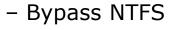
# Motivation

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

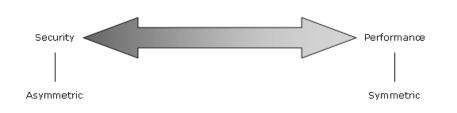


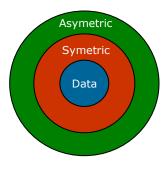
- Bypass ACL
- Bypass Ownership



# 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





#### Characteristics

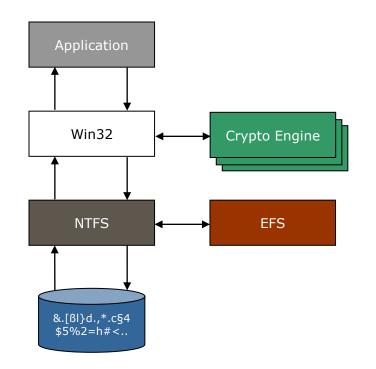
- Confortable
  - Applying encryption is just a matter of assigning a file attribute

Advanced Attributes
Choose the settings you want for this folder.
File attributes
File is ready for archiving
☑ Index this file for faster searching
Compress or Encrypt attributes
Compress contents to save disk space
Encrypt contents to secure data
OK Cancel

→ ○ ↓ · Computer	▶ Vista ▶ temp		✓ Search	Q
<u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites	<u>T</u> ools <u>H</u> elp			
Name	Date modified	Authors	Туре	Keywords
advanced attributes.PNG	19.03.2006 21:08		PNG Image	
📋 confidential.txt	19.03.2006 21:12	Marc@Ochsenmeier.de	Text Document	
Details Tab.PNG	19.03.2006 21:13		PNG Image	
encryption details.PNG	19.03.2006 21:15		PNG Image	
security tab.PNG	19.03.2006 21:07		PNG Image	
🔟 vista - efs - confidential.P	19.03.2006 21:06		PNG Image	
temp directory.PNG	19.03.2006 21:20		PNG Image	

## Characteristics

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



#### 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

# Availibility

• At the GUI, the availibility is determined by the product level

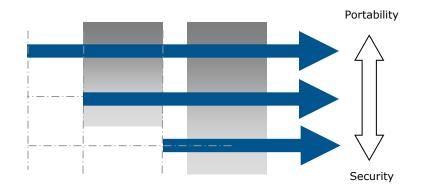
Vista	Home Basic	Home Premium	Business	Ultimate
EFS	No	No	Yes	Yes

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

# Portability

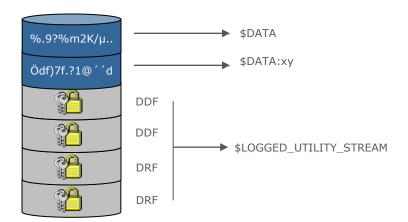
• Use the appropriate Symmetric encryption algorithm when data must be shared on different platforms

NTFS	Platform	Support ( <b>default</b> )
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, <b>AES</b>
7.0	Windows 7	DESX, 3DES, <b>AES</b>



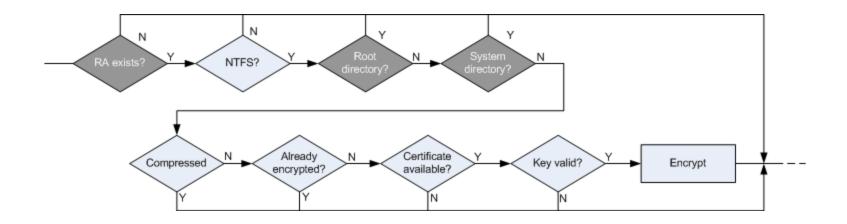
#### **Encryption – Internal Process**

- 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

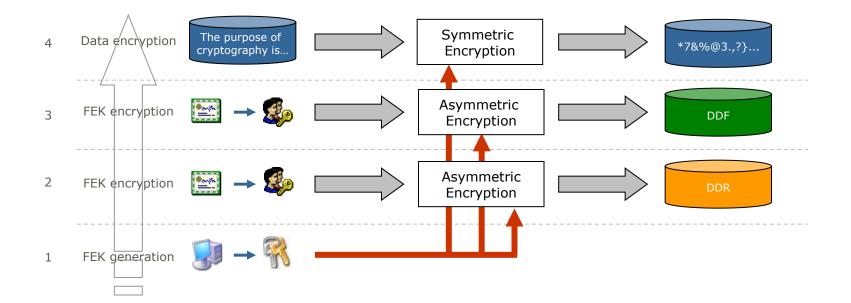


# Encryption -Functional Prerequisites

For a successful encryption, several conditions must be met



## Encryption – Logical View



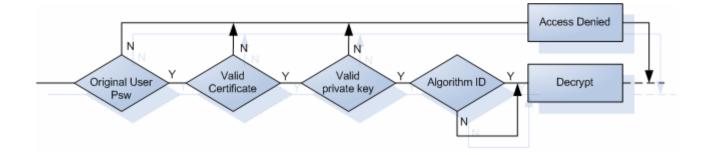
#### **Decryption – Internal Process**

- 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



## 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



#### **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

Set Pass	word for testuser				
⚠	Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset.				
	This data loss will occur the next time the user logs off.				
	You should use this command only if a user has forgotten his or her password and does not have a password reset disk. If this user has created a password reset disk, then he or she should use that disk to set the password.				
	If the user knows the password and wants to change it, he or she should log in, then press CTRL+ALT+DELETE and click Change Password.				
	For additional information, click Help.				
	Proceed Cancel <u>H</u> elp				

# Recovery - Paradigm

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

#### 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)

User Name	Certificate Thum
mochsenm(marc.ochsenmeier@hp.com)	2C82 C88F 82D
Add	Back up keys
	very policy: Certificate Thum
ata Recovery Agents for this file as defined by reco Recovery Agent Name marc@ochsenmeier.de	

# Recovery – Default DRA

#### • Scenario

v	V2K		ХР		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	

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

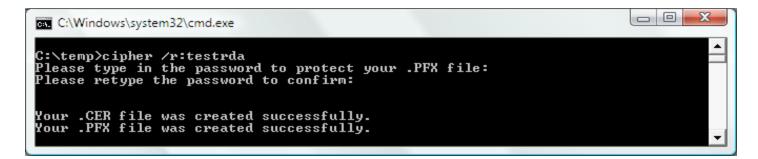
# Recovery - Manual Creation of a DRA

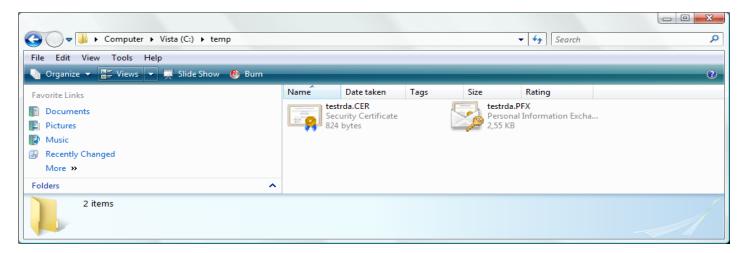
• DRA is not automatically assigned when running in standalone or member of a workgroup



# Recovery - Manual Creation of a DRA

• Use built-in Cipher tool





#### Issues

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

Computer → Vista → temp ✓ 4 Search 2 →					
<u>File Edit View Favorites Tools H</u> elp					
Name	Date modified	Authors	Туре	Keywords	
advanced attributes.PNG	19.03.2006 21:08		PNG Image		
📋 confidential.txt	19.03.2006 21:12	Marc@Ochsenmeier.de	Text Document		
Details Tab.PNG	19.03.2006 21:13		PNG Image		
encryption details.PNG	19.03.2006 21:15		PNG Image		
security tab.PNG	19.03.2006 21:07		PNG Image		
🔲 🔟 vista - efs - confidential.P	19.03.2006 21:06		PNG Image		
temp directory.PNG	19.03.2006 21:20		PNG Image		

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

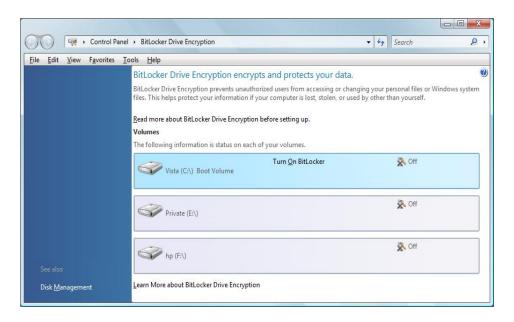
#### Issues

- 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



#### Issues

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



#### Warning

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

confidential.txt Properties	Encryption Details for C:\temp\confidential.txt
General Security Details	Users who can access this file:
Object name: C:\temp\confidential.txt	User Name Certificate Thumbprint
Group or user names:	mochsenm(marc.ochsenmeier@hp.com) 2C82 C88F 82DC 55DA 4C2E 2056
SYSTEM S marc (LAPTOP\marc)	
Administrators (LAPTOP\Administrators)	
🕵 Users (LAPTOP\Users)	
Edit	Add <u>R</u> emove <u>B</u> ack up keys
Permissions for SYSTEM Allow Deny	
Full control	
Modify 🗸	Data Recovery Agents for this file as defined by recovery policy:
Read & execute	Recovery Agent Name Certificate Thum
Read V	
Special permissions	
For special permissions or advanced settings, Advanced click Advanced.	
Learn about access control and permissions	OK Cancel
OK Cancel Apply	

# Links

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