ABC

CA for EFS Key Recovery Procedures v0.99

31st December, 1999

Table of Contents

1. Introduction

1.1. Background

ABC Integration Engineering Security and Privacy has been engaged to assist in the design of a file based encryption solution for DEF users who possess laptops which might potentially contain sensitive information; see TASC0999.

The solution proposed is based upon using Microsoft Encrypting File System (EFS) technology in conjunction with a Microsoft Windows Server 2003 Enterprise Root Certification Authority (CA).

Implementing solutions which encrypt data generally imposes a requirement to ensure that should a user's private (decryption) key become unavailable due to a "genuine incident" (as opposed to being compromised) then a mechanism should be in place to mitigate this scenario. For the ABC CA for EFS solution, that mechanism is to recover the user's "lost" private key.

1.2. Objective

The object of this document is to provide an indicative step-by-step guide to the end-to-end process of recovering a user's "lost" private key.

1.3. Document Scope

The scope of this document is limited to the following:

- Recovery procedures for the legitimate restoration of a user's private EFS decryption key material

The scope of this document excludes the following:

- Handling of KRA and user private key backup material and storage thereof
- Handling of any passwords created / used during this procedure
- Secure deletion of file based key material

1.4. Pre-Requisites

The following are pre-requisites for performing recovery of key material archived at the ABC EFS CA:

- One of the user(s) associated with the CA admin role must be available during the procedure
- One of the user(s) associated with the key recovery role must be in possession of their associated key backup material on CD-ROM (and corresponding password) and available to logon and perform key recovery operations during the procedure
- A Windows XP workstation (or laptop) joined to the HMPS AD domain… this is termed the recovery workstation throughout this document
- The Key recovery agents are members of the recovery workstations local administrators group
- The Windows 2003 Admin Pack must be installed on the recovery workstation
- The Windows Server 2003 Resource Kit tools must be installed on the recovery workstation

1.5. Overview of the Recovery Process

The ownership of the overall key recovery process is the designated key recovery agent; either key recovery agent can be employed to execute this process.

Four distinct steps are entailed in the key recovery process:

1. The recovery of the user's archived EFS private key from the CA database; this is performed by the CA administrator and results in the retrieval of an encrypted blob (encrypted with the key recovery agent(s) public key(s))

2. The installation of the designated key recovery agent's private key (from a CD-ROM) backup which was taken during the CA commissioning into the certificate store on the recovery workstation

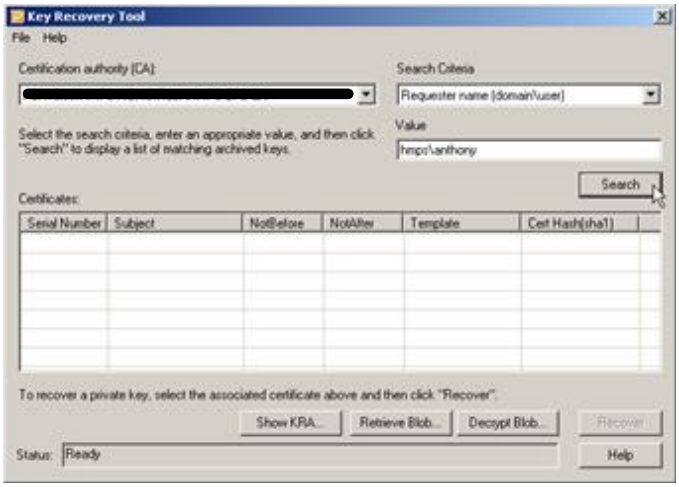
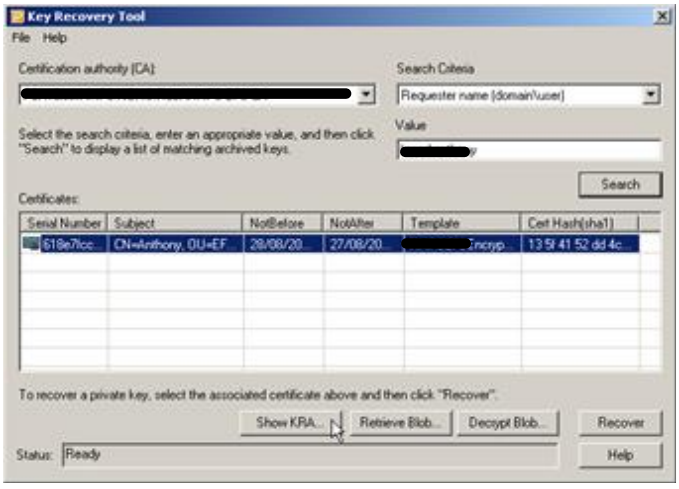
3. The decryption of the encrypted blob using the KRA decryption key, resulting in a PKCS #12 file containing the user's private key material

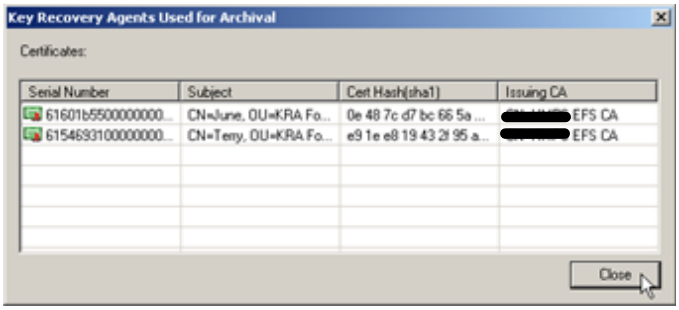
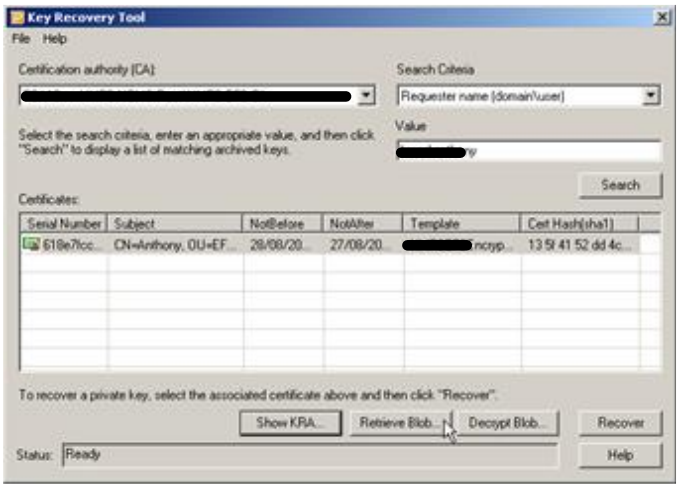
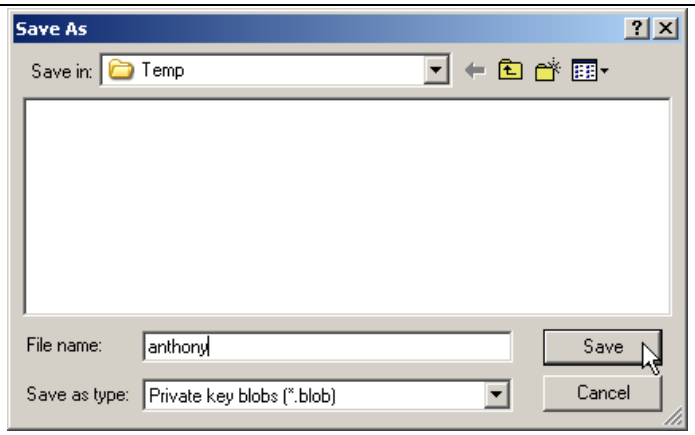
4. The installation of the PKCS #12 file containing the user's private key material into the certificate store on the user's workstation

A tabular summary of the steps involved in recovering archived key material is shown in the following table.

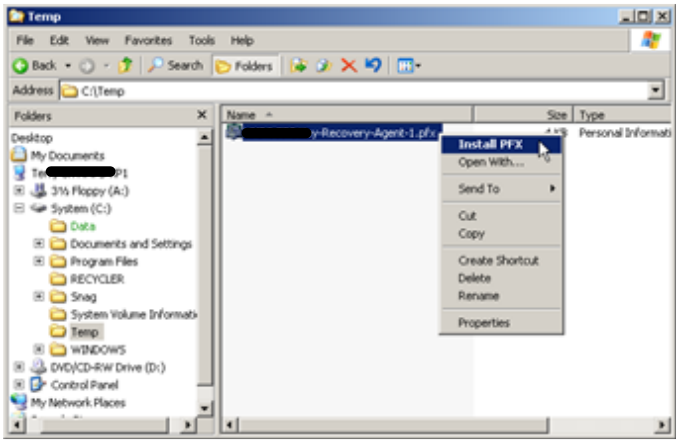
What	Who	Where
Recover the Encrypted User Private Key (BLOB) from the Certification Authority	CA Admin	Recovery Workstation
Install the Key Recovery user's Certificate and Private Key onto the Recovery Workstation	KRA	Recovery Workstation
Decrypt the Blob to Generate a PKCS #12 file Containing the User's Certificate and Private Key	KRA	Recovery Workstation
Install the Private Key by Means of Importing the Contents of the PKCS #12 file	User	User's Workstation

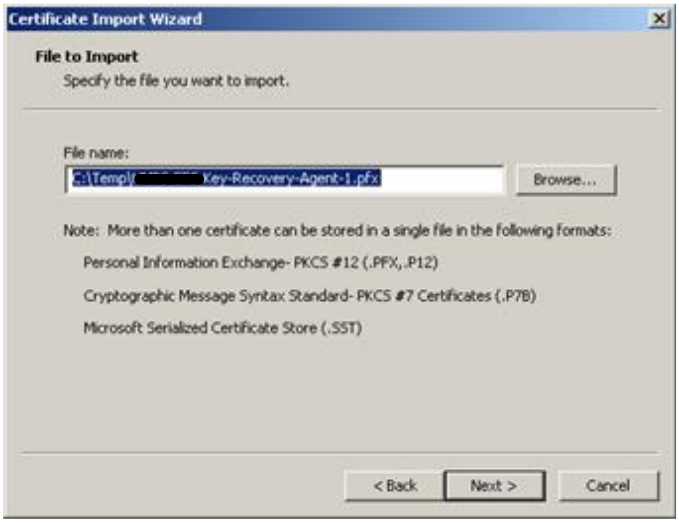
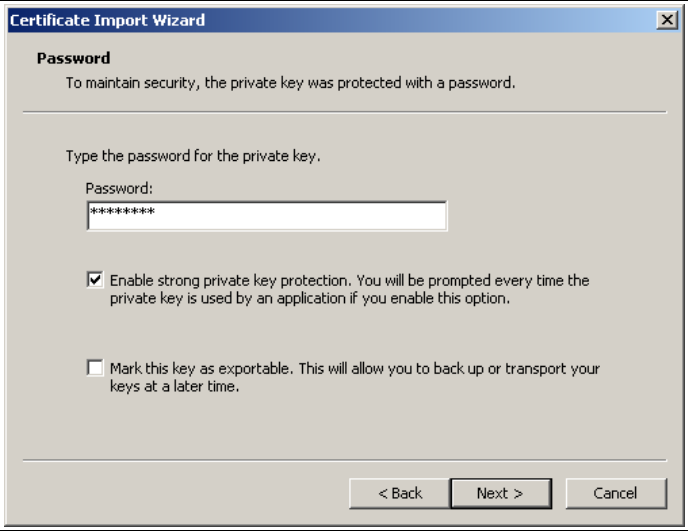
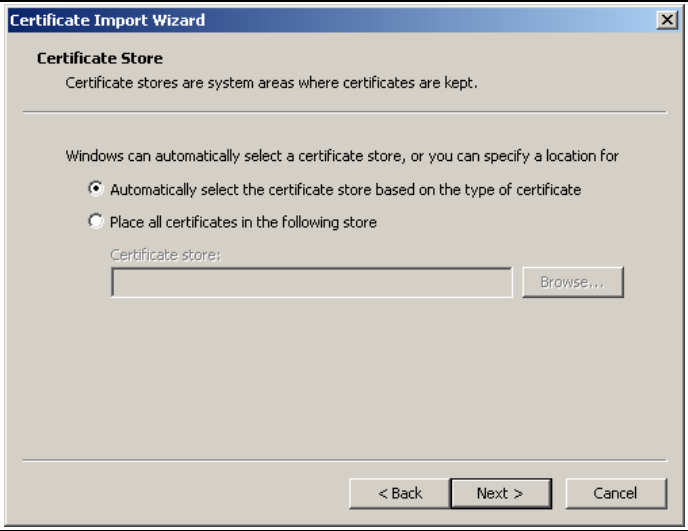
2. Retrieve Private Key (Blob) from CA Database

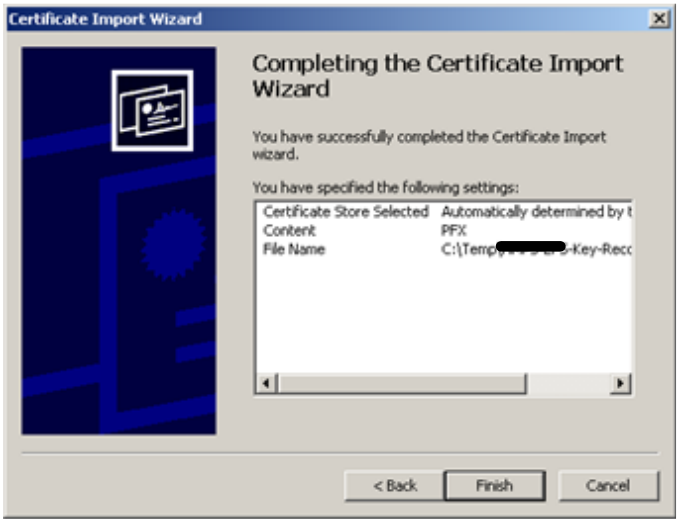
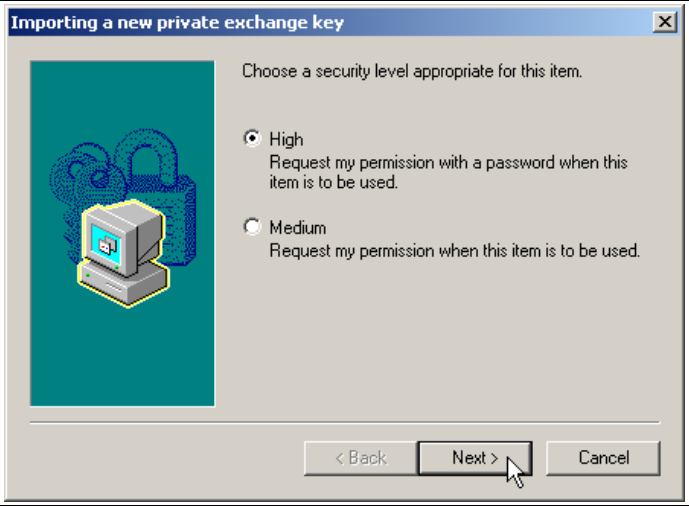
Action	Action Detail and Description
1. This task must be performed by a CA Administrator at a workstation (or server) where the Windows Server 2003 Resource Kit tools have been installed, typically this would be the Recovery Workstation The CA Administrator account must be added to the Local Administrators group on the Recovery Workstation The CA Administrator should log on at the Recovery Workstation	
2. Start the Key Recovery Tool from the Windows Server 2003 Resource Kit Command Prompt (Start/All Programs/Windows Resource Kit Tools/Command Shell) Execute `krt.exe` Retarget the Key Recovery Tool CA list box to the **ABC EFS CA** In the Search Criteria list box, select "**Requestor name (domain\user)**" In the Value field, specify the "Windows down-level" account name of the user Click the **Search** button	
3. Verify that the certificate of the user is retrieved *If there are multiple certificates for the user, it will be necessary to validate the precise serial number of the certificate to be retrieved* Click the **Show KRA** button	

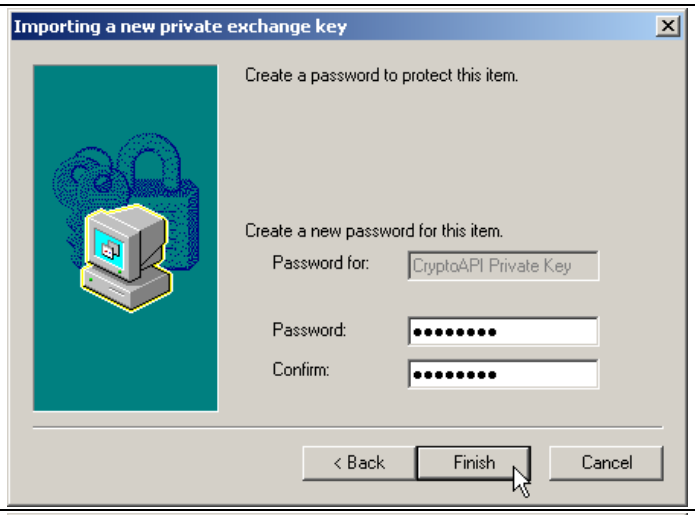
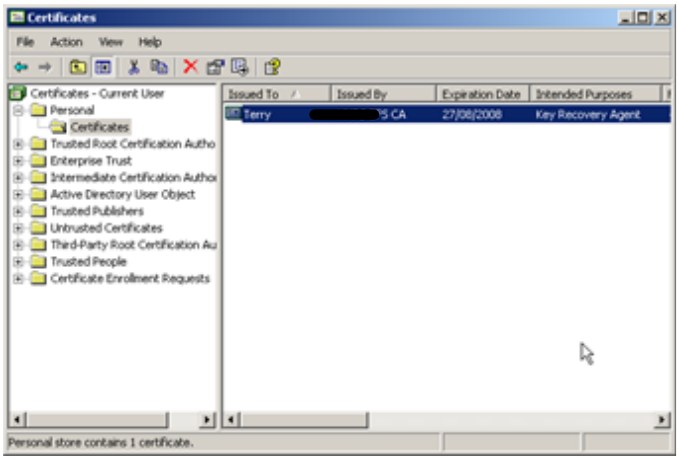
4. Verify that the private key has been archived using one of the two valid KRA certificates Click the **Close** button	
5. Click the **Retrieve Blob** button	
6. Specify a suitable location and filename in which to save the Blob, e.g. *C:\Temp\username* Click the **Save** button *Close the Key Recovery Tool* *It is assumed that the decryption of the blob will performed at the same recovery workstation, if this is not the case the Blob will need to be copied to removable media*	

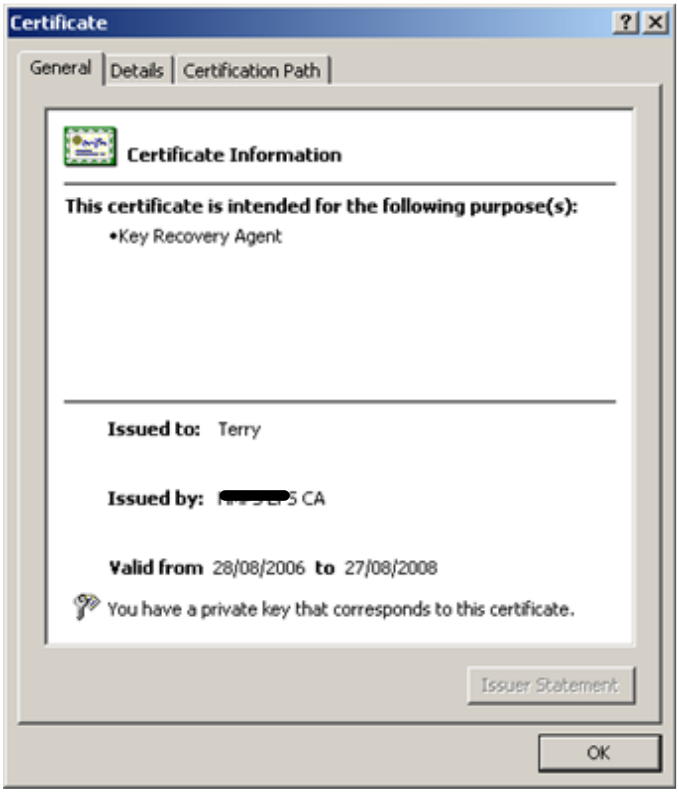
3. Install Key Recovery Certificate onto Recovery Workstation

Action	Action Detail and Description
1. One of the designated key recovery agents must log on at the Recovery Workstation to perform this sequence of tasks ***Note:*** *The Key Recovery agents need to be assigned to the local administrative group on the Key Recovery Workstation.*	
2. Insert the CD-ROM with the backed-up KRA key material Open an instance of Windows Explorer Select the KRA PKCS #12 file, then select **Install PFX** from the context menu (.pfx file) *Note: The screen capture here shows the KRA material being on the C-Drive, this will actually be the CD-ROM*	
3. Click the **Next** button	

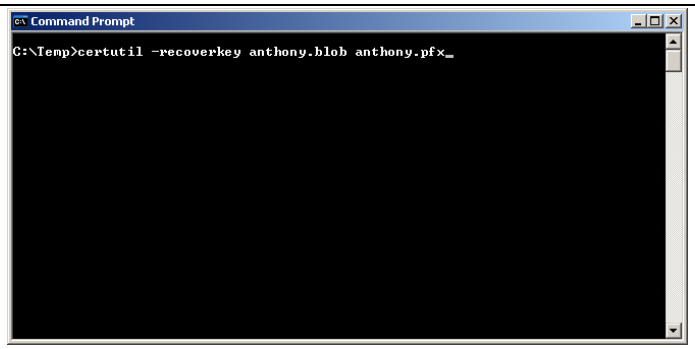
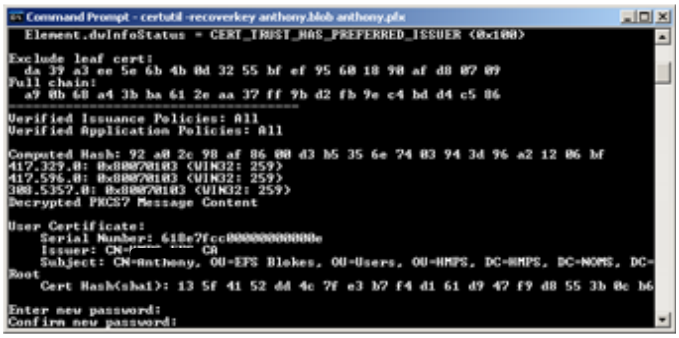
4. Click the **Next** button	
5. Enter the password associated with the backed up KRA material Enable the **Enable strong private key protection** option Click the **Next** button	
6. Click the **Next** button	

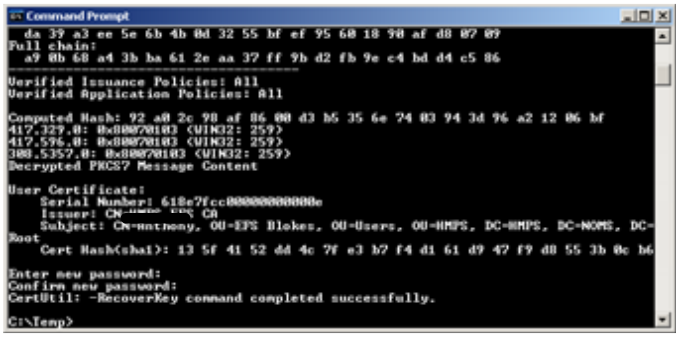
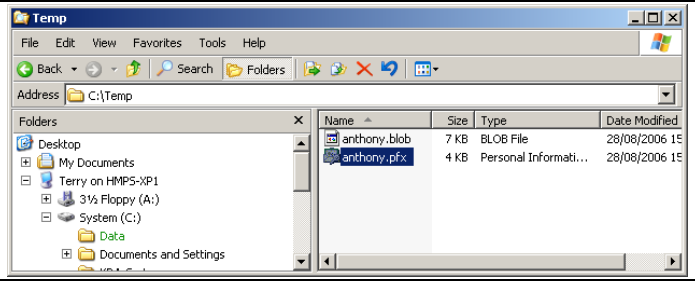
7. Click the **Finish** button	
8. Click the **Set Security Level** button	
9. Select the **High** option Click the **Next** button	

10. Re-Enter and Confirm the password associated with the KRA key material Click the **Finish** button	
11. Click the **OK** button	
12. Click the **OK** button	
13. Open an MMC focused on the **Certificates** snap-in Select the Current User - Personal - Certificates and verify that the KRA certificate has been retrieved Double click on the certificate to view the certificate details	

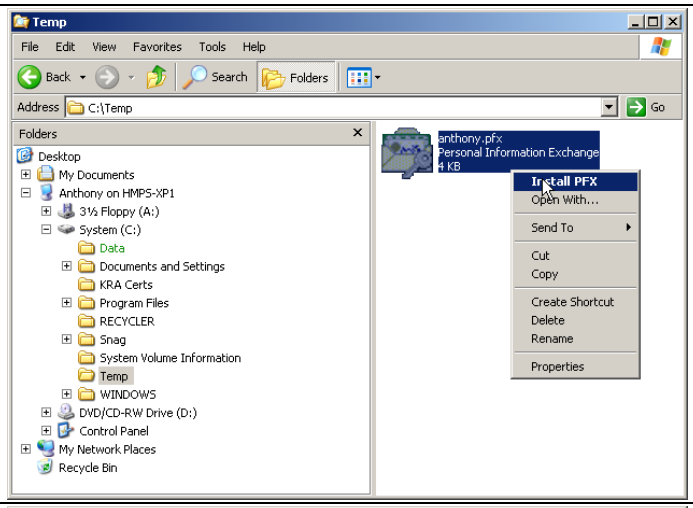
14. Verify there is a private key that corresponds to this certificate Click the **OK** button Close the Certificates MMC snap-in	

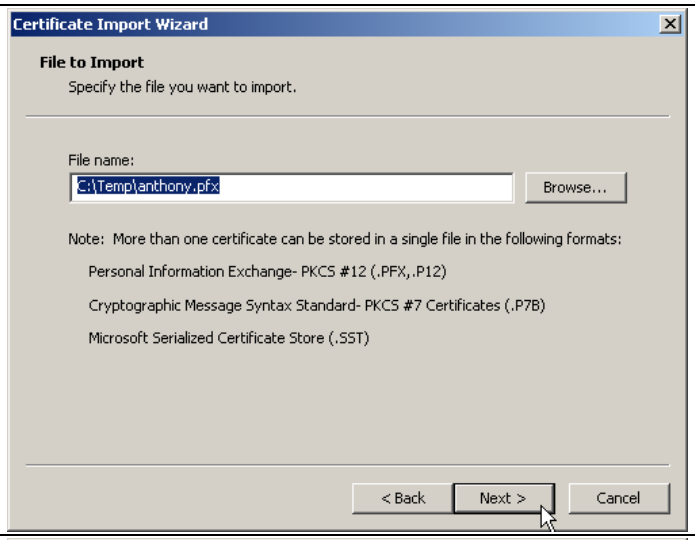
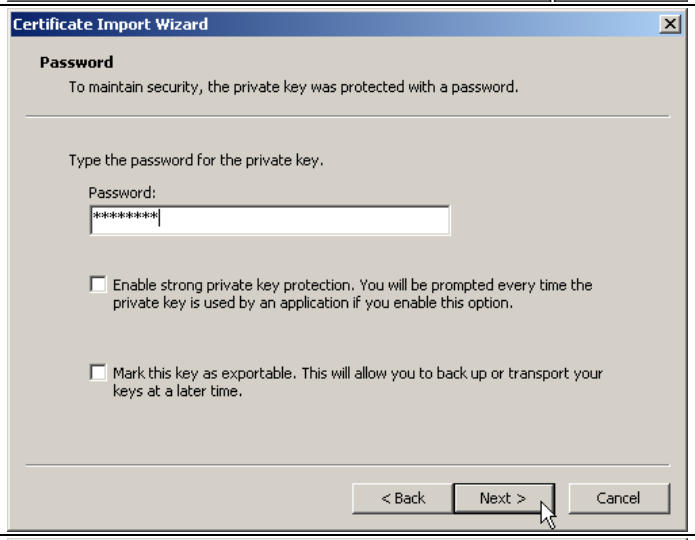
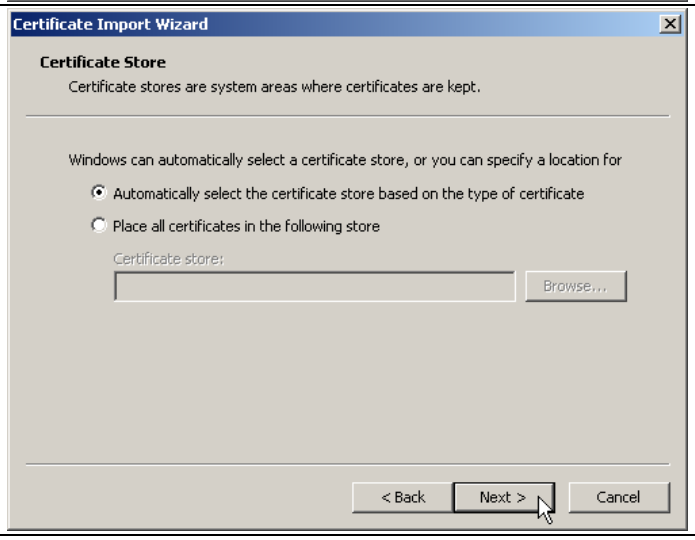
4. Decrypt Blob to Retrieve the User's Private Key

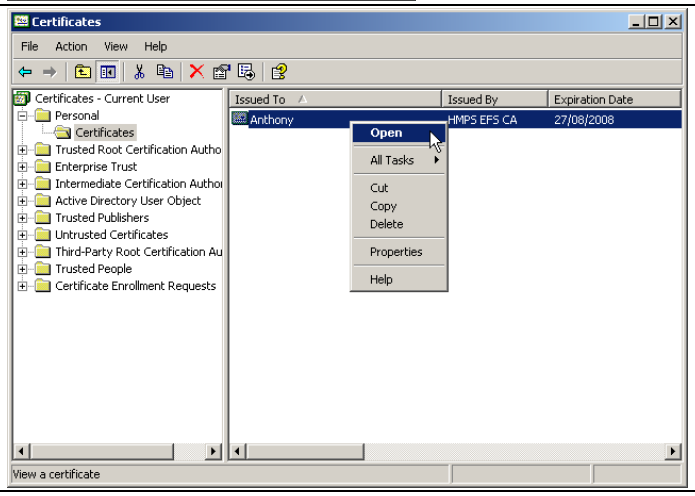
Action	Action Detail and Description
1. This chapter should be executed by the designated key recovery agent, whom installed their key recovery material into the certificate store on the recovery workstation in the previous chapter	
2. Open a command prompt and change the current folder to the folder where the blob was temporarily saved Issue the following command *(where anthony is used as an example)*: **certutil –recoverkey anthony.blob anthony.pfx** *Where anthony.blob is the name of the encrypted blob and anthony.pfx is the name of the PKCS #12 file which is be generated*	
3. Enter the **password** associated with the **KRA's private key** Click the **OK** button	
4. Assign a password to the newly created PKCS #12 file (and confirm password) *This password must be safely recorded as it will be given to the user at a later stage when he / she attempts to install the recovered private key into their certificate store*	

5. Verify the recovery command completed successfully	
6. Observe the newly created PKCS #12 in the file system (.pfx file)	
7. Copy the newly created PKCS #12 file onto removable media for transfer to the target user's workstation Ensure the password associated with the PKCS #12 file is securely recorded Securely delete the PKCS #12 file from the recovery workstation Securely delete the encrypted blob file from the recovery workstation	
8. Delete the KRA certificate from the certificate store on the recovery workstation Reboot the recovery workstation	

5. Import User's Private Key into their Certificate Store

Action	Action Detail and Description
1.	This chapter is performed at the user's computer, with the user logged on (no special user privileges are required). You will however be required to contact the DSMC to allow access to the removable media to import the users private key during this process, this privilege will be removed after the procedure. The recovered PKCS #12 file and associated password must be available
2. Insert the media containing the recovered PKCS #12 file Open an instance of Windows Explorer Select the PKCS #12 file, then select **Install PFX** from the context menu *Note: The screen capture here shows the PKCS #12 material being on the C-Drive, this may be on other media such as a USB memory stick or CD-ROM*	
3. Click the **Next** button	

4. Click the **Next** button ***Note:*** *The screen capture here shows the PKCS #12 material being on the C-Drive, this may be on other media such as a USB memory stick or CD-ROM*	
5. Enter the password which was communicated at the start of this process by the Key Recovery agent Do not enable strong private key protection Do not enable marking this key as exportable Click the **Next** button	
6. Click the **Next** button	

7. Click the **Finish** button	
8. Click the **OK** button	
9. Open an MMC focused on the **Certificates** snap-in Select the recovered certificate, then select **Open** from the context menu	

10. Verify there is a private key that corresponds to the certificate Click the **OK** button Close the Certificates MMC snap-in	
11. Remove the media containing the PKCS #12 file If the media was a CD-ROM, it must be destroyed; if the media was a USB memory stick, the PKCS #12 file must be securely deleted	
12. The user should attempt to open previously encrypted files to verify that the end-to-end key recovery process has been successful	