


Lucent Technologies
Bell Labs Innovations 

The Knowledge Behind The Windows 2000 Encrypting File System

Bruce K. Marshall
brucem@lucent.com
Distinguished Member of Consulting Staff

Lucent Worldwide Services
The knowledge behind the network

Bruce K. Marshall, CISSP, MCSE

Lucent Technologies – Worldwide Services

brucem@lucent.com

913-338-5090 x114

Overland Park, KS

<http://www.lucent.com/services>

Background & Overview

- **Lucent Technologies Worldwide Services is a provider of communications consulting, intelligent maintenance, and performance management solutions for next generation networks.**
- **Session Objectives**
 - **Encrypting File System (EFS)**
 - **Data Management & Recovery**
 - **EFS Challenges & Risks**

5/19/01

2

Lucent Technologies
Bell Labs Innovations



Lucent Technologies Worldwide Services offers a number of services that assist you in optimizing and adding value to your IT environment. Take a glance at <http://www.lucent.com/services>.

Participants are presumed to have a basic understanding of how symmetric (secret) and asymmetric (public-key) encryption works. Familiarity with Windows 2000 terminology is also beneficial.

Data Theft is a Growing Risk



- **More sensitive data is stored locally.**
- **Computers are increasingly mobile.**
- **Access controls can be bypassed.**

5/19/01

3

Lucent Technologies
Bell Labs Innovations



Larger and larger hard drives fuel the temptation to store more information locally on your computer.

We are still obligated to ensure a 'halo' of security around our data even when it is disconnected from our network. The META Group estimates that within a few years 40% of computers in our organizations will be laptops. In 2000 Safeware reported that approximately 387,000 stolen laptop claims were filed (a 19% increase from their 1999 figures). While most of those thefts were probably focused on selling the hardware for a profit, loss or disclosure of the stored data is a real and serious threat.

Data access controls are typically only meaningful when that operating system (OS) is active to enforce the rules. Accessing the data outside of the OS's control is typically trivial. In the case of Windows NT/2000 you can simply boot to another OS or mount a hard drive on another computer to gain full access to all information.

Data Encryption Challenges

- **Level of protection**
- **Ease of use**
- **Data sharing**
- **Recovering encrypted data**
- **Cost**
- **Performance**

5/19/01

4

Lucent Technologies
Bell Labs Innovations



Protection: The security offered by the product is adequate for your needs.

Ease of use: Attempt to make the benefits of data encryption attractive to users by simplifying the process of encrypting and decrypting information. If these operations are too difficult users may find ways around using encryption features.

Data sharing: Key (or secret) distribution and management are traditional challenges of encryption technology. This problem rears its ugly head when you attempt to share encrypted data. Any user needing access to the encrypted data must be provided secure access to the keys as well.

Recovering encrypted data: While we are interested in assuring the confidentiality and integrity of corporate data, we are also obligated to maintain the availability of that same data. Another challenge of key management is making sure that the appropriate support personnel can access encrypted data without the user's cooperation. This is obviously a function that requires trusted personnel and a close relationship with your normal support processes.

Cost: You shouldn't spend more on a file encryption solution than it would cost you to deal with data theft and disclosure. This probably means you should orient your data classification policy with your encryption policy.

Performance: Modern day computer processing power has made this worry obsolete. However, keep it in mind when dealing with files in large quantities or large sizes.

W2K Encrypting File System (EFS)

- **Enhancement in NTFSv5**
- **A compliment (not a replacement) of W2K access control lists (ACLs)**
- **Allows reasonably good encryption of files**
- **Built with data recovery in mind**



5/19/01

5

Lucent Technologies
Bell Labs Innovations



The Encrypting File System (EFS) comes packaged with Windows 2000 Professional and Server. No extra parts or accessories are required, but an instruction manual would have been nice.

EFS should not be thought of as a replacement for ACLs. As we'll discuss, ACLs still play an important part in maintaining the integrity and confidentiality of your corporate data.

The key word is "reasonably" good. Microsoft certainly could have offered options for improving the strength of EFS encrypted files. But, as William H. Murray once said "If 56-bit, or even 40-bit DES, is your weak link, you are orders of magnitude more secure than anyone else in the world." Most attackers will prefer to steal the encryption keys rather than attempting to find them through brute-force attacks.

Microsoft did think about our need to recover encrypted data when designing EFS. Data recovery was built-in and enabled from the start. However, they gave greater priority to making EFS easy to use. We'll examine how this decision can make our job harder when trying to recover data.

EFS Requirements

- ✓ **NTFSv5 partition (and no compression)**
- ✓ **“Write” permissions to the file or directory (no System attribute)**
- ✓ **Valid digital certificate for EFS**
- ✓ **EFS recovery agent certificate**

5/19/01

6

Lucent Technologies
Bell Labs Innovations



EFS will not work on FAT or older Windows NT NTFS partitions. You cannot encrypt files on floppy disk, CD-ROM, or most types of removable media. Compression and encryption are mutually exclusive in Windows 2000. If you attempt to encrypt compressed files they will be uncompressed first. If you attempt to compress encrypted files they will be unencrypted first.

Unfortunately, Microsoft did not create a new NTFS permission that specifies who can encrypt a file. This could have saved us from some headaches. As it stands, a user only requires Write access (not Modify or Full Control) to encrypt data.

You cannot encrypt files with the System attribute set. This is primarily to keep your users from causing a self-denial-of-service from generous applications of encryption. Too bad autoexec.bat doesn't have the System attribute. Oops!

A “valid” certificate is one that is stored in the user's personal certificate store, includes an X.509v3 Enhanced Key Usage extension field containing the Microsoft EFS OID, and has not expired. The private key linked to an expired certificate can still be used for data decryption, just not new encryption. The certificate can be revoked however, as EFS does not check a certificate revocation list (CRL).

A recovery policy containing a self-signed EFS recovery agent certificate is created by default on every computer, so the final requirement is not tough to meet.

EFS Encryption Examined

A File Encryption Key (FEK) is the random, secret key uniquely generated for every encrypted file.

Key size w/o encryption pack: 40-bit

Key size with encryption pack: 128-bit

Encryption uses RSA Security's DESX algorithm.

5/19/01

7

Lucent Technologies
Bell Labs Innovations



Before encrypting a file, the EFS subsystem will create a random secret key (the FEK). This particular FEK is only used for encrypting a single file.

DESX was created by RSA Security as a variation of the Data Encryption Standard (DES) algorithm. This algorithm is said to be stronger than DES when subjected to a brute-force attack, as well as differential or linear cryptanalysis.

A 64-bit portion of the key, known as the whitening key is used to XOR the plaintext data. Then the 56-bit portion of the key is used with the DES algorithm for encryption of the XORed plaintext. Finally, another 64-bit whitening key (derived from a one-way hash function of the full 120-bit key) is used to XOR the resulting ciphertext.

Without the Microsoft high encryption pack (HEP) the key lengths probably stay the same but use only 40 distinct bits (meaning the other 80 bits are padded with 0's). A file encrypted using the HEP must also be decrypted on a computer with the HEP.

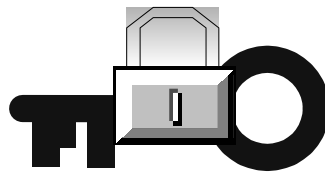
Microsoft's claim (in their Encrypting File System for Windows 2000 white paper) of a 128-bit key size for EFS is puzzling. The standard DESX algorithm specifies the use of a 120-bit key.

Certain Commerce Dept. export restrictions apply to using the high encryption pack outside of North America. The Microsoft high encryption pack can be downloaded at: <http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp>

Encryption Key Management

EFS uses public-key technology for FEK management.

The encrypted FEK is stored in the Data Decryption Field (DDF) of the encrypted file.



5/19/01

8

Lucent Technologies
Bell Labs Innovations



The public key, contained in the EFS certificate, is used to encrypt each FEK. The private key (held only by the user) is used to decrypt the FEK.

The Data Decryption Field (DDF) also contains the user's distinguished name, security identifier (SID), and thumbprint of the EFS certificate containing the associated public key. This allows EFS to quickly determine if a user has the appropriate private key to decrypt a file. The DDF also allows administrators to identify the individual who encrypted a file.

While Windows 2000 supports more than one DDF per file, you cannot add other DDFs through the GUI. Because of this Microsoft generally states that Windows 2000 does not support sharing encrypted files.

However, you can share the credentials needed to encrypt and decrypt a set of files. To do so would involve making the same certificate and private key available for every user wanting access to the encrypted data. In most environments this quickly becomes unmanageable.

Sources of EFS Certificates

- **Self-signed certificates**
 - 100-year validity period
- **Windows 2000 Enterprise CA-issued certificates (EFS or multi-purpose)**
 - 1-year validity period
- **Third-party certificates**
 - Variable validity period

5/19/01

9

Lucent Technologies
Bell Labs Innovations



How an EFS certificate is initially obtained is actually pretty important. Because once EFS will not normally change certificates (or keys) until the existing certificate expires. If you want to manually switch the credentials used for EFS read Microsoft Knowledge Base article Q273856 or use *cipher /k*.

When you implement a Windows 2000 Enterprise CA (by installing Certificate Services) it automatically grants EFS certificate enrollment permissions to the Domain Users group. A user's computer will request an EFS certificate on the user's behalf from an Enterprise CA the first time the user attempts to encrypt a file. When the certificate expires EFS will create a new private/public key pair and request a new certificate.

Certificates used for EFS are also published into the AD as an attribute under the user's Published Certificates tab. (Note: You can't see the Published Certificates tab unless Advanced View is turned on in the MMC.) This feature has no purpose in Windows 2000, but is used for encrypted file sharing in Windows XP (Whistler).

Companies like Entrust and Baltimore now offer PKI solutions that create EFS-compatible certificates. These same solutions can allow you to choose your own custom certificate validity period. However, they can not offer the same functionality for automatic certificate enrollment or renewal.

The EFS Certificate Key Pair

- **Certificates and keys reside in the Personal Certificate store**
- **Certificate store resides in a user's Windows 2000 profile**
- **Private key is exportable**
- **Cannot be stored on a smart card**

5/19/01

10

Lucent Technologies
Bell Labs Innovations



Certificates and private keys are encrypted fairly well for storage. It is infeasible that an attacker would ever have success conducting a brute force attack against the encrypted private keys.

However, storage in profiles means that the user's certificates and private keys are typically only protected by their logon password. This is usually the weak point in protecting access to encrypted data, especially if you aren't using domain accounts.

Roaming profiles add portability to EFS credentials. Otherwise a profile is limited to the computer it was created on. A new profile (and potentially EFS credentials) will be created on every other computer the user logs on to.

This will prevent you from being able to access files encrypted while logged onto one computer when you are logged onto a different computer (without roaming profiles). Using mandatory profiles also prevents the use of EFS.

An EFS certificate is one of the few certificates issued by a Windows 2000 CA that allow the keys to be marked as exportable by default. This allows you to copy a user's EFS credentials and move them to another machine (or archive them).

EFS From a User's Perspective

- **A certificate and key pair are obtained upon the first use of EFS.**
- **Files or folders can be encrypted using Windows Explorer or Cipher.**
- **Decryption transparently occurs during subsequent reads and writes.**

5/19/01

11

Lucent Technologies
Bell Labs Innovations



The private/public key pair are created locally. The private key never leaves the computer. The public key may be sent to an Enterprise CA along with other information in the form of a certificate request. A user shouldn't notice much difference (except for a slight delay) between obtaining a CA-issued or self-signed certificates.

To encrypt a file using Windows Explorer the user views the file/folder Properties, the Advanced properties, and selects the "encrypt contents to secure data" box. The user will be prompted whether they want to also encrypt the parent folder (if encrypting a single file) or all subdirectories and files (if encrypting a directory).

Using the cipher command line utility, a user types `cipher /e /s /a [pathname]` to encrypt a directory, all subdirectories, and files.

Best practices dictate encrypting only folders and then creating or copying files to be encrypted within those directories. This simplifies encrypted file management. If multiple partitions are available, you could also encrypt all directories on a drive (be aware of the limitations of this configuration).

If another user attempts to access an encrypted file they get an "Access is Denied" error message. They are not prevented from listing encrypted files. They can even delete encrypted files if they have proper permissions.

EFS Key Recovery

- **The Encrypted Data Recovery Agent (EDRA) policy contains one or more EFS File Recovery certificates.**
- **A second copy of each FEK is encrypted with the RA's public key.**
- **The RA's encrypted FEK is stored in the file's Data Recovery Field (DRF).**

5/19/01

12

Lucent Technologies
Bell Labs Innovations



The EDRA policy is applied to computers, not users or groups. A W2K Active Directory Group Policy Object (GPO) or a Local Security Policy can specify the data recovery agents. Within these policies, the setting is defined at *Computer Configuration \ Windows Settings \ Security Settings \ Public Key Policies \ Encrypted Data Recovery Agents*.

A policy is defined when a valid certificate is placed into the policy store. Multiple certificates can be placed in a policy to define multiple recovery agents. In the case of multiple certificates, multiple DRFs will be created for all encrypted files.

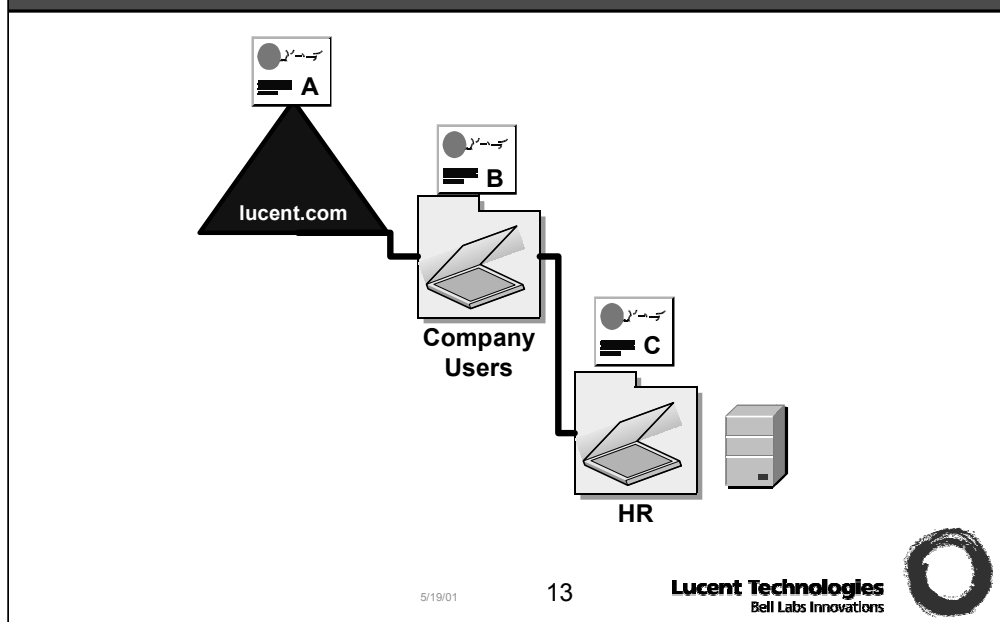
EFS File Recovery certificates are obtained from a Windows 2000 Enterprise CA. The ability to request these certificates is initially restricted to Domain Administrators. You can create an EFS Recovery Agent (RA) group and assign enroll right to that group. Keep in mind that a File Recovery certificate alone is useless. A certificate is placed in a policy, the policy is refreshed on the computers, and from that point on any files encrypted or accessed can be decrypted using the RA's private key.

An "empty" policy is different than "no" policy. Empty policies specify that EFS should be disabled. Microsoft has published two Knowledge Base articles on configuring empty policies on local computers and in a domain: Q222022 & Q243035

By default a unique EDRA policy is initialized on every Windows 2000 computer the first time the local Administrator account is used. The RA certificate in the policy is self-signed and the associated private key is stored in the local Administrator personal certificate store. This RA certificate has a validity period of 100 years.

The DRF will be checked against the current EDRA policy upon any access of the encrypted file. If the recovery agent has changed, the old DRF will be replaced with a DRF containing the new information.

Data Recovery Policy Example



In addition, an EDRA policy is specified in the Default Domain Policy object in the Windows 2000 Active Directory. The RA certificate in this policy is also self-signed and the associated private key resides in the domain Administrator account personal certificate store. However, the private key for this certificate can only be accessed by logging on as the Administrator from the first domain controller (DC) in the domain. This RA certificate has a validity period of 4 years instead of 100.

EDRA policies follow the normal Windows 2000 policy application process: Local – Site – Domain – OU. So, a domain EDRA policy will override a local computer EDRA policy. However, these policies are not accumulative. The last policy processed will set the effective RAs.

In the example above, a computer in the HR OU will only use the EDRA policy containing recovery agent C's certificate. If you needed A, B, and C to all act as recovery agents for the HR OU you would need to place each RA's certificate in the same HR EDRA policy.

Who acts as encrypted data RA may be a very politically sensitive decision in your organization. Your industry may also have legal requirements for managing data. Policies and procedures should be carefully developed with collaboration between the data custodians and the data consumers. Consider creating recovery agent and EDRA policy logs to offer an audit trail.

Recovering Encrypted Data

- 1. User's computer / User's credentials**
- 2. User's computer / RA's credentials**
- 3. RA's computer / RA's credentials**

5/19/01

14

Lucent Technologies
Bell Labs Innovations



The first scenario will normally occur if a user leaves the company or is terminated. You would disable their user account and take possession of their computer. Later you could change the account password, enable the account, log on as the user, and decrypt their data normally. The data could then be transferred to the appropriate department or manager.

The second scenario should only occur if the user loses access to their EFS private key. The appropriate EFS RA could export their File Recovery certificate and private key to floppy disk, log onto the user's computer, load their certificate/private key (or use a roaming profile), and decrypt their data. A RA should always delete their credentials off the machine after this operation. The user would then need to obtain a new EFS certificate and re-encrypt the data. Because of the increased exposure to the EFS RA's credentials I generally don't recommend this method of recovery.

The third scenario would again be used when access to the user's private key is lost. However, in this case you would transport the encrypted data to the recovery agent for decryption at a specially dedicated recovery computer. You could send the entire hard drive or back up the data in the encrypted format and send it electronically. This provides increased protection for the EFS RA, but introduces added inconvenience for the data owners.

Situations Requiring Recovery

- **Corruption of the user profile**
- **Deletion of the user profile**
- **No access to the user profile**
- **Deletion of the private key**

5/19/01

15

Lucent Technologies
Bell Labs Innovations



A user's profile is stored in the `\Documents and Settings\%username%` directory and loaded into the `HKEY_CURRENT_USER` registry subtree when they are logged on. If this directory, or user data stored within this directory, is damaged you may be unable to load the user's certificates and private keys.

The user profile will be deleted if you reformat a computer and fail to back up this data. Simply reinstalling the same OS shouldn't cause you to lose access to the profile, but I would manually back up the certificates/private keys to be certain.

You will lose access to a user profile if you delete the account associated with the profile. Creating a new account with the same username will not allow you to regain access since the profile is associated with the user's SID. There is no known ways of taking over orphaned profiles.

A user's access to their roaming profile may be temporarily lost if they cannot communicate with the server hosting their profile.

If the user, or someone else with access to the user's profile, deletes the private keys you will not be able to decrypt data. It may be possible to restore access to private keys if you have a backup of the user's profile.

Recovery Challenges

“47% of deployments involve Windows 2000 Professional only.”

-- GIGA/Sunbelt Software 02/2001 (1118 respondents)

Do you:

- **Turn off EFS?**
- **Export recovery agent credentials from every machine upon installation?**
- **Accept the risks of lost data?**

5/19/01

16

Lucent Technologies
Bell Labs Innovations



Turning off EFS is the simplest solution, but may not serve the needs of your users.

Without a Windows 2000 Active Directory domain you won't be able to easily apply EDRA policies. Each machine will start out with a local policy using the unique EFS File Recovery certificate associated with the local Administrator account. You will probably have to visit each computer individually to turn off EFS or export the Administrator RA certificate/private key. Or you may find some way to script a solution if you want to enable a secure enterprise policy for recovering data.

Keep in mind that the local computer accounts are at a much greater risk when it comes to accessing encrypted data. Because local accounts are stored in the local System Accounts Manager (SAM) database, attacker can manipulate this file. Tools exist that will hack or change the local Administrator account password. A person could then log on as the Administrator and change the logon password of any other local accounts. At this point they can simply log on as that user to gain access to private keys and thus the encrypted data.

When your computer and user accounts belong to a Windows 2000 domain, the local Administrator account can't manipulate the domain user account passwords. This makes the job of an attacker much tougher if they want to decrypt data.

Recovery Management Challenges

- **Restoring data may require multiple recovery agents**
 - **Files encrypted over time**
 - **Files encrypted on computers subject to different EDRA policies**
- **Efsinfo is an essential utility to identifying the proper RA.**

5/19/01

17

Lucent Technologies
Bell Labs Innovations



When a file is encrypted the current policy specifies the recovery agent. If that policy changes, the encrypted file will not be updated with the new recovery agent certificate until the next time it is accessed. This could result in the need to have multiple sets of RA credentials available when you attempt to recover encrypted data.

Also keep in mind that recovery policies do not follow users, they only pertain to computers. So a user might have to contact different RA personnel for file recovery depending on where they encrypted the data.

If you're relying on the self-signed local EFS RA credentials, good luck identifying the right RA. Make sure you keep good track of which credentials are associated with which computer. The RA name will show up as "Unknown". The only useful efsinfo output will be the certificate thumbprint.

Efsinfo can be purchased as part of the Windows 2000 Server Resource Kit. EFSDump is a fairly similar utility that can be obtained (along with source code) at <http://www.sysinternals.com/ntw2k/source/misc.shtml#EFSDump> . Unfortunately, EFSDump doesn't display certificate thumbprints.

Identifying Encrypted Data RAs

The screenshot displays a Windows Explorer window titled "E:\My Secure Documents". The file list includes "Executive Compensation.xls" with an "E" icon in the Attributes column. The file's properties are shown below the list: "Executive Compensation.xls", "Microsoft Excel Worksheet", "Modified: 2/19/2001 8:01 AM", "Size: 20.0 KB", and "Attributes: Encrypted". A red circle highlights the "Encrypted" attribute. Below the Explorer window is a Command Prompt window showing the command `efsinfo /u /c /r execut~1.xls` and its output:

```
E:\My Secure Documents>efsinfo /u /c /r execut~1.xls
E:\My Secure Documents\
Executive Compensation.xls: Encrypted
Users who can decrypt:
  INSMASTER\marsha_b <OU=EFS File Encryption Certificate, L=EFS, CN=marsha_b>
  Certificate thumbprint: 1871 CF84 9AF4 C7AD B193 81CC 5CCB 8F36 ED93 FC1B
Recovery Agents:
  Unknown <OU=EFS File Encryption Certificate, L=EFS, CN=Administrator>
  Certificate thumbprint: D4DE 5347 98FD DF22 DCD3 D76C F6B3 BC65 D63C F6B1
```

At the bottom of the screenshot, the date "5/19/01", the page number "18", the "Lucent Technologies Bell Labs Innovations" logo, and a circular graphic are visible.

You should make some effort to educate users on how to tell if their files are really encrypted. If the Windows Explorer Web content is turned on (which it is by default) they can see the encryption status by highlighting a file. If the Windows Explorer file Attributes column is visible (which it isn't by default) the user will see the "E" attribute for all encrypted files.

The Command Prompt window shows the result of running `efsinfo /u /c /r` on an encrypted file. The encryption status, user who performed the encryption, and file recovery agent are all displayed. The certificate thumbprints for the user and RA can both assist you in finding the right certificate/private key for file decryption.

When planning file recovery you would want to run `efsinfo` on all the encrypted data to verify that you have access to the appropriate RA credentials for decryption.

Can You Trust Your Admins?

Any user that can edit a GPO can implement an EDRA policy.

- 1. Restrict access to EFS File Recovery certificate enrollment.**
- 2. Limit who can edit GPOs.**
- 3. Audit GPO properties regularly.**
- 4. Maintain those ACLs!**

5/19/01

19

Lucent Technologies
Bell Labs Innovations



Most organizations will want to limit who has access to encrypted data. However, if you start delegating the ability to create Group Policy Objects you give these same administrators the right to change the encrypted data recovery agent policy.

If you are using a Windows 2000 Enterprise CA you can make sure that only authorized users or groups can enroll for the EFS File Recovery certificate. However, this is not foolproof. Any certificate containing the proper characteristics and issued from a trusted CA (or self-signed) can be placed in the EDRA policy.

As a normal rule you would want to restrict who has access to both editing and assigning GPOs to containers in the AD. The EFS recovery policy is a good example of why this is important. Consider centralizing the GPO management function while letting business units submit requests for changes or modifications.

If you must delegate the ability to create GPOs, make sure that you conduct regular checks to ensure the settings conform with corporate policy. The EDRA policy settings can be checked to see if any unauthorized certificates have been added.

Even if a user has the RA credentials to unencrypt a file, they cannot do so without adequate NTFS permissions (specified with ACLs). So, you may want to deny access to encrypted files for the RA groups or users. This helps ensure that they are working with other authorized personnel during the data recovery process.

EFS Data Exposure

- **Unintentional decryption**
- **Network transfers**
- **Printing**
- **Memory and page files**
- **Encryption temp files (efs0.tmp)**
- **Working temp files**
- **Synchronized offline files**



5/19/01

20

Lucent Technologies
Bell Labs Innovations



The #1 challenge will be making sure that users don't accidentally unencrypt files and overlook their mistake. Establishing simple, standardized encryption practices and educating end users are your best weapons in combating this problem.

When transferring or encrypting data on servers, the files travel unencrypted over the network. Data is likewise exposed in cleartext when sent to print spoolers or printers. Consider using IPSec to encrypt communications or maintaining a dedicated network for secure work.

Files are unencrypted in memory when you work on data. This means that the paging file (pagefile.sys) or hibernation file (hiberfil.sys) may contain unencrypted confidential data. Applications can create temp files when you open an encrypted file. Generally these temp files are also encrypted, but not all applications create temp files the same way. This may result in encrypted data exposure.

When encrypting an existing file a temporary file (efs0.tmp) containing the unencrypted data is created for crash recovery. This file is erased after successful encryption, but the file contents are not securely wiped from the hard drive. Sophisticated attackers may be able to access encrypted files by reading the file remnants off of the hard drive directly. Search the www.securityfocus.com Bugtraq archives for details.

Using folder redirection data can appear local but actually reside stored on a file server. This data can also be encrypted. However, when you synchronize data for offline use it is stored unencrypted in the %systemroot%\CSC\ directory.

EFS and Virus Protection

Virus protection software on server and desktops cannot scan encrypted files.

Files are only scanned when read into memory.

Vendor solutions forthcoming..?



5/19/01

21

Lucent Technologies
Bell Labs Innovations



I was unable to find any mention of this problem when searching the Web sites of major virus protection software vendors.

You may be able to work around this problem by creating an extra set of RA credentials and putting them in your EDRA policy. The certificate and private key for this RA could be imported into the service account used to run the virus protection software. This may allow the software to unencrypt and scan the files. I have not tested this configuration and will make no guarantees.

Alternatives to EFS

- **RSA Security – Keon Desktop**
- **PGP Security – Corporate Desktop**
- **PC Guardian – Encryption Plus**
- **I/O Software – SecureFolder**
- **INV Softworks – Kryptel**

5/19/01

22

Lucent Technologies
Bell Labs Innovations



- PGP Corporate Desktop – <http://www.pgp.com>
- RSA Security – Keon Desktop – <http://www.rsasecurity.com>
- PC Guardian – Encryption Plus – <http://www.pcguardian.com>
- I/O Software – SecureFolder – <http://www.iosoftware.com/>
- INV Softworks – Kryptel – <http://inv.co.nz>

Keep in mind the issues of: Protection, ease of use, data sharing, recovering encrypted data, cost, and performance. Each product will have its own unique pros and cons in these areas.

Outlook for EFS (Windows XP/2002)

- **Encrypted file sharing**
- **Colorized encrypted files**
- **Customizable EFS certificate validity periods**
- **Synchronized file encryption**
- **Cipher /U**
- **Additional encryption algorithms**

5/19/01

23

Lucent Technologies
Bell Labs Innovations



Since Windows XP & 2002 is still under development these comments are only predictions and may not reflect the final product release.

Encrypted data can be shared among multiple users. This will be accomplished by maintaining a file DDF for every user requiring access to the encrypted data. How well this will work in practice is yet to be seen.

Encrypted files can appear in a distinct color within Windows Explorer (much like compressed files can appear in blue today). This will do wonders for allowing users to quickly and easily determine whether a file is encrypted or not.

Certificate Services will include customizable certificate templates. This means you can create EFS and EFS File Recovery certificates that last longer than a single year.

Offline file synchronization should now allow the locally cached files to be encrypted.

The cipher /u command will search all system partitions for encrypted files and automatically update the DDF and DRF of encrypted files with the current user and RA certificate info.

Microsoft has added support for the triple DES (3DES) encryption algorithm.

Keys For Success



- **Plan (Interim)**
- **Learn & Educate**
- **Collaborate**
- **Plan (Long-term)**
- **Test**
- **Document**

5/19/01

24

Lucent Technologies
Bell Labs Innovations



Create a plan to match your data availability needs and support model. This helps to prevent accidental data loss or political problems pertaining to recovery agent personnel.

Learn as much as you can about how EFS works and what features are useful or harmful in your environment. Network with your counterparts in other organizations to share lessons learned. Read the EFS white paper at www.lucent.com/services.

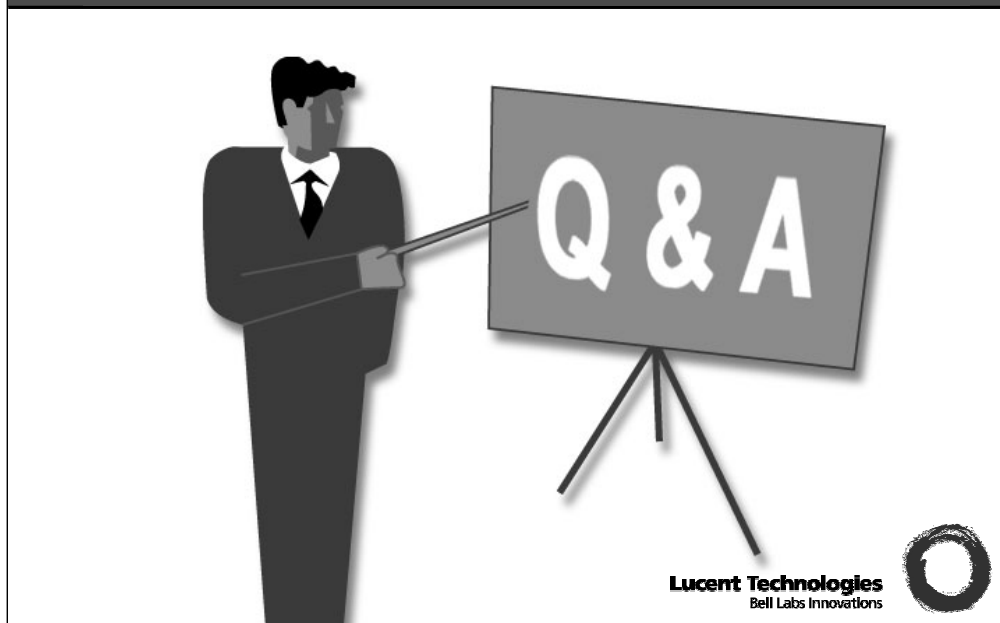
Collaborate with your peers, business units, and partners on the promises and pitfalls of EFS. Come up with a corporate strategy for where EFS makes sense and where it doesn't. Consider third-party solutions where necessary.

Use the requirements you've assembled along with your knowledge of how EFS can be supported in your organization. Put together a plan to implement EFS that works for you.

Test your proposed EFS infrastructure in a pilot. Find out how your users will react to this new functionality. You're bound to learn something new about EFS while refining your deployment strategy.

Document your plans, user guidelines, support processes, and policy changes. This documentation will be worth the work to ensure consistent use and incident handling.

Questions and Answers



Recommended resources for learning more about EFS:

[How to Back Up Your Encrypting File System Private Key](#), Microsoft Knowledge Base (KB) article Q241201

[Best Practices for Encrypting File System](#), Microsoft KB article Q223316

[Encrypting File System for Windows 2000](#), Microsoft white paper,
<http://www.microsoft.com/windows2000/library/unzippeddocs/encrypt.doc>

Deployment Planning Guide, Windows 2000 Server Resource Kit, Microsoft Press

Distributed Systems Guide, Windows 2000 Server Resource Kit, Microsoft Press

[Hardening EFS](#), Roberta Bragg, Information Security magazine,
www.infosecuritymag.com

[The Encrypted Data Recovery Policy for Encrypting File System](#), Microsoft KB article Q230490