Windows 2000's Encrypting File System

EFS is a new feature which provides a fast and transparent way to secure files. Only the user who encrypted the files can obtain access to them, but carefully-designed safeguards are provided.

By Dave Cook
Consultant And Journalist

To the average Administrator, plotting a solid security strategy can be a frustrating business. Think of all that time and effort spent building those much-needed perimeter defences, strong user authentication, permissions and so forth - and then look what happens. Once authenticated, your users are free to wander at will, with access to every file and folder inside any shared resource available on the network. Thankfully, Windows 2000 provides a solution in the shape of a new NTFS-based security feature called the Encrypting File System (EFS). EFS encrypts files using the Extended Data Encryption Standard (DESX) technology, which makes use of strong public key encryption to provide Administrators and their users with totally transparent, on-disk file encryption.

Unlike other cryptographic solutions, files can be accessed and saved without users having to bother or even be aware of the fact that they are encrypted. Users simply work with encrypted files and folders just as they do when using unencrypted data. Windows 2000 takes care of the rest, automatically decrypting the file or folder when the user accesses it, and then re-encrypting the data when the user is finished working with it.

Basically, EFS works like this: each encrypted file possesses a unique File Encryption Key (up to 128-bit FEK), and this is later used to decrypt the file's data. In turn, the FEK is in itself encrypted using Public Key Cryptography System (PKCS) technology, and protected by the user's public key corresponding to the user's EFS certificate. Hence, a user can decrypt the file only when he or she has a private key that matches the public key. If handled correctly, EFS can be highly secure. If the encryption algorithms are sound, and the methods used to secure the encryption keys are conducted with the utmost care, then security of the data is virtually guaranteed.

Safeguards

Users can encrypt files and folders under their authority in such a way that only the person who encrypted the data can open it again. If another user tries to access the encrypted file, the system displays an "Access Denied" message. What this means, of course, is that your users need to be aware of their responsibilities when encrypting files, because losing a password (or a user, for that matter) can mean losing access to an encrypted file forever. With care, however, this should never happen because, in addition to encrypting the FEK with the user's key, EFS also encrypts the FEK using a public key. This key is assigned to an account designated as the Data Recovery Agent (DRA) which, in a domain, is the Administrator's account. The DRA account enables trusted Administrators to access any files and folders that have been encrypted by their users.

The identity of the DRA in domains is specified by group policy. Called the File Recovery Policy, it provides each machine with the identity of at least one DRA to use when encrypting files. Standalone machines use local policy to hold this information. These policies are automatically created when users encrypt a file for the first time; without this group or local policy, or if a DRA has not been listed in the policy, then EFS will be unable to encrypt files. Before users go about encrypting and decrypting files and folders, Administrators need to ensure they have Read / Write access rights to the folder. An Encrypted Data Recovery Agent policy must also be in effect, with at least one DRA on the list. The DRA is selected automatically depending on the domain affiliation of the machine. For example, the

default DRA for a standalone machine running Windows Professional is the Admin account; the default DRA for a standalone server is the Administrator account; the default DRA in a domain is the domain Administrator account.

Usually, there are several accounts with Administrative privileges, so loss of the Administrative account is not normally disastrous. However, with EFS employed in a domain, losing the Administrator account also means losing the ability to recover encrypted files. Therefore it is important to add another DRA account immediately after EFS is enabled. This can be achieved with the help of the Add Recovery Agent wizard, which can be accessed from the group policy linked to the domain (see Figure 1).

Encrypting A Folder

By default, EFS uses standard, 56-bit encryption. Although 128-bit encryption is available in some countries, files encrypted to that standard cannot be decrypted, accessed or recovered on a system that only supports 56-bit encryption. Encryption can be performed either from Windows Explorer or by using the Cipher command-line alternative. Most users are likely to prefer the former option, so for the purpose of this example we shall encrypt the My Documents folder using Windows Explorer. Note, however, that roaming profile users may not be able to encrypt this folder. This is because the system does not normally permit encrypting the contents of a roaming profile.

To begin encrypting the My Documents folder (obviously you may choose to create a special new folder for this purpose instead), launch Windows Explorer and navigate to the folder in question. Right-click the My Documents folder, select Properties from the fly-out menu, and click Advanced on the General tab in the Folder Properties dialog box. Now check the Encrypt Contents To Secure Data option (see Figure 2). When selecting this option, observe that it is not possible to select both this and the Compress Contents To Conserve Disk Space option. Click OK to accept the Property change. If the Confirm Attribute Changes window appears, select Apply Changes To This Folder, Subfolders, and Files. Selecting this option ensures that all the contents of the My Documents folder, along with any subfolders the user may create later, will be encrypted from the very beginning. It also prevents the system from leaving any unencrypted temporary files. To encrypt the folder (whether or not the Confirm Attribute Changes windows appears), click OK. There will be a short delay while the affected files are encrypted, and then the Properties dialog box closes.

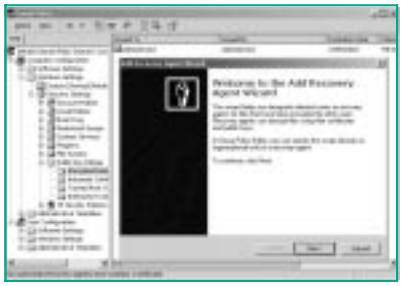

Figure 1 - Adding another Data Recovery Agent.

It really is that simple. There are no messages to confirm encryption, although the length of time involved in this process depends to a large extent on the machine's capabilities and the size of the folder. Once encrypted, renaming such files will not affect their encrypted status in any way. Even if the files are moved or copied to another folder (NTFS), regardless of that folder's encryption properties, they retain their original encryption properties. Alternatively, if an unencrypted file is moved into an encrypted folder, then that file will remain unencrypted. That is because it is not actually the folder that is encrypted, but rather the files contained within the folder.

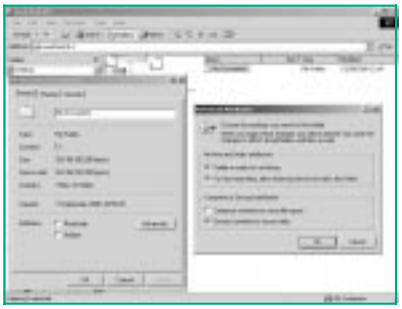

Figure 2 - Encrypting the My Documents folder.

In order to recover encrypted files, the user could log onto the computer as the DRA and then decrypt the files. For reasons of security, however, the user should not normally have access to the certificate and private key. In which case, the user can back up the encrypted files to be recovered - using Backup or a similar backup utility - and transfer the backup files to the designated DRA (usually the Administrator). The DRA can then decrypt the files using the recovery agent's own recovery certificate, before transferring the files back to the user.

Networking

Special attention is needed when using encrypted files over the network. For example, if a remote server is used to store encrypted files, be aware that the files are only secure when stored on disk and not when they are in transit across the network. Encryption cannot take place directly over the network because that would expose the file to possible interception. Other protocols, such as SSL/PCT or Internet Protocol Security (IPSec) must be used to encrypt data over the wire.

When a user encrypts or decrypts a file at the local level, EFS obtains the encryption keys from the user's EFS certificate. With a server, the process is slightly different. True, a server can obtain a copy of the user's access token, but it must also obtain access to the user's master key. Although this key is encrypted along with the user's password details, it is not available to the server. Hence, the server needs to obtain the user's master key from a domain controller on behalf of the user. This is achieved via a Kerberos ticket, issued from the client and marked as "forwardable", which allows the ticket to be passed on to the domain controller. This process is called delegation. Even so, be aware that a server must be configured as Trusted For Delegation before it will permit its network users to encrypt files.

While the Trusted For Delegation option is enabled on domain controllers, it is disabled by default on all non-domain controllers and desktops. Indeed, there is a good argument for leaving it disabled, since the alternative can mean leaving these machines open to Trojan horse attacks. That said, in the real world it is almost impossible to set up any successful implementation of EFS without enabling this option on at least one server. Otherwise users would be forced to save encrypted files to local drives only, which is a risky business as they could easily be damaged or wiped out completely. To enable the Trusted For Delegation option for a server, log on using an account with Administrator privileges over the trusted server's Computer object. Select Start, Programs, Administrative Tools and open the Active Directory Users And Computers snap-in. Expand the tree to the container storing the computer account - by default, this should be CN=Computers, and DC=<domain> - and open the Properties window for the computer. Now check the Trust Computer For Delegation option.

At this point, the system will warn Administrators that this act should not be performed indiscriminately, since trusting the computer for delegation is a security-sensitive operation. Before selecting this option, therefore, it is important that Administrators have taken all steps necessary to ensure that the server is protected as thoroughly as any domain controller. Click OK to acknowledge this fact and return to the Properties window. Then click OK to apply the change, and restart the computer.

To test the configuration, log on at a client and map the NTFS drive to a shared folder on the server by right-clicking My Computer and choosing Map Network Drive. From the list of available local drive letters, select the drive to be mapped as the remote drive, and type in the network path and drive letter for the remote computer (or click Browse and select the remote computer and drive). Select Reconnect At Logon and click Finish to map the drive as specified. The user should now be able to encrypt a file in that shared folder. If the encryption option is not displayed, it

"Files can be accessed and saved without users having to bother or even be aware of the fact that they are encrypted."

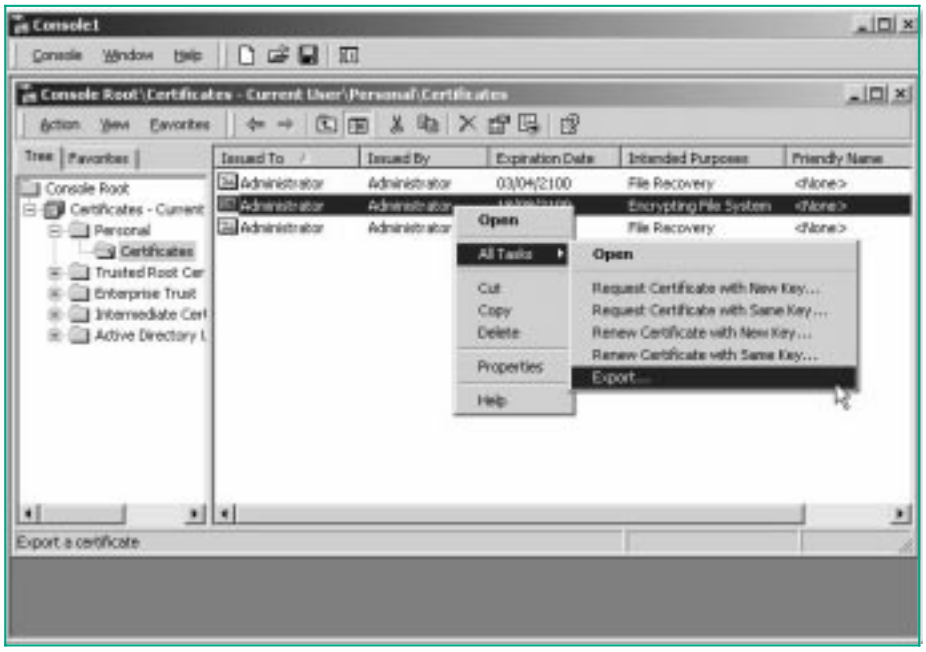

Figure 3 - Exporting a File Recovery certificate.

could be that the volume is configured as FAT or FAT32 and not NTFS. If the problem persists, check that both the client and the server have been restarted and are in contact with a domain server.

Caveats

So far we have discussed some of the benefits and safeguards of EFS. There are, however, several points that Administrators need to be aware of when introducing this feature to the organisation. Bear in mind that it is not possible to encrypt system files or compressed files, and note that users must use the Copy and Paste commands to retain encryption when moving files into an encrypted folder. Moreover, try to avoid using FAT volumes. An encrypted file is likely to become decrypted if it is copied or moved to a FAT partition. Temporary work files can also cause security hazards. A variety of programs create these temporary files, and they can easily compromise the organisation's file encryption security. To protect against problems of this nature, encrypt all Temp or Temporary folders so that any such files are automatically encrypted.

Whenever possible ensure that files are protected at the folder level instead of simply encrypting each file individually. For instance, the My Documents folder should be used if this is where users save most of their data. New files should then be created in that folder. In this way encryption occurs naturally, as files are saved without leaving exposed remnants spread all over the place. Also, due to potential frailties in the local SAM and Admin / Administrator accounts, be aware that file encryption on machines such as laptops and standalone desktop PCs may not be totally secure. It is important, therefore, that Administrators remove the File Recovery certificate from standalone machines in particular to help prevent encrypted files from being compromised. The best way to do this is to export the File Recovery certificate and the master key to a certificate that can be saved to a floppy (or burned to a CD). The certificate can then be safely removed from the standalone machine. It can, of course, be imported back temporarily when it is necessary to perform a file recovery.

One way to export a File Recovery certificate is to open the Certificates console at the computer currently holding the EFS certificate and then expand the tree to Certificates - Current User, Personal, Certificates. Right-click the Encrypting File System certificate and select All Tasks, Export (see Figure 3), which will fire up the Certificates Export Wizard. Click Next to open the Export Private Key window, select Yes, Export The Private Key, and click Next again to open the Export File Format window. If required, select Delete The Private Key If The Export Is Successful. Then click Next, type a password, and provide an appropriate name for the certificate in the File To Export window. Click Next, click Finish, and close the console. At this point, a file containing the user's certificate can be found in the root directory. Copy this file to a safe place, so that it is ready to be imported back to the machine if and when required.

Security can be further enhanced if all desktop machines using EFS are networked to the domain, thereby ensuring that only the domain DRA is used. It is also a good idea to save and remove the File Recovery certificate from the initial domain controller. This effectively blocks any unauthorised users in the domain from obtaining a copy of the File Recovery certificate.

Conclusion

The process of setting up EFS could not be easier. Once an option has been set in the file or folder's Properties window, files are encrypted within seconds, with users continuing to work on encrypted files as though they were like any other file. As always, however, the devil is in the detail. In particular, Administrators must pay close attention to recovery keys and policies. For example, store File Recovery certificates in a safe place, importing them back to the computer only when needed. The importance of these certificates cannot be over-emphasised. Without them, it will not be possible to recover encrypted files should the inevitable happen and the user either leaves the company, or simply loses his or her encryption certificate and associated private key.

PCNA

Further Information

Cryptography FAQ, including DESX
www.rsasecurity.com/rsalabs/-faq

Internet Draft of DESX standard
www.alternic.org/drafts/-drafts-s-t

Details of PKCS workshops etc
www.rsasecurity.com/rsalabs/-pkcs

MS guide to EFS
www.microsoft.com/WINDOWS2000/library/planning/security/-efssteps.asp

MS guide to Kerberos authentication
www.microsoft.com/WINDOWS2000/library/howitworks/-security/kerberos.asp

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.