

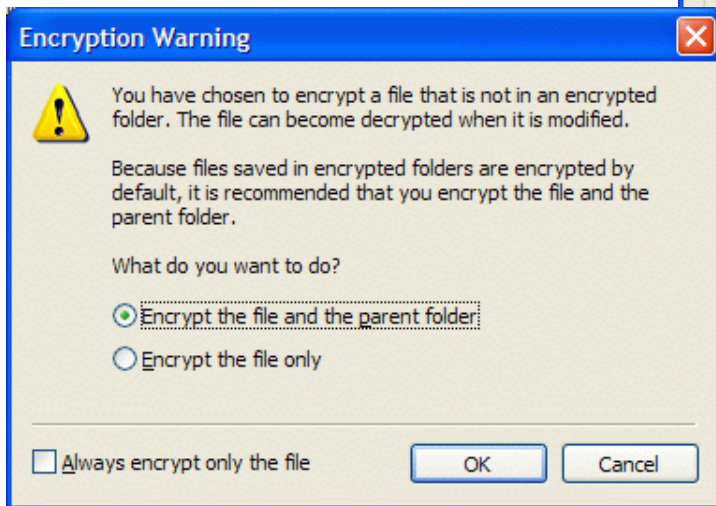
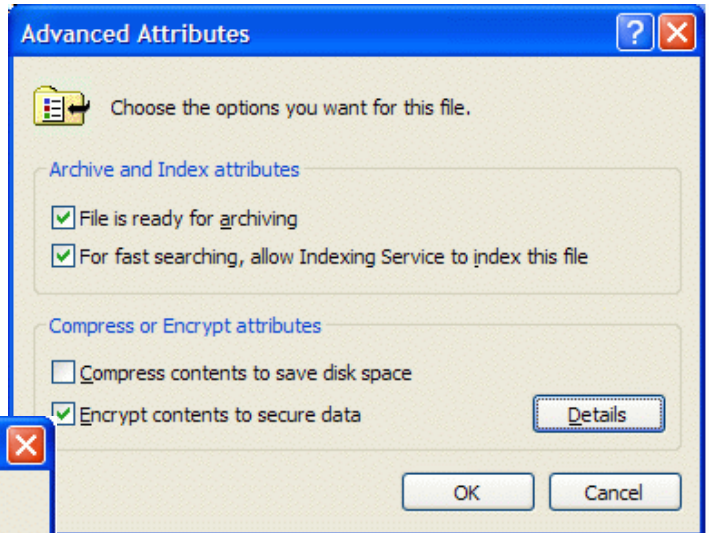
Using EFS in Windows computers

**Using TrueCrypt to protect your USB thumb drives**

# Using EFS

You can invoke EFS encrypting features of Windows2000 Professional and above through Windows Explorer. To use Windows Explorer to encrypt file, open File property window by right clicking on file name. Click **Advanced...** button - Advanced Attributes dialog will be opened allowing you to mark file as encrypted.

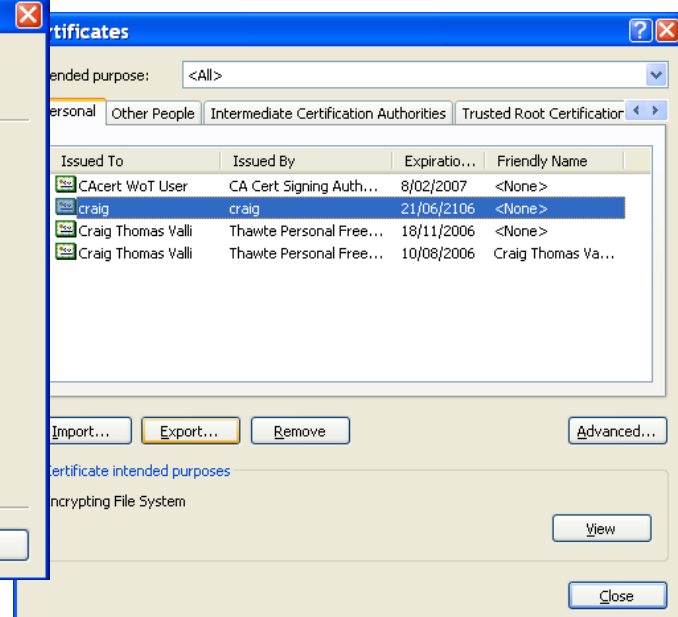
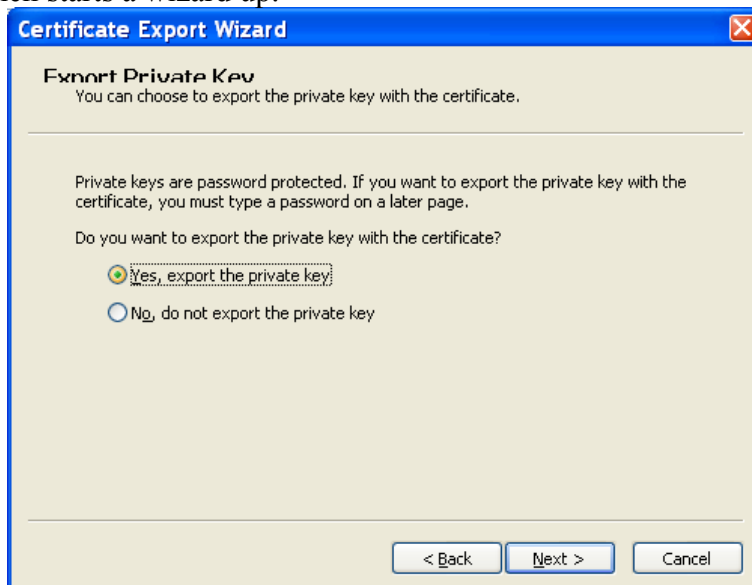
Before saving new settings Windows will prompt user to encrypt file only or the whole folder. It address very important issue - while the file itself could be perfectly protected, the application which opens the file may create a temporary copies of the file while working with the document. The example is Microsoft Word. When user opens encrypted document, EFS decrypts it transparently for Word. Then during the work, Word creates temporary hidden file where it automatically saves the document in the process of editing and deletes it on the exit. This hidden file presents a real breach in security because it contains user data in plain (not encrypted) form. Encrypting the **whole folder** instead of file only solves this problem.



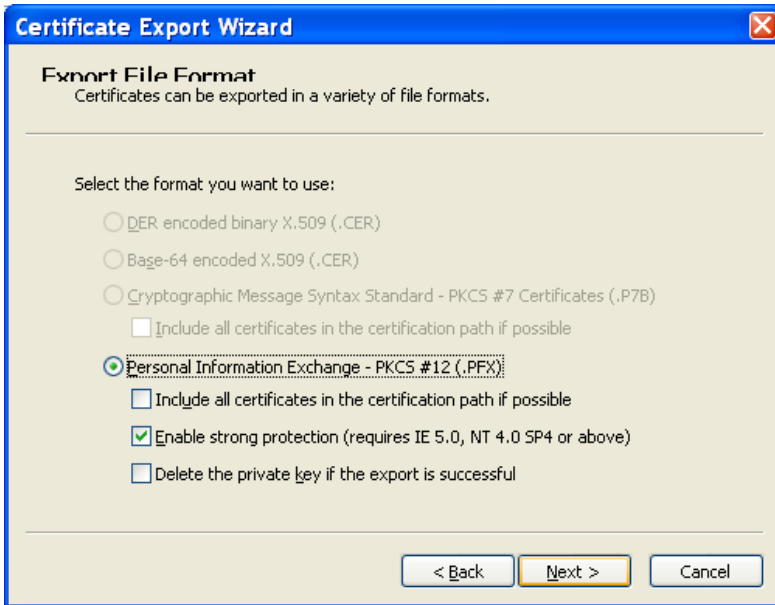
Also make sure that you back up to some other media your actual private key from your machine and store them in a safe place on safe media preferably a CD.

If you do not backup your private key you will not be able to recover files should something go wrong with your underlying operating system and say you had to re-install Windows.

To backup your private keys do this open Internet Explorer the Select **Tools, Internet Options, Content, Certificates**. Then select the certificate with your login name on and select **Export**. This then starts a wizard up.



Then select the **Yes export the private key options**.

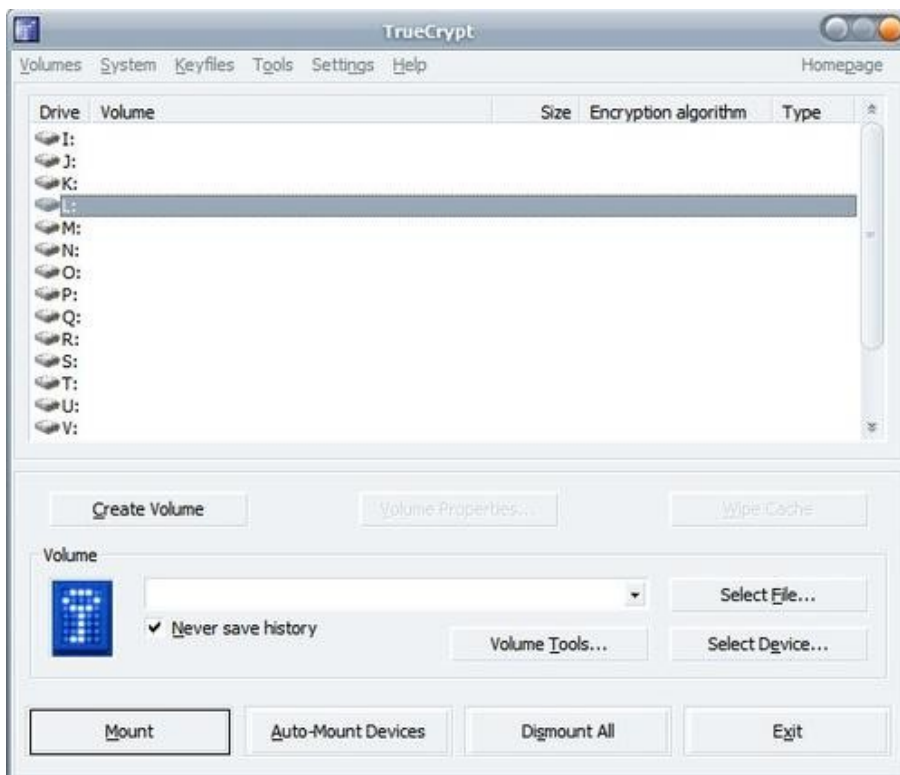


Then select **Enable strong protection**. Then select **Next** you will then be prompted to enter a password...do not forget this. Then select a location and a file name and save the file. Burn it to CD or some other reliable media and store in safe place.

## Using TrueCrypt to protect your USB thumb drives

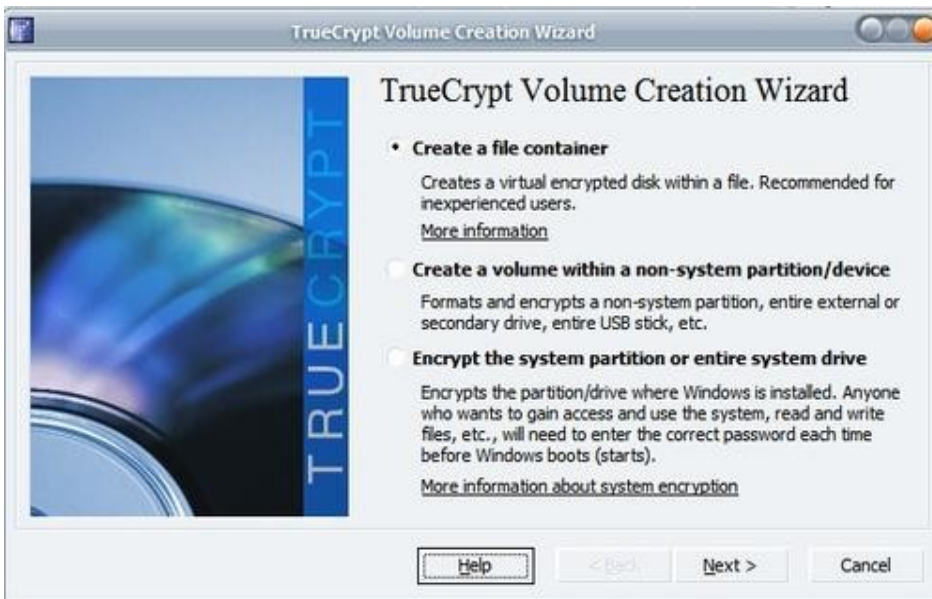
You obviously need True Crypt for this guide, the latest available is from [www.truecrypt.org](http://www.truecrypt.org) Download and install the software as usual and start it afterwards. You will also need truecrypt on all machines you are using. Its runs on all major platforms Linux, Windows and Mac OS and transparently so.

The main True Crypt window will load and look like the following:

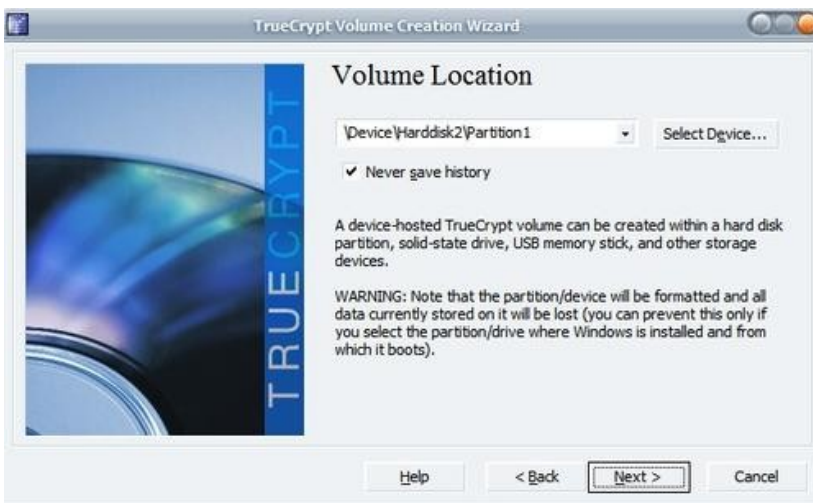


You obviously need to make some decisions before you continue. This guide will encrypt the full USB drive.

Click on the Create Volume button in the lower left corner. A window will appear asking about the type of volume that you want to create.



The choices are to create an encrypted container, encrypt a partition / drive or encrypt the system partition (the one running Windows). We are going to create a volume within a non-system device and check the second option in that screen. The next window gives us the choice to create a standard or hidden True Crypt volume. Hidden volumes are created in standard volumes. The reason is to give up only the standard password and not the password for the hidden volume when someone forces you. We are creating a standard volume therefore.



Now we are selecting the device that we want to encrypt, in our case the new USB drive. Next in the line are the encryption options.

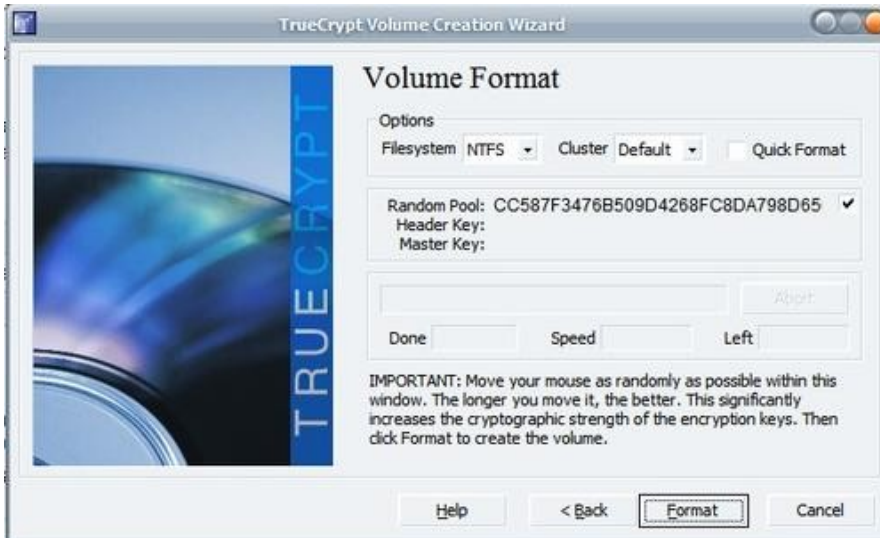


Which encryption and hash algorithm are you going to use. My selection was AES and SHA-512. You can run benchmarks in that window and get additional information about each algorithm. All algorithms are secure (unless someone proves otherwise, which has not happened yet)



The Volume Password is the most important part. You access your files with it and if you happen to forget it your files are lost. Make sure you use a large string, something that is not a dictionary word and not a combination of them. A password should be at least made of 20 characters and be made of upper and lower case chars, numbers and special chars. The maximum amount of chars is 64. A keyfile can be created as well which then works in combination with the password but for our purposes password is best.

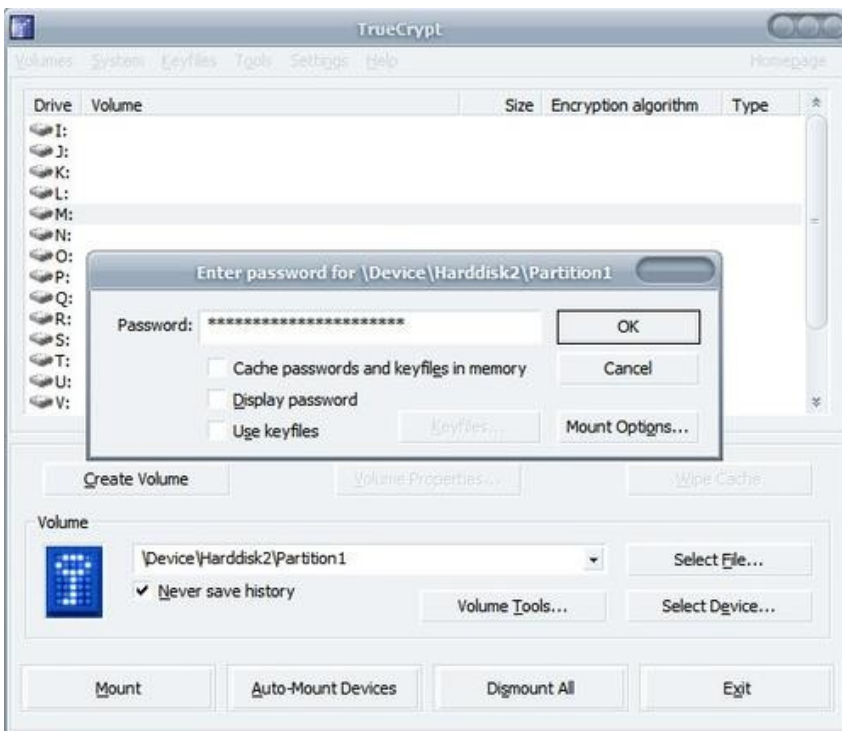
The drive will be formatted in



the end. You need to move your mouse randomly around the screen for some time to improve the quality of the encryption keys. The file system should and cluster size can remain as is unless you need them to be different. Using Quick Format since there have not been any files on the USB drive previously. The process is finished after this step. You need to mount the drive now to be able to use it.

## Mounting your encrypted USB drive

Select a drive letter currently not assigned and click on Select Device afterwards in the main menu. Now select the partition or drive that you have encrypted and click on ok.



Now click on Mount which opens up a password box where you have to enter the password that you have selected during setup. Click ok afterwards and work with the hard drive normally from there on if the password was correct

**IMPORTANT NOTE** If you place a truecrypt encrypted drive in a normal machine it appears as a drive that needs formatting ...don't format it... otherwise..

☺...💣\*....☹