

Windows Encrypting File System

Motivation

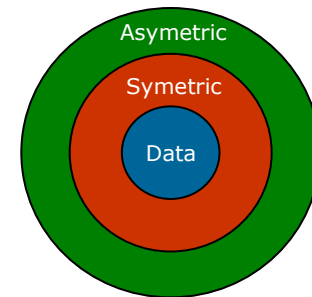
- Laptops are very integrated in enterprises...
 - Stolen/lost computers loaded with confidential/business data
 - Data Privacy Issues
 - Offline Access
 - Windows reinstallation
 - Administrators privilege
- Bypass NTFS
 - Bypass ACL
 - Bypass Ownership



Windows Encrypting File System

Mechanism

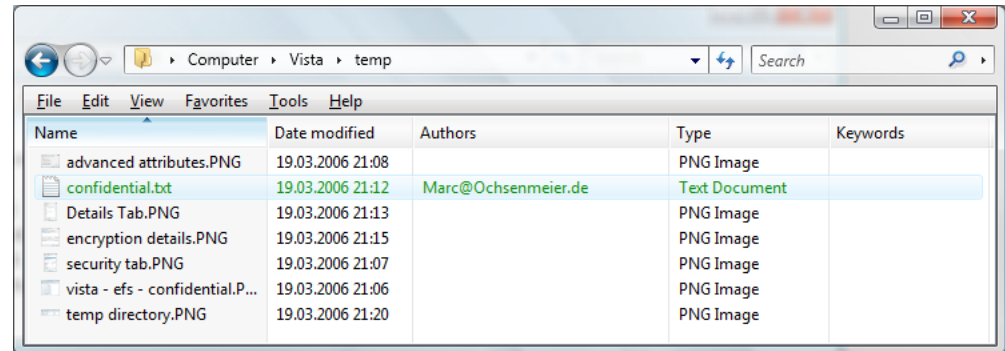
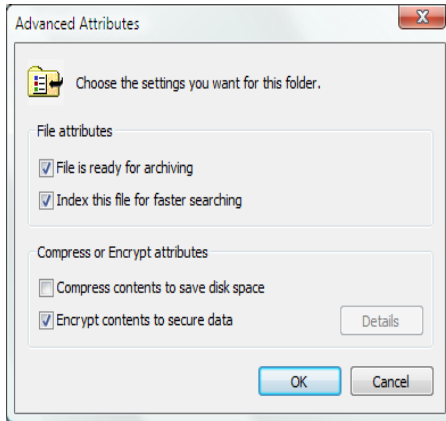
- Principle
 - A random - unique - symmetric key encrypts the data
 - An asymmetric key encrypts the symmetric key used to encrypt the data
- Combination of two algorithms
 - Use their strengths
 - Minimize their weaknesses
- Results
 - Increased performance
 - Increased security



Windows Encrypting File System

Characteristics

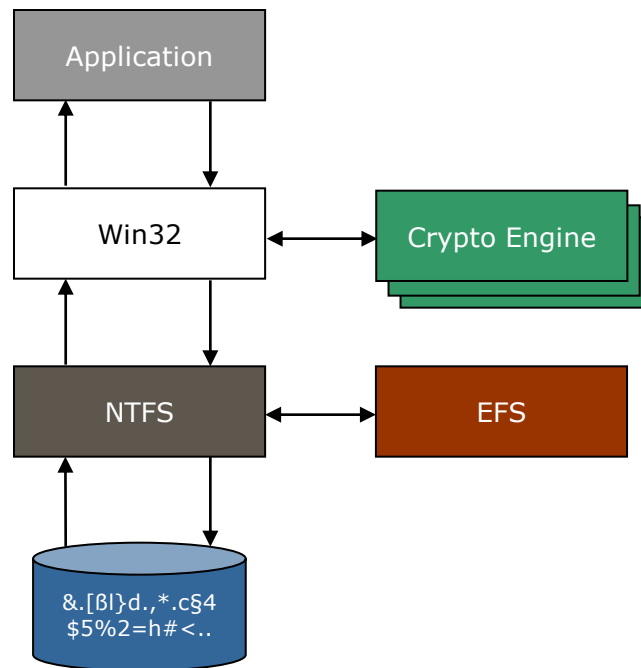
- Comfortable
 - Applying encryption is just a matter of assigning a file attribute



Windows Encrypting File System

Characteristics

- Transparent
 - Integrated into the operating system
 - Transparent to (valid) users/applications



Windows Encrypting File System

Characteristics

- Flexible
 - Supported at different scopes
 - File, Directory, Drive (Vista?)
 - Files can be shared between any number of users
 - Files can be stored anywhere
 - local, remote, WebDav
 - Files can be offline
- Secure
 - Encryption and Decryption occur in kernel mode
 - Keys are never paged
 - Usage of standardized cryptography services

Windows Encrypting File System

Availability

- At the GUI, the availability is determined by the product level

Vista	Home Basic	Home Premium	Business	Ultimate
EFS	No	No	Yes	Yes

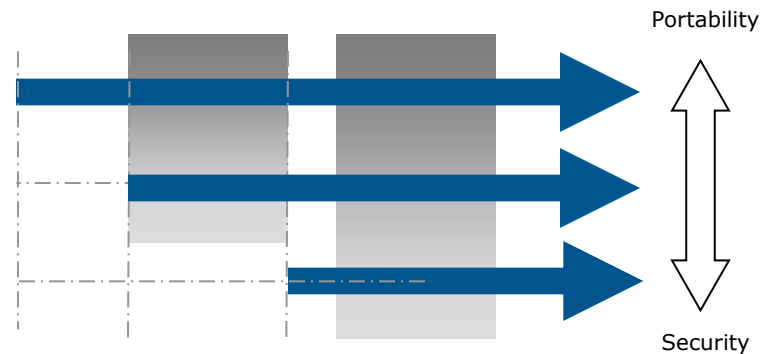
Windows 7	Home Premium	Professional	Enterprise	Ultimate
EFS	No	Yes	Yes	Yes

Windows Encrypting File System

Portability

- Use the appropriate Symmetric encryption algorithm when data must be shared on different platforms

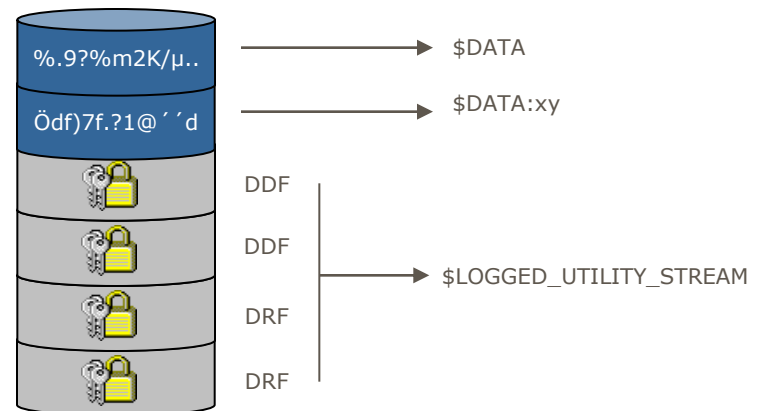
NTFS	Platform	Support (default)
5.0	W2K	DESX
5.1	XP PRO	DESX , 3DES
5.1	XP PRO SP1	DESX , 3DES, AES
5.2	W2K3	DESX , 3DES, AES
6.0	Vista	DESX, 3DES, AES
7.0	Windows 7	DESX, 3DES, AES



Windows Encrypting File System

Encryption – Internal Process

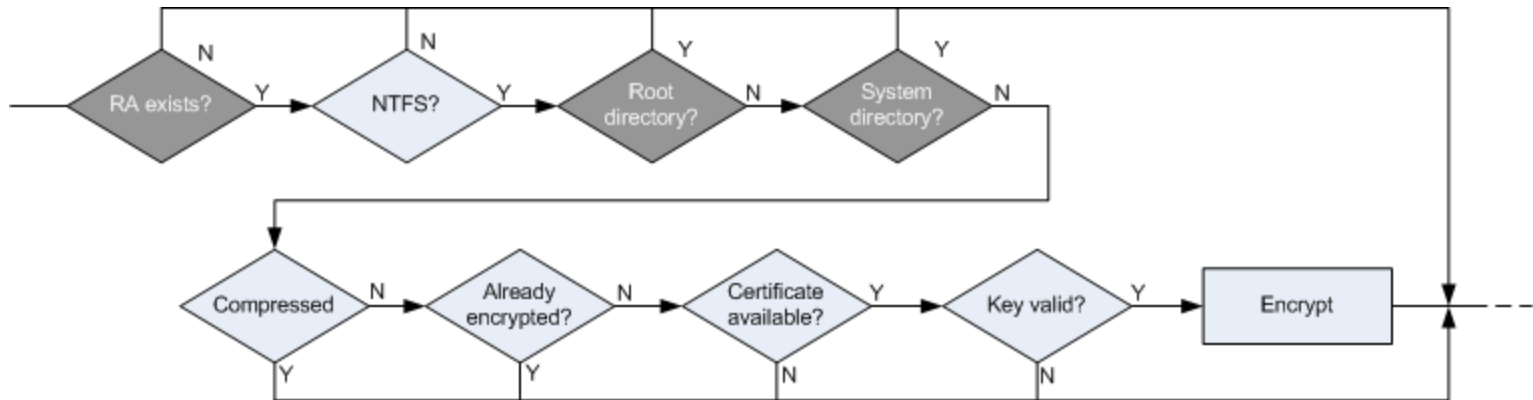
- Open file for exclusive access
- Create transaction log file in "System Volume Information" folder
- Generate the unique random FEK to encrypt the file content
- Generate user's Public/Private keys and request a certificate
- Create DDF rings containing the encrypted FEK
- Create DRF rings containing the encrypted FEK
- Create an empty backup file
- Add rings to the backup file
- Encrypt the backup file
- Copy *all* \$DATA streams to the backup file
- Destroy original file's content
- Copy backup file to original file
- Delete backup file
- Delete log file



Windows Encrypting File System

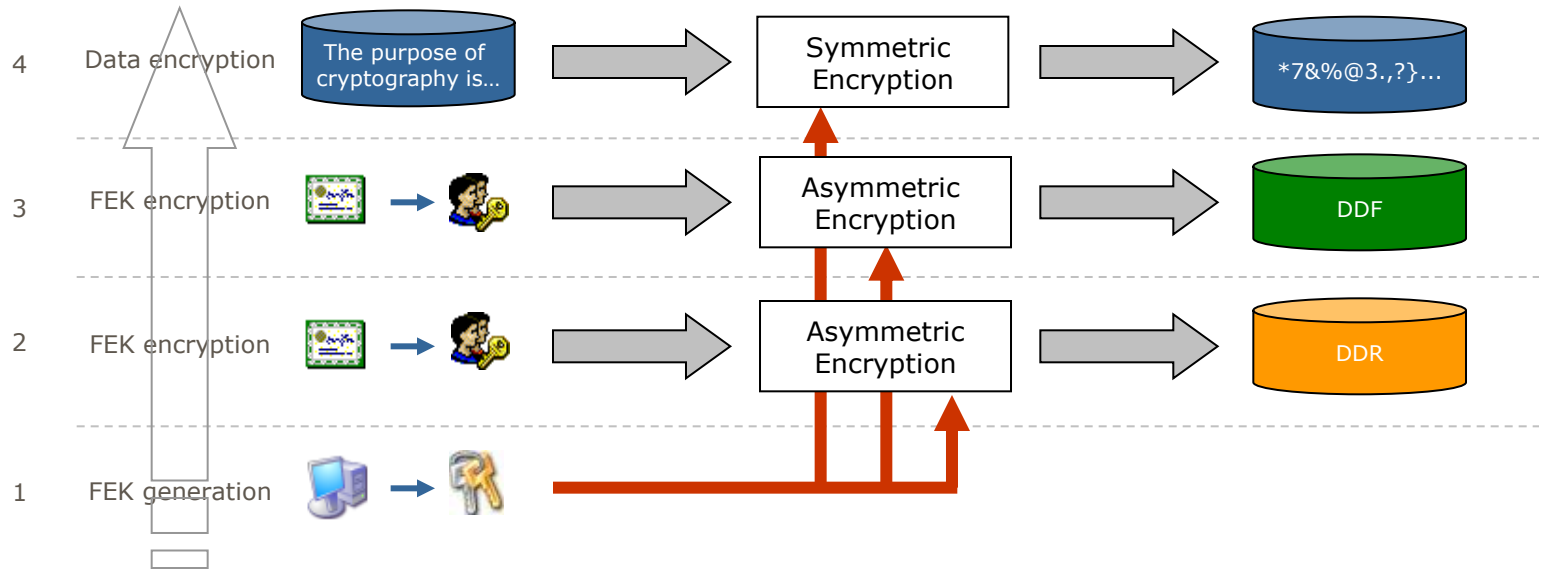
Encryption -Functional Prerequisites

- For a successful encryption, several conditions must be met



Windows Encrypting File System

Encryption – Logical View



Windows Encrypting File System

Decryption – Internal Process

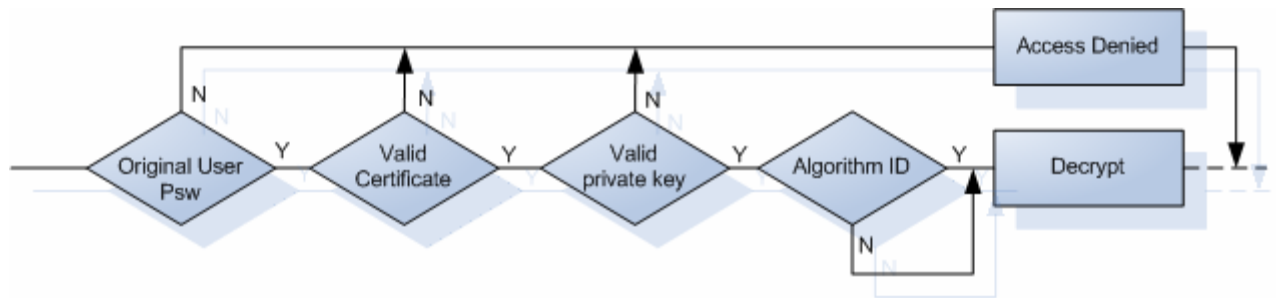
- Read user's identity (SID) in his/her token
- Locate user's identity (SID) in the DDF
- Load user's private key
- Decrypt the encrypted FEK stored in the DDF
- Decrypt the \$DATA using the decrypted FEK



Windows Encrypting File System

Decryption – Functional Prerequisites

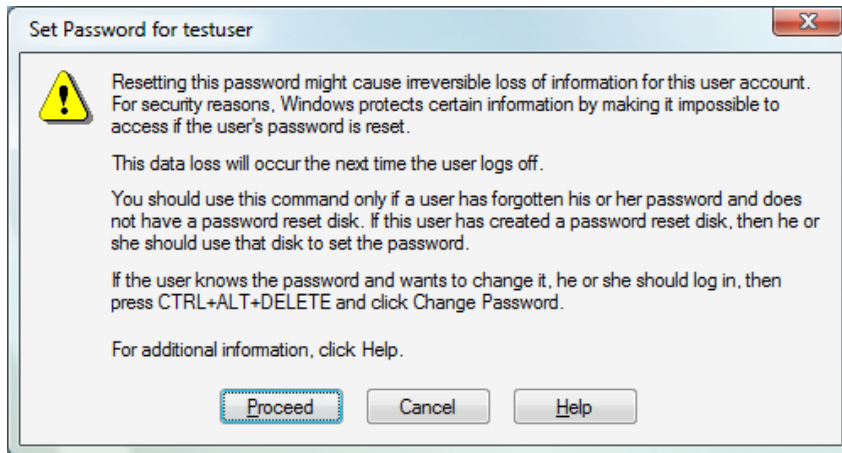
- Some conditions must be met in order to successfully open (decrypt) an encrypted document
 - User password must be original
 - Private key and Certificate must exist
 - Algorithm used to encrypt must be available



Windows Encrypting File System

Recovery - Motivation

- Employee is absent (vacation, left the company...)
- Employee account has been deleted
- Employee password has been reset by someone else
- Employee lost his/her decryption key



Windows Encrypting File System

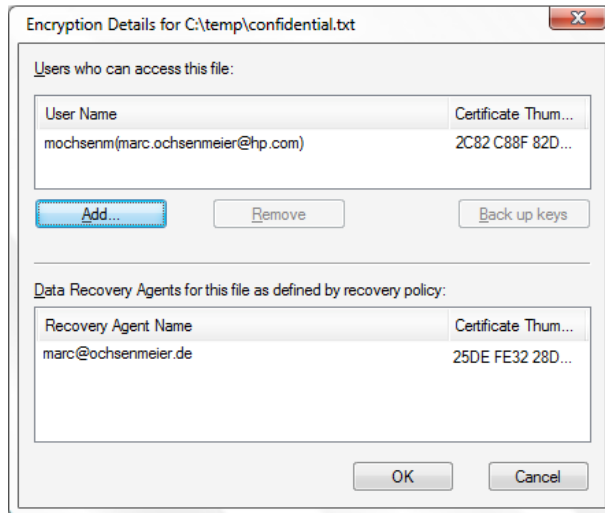
Recovery - Paradigm

- Data Recovery Agent (DRA)
 - Can only recover the encrypted files
 - Cannot retrieve any other user private information

Windows Encrypting File System

Recovery - Management

- As for the DACL and SACL settings management
 - The DDF is managed at the discretion of the file owner
 - The DRF is managed at the discretion of the administrator(s)





Windows Encrypting File System


Recovery – Default DRA

- Scenario

W2K		XP		Vista	
Stand-alone	Domain	Stand-alone	Domain	Stand-alone	Domain
Local Administrator	Domain Administrator	None.	Domain Administrator	None.	Domain Administrator


Security Risk


Usability Risk


Usability Risk

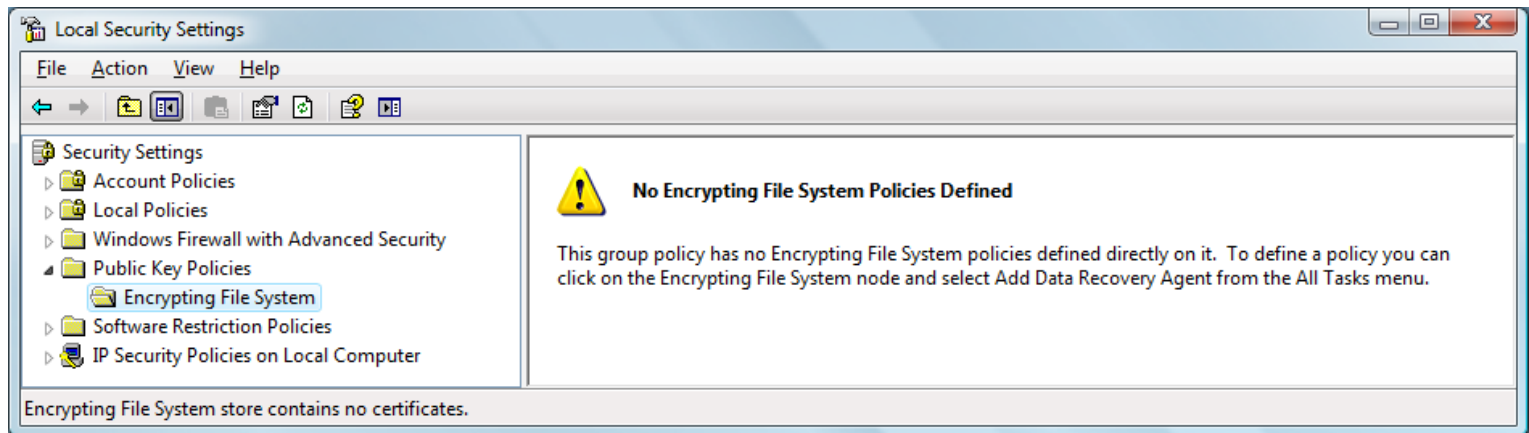
- Consequence

- While RA are automatically created in domains, users of stand-alone machines should create their agents manually

Windows Encrypting File System

Recovery - Manual Creation of a DRA

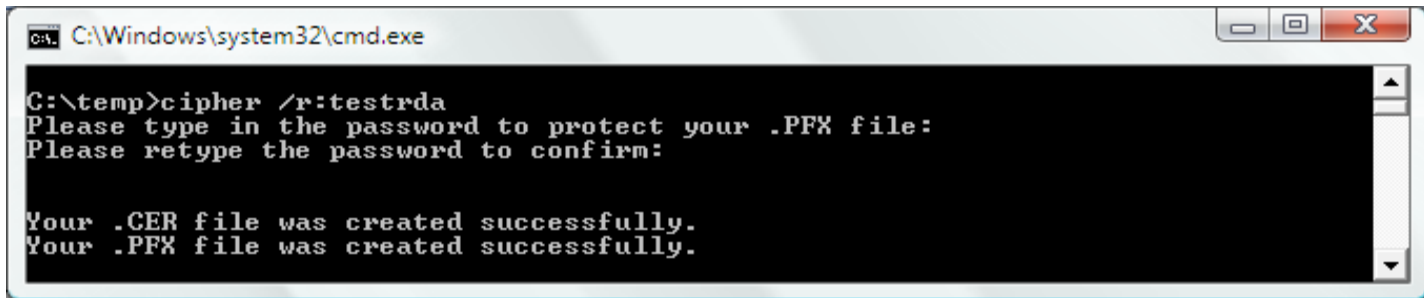
- DRA is not automatically assigned when running in stand-alone or member of a workgroup



Windows Encrypting File System

Recovery - Manual Creation of a DRA

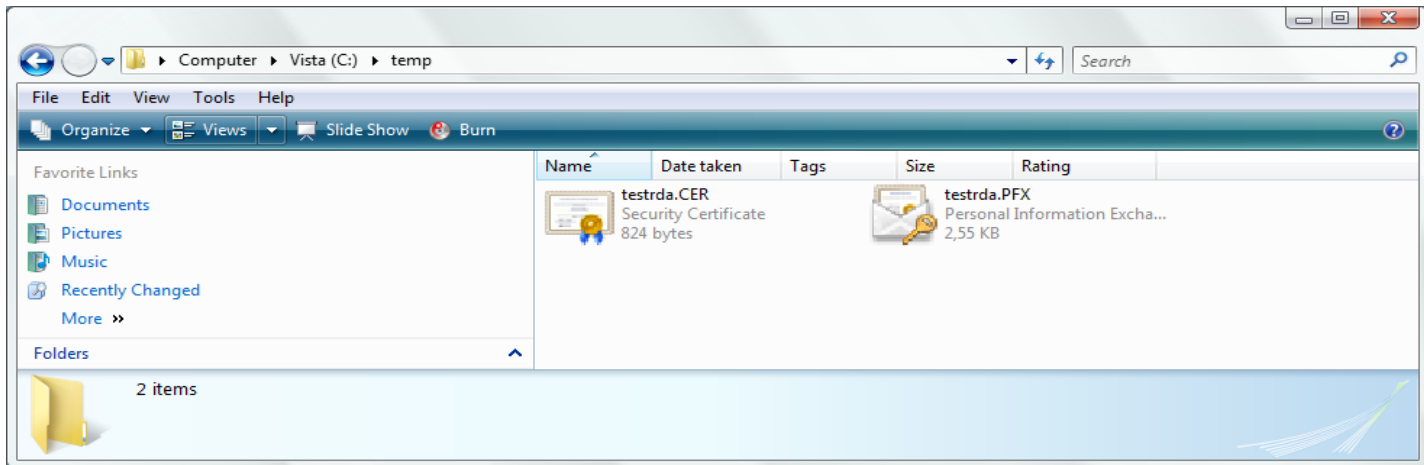
- Use built-in Cipher tool



```
C:\Windows\system32\cmd.exe

C:\temp>cipher /r:testrda
Please type in the password to protect your .PFX file:
Please retype the password to confirm:

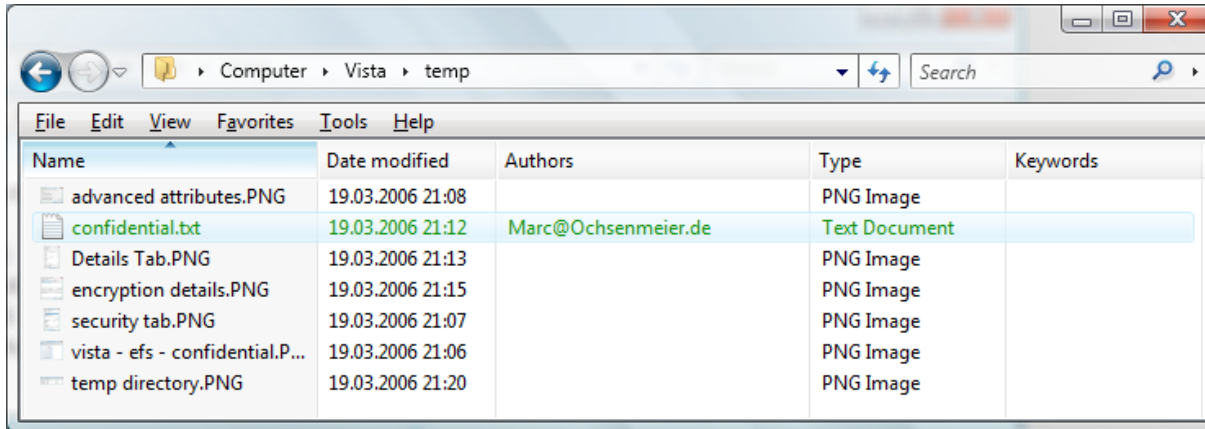
Your .CER file was created successfully.
Your .PFX file was created successfully.
```



Windows Encrypting File System

Issues

- Folder names and file names are not encrypted
- File attributes (creation, modification time) are visible

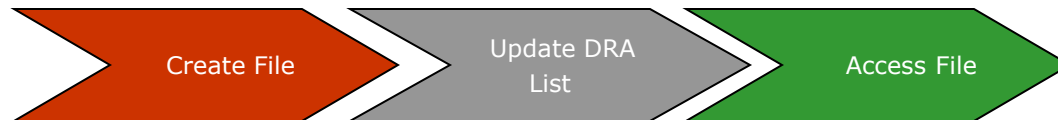


- Only available on hard disk
- Only available on NTFS partition

Windows Encrypting File System

Issues

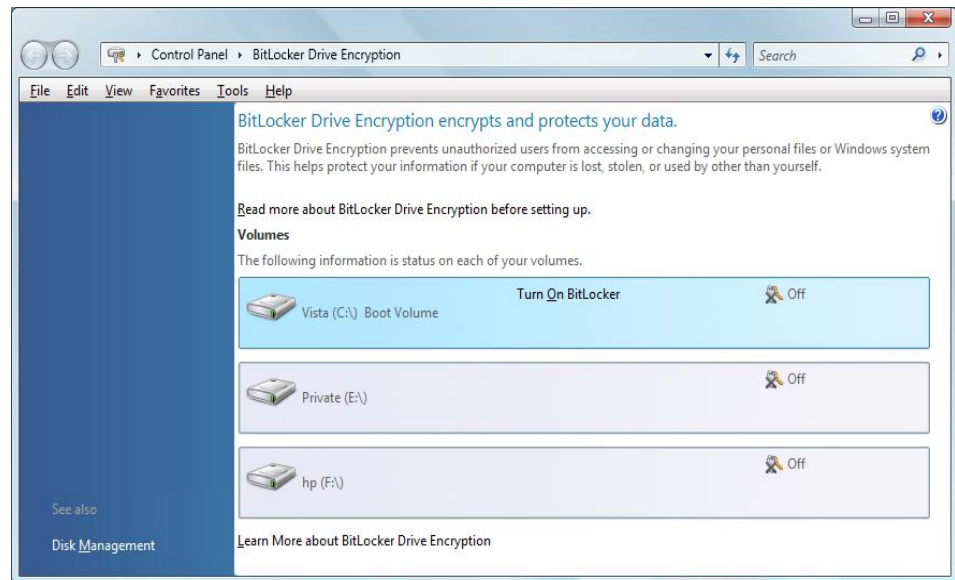
- Potential danger of unrecoverable data
 - Files stay a long time without being accessed
 - DRF rings are only updated when a file operation occurs
 - Use Cipher /U
 - Update DDFs and DRFs to reflect newest keys changes



Windows Encrypting File System

Issues

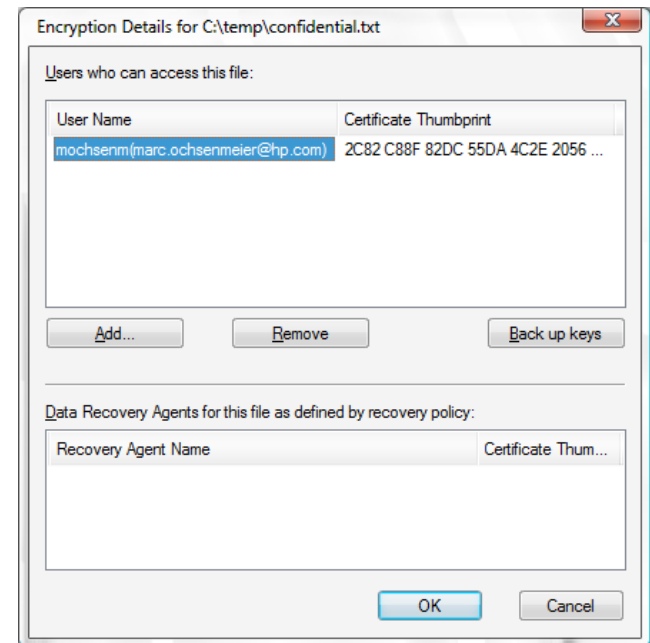
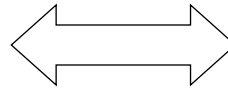
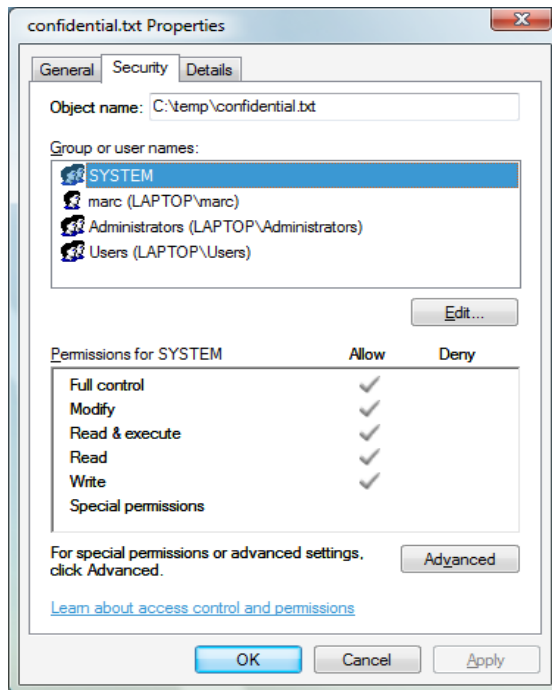
- Some critical system areas are only encrypted starting with Vista
 - Hibernation file
 - Paging file
 - Windows directory
 - Registry



Windows Encrypting File System

Warning

- EFS does not replace ACL management
- DDF settings should be synchronized ACL settings



Windows Encrypting File System

Links

- Microsoft Windows Internals (Microsoft Press, M.Russinovich)
- Network Security Essentials (Prentice Hall, William Stallings)
- The Encrypting File System, <http://technet.microsoft.com/en-us/library/cc700811.aspx>