

How To:

Encrypt Notebooks and Hard Drives

A completely integrated G/On and TrueCrypt Solution for securing data in transit and data at rest.

November 2008

Introduction

G/On is an end-to-end remote access solution that provides users with secure access from any PC to corporate applications such as e-mail, ERP, and office applications. On top, G/On can be configured to let data stay securely on the corporate network by preventing the user from downloading, copy/paste, attach/detach etc. However, many people are depending on Laptops in their job and are relying on access to corporate data even while working off-line. This imposes a significant risk to companies for losing sensitive data if Laptops are stolen, misplaced, lost, or simply left out of sight for a few minutes in, say, an airport lounge. In the City of London alone, more than ten thousand laptops are accidentally left in Taxi's every year. So, while G/On will securely connect the user from his or her Laptop to corporate applications and – if configured to allow – will securely download data to the Laptop, data themselves are not protected once downloaded to the Laptop unless additional measures are taken.

This How-To Guide explains how G/On can be fully integrated with a hardware encryption tool like TrueCrypt to encrypt data storage devices such as a data partition on a Laptop hard drive or on a USB stick. Encrypting a data partition on user Laptops will significantly enhance the protection of sensitive data even while stored on mobile devices that can easily be accessed by other people.

How-To Guide

The following description shows how to encrypt a Notebook with TrueCrypt. The encryption is protected by a combination of a user supplied password and the integrated "certificate", called the EDC, of the G/On USB key that is already used by G/On for the user authentication for remote access. Although not all that complicated, the instructions are technical in nature, and should only be carried out by IT-administrators or users with experience in setting up a computer. Giritech recommends that organizations wanting to implement encryption of offsite data storage, use the instructions below to enhance/build a standard image on their user's laptops.

The solution and this documentation were originally developed by Giritech GmbH, 2008.

Download TrueCrypt

Download link for the TrueCrypt Foundation

<http://www.TrueCrypt.org>

Prepare the Notebook

Notebook/PC System Preparation

Split the Notebook hard disk into two partitions:

- ➔ System – Operating system
- ➔ Data – Application and company data

Attention!

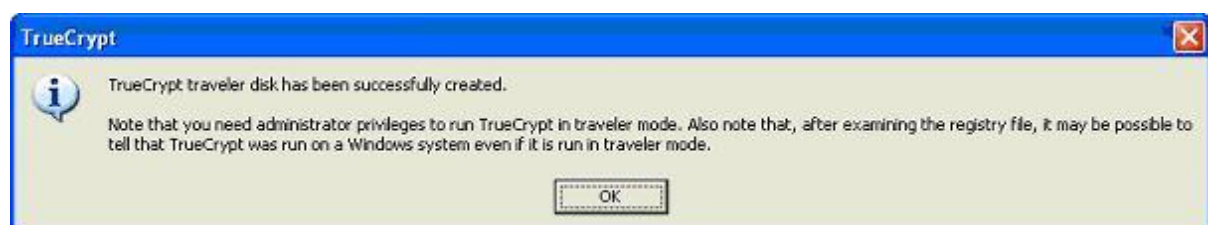
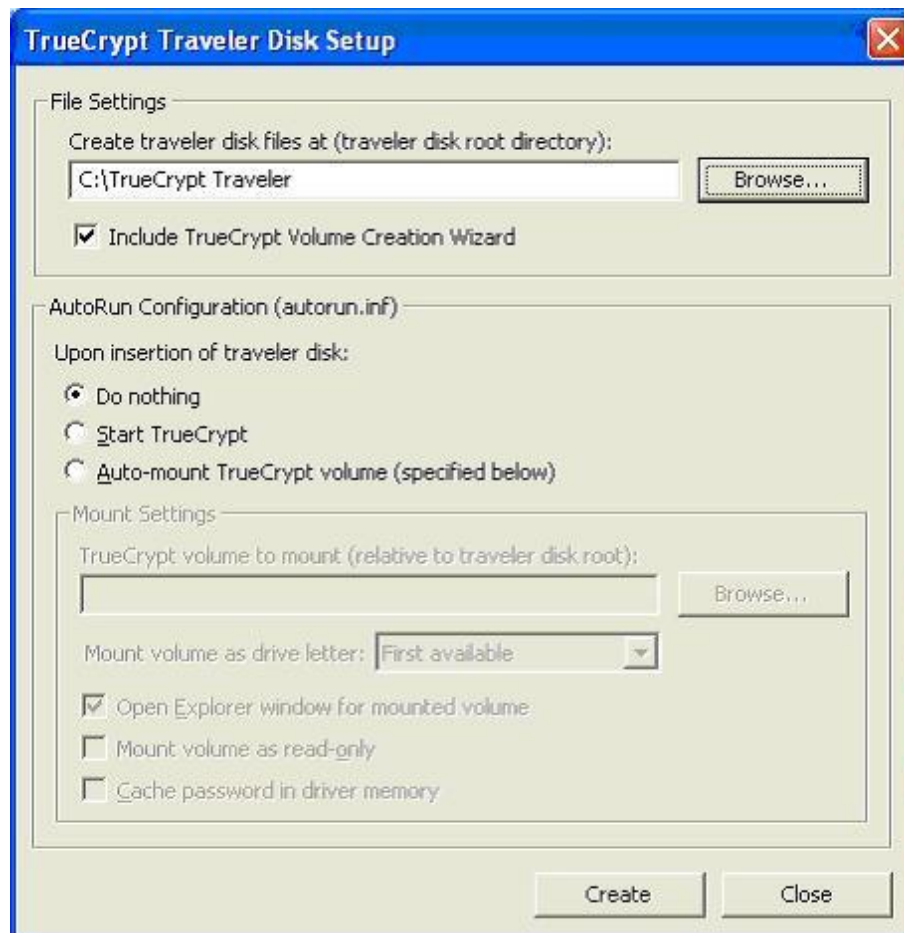
Do not use drive letter "D:" for your data partition. Use a higher drive letter like "V:" as "D:" is typically used by the operating system.

Hint: You may want to use the freeware "Driveimage XML" to help you to back up the partition before doing any changes: <http://www.runtime.org/driveimage-xml.htm>.

The freeware "Partiton Logic" can help you to resize the partition of your hard drives <http://partitionlogic.org.uk>. **Do not use without having a complete backup!**

Download and install TrueCrypt version 6 or higher from www.truecrypt.org

- ➔ Launch TrueCrypt and go to the menu "Tools" and crate a "Traveler Disk Setup" which is the portable version of TrueCrypt you can use from a G/On USB.



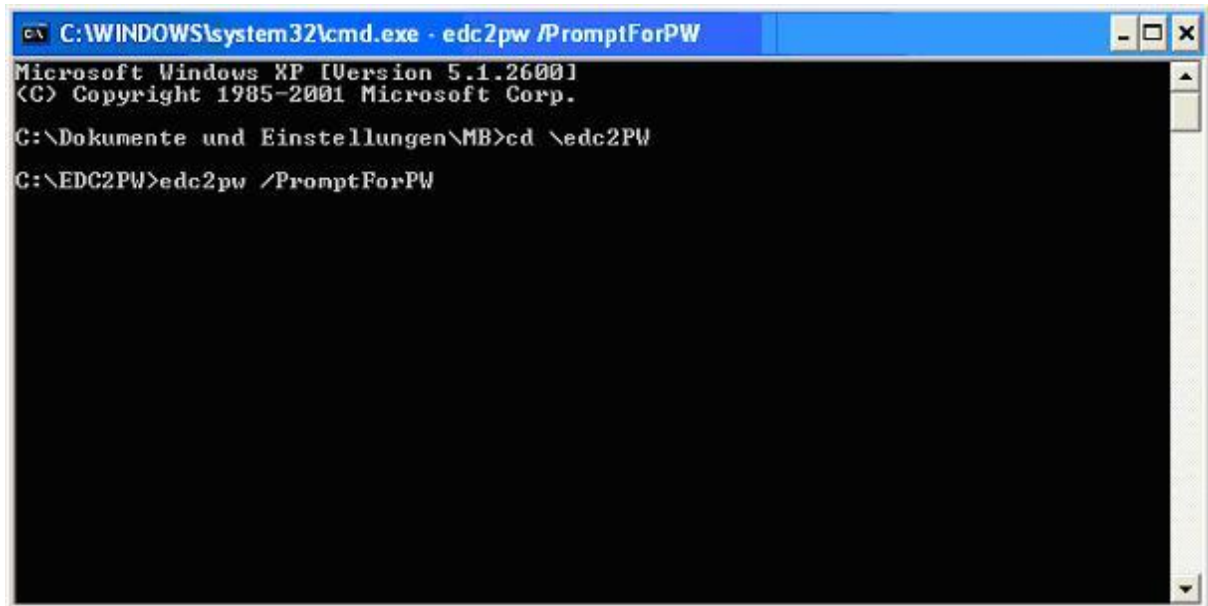
Take any picture and store it to the hard disk – for example “Company.jpg”, or use an existing (unique) picture already on your computer.

- ➔ The first megabyte of the image file will be used later for encryption. A picture is a good tool for that as you have to use the original file – no one will ever be able to do the same picture again with a camera.

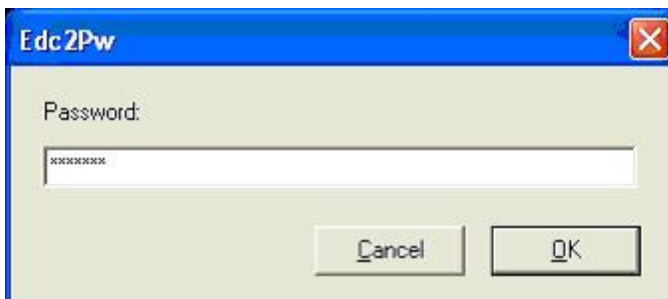
Copy the tool EDC2PW.exe to your hard disk

- ➔ You can find “EDC2PW.exe” in the “Clients” directory of G/On version 3.4.1.1341 or newer
- ➔ Run “EDC2PW /PromptForPW”.

Enter the password. Then copy and store the EDC/password hash in a text file for future use.



```
C:\WINDOWS\system32\cmd.exe - edc2pw /PromptForPW
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Dokumente und Einstellungen\MB>cd \edc2PW
C:\EDC2PW>edc2pw /PromptForPW
```

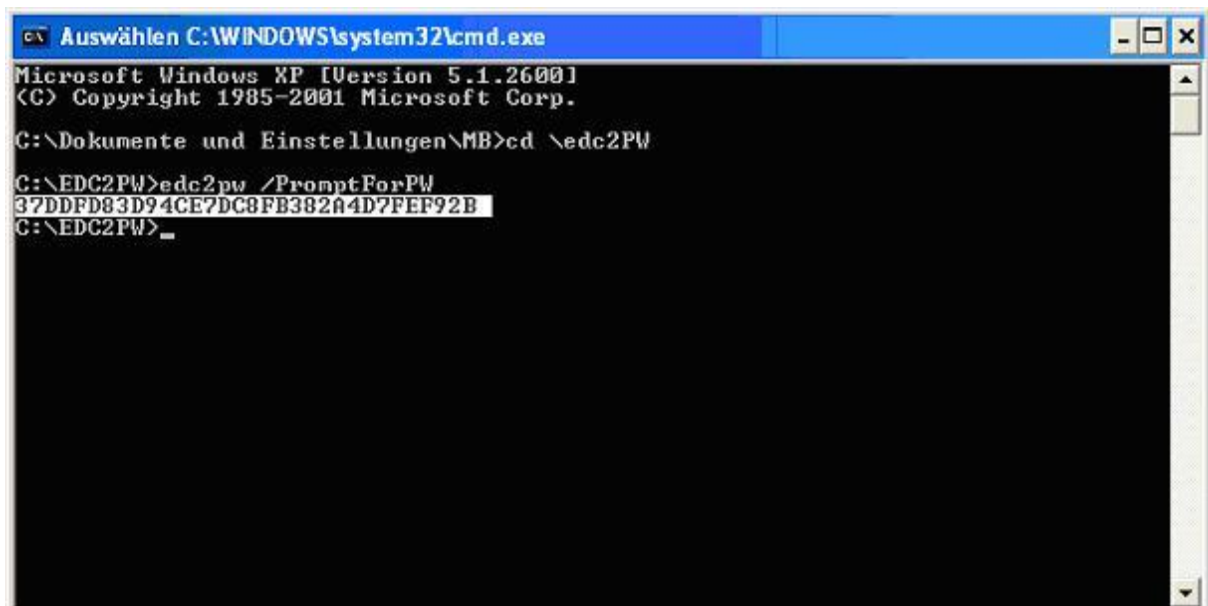


Edc2Pw

Password:

XXXXXXXXXX

Cancel OK

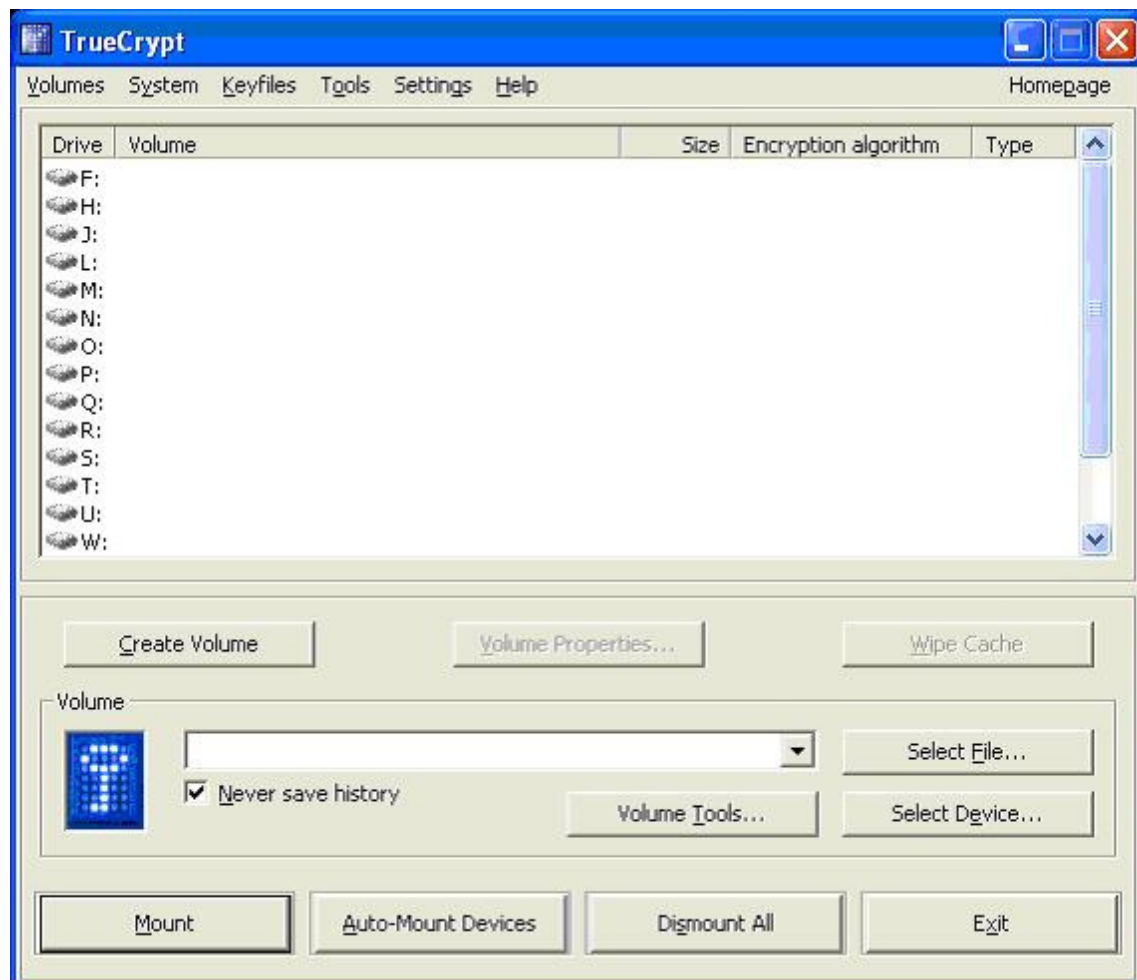
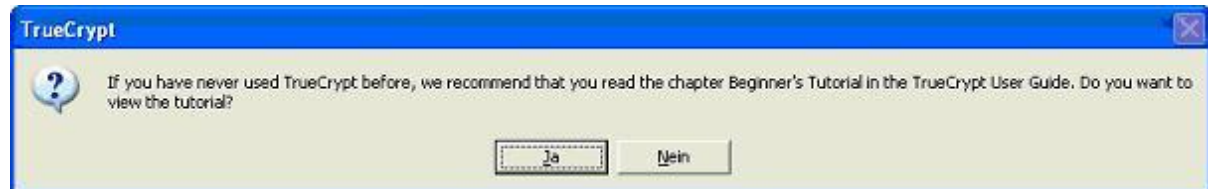


```
Auswählen C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Dokumente und Einstellungen\MB>cd \edc2PW
C:\EDC2PW>edc2pw /PromptForPW
37DDFD83D94CE7DC8FB382A4D7FEF92B
C:\EDC2PW>
```

Hard Disk Encryption

Encrypt partition

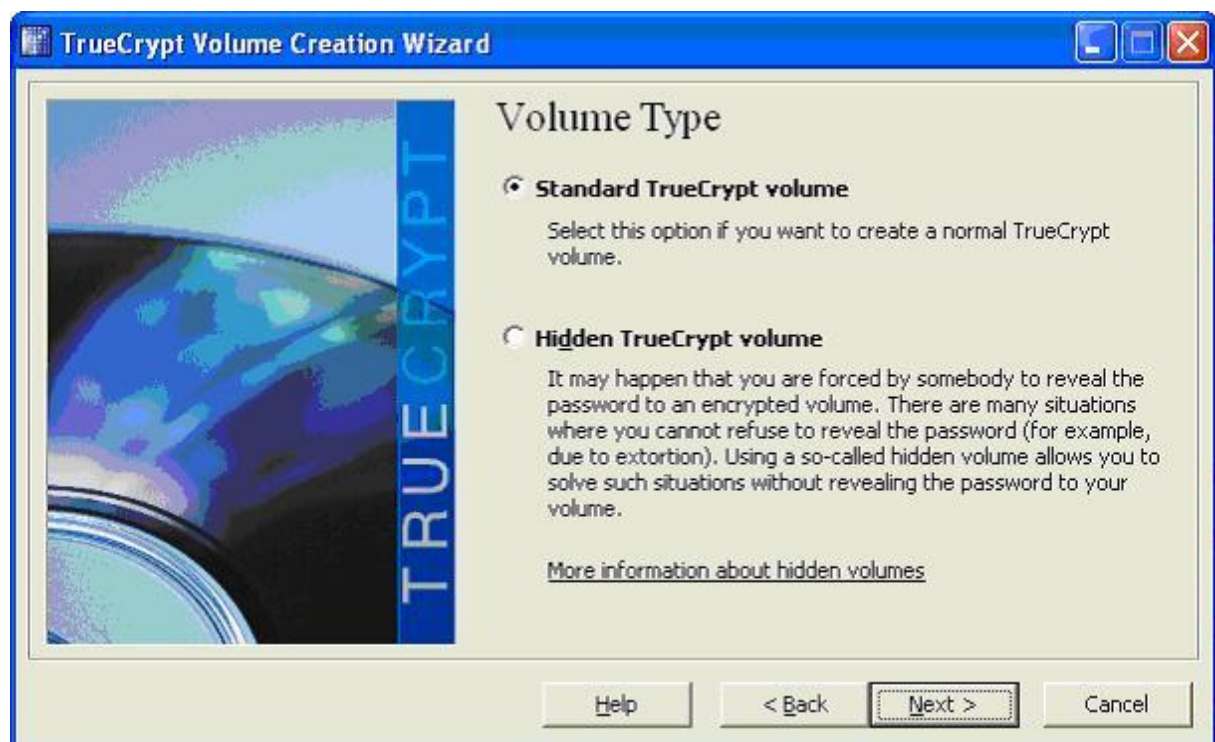
➔ Launch TrueCrypt – click „No“ if you get this message.



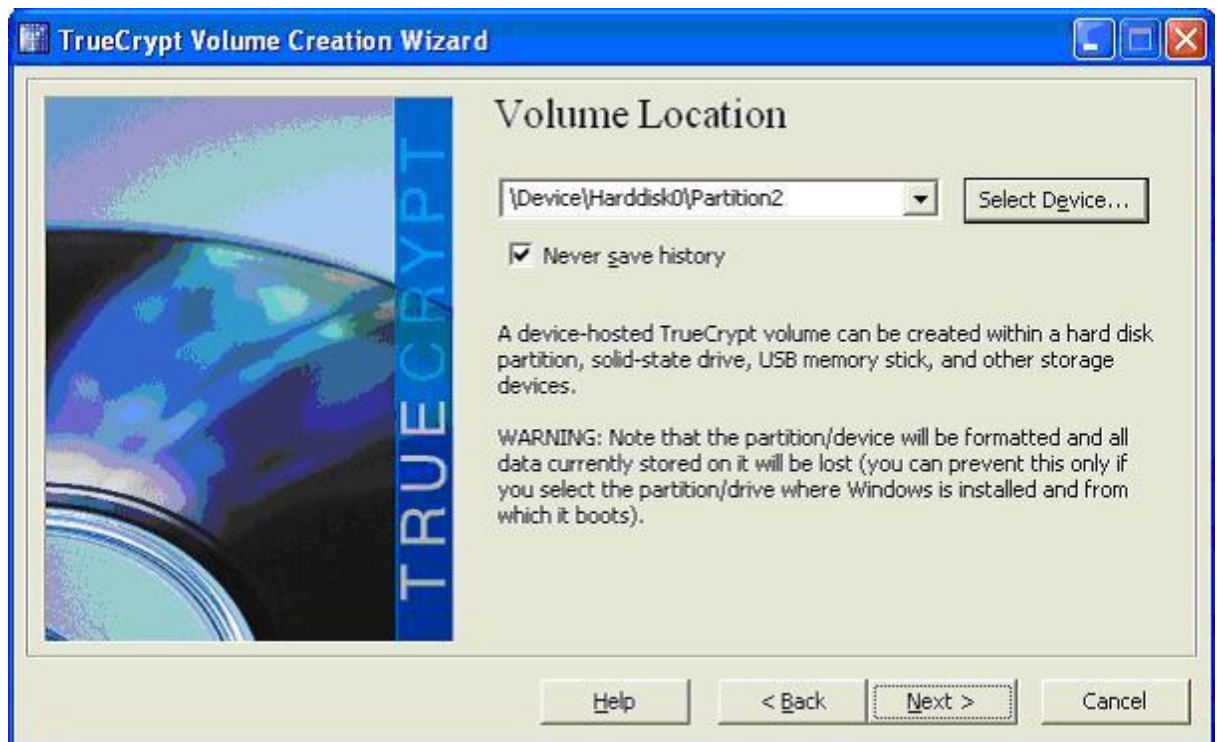
➔ Klick on „Create Volume“ and select “Create a volume within a non-system partition / device”



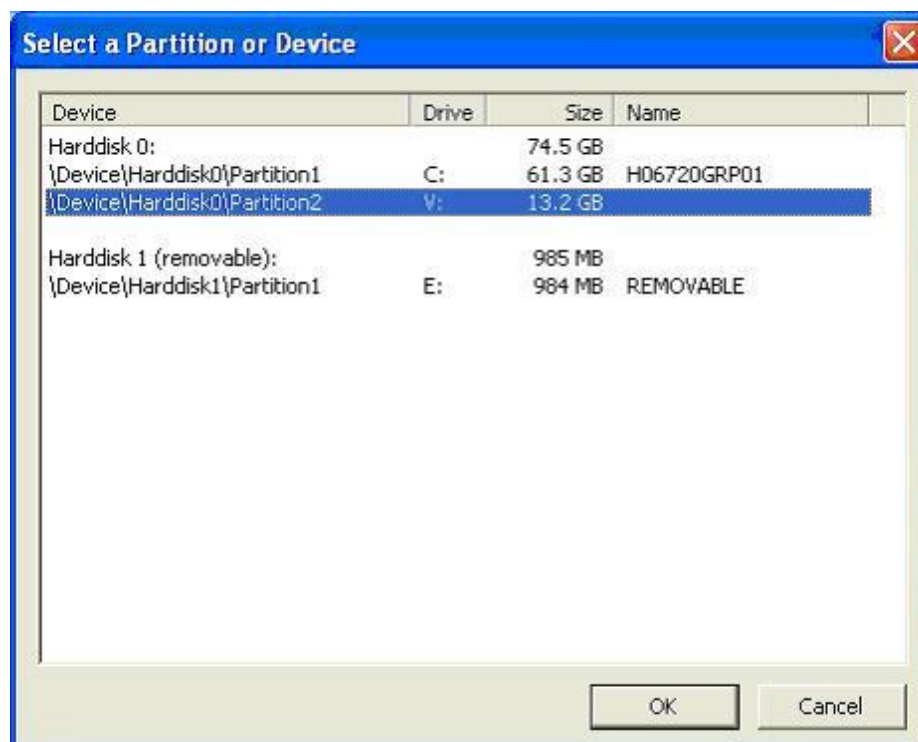
➔ Select “Standard TrueCrypt volume”



→ Klick on “Select Device...”



→ Chose the partition to be encrypted



→ Klick "Yes" to continue



→ Chose Encryption level or keep standard settings



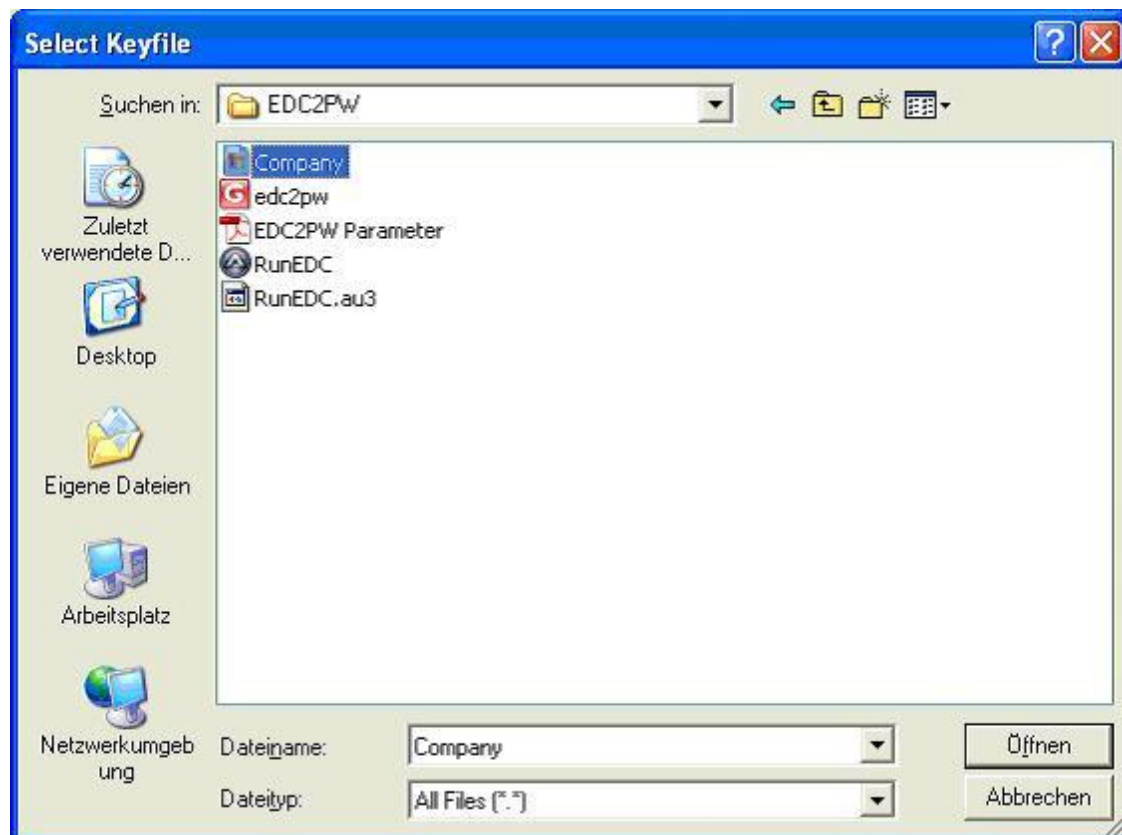
- ➔ To encrypt the partition you must confirm the size of the partition.
If you are encrypting a file, specify the size of the encrypted file.



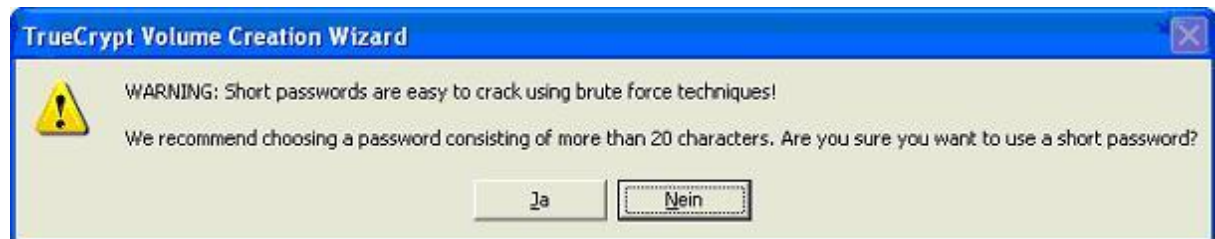
- ➔ Click in “Display password” and enter the EDC hash you previously created with the EDC2PW tool.
Use “copy and paste” to the field “Password” and select “Confirm”.
Verify if everything is OK.



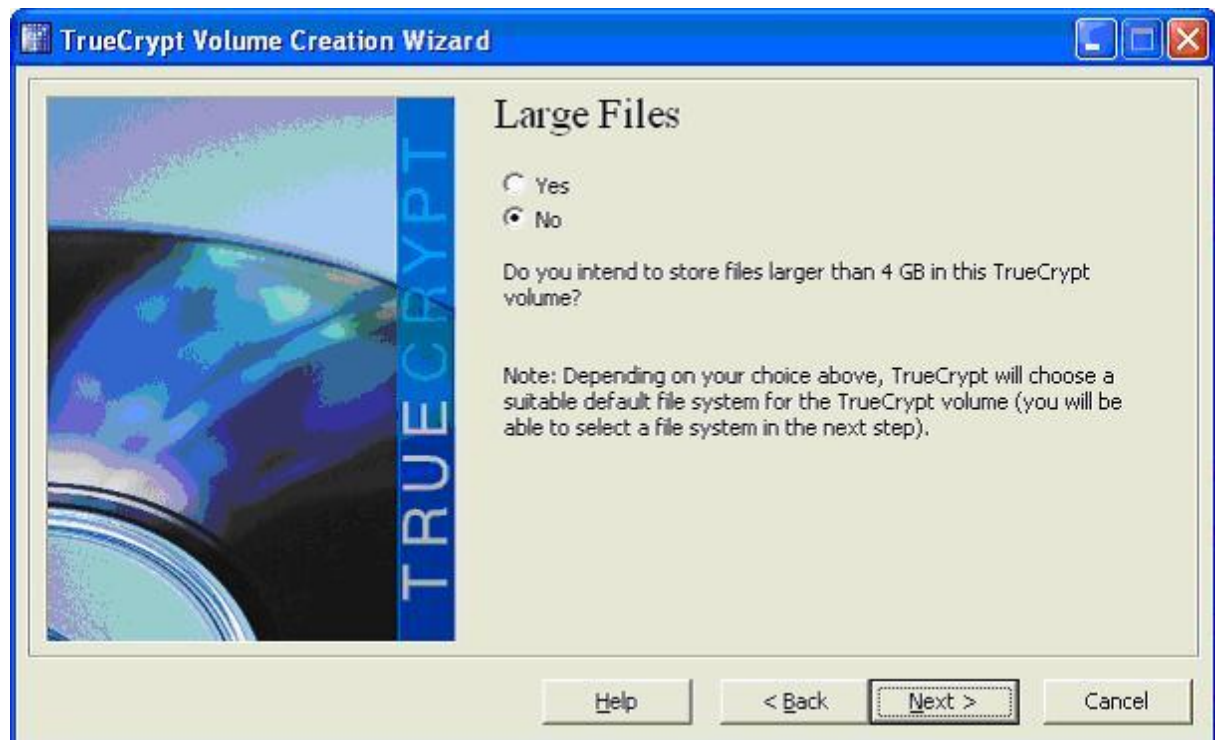
- ➔ Then click on „Keyfiles...” and select your image file “Company.jpg”. At this time you have to select the specific file – it is not enough just to select drive or path.



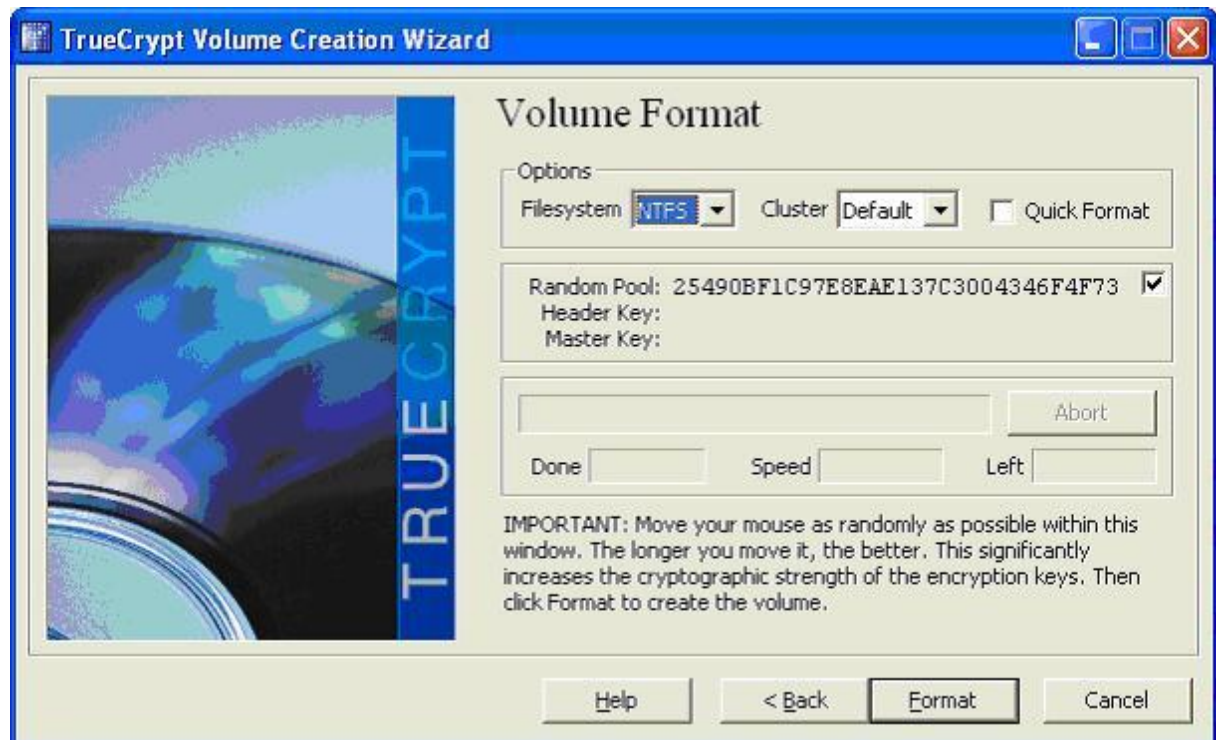
- Confirm the security warning in case you are using a short password



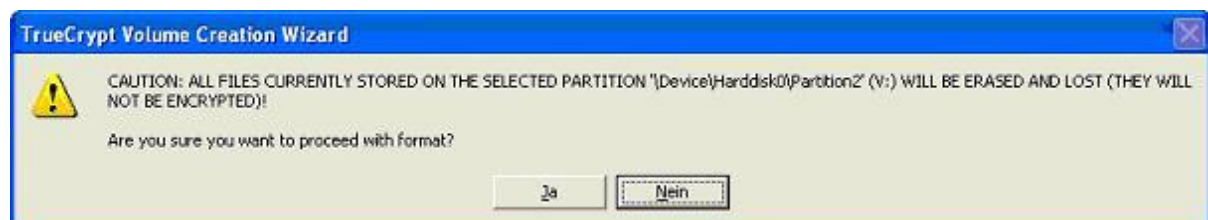
- Specify if you need files larger than 4 Gigabytes (default "No")



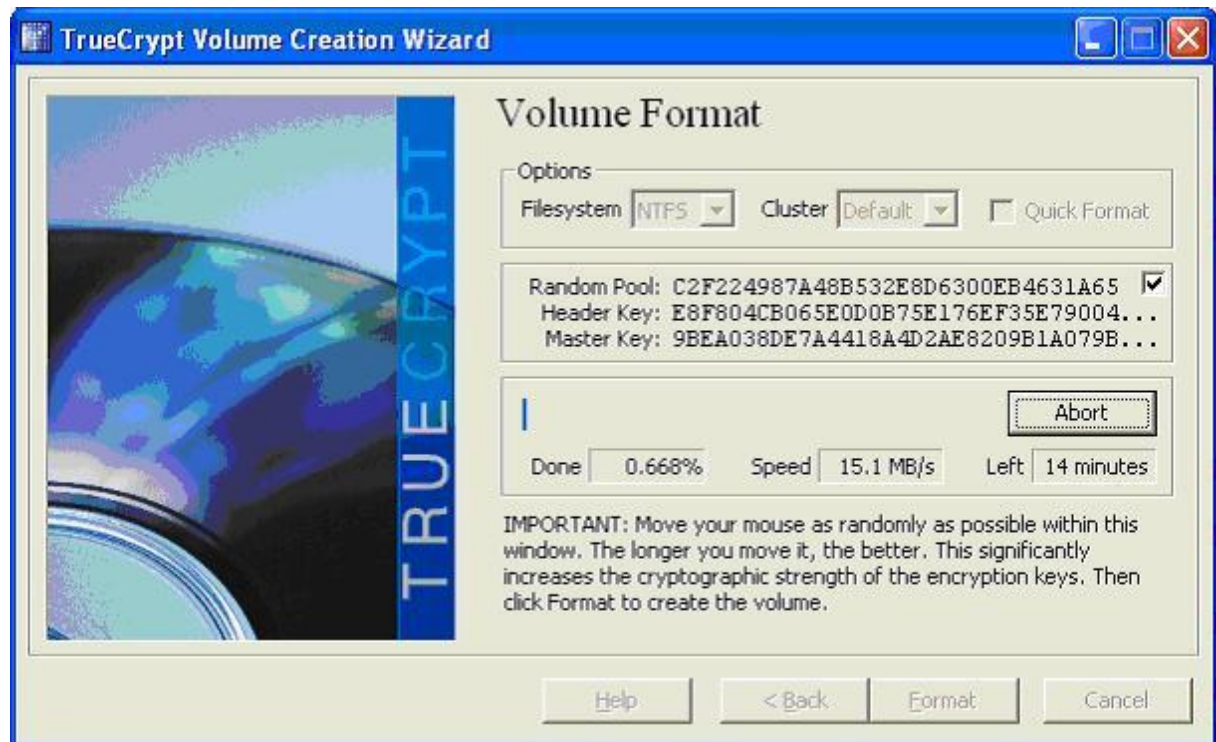
- ➔ Generate a "Random Pool" by moving the mouse
- ➔ Choose the file system you want to have – NTFS



- ➔ Confirm that all data will be lost during format of the partition



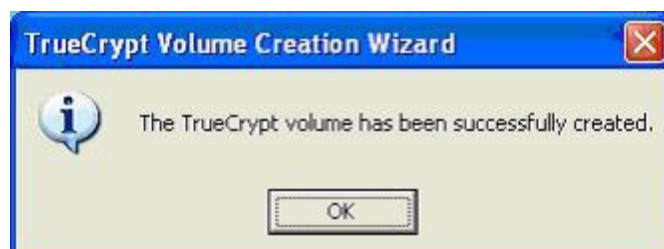
➔ Formatting will proceed – this may take some time depending on your volume size



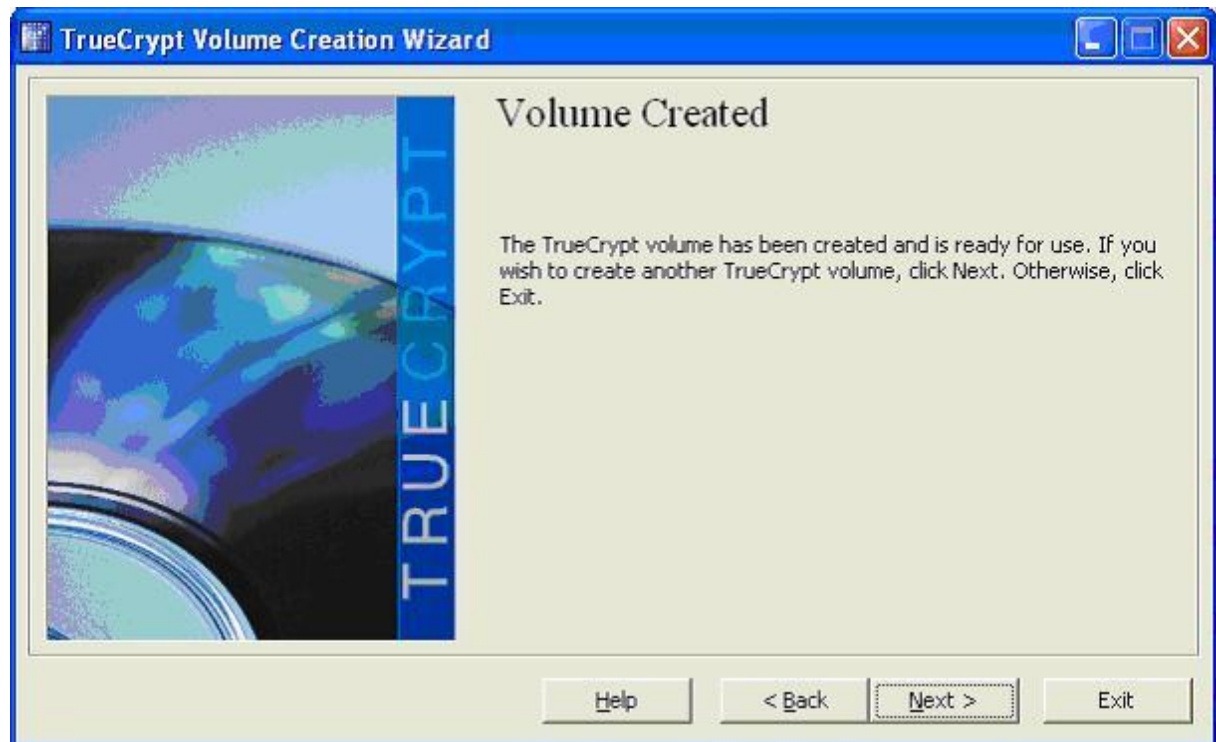
➔ Confirm that the encrypted volume can't be used / read without being mounted in TrueCrypt



➔ Confirm end of encryption process



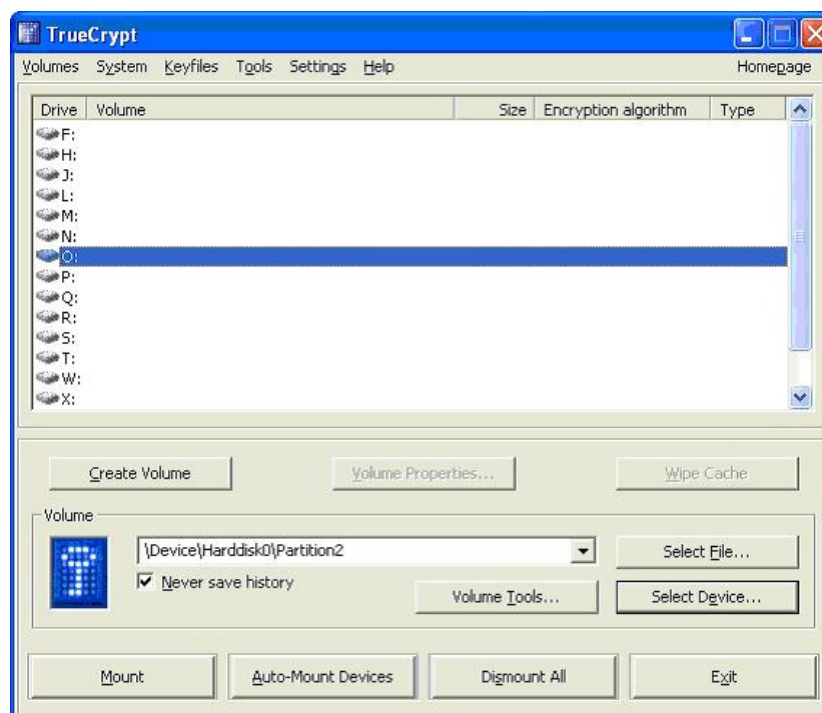
➔ Close the dialog with “Exit”



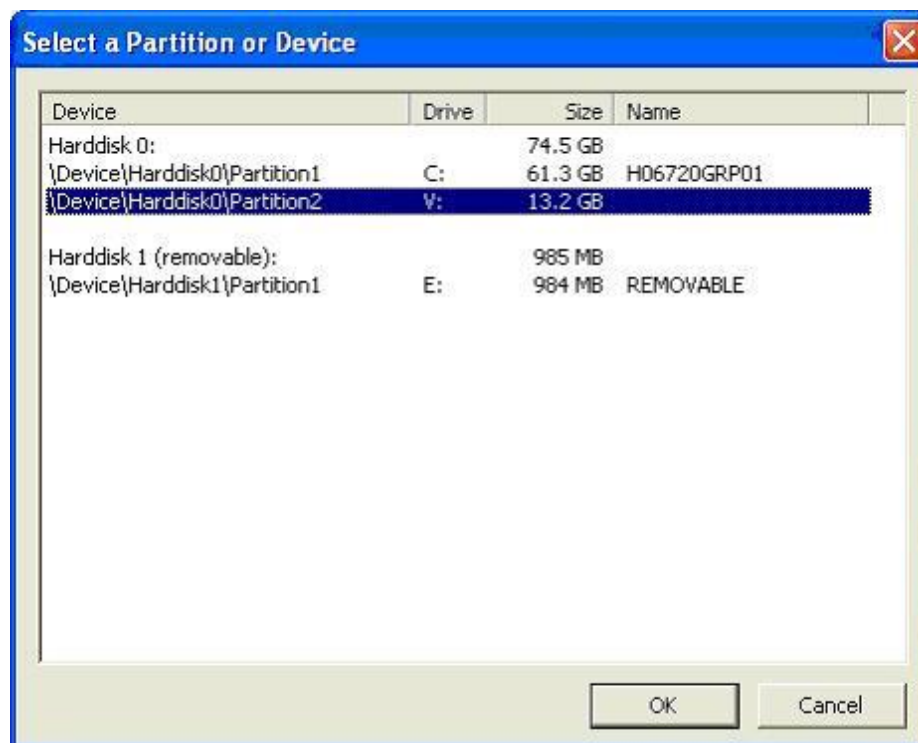
Enabling and testing the encrypted device

Test of the encrypted partition – first manual mount

➔ Launch TrueCrypt. Highlight the drive letter you want to use for the encrypted partition. In our example drive “O:”.



➔ Then click on “Select Device” and check the partition you have encrypted

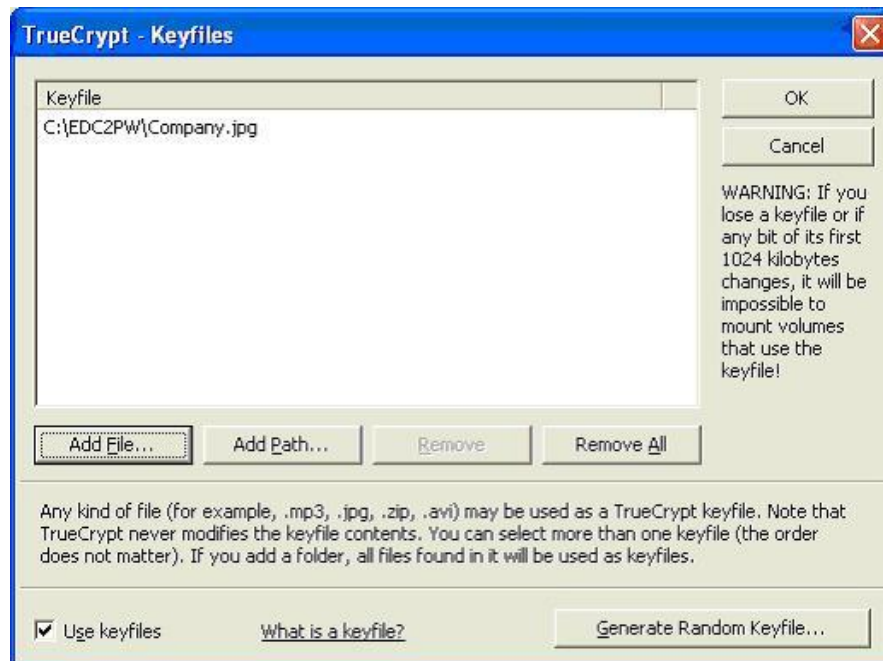


➔ Click on „Mount“ to bring up the password dialog.

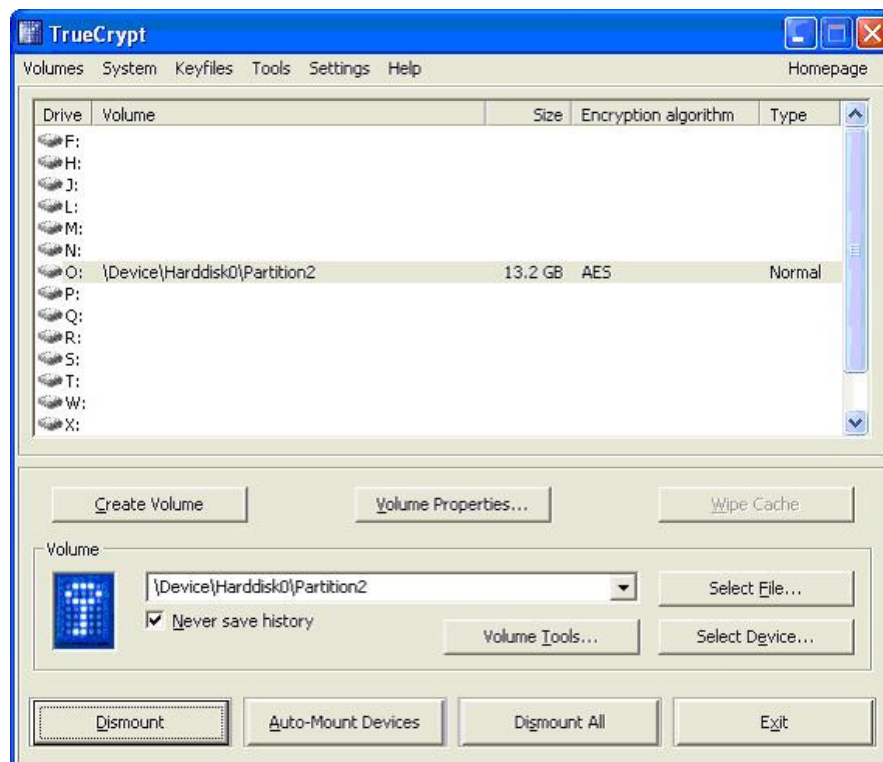
➔ Check “Display password” and copy the EDC hash you previously created with the EDC2PW tool into the password field



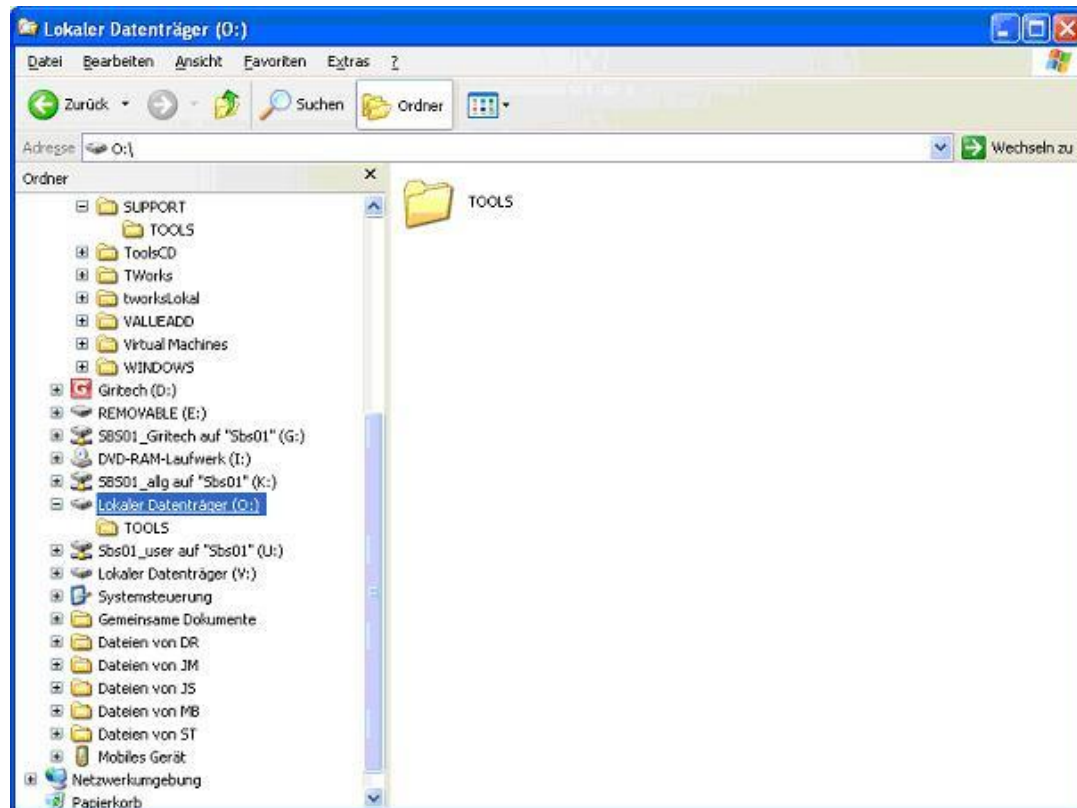
➔ Click on “Keyfiles” and “Add File..” to select your Company Image



➔ Then finish the mounting process. The result has to look like this



➔ You can now verify the function in the explorer and file system.



Hint:

Sometimes the explorer doesn't show the drive letter correctly. This is simply an update issue which can be solved by closing and reopening the explorer. It has no impact on the functionality of the decrypted drive O:

Automating hard disk decryption

Prepare RunEDC.exe

To make the decryption process simple for the user, G/On is delivered with a tool, RunEDC.exe that will automatically create the hash value needed for encryption. This tool uses AutoIT (a command line programming tool). Locate and download AutoIT version 3 or later from:
<http://www.autoitscript.com/autoit3/index.shtml>.

- ➔ Launch AutoIT.exe and open the RunEDC.AU3 file
- ➔ Edit the variables in the first section of this file as described
- ➔ Compile "RunEDC" with "F7"-key

Compiling the script is a nice way of hiding the settings and partition information from normal users and administrators. Obviously, reverse engineering the script makes the settings visible but the EDC and password are still not revealed to the engineer.

Prepare Autorun.inf

Normally, the G/On EClient.exe is launched by an auto start function when the G/On USB is inserted into the PC. When you use the USB for the encryption functionality described in this document, you want to be able to decrypt the hard disk partition or file independently of the G/On connection. This is handled by RunEDC. So, the autorun.inf on the CD-partition of the G/On USB should be modified to execute RunEDC.

It also should have a context menu where you can select both modules “RunEDC” and “Eclient” depending on what you want to do.

Here is an example for Autorun.inf:

```
[autorun]
open=RunEDC.exe
Label=Giritech
Icon=gon.ico
shell\verb0\command=RunEDC.exe
shell\verb0=G/On RunEDC - Data encryption
shell=verb0
shell\verb1\command=EClient.exe
shell\verb1=G/On EClient - G/On online connection
shell=verb1
shell\verb2\command=Gupdate.exe /getall /yestoall
shell\verb2=G/On Update CD
shell=verb2
shell\verb3\command=Gupdate.exe /updaterw /getall
shell\verb3=G/On Update RW
shell=verb3
```

Prepare the CD-partition of the G/On USB

Prepare G/On CD-Partition

Copy the following files to the folder “C:\Program Files\EMCADS\Clients” on the G/On Server. The content of this folder is copied to the CD-partition of the G/On USB when the USB is updated with the GUpdate function.

- ➔ TrueCrypt Traveler version: A total of 4 files
- ➔ Company.jpg – the image used for the encryption
- ➔ RunEDC.exe – Compiled AutoIT3 Script
- ➔ EDC2PW.exe – Giritech EDC hash tool.
- ➔ Autorun.inf – to start “RunEDC” instead of “Eclient”

Name	Größe	Typ	Geändert am
Company.jpg	530 KB	JPEG-Bild	07.07.2008 13:18
edc2pw.exe	2.187 KB	Anwendung	26.06.2008 14:43
RunEDC.exe	249 KB	Anwendung	02.07.2008 10:43
TrueCrypt Format.exe	1.326 KB	Anwendung	23.07.2008 15:00
TrueCrypt.exe	1.197 KB	Anwendung	23.07.2008 15:00
truecrypt.sys	231 KB	Systemdatei	23.07.2008 15:00
truecrypt-x64.sys	234 KB	Systemdatei	23.07.2008 15:00

Cleanup system

Remove all temporary files that are no longer needed from your hard disk:

- ➔ TrueCrypt – if you like to hide the application used for encryption
- ➔ EDC2PW, RunEDC, Company.jpg – they are on the G/On stick and G/On Server
- ➔ Delete the file with the stored hash or copy it to your administrator documentation.

Emergency Decryption Tool

Create emergency application string

In an emergency situation you can create a G/On application string which will give a user a G/On Menu option to allow the user to open the encryption with another G/On stick or Desktop client.

- ➔ Application Type: Application Launcher (9)
- ➔ Application to launch %GONPATH,noedit%TrueCrypt.exe
- ➔ Parameter Syntax:
/v <TrueCryptDevice> /l <MappedDrive> /k <TrueCryptImage> /p <EDC-Hash> /q /s
- ➔ Parameter example:
/v \Device\Harddisk0\Partition2 /l O /k Company.jpg /p 1234567890123456 /q /s