Microsoft Windows Encrypting File System (EFS) Certificate Migration from XP to VISTA (also works with Windows 7)

Instruction Guide

Army Information Assurance
CAC/PKI Division
2530 Crystal Drive
Arlington, VA 22202

July 2009

Revision History

Version Number	Preview Release	Section	Date

Table of Contents

Introduction

Microsoft Windows Encrypting File System (EFS) is a file system encryption process that allows users to encrypt and decrypt files or folders on their workstation. Windows XP EFS uses a Microsoft self-signing encryption certificate to encrypt the files or folders on the user's workstation. Windows VISTA can be configured to use either Microsoft's self-signed certificates or public key certificates. When upgrading from Windows XP to Windows Vista, the encryption certificate must be saved so that any encrypted data can be decrypted after the migration process is completed. This instruction guide outlines the procedures that must be followed to ensure a successful migration from Windows XP to Windows Vista. When a user attempts to encrypt or decrypt data, EFS looks in the user's personal certificate store for an EFS certificate.

Purpose

This document provides end-user and administrator guidance on the migration process of exporting user's Windows XP EFS certificates into a Windows VISTA configuration. This instruction guide outlines the procedures that must be followed to ensure a successful migration of your EFS Certificates from Windows XP to VISTA.

Requirements

For the purposes of EFS Certificate Migration, the following prerequisites apply –

- **User Type(s):** The end-user and an administrator (with administrator rights) must be available.
- **System Requirements:**
    a. One computer configured with Windows XP OS with the end-user's current public/EFS certificates.
    b. One computer configured with Windows Vista OS.
- **Network or Accessible Storage Media:** A location for the use of exporting and importing user data that can be accessed by both the XP and Vista systems.

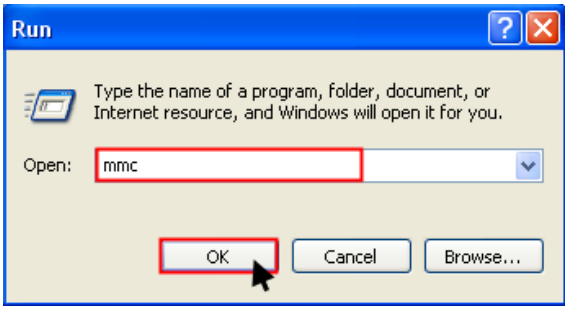
Exporting EFS Certificates from MS Windows XP (End-User)

To save the EFS certificate, it is necessary to export the EFS certificates from Windows XP and save it to a network drive or accessible storage media. The following procedures must be followed:

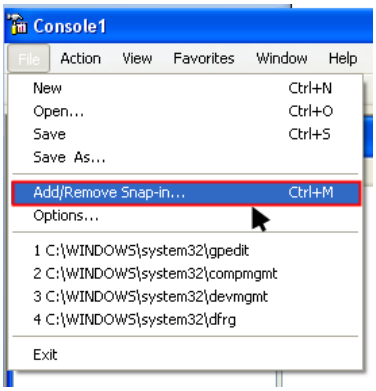
1. **End-user: Logon** to your assigned desktop/laptop (Windows XP)

2. From the desktop, click the **start** button, then click **Run**

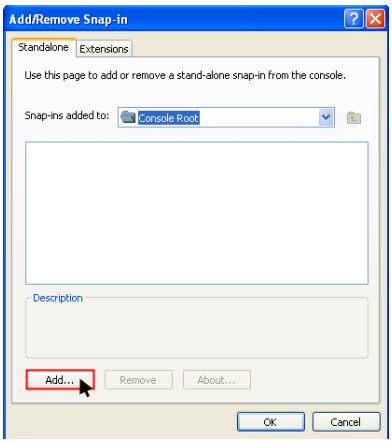
3. In the dialog box, Type **mmc** and click **OK**



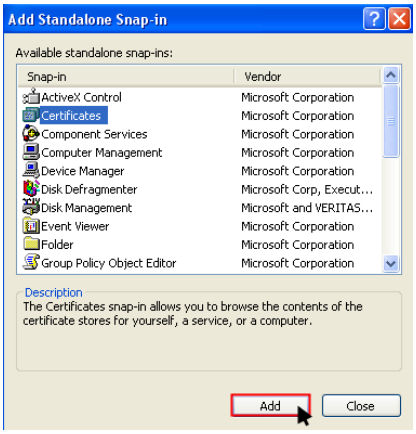
4. From the Main Menu, click **File**, then click **Add/Remove Snap-in**



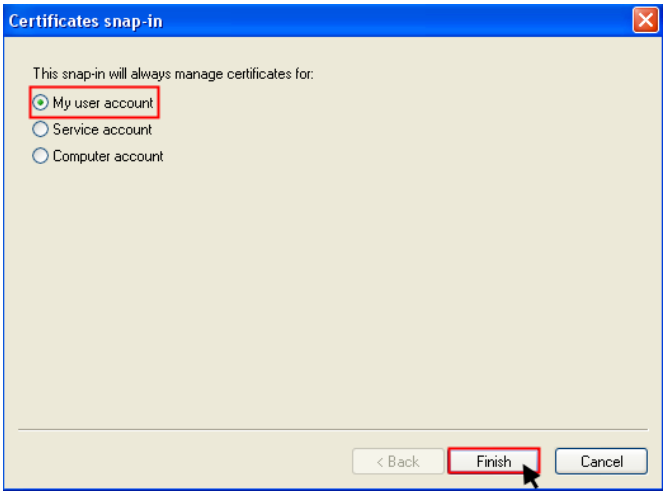
5. In the Add/Remove Snap-in dialog box, click **Add**



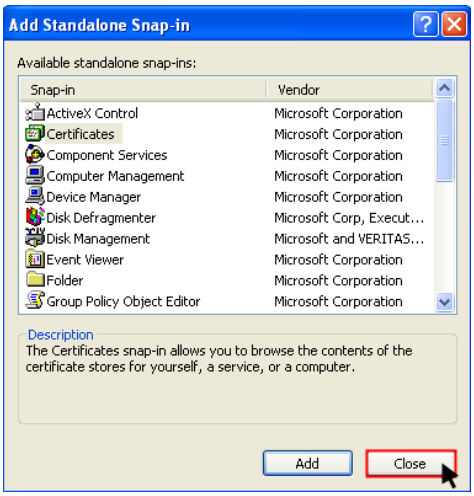
6. Select **Certificates**, then click **Add**



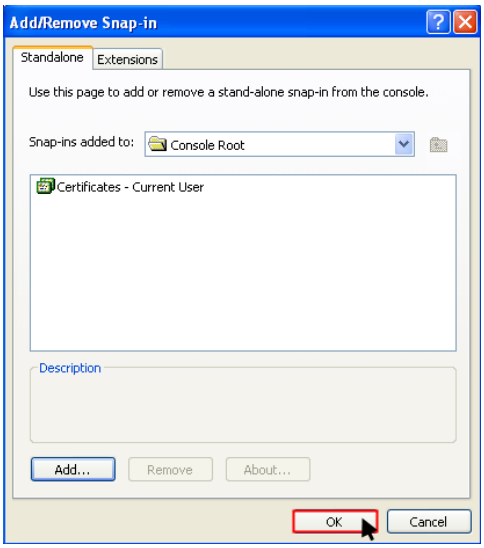
7. Underneath “This snap-in will always manage certificates for:” select **My user account** and select **Finish.**



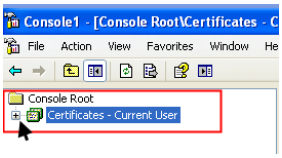
8. From the Add/Remove Snap-In box, click **Close**



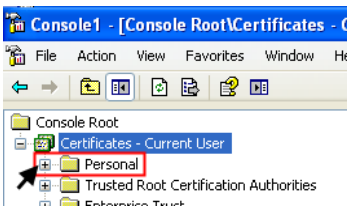
9. From the Add/Remove Snap-In box, Click **OK**



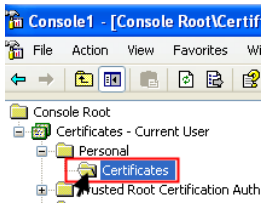
10. Browse to the Personal\Certificates folder --
    a. Click the **plus sign** ⊞ next to “Certificates – Current User”



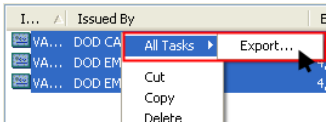
b. Click the **plus sign** next to the “Personal” folder



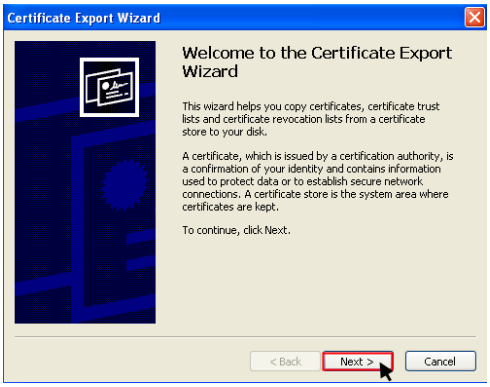
c. Click the **Certificates f**older



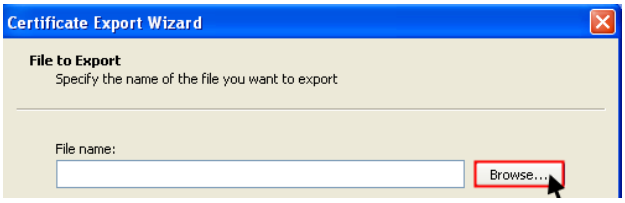
11. Export the certificate(s) --
    a. **Right-click** on the ***certificate(s)*** for migration.
    b. Click **All Tasks** and then click **Export.**



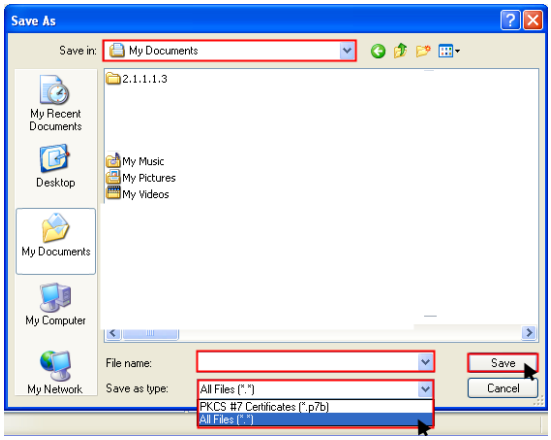
12. At the Certificate Export Wizard Welcome screen, click **Next**



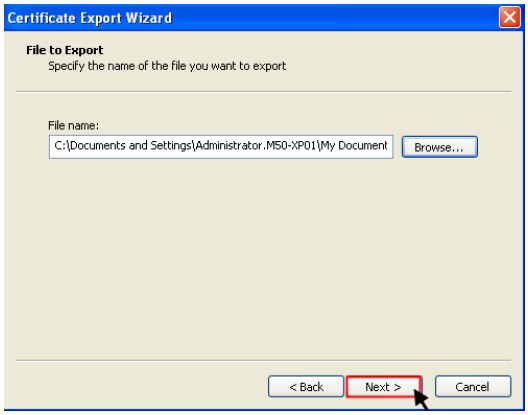
13. At the File to Export screen, click the **Browse** button



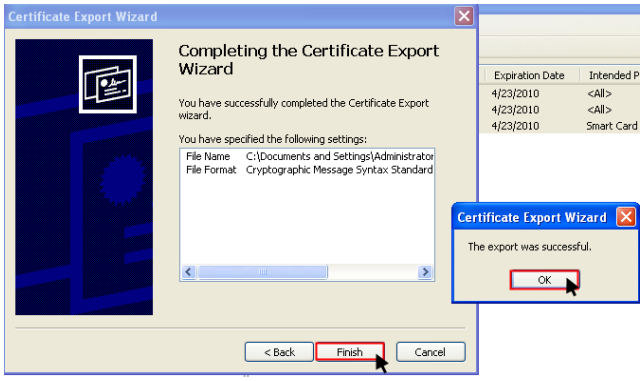
14. In the Save As dialogue box, **choose a file location** (e.g. a network drive or other accessible location or media), give the certificates a **File name** (e.g. MyPersonalCertificates1) and ensure file type is either ***.p12/*.pfx** or **All Files *.***Click **Save.**



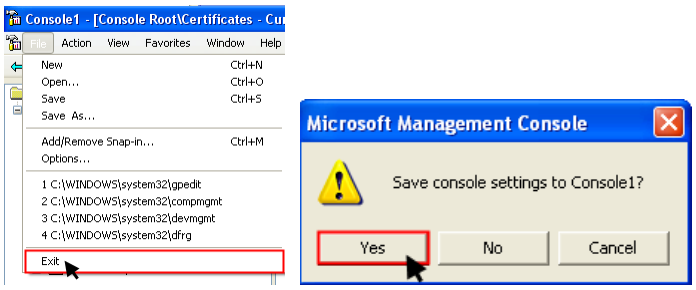
15. In the File to Export dialogue box, click **Next**



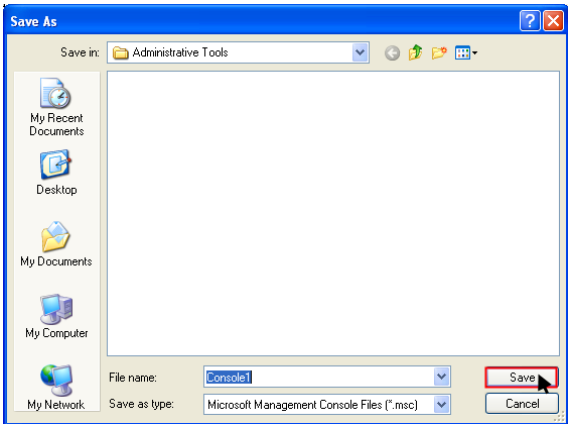
16. At the Completing Certificate Export dialogue box, click **Finish** and then click **OK**



17. Exit Console1, by clicking **File** and **Exit**, from the console's main menu, then click **Yes** to save



18. At the Save As dialogue box, click **Save**

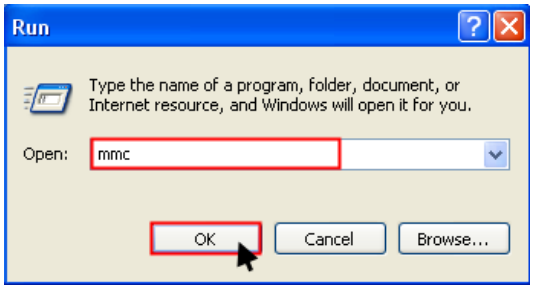


19. **End-user: Logoff** the desktop/laptop

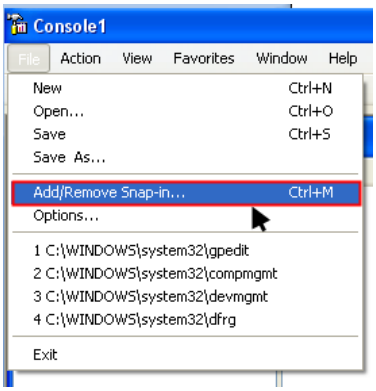
Importing EFS Certificates into Windows Vista (End-User)

1. **End-user: Logon** to your assigned, destination desktop/laptop
2. From the desktop, click the **start** button, then click **Run**

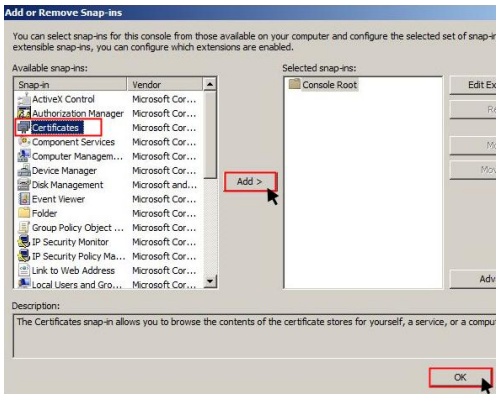
3. In the dialog box, **Type** mmc and click **OK**



4. From the Main Menu, click **File**, then click **Add/Remove Snap-in**



5. In the Add/Remove Snap-in dialog box, under the Available snap-ins column, click **Certificates,** then click **Add,** and then click **OK**



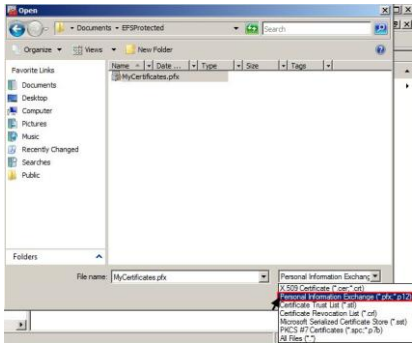
6. Importing the certificate(s) –

   a. In the Console1 dialogue window, click the ⊞ next to ***Certificates – Current User*** to expand the folder list
   b. Right-Click on the **Personal** folder
   c. Select **All Tasks** and then select **Import**

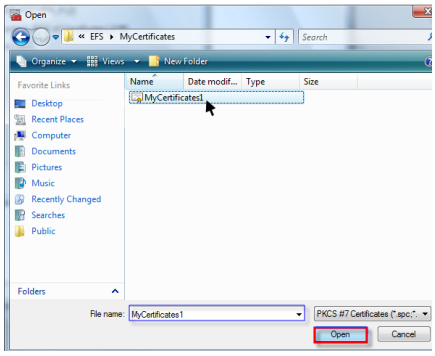
7. At the Certificate Import Wizard dialogue box, click Next

8. Locate your certificates for importing –
   a. Click the **Browse** button

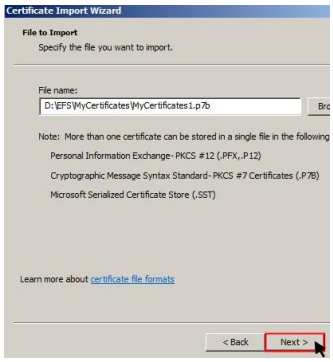
   b. Locate your file folder location, by clicking the down arrow and opening the folder or drive of your exported certificate from Windows XP, (*See:* Step 1.13).
   c. Change the file type to **PKCS #12 Certificates (*.p12/*.pfx) OR All Files *.* Note: Your *MyCertificates1* file should be available.**



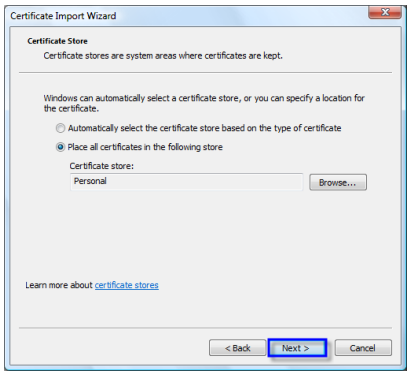
9. From the Open dialogue box, double-click your ***Certificates*** file and click the **Open** button



10. Click **Next**



11. Click **Next**



12. Click **Finish**

13. Exit Console1, by clicking **File** and **Exit**, from the console's main menu, then click **Yes** to save

14. At the Save As dialogue box, click **Save**

[END OF INSTRUCTIONS]

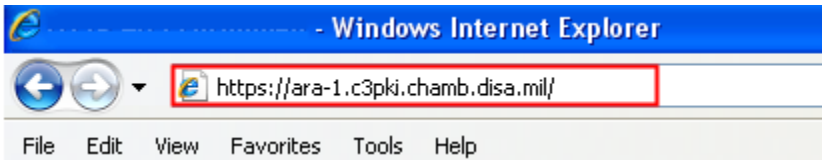
CAC Certificate Replacement Procedures for VISTA Encrypting File System (EFS)

Recovering your old Encryption Certificate:

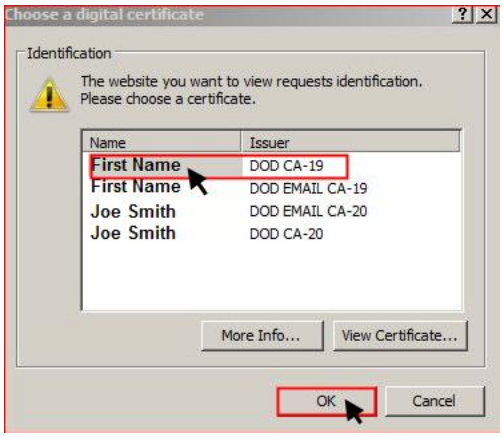
1. Insert your CAC into your CAC Reader and from the Window's desktop, double-click the **Internet Explorer** icon to open the browser.

2. User must recover and install his encryption key or certificate from their previous CAC (.p12 file) from the DISA Automated Key Recovery website. Go to the following URL: **https://ara-1.c3pki.chamb.disa.mil/**

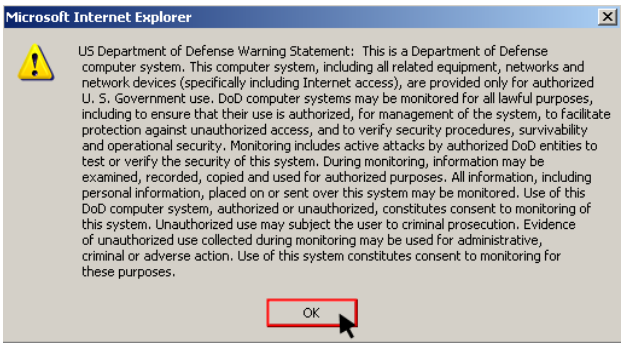
Note: If user is having application issues with IE the user may need to download the .p12 file using another computer and transfer the file to their computer.



3. This will prompt you to choose a digital certificate. Select your **ID Certificate** (won't have EMAIL listed under Issuer) and select **OK.**

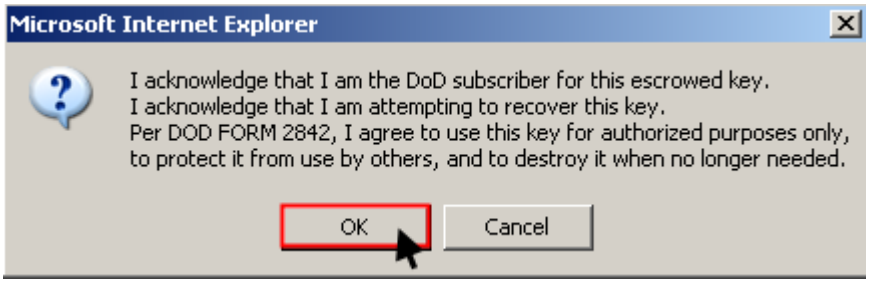


4. You will see the DoD Warning. Select **OK** to continue.



5. The site will come up and show you the keys available for download. You will need to select the key from your previous CAC. Once identified, select **Recover**

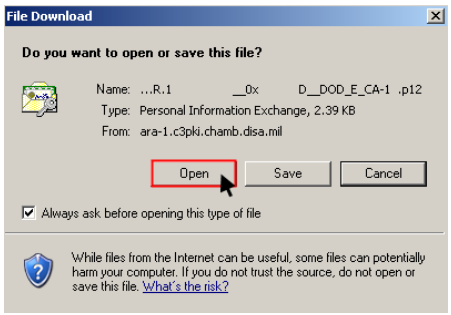
6. You will be prompted with a DoD prompt. Read the conditions carefully and select **OK.**



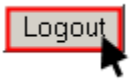
7. Please wait while Auto Key Recovery takes place. This can take up to 2 minutes.

8. Once completed, you will get a message saying "**The Automated Key Recovery Agent has recovered your key. To retrieve your key, select the following link**". Select **DOWNLOAD** to download the .p12 file from your previous certificate. You will also receive a one-time password that you will need to use to restore your encryption key or certificate to your system- take note of that password.

9. **Open** the .p12 file and allow it to install.



10. Select **Logout**

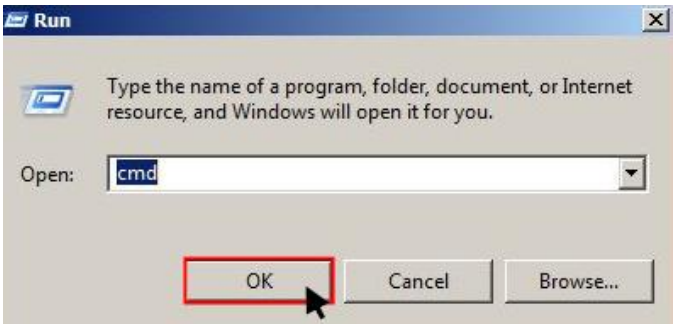


Once this key is recovered and installed on your system you will be able to view those previously encrypted files and have no problems with applications because you are viewing them with the certificate from your previous CAC.

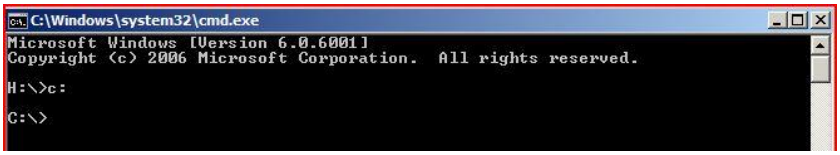
Update Existing Files with New Encryption Certificate:

Perform an update to all your files with your new certificate or encryption key that from your replacement CAC. This is done through use of the executable called rekeywiz.exe. The steps are as follows;

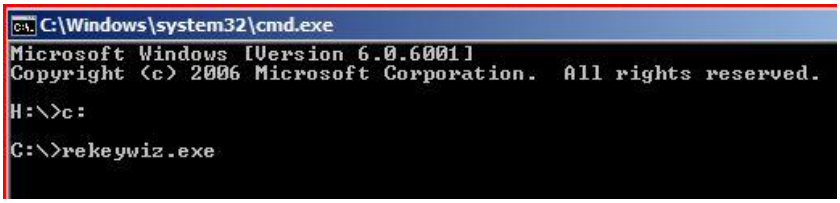
1. Close any open files or applications. Got to command prompt by selecting **Start → Run**, type in CMD, then enter the command prompt window will appear.



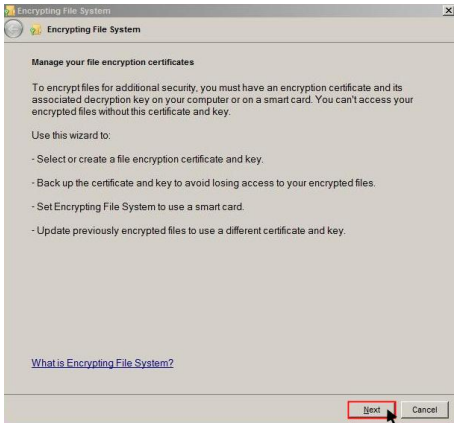
2. The command prompt will be displayed on your screen as follows. **Ensure you are at the root of your local drive i.e. C:\. To change to a different directory type the directory letter then a colon (C:). To go from a subdirectory to the root directory type cd and a back slash (CD\)**



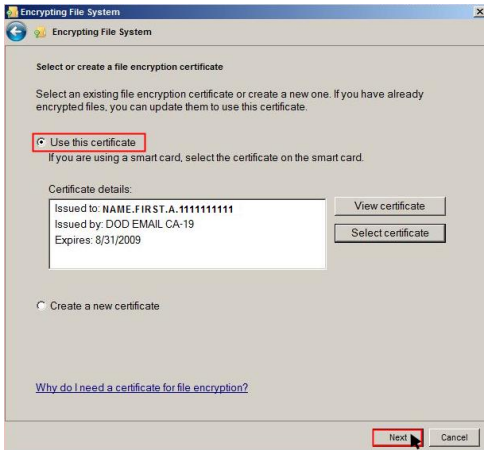
3. Type in **rekeywiz.exe** and then press **enter**.



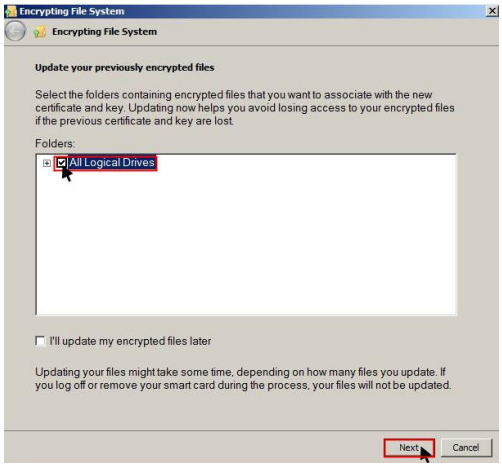
4. This will take you into the rekey wizard. Select **Next**.



5. You will be taken to another screen that ask whether you are creating a new encryption certificate or selecting an existing certificate. In this case select "**Use this certificate**" as shown. **DO NOT SELECT "CREATE A NEW CERTIFICATE."** Select **Next.**

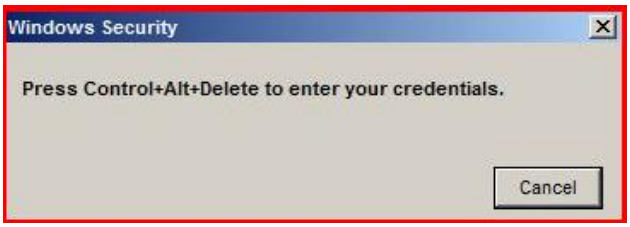


6. You will be taken to the **Update Previously Encrypted Files** Screen. Make sure "**All Logical Drives"** is checked, then select **Next**.



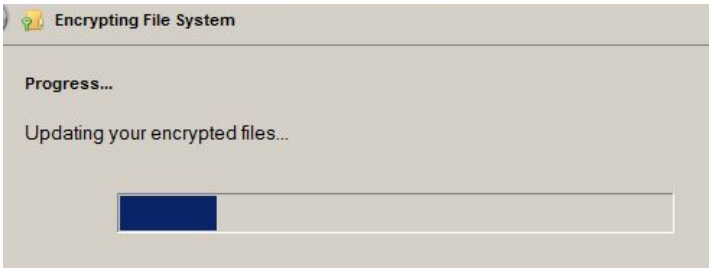
7. Select **I want to complete this action**

8. Press Control + Alt + Delete

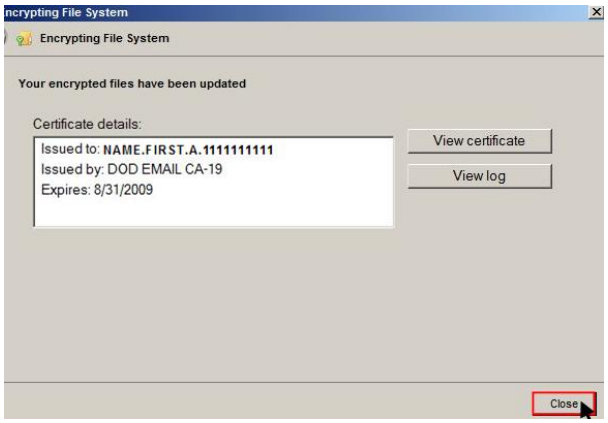


9. Enter your PIN and Select **OK.**

10. Your files are being updated. This may take a considerable amount of time depending on the number of files being updated.



11. Your files have been updated. You should now be able to view the previously encrypted files. Select **Close.**



If additional assistance is required, please contact the Army IA CAC/PKI Division Helpdesk.

COMM: (703) 602-7514
TOLL FREE: (866) 738-3222
DSN: (312) 332-7514
Email: iacacpki.helpdesk@us.army.mil