ABC

CA for EFS Key Recovery Procedures v0.99

31st December, 1999

Table of Contents

1.	In	troduction	2
1.1	L.	Background	2
1.2	2.	Objective	2
1.3	3.	Document Scope	2
1.4	ł.	Pre-Requisites	2
1.5	5.	Overview of the Recovery Process	3
2.	Re	etrieve Private Key (Blob) from CA Database	4
3.	In	stall Key Recovery Certificate onto Recovery Workstation	6
4.	De	ecrypt Blob to Retrieve the User's Private Key	11
5.	In	nport User's Private Key into their Certificate Store	13

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 ٠
- 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.	📴 Key Recovery Tool					×
	File Help					
Start the Key Recovery Tool from the	Certification authority (CA)			Search Criteria		
Windows Server 2003 Resource Kit			-	Requester name (d	iomain/\uper}	-
Command Prompt (Start/All	Select the search criteria, enter an a	ppropriate value, and t	hen click	Value		
Command Prompt (Start/All	"Search" to display a list of matching	archived keys.		https/anthony		
Programs/ windows Resource Kit	Contractor				Sea	ich N
Tools/Command Shell)	Secol Number Subject	NotRelaye	Notülter	Template	Cet Hashishall	100
Execute krt.exe	Contraction of Company	1000000		1 tongood		
Retarget the Key Recovery Tool CA list						
her to the ABC EES CA				-		
box to the ABC LFS CA						
	To many a spin to have related to	associated entities to		han olek "Ranna"		
In the Search Criteria list box, select	To recover a private key, select the	Show KBA	Dove and t	nen cick. Hecover	a Black 1	2000 C
"Requestor name (domain\user)"		ander Krak		Deciy	PR 0100	100
	Status: Ready				He	¢.
In the Value field, specify the "Windows						
down lovel" account name of the user						
down-level account name of the user						
Click the Search button						
3.	Key Recovery Tool					×
	File Help					-
	Certification authority (CA)			Search Criteria		
Verify that the certificate of the user is			•	Requester name (d	(omain/vuper)	•
retrieved				Value		1000
	"Search" to display a list of matching	ppropriate value, and t archived keys.	nen cilok	-		-
If there are multiple certificates for the					Sen	ch]
user it will be necessary to validate the	Certificates					
precise serial number of the certificate to	Serial Number Subject	NotBelore	NotAlter	Template	Cert Hash(sha1)	
be retrieved	Lastaence. CN-Anthony, 004	-EF26/08/20}	27708/20	anetys	13 5F41 52 88 4c	
De Tellieveu						
Click the Show KRA button						
	To recover a private key, select the	associated certificate a	bove and t	hen click "Recover".		
		CE. 1004	The Party of the P			
		Show KASA	N Retri	we Blob. Decry	pt Blob. Reco	wer
	Status: Ready	Show KISA	Retri	Ve Blob Decry	PEBlob Reco	wer

CA for EFS Key Recovery Procedures v0.99

1	
4.	Key Recovery Agents Used for Archival
	Certificates:
Verify that the private key has been	Serial Number Subject Cert Hash(sha1) Issuing CA
archived using one of the two valid KRA	Git 601b5500000000 CN-June, OU-KRA Fo 0e 48 7c d7 bc 66 5a Git Matter EFS CA Chi June, OU-KRA Fo 0e 48 7c d7 bc 66 5a Git Matter EFS CA
certificates	44 6154633100000000 CN=1etty, 00=NHA.Fo e91e e815 43 21 35 a 441 141 2 EFS CA
Click the Close button	
	Close N
	4
5.	Key Recovery Tool
	File Help
Click the Retrieve Blob button	Centilication authority (CA) Search Cateria
	Requester name (doman'water)
	Select the search criteria, enter an appropriate value, and then click. Value
	Cetticates
	Serial Number Subject NotBefore NotAlter Template Cet Hash(sha1)
	To recover a newsterker, release the according of particular above and then click "Recover"
	Show KRA. Retrieve Blob N Decrypt Blob. Recover
	Statur Ready Help
6.	Save As
Specify a suitable location and filename	Savein: 🗀 Temp 💽 🗭 🖽 🕶
in which to save the Blob e a	
C·\Temn\username	
e. (remp (username	
Click the Course button	
Click the Save button	
Close the Key Recovery Tool	
It is assumed that the decryption of the	File name: anthony Save
blob will performed at the same recovery	Save as tune: Private key blobs (* blob)
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.





4.	Certificate Import Wizard
Click the Next button	File to Import Specify the file you want to import.
	File name:
	< Back Next > Cancel
5.	Certificate Import Wizard
Enter the password associated with the backed up KRA material	Password To maintain security, the private key was protected with a password.
Enable the Enable strong private key protection option	Type the password for the private key. Password: *******
Click the Next button	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	< Back Next > Cancel
6.	Certificate Import Wizard
Click the Next button	Certificate Store Certificate stores are system areas where certificates are kept.
	 Windows can automatically select a certificate store, or you can specify a location for Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Browse
	< Back Next > Cancel

7.	Certificate Import Wizard
Click the Finish button	Completing the Certificate Import Wizard You have successfully completed the Certificate Import Wizard You have specified the following settings: Certificate Store Selected Automatically determined by t Content PFX File Name C:\Temp< Image: Certificate Store Selected Automatically determined by t Content PFX File Name C:\Temp Image: Certificate Store Selected Automatically determined by t Content PFX File Name C:\Temp Image: Certificate Store Selected Selected Image: Certificate Store Selected Automatically determined by t Content PFX File Name C:\Temp Image: Certificate Store Selected Automatically determined by t Content PFX File Name C:\Temp Image: Certificate Store Selected Selected Image: Certificate Store Selected Automatically determined by t Content PFX File Name C:\Temp Image: Cerificate Selected Selected
8.	Importing a new private exchange key
Click the Set Security Level button	An application is creating a Protected item. CryptoAPI Private Key Security level set to Medium OK Cancel Details
9.	Importing a new private exchange key
Select the High option	Choose a security level appropriate for this item.
Click the Next button	 High Request my permission with a password when this item is to be used. Medium Request my permission when this item is to be used.
	< Back Next > Cancel

10.	Importing a new private exchange key
Re-Enter and Confirm the password associated with the KRA key material Click the Finish button	Create a password to protect this item. Create a new password for this item. Password for: CryptoAPI Private Key Password: ••••••• Confirm: •••••••
	K Cancel
11.	Importing a new private exchange key
Click the OK button	An application is creating a Protected item. An application is creating a Protected item. CryptoAPI Private Key Security level set to High Set Security Level OK Cancel
12.	Certificate Import Wizard
Click the OK button	The import was successful.
13.	El Certificates
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	Contracts - Current User Personal Contracts - Current User Personal Contracts - Current User Contracts Contracts - Current User Contracts Contracts - Current User Contracts C
	Personal store contains 1 certificate.

Page 10

14.	Certificate	<u>?×</u>
Verify there is a private key that corresponds to this certificate Click the OK button Close the Certificates MMC snap-in	General Details Certification Path Image: Certificate Information This certificate is intended for the following purpose(s): •Key Recovery Agent	_
	Issued to: Terry Issued by: Throte 5 CA	
	Valid from 28/08/2006 to 27/08/2008	
	Issuer Stateme	int
		ж

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

Action	Action Detail and Description
1. This chapter should be executed by the de recovery material into the certificate store	signated key recovery agent, whom installed their key 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 	Command Prompt C:\Tenp>certutil -recoverkey anthony.blob anthony.pfx_
3. Enter the password associated with the KRA's private key Click the OK button	Using your private exchange key to decrypt An application is requesting access to a Protected item. CryptoAPI Private Key Bemember password
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	Command Prompt - certoid recoverkey anthony.bdo anthony.gdx Element.dwlnfoStatus - CERT_TRIST_MAS_PREFERED_ISSUER (0x100) Exclude leaf cert: da 37 a3 ee 5e 6b 4b 8d 32 55 bf ef 95 60 18 90 af d8 07 07 Pull chain a7 0b 68 ad 3b ba 61 2e aa 37 ff 9b d2 fb 9e c4 bd d4 c5 86 Verified Application Policies: All Verified Application Policies: All Verified Application Policies: All Computed Hash: 92 a8 2c 98 af 96 00 d3 b5 35 6e 74 03 94 3d 96 a2 12 06 bf 417.327.018 bdB0070103 (UHX2: 257) 300.5557.018 bdB0070103 (UHX2: 257) 300.557.018 bdB0070000000000000000000000000000000000

_	T		
5. Verify the recovery command completed successfully	<pre>Command Prompt da 37 a3 ee 5e 6h 4h 8d 32 55 bf ef 95 68 18 98 af d8 87 87 a7 8b 65 a4 3b ba 61 2e aa 37 ff 9b d2 fb 9e c4 bd d4 c5 86 Uerified Issuance Policies: All Uerified Replication Policies: All Computed Mach: 92 a8 2c 98 af 86 03 b5 35 6e 74 83 94 3d 96 a2 12 86 bf 417.578.8: BudBW708183 (UHR32: 259) 127.578.8: BudBW708183 (UHR32: 259) 1285.557.0: BudBW708183 (UHR32: 259) Decrypted PKCS7 Message Content User Certificate: Serial Manker 618-07 cc8888808088 Issuer: CH Serial Manker 618-07 cc88888080888 Issuer: CH Continue of the 25 blokes, OU-Users, OU-HMPS, DC-MMPS, DC-M</pre>		
6.	Temp III X		
	File Edit View Favorites Tools Help 🥂		
	🔇 Back 🔹 🕤 🖌 🌮 Search 🌮 Folders 🛛 😹 🍞 🗙 🆃 🛄 🔹		
Observe the newly created PKCS #12 in	Address 🛅 C:\Temp		
the file system (.pfx file)	Folders X Name A Size Type Date Modified		
	Desktop TKB BLOB File 28/08/2006 15		
	My Documents My Documents 4 KB Personal Informati 28/08/2006 15		
	Erry on HMPS-XP1		
	System (C:)		
	Data		
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 associate	ed 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 	Image: Second Properties File Edit View Favorites Tools Help Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties Image: Second Properties			
3. Click the Next button	Certificate Import Wizard Welcome to the Certificate Import Wizard University of the second			

CA for EFS Key Recovery Procedures v0.99

4.	Certificate Import Wizard
	File to Import
Click the Next button	Specify the file you want to import.
	· · · · · · · · · · · · · · · · · · ·
Note: The screen capture here shows	File name:
the PKCS #12 material being on the C-	C:\Temp\anthony.pfx Browse
Drive, this may be on other media such	
as a USB memory stick or CD-ROM	Note: More than one certificate can be stored in a single file in the following formats:
	Personal Information Exchange- PKCS #12 (.PFX,.P12)
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
	Microsoft Serialized Certificate Store (.SST)
	< Back Next > Cancel
5.	Certificate Import Wizard
	Password
Enter the password which was	To maintain security, the private key was protected with a password.
communicated at the start of this	
process by the Key Recovery agent	Turne the encoursed for the extincted law.
p , , , , , , , ,	Type the password for the private key.
Do not onable strong private key	Password:
protection	
protection	
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Do not enable marking this key as	
exportable	Mark this loss as assortable. This will allow you to back up as transport your
	keys at a later time.
Click the Next button	
	KK Cancel
6	Certificate Import Wizard
0.	
Click the Next button	Certificate store Certificate stores are system areas where certificates are kent.
Click the Next button	
	Windows can automatically select a certificate store, or you can specify a location for
	$oldsymbol{\odot}$ Automatically select the certificate store based on the type of certificate
	O Place all certificates in the following store
	Certificate store:
	Browse
	< Back Next > Cancel

7.	Certificate Import Wizard
Click the Finish button	Completing the Certificate Import Wizard Out have successfully completed the Certificate Import wizard. Out have specified the following settings: Content PFX File Name C:\Temp\anthony.pfx
8.	Certificate Import Wizard
Click the OK button	The import was successful.
 9. Open an MMC focused on the Certificates snap-in Select the recovered certificate, then select Open from the context menu 	

10.	Certificate	
Verify there is a private key that corresponds to the certificate Click the OK button	General Details Certification Path	
Close the Certificates MMC snap-in	Allows data on disk to be encrypted	
	Issued to: Anthony Issued by: Harabara CA Valid from 28/08/2006 to 27/08/2008	
	You have a private key that corresponds to this certificate. Issuer Statement	
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