So verschlüssele ich meinen PC

Anleitung zum verschlüsseln eines Rechners unter Windows XP mit Hilfe der Open-Source-Programme TrueCrypt, TCTemp und TCGINA.

Version: | | | | | | | | 1.0
Veröffentlicht: | | Dezember 2007
AutorInnen: | | | | | Acid Security
Lizenz: | | | | | | | | | | Creative Commons - by-nc - v3.0

0. Vorwort 03
1. Vorbereitung 05
1.1 Erforderliche Installationsdateien 05
1.2 Anzeigeverhalten im Windows Explorer 05
2. Installation von TrueCrypt 09
3. Installation von TCTemp 11
3.1 Voreinstellungen und Installation 11
3.2 TCTemp Volume Erstellung 14
3.3 TCTemp Image Erstellung 17
3.4 Windows XP Einstellungen 20
3.4.1 Disable LAN Manager Hashes 20
3.4.2 Aufrufen der Systemeinstellungen 21
3.4.3 Anpassung der Umgebungsvariablen 23
3.4.4 Anpassung der Auslagerungsdatei 25
3.4.5 Anpassung des Druckerspoolers 28
3.4.6 Anpassung des Internet Explorers 31
4. Verschlüsselung eines Benutzerprofils 34
4.1 Einrichten eines neuen Benutzerkontos 34
4.2 Aktivierung des Bildschirmschoners 38
4.3 Installation von TCGINA 39
4.4 Entfernen des Laufwerksbuchstabens bei Verwendung einer Partition 41
4.5 Anlegen eines TrueCrypt Volumes 45
4.6 Kopieren des Benutzerprofils 50
4.7 Aktivieren der Automatischen Windows Anmeldung 51
5. Aufräumen 54

0. Vorwort

Dieses Tutorial soll dir dabei helfen persönliche Daten auf deinem Computer vor dem Zugriff Anderer zu schützen. Der Schutz hält auch den professionellen Möglichkeiten stand, über die Geheimdienste und ähnlich gut ausgestattete Institutionen verfügen. Wenn alles beachtet wird ist der einzige Hemmschuh das Passwort, das deshalb stark genug sein muss.

Ein starkes Passwort zeichnet sich durch mehrere Faktoren aus. Zum einen durch die Passwortlänge, die mindestens zwanzig Zeichen betragen sollte. Außerdem sollten die Zeichen eine zufällige Kombination aus kleinen und großen Buchstaben, Zahlen und Sonderzeichen bilden. Dadurch wird das herausfinden des Passwortes erheblich erschwert. Bei Passworten die aus einem Wort bestehen, kann das Passwort durch automatisches Abarbeiten einer sehr langen Liste von Worten (Wörterbuchattacke) herausgefunden werden. Auch durch das Einfügen von Zahlen und Sonderzeichen in dieses Wort oder das Wechseln von groß und Kleinschreibung wird der Aufwand zum Ermitteln des Passwortes nur unerheblich vergrößert, da diese Veränderungen durch entsprechende Algorithmen berechnet werden können. Bei einer zufälligen Kombination der Zeichen lässt sich das Passwort nur durch das sehr aufwendige Durchprobieren aller Kombination (Brute-Force-Attacke) herausfinden. Der Aufwand der bei dieser Methode zum ermitteln des Passwortes notwendig ist, potenziert sich mit jeder weiteren Stelle die das Passwort hat und dauert je nach Länge des Passwortes und verfügbarer Rechenleistung Jahre bis Jahrzehnte.

Als Hilfsmittel um solche sicheren Passworte zu erzeugen, kann ein sogenannter Passwortsatz verwendet werden. Dabei dient ein selbst gewählter Satz als Gedankenstütze und jeder Anfangsbuchstabe als Stelle im Passwort. Durch die Verwendung von Zahlen (z.B. Uhrzeiten, Mengenangaben etc.) im Satz und das zusätzliche Einfügen von Sonderzeichen werden alle Vorraussetzungen an ein starkes Passwort erfüllt. Achte darauf, niemals persönliche Daten von dir oder dir bekannten Personen in das Passwort einfließen zu lassen. Ein Passwortsatz könnte zum Beispiel so entstehen: »**T**ante **K**lara **M**uss **J**eden **A**bend **U**m **H**alb **9 2 G**läser **B**ier **T**rinken« ergibt »**TKMJAUH92GBT**«. Jetzt sollten um die Sicherheit zu erhöhen zufällig gewählte Sonderzeichen eingefügt werden: »TK_mjA**%(**uh9**)!**2GBt«. Wem die Verwendung eines Passwortsatzes immernoch zu riskant ist, kann auf die große Anzahl von frei verfügbaren Passwortgeneratoren zurückgreifen. Das Open-Source-Programm **»KeePass Password Safe«**, mit dem sich die vielen verschiedenen eigenen Passworte verwalten lassen, enthält zum Beispiel einen solchen Passwort-Generator. (Website des Programms `http://keepass.info/`.)

Für die Verschlüsselung benutzen wir das kostenlose Open-Source-Programm TrueCrypt. Im gegensatz zu einigen kommerziell erhältlichen Programmen bietet TrueCrypt keine Pre-Boot-Encryption (Das ganze Betriebssystem wird verschlüsselt). Momentan gibt es nur kostenpflichtige Programme mit unveröffentlichtem Quellcode (proprietäre Software) wie z.B. **»DriveCrypt Plus Pack«**, die dazu in der Lage sind. Nur mit zusätzlichen Maßnahmen lässt sich auch mit TrueCrypt ein umfassender Schutz gewährleisten. Allerdings sind wir gespannt auf das nächste für Januar 2008 angekündigte TrueCrypt Release, dass auch mit diesem Feature aufwartet.

Zum jetzigen Zeitpunkt (TrueCrypt Version 4.3a) kann der Schutz nur in Verbindung mit den Zusatzprogrammen TCTemp und TCGINA auf vom Betriebssystem kontrollierte Vorgänge und Bereiche ausgedehnt werden. Dazu gehört die Verschlüsselung aller vom System oder Anwendungen erzeugten temporären Daten, der Windows Auslagerungsdatei und von Windows Benutzerprofilen. Auch wenn der hierfür erforderliche Aufwand etwas größer ist und darauf zu achten bleibt sensible Daten nur auf sicheren Bereichen des Computers zu speichern, raten wir zur Verwendung von TrueCrypt. Im Gegensatz zu proprietärer Software ist der Quellcode veröffentlicht und wird von einer großen Community weiterentwickelt. Dadurch ist sichergestellt, dass sich staatliche Stellen, Unternehmen oder sonstige Organisationen keine versteckten Zugriffsmöglichkeiten, sogenannte Hintertürchen, in das Programm haben einbauen lassen. Außerdem werden Sicherheitslücken schneller erkannt und entfernt.

Um sich mit der prinzipiellen Funktionsweise von TrueCrypt zu beschäftigen und weitere Einsatzmöglichkeiten kennenzulernen empfehlen wir die Lektüre des Handbuches. Grundlegend stehen zwei funktionsweisen von TrueCrypt zur Verfügung. Zum einen kann der gesamte Datenträger verschlüsselt werden (Device Encryption) zum anderen können auf einem existierenden Datenträger sogenannte Container Dateien angelgt werden die dann als Virtuelles Laufwerk ins System eingebunden werden. Bei der Benutzung von TCGINA befindet auch der Windows Desktop oder der Ordner **»Eigene Dateien«** in einem solchen Bereich, so dass dort sensible Daten abgelegt werden können.

Es ist sehr wichtig nach der Ausführung unserer Anleitung, die nicht mehr auf der Festplatte benötigten Dateien und den freien Speicherplatz sicher zu löschen. Durch normales Löschen bleiben Dateien nämlich physikalisch auf der Festplatte, lediglich der Speicherplatz wird wieder freigegeben und kann wieder genutzt werden. Mit einem Programm wie **»Eraser«**, wird dieser Speicherplatz bis zu 35 mal überschrieben. (Sieben mal gilt allerdings als ausreichend.) Dadurch können Daten anschließend nicht wiederhergestellt werden. **»Eraser«** ist auf der Seite **»`http://www.heidi.ie/eraser/download.php`«** erhältlich. Lade dir dort die Datei **»`Eraser586_setup.exe`«** herunter und installiere das Programm nach erfolgtem Download durch einem Doppelklick auf die Datei.

Wenn du jetzt von den vielen Informationen noch nicht erschlagen bist und weitermachen möchtest, sei noch erwähnt wieviel Zeit du benötigst. Abhängig von deinem Rechner kann es etwas mehr oder weniger sein, vier Stunden kannst du jedoch einplanen. Davon ist etwa eine Stunde reine Wartezeit. Und jetz viel Spass beim ausprobieren!

PS: Dieses Tutorial richtet sich eindeutig nicht an Computer-Experten, sondern an Computer-Laien, Einsteiger oder ältere Menschen, für die der Umgang mit dem Computer keine Selbstverständlichkeit darstellt. Daher haben wir darauf geachtet, alle Schritte inklusive von Zwischenschritten komplett nachvolziehbar zu machen - um niemanden auf halber Strecke stehen lassen zu müssen - und bestimmte technische Details nur wenn notwendig angesprochen.

Auch wenn dadurch einige technische Sachverhalte verkürzt dargestellt werden ist es uns wichtig dass die enthaltenen Informationen fachlich korrekt sind.

Wir bitten daher um zweierlei Feedback. Wenn du ein Experte bist, hilf mit fachliche Fehler in dieser Anleitung zu korrigieren und schicke uns Anmerkungen technischerseits.

Falls du dieses Tutorial als User durchgearbeitet hast, lass uns daran Teilhaben an welchen Stellen du aus welchen Gründen Schwierigkeiten hattest, damit wir entsprechende Verbesserungen am Text vornehmen können.

Wenn du uns kontaktieren möchtest findest du unsere Email-Adresse und den dazugehörigen GnuPG-Key auf unserer Homepage **`it-sicherheit.jimdo.com`**.

1. Vorbereitung

1.1 Erforderliche Installationsdateien

1.1.1 Um die nachfolgend aufgeführten Installationsdateien zu entpacken, lade dir die aktuelle Version des Programms **»7zip«** von der Seite **»`http://www.7-zip.org`«** herunter. Es stehen zwei Varianten zur Auswahl. Wenn auf deinem Rechner Windows für 32bit Prozessoren läuft, wähle die erste (mit **32bit** gekennzeichnete) Variante. Läuft auf deinem Rechner Windows mit 64bit Unterstützung wähle die zweite (mit **64bit** gekennzeichnete) Variante. Diese Unterscheidung gilt für alle nachfolgenden Programme die heruntergeladen und installiert werden. Falls du dir nicht sicher bist, welche Variante die richtige für dein Betriebssystem ist, kannst du immer die 32bit Variante nutzen. Falls du fälschlicherweise die 64bit Variante ausführst, erhälst du eine Fehlermeldung die dich darauf hinweist dass du ein 32bit Betriebssystem hast. Die heruntergeladene Datei heißt also **»7z457.exe«** oder **»7z457.msi«**. (Die Nummer vor der Dateiendung wird sich bei einer neueren Version unterscheiden.) Starte die Installation von 7zip durch einen Doppelklick auf **»7z457.exe«** oder **»7z457.msi«**.

1.1.2 Lade dir das TrueCrypt Installationspaket **»`truecrypt-4.3a.zip`«** von der Seite **»`http://www.truecrypt.org/downloads.php`«** herunter. Im Download-Bereich der TrueCrypt-Webseite findest du unter der Überschrift **»Latest stable Version«** den Button [Download]. Durch einen klick auf diesen Button startet der Download. Erstelle anschließend einen Orner und verschiebe die Datei dort hin. Klicke mit der rechten Maustaste auf die Datei **»`truecrypt-4.3a.zip`«** damit sich das Kontextmenü öffnet. Wähle dort den Eintrag **»Extrac Here«** um den Inhalt der Datei zu entpacken.

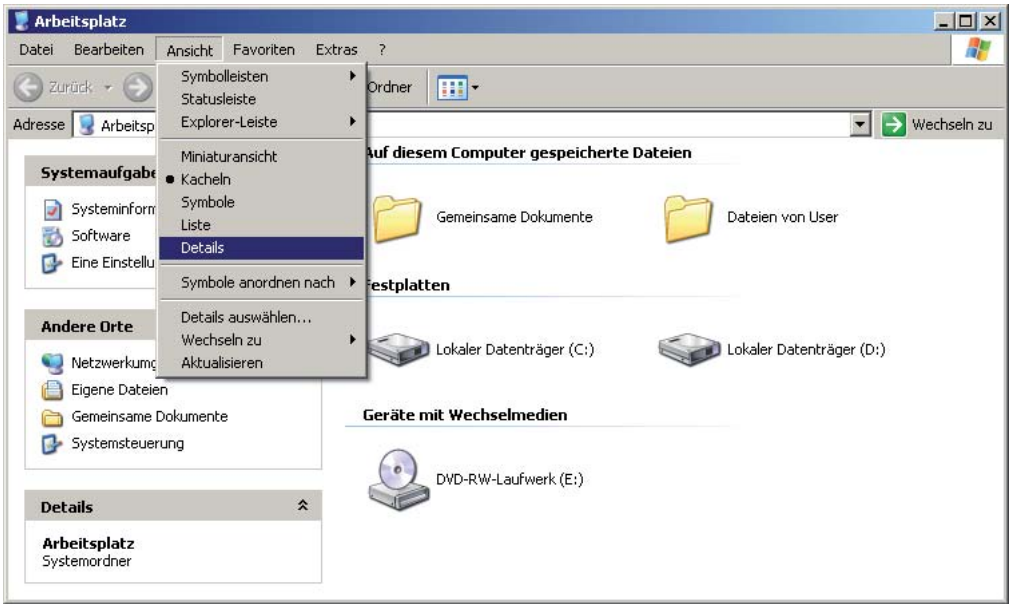
1.1.3 Das Zusatzprogramm TCTemp findest du unter **»`http://www.truecrypt.org/third-party-projects/tctemp/`«**. Im unteren Bereich der Seite befindet sich eine Tabelle mit den Download-Links. Die aktuelle Version steht ganz oben in der Tabelle, momentan ist das Version 1.6. Lade dir also die Datei **`tctemp-1.6-pack.zip`** herunter, erstelle einen Ordner in dem du die Datei ablegst. Öffne durch einen Rechtsklick das Kontextmenü und wähle den Eintrag **»Extract here«** um die Datei zu entpacken. Du erhältst eine ebenfalls gepackte Datei mit dem Namen **»`tctemp-1.6.7z`«**. Entpacke die Datei mit der gleichen Methode.

1.1.4 Das Zusatzprogramm TCGINA ist auf der Seite**«`http://www.truecrypt.org/third-party-projects/tcgina/`«** erhältlich. Der Download-Link befindet sich wieder weiter unten auf der Seite. In einer Tabelle stehen mehrere Downloads zur Verfügung. Die aktuellste Version (momentan Version 1.17) findest du wieder an oberster Stelle. Wenn du ein 64bit Betriebssystem benutzt, klicke auf den Download-Link in der mit **»Windows XP/2003 x64 Edition«** überschriebenen Spalte. Die Datei heißt dann **`tcgina-1.17-x64-pack.zip`** Wenn du die 32bit Version von Windows benutzt klicke auf den Download-Link in der Spalte **»Windows XP/2000/2003«** um die Datei **»`tcgina-1.17-pack.zip`«** herunterzuladen. Lege die Datei in einem eigenen Ordner ab. Öffne mit einem Rechtsklick auf die Datei das Kontextmenü und wähle **»Extract here«** um die Datei zu entpacken. Du erhälst eine Datei mit dem Namen **»`tcgina-1.17.7z`«** bzw. **»`tcgina-1.17-x64.7z`«** die du ebenfalls entpackst.

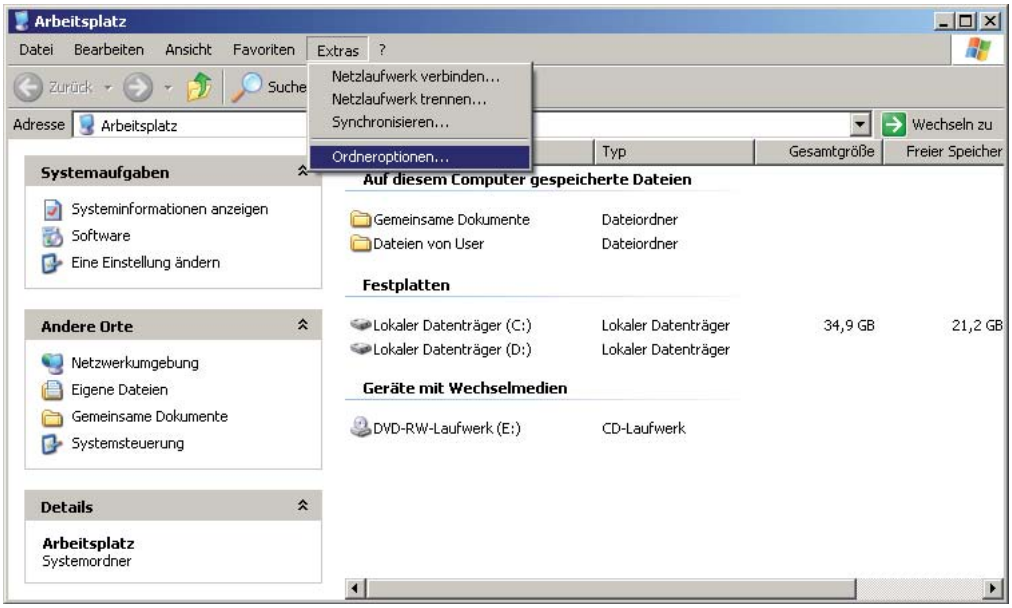
1.2 Anzeigeverhalten im Windows Explorer

1.2.1 Die folgenden Einstellungen betrefen die Anzeige innerhalb des Windows Explorers - nicht mit dem Internet Explorer zu verwechseln. Sie gleichen die Darstellung innerhalb deines Windows Explorers an die Bilder (Screenshots) in diesem Tutorials und ermöglichen eine bessere Benutzbarkeit. Um den Windows Explorer zu öffnen gibt es folgende Möglichkeiten: 1. Drücke die [⊞] + [E]. 2. Klicke auf dem Desktop auf das Symbol für den **»Arbeitsplatz«** 3. Klicke im Startmenü auf den Menüpunkt **»Arbeitsplatz«**.

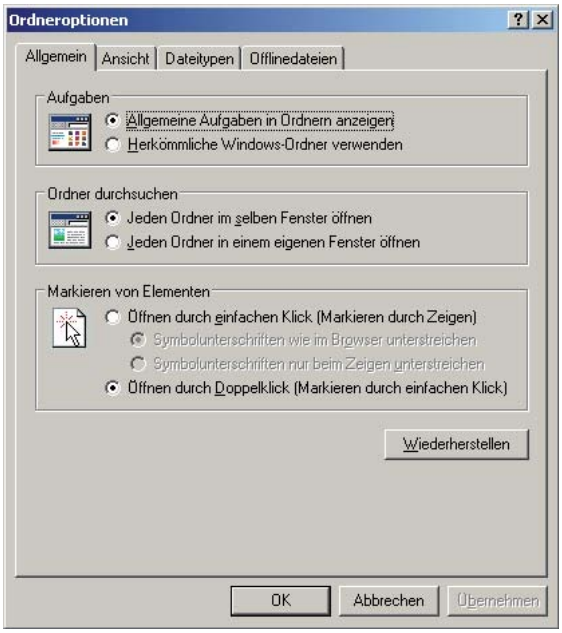
1.2.2 Wähle im Explorer-Fenster in der Menüleiste unter **»Ansicht«** den Menüpunkt **»Details«**.



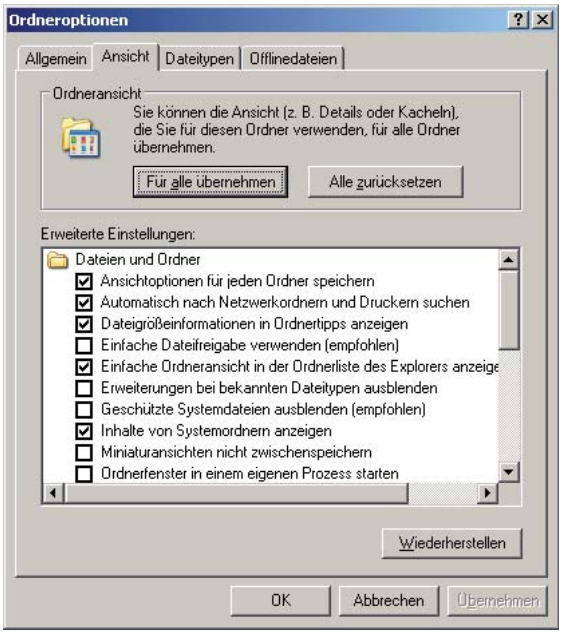
1.2.3 Klicke ebenfalls in der Menüleiste unter **»Extras«** auf den Menüpunkt **»Ordneroptionen«**.



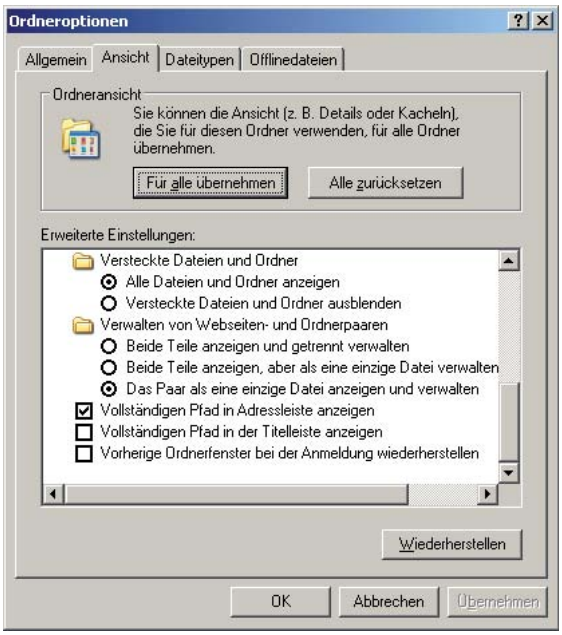
1.2.4 Aktiviere im Fenster **»Ordneroptionen«** die Registerkarte **»Ansicht«** und nimm dort die Folgenden Einstellung(en) vor.



1.2.5 Kein Häkchen bei **»Erweiterung bei bekannten Dateitypen ausblenden«**.



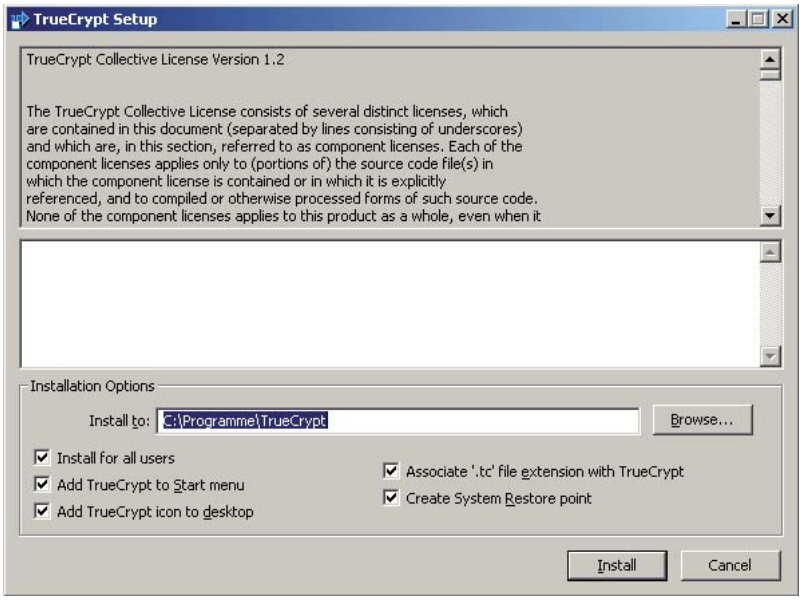
1.2.6 Scrolle ans Ende der Liste herunter und aktiviere bei **»Versteckte Dateien und Ordner«** den Radiobutton **»Alle Dateien und Ordner anzeigen«**. Klicke dazu in den kleinen weißen Kreis vor **»Alle Dateien und Ordner anzeigen«**. Die Markierung (kleiner schwarzer Punkt) springt daraufhin in den Kreis in den du geklickt hast. Bestätige deine Änderungen durch Klicken auf die Schaltfläche `Für alle übernehmen`. Beantworte die Sicherheitsabfrage mit `Ja` und schließe das Fenster **»Ordneroptionen«**.



2. Installation von TrueCrypt

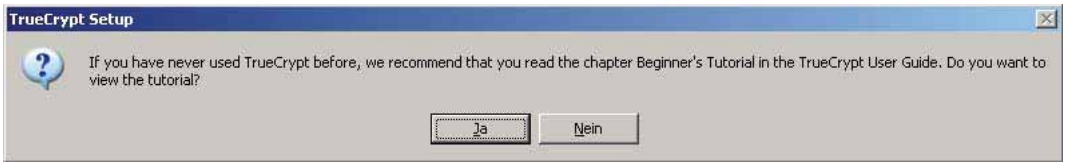
2.1 Geh in den Ordner, in den du das TrueCrypt Paket entpackt hast und starte das Programm **»TrueCrypt Setup.exe«**

2.2 Gib in dem Fenster **»TrueCrypt Setup«** bei **»Install to:«** den Installationspfad **»c:\Programme\TrueCrypt«** an. Die Installation erfolgt beim Klicken auf [Install].

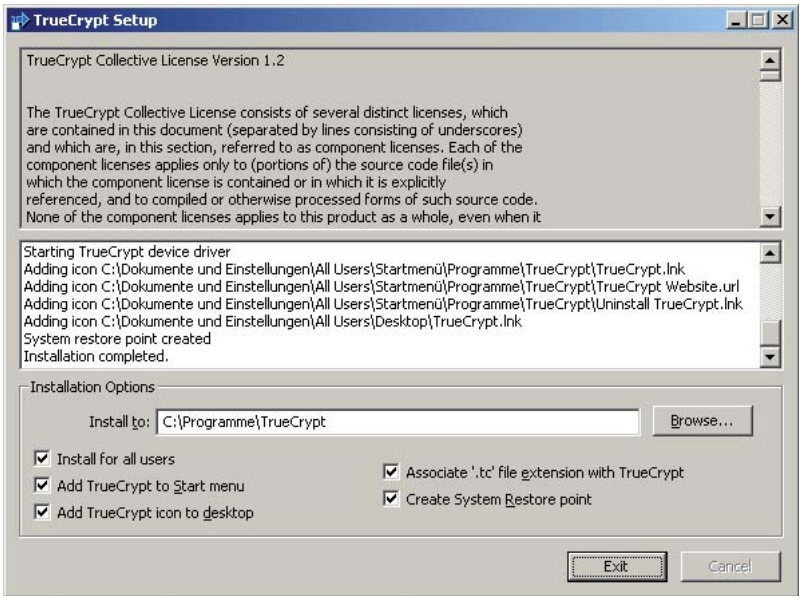


2.3 Nach erfolgreicher Installation erscheint eine Erfolgsmeldung. Bitte mit [OK] bestätigen.

2.4 Die Frage, ob du das TrueCrypt Handbuch lesen möchtest kannst du zunächst verneien. Zur späteren Lektüre öffne die Datei **»C:\Programme\TrueCrypt\TrueCrypt User Guide.pdf«** mit einem entsprechenden Programm. (Beispielsweise: Acrobrat Reader)



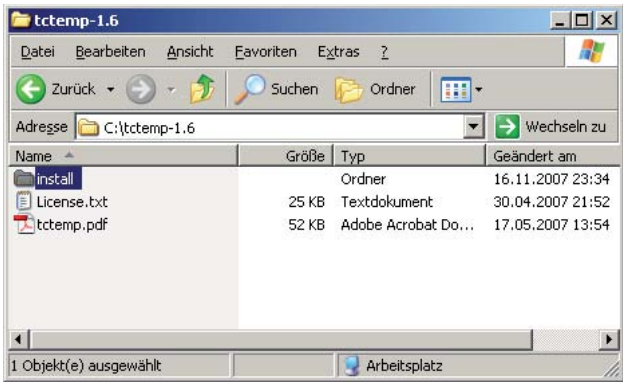
2.5 Der Installationsdialog kann durch klicken auf [Exit] geschlossen werden.



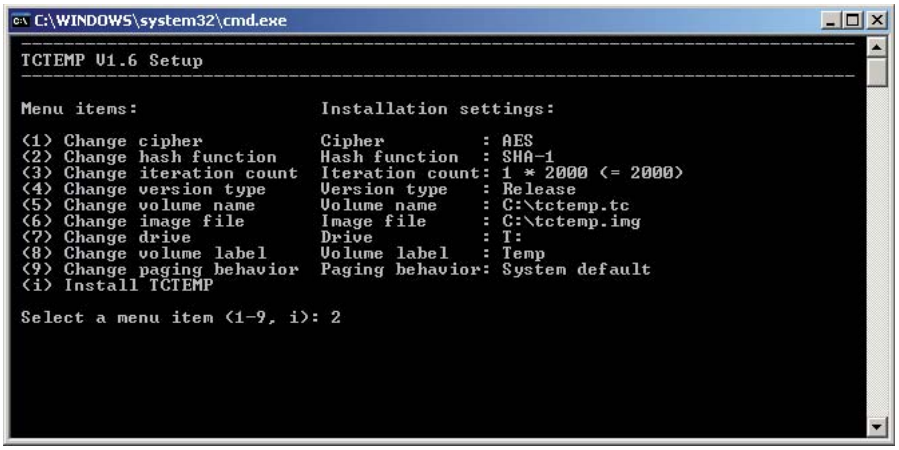
3. Installation von TCTemp

3.1 Voreinstellungen und Installation

3.1.1 Begib dich in den Ordner, in dem du TCTemp entpackt hast und Starte im Unterordner **»install«** die Datei **»install.cmd«**.

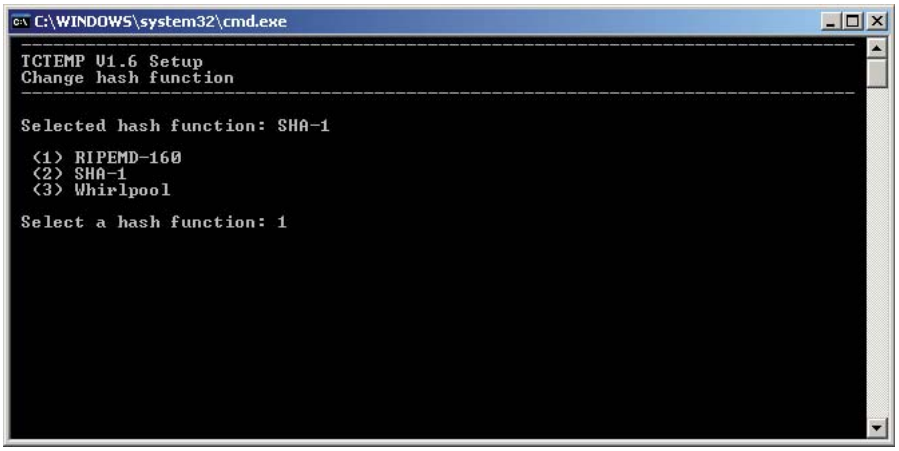


3.1.2 Die nächsten Schritte der TCTemp-Installation erfolgen in einem Fenster mit schwarzem Hintergrund und weißer Schrift, der sogenannten DOS-Eingabeaufforderung. Dort werden verschiedene Einstellungen für TCtemp vorgenommen.

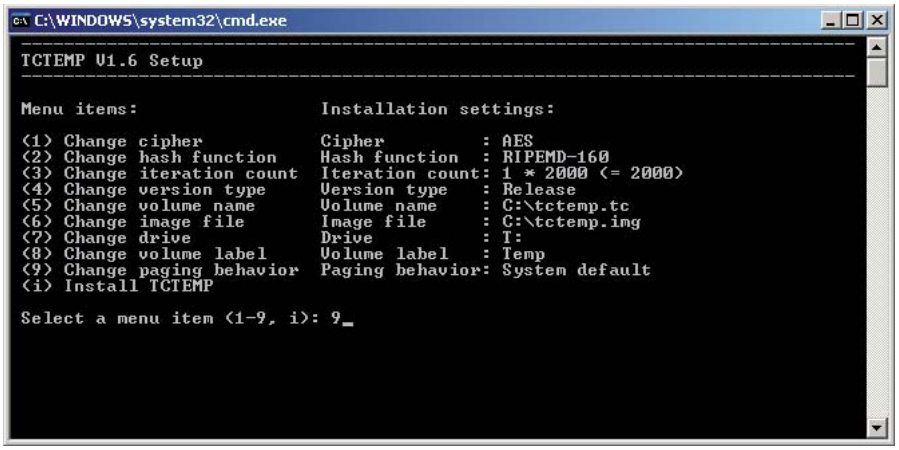


3.1.3 Die Punkte eins und zwei des Menüs geben Auskunft über die verwendete Verschlüsselungsmethode. Verwende am besten die Standard-Einstellung für den ersten Punkt: **»AES«**. Verändere beim zweiten Punkt die Einstellung für **»Hash Function«** auf **»RIPEMD-160«**. (Beim Algorithmus **»SHA-1«** wurde eine Schwachstelle gefunden weshalb dieser als theoretisch angreifbar gilt.) Gib eine *»2«* ein und bestätige mit [Enter] um ins Untermenü zu gelangen.

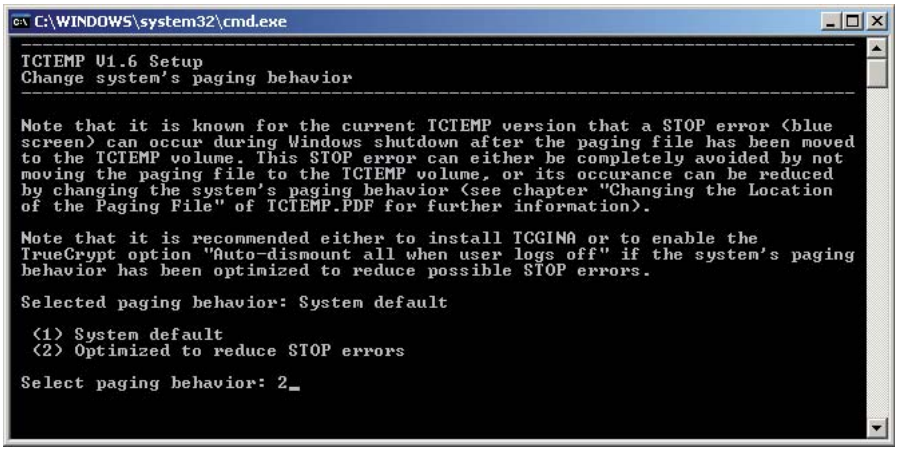
3.1.4 Gib eine *»1«* ein und bestätige mit [Enter] um **»RIPEMD-160«** auszuwählen.



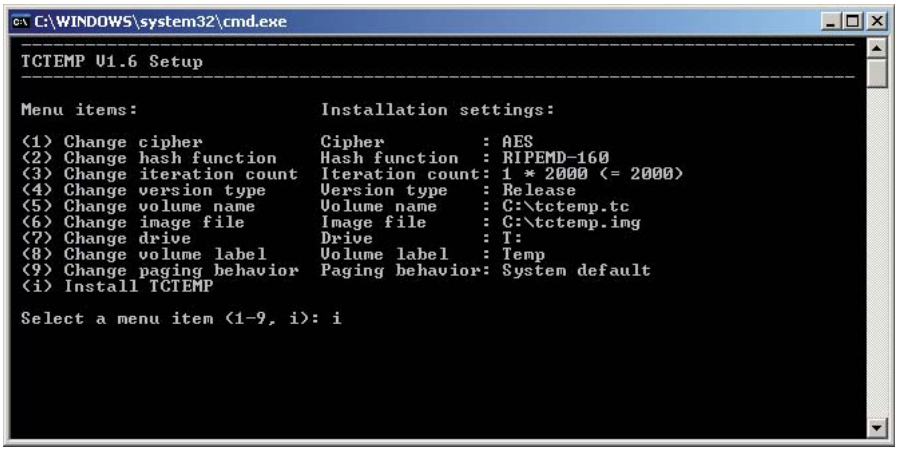
3.1.5 Wieder im Hauptmenü gib eine *»9«* ein und bestätige mit [Enter] um ins Untermenü **»Change paging behavior«** zu wechseln.



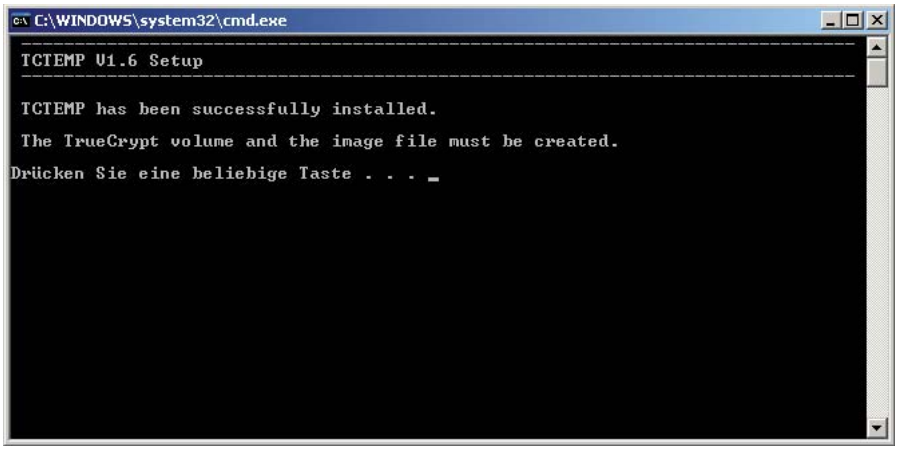
3.1.6 Dort wählst du mit *»2«* und [Enter] die Einstellung **»optimized to reduce STOP errors«**. (Diese Einstellung kann helfen Schwierigkeiten beim Herunterfahren des Rechners zu vermeiden.)



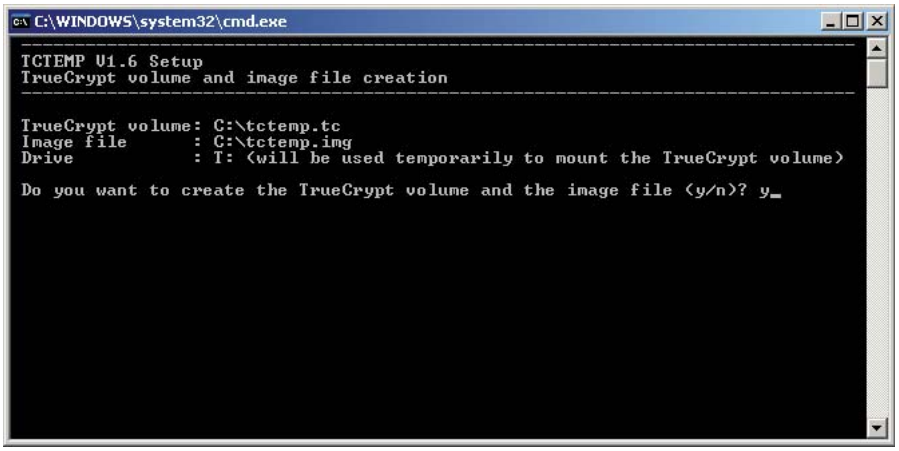
3.1.7 Zurück im Ausgangsmenü überprüfe nochmal alle Einstellungen. Es sollte folgendes angezeigt werden: **»Cipher« = »AES«, »Hash Function« = »RIPEMD-160«, »Iteration Count« = »1 * 2000 (= 2000)«, »Version Type« = »Release«, »Volume Name« = »C:\tctemp.tc«, »Image File« = »C:\tctemp.img«, »Drive« = »T:«, »Volume Label« = »Temp«, »Paging behavior« = »Optimized to reduce STOP errors«**. Starte die Installation durch Eingabe von *»i«* und Enter.



3.1.8 Nach erfolgreicher Installation erscheint der Hinweis, dass ein TrueCrypt Volume (in diesem Fall ein sogenannter Container) und ein dazugehörige Imagedatei (Abbild der zukünftigen Datei- und Ordnerstruktur des temporären Laufwerks) benötigt wird. Drücke eine beliebige Taste um Fortzufahren.

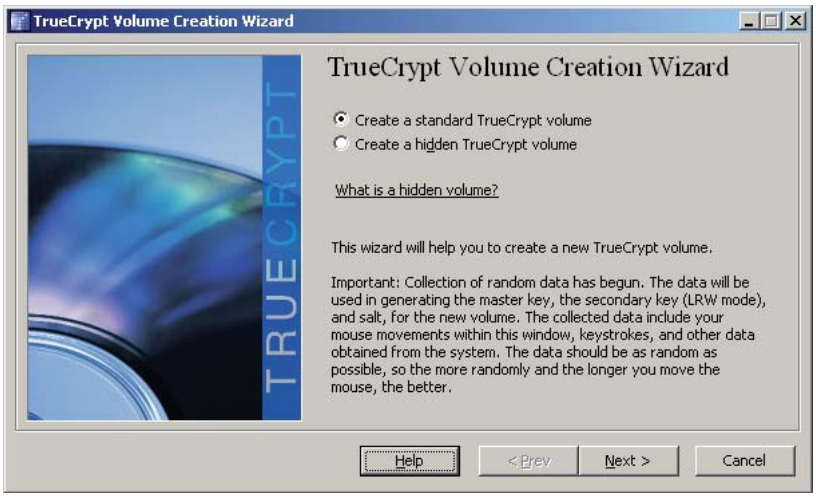


3.1.9 Durch drücken von *»y«* und Enter startest du den **»TrueCrypt Volume Creation Wizard«** in dem weitere Einstellungen erfolgen. Die DOS-Eingabeaufforderung wird später wieder benötigt und bleibt daher im Hintergrund geöffnet.

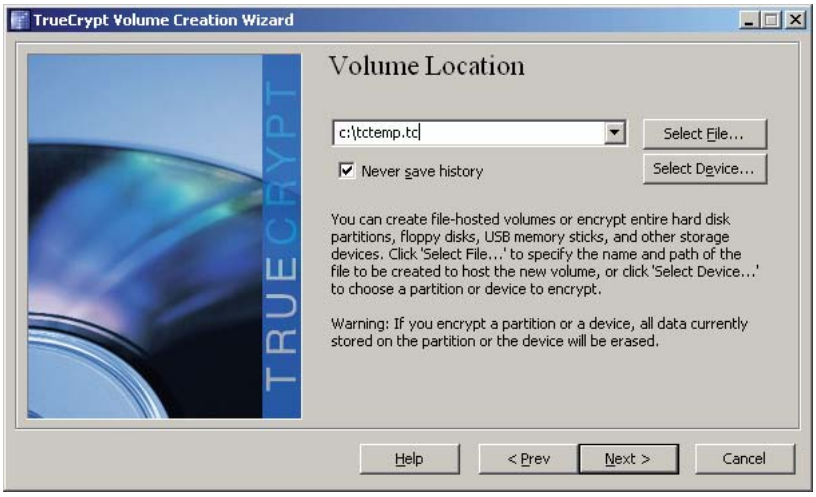


3.2 TCTemp Volume Erstellung

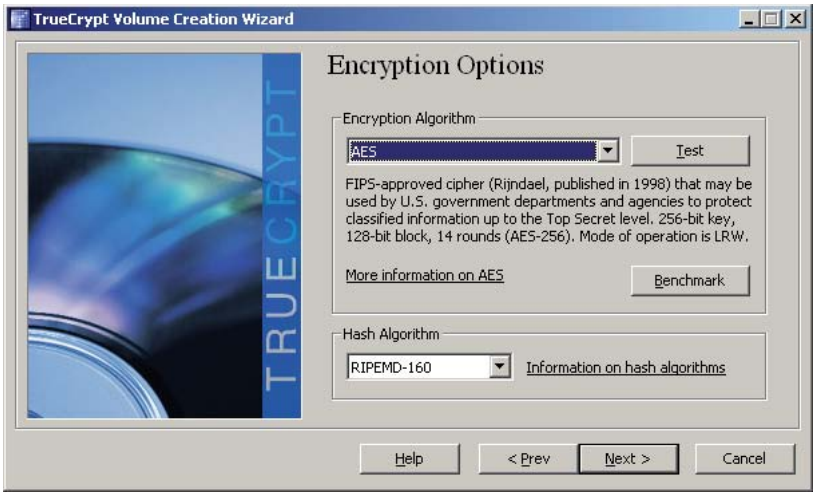
3.2.1 Im **»TrueCrypt Volume Creation Wizard«** wirst du nach der Art des zu erstellenenden Volumes gefragt. In diesem Fall benötigst du ein standard TrueCrypt Volume, kannst die Voreinstellung, **»Create a standard TrueCrypt Volume«** ausgewählt lassen und mit [Next] bestätigen.



3.2.2 Als **»Volume Location«** des TrueCrypt-Containers machst du die gleichen Angaben wie in Schritt 3.1.7 : **»`c:\tctemp.tc`«**. (die Eingabe eines Backslashes erfolgt durch gleichzeitiges drücken der Tasten [Alt Gr] und der Taste auf der sich das **»ß«** und das Fragezeichen befinden. Zum Fortfahren [Next] drücken.

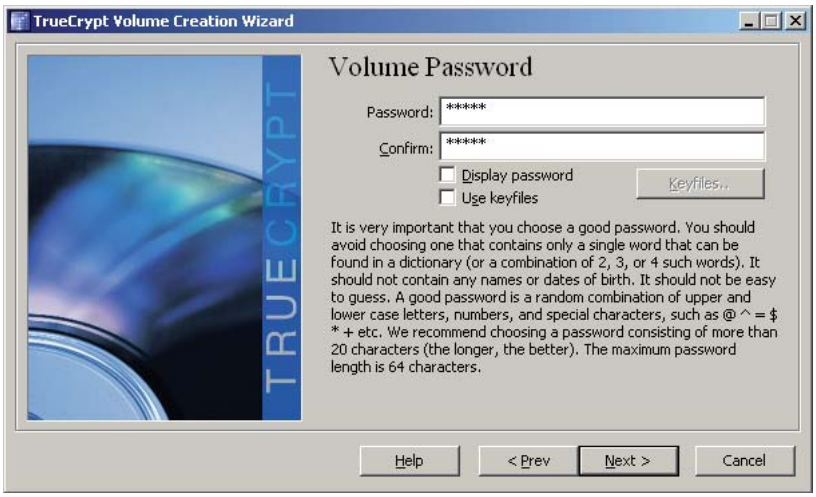


3.2.3 Die Verschlüsselungsoptionen haben wir bereits unter Punkt 3.1.4 ausgewählt. Wenn **»AES«** und **»RIPEMD-160«** eingestellt ist und du keine Änderungen vornehmen möchtest kannst du mit [Next] fortfahren.

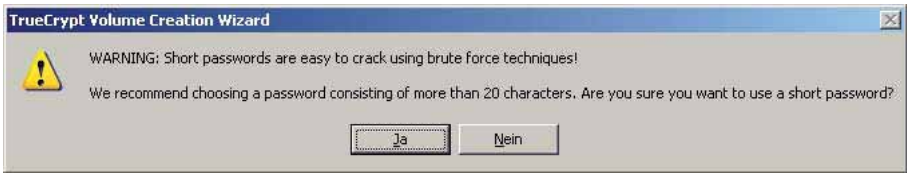


3.2.4 In das Feld unter der Überschrift **»Volume Size«** haben wir einen Wert von 7000 MB eingegeben. Gemessen an der Größe unserer Festplatte waren das etwa 15% der gesamten Kapazität. Dieser Wert kann als Richtwert dienen, wenn du nicht weißt wie groß dein TCTemp Laufwerk sein soll. Damit der Wert in Megabyte angegeben wird, achte darauf, den Radiobutton vor **»MB«** auszuwählen. Bestätige mit [Next].

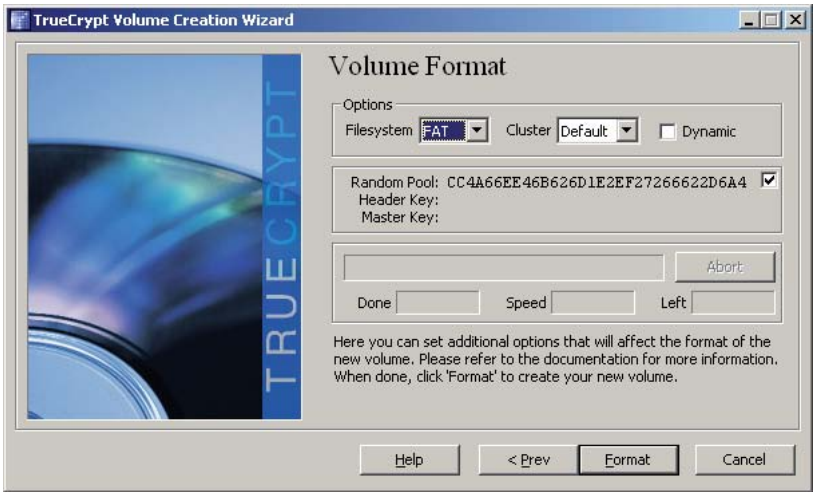
3.2.5 Ausnahmsweise darfst du hier ein schwaches Passwort vergeben (z.B. *»test«* oder *»12345«*), da dieses Passwort keine weitere Verwendung findet. Du wirst es in einem der nächsten Schritte noch einmal benutzen, bevor zukünftig bei jedem Hochfahren des Rechners aus komplizierten Zufallsallgorithmen ein sehr starkes Passwort generiert wird. Damit wird der Zugriff auf die während einer Windows Sitzung angefallenen temporären Daten nach einem Neustart des Rechners unmöglich.



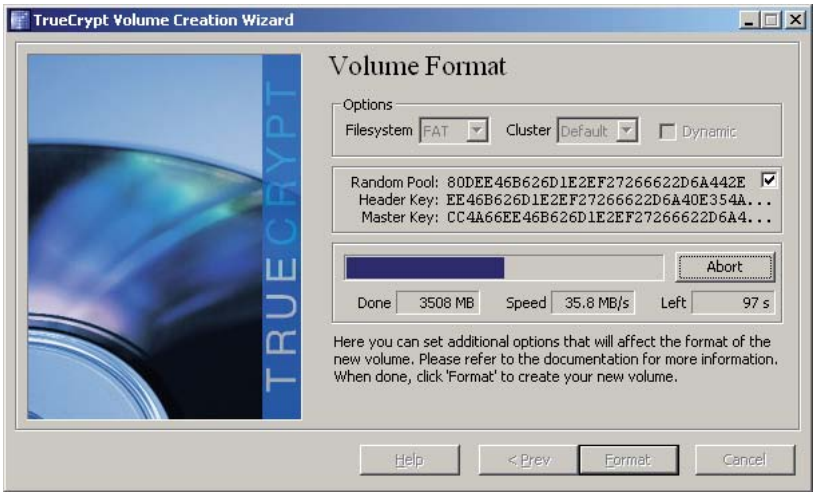
3.2.6 Die anschließende Warnung erinnert dich auch in diesem Fall daran komplexe Passworte zu verwenden. Die Sicherheitsabfrage kannst du hier aber mit [Ja] beantworten.



3.2.7 Für das Temporäre TrueCrypt Volume kannst du sowohl NTFS als auch FAT als Dateisystem auswählen. Behalte die Voreinstellung, wenn du nicht sicher bist was du wählen sollst. Durch klicken auf [Format] beginnt die Formatierung, die einige Minuten benötigt.



3.2.8 Im Anschluss an die Formatierung des TrueCrypt Volumes erscheint eine Erfolgsmeldung, die du mit [OK] bestätigen kannst.

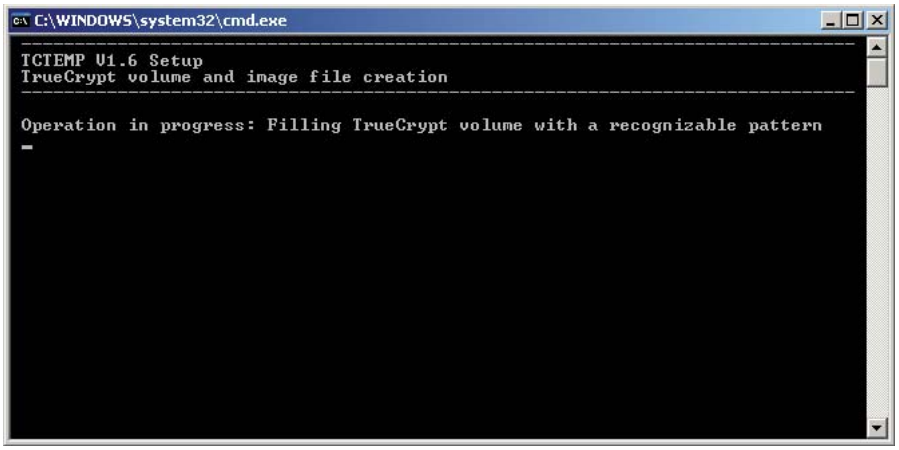


3.2.9 Der **»TrueCrypt Volume Creation Wizard«** kann jetzt durch drücken auf [Exit] geschlossen werden.

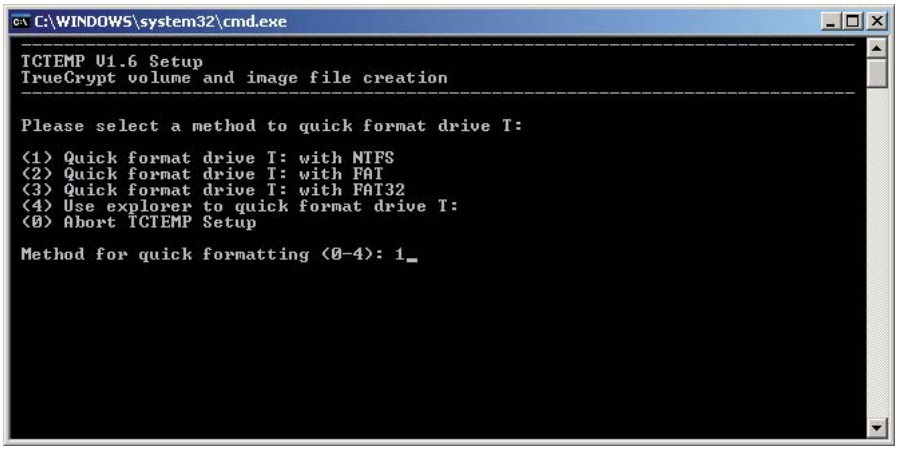
3.2.10 Es erscheint ein Fenster, in dem du aufgefordert wirst, das Passwort für **»tctemp.tc«** einzugeben. Gib hier das unter Punkt 3.2.7 vergebene Passwort ein und bestätige mit [OK] oder [Enter].

3.3 TCTemp Image Erstellung

3.3.1 Die nächsten Schritte erfolgen wieder in der DOS-Eingabeaufforderung, die sich während der letzten Schritte im Hintergrund befand. Zunächst erscheint jedoch eine Fortschrittsanzeige während Zufallsdaten auf das TCTemp-Laufwerk geschrieben werden. Dies kann je nach größe des Laufwerks wieder einige Minuten dauern, jedoch etwas länger als die soeben erfolgte Formatierung.



3.3.2 Anschließend ist eine Schnellformatierung erforderlich. Um mit der Voreinstellung - FAT32 - zu formatieren drücke *»3«* und [Enter].



3.3.3 Es erscheint ein Warnhinweis, dass alle Daten auf dem TrueCrypt Volume gelöscht werden. Bestätige die Formatierung nochmals mit *»j«* und Enter.

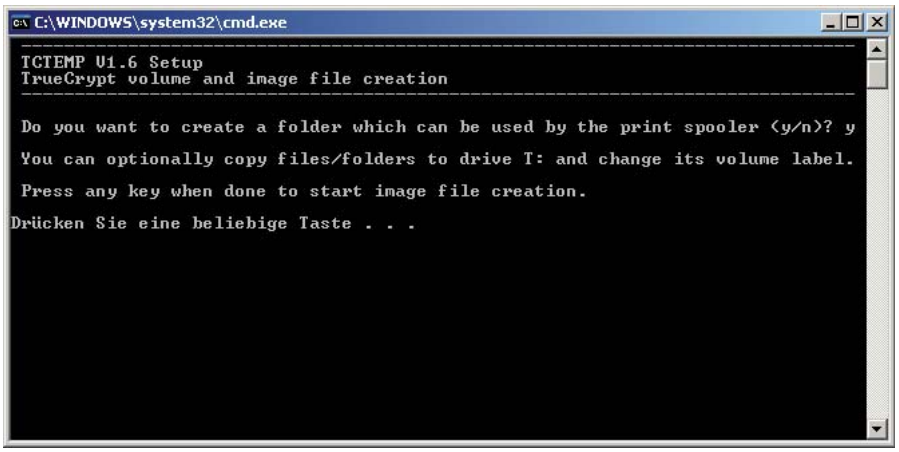
```
C:\WINDOWS\system32\cmd.exe
 ---------------------------------------------------------------------------
 TCTEMP V1.6 Setup
 TrueCrypt volume and image file creation
 ---------------------------------------------------------------------------

 Please select a method to quick format drive T:

 (1) Quick format drive T: with NTFS
 (2) Quick format drive T: with FAT
 (3) Quick format drive T: with FAT32
 (4) Use explorer to quick format drive T:
 (0) Abort TCTEMP Setup

 Method for quick formatting (0-4): 1
Der Typ des Dateisystems ist RAW.
Das neue Dateisystem ist NTFS.

ACHTUNG: ALLE DATEN AUF DEM
FESTPLATTENLAUFWERK T: GEHEN VERLOREN!
Formatierung durchführen (J/N)? j
```

3.3.4 Nun kann TCTemp einen Ordner anlegen, in dem der Windows-Druckerspooler (Drucker-Warteschlange) zukünftig Druckaufträge zwischenzuspeichert. Diese Druckaufträge, die möglicherweise auch sensible Daten enthalten, würden sonst in einem unverschlüsselten Bereich der Festplatte zwischengespeichert. Das anlegen dieses Ordners erfolgt durch Eingabe von *»y«* und Enter.

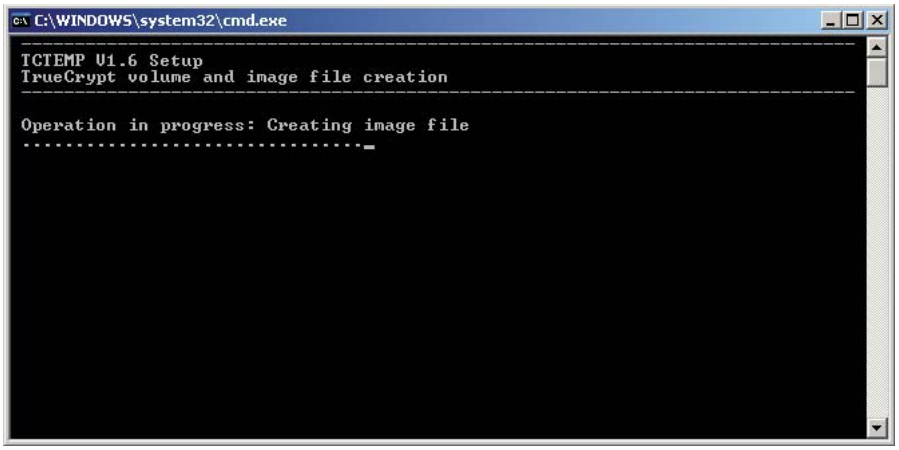
```
C:\WINDOWS\system32\cmd.exe
 ---------------------------------------------------------------------------
 TCTEMP V1.6 Setup
 TrueCrypt volume and image file creation
 ---------------------------------------------------------------------------

 Please select a method to quick format drive T:

 (1) Quick format drive T: with NTFS
 (2) Quick format drive T: with FAT
 (3) Quick format drive T: with FAT32
 (4) Use explorer to quick format drive T:
 (0) Abort TCTEMP Setup

 Method for quick formatting (0-4): 1
Der Typ des Dateisystems ist RAW.
Das neue Dateisystem ist NTFS.

ACHTUNG: ALLE DATEN AUF DEM
FESTPLATTENLAUFWERK T: GEHEN VERLOREN!
Formatierung durchführen (J/N)? j
Formatieren mit Schnellformatierung 6999 MB
Struktur des Dateisystems wird erstellt.
_
```

```
C:\WINDOWS\system32\cmd.exe
 ---------------------------------------------------------------------------
 TCTEMP V1.6 Setup
 TrueCrypt volume and image file creation
 ---------------------------------------------------------------------------

 Do you want to create a folder which can be used by the print spooler (y/n)? y
```

3.3.5 Anschließend drücke in der DOS-Eingabeaufforderung eine beliebige Taste um die Erstellung der Image-Datei zu veranlassen.

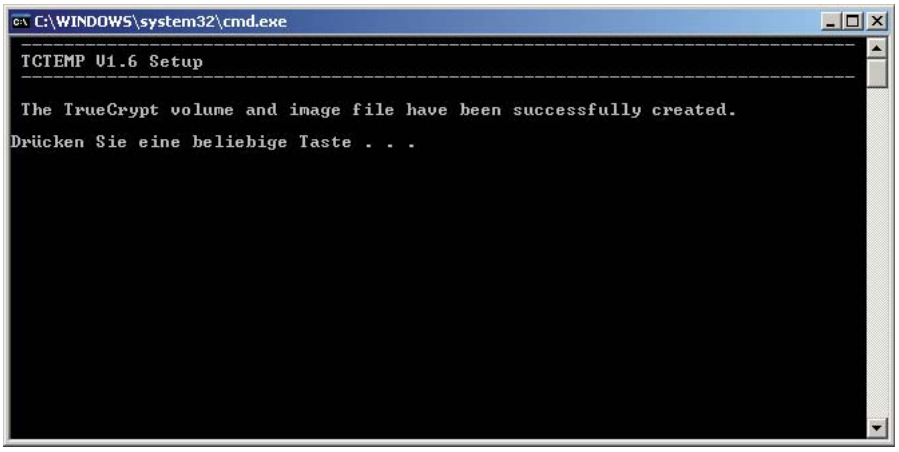


3.3.6 Dieser Vorgang kann mehrere Minuten dauern. Die Dauer ist abhängig von der Volumen-Größe beträgt aber wahrscheinlich mehr als zehn Minuten. Solange ist eine Fortschrittsanzeige zu sehen.



3.3.7 Die Erstellung des TCTemp Laufwerks ist nun abgeschlossen. Durch drücken irgendeiner Taste wird die DOS-Eingabeaufforderung geschlossen.

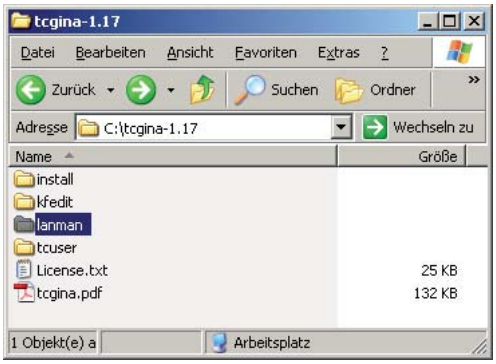
3.3.8 Starte jetzt deinen Rechner neu!



3.4 Windows XP Einstellungen

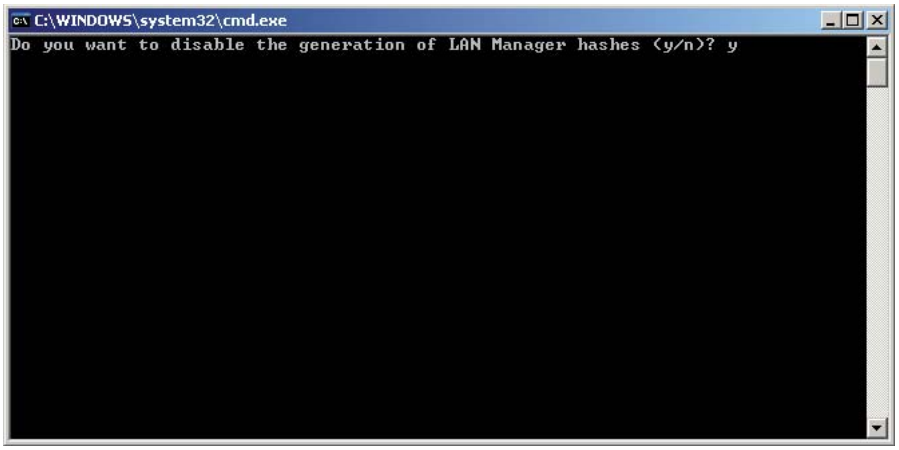
3.4.1 Disable LAN Manager Hashes

3.4.1.1 Begib dich in das Verzeichnis in das du TCGINA enpackt hast und gehe in dem Unterordner **»lanman«**.

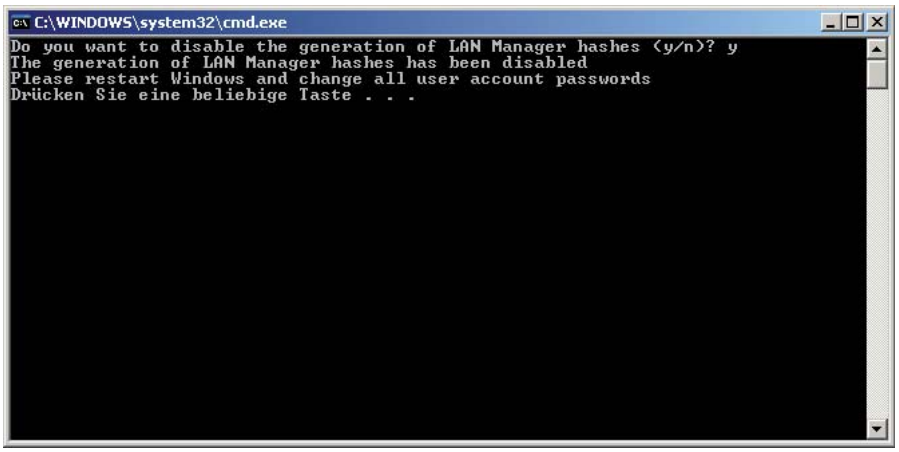


3.4.1.2 Starte dort die Datei **»Disable_LAN_Manager_hashes.cmd«** durch einen Doppelklick oder Klick und Enter.

3.4.1.3 Bestätige die Nachfrage innerhalb der DOS-Eingabeaufforderung mit *»y«* + Enter.

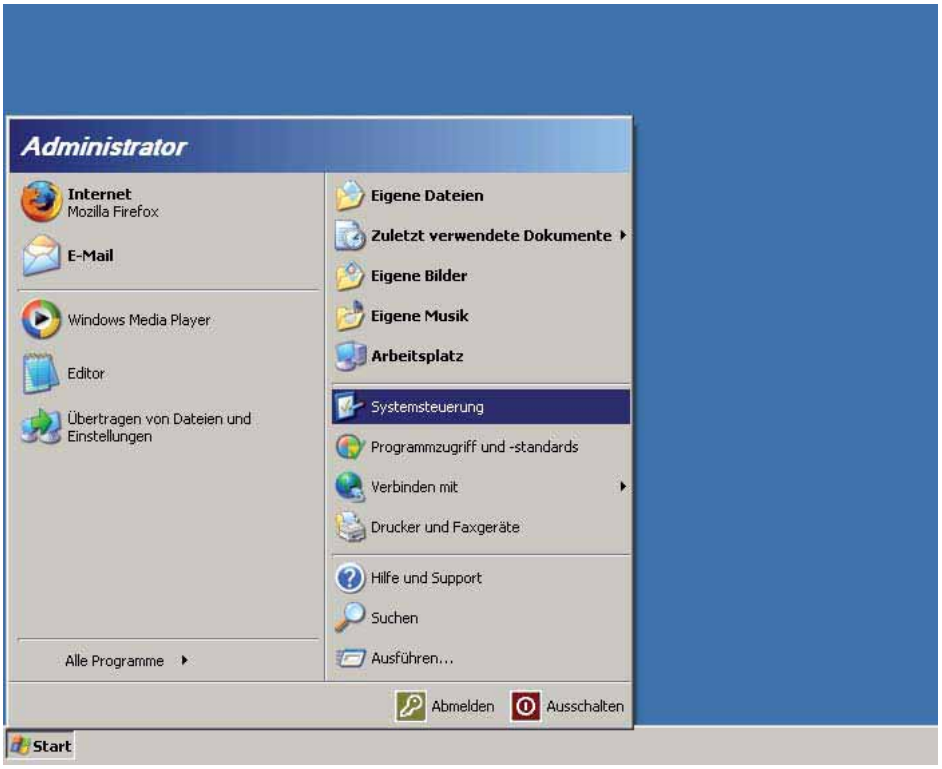


3.4.1.4 Drücke irgendeine Taste zum bestätigen der Erfolgsmeldung. Die DOS-Eingabeaufforderung schließt sich daraufhin automatisch.

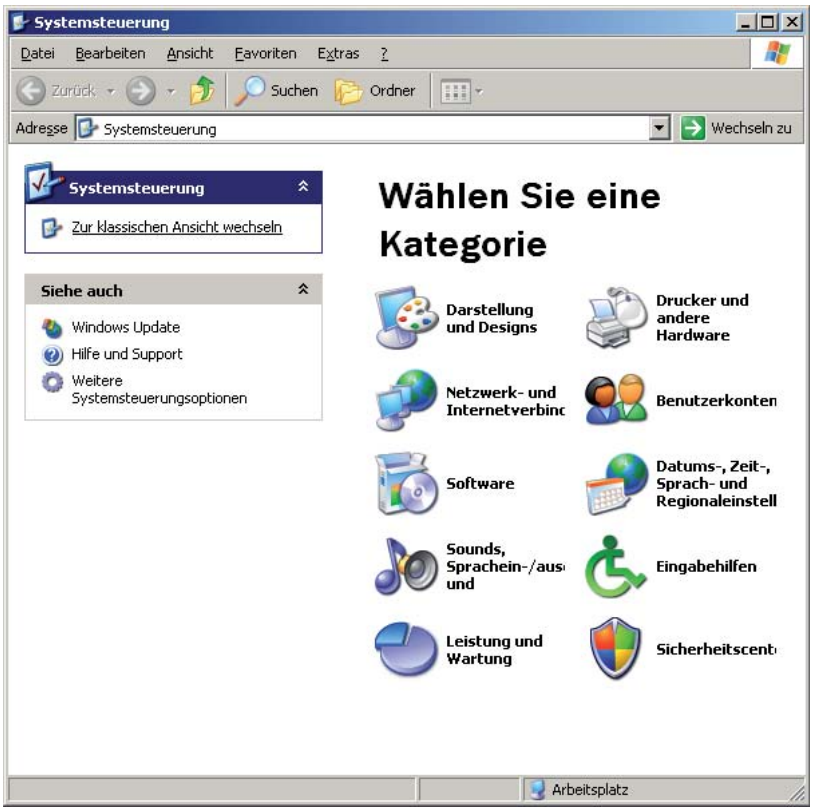


3.4.2 Aufrufen der Systemeinstellungen

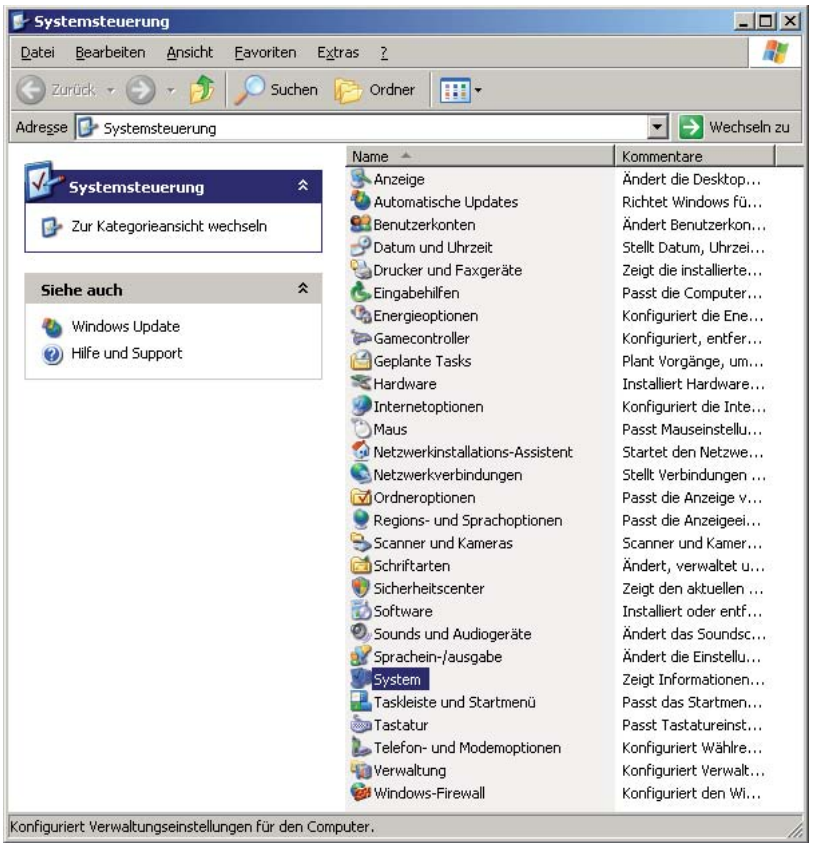
3.4.2.1 Klicke in der Windows XP Taskleiste auf **»Start«** um das Startmenü anzeigen zulassen. Öffne durch einfachen Klick die Systemsteuerung.



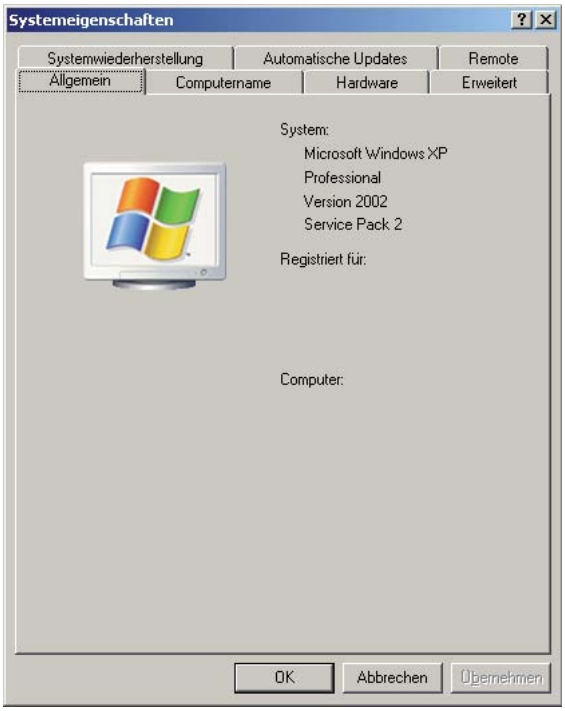
3.4.2.2 Klicke in der Systemsteuerung auf den Link **»Zur klassischen Ansicht wechseln«**. Wenn die klassische Ansicht bereits aktiviert ist, steht dort**«Zur modernen Ansicht wechseln«**.



3.4.2.3 Rufe innerhalb der klassischen Ansicht der Systemsteuerung durch Doppelklick auf den Menüpunkt **»System«** die Systemeigenschaften auf.

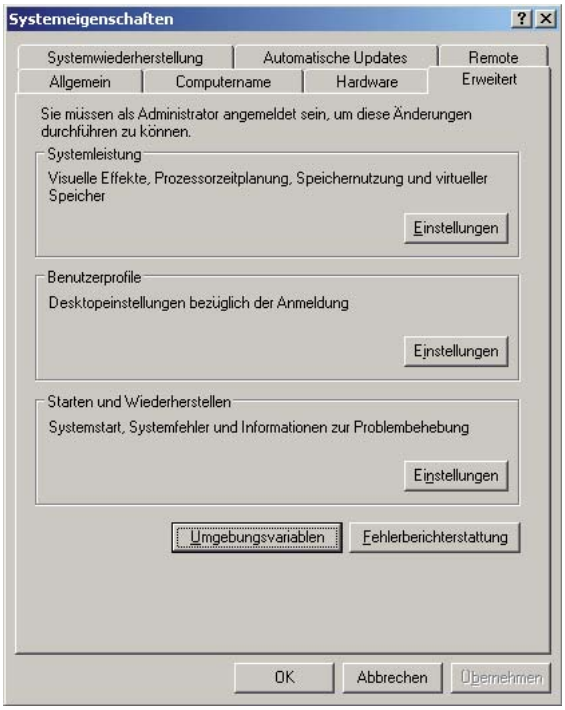


3.4.2.4 Die notwendigen Einstellungen erfolgen auf der Registerkarte **»Erweitert«**.

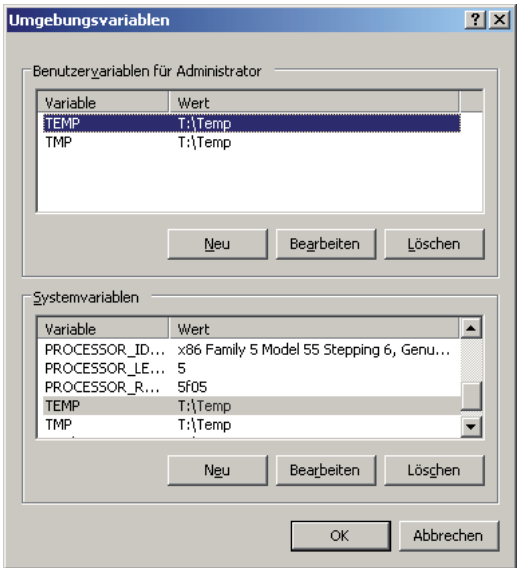


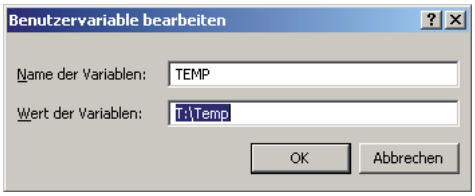
3.4.3 Anpassung der Umgebungsvariablen

3.4.3.1 Durch klicken auf die Schaltfläche `Umgebungsvariablen` erscheint ein weiteres Fenster.



3.4.3.2 In der oberen Hälfte des Fensters sind die Variablen **»TEMP«** und **»TMP«** aufgeführt. Durch Doppelklick auf den Namen der Variablen erscheint ein Fenster in dem du sowohl Namen als auch Wert der Variablen ändern kanst. Die Namen der Variablen bleiben unverändert. Gib jeweils den Pfad **»`T:\Temp`«** ein drücken anschließend auf OK.





3.4.3.3 In der unteren Hälfte des Fensters befindet sich eine weitere Liste mit **»Systemvariablen«**. Benutze den Scrollbalken um ans Ende der Liste zu gelangen. Dort stehen ebenfalls zwei Variablen mit den Namen **»TEMP«** und **»TMP«**. Durch Doppelklick auf die Variable öffnet sich wieder ein Fenster in dem du Namen und Wert der Variablen ändern kannst. Ändere die Werte beider Variablen auf **»`T:\Temp`«** und drücke auf OK. Drücke im Fenster **»Umgebungsvariablen«**ebenfalls auf OK um die Änderungen zu übernehmen.

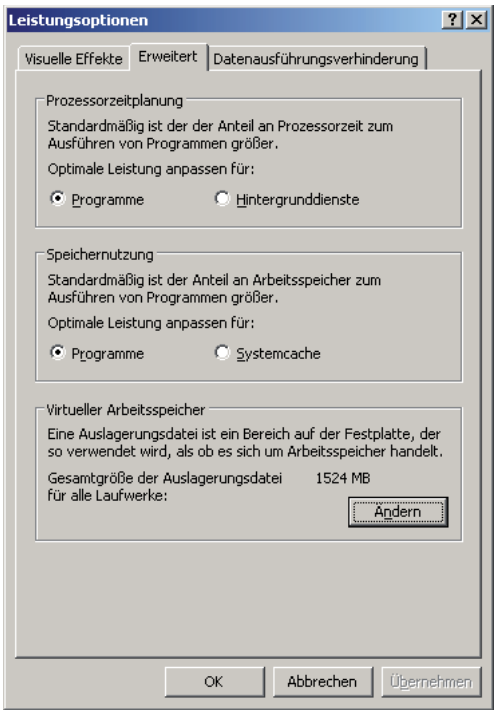
3.4.3.4 Das Fenster **»Umgebungsvariablen«** kann jetzt geschlossen werden.

3.4.4 Anpassung der Auslagerungsdatei

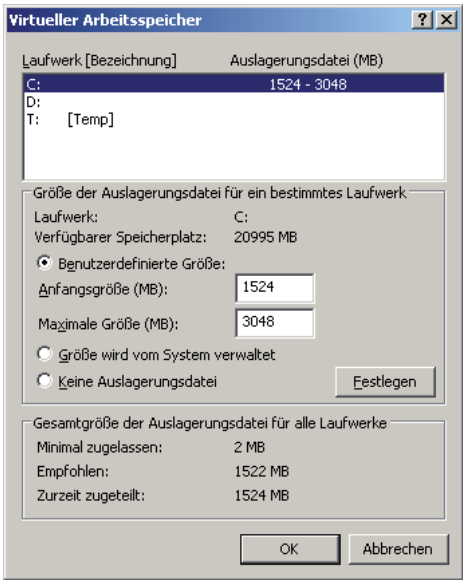
3.4.4.1 Auf der Registerkarte **»Erweitert«** im Fenster **»Systemeigenschaften«** befindet sich ein mit **»Systemleistung«** bezeichneter Bereich. Durch klicken auf die Schaltfläche [Einstellungen] gelangst du zu den **»Leistungsoptionen«**.

3.4.4.2 Im Fenster **»Leistungsoptionen«** wählst du die Registerkarte **»Erweitert«**.

3.4.4.3 Weiter unten auf dieser Registerkarte befindet sich ein mit **»Virtueller Arbeitsspeicher«** bezeichneter Bereich. Dort klickst du auf die Schaltfläche [Ändern].

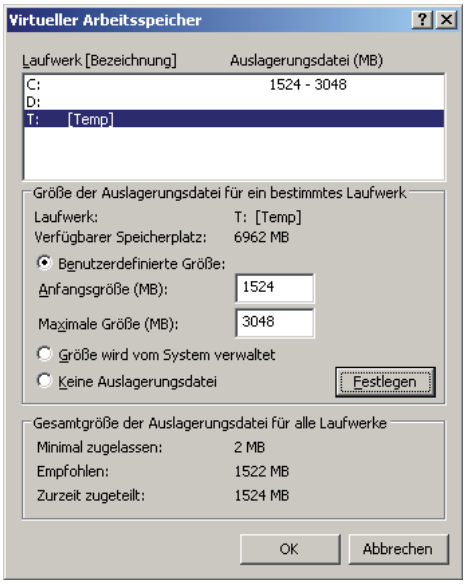


3.4.4.4 Es erscheint das Fenster **»Virtueller Arbeitsspeicher«**. Im oberen Bereich dieses Fenster werden auf der linken Seite alle Festplatten (Partitionen) des Rechners mit deren Laufwerksbuchstaben angezeigt. Daneben findet sich in eckigen Klammern die selbst gewählte Bezeichnung des Laufwerks. In der linken Spalte steht die Größe der auf dem Laufwerk angelgten Auslagerungsdatei.

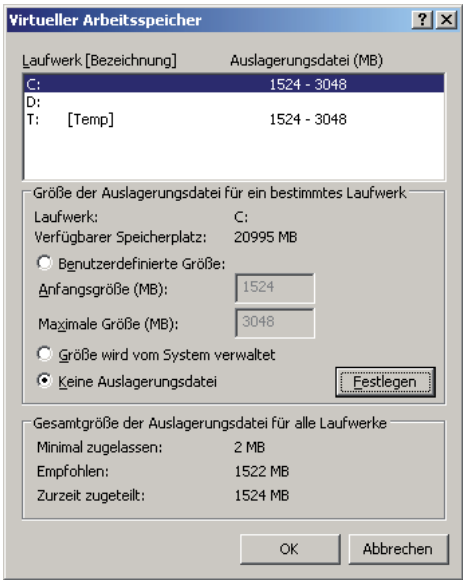


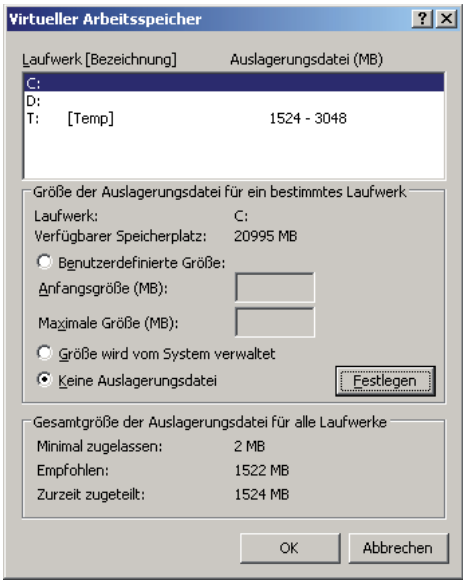
3.4.4.5 Klicke jetzt einmal auf das Laufwerk mit dem Buchstaben **»T:«** bzw der in eckigen Klammern stehenden Laufwerksbezeichnung **»TEMP«** (Vorausgesetzt du hast das Laufwerk auch so benannt). Die entsprechende Zeile ist jetzt Blau hinterlegt.

3.4.4.6 In dem Fenster befindet sich ein Bereich mit der Bezeichnung **»Größe der Auslagerungsdatei für ein bestimmtes Laufwerk«**. Wähle hier den ersten Radiobutton mit dem Namen **»Benutzerdefinierte Größe«** und übertrage die für das Systemlaufwerk (in den meisten Fällen Laufwerksbuchstabe **»C:«**) vergeben Werte in die Felder **»Anfangswert«** und **»Maximalwert«** (Die Größe wird oben angezeigt). Anschließend klickst du auf die Schaltfläche `Festlegen`.



3.4.4.7 Wähle nun das Systemlaufwerk (Laufwerksbuchstabe **»C:«**) an, so dass die entsprechende Zeile in der Laufwerksübersicht blau hinterlegt ist. Setze im mittleren Bereich den Radiobutton vor **»Keine Auslagerungsdatei«** und bestätige durch Drücken auf die Schaltfläche [Festlegen]. Anschließend ist eine erneute Bestätigung erforderlich. Drücke dazu auf [OK].

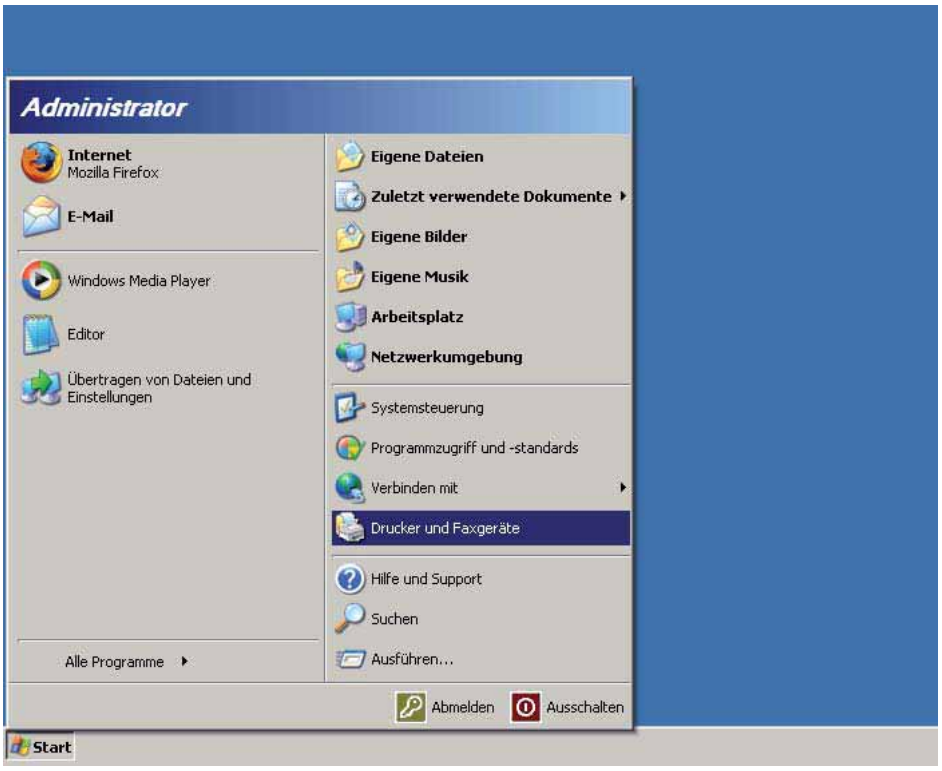




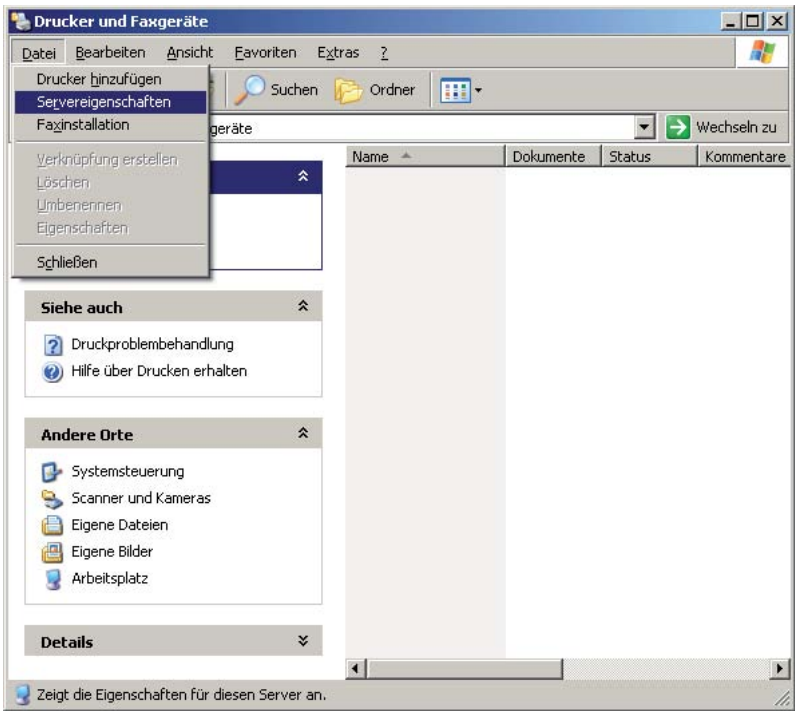
3.4.4.8 Es erscheint der Hinweis, dass die Änderungen erst nach dem nächsten Rechnerneustart wirksam werden. Bestätige diese Meldung mit [OK]. (Du wirst den Rechner später manuell neustarten.)

3.4.5 Anpassung des Druckerspoolers

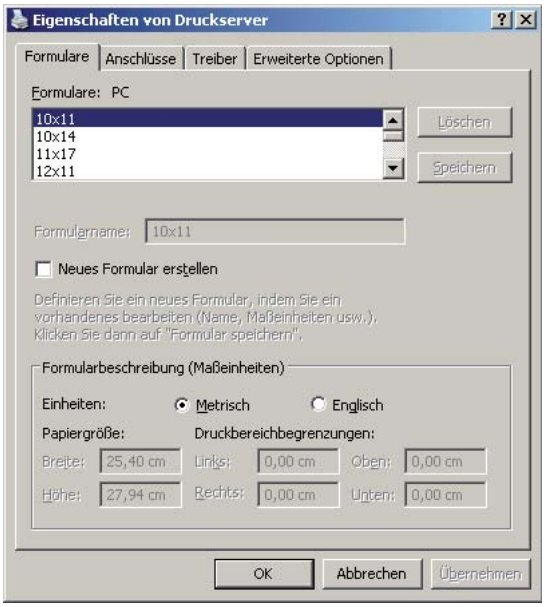
3.4.5.1 Öffne das Startmenü und klicke auf den Menüpunkt **»Drucker und Faxgeräte«**. (alternativ ist dieser Menüpunkt auch in der Systemsteuerung zu finden)



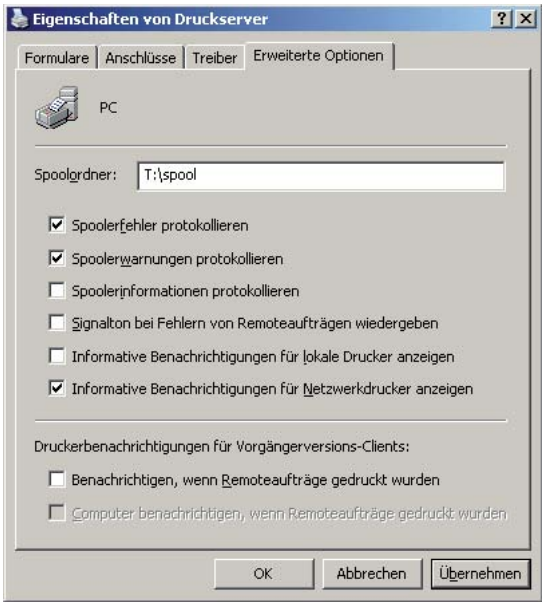
3.4.5.2 In dem Fenster **»Drucker und Faxgeräte«** klickst du im Menü unter **»Datei«** auf den Menüpunkt **»Servereigenschaften«**.



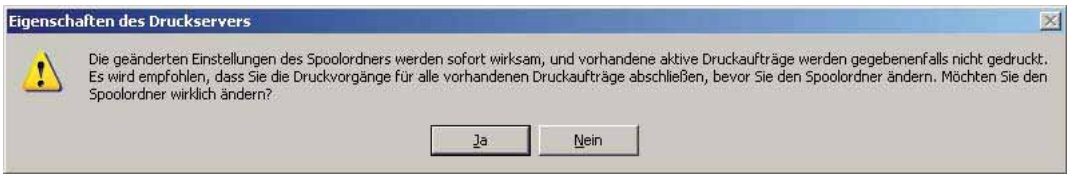
3.4.5.3 Im sich daraufhin öffnenden Fenster **»Eigenschaften von Druckserver«** wählst du die Registerkarte **»Erweiterte Optionen«**.



3.4.5.4 In dem Eingabefeld mit der Bezeichnung **»Spoolordner«** trägst du den Laufwerksbuchstaben des TCTemp Laufwerks (in unserem Fall **»`T:`«**) gefolgt von einem Backslash und dem Ordnernamen **»`spool`«** ein. Also **»`T:\spool`«**. Anschließend mit klicken auf [Übernehmen] bestätigen.

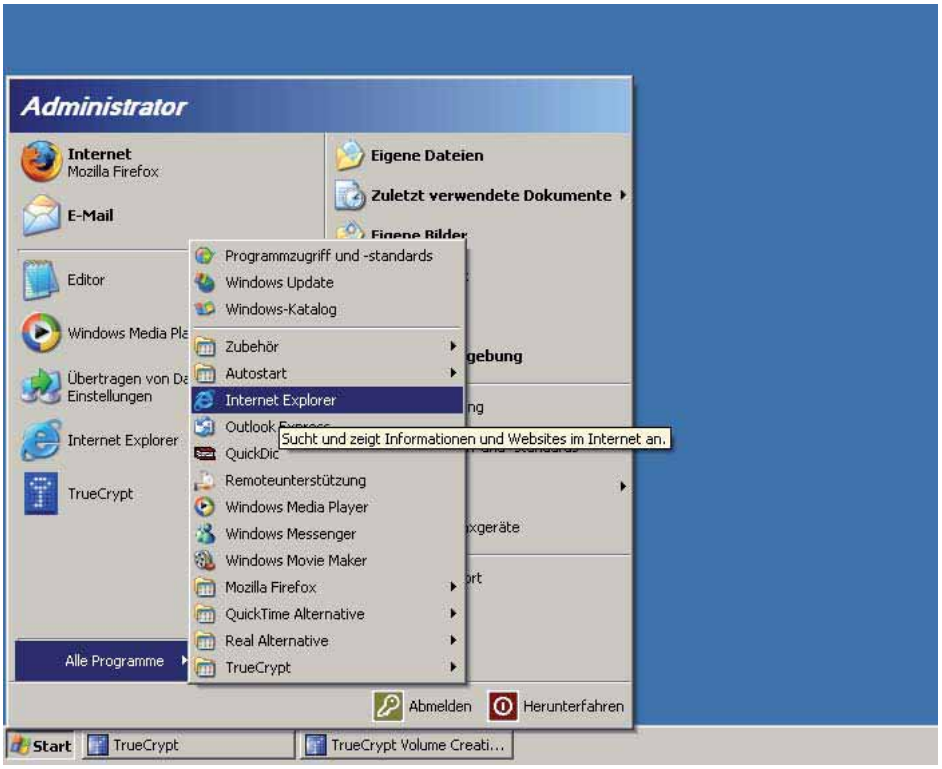


3.4.5.5 Es erscheint ein Hinweis, dass nach erfolgter Änderung des Druckerspoolers, zuvor abgeschickte Druckaufträge nicht mehr gedruckt werden. Die Frage ob du den Spoolordner wirklich ändern möchtest beantwortes du mit [Ja]. Die beiden Fenster »Eigenschaften von Druckserver« und »Leistungsoptionen« kannst du nun schließen.

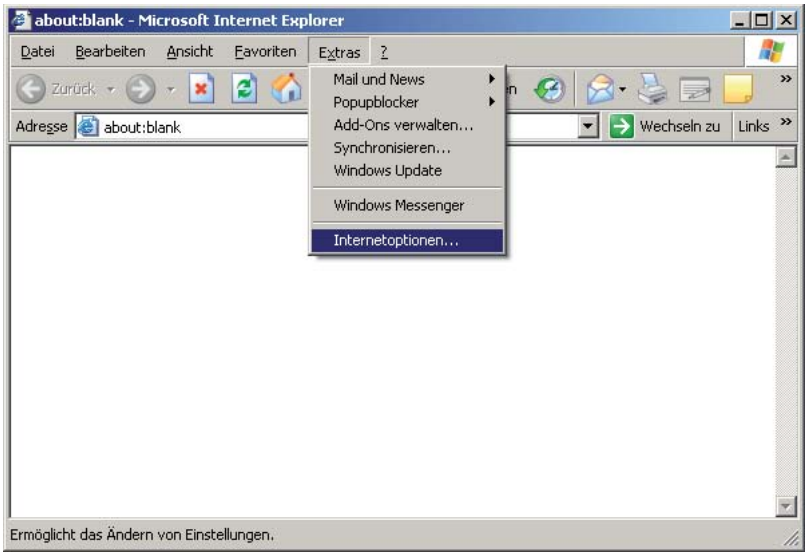


3.4.6 Anpassung des Internet Explorers

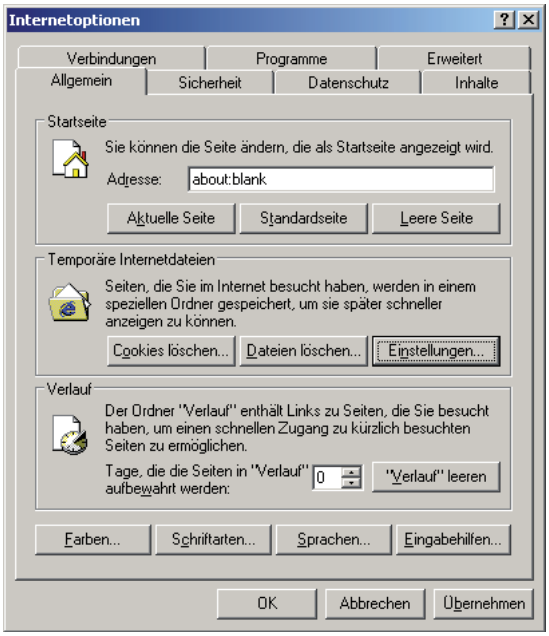
3.4.6.1 Die folgenden Änderungen, betreffen den **»Internet Explorer«** und sollen ebenfalls verhindern das sensiblen Daten (z.B. besuchte Webseiten, Cookies) auf unverschlüsselten Bereichen des Rechners gespeichert werden. Öffne dazu das Startmenü und klicke auf den Eintrag **»Internet Explorer«**.



3.4.6.2 Im Internet Explorers klickst du im Menü unter **»Extras«** auf den Menüpunkt **»Internetoptionen«**.



3.4.6.3 In dem erscheinenden Fenster **»Internetoptionen«** ist die benötigte Registerkarte **»Allgemein«** ausgewählt. Setze im unteren Bereich der Registerkarte mit der Bezeichnung **»Verlauf«** den Wert für **»Tage, die die Seiten im 'Verlauf' aufbewahrt werden:«** auf *»0«*. Anschließend klickst du auf die Schaltfläche `'Verlauf' leeren`.



3.4.6.4 Die Rückfrage, ob der Verlauf wirklich gelöscht werden soll, mit `Ja` beantworten.

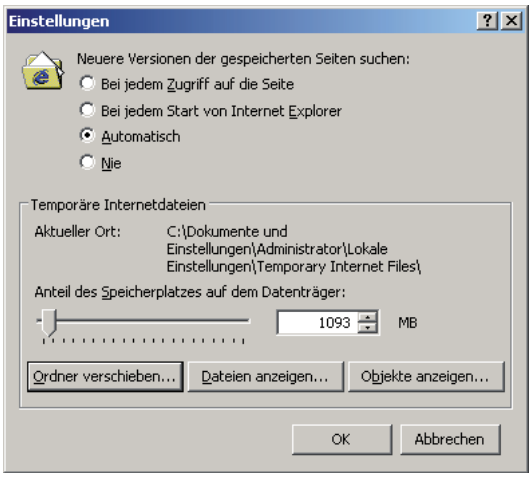
3.4.6.5 Im mittleren Bereich mit der Bezeichnung **»Temporäre Internetdateien«** klickst du auf die Schaltfläche `Cookies löschen...`.

3.4.6.6 Die Rückfrage wird mit `OK` beantwortet.

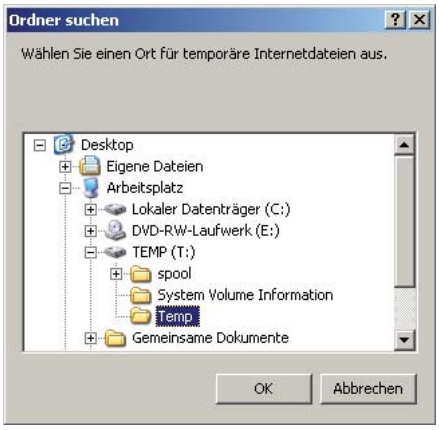
3.4.6.7 Ebenfalls im mittleren Bereich der Registerkarte klickst du auf die zweite Schaltfläche `Dateien löschen...`.

3.4.6.8 Bevor die Rückfrage mit `OK` erfolgen kann, sicherstellen, dass das Häkchen bei **»Alle Offlineinhalte löschen«** gesetzt ist.

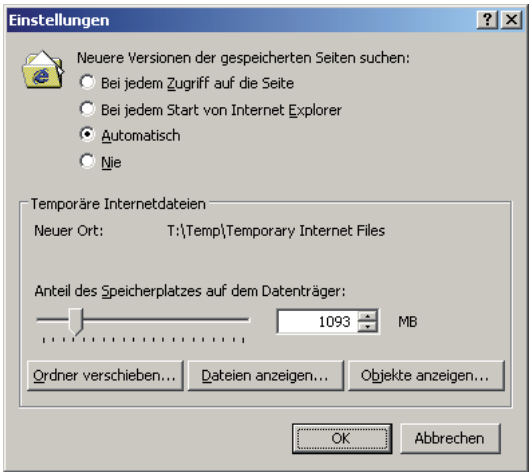
3.4.6.9 Die dritte Schaltfläche mit der Bezeichnung `Einstellungen` anklicken. Im Fenster **»Einstellungen«** auf die Schaltfläche `Ordner verschieben...` klicken.



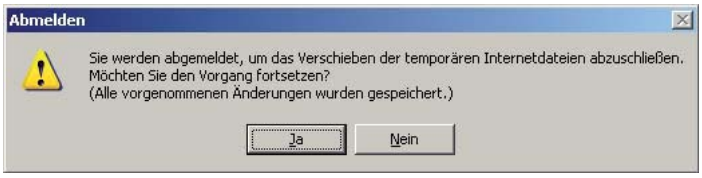
3.4.6.10 In dem sich öffnenden Fenster, klickst du auf das kleine Pluszeichen vor dem Laufwerk **»Temp (T:)«**. Die Ordnerstruktur ist mit dem Ordner **»`Temp`«** ist jetzt sichtbar. Wähle diesen Ordner an, so dass er blau hinterlegt ist und drücken auf `OK` um deine Änderung zu bestätigen.



3.4.6.11 Im Fenster Einstellungen wird jetzt als **»Neuer Ort:«** **»`T:\Temp\Temporary Internetfiles`«** angezeigt. Drücke hier nochmalsauf `OK` damit die Änderung wirksam wird.



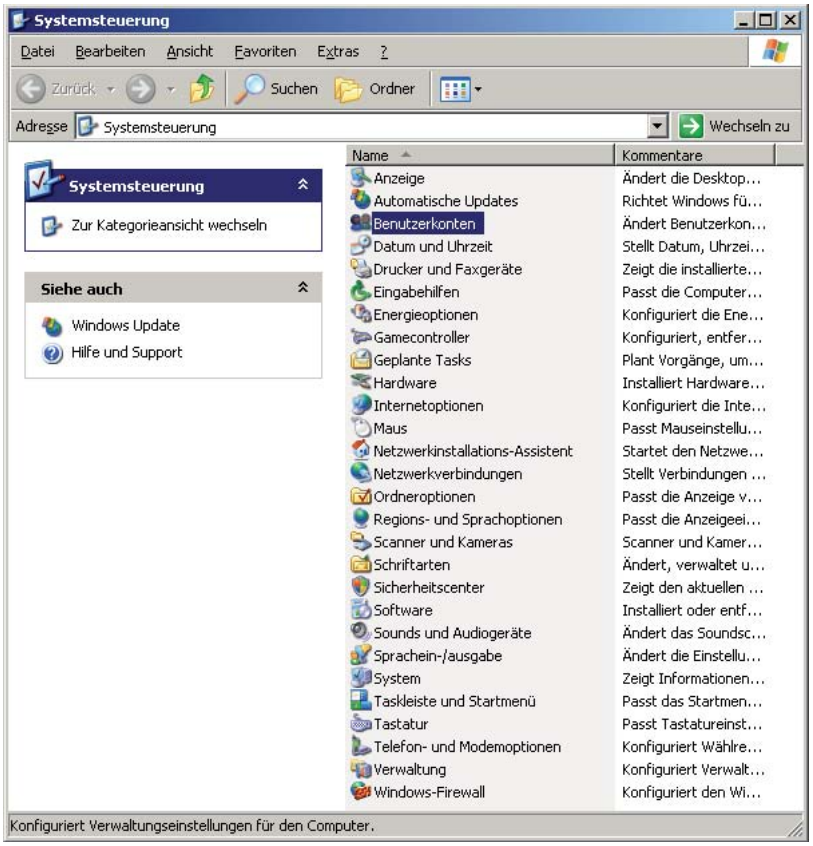
3.4.6.12 Bevor du die folgende Nachfrage mit `Ja` beantwortest, stelle sicher dass du alle eventuell geöffneten Dateien (z.B. ein Word Dokument) gespeichert hast. Du wirst anschließend abgemeldet und Windows verschiebt die temporären Internetdateien.



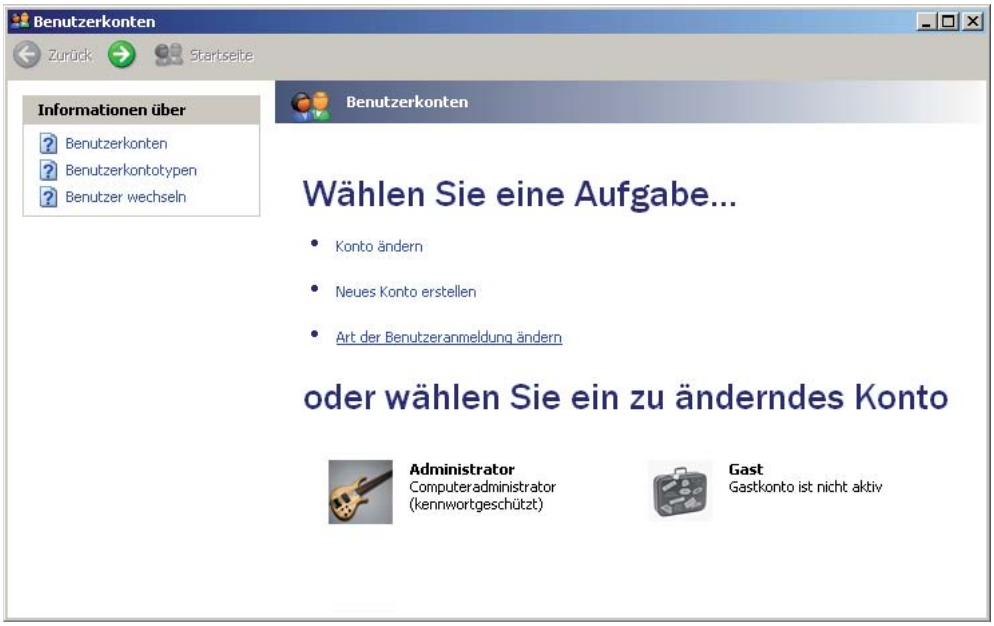
4. Verschlüsselung eines Benutzerprofils

4.1 Einrichten eines neuen Benutzerkontos

4.1.1 Begib dich erneut in die Systemsteuerung (siehe 3.4.1.1) und klicke auf **»Benutzerkonten«**.



4.1.2 Im Fenster **»Benutzerkonten«**, der sogenannten Benutzerkontenverwaltung klickst du auf **»Neues Konto erstellen«**

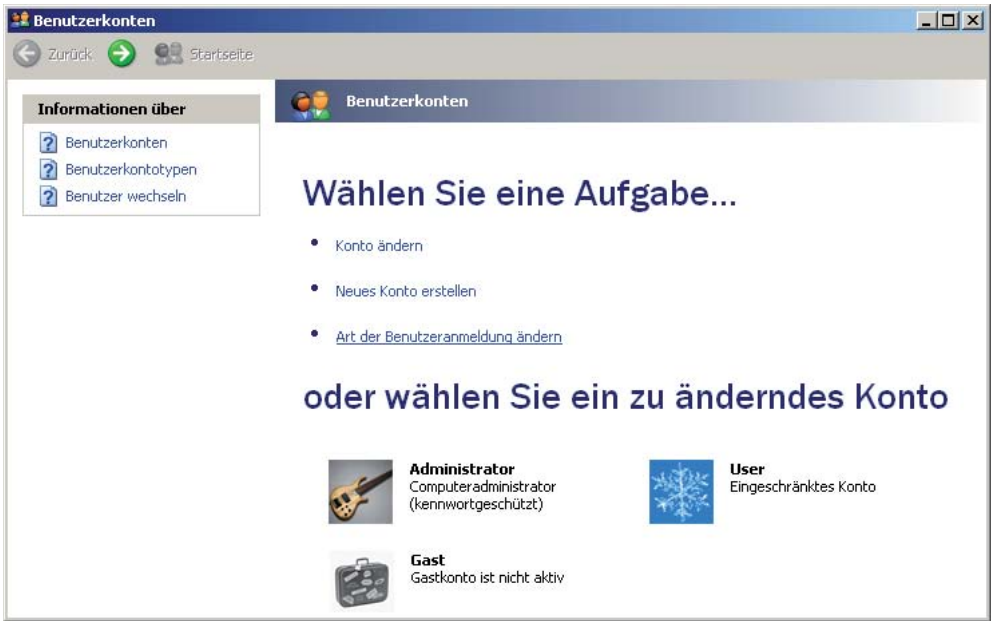


4.1.3 Im nächsten Schritt gibst du einen Namen für das neue Konto an und bestätigst diesen durch klicken auf die Schaltfläche `Weiter`.

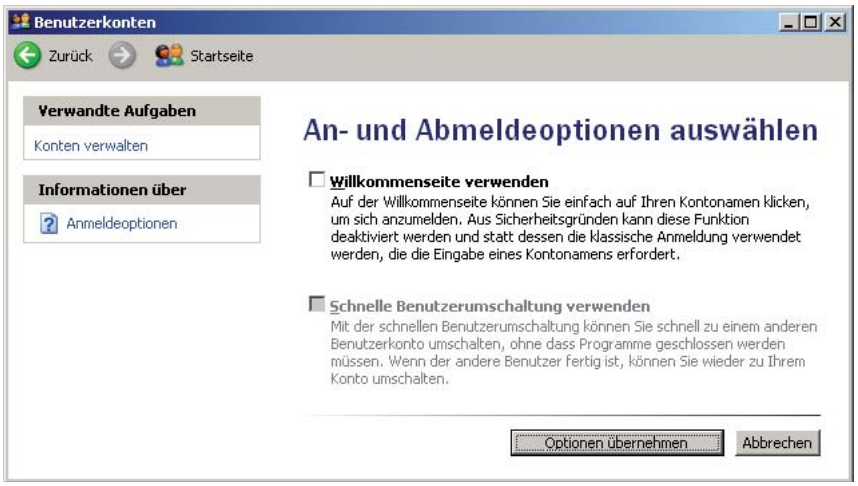
4.1.4 Wähle unter der Überschrift **»Wählen Sie einen Kontotypen«** mit dem Radiobutton den Kontotyp

4.1.5 **»Eingeschränkt«** aus und klicke auf die Schaltfläche `Konto erstellen`. Falls du **»Windows XP (Home)«** benutzt und bisher noch kein Adminstratorkonto angelegt wurde, lässt sich hier zunächst nur **»Computeradminstrator«** auswählen. Erstelle in diesem Fall zunächst ein Administratorkonto durch Klicken auf `Konto erstellen`. Gehe anschließend zurück zum Schritt 4.1.2 um ein weiteres Konto, diesmal ein eingeschränktes Konto anzulegen.

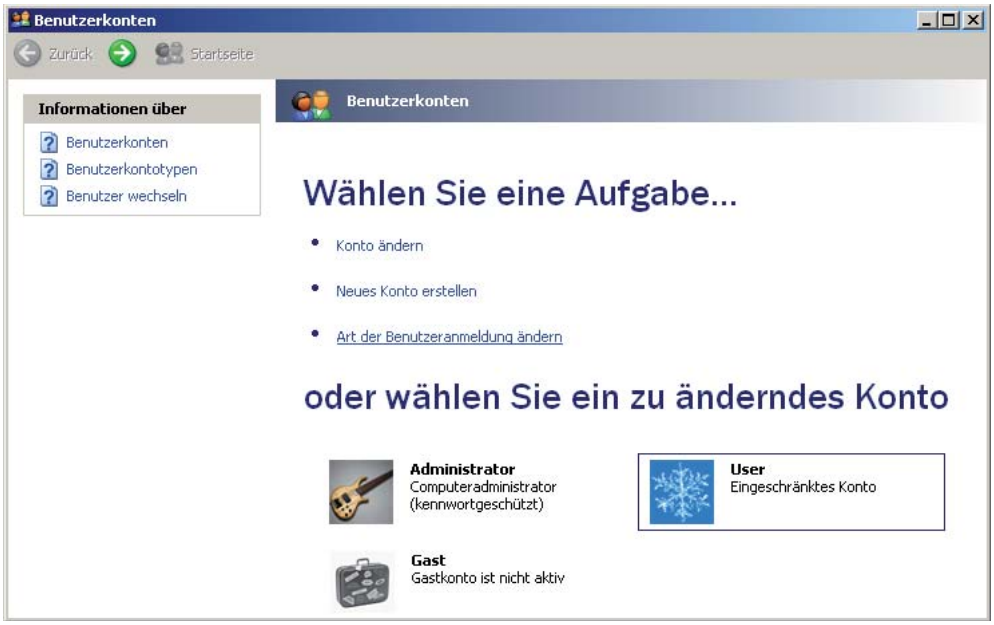
4.1.6 Das neue Benutzerkonto wird nun in der Benutzerkontenverwaltung aufgeführt. Klicke jedoch zuerst auf auf **»Art der Benutzeranmeldung«** ändern



4.1.7 Unter der Überschrift **»An- und Abmeldeoptionen auswählen«** entferne das Häkchen bei **»Willkommensseite verwenden«** und bestätige die Änderung durch klicken auf `Optionen übernehmen`.



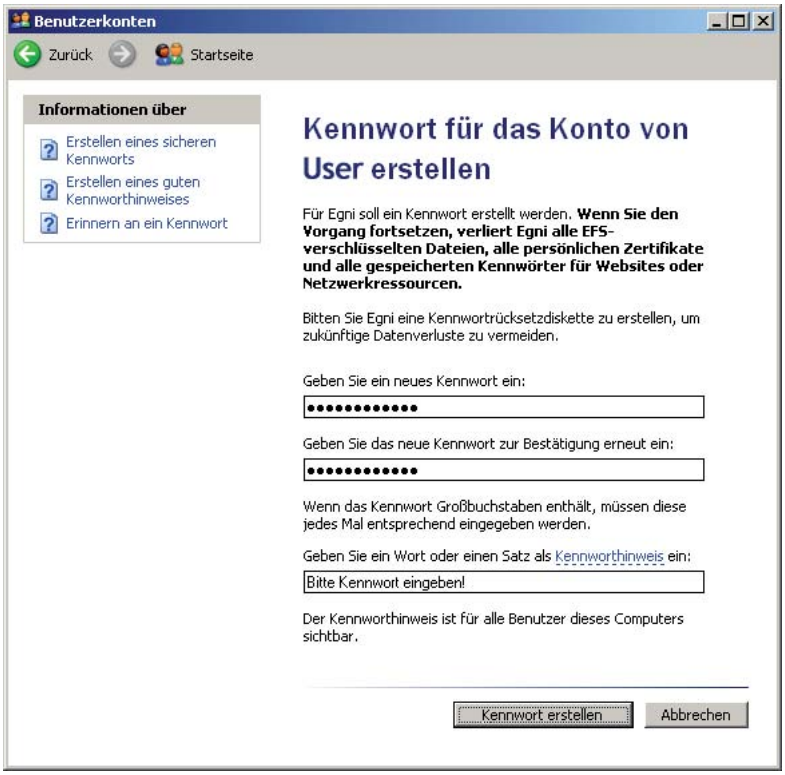
4.1.8 Zurück in der Benutzerkontenverwaltung klicke auf das neu Konto, um weitere Änderungen daran vorzunehmen.



4.1.9 Unter der Frage **»Welche Änderungen möchten Sie am Konto ... vornehmen?«** findet sich eine Liste mit den Änderungsmöglichkeiten. Klicke auf den dritten Punkt **»Kennwort erstellen«** um dein Konto mit einem Passwort zu schützen. (Wenn bereits ein Kennwort erstellt wurde heißt dieser Punkt **»Kennwort ändern«**.)

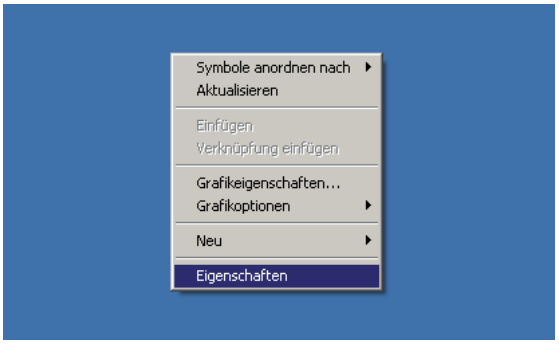
4.1.10 Im nächsten Schritt, gibst du in das erste und zweite Feld dein Kennwort ein. Ins dritte Feld kommt ein Kennworthinweis wie z.B. *»Bitte Kennwort eingeben!«*. Bitte verwende auch hier ein starkes Passwort.

4.1.11 Du kannst das Fenster **»Benutzerkonten«** jetzt schließen.

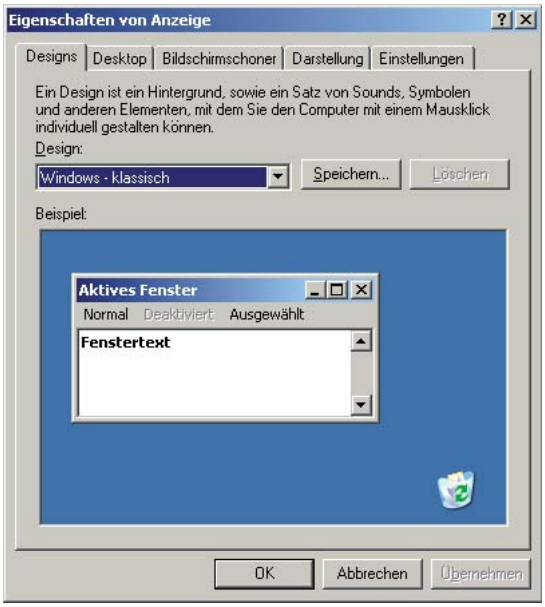


4.2 Aktivierung des Bildschirmschoners

4.2.1 Durch Rechtsklick auf den Desktop erscheint ein Kontextmenü. Klicke auf den Menüeintrag **»Eigenschaften«**. Alternativ findest du die Anzeigeeigenschaften in der in der Systemsteuerung unter **»Anzeige«**



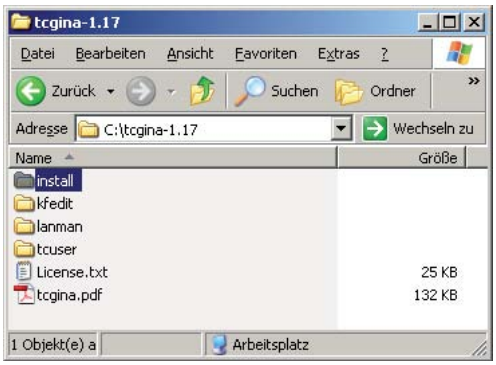
4.2.2 Wähle im Fenster **»Eigenschaften von Anzeige«** die Registerkarte **»Bildschirmschoner«**



4.2.3 Setze das Häkchen vor **»Kennworteingabe bei Reaktivierung«**, stell die **»Wartezeit«** auf einen dir passenden Wert und bestätige die Änderungen mit [Übernehmen]. Die Aktivierung des Bildschirmschoners gilt nur für das laufende Konto, so dass die vorangegangenen Schritte für alle weiteren Konten ebenfalls erforderlich sind.

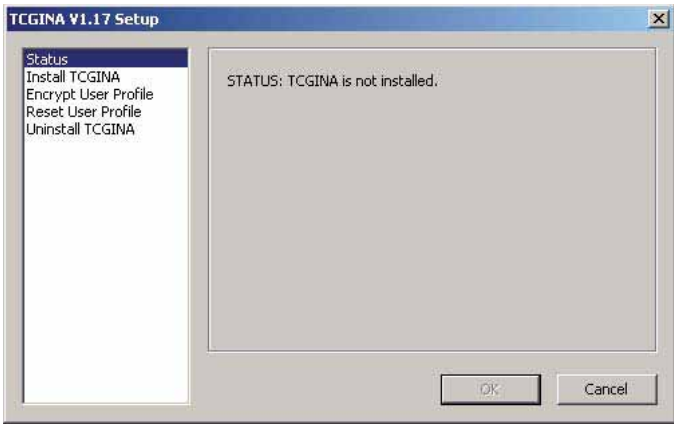
4.3 Installation von TCGINA

4.3.1 Begib dich in den Ordner, in dem sich die Installationsdateien für TCGINA befinden

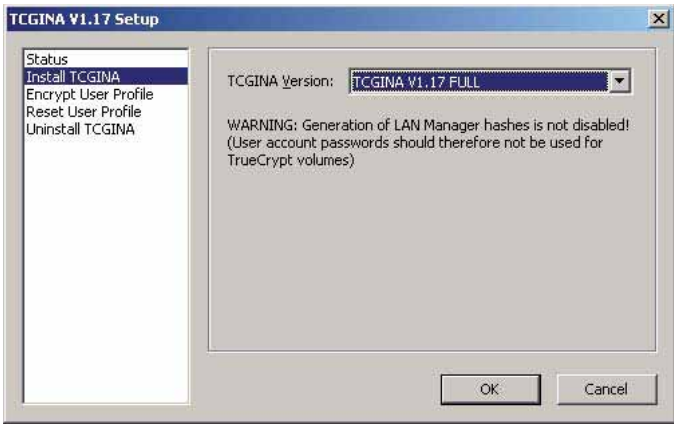


4.3.2 Starte im Unterordner **»install«** das Programm **»Setup.exe«**.

4.3.3 Das Fenster des TCGINA Installationsprogramms zeigt auf der linken Seite ein Menü, über die verfügbaren Funktionen. Auf der rechten Seite werden dazugehörige Statusmeldungen angezeigt oder weiter Einstellungen vorgenommen.



4.3.4 Klicke auf den Menüpunkt **»Install TCGINA«**, wähle die Einstellung **»TCGINA V1.17 Full«** und bestätige mit OK. (Falls du eine neuere Version des Programms verwendest, wird bei dir die entsprechende Versionsnummer angezeigt.)

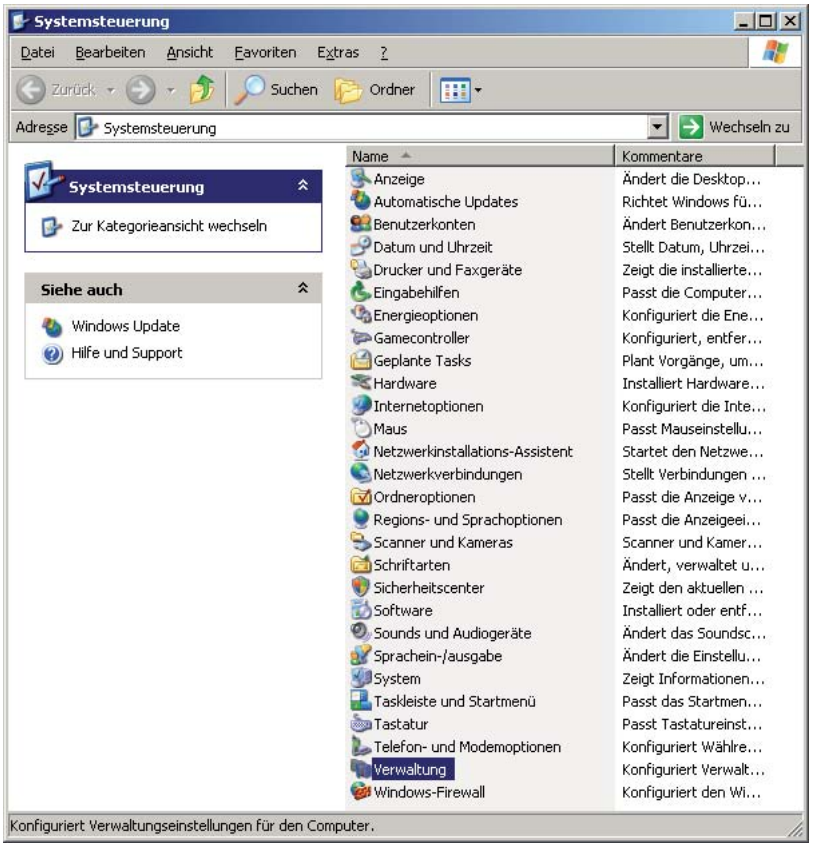


4.3.5 Die vom Programm ausgegeben Meldung über die erfolgreiche Installation, wird mit OK bestätigt.

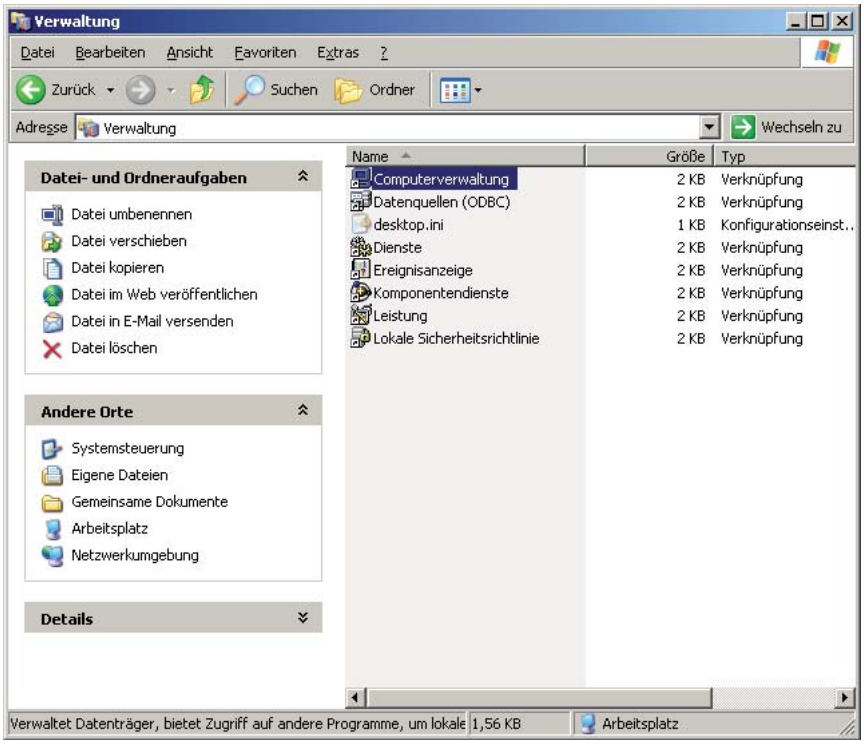
4.3.6 Starte den Rechner jetzt neu! Melde dich anschließend mit deinem bisherigen Benutzernamen und Passwort an. Durch die Änderungen an den Benutzerkonteneinstellungen kann der Auschalten-Dialog anders aussehen als du es bisher gewohnt warst.

4.4 Entfernen des Laufwerksbuchstabens bei Verwendung einer Partition

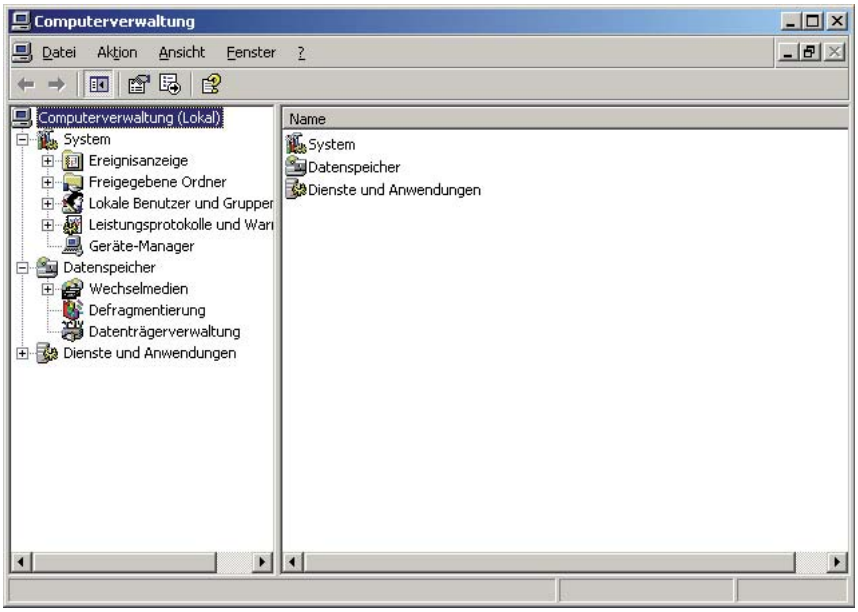
4.4.1 Wenn dein Beutzerprofil auf einer weiteren Festplatte (intern/extern) oder einem Teil (Partition) einer vorhandenen Fesplatte liegen soll, empfehlen wir, den Laufwerksbuchstaben in der Datenträgerverwaltung zu entfernen um ein versehentliches Formatieren und damit einhergehnden Datenverlust zu verhindern. Gehe dazu in die Systemsteuerung und klicke doppelt auf **»Verwaltung«**



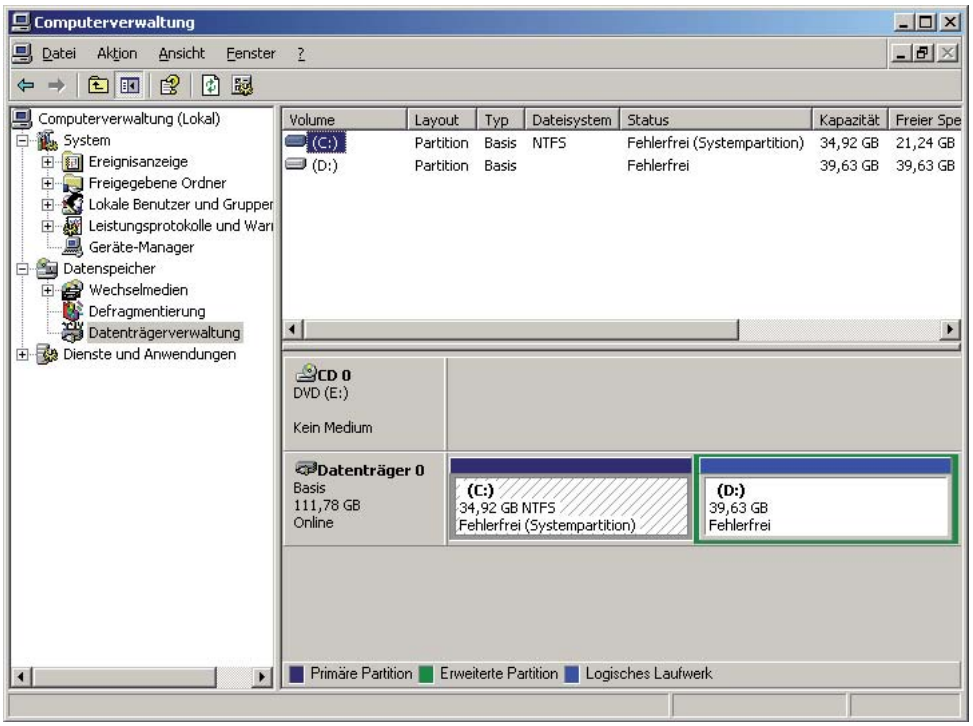
4.4.2 Im Fenster **»Verwaltung«** klicke doppelt auf den Punkt **»Computerverwaltung«**.



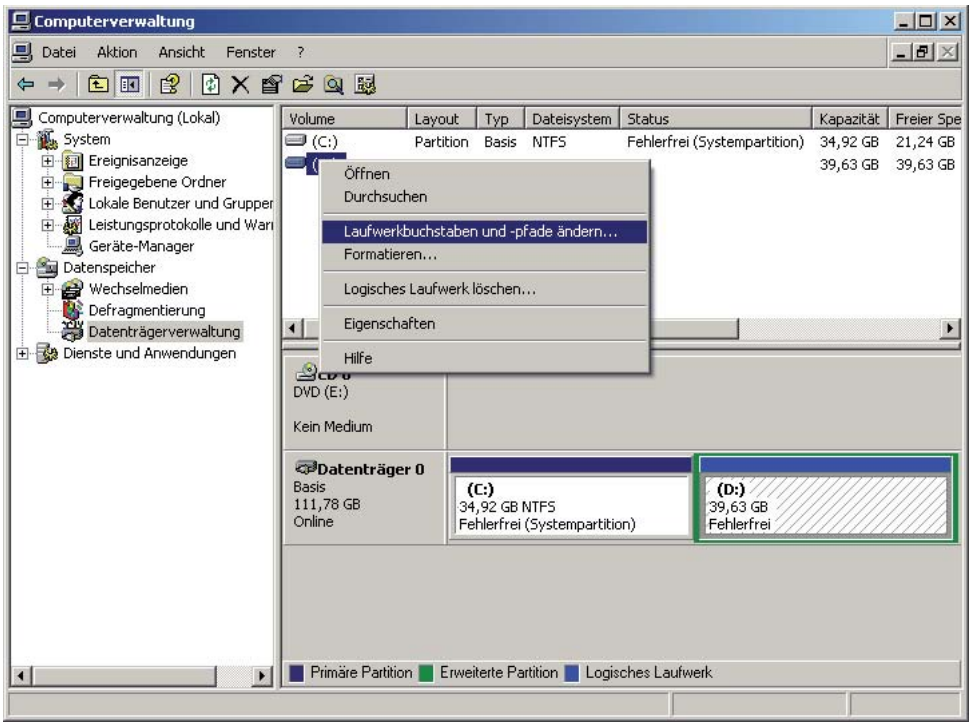
4.4.3 Innerhalb der **»Computerverwaltung«** klicke auf der linken Seite im Abschnitt **»Datenspeicher«** auf den Punkt **»Datenträgerverwaltung«**.



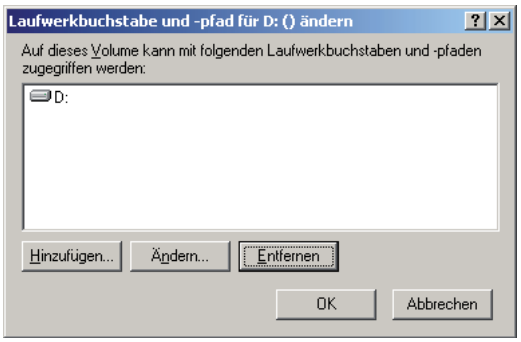
4.4.4 Auf der Rechten Seite des Fensters **»Datenträgerverwaltung«** befindet sich eine Übersicht aller im Rechner eingebauten oder am Rechner angeschlossenen Festplatten und Laufwerke.



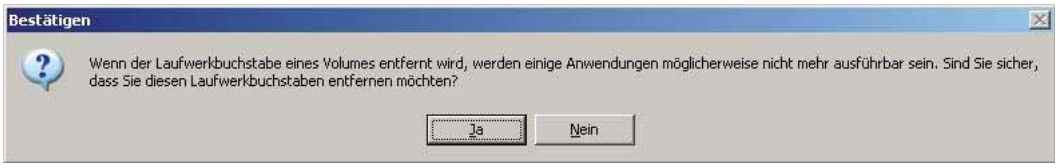
4.4.5 Klicke im oberen Bereich dieser Übersicht mit der rechten Maustaste auf das Laufwerk dass du als Speicherort für dein Benutzerprofil gebrauchen möchtest. Halte die rechte Maustaste gedrückt und wähle im Kontextmenü den Punkt **»Laufwerksbuchstaben und -pfade ändern«** um mit der linken Maustaste daruf zu klicken.



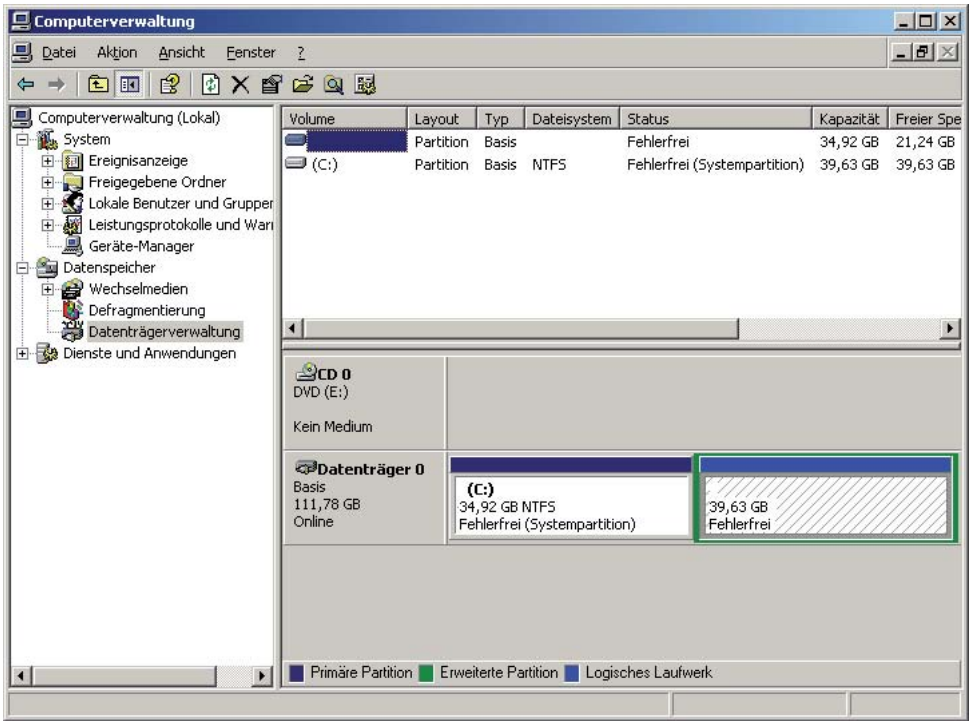
4.4.6 Klicke im Fenster **»Laufwerksbuchstabe und -pfad für ... ändern«** auf den entsprechenden Laufwerksbuchstaben, so dass dieser blau hinterlegt ist und anschließend auf die Schaltfläche [Entfernen].



4.4.7 Die folgende Sicherheitsabfrage beantwortest du mit [Ja].

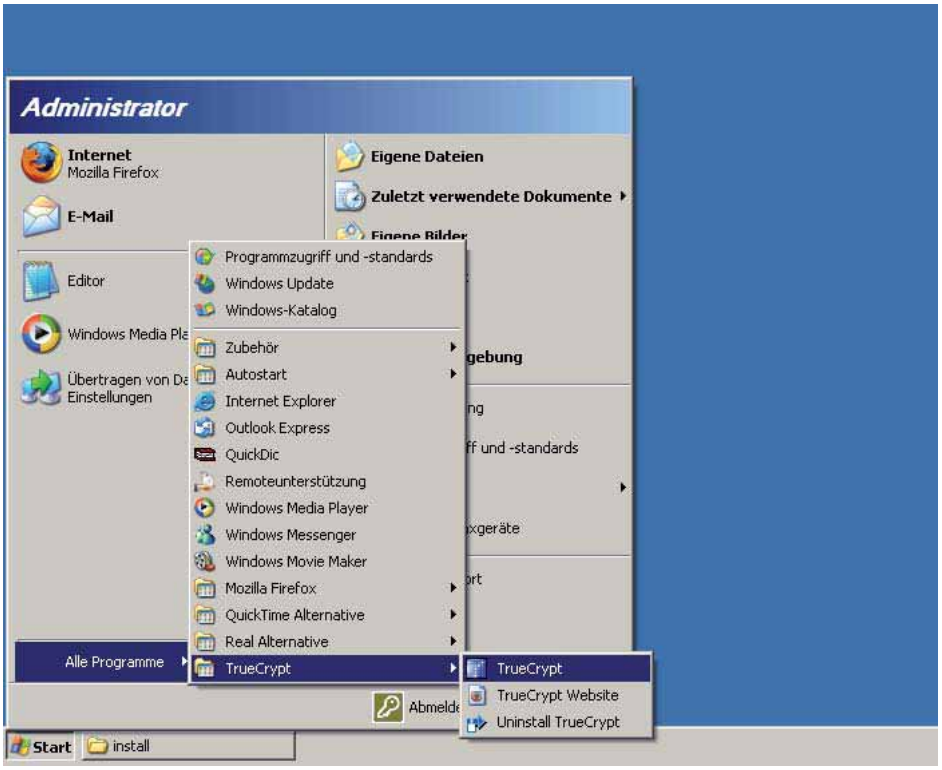


4.4.8 In der **»Computerverwaltung«** unter **»Datenträgerverwaltung«** wird bei dem entsprechenden Laufwerk jetzt kein Laufwerksbuchstabe mehr angezeigt. Du kannst alle offenen Fenster schließen.

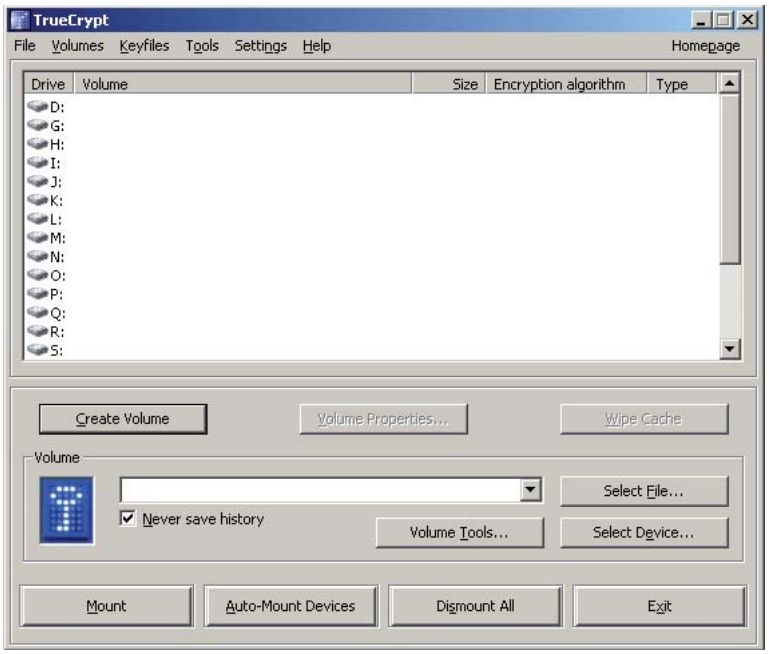


4.5 Anlegen eines TrueCrypt Volumes

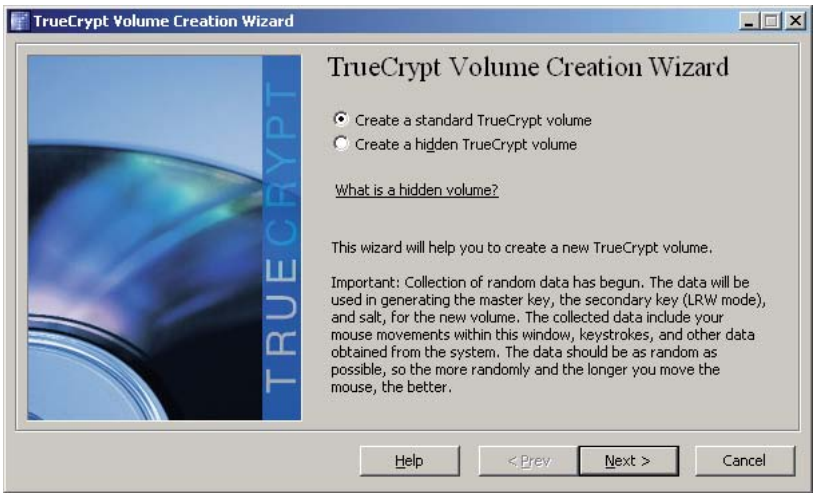
4.5.1 Rufe durch klicken auf Start in der Taskleiste das Startmenü auf, starte unter **»Alle Programme«** das Programm **»TrueCrypt«** .



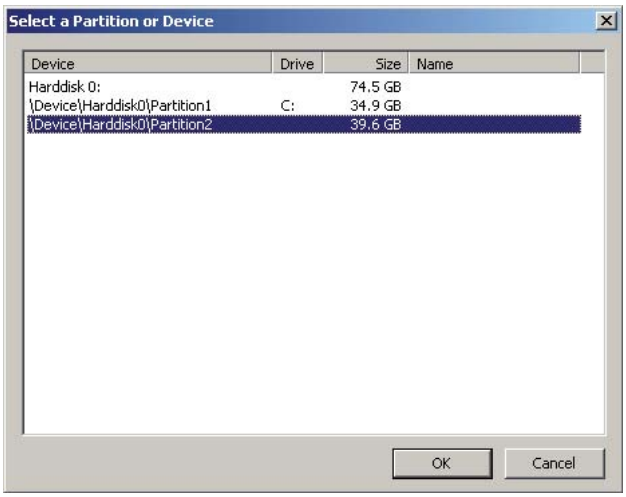
4.5.2 Starte durch klicken auf die Schaltfläche Create Volume den **»TrueCrypt Volume Creation Wizard«**.



4.5.3 Setze den Radiobutton vor **»Create a standard TrueCrypt Volume«** (Standardeinstellung) und fahre fort durch klicken auf Next.

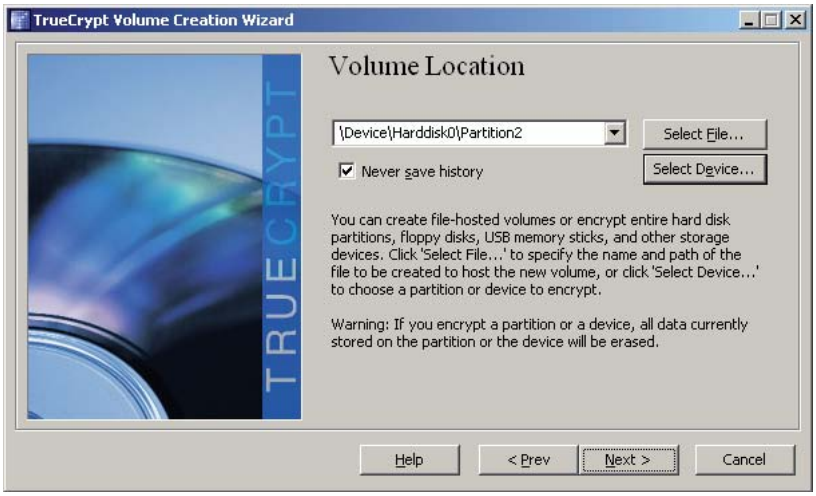


4.5.4 Falls du keine eigene Partition für dein Benutzerprofil verwenden möchtest fahre bei Schritt 4.5.7 fort. Falls doch klicke auf Select Device und wähle im nächsten Fenster die entsprechende Partition aus. Existieren auf einer Festplatte mehrere Partitionen, stehen diese untereinander. Die TrueCrypt Partition erkennst du daran, dass kein Laufwerksbuchstabe angezeigt wird (hast du in Schritt 4.4 entfernt). Wähle in keinem Fall den Obereintrag (Beispiel: **»Harddisko:«**) für Partitionen da auf allen unter diesem Eintrag aufgeführten Partitionen mit Datenverlust zu rechnen ist. Dass du es sich um einen Untereintrag handelt erkennst du an der Benennung (Beispiel: **»\Device\Harddisko\Partition2«**. Wenn die TrueCrypt Partition blau hinterlegt ist kannst du durch klicken auf OK fortfahren

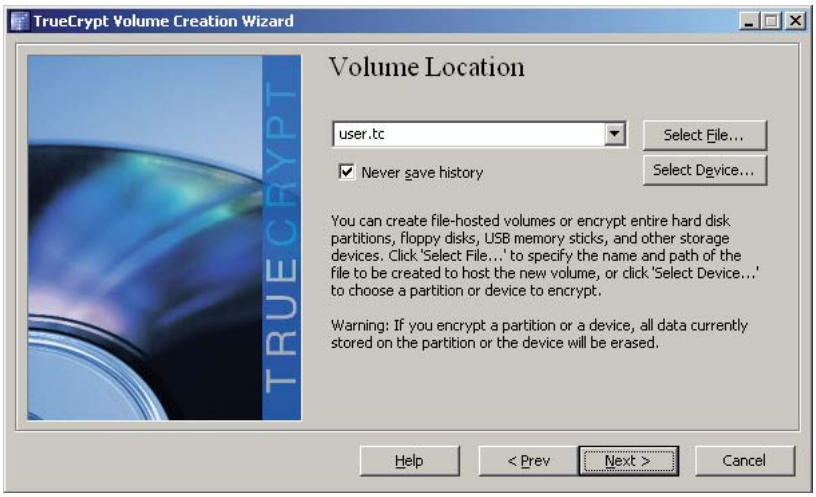


4.5.5 Die Sicherheitsabfrage beantwortest du mit Ja

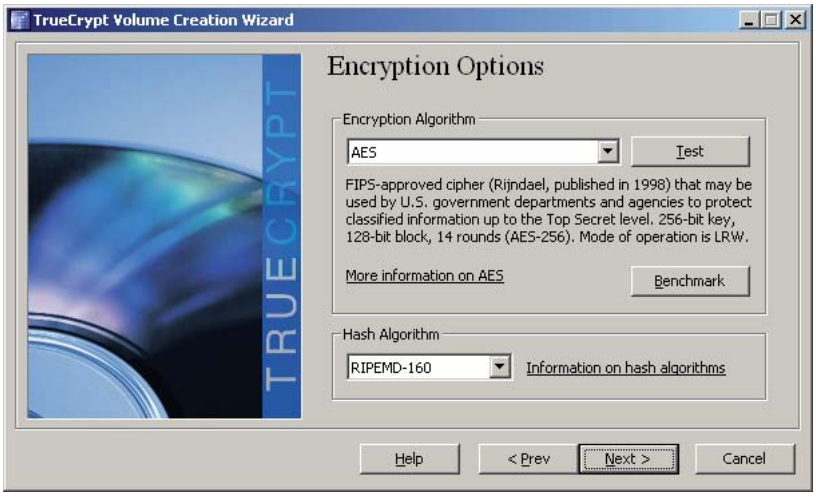
4.5.6 Der Pfad zu deiner Partition steht jetzt in dem weißen Feld unter der Überschrift **»Volume Location«**. Bestätige diesen durch Klicken auf die Schaltfläche `Next` und fahre fort bei Schritt 4.5.8.



4.5.7 Wenn du die vorherigen drei Schritte Übersprungen hast klicke in das weiße Feld unter der Überschrift **»Volume Location«**, gib den Dateinamen deiner Containerdatei an die zukünftig dein Benutzerprofil enthalten soll (Beispiel: **»`c:\user.tc`«** und klicke auf die Schaltfläche `Next`.

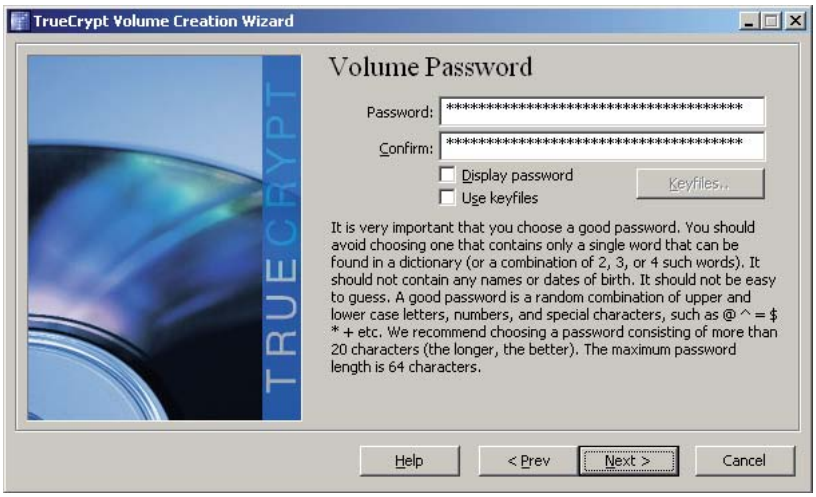


4.5.8 Beim Schritt **»Encryption Otions«** wählst für das erste, mit **»Encryption Algorithm«** überschriebene Feld den Algorithmus **»AES«** und für das zweite, mit **»Hash Algorithm«** überschriebe Feld den Algorithmus **»RIPEMD-160«**.

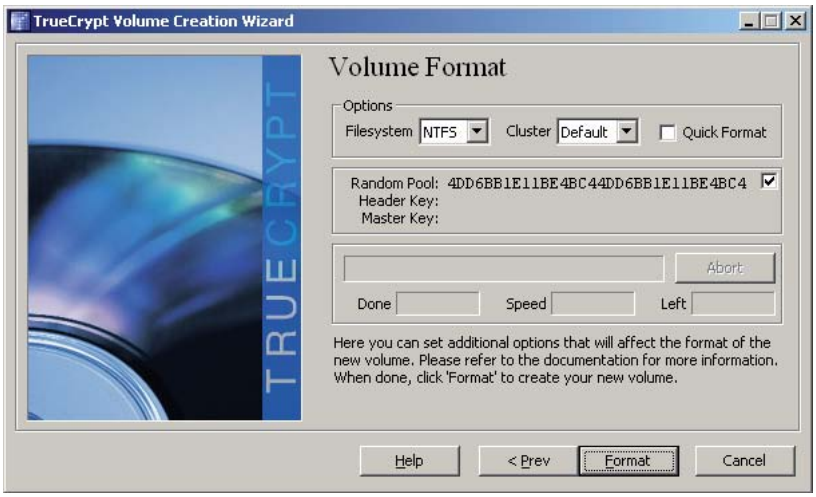


4.5.9 Verwendest du eine Partition kannst du in dem Feld unter der Überschrift **»Volume Size«** keine Angaben machen (Feld ist deaktiviert), da der gesamte verfügbare Speicherplatz der Partition genutzt wird. Falls du eine Containerdatei benutzt trägst du in das Feld unter der Überschrift einen Wert in MB ein (siehe Punkt 3.2.6), der deinen Ansprüchen an Speicherplatz gerecht wird. (Dies hängt von den Daten ab die du in deinem Benutzerprofil, also auch auf dem Desktop, ablegst. Audio und Video Dateien benötigen zum Beispiel sehr viel Speicherplatz.)

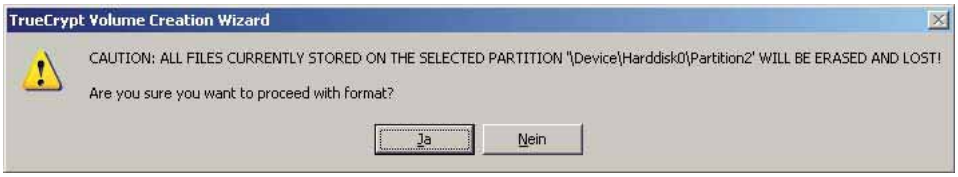
4.5.10 Im nächsten Schritt **»Volume Password«** wirst du aufgefordert ein Passwort für dein TrueCrypt Volume anzugeben. Verwende unbedingt ein starkes Passwort. (Hier seien die Voraussetzungen nocheinmal kurz angeführt: mehr als 20 Zeichen, zufällig gewählte Zeichen, Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Etwas ausfürlicher ist der Absatz zu starken Passworten im Vorwort) Gib also in beide Felder das gleiche Passwort ein. Bei Übereinstimmung kannst du auf `Next` klicken um fortzufahren.



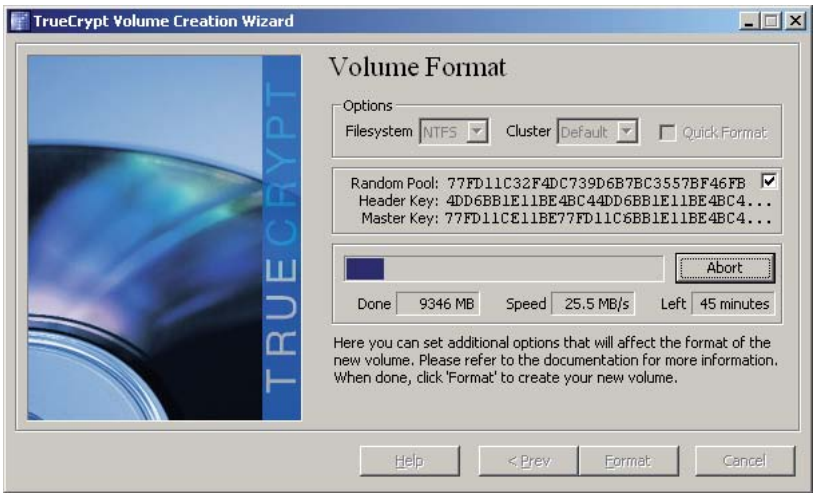
4.5.11 Du hast jetzt die möglich vor der Formatierung des TrueCrypt Volumes das Dateisystem auszuwählen. Wir empfehlen die Verwendung von NTFS, wo das Dateisystems vor Beschädigung durch unvollständige Schreibvorgänge (z.B. Stromausfall) geschützt ist. Beachte dass kein Häkchen bei **»Quickformat«** gesetzt ist. Bevor du die Formatierung durch Klicken auf [Format] startest, bewege mindestens 30 Sekunden lang die Maus innerhalb des Fensters. Dadurch werden Zuffallszahlen erzeugt die die Sicherheit des zu erstellenden Schlüssels erhöhen.



4.5.12 Für den Fall, dass du eine Partition formatierst, beantworte die erneute Sicherheitsabfrage mit [Ja].



4.5.13 Die Formatierung kann anhängig von der Größe des TrueCrypt Volumes sehr lange dauern. Bei einer Festplatte mit 100GB wird die Formatierng etwa eine Stunde dauern. Eine Fortschrittsanzeige hält dich auf dem Laufenden. Nach der Formatierung kann der **»TrueCrypt Volume Creation Wizard«** durch Klicken auf [Exit] beendet werden.

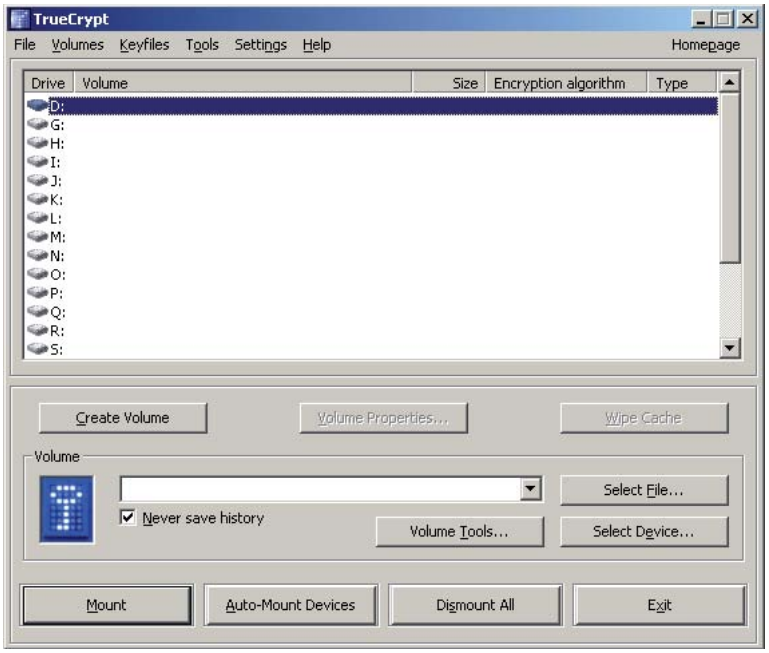


4.6 Kopieren des Benutzerprofils

4.6.1 Damit dein Benutzerkonto verschlüsselt werden kann muss es zunächst vollständig erstellt worden sein. Dazu ist es erforderlich sich unter dem neuen Konto anzumelden. Bei dieser Gelegenheit, solltest du alle Einstellungen die Kontospezifisch sind in deinem Benutzerkonto überprüfen. Dazu zählen: Bildschirmschoner aktivieren, Umgebungsvariablen anpassen, Internet Explorer anpassen, (Windows Explorer anpassen)

4.6.2 Wenn du alles erledigt hast, melde dich ab und unter deinem alten Konto wieder an.

4.6.3 Starte TrueCrypt, und binde das soeben erstellte TrueCrypt Volume als Laufwerk ein. Dazu klickst du im Fenster **»TrueCrypt«** im oberen Bereich auf einen Laufwerksbuchstaben, der dadurch blau hinterlegt ist. Den Laufwerksbuchstaben kannst du frei wählen. Du legst damit jedoch auch fest unter welchem Laufwerksbuchstaben zukünftig dein Benutzerprofil zu finden ist. Anschließend klickst du auf die Schaltfläche `Select File` (wenn du eine Containerdatei verwendest) oder `Select Device` (wenn du eine Partition verwendest), um deine Containerdatei/ Partition auszuwählen. Durch klicken auf `Mount` gehts weiter.



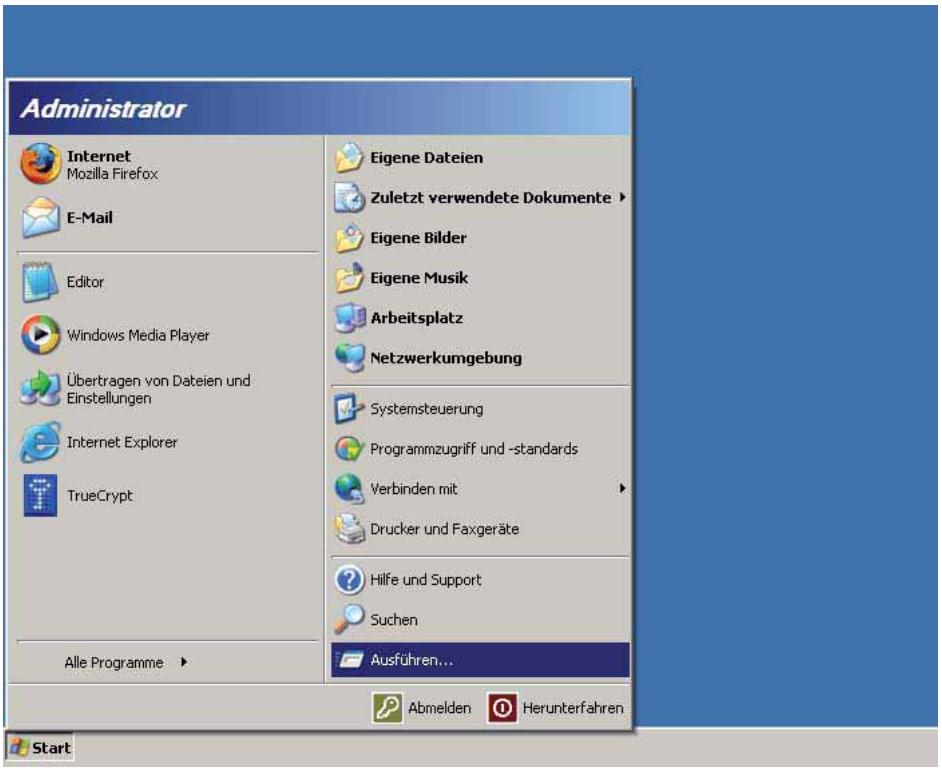
4.6.4 Gib dein soeben festgelgtes Passwort ein und bestätige mit `Enter` oder `OK`

4.6.5 Begib dich erneut in das Verzeichnis in das du TCGINA enpackt hast (siehe Schritt 4.3.1), starte aus dem Unterordner **»install«** das Program **»setup.exe«** und wähle auf der linken Seite im Fenster des TCGINA Installationsprogramms den Menüpunkt **»Encrypt user profile«**. Auf der rechten Seite des Fensters wählst du bei **»User Name:«** den Namen des Benutzerkontos, dass du in Schritt 4.1 erstellt hast, und bei **»TrueCrypt Drive«** den Laufwerksbuchstaben, unter dem du das TrueCrypt Volume in Schritt 4.6.1 eingebunden hast. Bestätige mit [OK].

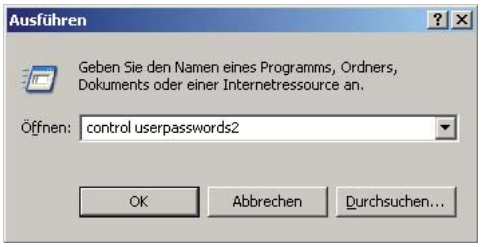
4.6.6 Es wird ein Hinweis ausgegeben, dass das Benutzerprofil erfolgreich verschlüsselt wurde und das alte Verzeichnis auf sichere Art und Weise entfernt werden sollte. Bestätige mit [OK].

4.7 Aktivieren der Automatischen Windows Anmeldung

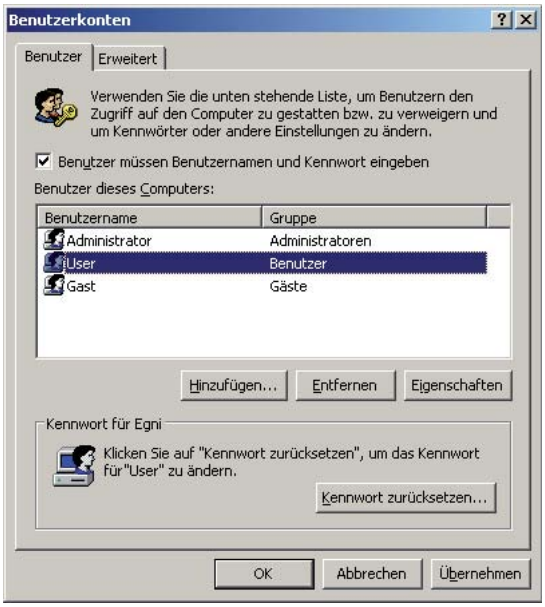
4.7.1 Damit du in Zukunft nicht immer zwei Passworte hintereinander eingeben musst, lässt sich die Windows Anmeldung automatieseren. Klicke dazu in der Taskleiste auf [Start] und anschließend auf **»Ausführen«**.



4.7.2 Gib im Fenster **»Ausführen«** in das weiße Feld *»control userpasswords2«* ein und bestätige mit [OK] oder [Enter].

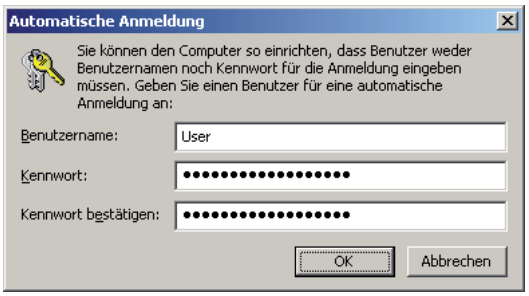


4.7.3 Im Fenster **»Benutzerkonten«** wählst du den Benutzernamen deines verschlüsselten Profils, so dass die entsprechende Zeile blau hinterlegt ist.



4.7.4 Anschließend entfernst du dass Häkchen vor **»Benutzer müssen Benutzernamen und Kennwort eingeben«** und bestätigst durch Klicken auf [Übernehmen].

4.7.5 Gib dein Windows Kennwort (nicht das TCGINA Kennwort) jetzt zwei mal hintereinander ein und bestätige mit OK



4.7.6 Nach einem Neustart deines Rechners wirst du von einer anderen Anmeldung begrüßt. Nach eingabe deines TCGINA Passwortes steht dir dein verschlüsseltes Benutzerprofil zur Verfügung.

5. Aufräumen

5.1 Spätestens jetzt ist es an der Zeit die Festplatte(n) einer Grundreinigung zu unterziehen.

5.2 Alle Ordner und Dateien eines Benutzerprofils befinden sich im Windows Systemordner **»C:\ Dokumente und Einstellungen**. In diesem Systemordner befindet sich wiederum ein Ordner mit deinem Benutzernamen der das gesamte Profil enthält. Diesen kannst du löschen.

5.3 Verschiebe alle sensiblen Daten, die sich noch auf dem unverschlüsselten Bereich deiner Fesplatte befinden in den verschlüsselten Bereich. Dazu zählt das gesamte virtuelle Laufwerk, das dein Benutzerprofil enthält. Du erkennst das Laufwerk an dem von dir vergebenen Laufwerksbuchstaben und der Laufwerksbezeichnung die den Benutzernamen des verschlüsselten Profils trägt. Während du unter deinem verschlüsselten Konto angemeldet werden alle Dateien die du auf dem Desktop oder im Ordner **»Eigene Dateien«** speicherst verschlüsselt.

5.4 Installiere das Programm **»Eraser«**. (Eventuell ist ein Neustart erforderlich). Öffne den Arbeitsplatz und klicke mit der rechten Maustaste auf eine unverschlüsselte Festplatte. Wähle in dem sich öffnenden Kontextmenü den Eintrag **»Erase unused Space«**. Klicke in dem sich öffnenden Fenster auf die Schaltfläche [Options]. Wähle die Registerkarte **»Unused Disk Space«** und wähle eine Lösch-Methode. Eine der ersten beiden Methoden sollte blau hinterlegt sein. Die zweite Methode, mit sieben Durchgängen ist bereits ausreichend. Überprüfe außerdem dass alle drei Häkchen bei **»Overwrite«** gesetzt sind. Bestätige die Einstellungen mit [OK] und starte den Löschvorgang durch Klicken auf [Yes]. Das Löschen dauert wahrscheinlich einige Stunden, der Vorgang sollte anschließend für alle weiteren unverschlüsselten Festplatten wiederholt werden.