How to create a portable encrypted USB Key using TrueCrypt

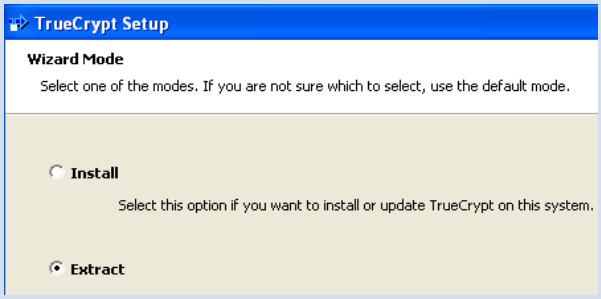
INTRODUCTION

TrueCrypt 'Traveler Mode' provides secure encryption for programs/files on portable devices such as USB Memory keys. It uses strong encryption for storage, and results in secure file storage that is highly portable, and can be backed up safely without compromising security.

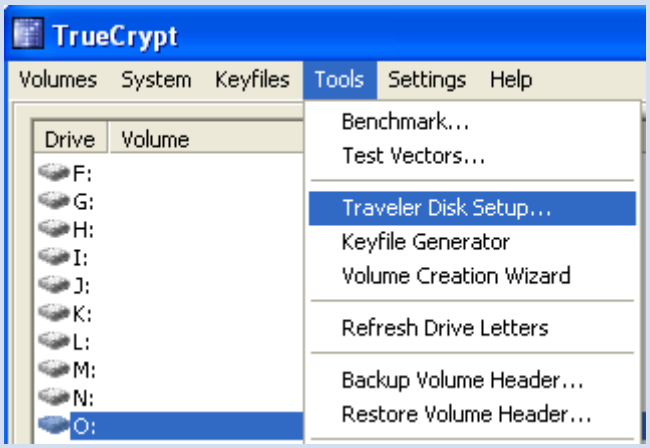
INSTRUCTIONS

To create an encrypted USB memory stick we perform the following steps:

- ✓ Install and configure the required software on a blank USB Stick (steps 1-4)
- ✓ Create an encrypted file that acts as a secure file container (the encrypted drive)on the USB drive. (steps 5-12)
- ✓ Create a backup of the encrypted drive password header (for backup in case password is lost)- This is VERY IMPORTANT. (next section)

Step	Action	
1.	Download TrueCrypt 6.0 www.truecrypt.org Double-click on exe. File or desktop shortcut. Choose **Extract** to unpack the files. Connect your USB key and backup and delete all current contents.	
2.	Browse to the extracted file area and double click the **trueCrypt icon**.	

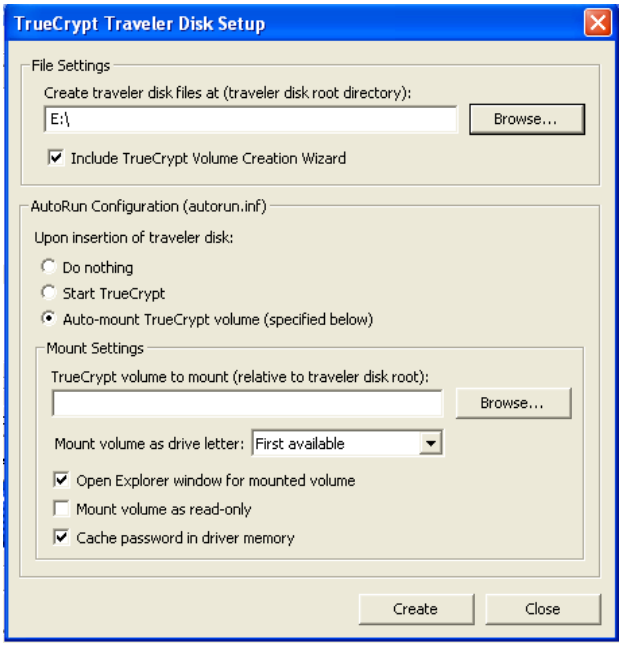
3. Go to **Tools** and choose **Traveler Disk Setup** from the drop down menu.



4. To set up USB key to support traveler mode, use **Browse** to choose your USB key drive letter. In this example the drive is E:\

Other settings you should use are:

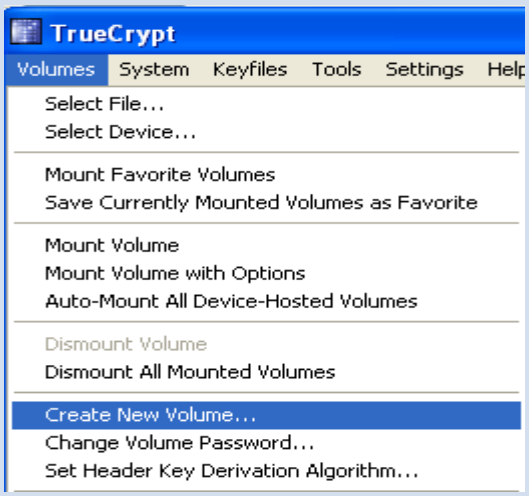
- ✓ **Auto-Mount volume** (you must specify here the proposed name of your truecrypt volume e.g. secure_drive_file) **Note the filename (you'll need to reenter it later)**
- ✓ **Open Explorer window for mounted volume-** this is convenient when you connect a drive.
- ✓ **Cache password in driver memory** this means that you only need to enter the drive password



once while the key is connected.

Click **Create.**

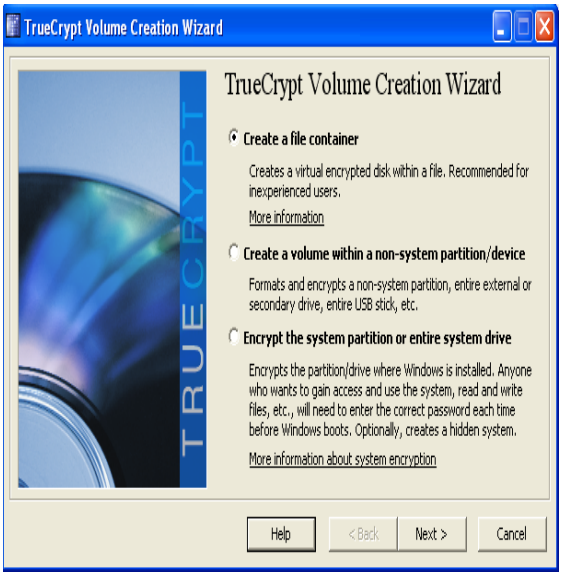
5. To create a new volume Select **Volumes** from the menu and **Create New Volume…**



6. Select **Create a file container.**

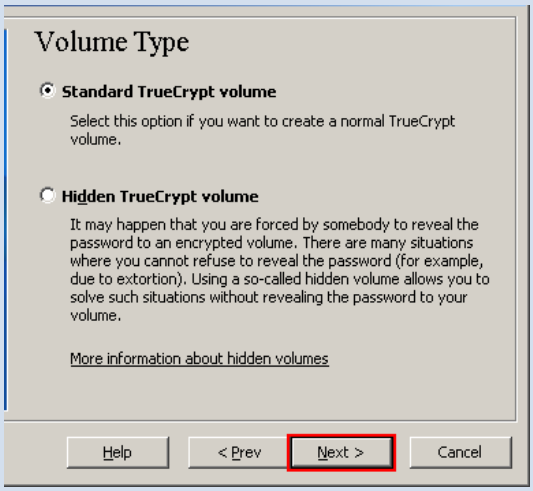
Note: This approach creates a file that is used by Truecrypt to provide a secure storage space for other files. It is fixed in size, and we recommend that it occupy 90% of the available space on the drive.

Click **Next.**



7. Select **Standard TrueCrypt volume.**

Click **Next.**

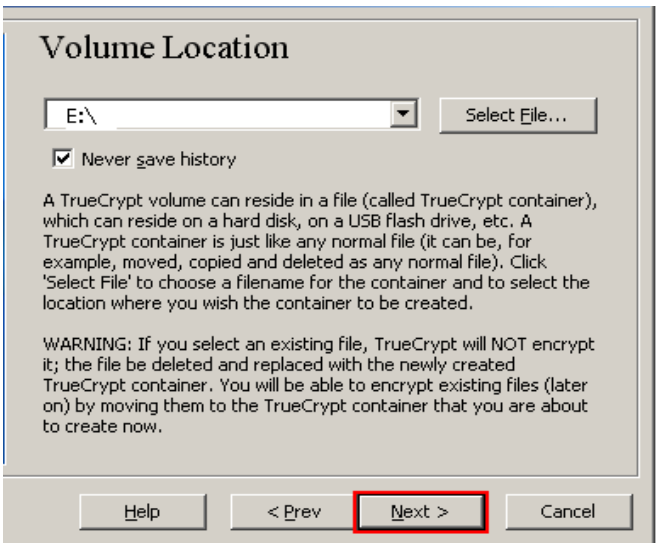


8. Hit **Select File** and enter your USB location i.e. E:\

Name the file the same as the filename specified in step 4 and hit **Save**

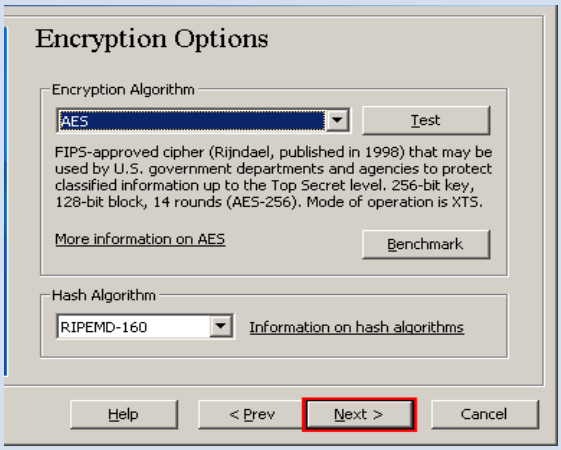
Warning: Do not select existing files - Truecrypt will not encrypt any existing file, if selected, existing files will be overwritten and lost.

Click **Next.**



9. Select **AES** from the drop-down menu.

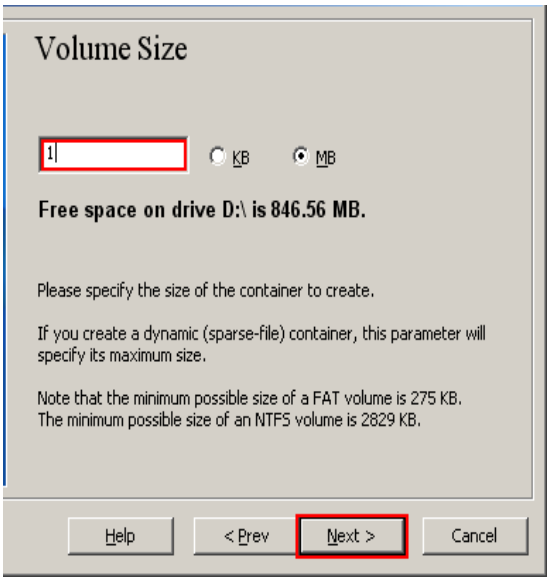
Note: AES (Advanced Encryption Standard) is recommended for two reasons. First, it's the fastest algorithm of the available options, and it's the encryption standard recommended by the US Government for commercial use; and has been certified for use on US classified documents.



Select the default Hash Algorithm.

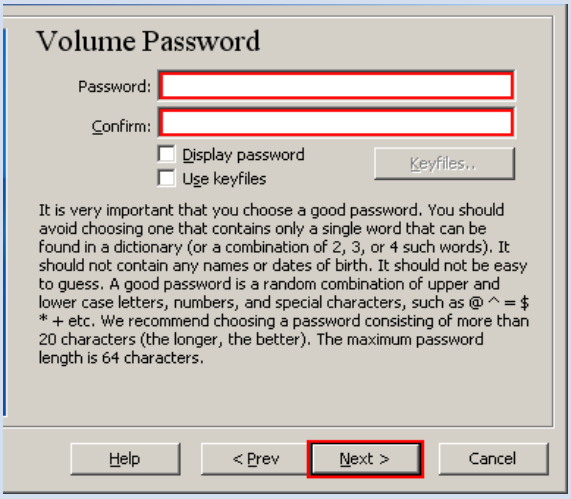
Click **Next.**

10. Specify the size you want to allocate to the TrueCrypt container – we recommend that you leave about 10% of available space free for technical reasons.



Click **Next.**

11. Choose a strong volume password and confirm it.



Click **Next.**

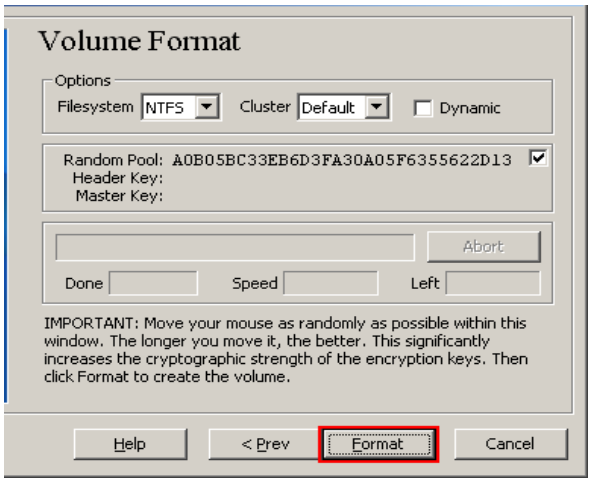
12. To generate the Header and Master Key, Move the mouse randomly within the window for at least 30 seconds.

The longer you move the mouse the better, as it increases the strength of keys used for encryption.

Click **Format** to create the TrueCrypt Volume.

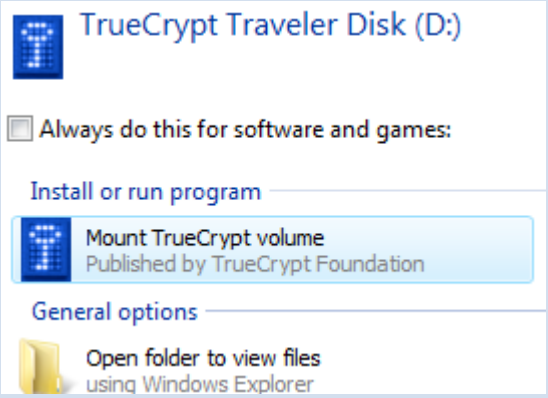
Depending on the size of container file, this step may take several minutes.

This is the final step to create a Truecrypt USB key.



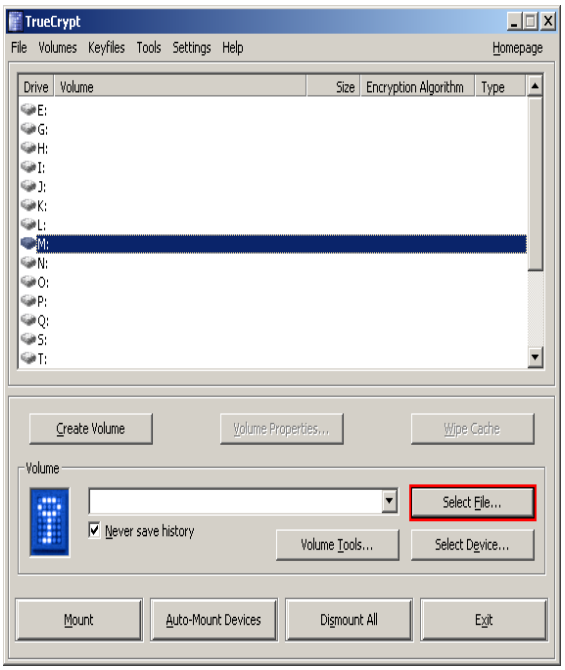
To use the newly created key, quit Truecrypt, remove the USB key and reinsert it. Autoplay will give you the option of running truecrypt, and you will be prompted for your password.

Truecrypt will mount two disks- the open area of the disk containing the software, and a new drive which has the capacity of the encrypted file created earlier. All files placed in this container are encrypted.



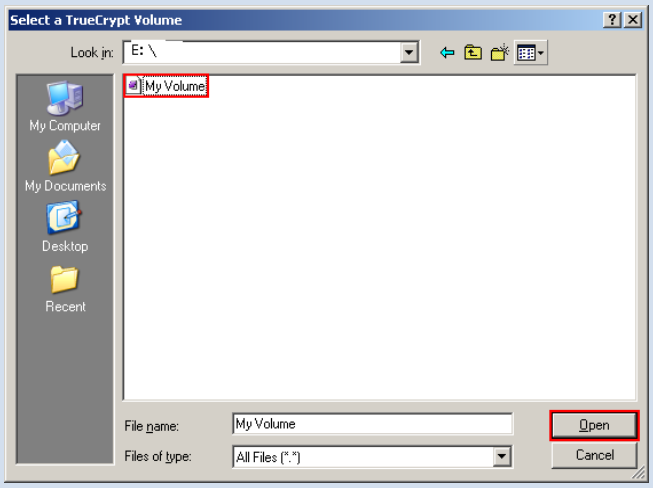
Note: If autoplay doesn't work, run truecrypt when the drive is connected, and go through steps 13-17

13. Choose a Drive to use in this case we Select Drive **M:**



Click on **Select File.**

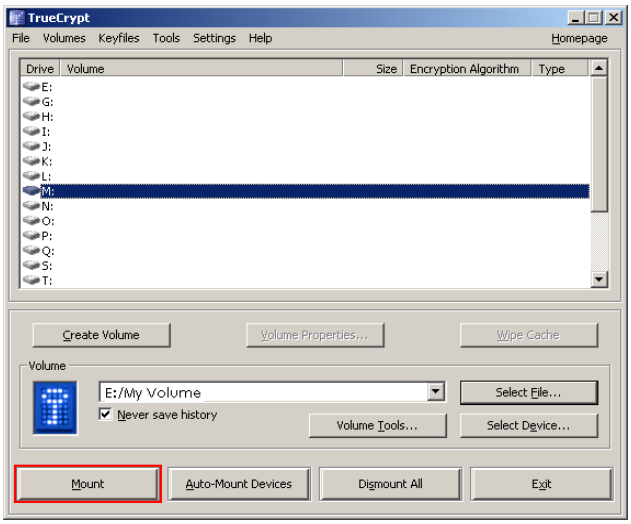
14. In the file selector browse to your USB drive and select the **container file** - ('My Volume' file you previously created).



Click **Open.**

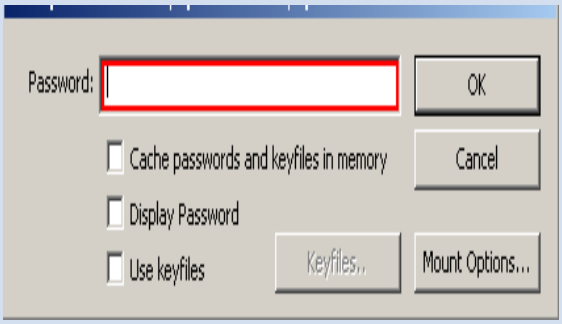
15. Go to the TrueCrypt main window and choose a drive letter to which the TrueCrypt Container will be mounted.

Click **Mount.**



16. Enter the **password** you created in step 11.

Click **OK.**



17. The USB key is now mounted in a container on a drive M.

*For more information on how to **use TrueCrypt** visit the TrueCrypt Website @ www.truecrypt.org*

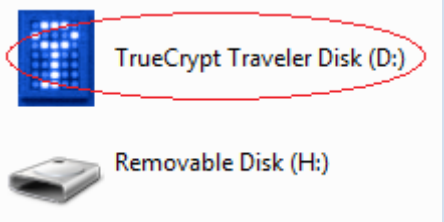
BACKING UP THE DRIVE AND KEY FILES.

The encrypted file password cannot be recovered if forgotten. For this reason, it is a very good strategy to create a backup key file with a known password to be kept safely elsewhere (this is a small file, so you can email it to yourself for example, just don't send the password with it). The steps for this are detailed below.

You should also consider that material held on the USB key, though it can't be read, may be lost. Anything you hold on such a key should also be held somewhere else. In this case you can simply copy the encrypted file container to another computer or disk you have available (the file will almost certainly be too big to email!).

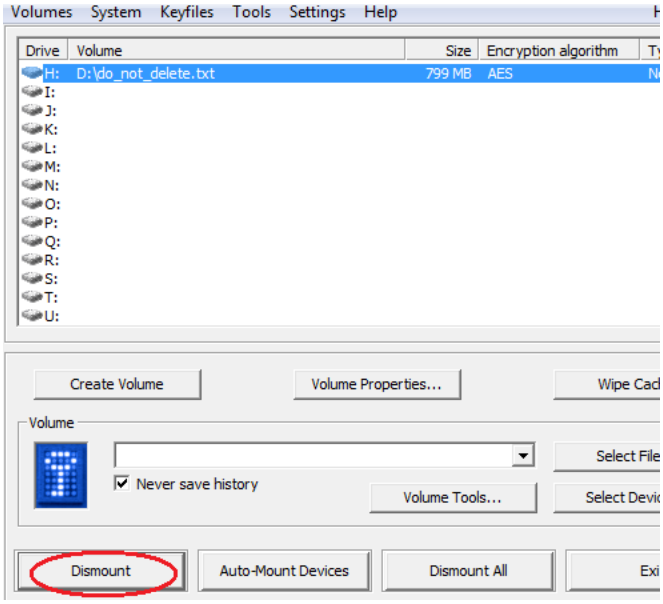
Step	Action

1. Browse the Truecrypt Drive (it has the truecrypt Icon), and run truecrypt.exe. Note that the encrypted drive is a separate drive letter (in this case H:)

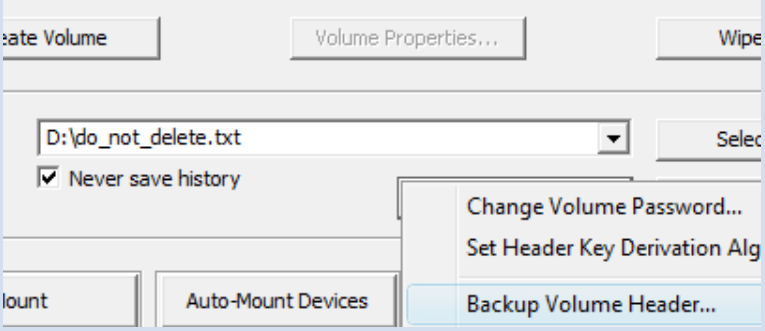


2. Click to select the encrypted drive, and click on **Dismount-**

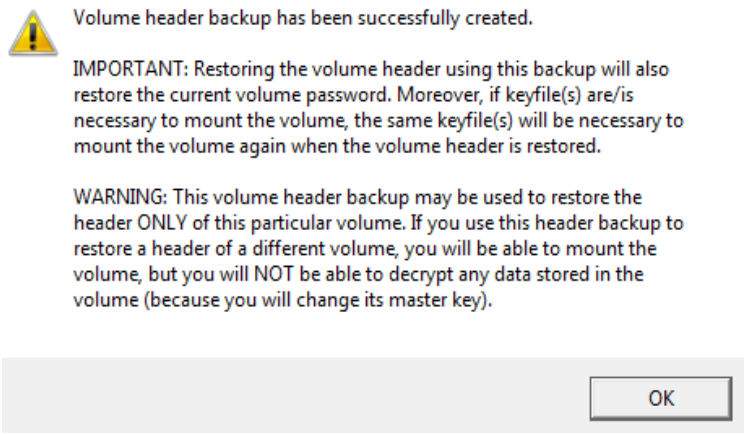
   Note: Dismount appears as an option once you select a drive.



3. Using the "Select file" option, choose the volume file you just dismounted. Click on "Volume tools", and select Backup Volume Header.



4. Enter your password as directed, and select that the file does not have a hidden volume. After the various warnings, give the file a name and store it somewhere secure e.g. copy to CD and store securely.



Note: If you restore this header you also restore the current password. You should consider storing this file and password somewhere safe, e.g. burn it to a CD and add a file with the password in it, then change the password on the current volume.

APPENDIX: AES ENCRYPTION AND SECURITY CONSIDERATIONS

This document describes a process for creating a portable secure store for documents and files. When using it, bear in mind the following:

Files stored on this key may also be in temporary storage on the machine where they were last created or edited. Other users of these computers may be able to retrieve older copies of the files. For this reason, files on these drives should only be used on secure computers in trusted locations.

Within Truecrypt, AES is used in 256 bit mode, with initial key vectors randomized based on user input. Truecrypt itself has not been subjected to FIPS evaluation, though the AES algorithm is FIPS approved.

For details on the AES standard and approval process, see the following additional external references:

Wikipedia: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Official AES Standard Document: http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Joan Daemen and Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer-Verlag, 2002. ISBN 3-540-42580-2.

Finally, the Truecrypt guide documentation provides details on other aspects of the uses of Truecrypt.