

Haben Sie schon einmal überlegt, was mit Ihren Daten passieren kann, wenn Ihr Rechner, Ihr Laptop, Ihre Daten-CDs oder Ihr USB-Stick in die falschen Hände geraten? Ein Laptop ist schnell gestohlen – ein USB-Stick schnell verloren. Was, wenn Unbefugte sich dann Zugriff auf Ihre persönlichen Fotos oder geschäftlichen Dateien verschaffen? Um diese Gefahr zu bannen, sollten Sie sensible Daten grundsätzlich verschlüsseln. Wir zeigen Ihnen, wie Sie das schnell und professionell erledigen. Alles, was Sie dazu benötigen, ist ein kleines, kostenloses Tool und eine halbe Stunde Zeit, um Ihren ersten Datensafe zu bauen.

- Ihre Daten sind unter Windows nicht sicher! T 94/2
- TrueCrypt: Schneller und professioneller Datenschutz auch für unerfahrene Anwender T 94/3
- Hier bekommen Sie TrueCrypt T 94/4
- So installieren Sie TrueCrypt T 94/4
- Schritt für Schritt zum ersten Datensafe T 94/6
- So öffnen Sie Ihren Datensafe T 94/12
- So schließen Sie Ihren Datensafe T 94/13
- So schützt TrueCrypt Ihre Daten T 94/15
- Sicherheit für unterwegs! TrueCryptTraveller T 94/15
- So pflegen Sie Ihre Datensafes T 94/17
- Sichern Sie den Volume-Header Ihres Datensafes T 94/18
- Tipps & Tricks zu TrueCrypt T 94/20

Autor: **Rainer Rudolf**

**Ihre Daten sind unter Windows nicht sicher!**

**Ihr Benutzerkonto schützt Ihre Daten nicht**

Viele Anwender glauben, ihre sensiblen Daten wären schon durch die Windows-Benutzerkonten ausreichend gegen unbefugten Zugriff gesichert. Dies ist ein Trugschluss. Benutzerkonto und -Passwort schützen Ihre Daten nur, wenn mit Ihrem Windows auf Ihre Daten zugegriffen wird. Wird auf Ihrem PC ein anderes Betriebssystem gestartet oder Ihr Laufwerk in einen anderen Rechner eingebunden, sind Ihre Daten schutzlos.

**Sie können unter Windows mit EFS verschlüsseln**

Um Ihnen die Möglichkeit zu geben, Ihre Daten auch in solchen Situationen vor unbefugtem Zugriff schützen zu können, verfügen viele Versionen von Windows 2000, XP und Vista über ein Feature zum Verschlüsseln von Dateien, das „Encrypted File System“ (EFS). Sie können mit drei Mausklicks eine Datei verschlüsseln und dabei testen, ob Ihr Windows über EFS verfügt:



1. Klicken Sie mit der rechten Maustaste auf eine Datei und wählen Sie im Kontextmenü die Option „Eigenschaften“. Klicken Sie dann auf „Erweitert“. Verfügen Sie über EFS, sollten Sie im folgenden Fenster die Option „Inhalt verschlüsseln, um Daten zu schützen“ vorfinden. Sie wird aber nur auf NTFS-formatierten Laufwerken angeboten.
2. Diese Option muss aktiviert werden, um eine Datei zu verschlüsseln. Bestätigen Sie dann alle weiteren Abfragen mit „OK“. Greifen Sie später auf diese Datei zu, entschlüsselt Windows sie automatisch im Hintergrund. Andere Benutzer erhalten keinen Zugriff.

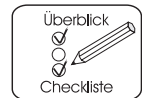
**EFS hat deutliche Nachteile**

Leider wartet EFS aber mit einigen Nachteilen auf. So wird es beispielsweise von „XP Home“ nicht unterstützt und die EFS-Verschlüsselung von Windows 2000 gilt als geknackt. EFS

funktioniert auch nur auf Datenträgern, die mit dem NTFS-Dateisystem formatiert sind. Verschieben Sie also EFS-verschlüsselte Dateien auf Datenträger, die anders formatiert sind, wie FAT- oder CD-Laufwerke, so gehen Verschlüsselung und Zugriffsschutz dabei verloren.

## TrueCrypt: Schneller und professioneller Datenschutz auch für unerfahrene Anwender

Wenn Sie nach einem Tool suchen, mit dem Sie Ihre Dateien „hacker- und idiotensicher“ vor unbefugtem Zugriff schützen wollen, ist „TrueCrypt“ deshalb die bessere Alternative.



- Anders als EFS verschlüsselt dieses kostenlose Open-Source-Programm Ihre Daten nicht auf Dateiebene, sondern erstellt für Sie Datensafes, die Sie wie reguläre Laufwerke nutzen können.
- Ein geschlossener TrueCrypt-Datensafe schützt Ihre Daten mit einer bis zu 448 Bit starken Verschlüsselung und lässt sich garantiert nur mit Hilfe Ihres Passwortes öffnen.
- Ist Ihr Datensafe hingegen geöffnet, können Sie ihn wie ein ganz normales Laufwerk nutzen, um darin Dateien zu sichern oder von dort aufzurufen. Die Ver- und Entschlüsselung erledigt TrueCrypt im Hintergrund.
- Alles, was Ihnen zu tun bleibt, ist, Ihren Safe aufzusperren, wenn Sie mit Ihren sensiblen Daten arbeiten wollen, und ihn wieder zu schließen, wenn Sie Ihren Rechner verlassen. So wird professioneller Datenschutz auch für unerfahrene Anwender zum Kinderspiel.
- TrueCrypt-Datensafes können Sie auf Festplatten ebenso

**Die Vorteile von TrueCrypt auf einen Blick**



nutzen, wie auf USB-Sticks, Disketten oder CDs.

- TrueCrypt kann für Sie ganze Partitionen in Datensafes verwandeln oder solche Datensafes als Datei speichern.

## Hier bekommen Sie TrueCrypt

### Laden Sie TrueCrypt herunter

TrueCrypt ist ein kleines Tool und schnell installiert. Hier finden Sie die passende Version für Ihr Betriebssystem:

<http://www.truecrypt.org/downloads.php>

### Entpacken Sie seine Installationsdateien

TrueCrypt kommt als gepackte Zip-Datei zu Ihnen und muss zunächst entpackt werden. Dazu benötigen Sie ein Zip-Tool. Unter Windows XP und Vista ist dies standardmäßig installiert. Hier genügt es, auf die eben herunter geladene ZIP-Datei zu klicken, um sie zu öffnen. Mit einem Doppelklick starten Sie dann die Installationsdatei „TrueCrypt Setup.exe“.

### 7-Zip: Kostenloses Zip-Tool

Ist auf Ihrem PC noch kein Zip-Tool installiert, können Sie sich beispielsweise „7-Zip“ kostenlos aus dem Web herunterladen und auf Ihrem PC installieren (<http://www.7-zip.org>).

### Entpacken mit 7-Zip

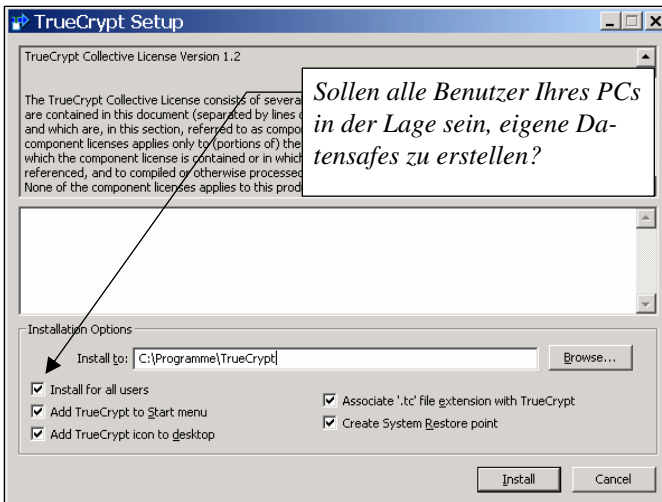
Um die TrueCrypt-Installationsdatei mit 7-Zip zu entpacken, starten Sie zunächst 7-Zip, öffnen damit die TrueCrypt-Zip-Datei, markieren alle enthaltenen Dateien und klicken dann auf „Entpacken“. Nun müssen Sie 7-Zip nur noch sagen, in welchen Ordner es die temporären Installationsdateien entpacken soll. Nach dem Entpacken wechseln Sie in diesen Ordner und starten hier die Datei „TrueCrypt Setup.exe“.

## So installieren Sie TrueCrypt

Im Installationsfenster von TrueCrypt legen Sie fest, wo und wie TrueCrypt installiert werden soll. Die fünf Optionen, die Ihnen hier angeboten werden, können Sie bedenkenlos mit

Häkchen versehen. Lediglich bei „Install for all Users“ müssen Sie entscheiden, ob alle unter Windows angemeldeten Benutzer Ihres PCs in der Lage sein sollen, eigene Datensafes zu erstellen. Soll dies nicht der Fall sein, so lassen Sie dieses Häkchen weg.

**Eigene Datensafes für alle Benutzer?**



*Die Installations-Routine von TrueCrypt*

Klicken Sie dann auf „Install“ und quittieren Sie alle weiteren Nachfragen mit „OK“. Ein Klick auf „Exit“ beendet die Installation schließlich.

Um TrueCrypt unter Windows 2000, XP und Vista installieren zu können, müssen Sie sich mit Administrator-Rechten anmelden. TrueCrypt benötigt einen eigenen Gerätetreiber und die Installation solcher Treiber ist bei Windows nun einmal „Chefsache“. Nutzen können Sie TrueCrypt danach auch ohne diese Admin-Privilegien.

**Melden Sie sich mit Admin-Rechten an**

## Deutsche Sprachdatei herunterladen und einbinden

Sie werden es bemerkt haben. Noch spricht TrueCrypt englisch mit Ihnen. Wenn Sie Ihrer Safeschmiede Deutsch beibringen wollen, müssen Sie noch ein Sprachpaket installieren.

Klicken Sie in der Menüzeile auf „Settings\ Language\ Download Language pack“. Sie werden dann auf eine Webseite geleitet, von der Sie sich das deutsche Sprachpaket herunterladen können. Diese Zip-Datei entpacken Sie dann in den Ordner, in den Sie zuvor TrueCrypt installiert haben.

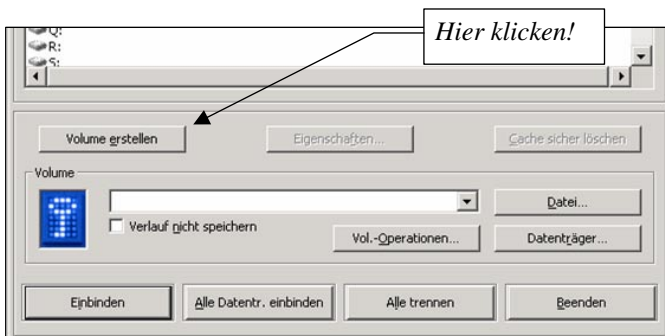
TrueCrypt sollte diese Änderung selbstständig erkennen und beim nächsten Programmstart deutsch sprechen. Ist das nicht der Fall, so klicken Sie abermals in der Menüzeile „Settings\ Language“ und wählen hier die Option „Deutsch“ aus.

## Schritt für Schritt zum ersten Datensafe

TrueCrypt ist installiert und Sie können Ihren ersten Datensafe bauen. TrueCrypt nennt diese Safes übrigens „Volumes“.

## Starten Sie TrueCrypt

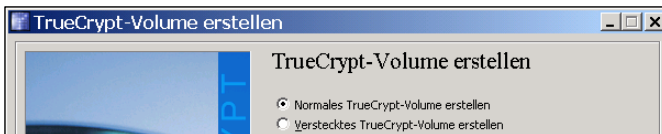
1. Starten Sie TrueCrypt und klicken Sie dann auf „Volume erstellen“.



*Die Schaltzentrale von TrueCrypt. Von hier aus erstellen und verwalten Sie Ihre Datensafes.*

2. Sie werden nun gefragt, ob Sie ein normales oder ein verstecktes Volume erstellen wollen. „Normal“ ist die beste Wahl für die meisten Anwendungssituationen. „Versteckte Volumes“ werden nur unter sehr exotischen Umständen benötigt.

**Erstellen Sie ein „normales Volume“**



*Entscheiden Sie sich für ein Volume vom Typ „normal“.*

Ein verstecktes Volume ist ein „Safe im Safe“. TrueCrypt richtet in einem Volume ein zweites „verstecktes“ Volume ein. Für beide Volumes, das äußere und das darin versteckte Volume, vergeben Sie unterschiedliche Passwörter. Je nachdem, welches Passwort Sie nun beim Öffnen Ihres Datensafes eingeben, wird entweder das äußere oder das darin versteckte innere Volume geöffnet.

**Das versteckte Volume ...**

**... ist ein geheimer „Safe im Safe“**

Sinnvoll ist der Einsatz dieses Features, wenn Sie gezwungen werden könnten, Ihr Datensafe-Passwort herauszugeben. In diesem Fall geben Sie dann einfach das Passwort für das äußere Volume preis, in dem Sie natürlich nur unsensible Daten gespeichert haben.

Der Clou: Es ist nicht möglich nachzuweisen, dass in Ihrem Datensafe noch ein zweites verstecktes Volume existiert.

3. Klicken Sie nun auf „Datei“. Damit weisen Sie TrueCrypt an, Ihren Datensafe als eigene Datei zu speichern. TrueCrypt nennt diese Dateien übrigens „Containerdateien“.

**Erstellen Sie eine Containerdatei**

## Datensafes in Containerdateien lassen sich flexibler einsetzen

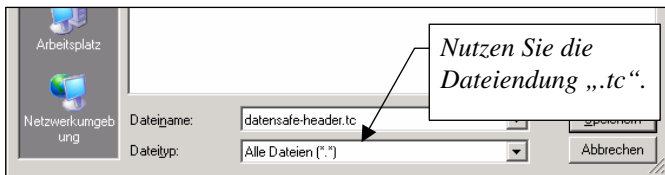
Mit einem Klick auf „Datenträger“ könnten Sie hier auch einen Datensafe anlegen, der eine ganze Partition umfasst. Für die meisten Anwendungszwecke empfehlen sich aber die Containerdateien, weil sie wie ganz normale Dateien gesichert, verschoben oder auf mobilen Datenträgern mitgeführt werden können.



*In diesem Fenster entscheiden Sie, ob Ihr Safe als Datei oder Partition gespeichert werden soll.*

## Wählen Sie den Dateinamen und den Speicherort

4. Legen Sie nun fest, in welchem Ordner und unter welchem Namen Sie Ihren Datensafe speichern wollen. Klicken Sie auf „Speichern“ und dann auf „Weiter“.



*Soll Ihr Safe als solcher nicht auffallen, so wählen Sie einen weniger signifikanten Dateinamen als wir.*

Wir haben unseren Safe „datensafe.tc“ genannt. Die Dateierweiterung ".tc" wurde bei der Installation von TrueCrypt mit diesem verknüpft. Verwenden Sie diese Dateierweiterung, so

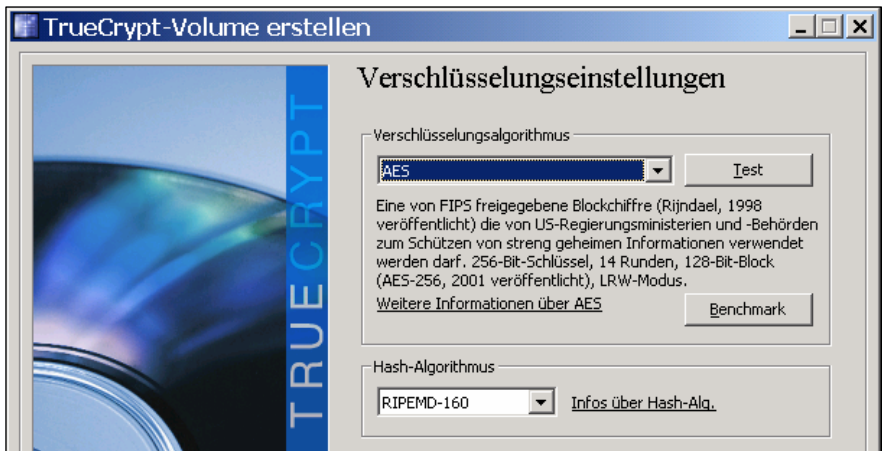
können Sie Ihren Datensafe durch einen Doppelklick auf die .tc-Datei bequem direkt in TrueCrypt öffnen. Sie können Ihre Containerdatei später übrigens beliebig verschieben oder umbenennen.



5. Im nächsten Fenster legen Sie fest, nach welchem Verfahren Ihr Datensafe verschlüsselt werden soll. TrueCrypt bietet Ihnen verschiedene Verschlüsselungs- und Hash-Algorithmen an.

**Die beste Verschlüsselungsmethode**

„AES“ ist eine gute Wahl. Dieser Algorithmus arbeitet mit einer extrem sicheren und ausgesprochen schnellen 256bit-Verschlüsselung. In der Kategorie „Hash-Algorithmus“ können wir Ihnen die Einstellung „RIPEMD-160“ empfehlen.



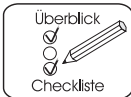
*AES und RIPEMD-160 bilden ein gutes Schlüsselteam.*

6. Legen Sie jetzt fest, wie groß Ihr Datensafe werden soll. Für Ihren ersten Probesafe sollten 100 MB genügen.

**Wie groß darf's sein?**



*Wie groß soll Ihr Safe werden?*



Bei der Planung der Größe Ihres Datensafes sollten Sie diese 4 Aspekte beachten:

- Ihr Volume sollte so groß sein, dass die Dateien, die Sie darin verstecken möchten, auch Platz finden.
- Ihr Datensafe sollte aber auch so klein sein, dass er auf den Datenträger passt, auf dem Sie ihn transportieren oder sichern möchten.
- Wollen Sie große Datenmengen verschlüsseln, empfiehlt es sich deshalb oft, mehr als einen Datensafe anzulegen und die Dateien thematisch auf diese Safes zu verteilen.
- Die Größe eines Volumes sollte übrigens nachträglich nicht verändert werden. TrueCrypt bietet zwar die Möglichkeit, die Volume-Größe dynamisch zu verwalten, doch verringert dieses Verfahren die Sicherheit und die Transfer-Performance Ihrer Datensafes spürbar.

**Vergeben Sie ein knacksicheres Passwort**

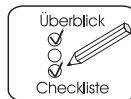
7. Vergeben Sie nun ein Kennwort. Je länger und kryptischer das Kennwort, desto sicherer sind Ihre Daten insbesondere vor Brute-force- oder Wörterbuch-Angriffen. Ihr Kennwort sollte mindestens 10 Zeichen lang sein und neben Buchstaben auch Ziffern und Sonderzeichen enthalten.

**Wählen Sie das passende Format**

8. Wählen Sie nun das Dateisystem aus, in dem Ihr Datensafe formatiert werden soll. Zur Wahl stehen das FAT- und das NTFS-Format. Ihre Anwendungssituation entscheidet

darüber, welches Format für Sie das richtige ist:

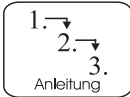
- NTFS ist grundsätzlich die beste Wahl, weil es Ihren Dateien bei geöffnetem Datensafe am meisten Sicherheit bietet. NTFS-formatierte Datensafes lassen sich aber nur unter Windows 2000, XP und Vista problemlos öffnen.
- FAT ist das ideale Format, wenn Sie Ihren Datensafe auch unter anderen Betriebssystemen wie Windows 98, ME, Linux oder Apple Macintosh öffnen wollen. Mobile Safes sollten Sie also FAT-formatieren.
- Wollen Sie Dateien verschlüsseln, die mehr als 4 GB groß sind, so müssen Sie sich für NTFS entscheiden.
- Möchten Sie hingegen ein verstecktes Volume anlegen, so ist dies nur unter FAT möglich.



*Wählen Sie ein Dateisystem und lassen Sie die Maus tanzen.*

9. Jetzt kommen wir zum sportlichen Teil unserer Übung. Lassen Sie Ihren Mauszeiger für gut 20 Sekunden über Ihrem TrueCrypt-Fenster „tanzen“. Sie werden sehen, wie

**Lassen Sie Ihre Maus tanzen**



die Zeichenkette in der Zeile „Zufallswerte“ auf diese zufälligen Bewegungen reagiert. Sie erzeugen auf diese Weise einen besonders sicheren, weil tatsächlich zufälligen Verschlüsselungscode.

10. Nun sind alle Einstellungen für Ihren Datensafe festgelegt und Sie können auf „Formatieren“ klicken. Bestätigen Sie alle folgenden Meldungen. Im Fenster „Volume wurde erstellt“ klicken Sie dann auf „Beenden“.

### So öffnen Sie Ihren Datensafe

Öffnen Sie nun Ihren neuen Datensafe, um die ersten Dateien darin zu sichern.

#### Laufwerksbuchstaben zuweisen

1. Markieren Sie dazu im TrueCrypt-Fenster den Laufwerksbuchstaben, den Sie Ihrem Datensafe zuweisen wollen. Klicken Sie dann auf „Datei“. Diese Laufwerkszuweisung ist nicht endgültig. Sie können Ihrem Safe jederzeit einen anderen Laufwerksbuchstaben zuweisen.
2. Im folgenden Fenster wählen Sie die zugehörige Containerdatei aus und klicken dann auf „Öffnen“.

#### Datensafe wird als virtuelles Laufwerk eingebunden

3. Sie landen wieder im Hauptfenster. Klicken Sie auf „Einbinden“. Sobald Sie die Passwortabfrage bestätigt haben, wird Ihr Datensafe als virtuelles Laufwerk eingebunden.
4. Ein Doppelklick auf die entsprechende Laufwerkszeile im TrueCrypt-Fenster lädt dieses Laufwerk im Explorer.
5. Ihr geöffneter Datensafe verhält sich nun wie ein ganz normales Laufwerk. Sie können darauf wie gewohnt Dateien erstellen, ablegen, umbenennen oder von dort aufrufen.

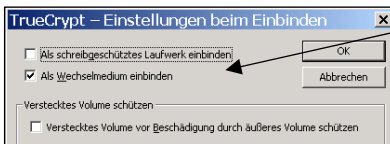
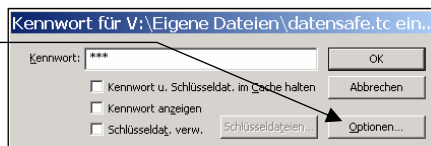
Windows interpretiert das virtuelle Laufwerk Ihres Datensafes als ein reguläres Laufwerk. Windows ME, XP und Vista legen deshalb die Systemobjekte „Papierkorb“ und „System Volume Information“ in Ihrem Datensafe an. Dieser Umstand kann Ihnen später Zugriffskonflikte beschicken. Diese treten dann auf, wenn Sie Ihren Safe schließen wollen, Windows aber weiter auf die genannten Systemobjekte zugreifen will.

Um solche Konflikte zu vermeiden, können Sie Ihre Datensafes gezielt als „Wechselplattenlaufwerk“ öffnen. In diesem Modus wird Windows seine Systemobjekte nicht in Ihren Safes installieren oder weiter darauf zugreifen. Klicken Sie dazu im Fenster der Kennwortabfrage auf „Optionen“ und setzen Sie im nächsten Fenster ein Häkchen vor „Als Wechselmedium einbinden“.



## Datensafe als Wechselmedium entkoppeln

*Schritt 1:  
„Optionen“  
anklicken*

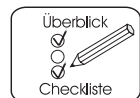


*Schritt 2:  
Häkchen bei „Als  
Wechselmedium ein-  
binden“ setzen*

*So binden Sie Ihren Safe als Wechselplattenlaufwerk ein.*

## So schließen Sie Ihren Datensafe

Um Ihren Datensafe zu verriegeln, markieren Sie im TrueCrypt-Fenster das entsprechende Laufwerk und klicken dann auf „Trennen“. Speichern und schließen Sie unbedingt vorher



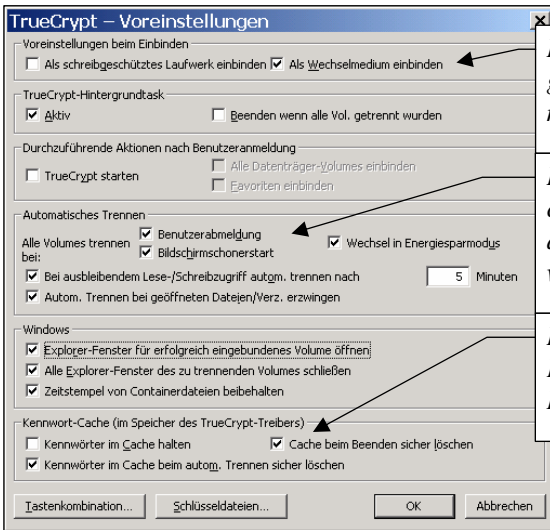


## Bedingungen fürs automatische Trennen festlegen

alle Dateien des Safes, die gerade in Anwendungen geöffnet sind.

Sie können übrigens auch festlegen, in welchen Situationen TrueCrypt Ihre Safes automatisch schließen soll. Das ist dann sinnvoll, wenn auch andere User Zugriff auf Ihren PC haben. Klicken Sie dazu in der Menüzeile auf „Einstellungen/Voreinstellungen“. Im Block „Automatisches Trennen“ können Sie bestimmen, ob Ihre Safes durch Ereignisse wie die Benutzerabmeldung oder den Start des Bildschirmschoners geschlossen werden sollen.

Um das Schließen des Safes unter allen Umständen durchzusetzen, muss hier auch die Option „Automatisches Trennen bei geöffneten Dateien/Verz. erzwingen“ aktiviert sein. Nicht gespeicherte Änderungen an den geöffneten Dateien des Safes gehen dann allerdings beim Schließen verloren.



Hier können Sie Ihre Safes grundsätzlich als Wechselmedien öffnen lassen.

Hier legen Sie fest, in welchen Situationen Ihre Safes automatisch geschlossen werden.

Dies sind die sichersten Einstellungen zum Schutz Ihrer Kennwörter.

Hier legen Sie fest, wie sich TrueCrypt verhalten soll.

## So schützt TrueCrypt Ihre Daten



Wie sorgt TrueCrypt eigentlich dafür, dass Ihre Dateien zu jeder Zeit vor fremden Zugriffen sicher sind?

TrueCrypt speichert weder Ihre Passworte noch entschlüsselte Dateien auf Ihren Datenträgern. Es entschlüsselt diese lediglich temporär in den flüchtigen Arbeitsspeicher und übergibt sie von dort aus an Windows.

Es werden auch immer nur die Dateien entschlüsselt, auf die Sie gerade zugreifen. Klicken Sie beispielsweise auf eine in Ihrem Datensafe gespeicherte Word-Datei, so wird diese – wie gewohnt – automatisch in Word geladen. Das TrueCrypt diese Datei zunächst in Ihrem Arbeitsspeicher entschlüsselt und von dort an Word übergibt, bemerken Sie als Anwender nicht.

Umgekehrt werden Dateien, die Sie in Ihrem Datensafe speichern, auf dem Weg dorthin von TrueCrypt im Arbeitsspeicher verschlüsselt, ehe sie auf den Datenträger geschrieben werden. Auch wenn Ihr Datensafe geöffnet ist, sind die Daten darin also immer vollständig verschlüsselt.

## Sicherheit für unterwegs! TrueCryptTraveller

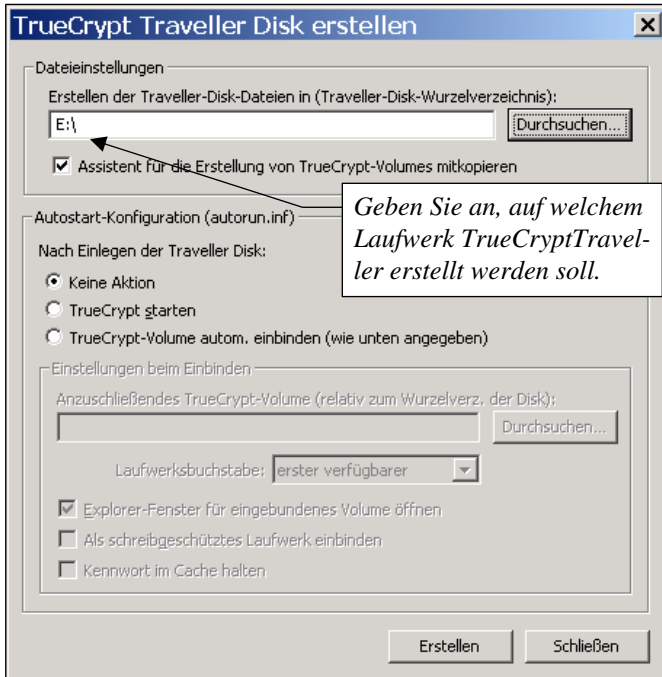
Ein großer Vorteil von TrueCrypt: Dieses Tool ist „mobil“. Sie können es zusammen mit Ihrem Datensafe auf einem USB-Stick speichern und von dort auch auf Rechnern starten, auf denen TrueCrypt nicht installiert ist.

TrueCrypt nennt seine mobile Variante „Traveller“. Diesen Traveller können Sie mit wenigen Mausklicks erstellen:

**So erstellen  
Sie TrueCrypt-  
Traveller**

1. →  
2. →  
3.  
Anleitung

Klicken Sie in der Menüzeile von TrueCrypt auf „Extras \Traveller Disk erstellen“ und geben Sie dann an, auf welchem Laufwerk das mobile Tool eingerichtet werden soll. Hier wird dann ein Ordner mit Namen TrueCrypt erstellt. Er enthält die Programmdateien von TrueCryptTraveller.



*TrueCryptTraveller ist schnell erstellt.*

### So arbeiten Sie mir TrueCryptTraveller

1. Um TrueCryptTraveller auf einem fremden PC auszuführen, öffnen Sie diesen Ordner und starten die Programmdatei „TrueCrypt.exe“.
2. Ihren Datensafe öffnen Sie dann, indem Sie seine Container-Datei mit der Maus in das TrueCrypt-Fenster ziehen.

3. Nun markieren Sie einen der hier aufgeführten freien Laufwerksbuchstaben und klicken dann auf „Einbinden“. Verfahren Sie ansonsten, wie Sie es gewohnt sind.



- Um TrueCryptTraveller unter Windows 2000, XP oder Vista zu starten, benötigen Sie Administrator-Rechte.

## So pflegen Sie Ihre Datensafes

Nun sind Ihre wichtigen Daten im Safe vor fremdem Zugriff sicher. Aber wie wirkt sich die Verwendung Ihres neuen Datensafes auf die „andere Datensicherheit“ aus? Die Sicherheit vor Datenverlust? Werfen wir mal einen Blick auf die drohenden Gefahren ...

**Datenverlust  
droht Ihnen  
trotzdem**

- Ist Ihr Datensafe geöffnet, können Viren und Hacker auf die Daten im Safe zugreifen. Genauso gut oder schlecht, wie auf die Daten Ihrer anderen regulären Laufwerke.
- Ist Ihr Datensafe geschlossen, sind die Dateien darin vor fremdem Zugriff sicher. Aber: Die Containerdatei Ihres Safes kann, wie jede andere Datei, durch Viren, Userfehler oder eine defekte Festplatte beschädigt werden.

Leichte Beschädigungen des Dateisystems Ihres Datensafes lassen sich meist reparieren. Haben Sie also Probleme beim Zugriff auf Dateien im Safe, so tun Sie Folgendes:

1. Schließen Sie den Safe, um eine Sicherungskopie seiner Containerdatei zu erstellen. Das ist nötig, weil so ein Reparaturversuch den Zustand Ihrer Daten durchaus auch verschlimmbessern kann.
2. Öffnen Sie den Datensafe nun wieder und klicken Sie mit der rechten Maustaste auf seinen Laufwerkseintrag im

**So gehen Sie  
mit leichten  
Beschädigungen  
um**

TrueCrypt-Fenster. Wählen Sie hier die Option „Dateisystem prüfen“ oder gegebenenfalls „Dateisystem reparieren“. Ihr Datensafe wird dann standardmäßig mit „CHKDSK“, dem Bordtool von Windows, repariert.

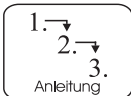
**Datenverlust droht!**

Schwer beschädigte Datensafes hingegen lassen sich weder reparieren noch öffnen. In diesem Fall sind alle Dateien im Safe unwiederbringlich verloren.

Sie sollten Ihre Datensafes deshalb unbedingt regelmäßig sichern – am besten auf anderen Datenträgern. Berücksichtigen Sie diesen Punkt schon bei der Planung Ihrer Safes, denn seine Containerdatei muss auf Ihr Sicherungsmedium passen.

**Nur Header sichern**

Selbst wenn Sie nicht genug freien Speicherplatz für ein so umfassendes Backup haben oder ein unverbesserlicher Sicherungsmuffel sind, sollten Sie dennoch unbedingt das folgende Backup durchführen ...

**Sichern Sie den Volume-Header Ihres Datensafes**

Diese Sicherung muss nur einmal durchgeführt werden, ist mit drei Mausklicks erledigt und verbraucht kaum ein KB Speicherplatz.

1. Schließen Sie Ihren Safe, klicken Sie dann unter TrueCrypt erst auf „Vol.-Operationen“ und danach auf „Volume-Header sichern“.
2. Im nächsten Fenster weisen Sie der Sicherungsdatei dann einen Namen zu.
3. Um im Ernstfall einen beschädigten Header zu ersetzen, klicken Sie auf „Volume-Header wiederherstellen“ und wählen dann die passende Sicherungsdatei aus.

Der Volume-Header ist der Teil der Containerdatei, in dem der „Master-Key“ Ihres Datensafes steckt. Wird der Header beschädigt, können Sie den Safe nicht mehr öffnen.



Beachten Sie diese fünf Tipps zum Umgang mit dem Volume-Header:



- Die Sicherungsdatei des Volume-Headers kann zwar ohne Ihr Passwort nicht entschlüsselt werden, sollte aber dennoch in einem Datensafe verwahrt werden. Aber natürlich nicht in dem Safe, der dieses Backup sichern soll!
- Wenn Sie das Passwort Ihres Datensafes ändern, muss Ihr Volume-Header erneut gesichert werden, denn das Passwort ist Bestandteil des Volume-Headers.
- Müssen Sie bei der Wiederherstellung eines solchen Headers auf eine ältere Sicherung zurückgreifen, wird dabei das Passwort reaktiviert, das zum Zeitpunkt dieser Sicherung galt.
- Bedenken Sie dies auch, wenn Sie Ihr Passwort ändern, um jemanden nachträglich von der Nutzung Ihres Datensafes auszuschließen.
- Hatte diese Person Gelegenheit, Ihren Volume-Header zu sichern oder eine Kopie des Datensafes anzulegen, so kann sie den alten Volume-Header auf Ihrem Datensafe wiederherstellen. So wird dann das alte, ihr bekannte Passwort reaktiviert und gewährt erneut Zugriff auf Ihre Daten. In diesem Fall sollten Sie einen ganz neuen Datensafe erstellen und die Daten des alten Safes in den neuen übertragen.

**Vorsicht!**  
**Datenklau mit**  
**Hilfe des**  
**Volume-**  
**Headers**

**Tipps & Tricks zu TrueCrypt****Große Safes  
auf DVD  
brennen**

Sie möchten einen Datensafe brennen, der mehr als 2 GB groß ist, aber Ihr Brennprogramm quittiert dies mit einer Fehlermeldung? Verwenden Sie ein anderes DVD-Format. Im Format „UDF“ lassen sich große Dateien problemlos brennen.

**Datensafe zu  
langsam**

Haben Sie den Eindruck, dass die Zugriffe auf Ihren Datensafe zu langsam erfolgen? Dann schließen Sie Ihren Datensafe und defragmentieren Sie das Laufwerk, auf dem seine Containerdatei liegt. Stark fragmentierte Containerdateien verzögern den Datentransfer von und zum Safe deutlich.

**Datensafe  
beim Booten  
automatisch  
öffnen**

Sie können Ihren Datensafe beim Start von Windows automatisch bis zur Kennwort-Abfrage laden lassen.

Öffnen Sie dazu den betreffenden Safe und klicken Sie dann in der Menüzeile auf „Volumes\Favoriten einbinden“.

Klicken Sie dann auf „Einstellungen\Voreinstellungen“. Aktivieren Sie „TrueCrypt starten“ und „Favoriten einbinden“.

**Programme  
aus dem Safe  
ausführen**

Sie können übrigens auch ganze Programme in Ihrem Datensafe installieren und von dort ausführen. Das ist sinnvoll, wenn Sie beispielsweise Ihren Browser und seine Bookmarks oder den Mailclient und Ihre Mails komplett vor fremdem Zugriff schützen wollen. Sie sollten dann aber Programme verwenden, die keine Daten in der Windows-Registry oder den temporären Verzeichnissen von Windows speichern. In Frage kommen hier also in erster Linie „portable“ Tools wie:

- Mozilla Thunderbird, Portable Edition  
[http://portableapps.com/de/apps/internet/thunderbird\\_portable](http://portableapps.com/de/apps/internet/thunderbird_portable)
- Mozilla Firefox, Portable Edition  
[http://portableapps.com/de/apps/internet/firefox\\_portable](http://portableapps.com/de/apps/internet/firefox_portable)