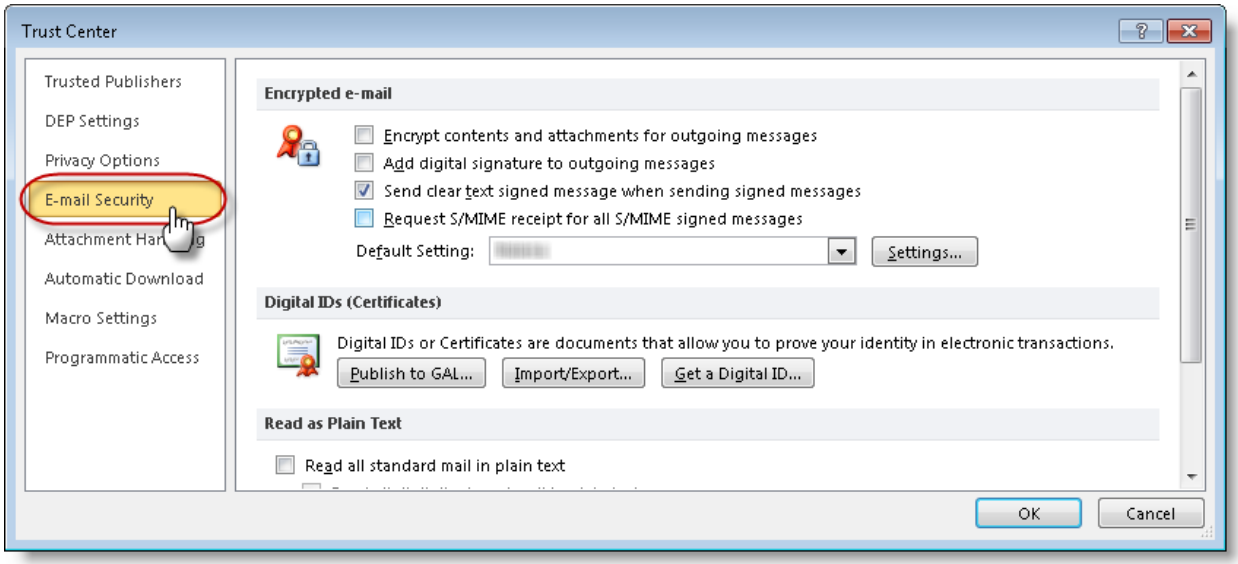
1. Log in to your NIH computer using your PIV smart card and PIN, and open Microsoft Outlook.
2. With the PIV smart card inserted in your computer's card reader, go to the **File** tab and select **Options** from the left pane.



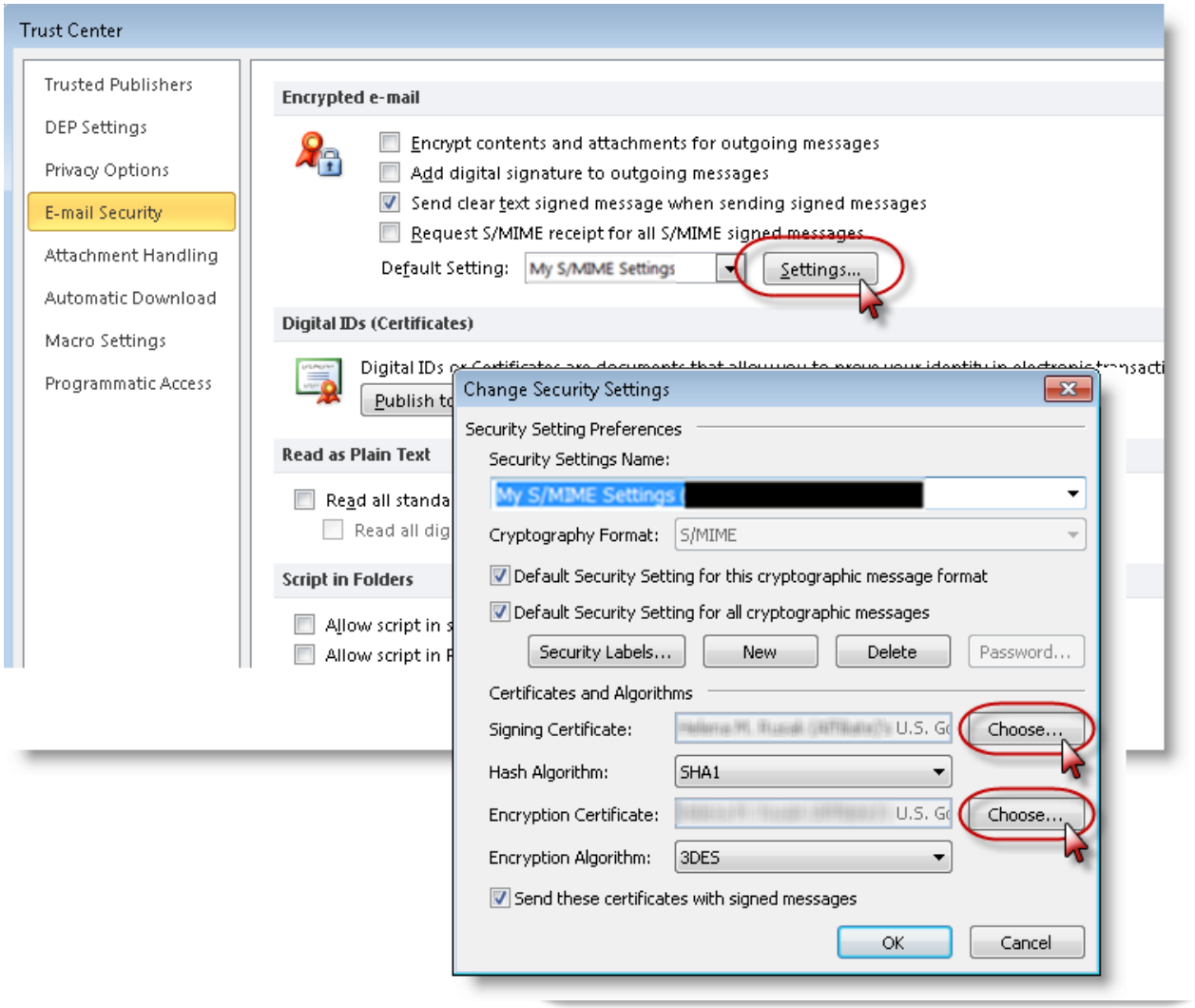
3. From the Outlook Options dialog box, select **Trust Center** from the left pane, then click the **Trust Center Settings** button from the right pane.



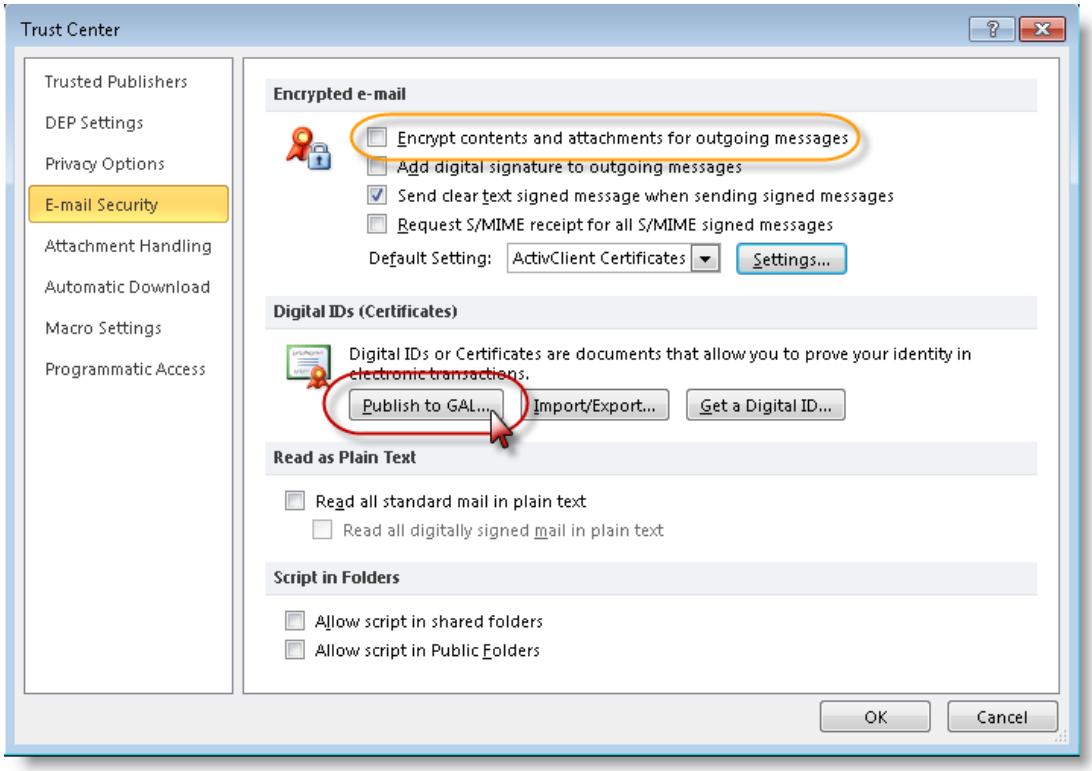
4. From the Trust Center dialog box, select **E-mail Security** from the left pane.



5. In the right pane under *Encrypted E-mail*, click the **Settings** button, and then click each one of the **Choose** buttons next to both the Signing Certificate and Encryption Certificate options. When prompted, select your current and valid certificate. When ready, click **OK**. This will ensure your certificates are properly loaded and ready for publishing.



6. Click the **Publish to GAL** button under the *Digital IDs (Certificates)* section to publish your certificates to the global address list. If you want to encrypt all outgoing email messages by default, first click the option to *Encrypt contents and attachments for outgoing messages***.** When you click the **Publish to GAL** button, follow the prompts to affirm.



7. Click **OK** to close the *Trust Center* dialog box, and then **OK** again to close the *Options* dialog box.

The Air Force Public Key Infrastructure System Program Office (AF PKI SPO) is tasked with implementing DoD PKI within the AF community. Our mission is to provide comprehensive PKI solutions to satisfy end user needs as directed by the DoD and the AF.

AF PKI SPO
(210) 925-2562/DSN 945-2562
Web site: **https://afpki.lackland.af.mil**

AF PKI Help Desk
(210) 925-2521/DSN 945-2521
E-mail: **afpki.helpdesk@us.af.mil**

The AF PKI SPO is the Public Key Infrastructure Section of the Information Assurance Branch, Cryptologic Systems Division, C3I & Networks Directorate, Wright-Patterson AFB, OH.

DISTRIBUTION C: Distribution authorized to U.S. Government agencies and their contractors; administrative/operational use; 3 January 2013. Other requests for this document shall be referred to AFLCMC/HNCDP, (210) 925-2521, DSN 945-2521, (e-mail: afpki.helpdesk@us.af.mil).

HANDLING AND DESTRUCTION NOTICE: Handle in compliance with distribution statement and destroy by any method that will prevent disclosure of contents or reconstruction of the document.

(As of : 3 January 2013)

AIR FORCE
PUBLIC KEY INFRASTRUCTURE
SYSTEM PROGRAM OFFICE

AUTOMATED KEY RECOVERY
E-MAIL ENCRYPTION CERTIFICATE/KEY

DELIVERING CYBER DEFENSE AND INFORMATION ASSURANCE SOLUTIONS TO THE AIR FORCE

Key Recovery

Background Information

Encrypted e-mail can only be opened with your private encryption key. When your CAC is replaced, previously encrypted e-mail messages are not accessible with the new CAC because it contains a new private e-mail encryption key. To enable access to e-mail encrypted and accessed with the previous CAC's encryption key, you need to recover the e-mail encryption key that was associated with the previous CAC.

The Defense Information Systems Agency (DISA) escrows your encryption keys for data recovery purposes.

Key Recovery is a process that allows you to recover your current or previous encryption certificate/key, providing continued access to existing encrypted e-mail.

You should try to recover your current encryption certificate/key PRIOR to obtaining a new CAC. If there is a change of affiliation affecting the first Organizational Unit (OU) of your Distinguished Name, automated recovery is not possible, due to configurations at the Automated Recovery Agent, and you will need to use the Manual Key Recovery process.

Procedures to Recover a Previous E-mail Encryption Key

1. Type one of the following URLs into the Web browser's address bar; then press **Enter**. (The URLs are case sensitive) **https://ara-3.csd.disa.mil/ara/Key or https://ara-4.csd.disa.mil/ara/Key**
2. At the Web site, you will be prompted to select your **Identity certificate** (the one that does not reflect e-mail in its description/title). Highlight it and click **OK**. **Note**: *If you selected your e-mail certificate, close and reopen the browser; then type the URL again.*
3. If prompted, enter your CAC PIN; then click **OK.**
4. Read the US Department of Defense Warning screen, and then click **OK.**
5. You will receive notice that the Web site is gathering a list of escrowed keys pertaining to you. It may take a few seconds for the list to appear.

Note: *If a listing of certificates appears, proceed to Step 6. If a listing of certificates does not appear, or there is no recover button, then request MANUAL Recovery. For manual recovery, type the following Web page URL into the browser's address bar. Once you arrive at the Key Recovery Web page, go to the Manual Key Recovery Process section and follow the instructions.*

https://afpki.lackland.af.mil/html/keyrecovery.cfm

Never leave your CAC unattended in your card reader.

6. Review the list of keys to find the serial number and dates that match the timeframe of the key to be recovered. Click the **Recover** button next to that key.

Note: *After clicking Recover, you may receive the following error: **The Automated Key Recovery Agent was unable to recover the requested key.** Please try again in one hour to see if the problem was corrected. If you try later and get the same result, then process a Manual Key Recovery Request (see Step 5) to recover the old encryption key.*

7. Click **OK** when prompted to acknowledge the … *DoD subscriber for this escrowed key*…

8. A Web page displays a 16-character password. Copy (handwrite) the password exactly as shown. Once copied, click on the **Download** link.

9. You will be prompted to choose **Save** or **Open;** click **Open. Save** may be chosen for transfer to an additional computer or for personal archive. The key may be imported later to the browser by double clicking on the file. The following steps will be the same after double clicking the file.

Note: *If you choose the Save option, the file must not be saved to an online file storage system; it can only be saved to an approved removable storage media, such as a CD.*

10. At the *Certificate Import Wizard* window, click **Next**.

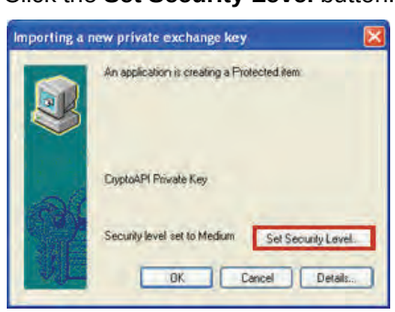
11. The next prompt indicates the *File to Import*; click **Next**.

12. Enter the 16-character password copied earlier, and then click the box for the first option: **Enable strong private key protection**, ***uncheck*** the **Mark this key as exportable** box; then click **Next**.

13. At the next prompt (Certificate Import Wizard), select **Automatically select the certificate store**, and then click **Next**.

14. On the **Completing the Certificate Import Wizard** screen, click **Finish**.

15. Click the **Set Security Level** button.



16. Select the **High** security level; then click **Next**.

17. At the next prompt, create a password to use with the recovered key. A PIN may be used here. The password or PIN must meet Operating System requirements with the required number of characters (Vista requires 16 characters). Enter it twice and click **Finish.** At the next prompt, click **OK.**

18. At the **Completing the Certificate Import Wizard** window, click **Finish**.

19. A window stating the import was successful will display; click **OK**.

20. The key is now installed and ready for use. Outlook automatically selects this key when opening any e-mail previously encrypted with that key.

Note: *An e-mail with the subject **ALERT! Key Recovery Attempt Using Automated Key Recovery Agent** will be sent to the original owner of the key. If you ever get this message and you did not initiate the action, immediately report the event via a signed e-mail to afpki.ra@us.af.mil.*

Verify the Recovered Key is in the Certificate Store

To verify the key is in the certificate store, open **Internet Explorer.**

1. Click **Tools**, then select **Internet Options** from the dropdown menu.
2. Click on the **Content** tab.
3. Click on the **Certificates** button.
4. Under the *Friendly Name* column on the *Personal* tab, the certificate with a **CN** and Last Name is the recovered key.