

Arbeiten mit Windows Freigaben innerhalb von TrueCrypt Containern

Von Christian Küken (www.kueken.de), 22.03.2008

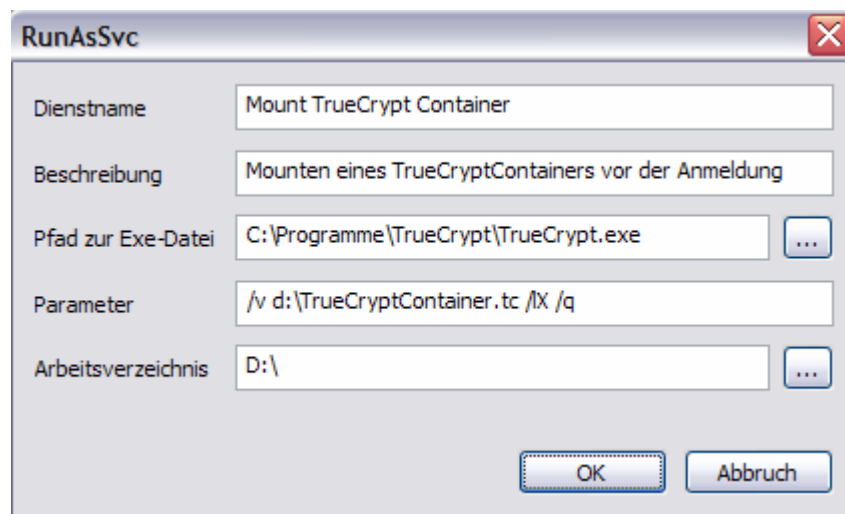
Häufig möchte man Inhalte verschiedenen Benutzern im Netzwerk zur Verfügung stellen. Das geschieht häufig über Freigaben. Diese werden jedoch nur dann bei einem Systemstart wieder zur Verfügung gestellt, wenn es die entsprechenden Ordner vor der Anmeldung am System bereits gibt. Möchte man diese Daten nun verschlüsseln, dann hat man zwei Möglichkeiten.

1. Man erstellt ein verschlüsseltes System Laufwerk.
Vorteil: Komplette Verschlüsselung des Systems einschl. Swap, Temp, etc
Nachteil: Geringe Flexibilität
2. Man erstellt einen verschlüsselten Container und mountet diesen
Vorteil: Container kann an beliebiger Stelle gespeichert werden
Nachteil: Freigaben verschwinden beim Neustart des Systems, da die Laufwerke erst dann gemountet werden können, wenn man schon angemeldet ist. In diesem Fall findet jedoch Windows die freigegebenen Verzeichnisse nicht.

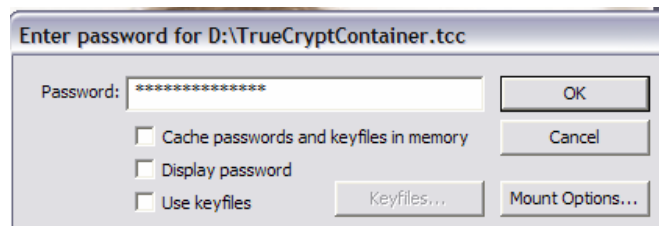
Um alle Vorteile miteinander zu verbinden und die Nachteile abzustellen, kann wie folgt vorgegangen werden:

1. Verschlüsselung des gesamten Systems
2. Erstellung eines verschlüsselten Containers (Hier: „TrueCryptContainer.tc“), der an beliebiger Stelle abgelegt werden kann.
3. Mounten des Containers zum Startzeitpunkt vor der Anmeldung als Dienst.

Die ersten beiden Schritte sind hinreichend in der Dokumentation auf <http://www.truecrypt.org> beschrieben. Hierauf soll nicht weiter eingegangen werden. Für das mounten des TrueCrypt Containers benötigt man ein zusätzliches Programm, bei dem es sich, wie bei TrueCrypt, um frei erhältliche Software handelt. Das Programm RunAsSvc von Dieter Schmeer ist auf <http://www.primasoft.de> als Download frei erhältlich. Es benötigt keine Installation, sondern wird einfach in einem beliebigen Verzeichnis abgelegt. Nach dem Start zeigt es ein einziges Fenster, in dem wir auf unsere lokale TrueCrypt Installation verweisen und die notwendigen Kommandozeilenparameter übergeben. Auch diese sind auf der TrueCrypt Homepage beschrieben. OK, das Fenster sieht wie folgt aus:



Die Software sorgt dafür, dass aus einem ausführbaren Exe-Programm ein Service erstellt wird. Nach einem Druck auf die OK-Taste erscheint der frisch erstellte Service unter /Systemsteuerung/Verwaltung/Dienste in der bekannten Dienste Liste. Wenn man hier den Dienst auf Automatisch stellt, dann wird die angegebene TrueCrypt Container Datei beim Systemstart gemountet. Wenn man bei den Parametern das Passwort (wie hier im Beispiel) nicht mit übergeben hat, wovon auch generell abzuraten ist, dann erhält man im Anmeldebildschirm die bekannte Passwortabfrage von TrueCrypt, jedoch nicht das Programmhauptfenster. Man beachte: eine Anmeldung ist bisher noch nicht erfolgt. Generell könnte hier auch per UltraVNC aus der Ferne das Passwort eingegeben werden. Das funktioniert natürlich nur bei einem unverschlüsselten System.



Wenn man darauf irgendwann keine Lust mehr hat, dann muss man lediglich in den Diensten den Dienst mit dem Namen „Mount TrueCrypt Container“ auf Deaktiviert stellen. Der Dienstname sieht aus wie ein in Windows üblicher UID. Wenn man den Eintrag aus der Windows Dienstliste wieder komplett entfernen möchte, dann benötigt man das Tool „SC“ auf der Konsole, die man durch Ausführen von „CMD.EXE“ erreicht. Gibt man „sc query“ an der Konsole ein, dann werden alle derzeit aktiven Dienste angezeigt. Man sucht sich den entsprechenden Dienst und kopiert den ewig langen Service Namen mit Hilfe der rechten Maustaste (QuickEdit). Dann kann den Dienst mit „sc Stop {3434-344-34“ zunächst beenden. Anschließend muss der Dienst mit Hilfe des „sc delete {UID}“ Befehls gänzlich aus Windows verbannt werden. Die Abfolge ist mit Screenshots auf der nächsten Seite erklärt.

```

Konsole
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT         : 0x0
WAIT_HINT          : 0x0

C:\>sc
DESCRIPTION:
SC is a command line program used for communicating with the
NT Service Controller and services.
USAGE:
sc <server> [command] [service name] <option1> <option2>...

The option <server> has the form "\\ServerName"
Further help on commands can be obtained by typing: "sc [command]"
Commands:
query-----Queries the status for a service, or
              enumerates the status for types of services.
queryex-----Queries the extended status for a service, or
              enumerates the status for types of services.
start-----Starts a service.
pause-----Sends a PAUSE control request to a service.
interrogate----Sends an INTERROGATE control request to a service.
continue-----Sends a CONTINUE control request to a service.
stop-----Sends a STOP request to a service.
config-----Changes the configuration of a service (persistent).
description----Changes the description of a service.
failure-----Changes the actions taken by a service upon failure.
qc-----Queries the configuration information for a service.
qdescription---Queries the description for a service.
qfailure-----Queries the actions taken by a service upon failure.
delete-----Deletes a service (from the registry).
create-----Creates a service. (adds it to the registry).
control-----Sends a control to a service.
sdshow-----Displays a service's security descriptor.
sdset-----Sets a service's security descriptor.
GetDisplayName--Gets the DisplayName for a service.
GetKeyName-----Gets the ServiceKeyName for a service.
EnumDepend-----Enumerates Service Dependencies.

The following commands don't require a service name:
sc <server> <command> <option>
boot----- (ok | bad) Indicates whether the last boot should
              be saved as the last-known-good boot configuration
Lock-----Locks the Service Database
QueryLock-----Queries the LockStatus for the SCManager Database

EXAMPLE:
sc start MyService

Would you like to see help for the QUERY and QUERYEX commands? [ y | n ]: n
C:\>sc query

```

Ergebnis des „sc query“ Kommandos.

```

          WAIT_HINT          : 0x0
SERVICE_NAME: WZCSVC
DISPLAY_NAME: Konfigurationsfreie drahtlose Verbindung
          TYPE               : 20  WIN32_SHARE_PROCESS
          STATE               : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
          WIN32_EXIT_CODE      : 0   (0x0)
          SERVICE_EXIT_CODE   : 0   (0x0)
          CHECKPOINT          : 0x0
          WAIT_HINT           : 0x0

SERVICE_NAME: {08CECC71-A9B1-417d-AB3A-C57C4F854F53}698688194
DISPLAY_NAME: MOUNT TrueCrypt Container
          TYPE               : 10  WIN32_OWN_PROCESS
          STATE               : 4   RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
          WIN32_EXIT_CODE      : 0   (0x0)
          SERVICE_EXIT_CODE   : 0   (0x0)
          CHECKPOINT          : 0x0
          WAIT_HINT           : 0x0

C:\>

```

Anhalten des Dienstes mit dem „sc Stop {...UID mit QuickEdit kopieren ...}“ Kommando

```

EXAMPLE:
sc start MyService

Would you like to see help for the QUERY and QUERYEX commands? [ y | n ]: n
C:\>sc stop {08CECC71-A9B1-417d-AB3A-C57C4F854F53}698688194

```

Entfernen des Dienstes aus der Registry und damit aus der Liste mittels:

```
C:\>sc delete {08CECC71-A9B1-417d-AB3A-C57C4F854F53}698688194
[SC] DeleteService SUCCESS
C:\>
```

So, nun ist der Dienst wieder verschwunden und alles ist wie es mal war.

Nun aber zu den Freigaben. Windows „vergisst“ die Freigaben nicht einfach sobald die zugehörigen Verzeichnisse nicht mehr vorhanden sind. Das bedeutet, man kann den Container auch zunächst völlig normal mit dem TrueCrypt Programm mounten. Wichtig ist, dass man sich vor dem Erstellen von irgendwelchen Netzwerkfreigaben im Klaren darüber ist, unter welchem Laufwerksbuchstaben der Container im gemounteten Zustand künftig auftauchen soll. Es ist zu empfehlen für diese Aktion nicht die Auto Mount Funktion von TrueCrypt zu benutzen, da sich bei der Erstellung von weiteren Containern u.U. die Laufwerksbuchstaben verändern und die Freigaben dann bis zum nochmaligen Mounten auf den ursprünglichen Buchstaben über das Netzwerk nicht mehr erreichbar sind.

Wenn man also zur Vorbereitung einen Container erstellt und diesen beispielsweise als Laufwerk X: mit TrueCrypt einhängt, dann sollte man vor der Erstellung von Freigaben auf dem eingehängenen Laufwerk sicher sein, dass man den Container auch zukünftig als Laufwerk X: verwenden möchte, da Windows nach diesem Laufwerk als Quelle für die Freigaben sucht.

Nun kann man ganz normal Netzwerkfreigaben auf die Verzeichnisse des Laufwerkes oder auch auf das gesamte Laufwerk erstellen. Die Zugriffsrechte können wie gewohnt über die Berechtigungen der Freigaben gesetzt werden.

Eine andere Möglichkeit besteht darin, dass Mounten manuell nach dem Systemstart einzuleiten. Auch hier können Freigaben wie zuvor beschrieben eingerichtet werden. Wird der Rechner jedoch neu gestartet und man meldet sich, dann sind die Freigaben zunächst verschwunden – Klar, der Container ist ja auch noch nicht eingehangen. Das Mounten kann man nun konventionell oder mittels einer Batch Datei erledigen. Ist der Container eingehangen, kann man Windows dazu überreden, doch noch mal von vorne nachzuschauen, ob die alten Freigaben (die innerhalb des Containers, also auf dem eingehängenen Laufwerk X:) nicht doch vorhanden sind. Windows hat nämlich nicht vergessen, dass dort einmal Freigaben waren, sondern hat diese nur nicht angezeigt, weil das Laufwerk X: zum Anmeldezeitpunkt noch nicht vorhanden war. Der Trick besteht in einem Stoppen der entsprechenden Server Dienste, um so anschließend gleich wieder zu starten. Also Mounten, Server stoppen, Server starten → alles ist wieder da ☺

Hier die Batch Datei „MountTrueCryptContainer.bat“

```
@echo off
truecrypt /v d:\TrueCryptContainer.tc /lX /q

net stop Computerbrowser /Y
net stop lanmanserver /Y
net start lanmanserver /Y
net start computerbrowser /Y
```

So, das wär's. Wer Tippfehler findet darf sie behalten.