

## Re: efs and "encryption" overall... help?

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2004-10/0562.html>

---

**From:** Miha Pihler (*mihap-news\_at\_atlantis.si*)

**Date:** 10/14/04

Date: Thu, 14 Oct 2004 20:24:38 +0200

<snip>

> *but what good is this if the certificate is stored on the same drive? im sure it*

> *could be obtained and used to decrypt files if the drive was removed.*

Private key is encrypted in user's profile. User's profile is protected with user's password. You have to "physically" logon to the profile to get access to private keys that will decrypt the files. There is no known reliable way to break this protection of private keys if you don't know the password to access the profile (if you don't believe me, check the WindowsXP newsgroup with people asking how they get their files after they lost their profiles...)

If users use strong — hard to guess passwords keys are safe on the hard drive.

Even if you backup the files on NTFS (EFS only works on NTFS) and restore the files to FAT or FAT32 you won't get your encrypted files. From the backup you will get the list of files where size of each file will be 0 (empty file)...

If administrator changes user's password and then logons to users computer with his username and password he won't be able to read user's documents that were protected with EFS since password change was done in the "forceful" way. If user changes his password this won't be a problem...

If you decide to implement the EFS, be smart about it and have a very good plan. Plan should include how to recover data if user loses his profile/private key... Implement Recovery Agent before you implement EFS.

Above solution is based on self signed certificate. You can also look at setting up your own CA and issuing EFS certificate on this CA server.

Check this article on Microsoft website on EFS. Also read the documents mentioned in this article...

Encrypting File System in Windows XP and Windows Server 2003

microsoft.public.windows.server.networking: Re: efs and "encryption" overall... help?

<http://www.microsoft.com/technet/prodtechnol/winxpro/deploy/cryptfs.mspx>

Mike