Truecrypt

In den Medien tauchen immer wieder Berichte auf, wo auf verlorenen USB-Sticks oder gebraucht gekauften Datenträgern noch persönliche oder anderweitig sensible Daten gespeichert sind. In den anschließenden Diskussionen wird dann regelmäßig gefragt, warum die Daten nicht verschlüsselt waren.

Diese Technik soll im Folgenden gezeigt werden und daß sich im praktischen Einsatz der geringe Mehraufwand durchaus ausgleichen kann.

Die Programme

Es gibt heute mehrere Programme, bekannt ist noch Steganos, ebenso Drivecrypt, beide kosten einige Euro. Längst gibt es auch kostenlose Tools, einige Linux-Distributionen wie Ubuntu bringen es von Haus aus mit, man braucht die Option bei der Installation nur anzuwählen. Für Windows und Linux gibt es ein kostenloses Programm, es ist Truecrypt.

Dieses Programm beherrscht verschiedene Anwendungsgebiete, es sollen zwei herausgegriffen werden, der Datencontainer und die Systemverschlüsselung.

Das Programm selbst kann für verschiedene Betriebssysteme als Freeware von www.truecrypt.org heruntergeladen werden. Den Bereich Documentation sollte man sich durchlesen.

Das Programm kennt zwei Betriebsarten, entweder man installiert es fix auf dem Rechner oder benutzt den Portable-Mode, hier hat man es schlicht auf einem externen Datenträger und startet es von dort.

Wie arbeitet so ein Programm?

Im Datenbereich werden alle Bytes gemäß eines Schlüssels durch andere ersetzt, vor dem Datenbereich gibt es einen Schlüsselbereich. Da man über die Häufigkeit von Bytes jedoch Rückschlüsse ziehen könnte, welches Byte durch welches ersetzt wurde, sind die Algorithmen wesentlich weiter ausgebaut.

Der autorisierte Benutzer selbst bekommt durch ein Passwort Zugang zum Schlüssel, der Passwortbereich ist in sich verschlüsselt und das Programm vergleicht, ob das eingegebene Passwort korrekt ist oder nicht, schaltet nur bei richtigem Passwort den Zugang zum Hauptschlüssel frei.

Das bedeutet, daß man das Passwort durchaus ändern kann, ohne den Datenbereich neu verschlüsseln zu müssen, wer jedoch den Hauptschlüssel irgendwoher hat, kann ohne

Passwort auch den Datenbereich entziffern, wenn der zugehörige Container nur kopiert und nicht neu verschlüsselt wurde.

Der Datencontainer

Das ist die gängigste Arbeitsweise. Hier legt man sich eine Datei an, bestimmt deren Größe und gibt ihr einen Namen, diese kann wenige MB groß sein oder auch 32GB und mehr. Das Programm selbst führt durch einen Dialog, der u. a. auch den Hauptschlüssel individuell erstellt. Diese Datei wird als Laufwerk mit Laufwerkbuchstaben dem Betriebssystem bekannt gemacht.

Den Container öffnet man durch Eingabe des Passworts, wenn man Daten von dort lesen oder bearbeiten möchte, er verhält sich wie ein gewöhnliches Laufwerk und schließt ihn wieder, wenn man ihn nicht mehr braucht, jetzt ist er von aussen nur noch eine etwas größere Datei mit unidentifizierbarem Inhalt.

Man kann nun diesen Container fast beliebig kopieren und verschieben, wenn man ihn öffnen will, wählt man diese Datei an und vergibt den Laufwerksbuchstaben.

Kleine Datencontainer eignen sich sehr gut für E-Mails, man verschickt nur die Containerdatei und der Empfänger kennt das Passwort, um den Container und die darin befindlichen Dateien benutzen zu können.

Da Datencontainer sich wie Laufwerke verhalten, können darin auch Programme installiert werden.

Die Systemverschlüsselung

Da Betriebssysteme heute Daten vielfach auch in temporären Verzeichnissen und Dateien ablegen und danach nur noch unzuverlässig vernichten, bietet es sich an, nicht nur diese, sondern das gesamte Betriebssystem in sich zu verschlüsseln, so daß auch die temporären Dateien nicht wiederhergestellt werden können.

Truecrypt erlaubt das nachträgliche Verschlüsseln des Betriebssystems ab Windows-XP.

Der Vorgang selbst ist relativ einfach, man benötigt jedoch zwingend einen CD-Brenner. Das Programm führt in einem schrittweisen Dialog. Zuerst wird ein Passwort vergeben, mit dem man später ins Betriebssystem gelangen kann, es wird ein Hauptschlüssel ermittelt, eine CD gebrannt, die als Sicherung dient, falls der Hauptschlüssel auf der Festplatte beschädigt werden sollte, man testet hier auch das Passwort. Danach wird in einem – bisweilen mehrstündigen – Vorgang die gesamte Systempartition verschlüsselt.

Es kann vorkommen, daß Truecrypt mittendrin abbricht, einen Fehler auf der Platte meldet. Das ist ein Hinweis, daß es nicht mehr lange dauern wird, bis sich Plattenfehler mehren, man kann eine solche teilweise Verschlüsselung wieder rückgängig machen.

Hat alles geklappt, startet der Rechner wie gewohnt, fragt aber vor dem Betriebssystemstart das Passwort ab, das man auch nicht mehr mit Zusatztools ggf. umgehen kann. Ein vergessenes Passwort bedeutet das Aus. Der Passwortabfragebildschirm kann selbst gestaltet werden, also durchaus das alte MS-DOS nachbilden oder auf vermeintlich irreparable Hardwareschäden hindeuten.

Ansonsten merkt man von der Verschlüsselung kaum mehr etwas, sie läuft für den Benutzer transparent, nur ein geringer Performanceverlust, wenn man mit der Stoppuhr vergleicht.

Im Betrieb ist der Rechner nicht von ungebetenen Gästen geschützt, wer aber die Festplatte, das Notebook oder den PC klaut, kann mit den darauf befindlichen Daten nichts mehr anfangen.

Gerade bei Notebooks ist drauf zu achten, wie diese sich verhalten, wenn sie bei leerem Akku oder geschlossenem Display in den Ruhezustand gehen, ob diese präzise dort wieder starten, wo sie schlafen gingen, weil dann das System ohne Passwort zugänglich ist.

Wie wird eine Verschlüsselung geknackt?

Zunächst wird der Angreifer gängige Passwörter probieren bzw. von seinem Rechner probieren lassen, ein Wörterbuch durchspielen. Auch einige persönliche Daten des früheren Besitzers.

Führt das nicht zum Ziel, kann er noch bekannte Datenschlüssel verwenden, evtl. handelt es sich um einen nur kopierten Container.

Hat der Programmhersteller keine Hintertüren eingebaut, hilft nur noch Probieren, also alle möglichen Zeichenkombinationen der Reihe nach von einem Rechner probieren lassen. Dies ist der bekannte „Brute-Force“-Angriff.

Daher sollten Passwörter mindestens etwa 40 Zeichen lang sein, Zahlen und Sonderzeichen enthalten, damit der Angreifer selbst dann einige Monate oder auf Jahre hinaus beschäftigt ist, selbst wenn er auf vorberechnete Tabellen zurückgreifen kann.

Da der Aufwand zum Knacken unabhängig von der Größe des Datenbereiches ist, kann man eine größere Anzahl von Datencontainern als Dummys bereitstellen, die ein Angreifer nacheinander (oder mit viel Hardware parallel) zu knacken versuchen kann, während man selbst die echten Datencontainer kennt.

Die Hidden-Technik – die erste Kaskade.

Verschlüsselte Container lassen sich ineinander verschachteln, es kann Situationen geben, wo man gezwungen ist, eine Verschlüsselung zu öffnen, die Präsenz dieser Untercontainer wäre sichtbar. Professionelle Systeme und Truecrypt bieten daher eine weitere Technik an.

Der Normalanwender wird nur ein Passwort verwenden. Die Hidden-Technik benutzt zwei Passwörter. Gibt man das erste korrekt ein, öffnet sich der Container zwar, man sieht auch einige Dateien, diese sind jedoch nur Dummydateien. Nur bei der korrekten Eingabe des zweiten Passworts, öffnet sich der eigentliche Datenbereich.

Dieser zweite Datenbereich kann vorhanden sein, muß nicht, wenn er nicht angelegt wurde, man kann also ggf. dort falsche Passwörter eingeben. Änderungen am ersten Datenbereich überschreiben ohne Vorwarnung auch den zweiten, da auch das System selbst von der Existenz des zweiten keine Kenntnis hat.

Wird bei einem Brute-Force-Angriff das erste Passwort erfolgreich gefunden, findet der Angreifer auch nur den dortigen Datenbereich und kann sich jetzt überlegen, ob er nochmal mindestens denselben Aufwand treiben will, ein nur vielleicht existierendes Hidden-Volume zu finden, da er an dieser Stelle nicht feststellen kann, ob der freie Bereich im Container nun benutzt wird oder nicht.

Die Gefahren

Ein vergessenes Passwort bedeutet, daß man selbst auch nicht mehr an die Daten kommt.

Eine Systemverschüsselung benutzt den sog. MBR, den Master-Boot-Record, dort stehen u. a. auch Bootmanager für verschiedene Betriebssysteme und nicht selten auch Lizenzdateien, da der MBR beim Formatieren nicht mitformatiert wird.

Obwohl es bei mir nicht passiert ist und auch kein befragter Hersteller dazu Angaben machen konnte, kann es sein, daß Truecrypt Lizenzdateien überschreibt. Dann muß die Lizenz neu angefordert werden und die überschreibt dann Daten, die Truecrypt für den Systemstart eines verschlüsselten Betriebssystems braucht. Der funktioniert dann nicht mehr, weswegen die CD gebrannt werden muß und mit dieser gestartet werden kann. Die CD kann man sich beliebig oft kopieren.

Defragmentierungstools und Virenscanner können in seltenen Fällen Ärger machen.

Acronis darf nur von der DVD gestartet werden und es kann auch nur noch die gesamte Platte klonen. Startet man es vom Betriebssystem aus und klont die Platte, ist diese nicht lauffähig.

Möchte man die Systempartition in ihrer Größe ändern, muß sie entschlüsselt, vergrößert und neu verschlüsselt werden.

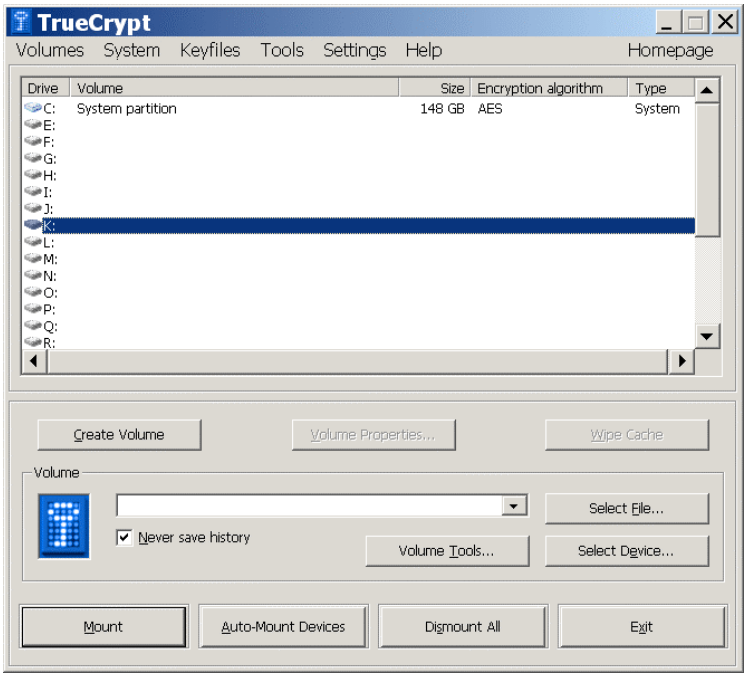
Gibt es einen Weg zurück?

Sicher, Daten zieht man einfach aus einem Container heraus, die Systemverschlüsselung macht Truecrypt auf Wunsch rückgängig, das dauert allerdings einige Zeit, da wieder alle Sektoren überschrieben werden müssen.

Das ist alles viel zu kompliziert – jetzt die Praxis!

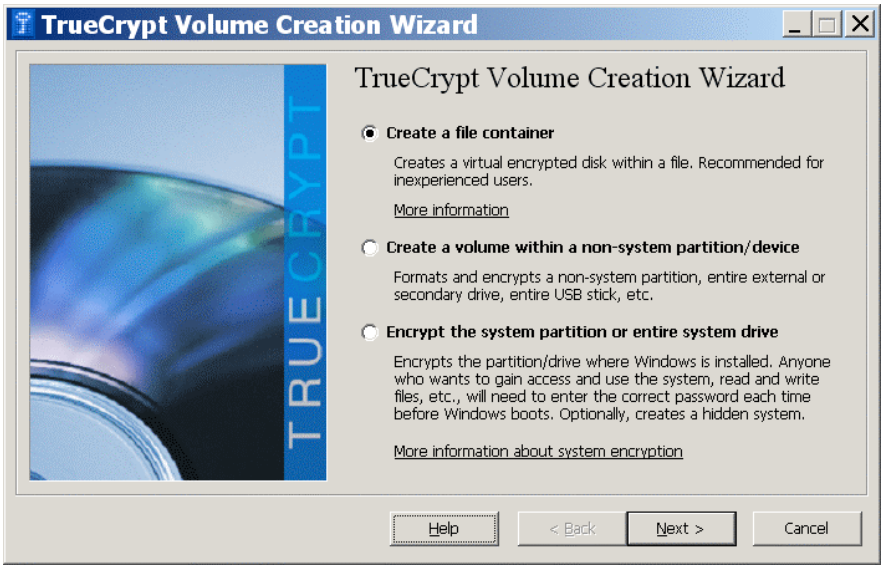
Truecrypt herunterzuladen und zu installieren, ist problemlos.

Wir starten Truecrypt, es meldet sich mit einer Dialogbox.

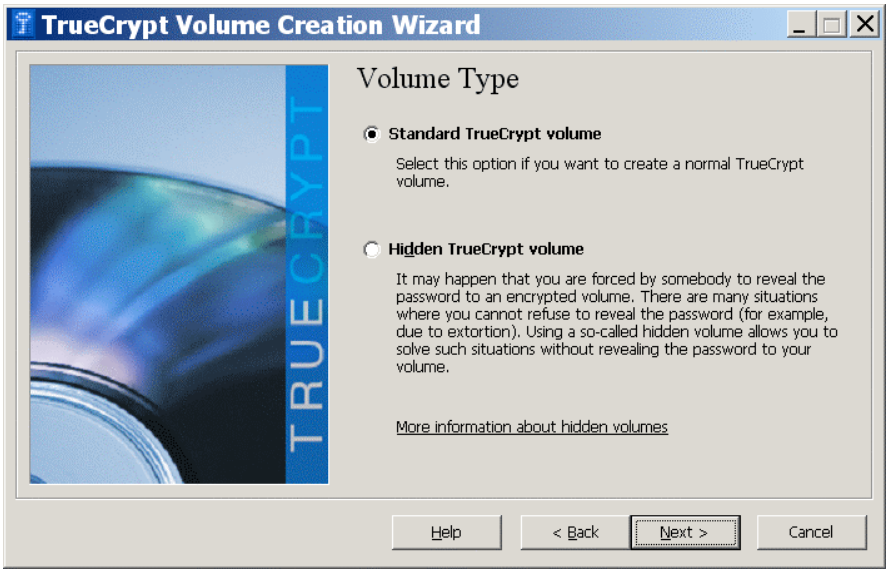


Im konkreten Fall meldet Truecrypt bereits ein System mit AES-verschüsselter Systempartition und die frei verfügbaren Laufwerksbuchstaben.

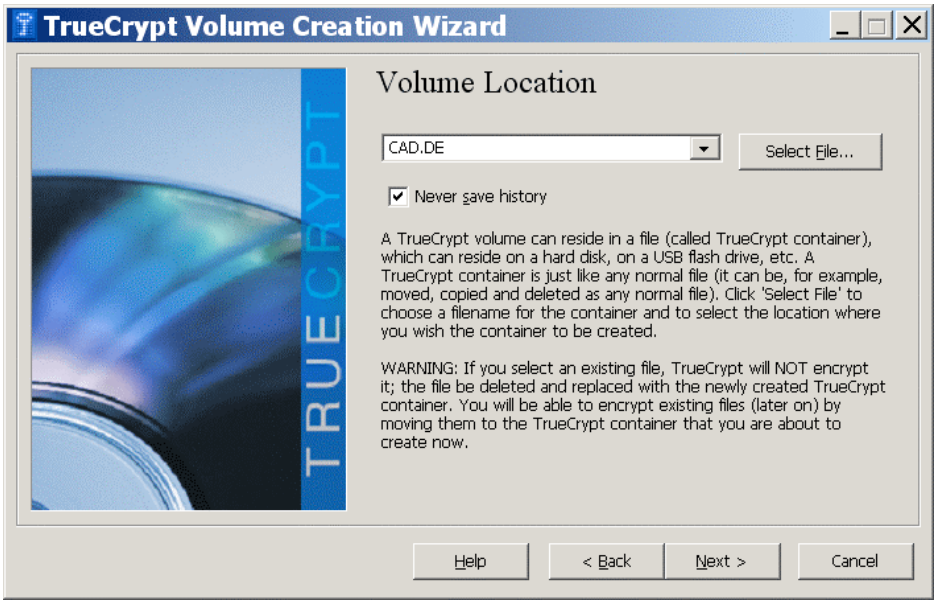
Wir wollen zuerst einen Datencontainer erstellen, wählen daher CREATE VOLUME und bekommen eine zweite Dialogbox und wählen die erste Option „Create a file container“ und dann die Schaltfläche NEXT, fortan führt uns das Programm Schritt für Schritt weiter, mit BACK kann man ggf. auch wieder rückwärts gehen.



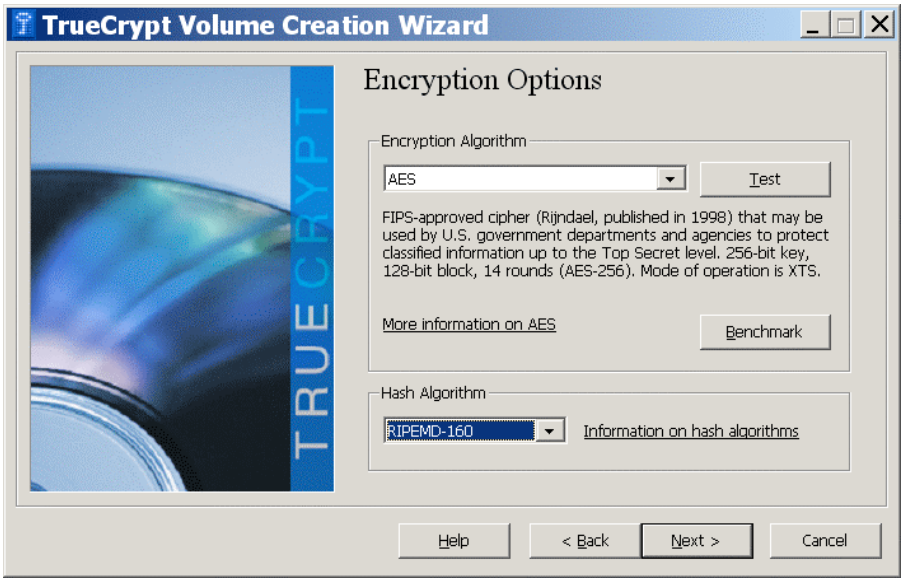
Hier soll ein einfacher Container reichen, wir bleiben bei der ersten Option FILE CONTAINER und wählen NEXT und wählen dann das Standard-Truecrypt-volume.



Nun kommt der Dateiname, diesen geben wir ein und wählen wieder NEXT. Soll die Datei an einer bestimmten Stelle erstellt werden, muß der gesamte Pfad angegeben werden, man kann die Datei jedoch problemlos später verschieben. Besser ist, über SELECT FILE zu gehen, das Verzeichnis zu wählen und dort auch den Containernamen einzutragen. Die Endung ist egal.

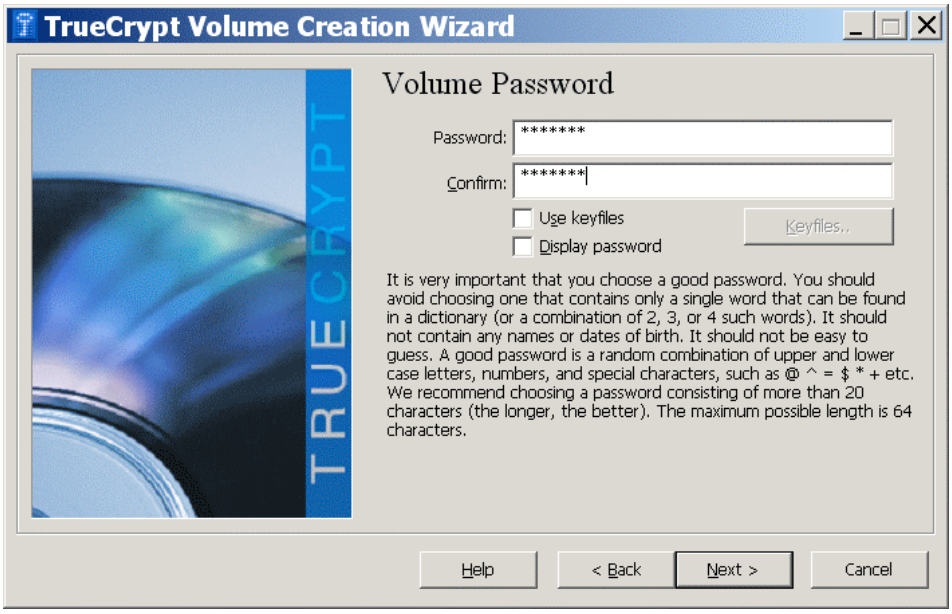


Nun können wir zwischen verschiedenen Verschlüsselungsalgorithmen wählen, im Regelfall wird AES eine gute Wahl sein, da es recht flott arbeitet.

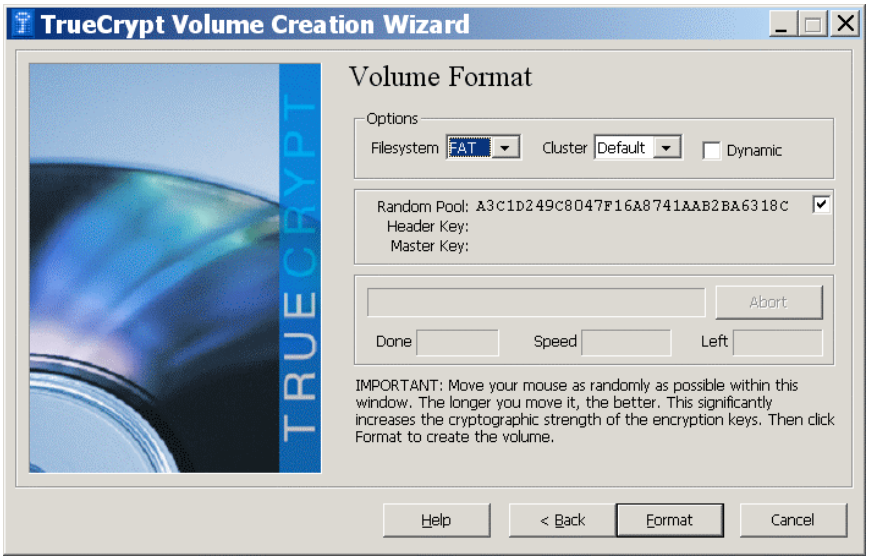


Die Größe der Datei kann jetzt festgelegt werden, ich wähle hier 500MB und danach NEXT. In der Praxis sollte man krumme Werte nehmen, da gerade Werte eher auffallen.

Nun wird das Passwort festgelegt, Ist es zu kurz (weniger als 20 Zeichen), warnt Truecrypt. Man muß es zweimal identisch eingeben, hier dürfen sich keine Fehler einschleichen, dazu kann man es sich auch im Klartext anzeigen lassen.



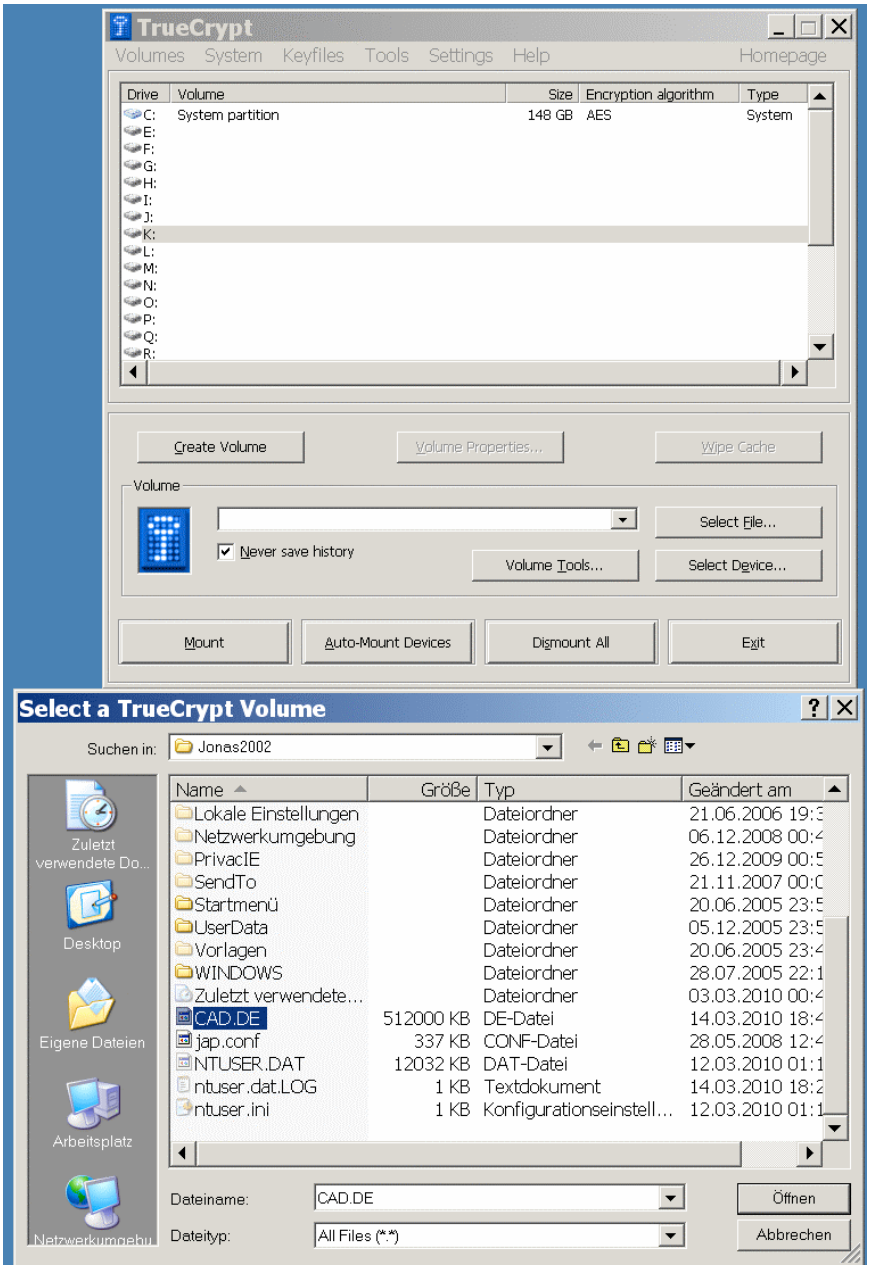
Nun wird die Datei wie ein Laufwerk formatiert, Truecrypt fordert dazu auf, die Maus zu bewegen, daraus entsteht der Schlüssel. Und danach die Schaltfläche FORMAT. Ist Truecrypt damit fertig, dauert bei 500MB nur wenige Sekunden, meldet es dies, für größere Container sollte man auf NTFS gehen.



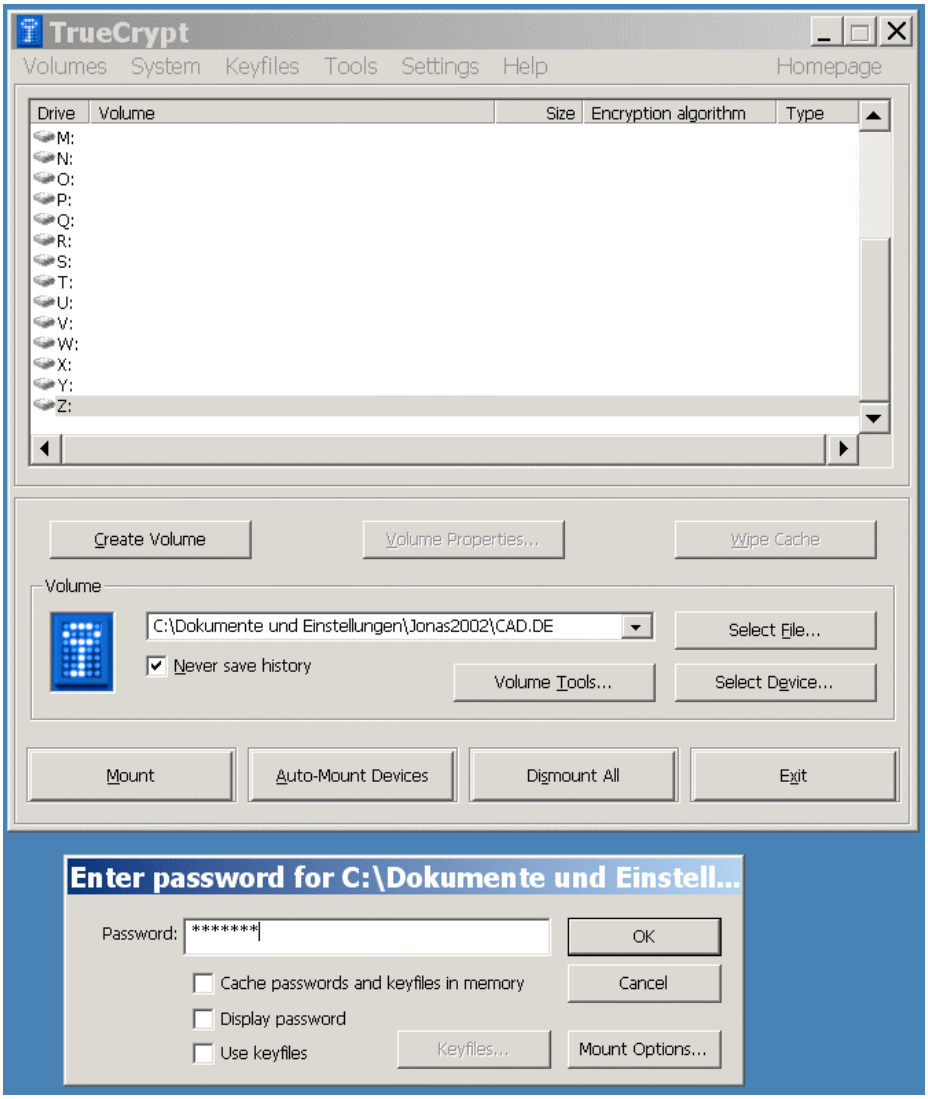
Mit NEXT kommt man wieder in die Dialogbox, die zum Anlegen des Containers auffordert, man verlässt Sie jetzt mit CANCEL.

Den Container öffnen:

Im Startdialogfeld SELECT FILE wählen und danach zum Ort der Datei navigieren und sie auswählen, hier ist es CAD.DE, geringfügig größer als die vorgegebenen 500MB, zudem sollte noch die Zeile mit dem gewünschten Laufwerksbuchstaben gewählt werden.

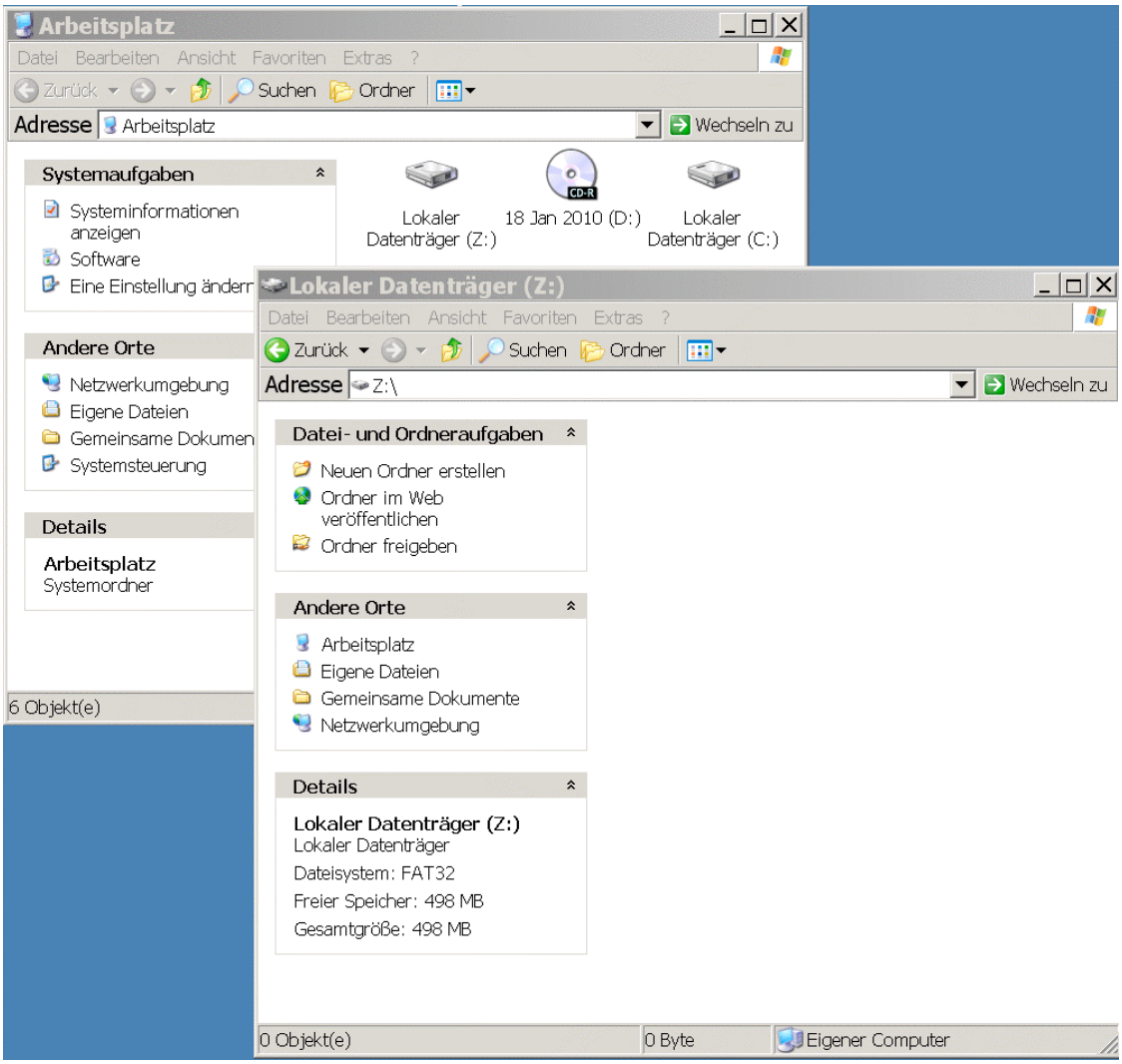


Wir wählen die Schaltfläche MOUNT, Truecrypt fragt jetzt nach dem Passwort, bei einem Hidden-Volume das zur Situation passende wählen und bestätigen. Truecrypt trägt die Datei in seine Liste der Laufwerke ein, uns steht jetzt das Laufwerk Z mit 500MB Größe zur Verfügung, das man mit einem Doppelklick auf die Zeile in der Truecrypt-Tabelle auch gleich öffnen kann.



Truecrypt selbst kann jetzt in die Taskleiste miniminert werden.

Brauchen wir das Laufwerk nicht mehr, schließen wir es einfach mit DISMOUNT.



Prototyping mit Truecrypt und Solidcam

Solidcam stellte lange Zeit keine Projektverwaltung bereit, es gab nur ein Arbeitsverzeichnis, das man entweder ständig ändern musste oder alles landete in diesem immer umfangreicher werdenden Verzeichnis. Ebenso war es wegen der Dateibezüge nicht mehr einfach, ein programmiertes Teil, das mehrere Aufspannungen hatte, zu kopieren, um mit wenigen Änderungen ein ähnliches Teil zu bearbeiten, ohne es komplett neu programmieren zu müssen.

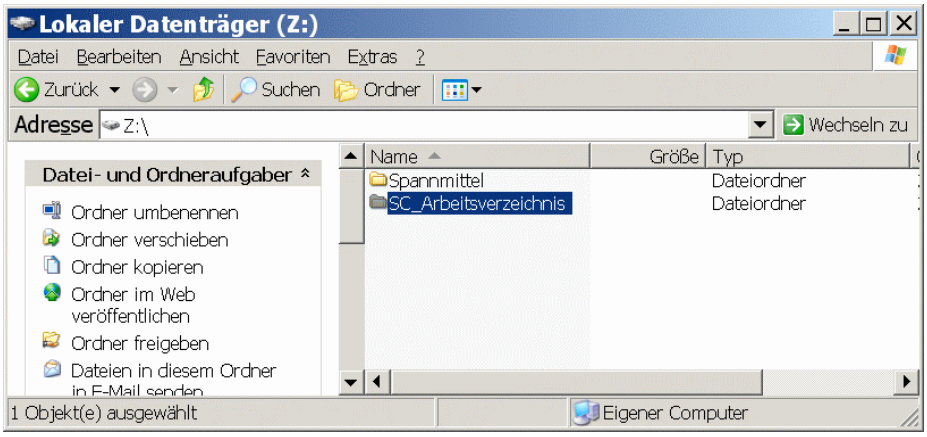
Das von Truecrypt bereitgestellte Laufwerkssystem beseitigt diese Probleme und erlaubt zudem, viele der anfänglichen Routinearbeiten mit in dieses Prototypcontainer zu verlagern.

Wie geht man vor?

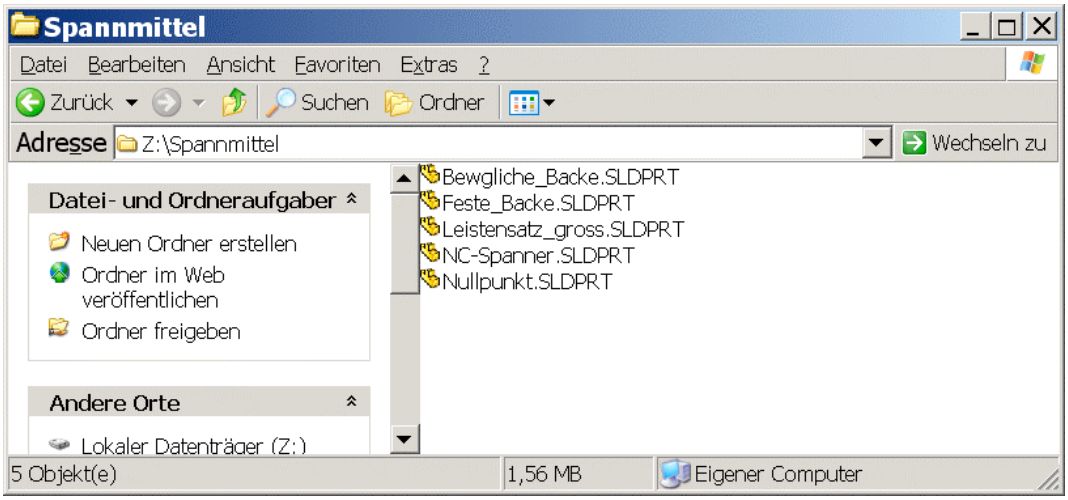
Zuerst erstellt man einen Container, er muß eine Größe haben, die man für seine CAM-Projekte braucht mit Reserve, da hier die Verschlüsselung nur ein angenehmer Nebeneffekt ist, wählt man ein sehr kurzes Passwort, kann aus nur einem Buchstaben bestehen, ich habe für das Beispiel 100MB benutzt.

Dieser Container wird als Laufwerk gemountet, hier kommt es darauf an, daß man fortan immer denselben Laufwerksbuchstaben benutzt, ich verwende hier wieder Z.

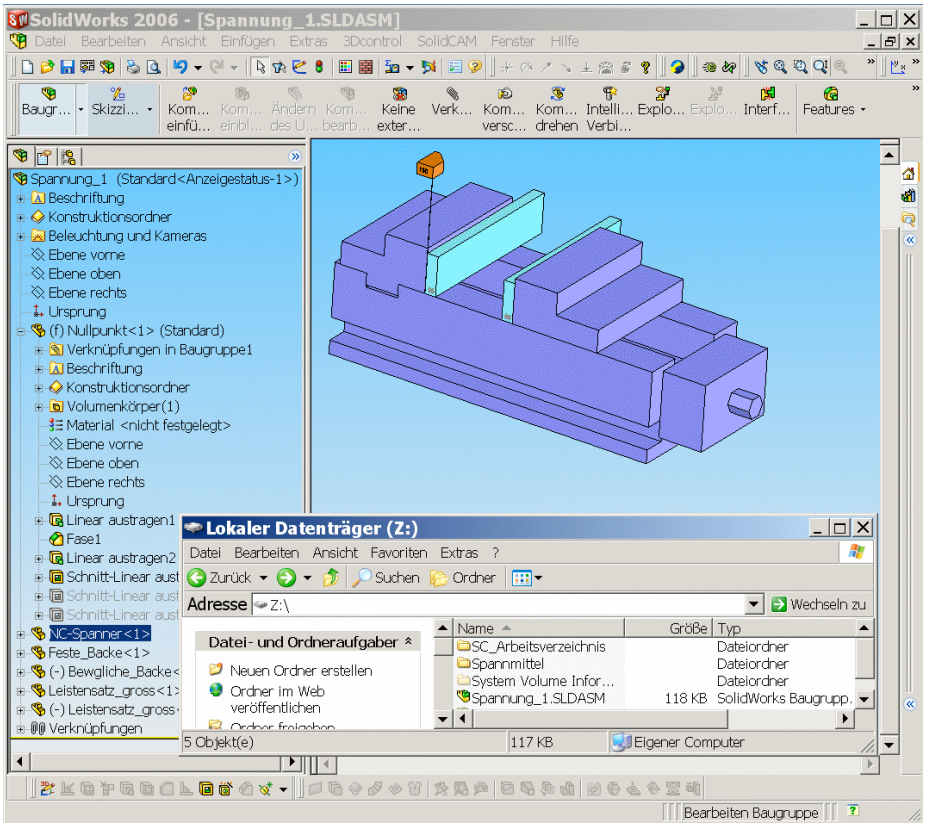
In diesem Laufwerk erstelle ich mir Ordner, hier sind es die Spannmittel und das Solidcam-Arbeitsverzeichnis. Solidcam kopiert sich alle Daten in sein Arbeitsverzeichnis und arbeitet selbst nur auf diesen Kopien, synchronisiert ggf. mit den Ursprungsdateien, auf denen man selbst die Geometrien und Skizzen erstellen sollte.



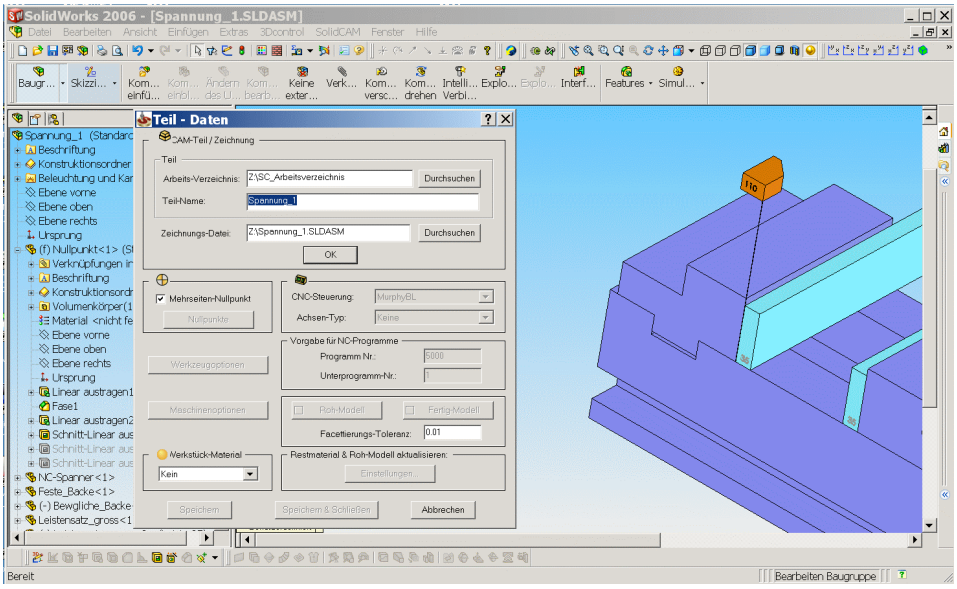
Spannmittel sollte man in den Container legen, referenziert man sie extern, fehlen sie, wenn ein Projekt ggf. doch einmal auf einem anderen Rechner bearbeitet werden muß.



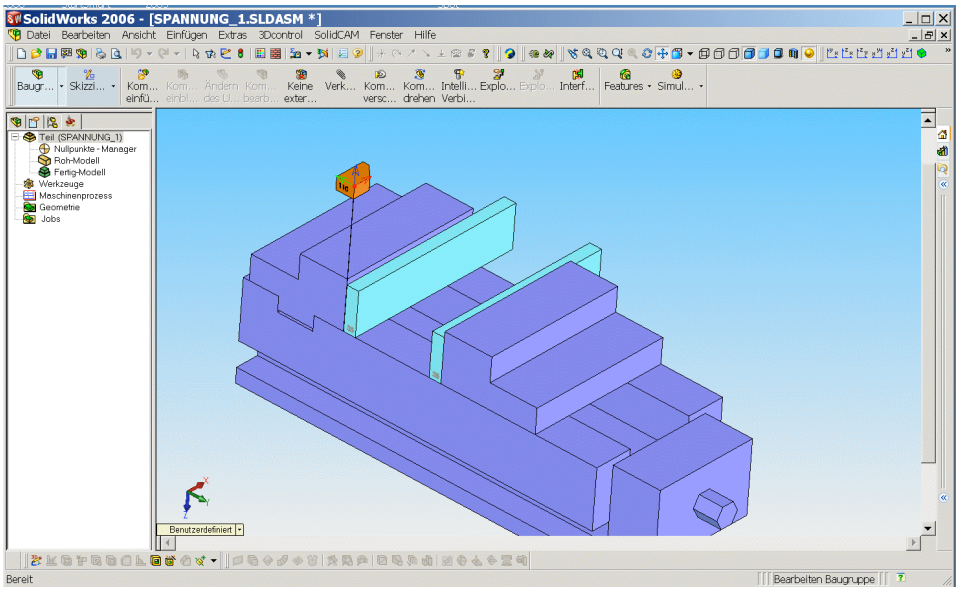
Im Wurzelverzeichnis baut man sich jetzt die gängige Spannsituation auf, macht sie mit Konfigs flexibel, nur das Werkstück lässt man weg. Der orangfarbene Nullpunktklotz sollte das einzige fixierte Teil sein.



In den Optionen von Solidcam trägt man nun als Arbeitsverzeichnis den Ordner ein, den man als solches im Container erstellt hat, man startet Solidcam, durchläuft den Teil-Daten-Dialog und auch den Nullpunktdialog. Roh- und Fertigteil fehlen.

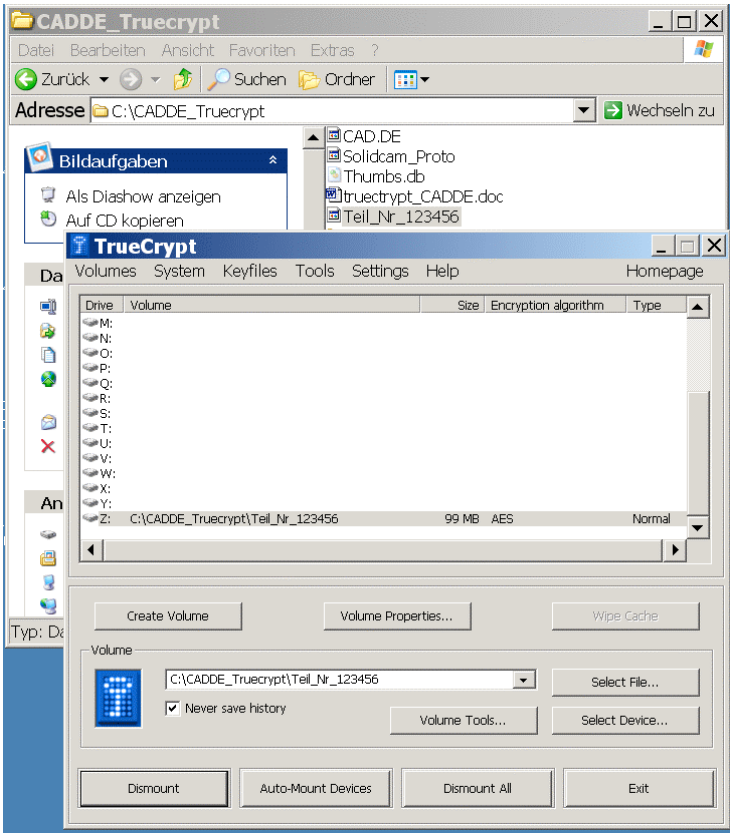


Danach sind wir wie gewohnt in der Programmierumgebung

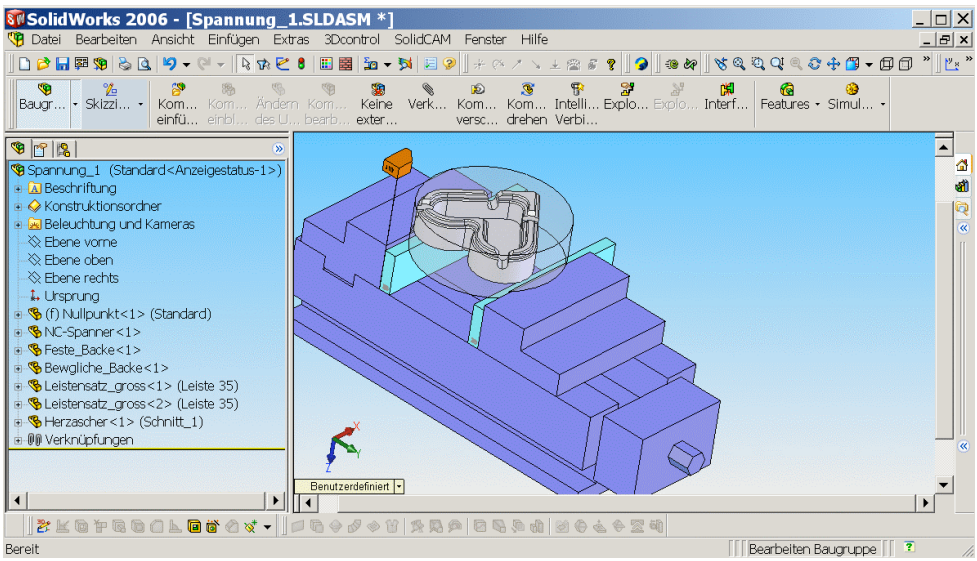


Nachdem die Ausgangssituation hergestellt ist, verlassen wir Solidcam und Solidworks, dismounten auch den Container. Damit ist der Prototypencontainer fertig.

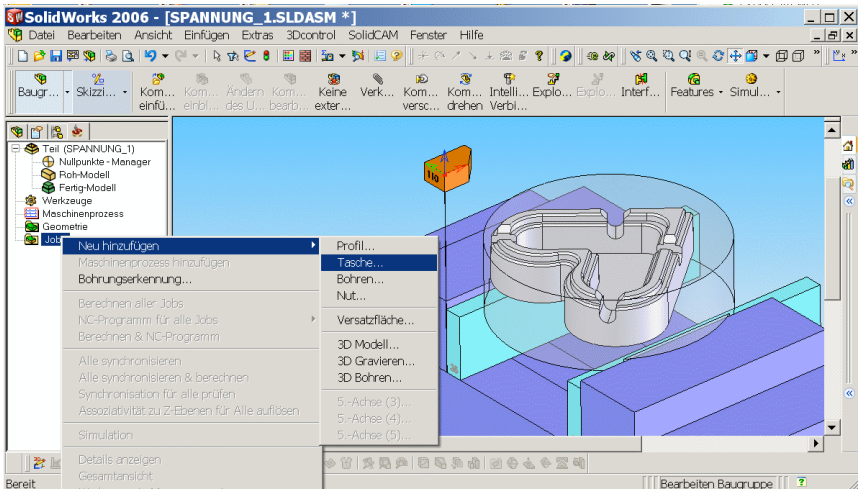
Diesen Container kopieren wir jetzt wie eine Datei mit KOPIEREN und EINFÜGEN, benennen die Kopie um, normalerweise wird es die Teilenummer sein, mounten diesen neuen Container wieder mit demselben Laufwerksbuchstaben und Passwort.



Im Zusammenbau im Wurzelverzeichnis fügen wir nun das Werkstück hinzu und speichern ab.



Danach Solidcam starten, wählen auch dort das bereits angelegte Teil aus dem Drop-Down-Menue, auch Solidcam bemerkt diesen Austausch nur insofern, daß eine Synchronisation nötig ist, man wählt Roh- und Fertigteil und kann sofort mit dem Programmieren beginnen.



Nach Abschluß der Arbeit oder auch bei Unterbrechungen wird der Container geschlossen, ist fortan nur eine einzelne Datei.

Mit dieser Technik verfügt auch das alte (und neue) Solidcam über ein sehr elegantes Prototyping, bei dem auch jedes vorhandene, programmierte Teil problemlos vollständig mit allen Bezügen kopiert werden kann, es spielt auch keine Rolle mehr, wo sich die Daten befinden. Solidcam und Solidworks sehen immer nur das Laufwerk mit Inhalt.

Für die Praxis bedeutet es, einen Vorlagencontainer zu kopieren und umzubenennen, mit dem einmal (für die Bezüge) festgelegten Laufwerksnamen zu mounten und darin zu arbeiten.

Damit soll der kurze Ausflug in das weite Feld der Verschlüsselungstechnik wieder beendet werden. Zieht man die Entwicklungen der jüngeren Vergangenheit in Betracht, erscheint es ratsam, sich rechtzeitig damit zu beschäftigen.