COMPAQ
Inspiration Technology

25. DECUS München e.V. Symposium 2002

2C02

EFS / Recovery

Josef Beeking

Compaq Computer GmbH

COMPAQ

Overview

- How EFS Works
- Recovery Basics
- Windows 2000 Standalone Scenarios
- Windows 2000 Domain Scenarios
- Windows .NET Server Enhancements
- Windows .NET Scenarios
- Best Practices

COMPAQ

Encrypting File System

- Privacy of data that goes beyond access control
  - Protect confidential data on laptops
  - Configurable approach to data recovery
- Integrated with core operating system components
  - Windows NT File System - NTFS
  - Crypto API key management
  - LSA security policy
- Transparent and high performance

COMPAQ
Inspiration Technology

How EFS Works

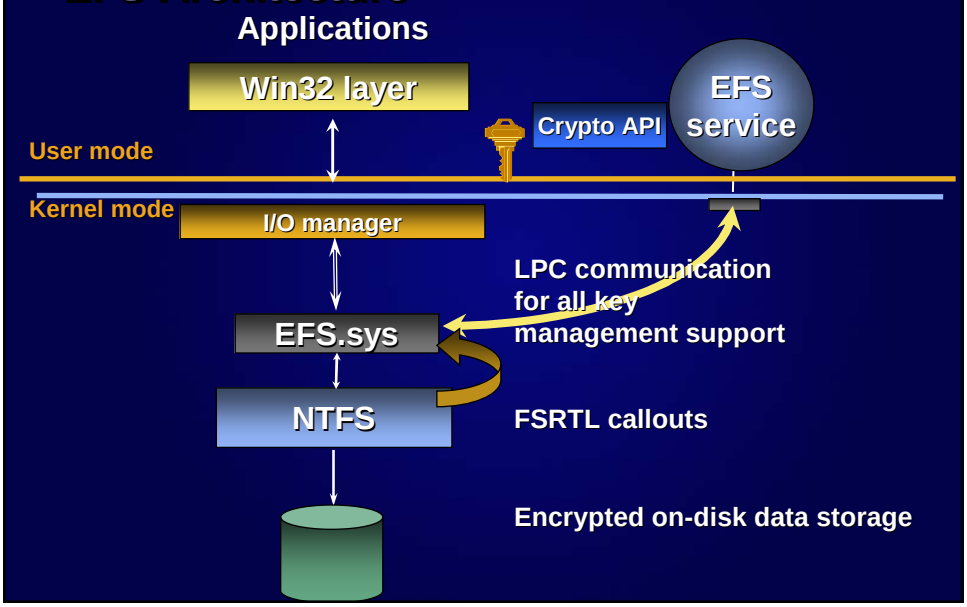
COMPAQ

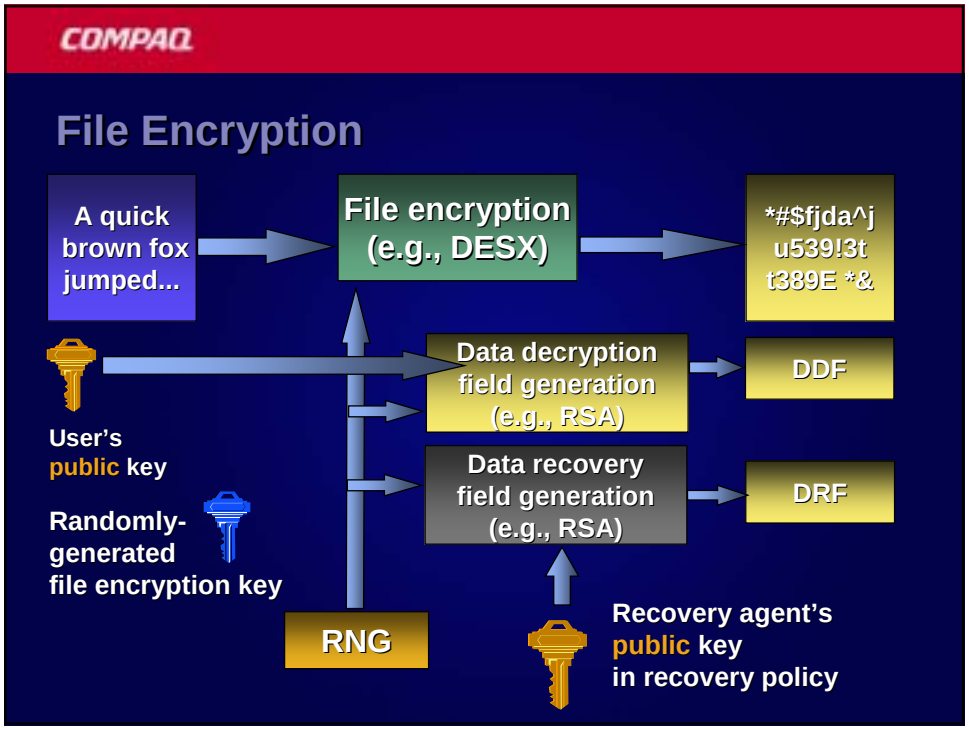
EFS Fast Facts

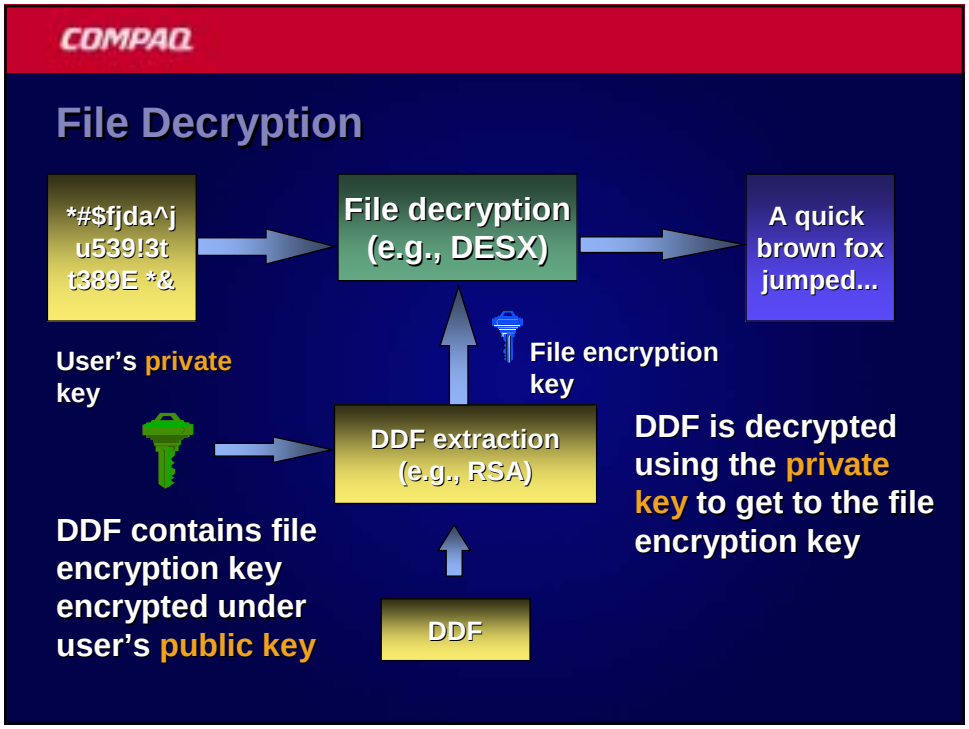
- EFS uses a combination of symmetric and asymmetric encryption
  - Symmetric = File Encryption Key
  - Asymmetric = Public/Private Key Pairs
- Key Security Principals
  - User that encrypted the file
  - Data Recovery Agent

COMPAQ

EFS Architecture

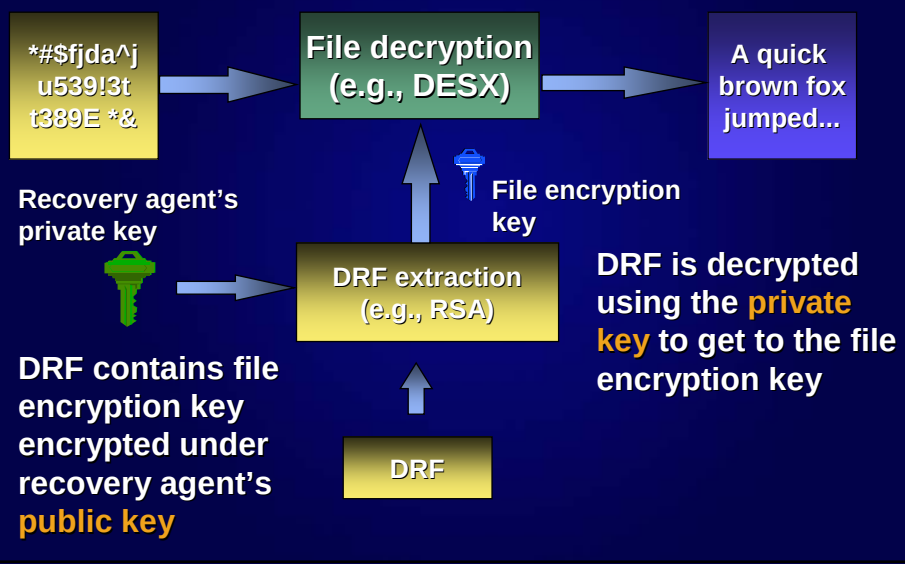



COMPAQ
File Encryption
A quick brown fox jumped...
File encryption (e.g., DESX)
*#$fjda^j u539!3t t389E *&
Data decryption field generation (e.g., RSA)
DDF
User's public key
Randomly-generated file encryption key
Data recovery field generation (e.g., RSA)
DRF
RNG
Recovery agent's public key in recovery policy


COMPAQ
File Decryption
*#$fjda^j u539!3t t389E *&
File decryption (e.g., DESX)
A quick brown fox jumped...
File encryption key
User's private key
DDF extraction (e.g., RSA)
DDF is decrypted using the private key to get to the file encryption key
DDF contains file encryption key encrypted under user's public key
DDF

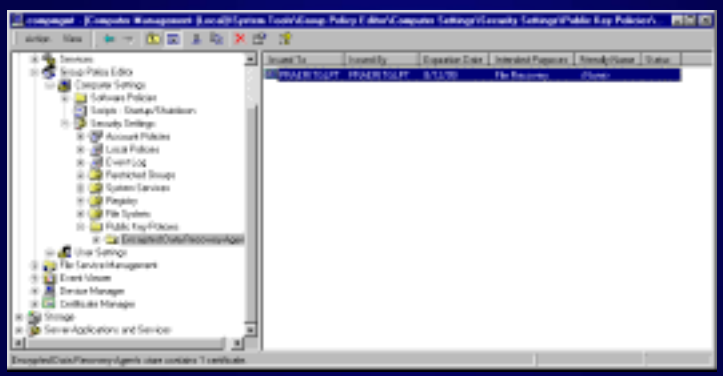
COMPAQ

File Recovery



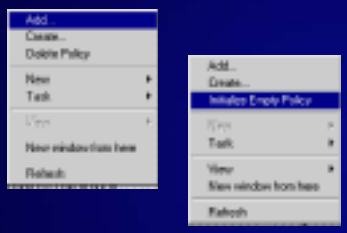
COMPAQ

Encrypted Data Recovery Agents



COMPAQ

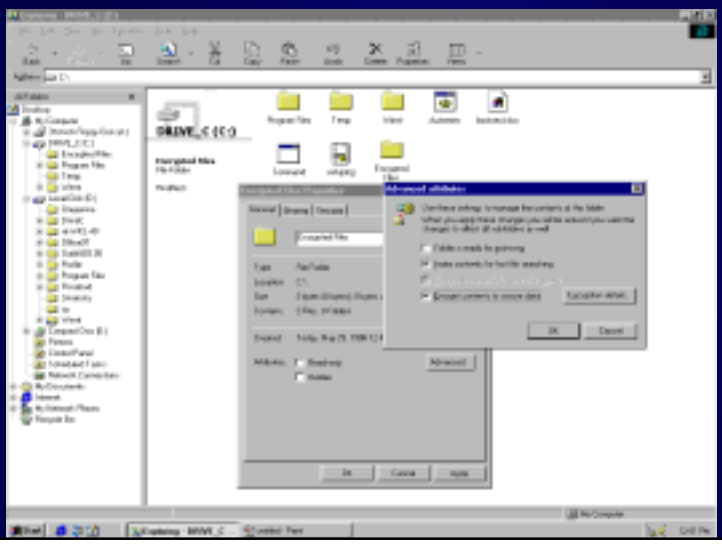
Encrypted Data Recovery Agents



NOTE: *Setting up an "empty policy" will turn EFS off, thereby not allowing users to encrypt files on computers that fall in that category. Setting up "no policy" (deleting policy) will allow the default local policy on computers to be used, in effect allowing local administrators to control the recovery of data on their individual computers.*

COMPAQ

Encrypt a File or Folder



COMPAQ

Encrypt File or Folder 2

COMPAQ

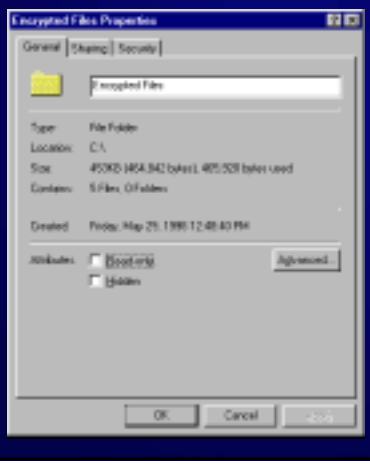
Cipher command line utility

- Examples:
- To encrypt the C:\My Documents directory, the user types:
- C:\>cipher /e My Documents
- To encrypt all files with “cnfdl” in the name, the user types:
- C:\>cipher /e /s *cnfdl*
- The complete cipher command supports the following options:
- D:\>cipher /?
- Displays or alters the encryption of files on NTFS partitions.
- CIPHER [/E | /D] [/S:dir] [/P:keyfile] [/K:keyfile] [/L:keyfile] [/I] [/F] [/Q] [filename [...]]
- /E Encrypts the specified files. Directories will be marked so that files added afterward will be encrypted.
- /D Decrypts the specified files. Directories will be marked so that files added afterward will not be encrypted.
- /S Performs the specified operation on files in the given directory and all subdirectories.
- /I Continues performing the specified operation even after errors have occurred. By default, CIPHER stops when an error is encountered.
- /F Forces the encryption operation on all specified files, even those which are already encrypted. Already-encrypted files are skipped by default.

COMPAQ

Encrypt a folder on local machine

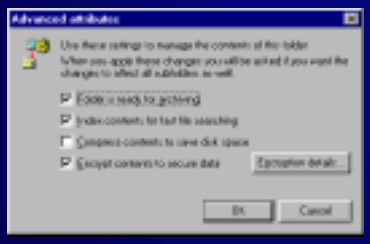
- Right-click on the selected folder to bring up Properties
- Click Advanced on the General Tab



COMPAQ

Encrypt a folder on local machine 2

- Select **Encrypt contents to secure data**.

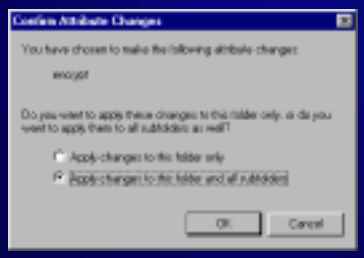


- Click **OK** to close the dialog box.
- Click **OK** to apply and close the property page

COMPAQ

Encrypt a folder on local machine 3

- A dialog box will prompt you to encrypt the folder only or all existing content.



COMPAQ

Encrypt a folder on a remote machine

- Use the Tools menu in Windows Explorer to map a network share on the remote machine as a drive.
- Once mapped, you can navigate to the folder as in the local case above.
- Follow the steps in previous example to perform the operation.
- Note that if the remote volume is not NTFS version 5, this operation will not be allowed.

- **NOTE**: *If the remote machine is a "trusted server" (trusted for delegation), EFS will be able to use the key from user's roaming profile so that same key is used across systems. If the remote machine is not "trusted", then a local profile is created on the machine and key is local to that machine and can be used on that machine only. Thus moving these files between machines would require you to move your keys also.*

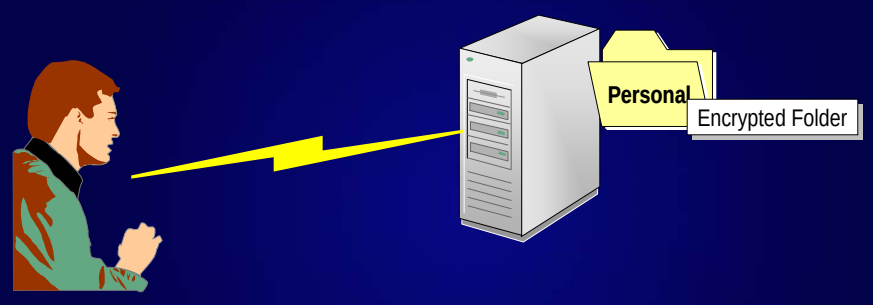
COMPAQ

Encrypted Files on Servers

- Must meet the following requirements:
  - Windows 2000 or .NET domain
  - The server's computer account must be trusted for delegation in Active Directory
  - NTFS file system
  - User must have an account in the Active Directory

COMPAQ

Encrypted Files on Servers



- User's profile exists on the remote server
- Server accesses profile using Kerberos delegation

COMPAQ

Encrypted Files on Servers

- Users' profile is obtained in one of two ways:
  - User's defined Roaming Profile is downloaded
  - Server generates a new local user profile
- Big gotcha
  - Must include user profiles in backup plans
  - If generated at the server, this is the only copy of the user's private key!

COMPAQ

Best Practices for Remote Encryption

- Include the full operating system and profile hives in your backup strategy
- Implement Roaming User Profiles
- Only implement the Trusted for Delegation option on selected servers
- See Q283223 – Recovery of Encrypted Files on a Server for more details
- See Q262797 - Reparse Point Support in Windows 2000-Based Clusters

COMPAQ
Inspiration Technology

Recovery Basics

COMPAQ

Defining a Recovery Policy

- Recovery Agent Policy
  - Defines one or more EFS Recovery Agents
  - Default is the “Administrator” account
    - The first administrator account on a member server / workstation
    - The administrator account on the first DC installed in a domain.
- Empty Recovery Policy
  - Disables EFS in Windows 2000
  - No Recovery Agent = No EFS
    - Apply in Group Policy to prevent local policy from taking affect

COMPAQ

Defining a Recovery Policy

- No Recovery Policy
  - Used in cases where security does not allow an EFS recovery account
  - EFS enabled locally and not defined Group Policy in AD environment
  - At local computer
    - Private key for DRA deleted

COMPAQ

Changing Between Policies

- If you decide to disable EFS, the following occurs:
  - Users can open (decrypt) previously encrypted files
  - Users cannot update encrypted files
  - Users cannot encrypt new files
  - Modified files must be saved in an unencrypted format

COMPAQ

Generating EFS Recovery Certificates

- Local Admin on first DC in the domain is auto-generated Recovery Agent
- Require a Windows 2000 or Windows .NET Server Enterprise Certification Authority (CA)
  - Change permissions for the EFS Recovery Certificate Template
  - Configure a CA to issue the certificate
  - Request the certificate with the recovery account

COMPAQ

Importing/Exporting Existing Certificates

- Can work with existing certificates and public/private keys
  - Whoever has the private key wins
  - Export the certificates using a PKCS #12 format (includes private key)
  - Delete the private key when exporting
  - Store the private key on a secure media in a secure location

COMPAQ
Inspiration Technology

Windows 2000 Standalone Scenarios

COMPAQ

This Scenario includes…

- Windows 2000/XP Computers in a workgroup
- Windows 2000/XP Computers in a Windows NT domain
- Windows 2000/XP Computers in a different Network environment

COMPAQ

Key Issues

- No centralized Data Recovery Agent
- EFS only supported on Windows 2000/Windows XP computers
  - Not supported for Windows XP Home Edition
- Local Administrator account is the recovery agent
  - Potential for disk editor attacks
- Reinstalls can result in loss of data
- No central key database for recovery

COMPAQ

Best Practices

- Always remove the DRA key from the computer and store separately
- Backup Users private keys and even consider removing from system
- Configure SYSKEY to require a boot floppy or password at startup

COMPAQ

Command Line Tool SYSKEY

- At the command line, type:
- syskey
- 2. Click **Encryption Enabled**, and then click **OK**.
- – or –
- Click **Update**, if encryption was previously enabled.
- 3. Select an option for the key.
- The default option is a system-generated password that is stored locally. If you use the password-derived startup key option, **syskey** does not enforce a minimum password length. However, passwords longer than 12 characters are recommended. The maximum length is 128 characters.
- 4. Click **OK** to restart the computer.
- When the system restarts, you might be prompted to enter the startup key, depending on the key option you selected. The first use of the startup key is detected and a new random password encryption key is generated. The password encryption key is protected by using the startup key, and then all account password information is strongly encrypted.
- After the startup key has been enabled, the following process occurs at system startups:
- · The startup key is retrieved from the locally stored key, the password entry, or insertion of a floppy disk, depending on the option you selected.
- · The startup key is used to decrypt the master protection key.
- · The master protection key is used to derive the per-user account password encryption key, which is then used to decrypt the password information in Active Directory or the local SAM registry key.
- The **syskey** command can be used again later to change the startup key storage option or to change the password. Changing the startup key requires knowledge of, or possession of, the current startup key.
- **To change the startup key option or password**
- 1. At the command line, type:
- syskey
- 2. In the first dialog box, click **Update**.
- 3. In the next dialog box, select a key option or change the password, and then click **OK**.
- 4. Restart the computer.

COMPAQ

Best Practices

- Replace DRA at installation with a central DRA
  - Use combination of Sysprep and the RunOnce option
- Be aware that a migration to a Windows 2000 or Windows .NET Server domain will change the recovery agent
- Get users to use strong passwords!

COMPAQ
Inspiration Technology

Windows 2000 Domain Scenarios

COMPAQ

The Default Scenario

- The Domain Administrator account for the domain is the default recovery agent
- More specifically
  - The EFS recovery private key is stored in the Administrator's local profile on the first domain controller installed in the domain
- EFS Recovery Agent is defined in the Default Domain Policy

COMPAQ

Best Practices

- Always make laptop computers a member of a Windows 2000 domain
- Encrypt folders such as the My Documents folder
- Enforce encryption through a combination of Group Policy, login scripts and security templates
- Configure Syskey to use passwords or startup disks

COMPAQ

Best Practices

- To selectively implement EFS encryption
  - Define EFS Recovery Agents at the OU level
  - Place computers in the OU that defines an EFS Recovery Agent
  - Implement an Empty Recovery Agent policy at the domain

COMPAQ
Inspiration Technology

Windows .NET Server Enhancements

COMPAQ

Data Recovery Changes

- Domain Model
  - Removed requirement for Data Recovery Agent
  - Can operate with no data recovery policy or a separate key recovery policy
  - Domain Administrator is DRA by default when domain is created
- Standalone and NT 4.0 Domains
  - No data recovery agent by default
  - Must be created manually “cipher.exe /R”

COMPAQ

EFS Enhancements

- Encrypted file sharing in the UI
- Encrypted files marked with alternate color
- Encrypted client side cache
  - Used for offline folders
  - Files are stored in encrypted CSC database
- Support kernel-mode FIPS-compliant cryptography
  - 3DES algorithm
  - Enabled through Group Policy

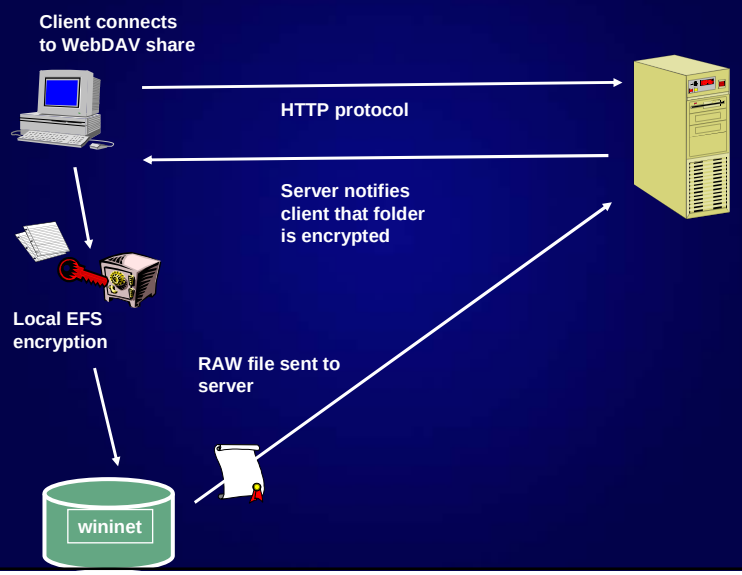
COMPAQ

EFS over WebDAV

- Enable encrypted storage on Internet servers – EFS integrated with WebDAV
- End to end encryption
- WebDAV is a file sharing protocol over HTTP
  - Alternative to SMB; Internet Standard RFC 2518
  - Supported by numerous ISVs
- IIS 5.0 and IIS 6.0 support WebDAV as web folders

COMPAQ

EFS over WebDAV



COMPAQ

PKI Enhancements

- User Auto-Enrollment
  - Configure auto enrollment for EFS Encryption Certificates
  - Allows for auto-renewal
- Key Recovery
  - Windows .NET Server CA allows archival of private keys
  - Only Certificates issued with v2 templates can be recovered
  - Data and Key Recovery can be combined

COMPAQ

Key Recovery Analysis

- Advantages
  - Users does not have to re-enroll for certificates
  - Existing certificates may not have to be revoked
  - All encrypted data can be opened by user
- Disadvantages
  - Key recovery is a manual process
  - Administrators can access a user's private key
  - Non-repudiation is not possible due to Administrator access to private keys

COMPAQ

Data Recovery Analysis

- Advantages
  - Does not require an existing PKI structure
  - Centrally managed using Active Directory
  - Can limit decryption to the user by removing the DRA's certificate
- Disadvantages
  - The DRA must be involved to recover an encrypted file
  - Recovery is performed on a file by file basis
  - No central management without Active Directory

COMPAQ

Best Practices for Key Recovery

- Always revoke certificates for a compromised key
- Define which private keys can be recovered
- Only recover keys after the original certificate is revoked
- Never archive certificates that are used for digital signing

COMPAQ

Windows XP Best Practices

- Operate in a domain environment!
- Use key archival with a Windows .NET Server CA
- File sharing works best in an Active Directory environment
- Windows XP does revocation checking on certificates
  - No CRL available, no EFS
- Do not use 3DES if in a mixed Windows 2000 environment
  - Unless all work is done on the server side

COMPAQ
Inspiration Technology

Tricks and Tips

COMPAQ

Determine if EFS is used

- Determine the existence of the following registry keys:
- Windows 2000
  - HKCU\Software\Microsoft\Windows NT\Current Version\EFS\CurrentKeys\CertificateHash
- Windows XP
  - HKCU\Software\Microsoft\Windows NT\Current Version\EFS\CurrentKeys\CertificateHash
  - HKCU\Software\Microsoft\Windows NT\Current Version\EFS\CurrentKeys\Flag

COMPAQ

Encrypt/Decrypt Menu Options

- To enable Encrypt and Decrypt on the Context menu
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
    - Name: EncryptionContextMenu
    - Type: DWORD
    - Value: 1
- Must restart Explorer

COMPAQ

Updating the DRA

- Windows XP Only!
- Update the DRF when the DRA is changed by using Cipher
  - Cipher.exe /U

COMPAQ

Potential For Clear Text

- Temporary files
- Page file
- Hibernation file
- Conversion of existing plain text files
  - Temp file created
  - NTFS may not overwrite original block
  - Cipher /W in Windows XP

COMPAQ

Clearing the Page File

- Ensures the pagefile is cleared at shutdown
- Prevents clear text memory fragments
- Set through local policy or group policy

Computer Configuration
Windows Settings
Security Settings
Local Policies
Security Options
Shutdown: Clear virtual memory pagefile

COMPAQ

Using 3DES Encryption

- Windows XP Only
- Increases strength of encryption from the default of DESX encryption
- Set through local policy or group policy

  Computer Configuration
  Windows Settings
  Security Settings
  Local Policies
  Security Options
  System Cryptography: Use FIPS compliant algorithms for encryption object

COMPAQ

For More Information

- Using 3rd Party CAs for issuing EFS and EFS Recovery certificates
  - Knowledge Base Article Q273856
- Encrypting File System for Windows 2000
  - http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/nt5efs.asp
- Best Practices for Encrypting File System
  - Knowledge Base Article Q223316

COMPAQ
Inspiration Technology

Questions?