

# Moneyplex 2007 mit TrueCrypt unter SuSE Linux 10.1 Howto

Autor

Jörg Major

## Inhaltsverzeichnis

1. Einleitung.....	2
2. Wichtige Anmerkungen.....	2
3. Voraussetzungen.....	3
4. Nun geht's los.....	3
4.1 TrueCrypt unter Linux einrichten.....	3
4.2 TrueCrypt Volume erstellen.....	4
4.3 Container File mounten und unmounten.....	6
4.4 Die wichtigsten TrueCrypt Befehle.....	6
4.5 Konfiguration von /etc/sudoers .....	6
4.6 Moneyplex in TrueCrypt Volume verschieben.....	8
5. Moneyplex per Icon auf KDE Desktop starten.....	8
5.1 Shell Script.....	9
5.2 Moneyplex Start-Script anpassen.....	10
5.3 Einstellungen in Moneyplex.....	11
6. Sicherheitstipps und Ausblick.....	13
6.1 Probleme beim Aushängen.....	13
6.2 TrueCrypt-Header Backup.....	13
6.3 Schwachstelle: Journaling Filesysteme.....	14
6.4 TrueCrypt mit Keyfiles.....	14
6.5 Hidden Volume.....	15
6.6 Gemeinsame Nutzung unter Linux und Windows.....	15
7. Fazit.....	15
8. Literatur und Links.....	16

GNU Free Document License

Die Originalversion der GFDL finden Sie unter: [www.gnu.org/copyleft/fdl.html](http://www.gnu.org/copyleft/fdl.html)

## 1. Einleitung

Sicheres Homebanking nach Stand der Technik ist zur Zeit nur mit HBCI und einem externen Cardreader mit separatem Keypad möglich. Wohl dem, der die technischen Hürden für HBCI mit seiner Bank genommen und das Kartenlesegerät zur Zusammenarbeit mit dem Linux Rechner überredet hat.

Leider schleicht sich unweigerlich ein ungutes Gefühl ein, wenn man seine Kontodaten unverschlüsselt auf der Festplatte ablegt und das nicht erst seit unser Innenminister den „Bundestrojaner“ zu unser aller „Sicherheit“ angekündigt hat.

Hier bietet sich Verschlüsselung als ein adäquates Mittel an, da niemand ernsthaft zulassen wird, dass private Daten in fremde Hände fallen und missbraucht werden. Die wichtigsten Kriterien bei Verwendung von Verschlüsselungstechniken sind Quelloffenheit, starke Verschlüsselungsalgorithmen und eine möglichst einfache Handhabung.

Die Open-Source Software TrueCrypt [1] erfüllt diese Kriterien und unterstützt eine ganze Reihe offener Algorithmen zur Datenverschlüsselung, darunter sind u.a AES (Advanced Encryption Standard), Blowfish und 3DES die bekanntesten.

TrueCrypt wurde ursprünglich für Windows entwickelt. Daher fehlten unter Linux bisher noch einige Features wie z.B. eine grafische Oberfläche (GUI) oder die dynamische Grössenanpassung von Containern. Inzwischen scheint es auch für Linux die erste GUI zu geben [2]. Sowohl unter Linux als auch unter Windows erstellte verschlüsselte Container und Partitionen mountet TrueCrypt anstandslos auch auf dem jeweils anderen Betriebssystem, sofern dieses das verwendete Dateisystem unterstützt.

Dieses Howto beschreibt die Verwendung von Moneyplex 2007 auf SuSE Linux 10.1 (Kernel 2.6.16-smp, 64 bit) zusammen mit TrueCrypt 4.3a. Das Hauptaugenmerk liegt dabei auf der einfachen Bedienung, d.h. dem scriptgesteuerten Starten und Beenden der Moneyplex Anwendung vom Desktop der KDE 3.5 Oberfläche in einem verschlüsselten TrueCrypt Container.

Auch wenn Moneyplex 2007 bei Ihnen schon längere Zeit im Einsatz ist, kann nachträglich eine Umstellung auf einen TrueCrypt Container erfolgen, da die Moneyplex Verzeichnisstruktur mit allen Daten 1:1 in das Container File verschoben werden kann.

Das beschriebene Vorgehen in diesem Howto sollte mit geringfügigen Änderungen auch auf andere Linux Distributionen mit Kernel 2.6 sowie 32 bit Kernel oder Gnome statt KDE übertragbar sein.

## 2. Wichtige Anmerkungen

Dieses Howto wurde nach bestem Wissen und Gewissen verfasst und soll als Hilfestellung sowie als Lösungsvorschlag dienen. Der Autor kann jedoch keinerlei Garantie für die Richtigkeit und Funktionsfähigkeit aller Schritte in dieser Anleitung geben. Tippen Sie bitte kein Kommando ein, ohne zu wissen, was dieses bewirken kann. Weitergehende Links finden Sie am Ende dieses Artikels.

Lassen Sie Sorgfalt bei der Auswahl Ihres TrueCrypt Container Passworts walten. Wählen Sie ein Passwort ausreichender Länge mit Sonderzeichen, Zahlen und Gross/Kleinschreibung der Buchstaben.

Sollten Sie Ihr Container Passwort vergessen, gibt es keine Möglichkeit mehr an

den Inhalt des verschlüsselten Containers zu kommen, ausser Sie wären in der Lage Ihren TrueCrypt Container mit Brute-Force Methoden zu knacken! Wie lange das bei einem 256 Bit AES-Schlüssel dauern kann, ist im Kryptographie Standardwerk [3] von Bruce Schneier nachzulesen.

Befehle, die am Zeilenanfang mit "#" beginnen, müssen als *root* ausgeführt werden. Zeilen, die "\$" als Shellsymbol haben, können als User eingegeben werden.

Das Schlüsselwort "user/User" in Pfadangaben und Scripts muss durch den eigenen Linux Usernamen ersetzt werden!

Das in diesem Howto abgedruckte Shell Script des Autors unterliegt der GPL v3 [4] und darf demgemäss nach Belieben den eigenen Belangen angepasst und als **freie Software** weitergegeben werden.

### 3. Voraussetzungen

- SuSE Linux, Kernel 2.6 oder höher
- Installiertes und funktionierendes Moneyplex 2007
- Installiertes und funktionsfähiges TrueCrypt 4.3a  
Ein erster Test nach der TrueCrypt Installation:  
`#!/usr/bin/truecrypt --test`  
sollte folgendes Ergebnis liefern:  
**Self-tests of all algorithms passed.**
- Ruhe und gute Nerven

## 4. Nun geht's los...

### 4.1 TrueCrypt unter Linux einrichten

Passende Archiv-Dateien gibt es für viele Distributionen [1]. Als Beispiel für ein RPM-Paket installieren Sie TrueCrypt mit dem folgenden Aufruf:

```
#rpm -ivh truecrypt.rpm
```

oder als DEB-Archiv mit dem Befehl

```
#dpkg -i truecrypt.deb
```

Da TrueCrypt ein Kernelmodul einrichtet, kommt es vor, dass die Installation scheitert, wenn ein modifizierter oder aktualisierter Kernel zum Einsatz kommt. In diesem Fall kompilieren und installieren Sie das Programm aus dem Quelltext.

Sie benötigen dafür - falls noch nicht vorhanden - folgende Programme und Dateien auf Ihrem Rechner:

make, gcc, ld, sowie die Kernel-Quellen.

Zur Installation gehen Sie wie folgt vor:

Extrahieren Sie das Quellpaket "*truecrypt-source-code.tar.gz*" als root mit

- Download des Quellpakets "*truecrypt-source-code.tar.gz*" von [1]
- Extrahieren Sie das Quellpaket als root mit  
`#tar xvfz truecrypt-4.3a-source-code.tar.gz -C /usr/local/src`

- Wechseln Sie in das neue Verzeichnis  
`#cd /usr/local/src/truecrypt-4.3.a-sorce-code/Linux`
- Starten Sie den Compiliervorgang mit dem Script `#!/build.sh`
- Nach erfolgreichem Compilieren starten Sie die Installationsroutine mit dem Befehl `#!/install.sh`

**Wichtig:** Unter Umständen müssen Sie diese Prozedur nach einem Kernel-Update wiederholen, damit die benötigten Truecrypt Module neu eingerichtet werden!

## 4.2 TrueCrypt Volume erstellen

Tippen Sie in Ihrem Homeverzeichnis als User im Terminalfenster bitte folgendes Kommando:

```
$truecrypt -c
```

Es folgt eine Abfrage der wichtigsten Parameter zum Einrichten des Container Files:

**Volume type:**

- 1) Normal
- 2) Hidden

**Select [1]**

Die Default Werte stehen in eckigen Klammern. Wählen Sie hier 1.

**Enter file or device path for new volume:**

/media/sdb5/moneyplex.tc (zum Beispiel) Wählen Sie die Partition für das TrueCrypt Volume mit Bedacht (siehe Kap. 6.3).

**Filesystem:**

- 1) FAT
- 2) None

**Select [1]: 1**

FAT ist hier die einfache Wahl.

**Enter volume size (bytes – size/sizeK/sizeM/sizeG): 650M**

650M bis 700M sind eine gute Wahl, da genug Platz für wachsende Moneyplex Dateien inklusive automatischer ZIP-Backups bleibt und diese Größe gut auf eine CD passt. Moneyplex selbst belegt nach der Erst-Installation weniger als 70 MB. Sollten sich bereits viele Backupdateien und Kontodaten angesammelt haben, muss die Größe des Containers evtl. noch oben korrigiert werden.

**Hash algorithm:**

- 1) RIPEMD-160
- 2) SHA-1
- 3) Whirlpool

**Select [1]: 1**

Wählen Sie den Hash-Algorithmus. Definitionen und Bitlängen der Hash-Algorithmen sind im *TrueCrypt User Guide* beschrieben [5]. Wenn Sie sich nicht sicher sind,

welchen Sie verwenden sollen, so ist der Standard die einfachste Wahl. Der Hash-Algorithmus dient zur Integritätssicherung.

**Encryption algorithm:**

- 1) **AES**
- 2) **Blowfish**
- 3) **CAST5**
- 4) **Serpent**
- 5) **Triple DES**
- 6) **Twofish**
- 7) **AES-Twofish**
- 8) **AES-Twofish-Serpent**
- 9) **Serpent-AES**
- 10) **Serpent-Twofish-AES**
- 11) **Twofish-Serpent**

**Select [1]: 1**

Der Standard AES (Advanced Encryption Standard, 256-bit Key) ist keine schlechte Option. Hiermit wird das Verschlüsselungsverfahren definiert, mit dem TrueCrypt das komplette Container File chiffriert.

**Enter password for new volume '/media/sdb5/moneyplex.tc':**

**Re-enter password:**

Hier müssen Sie Ihr Passwort zweimal eingeben. Achtung: Die Eingabe ist nicht sichtbar! Merken Sie sich das Passwort gut, denn Sie haben sonst keinen Zugriff mehr auf den Inhalt Ihres verschlüsselten Volumes.

**Enter keyfile path [none]:**

Der Einfachheit halber bleiben wir bei „none“. Die Verwendung eines zusätzlichen Keyfiles (siehe Kap. 6.4), welches auf einem Wechselmedium z.B. einem USB Stick oder einer Diskette abgespeichert wird, erhöht die Sicherheit. Als Keyfile kann eine beliebige Datei dienen. TrueCrypt verwendet den Inhalt der ersten 1048 KB der Datei als Passwort. D.h. dieses Keyfile sollte dann in diesem Bereich tunlichst nicht mehr verändert werden!

Diese Methode kann ich nur Anwendern empfehlen, die schon ein wenig Erfahrung im Umgang mit TrueCrypt gesammelt haben.

**Is your mouse connected directly to computer where TrueCrypt is running?**

**[Y/n]: Y**

**Please move the mouse randomly until the required amount of data is captured...**

**Mouse data captured: 100%**

**Done: 540 MB Speed: 3.15 MB/s Left:0.00:00**

**Volume created.**

Anschliessend sollte sich in dem angegebenen Verzeichnis die Datei "moneyplex.tc" befinden.

### 4.3 Container File mounten und unmounten

Nun ist es an der Zeit das verschlüsselte Volume zu mounten. Als Mount Point habe ich auf meinem System als root zuvor das Verzeichnis /mnt/tc erstellt:

```
drwxrwx--- 2 root users 48 Jun 25 23:08 tc
```

Der Mount-Befehl hierfür ist:

```
#truecrypt /media/sdb5/moneyplex.tc /mnt/tc
```

Nach der Eingabe des richtigen Passwortes sollte „truecrypt -l“ folgende Zeile ausgeben:

```
/dev/mapper/truecrypt0 /home/user/moneyplex.tc
```

Mit dem Kommando "df" sieht man das virtuelle Device "/dev/mapper/truecrypt0" als Eintrag in der Datei "/etc/fstab" neben anderen gemounteten Filesystemen mit den gewohnten Angaben über "Grösse, Benutzt, Verfügbar und Mount Point".

Um das TrueCrypt-Volumen auszuhängen, geben Sie truecrypt mit der Option -d ein, z.B.:

```
#truecrypt -d /mnt/tc
```

### 4.4 Die wichtigsten TrueCrypt Befehle

\$truecrypt -l	zeigt alle virtuellen Devices und Mount Points
#truecrypt -d	ohne Angabe des Mount Points hängt alle gemounteten Container Files aus.
#truecrypt -C <Containerdatei>	ändert nachträglich die Art der Authentifizierung für einen Container oder ein verschlüsseltes Laufwerk.
#truecrypt --backup-headers --restore-headers	Sicherung und Wiederherstellung des TrueCrypt Headers.

### 4.5 Konfiguration von /etc/sudoers

Für den User root funktioniert alles einwandfrei. Wird TrueCrypt jedoch als nicht privilegierter User ausgeführt, öffnet es das gewünschte Volume nur im Read Only Modus!

Damit der User einzelne Unix Befehle als root ausführen darf, greift man auf das sudo Kommando zurück. Die erlaubten Befehle stehen in der Datei "/etc/sudoers".

**Wichtig:** Diese Datei wird als root mit dem Kommando **#visudo** editiert!

**Beispiel für /etc/sudoers:**

```
# sudoers file.
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#
# Host alias specification

# User alias specification

# Cmnd alias specification

# Defaults specification

# prevent environment variables from influencing programs in an
# unexpected or harmful way (CVE-2005-2959, CVE-2005-4158,
# CVE-2006-0151)
Defaults always_set_home
Defaults env_reset

# In the default (unconfigured) configuration, sudo asks for the root password.
# This allows use of an ordinary user account for administration of a freshly
# installed system. When configuring sudo, delete the two following lines:
##Defaults targetpw # ask for the password of the target user i.e. root
##ALL ALL=(ALL) ALL # WARNING! Only use this together with 'Defaults targetpw'!

# Runas alias specification

# User privilege specification
root ALL=(ALL) ALL
Linux_user ALL=NOPASSWD: /sbin/modprobe truecrypt
Linux_user ALL=NOPASSWD: /usr/bin/truecrypt /media//sdb5/moneyplex.tc /mnt/tc
Linux_user ALL=NOPASSWD: /usr/bin/truecrypt -d /mnt/tc
Linux_user ALL=NOPASSWD: /usr/bin/truecrypt -d
# Uncomment to allow people in group wheel to run all commands
# %wheel ALL=(ALL) ALL
# Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
# Samples
# %users ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users localhost=/sbin/shutdown -h now
```

Dabei muss "Linux\_user" durch den gewünschten Linux Usernamen ersetzt werden. Die Option "ALL=NOPASSWD" erlaubt das Ausführen der anschließenden Befehle ohne zusätzliche Passwort Eingabe des Users!

Man mag hier einwenden, dass die Verwendung der NOPASSWD-Option eine Sicherheitslücke sei. Aber in unserem Fall ist die korrekte Eingabe des Truecrypt Passworts erforderlich, da ansonsten das Mount Kommando ohnehin fehlschlagen würde.

Zum Testen mounten Sie Ihre Container Datei manuell und prüfen, ob Sie Schreib- und Leserechte im eingehängten Filesystem haben. Verwenden Sie die genauen Befehle (mit Pfadangaben!) wie in */etc/sudoers* und stellen Sie den Befehl "sudo" voran.

## 4.6 Moneyplex in TrueCrypt Volume verschieben

Zunächst mounten wir unser bereits erstelltes Container File mit:

```
$sudo truecrypt /media/sdb5/moneyplex.tc /mnt/tc
```

Wenn /etc/sudoers richtig konfiguriert ist, sollte nur eine Abfrage nach dem TrueCrypt Passwort erfolgen und Ihr Container sollte nun für den Linux User „rwx“ eingehängt sein.

Beispiel:

```
drwxrwxrwx 5 root users 4096 2007-09-28 01:55 tc (im Verzeichnis /mnt)
```

Prüfen Sie ob Sie in Ihrem Container als User Dateien anlegen können, z.B. mit

```
$touch <Dateiname>
```

Erhalten Sie die Fehlermeldung "Keine Berechtigung...", dann ist das Mounten der Container Datei nicht mit den passenden User Schreibrechten erfolgt.

Wenn alles geklappt hat, kann die Verzeichnisstruktur von Moneyplex 1:1 in den Container verschoben werden. Eine von vielen Methoden unter Linux ist:

```
$mv /home/user/moneyplex /mnt/tc
```

Vorsichtige Naturen werden die Moneyplex Verzeichnisse wahrscheinlich zunächst kopieren wollen:

```
$cp -Rp /home/user/moneyplex /mnt/tc
```

Nun sollte es im TrueCrypt Container das Verzeichnis "moneyplex" geben, mit allen Unterverzeichnissen und Dateien der originalen Moneyplex Installation:

```
/mnt/tc-- moneyplex
    |-- backups
    |-- ctapi
    |-- doku
    |-- import
    |-- mdaten
    |-- protokoll
    |-- reports
    `-- rup
```

## 5. Moneyplex per Icon auf KDE Desktop starten

Damit wir später mit einem einfachen Mausklick von der KDE Oberfläche aus Moneyplex starten können, erstellen wir ein kleines Shell Script, welches für uns das Einhängen des Volumes, das Starten von Moneyplex und das Aushängen des Containers ausführt.

## 5.1 Shell Script

Erstellen Sie bitte ein Bash-Script nach folgendem Muster:

### moneyplexmnt.sh

```
#!/bin/bash
# moneyplexmnt.sh
# Bash Script zum Mounten eines TrueCrypt Containers
# und Starten von Moneyplex 2007 in KDE
# Copyright (c) 2007 Joerg Major, jmajor@quantentunnel.de
#
# Dieses Programm ist freie Software. Sie können es unter den Bedingungen der GNU General Public
# License, wie von der Free Software Foundation veröffentlicht, weitergeben und/oder modifizieren.
# Die Veröffentlichung dieses Programms erfolgt in der Hoffnung, daß es Ihnen von Nutzen sein wird,
# aber OHNE IRGEND EINE GARANTIE, sogar ohne die implizite Garantie der MARKTREIFE oder der
# VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK.
# Details finden Sie in der GNU General Public License. <http://www.gnu.org/licenses/>.
#-----
#
# Prüfen, ob FAT32 Partition gemountet und moneyplex.tc vorhanden...
ls /media/sdb5/moneyplex.tc >/dev/null 2>&1
if [ $? -eq 0 ]; then
    # TrueCrypt Volume mounten...
    if [ "`df | grep -e 'truecrypt0'" = "" ]; then
        echo "moneyplex.tc wird nach '/mnt/tc' gemountet..."
        sudo /usr/bin/truecrypt /media/sdb5/moneyplex.tc /mnt/tc
        # Hier wird moneyplex im TrueCrypt Volume gestartet...!
        [ "`df | grep -e '/mnt/tc'" != "" ] && /mnt/tc/moneyplex/start
    else
        df
        echo
        echo "TrueCrypt Volume bereits gemountet...!"
        echo "**** Script wird beendet ! ****"
        sleep 5
        exit 1
    fi
else
    echo "TrueCrypt Volume nicht gefunden!"
    echo "**** Script wird beendet ! ****"
    sleep 5
    exit 1
fi
# TrueCrypt Container schliessen nach Beenden von Moneyplex
echo
echo "umount /mnt/tc..."
sleep 1
/usr/bin/truecrypt -d /mnt/tc
# Test ob TrueCrypt Volume angehaengt ist...
if [ "`df | grep -e 'truecrypt0'" != "" ]; then
    echo
    echo "**** Warnung! ****"
    echo "umount des TrueCrypt Volumes fehlgeschlagen...!"
    df | grep -e '/mnt/tc'
    echo "Bitte prüfen, welche Prozesse oder geöffnete Programme"
    echo "auf das TrueCrypt Volume zugreifen:"
    lsof /mnt/tc
    echo
    echo "...und '/usr/bin/truecrypt -d /mnt/tc' aufrufen!"
    echo
```

**Fortsetzung von `moneyplexmnt.sh`**

```
echo "* Zum Schliessen des Terminal Fensters STRG-C drücken! *"
echo
# Schleife kann mit CTRL-C abgebrochen werden
while : ; then
    sleep 1
done
fi
exit 0

#EOF#
```

Vergessen Sie bitte nicht, das Script `moneyplexmnt.sh` für den User "executable" zu machen mit:

```
$ chmod +x moneyplexmnt.sh
```

Wer mag, kann statt eines Shell Scripts ein Perl oder Python Script erstellen.

## 5.2 Moneyplex Start-Script anpassen

Moneyplex wird mit dem Bash-Script „start“ gestartet. Damit dies auch in der neuen Container Umgebung einwandfrei funktioniert muss die Variable `APPPATH` im Script in `"/mnt/tc/moneyplex/start"` geändert werden:

### **Moneyplex Script: start**

```
#!/bin/bash

# Name und Pfad der Applikation
APPNAME='moneyplex'
PRENAME='prestart'
APPPATH='/mnt/tc/moneyplex' # geändert!
# Pfad auf Existenz pruefen.
if [ ! -d "$APPPATH" ]; then
    echo "$APPPATH wurde nicht gefunden."
    exit 1
fi
# Applikation auf Existenz pruefen.
if [ ! -f "$APPPATH/$APPNAME" ]; then
    echo "$APPPATH/$APPNAME wurde nicht gefunden."
    exit 1
fi
cd "$APPPATH"
export LD_LIBRARY_PATH="$APPPATH:$LD_LIBRARY_PATH"
export LC_ALL=
export LANG=de_DE
# Applikationsstart vorbereiten (Updates einspielen usw.).
"$APPPATH/$PRENAME"
# Applikation starten.
chmod 700 "$APPPATH/$APPNAME"
"$APPPATH/$APPNAME"
exit $?
```

Ein Probelauf des `moneyplexmnt.sh` Scripts aus dem Home Verzeichnis des Users sollte nun durch den Aufruf des Shell-Scripts funktionieren:

```
$. /moneyplexmnt.sh
```

Zuerst muss das TrueCrypt Passwort eingegeben werden, darauf erscheint ein kleines Fenster mit der Passwort Angabe des Mandanten und danach startet das gewohnte Moneyplex Programmfenster!

Wenn Moneyplex beendet wird, läuft wie gewohnt das ZIP-Backup, wenn es in den Moneyplex Einstellungen konfiguriert wurde. Damit das Backup vor dem Schliessen des TrueCrypt Containers vollständig durchlaufen kann, ist im "moneyplexmnt.sh" Script mit "sleep 1" eine Pause von einer Sekunde eingebaut. Diese Zeit kann für umfangreiche Moneyplex Installationen entsprechend verlängert werden.

Danach wird der Container ausgehängt und ist somit wieder vor unbefugten Zugriffen gesichert.

### 5.3 Einstellungen in Moneyplex

Wichtige Moneyplex Konfigurationen sind auf der Menüleiste rechts unter *Einstellungen* hinterlegt. Bei Verwendung des TrueCrypt Volumens sollte der Pfad für CTAPI Chipkartentreiber angepasst werden (siehe Abb. 1).

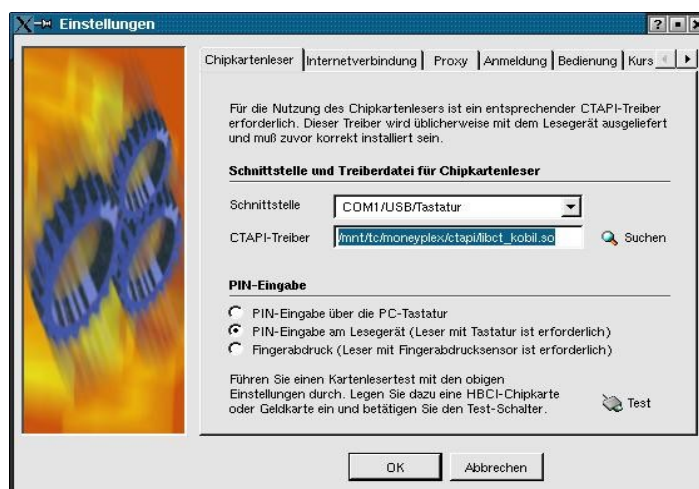


Abbildung 1: Korrektur des CTAPI Treiber Verzeichnispfads

Ebenfalls in den *Einstellungen* unter dem Reiter *Daten* wird die "Automatische Datensicherung" konfiguriert. Hier empfiehlt es sich die Anzahl der ZIP-Backups auf z.B. 20 zu begrenzen, damit der TrueCrypt Container nicht eines Tages durch die Autobackup Funktion unbeabsichtigt vollgeschrieben wird.

### 5.4 Einstellungen für die KDE

Damit später der komfortable Start per Mausklick vom KDE Desktop aus erfolgen kann, kopieren wir zunächst aus dem Moneyplex-Verzeichnis das Icon "mpx48.png" ins Verzeichnis:

```
"/opt/kde3/share/icons/kdeclassic/48x48/apps/"
```

Nun erstellen wir das Symbol in KDE:

Rechte Maustaste auf dem Desktop -> *Neu erstellen* -> *Verknüpfung zu Programm*.

Im X-Fenster *"Eigenschaften für Programdesktop - KDesktop"* werden jetzt folgende Einstellungen vorgenommen:

Im Tabulator *"Allgemein"* wird der Symbolname eingetragen, z.B. Moneyplex.tc

Durch Anklicken des Zahnradsymbols können wir dieses durch das Original Moneyplex-Symbol ersetzen.

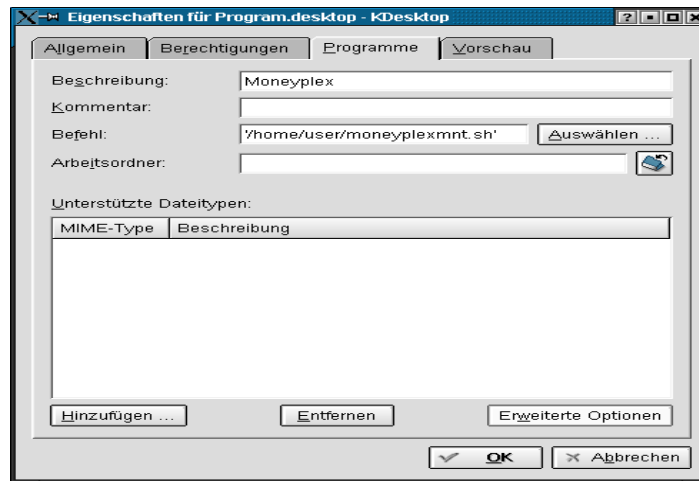


Abbildung 2: Shell Script starten

Im Tabulator *"Programme"* (siehe Abb. 2) können Beschreibung und Kommentar und der Befehl zum Starten eingegeben werden, entweder von Hand den Pfad und Scriptnamen eingeben oder mit "Auswählen" einstellen:

*Befehl:* `'/home/user/moneyplexmnt.sh'`

Ein Eintrag für *"Arbeitsordner"* ist nicht erforderlich. Wichtig ist noch eine Einstellung in den *"Erweiterten Optionen"* rechts unten im Tabulator *"Programme"* (s.o.) *"Terminal: In Terminal starten"* (siehe Abb. 3)!

Denn wir starten kein Programm, sondern ein Shell Script vom Terminal aus, welches wiederum Moneyplex startet.

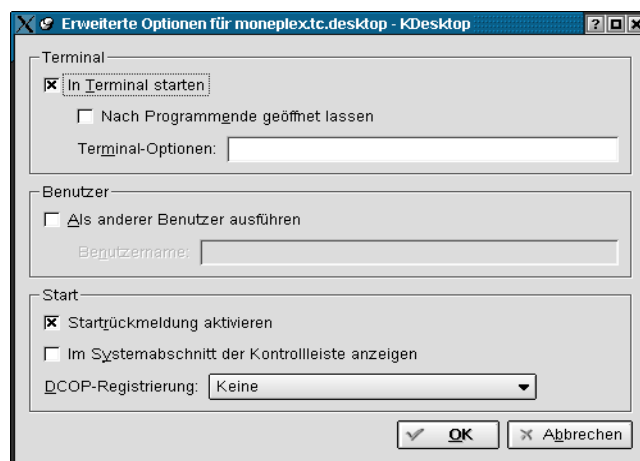


Abbildung 3: Erweiterte Optionen

Nach Bestätigung mit „OK“ sollte sich jetzt auf dem Desktop das bekannte

Moneyplex Symbol befinden.

Durch einen Klick auf das Desktop Symbol öffnet sich zunächst ein Terminalfenster in dem nach dem Passwort für den TrueCrypt Container gefragt wird (siehe Abb. 4):

**Enter password for '/media/sdb5/moneyplex.tc':**

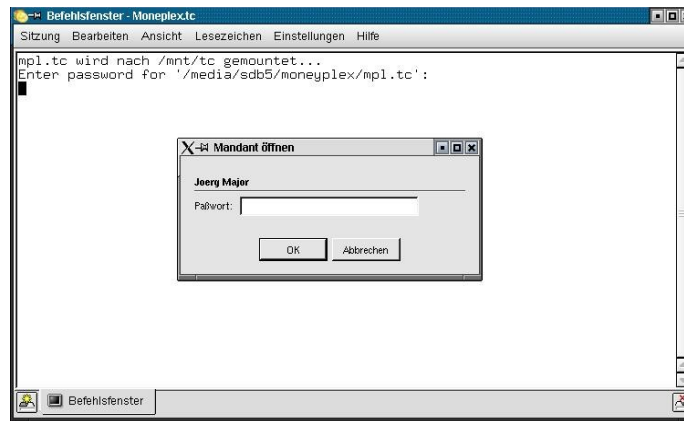


Abbildung 4: Passwort Eingaben

Nach korrekter Passwort Eingabe erscheint die Moneyplex Mandanten Passwort Eingabe und das gewohnte Moneyplex startet aus dem gemounteten TrueCrypt Container (siehe Abb. 5).

Lassen Sie sich nicht irritieren, wenn im Hintergrund das Terminal-Fenster geöffnet bleibt, so lange Sie in Moneyplex arbeiten. Wenn Moneyplex beendet wird und das Autobackup gelaufen ist, schliesst sich auch das Terminal-Fenster wieder mit dem Hinweis: "umount /mnt/tc..."

## 6. Sicherheitstipps und Ausblick

### 6.1 Probleme beim Aushängen

Gelegentlich kann es vorkommen, dass das TrueCrypt Volume nicht ausgehängt wird, wenn ein Programm oder ein Prozess, der auf das Container-File zugreift, nicht beendet wird.

Leider gibt TrueCrypt in solchen Fällen keine Fehlermeldung aus. Das Script "moneyplexmnt.sh" versucht diesen Fehler abzufangen und gibt eine Warnung aus.

### 6.2 TrueCrypt-Header Backup

Sollte aus irgendeinem Grund der Header einer TrueCrypt Container Datei beschädigt sein, so ist in den meisten Fällen das Mounten des Volumens nicht mehr möglich.

Daher empfiehlt es sich, den Header mit folgendem Befehl zu sichern:

```
$truecrypt --backup-header <Sicherungsdatei> Volumenname
```

Der Aufruf

```
$truecrypt --restore-header <Sicherungsdatei> Volumenname
```

stellt den TrueCrypt-Header im Fehlerfall wieder her.

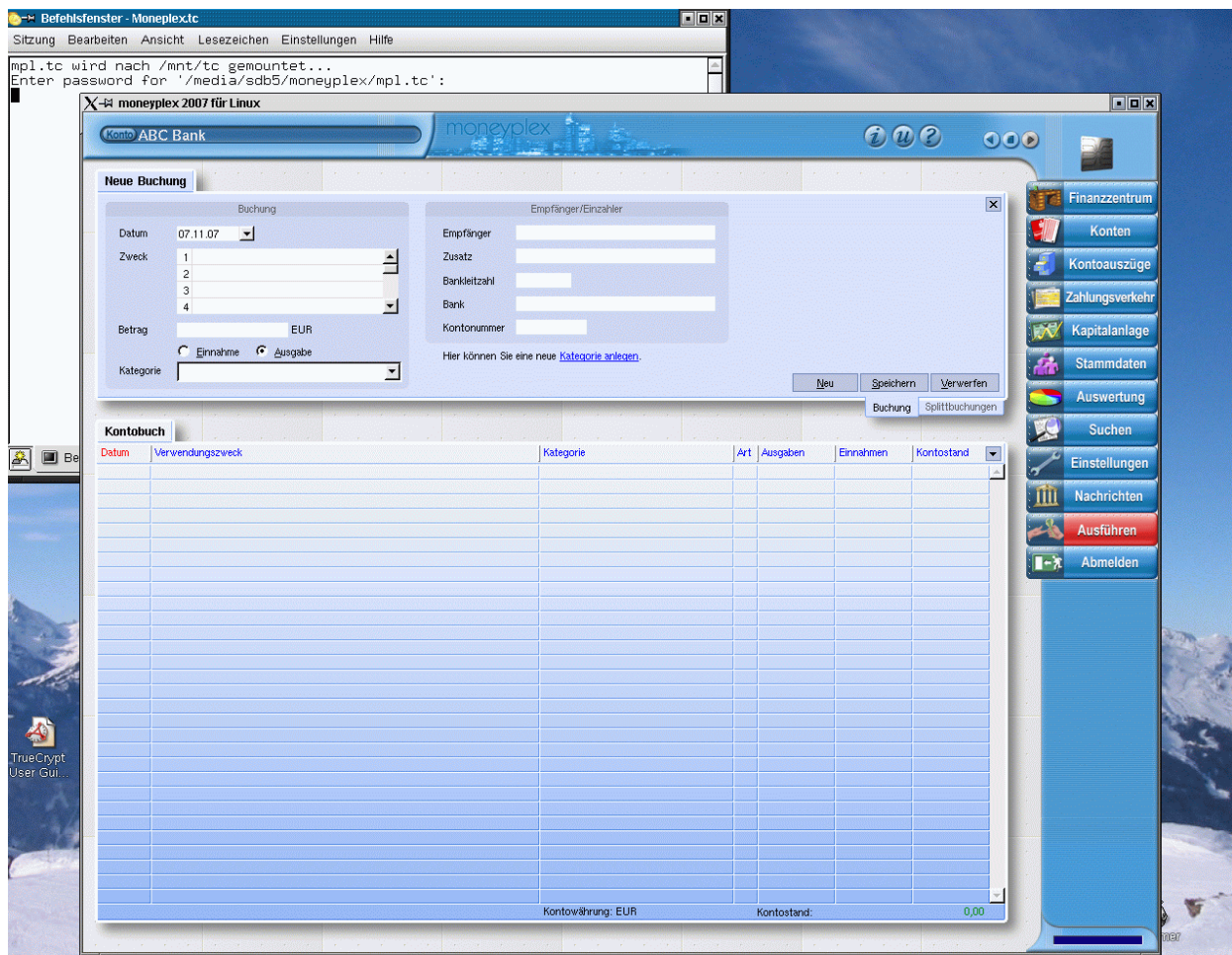


Abbildung 5: Moneyplex aus TrueCrypt Container gestartet

### 6.3 Schwachstelle: Journaling Filesysteme

Befindet sich das TrueCrypt-Volumen auf einem Journaling-Filesystem wie NTFS, Ext3 oder ReiserFS, enthält das Journal unter Umständen eine Kopie des Containers bzw. eines Containerfragments, die es erlauben würden, diesen - beispielsweise nach einem Passwortwechsel - mit dem alten kompromittierten Passwort zu mounten. Der alte Header von 1024 Bytes wäre hierfür ausreichend. Zugegeben, das klingt etwas konstruiert, aber entsprechende forensische Analysemethoden für solche Zwecke gehören zum Standard.

Diese potentielle Sicherheitslücke lässt sich umgehen, indem der TrueCrypt-Container auf einem Filesystem ohne Journal, z.B. FAT oder Ext2, angelegt wird.

### 6.4 TrueCrypt mit Keyfiles

Zum Ver- und Entschlüsseln eines Volumes wird normalerweise ein Passwort verwendet. TrueCrypt bietet mit der Option "--keyfile-create <dateiname>" die Möglichkeit Keyfiles zu erstellen und Container-Files mit Hilfe einer "Schlüssel-datei" zu entschlüsseln. Als Keyfile kann eine beliebige Datei grösser als 1 MB dienen, die dann allerdings tunlichst nicht mehr verändert werden darf.

Der Einsatz eines oder mehrerer Keyfiles, z.B. auf einem USB-Stick gespeichert, kann mit der Verwendung eines Passwortes kombiniert werden, um so eine optimierte Sicherheit zu gewährleisten.

## 6.5 Hidden Volume

Truecrypt ermöglicht es als besonderes Feature in einem freien Bereich einer Container-Datei TrueCrypt-Volumes zu verstecken.

Die Methode ist dabei folgende:

Wenn man ein TrueCrypt Volume mountet, so versucht TrueCrypt mit dem eingegebenen Passwort zuerst den äusseren TrueCrypt Header zu entschlüsseln. Gelingt dies nicht, versucht TrueCrypt automatisch den nächsten Header zu entschlüsseln.

Als Unterscheidungsmerkmal, welches Volume gemeint ist, dient das Passwort oder das Keyfile. Zum Mounten des Wirtscontainers tippen Sie beispielsweise

```
$truecrypt hidden.tc /media/tc -p Passwort1
```

während Sie das geschützte Volume mit

```
$truecrypt hidden.tc /media/tc -p Passwort2 einhängen.
```

Um das versteckte Volume vor dem Überschreiben zu schützen, empfiehlt es sich, das äussere Volume immer mit der Option *-P* wie *protect* zu mounten. In diesem Fall fragt TrueCrypt zuerst nach dem Passwort des äusseren, und anschliessend nach dem des inneren Volumes.

## 6.6 Gemeinsame Nutzung unter Linux und Windows

Verschlüsselte Container Dateien mountet TrueCrypt sowohl unter Linux als auch Windows unabhängig davon, auf welcher Plattform sie erstellt wurden. Wenn also jemand Moneyplex unter beiden Betriebssystemen einsetzt [6], der sollte dies auch mit dem TrueCrypt Container tun können (siehe Matrica Howto). Die einzige Voraussetzung ist, dass das Filesystem unter beiden Betriebssystemen unterstützt wird. FAT bzw. FAT32 ist daher die Default Einstellung bei der Erstellung eines verschlüsselten Containers. Der Nachteil ist, dass mit diesem Filesystem keine User spezifischen Eigenschaften, z.B. Zugriffsrechte, definierbar sind. Ausser FAT sind prinzipiell auch Ext2 oder Ext3 Filesysteme verwendbar, wenn man für Windows die IFS-Treiber nachrüstet [7,8].

## 7. Fazit

TrueCrypt ist ein flexibel einsetzbares und schnelles Open-Source Programm [9] zur Verschlüsselung ganzer Festplattenpartitionen, eines USB Sticks oder von Container Dateien. Vom eigentlichen Ver- und Entschlüsselungsvorgang merkt der Anwender normalerweise nichts. Es werden bei sorgfältigem Umgang und bei richtiger Auswahl des Filesystems keinerlei entschlüsselte Daten auf die Festplatte geschrieben. Ein verschlüsseltes TrueCrypt Volume ist als solches auf der Festplatte nicht ohne weiteres zu erkennen, da der Dateiname frei festgelegt werden kann.

Mit den hier in aller Kürze beschriebenen Massnahmen wie z.B. der Verwendung von Keyfiles oder Hidden Volumes kann man TrueCrypt den persönlichen Sicherheitsbedürfnissen weiter anpassen und den Sicherheitsstandard verbessern - wenn man will.

Man sollte jedoch bedenken, dass damit die Komplexität und Fehlermöglichkeiten beim Umgang mit TrueCrypt zunehmen werden.

Man kann mit der hier aufgeführten Methode, der Verwendung eines verschlüsselten Containers, eine hinreichende Sicherheit erzielen, ohne gleich eine bootfähige Neuinstallation seines Betriebssystems auf einer verschlüsselten Festplatte durchführen zu müssen.

TrueCrypt ist ideal geeignet, um auf einfache Weise für Moneyplex 2007 einen verschlüsseltes Container File zur Verfügung zu stellen. Das Script *moneyplexmnt.sh* vereinfacht den Umgang mit dem TrueCrypt Volume wesentlich. Die Daten im Container File sind gut geschützt, da der TrueCrypt "Tresor" erst dann geöffnet wird, wenn Moneyplex gestartet wird und nach dem Schliessen der Anwendung ebenfalls wieder geschlossen wird.

Und nun – viel Spass bei der Umsetzung!

## 8. Literatur und Links

[1] TrueCrypt: <http://www.truecrypt.org>

[2] LinuxUser 08/2007, S. 50ff.

[3] Angewandte Kryptographie, Bruce Schneier, Addison-Wesley, ISBN 3-89319-854-7

[4] <http://www.gnu.org/licenses/>

[5] TrueCrypt User Guide.pdf, enthalten in der Windows Version *truecrypt-4.3a.zip*

[6] Matrica Homepage: [www.matrica.de](http://www.matrica.de), "7.2 Zeitversetzter Betrieb unter Windows und Linux auf dem gleichen Datenbestand"

[7] Ext2IFS: <http://fs-driver.org/>

[8] Ext2IFS im Einsatz: T. Leichtenstern, "Grenzübertritt", LinuxUser 10/2006, S. 50

[9] TrueCrypt Lizenz: <http://www.truecrypt.org/license.php>