



PrimalCrypt

Benutzerhandbuch

PrimalCrypt Version 2.0

ApteryX Software Research
Wollerweg 18, D-70329 Stuttgart

Copyright © 2006

Inhaltsverzeichnis

1. Einführung	4
1.1 Verschlüsselungsverfahren	4
1.2 Passwörter und Schlüssel	5
1.3 Schlüsselzertifikate	7
2. Laufwerke und Images	8
2.1 Neue Images erstellen	9
2.1.1 ISO CD-Images	10
2.1.2 Image-Dateien	10
2.1.3 Laufwerkseigenschaften	11
2.1.4 Passwortschutz	13
2.1.5 Schlüsselschutz	14
2.2 Portable Automount Images	16
2.3 Laufwerke verwalten	18
2.4 Laufwerksverwaltung	23
3. Dateiverschlüsselung	26
3.1 DropCrypt	26
3.2 Dateien verschlüsseln	27
3.3 Dateien entschlüsseln	29
4. Passwortlisten	31
4.1 Neue Listen erstellen	31
4.2 Einträge hinzufügen und bearbeiten	32
4.3 Passwortlisten öffnen	34
5. Schlüsselverwaltung	38
5.1 Zweitschlüssel für ein Image erstellen	38
5.2 Schlüssel duplizieren oder reparieren	41
5.3 Zertifikate übertragen oder reparieren	43
5.4 Zertifikate löschen	45
6. Sicheres Löschen	46
7. Steganografie	47
7.1 Dateien verstecken	48
7.2 Versteckte Dateien sichtbar machen	49

8. Einstellungen	50
8.1 Zugangspasswort	50
8.2 Passwortlisten	50
8.3 Laufwerke	51
8.4 DropCrypt Einstellungen	52
 9. Taskleistensymbol	 54
 10. Updates	 55
 11. Installation, Deinstallation und Registrierung	 57
11.1 Registrierung	57
11.2 Lizenzierung	59
11.3 Installation und Deinstallation	59

1 Einführung

Datensicherheit wird für viele Arbeitsbereiche immer wichtiger. Dabei geht es nicht nur um die physikalische Sicherheit der Daten – also den Verlust durch versehentliches Löschen oder den Defekt des Datenträgers – sondern auch um die Geheimhaltung sensibler Daten, wie z.B. Bauplänen, Umsatzzahlen oder Passwörtern bei einem Verlust des Datenträgers durch Diebstahl.

Immer öfter werden solche sensiblen Daten auf Notebooks, externen portablen Festplatten oder USB-Memorysticks abgelegt. Der Verlust des Datenträgers wiegt hierbei zumeist nicht so sehr, wie die darauf befindlichen Daten und deren Schutz vor der Einsicht fremder Personen.

PrimalCrypt kann Ihnen hierbei helfen, indem es durch moderne Verschlüsselungsverfahren, die für Sie wichtigen Dateien für Dritte unleserlich macht. Dazu bedient sich PrimalCrypt verschiedener Verfahren, die je nach Ihren Bedürfnissen genutzt werden können.

Um den Umgang mit dem Ver- und Entschlüsseln aller im alltäglichen Arbeitsprozess anfallender Daten so einfach wie möglich zu gestalten, bietet Ihnen PrimalCrypt die Möglichkeit, Dateien und Programme auf sogenannten Image-Dateien zu speichern.

Diese Image-Dateien können wie eine normale Festplatte genutzt werden. D.h. Sie müssen keine komplizierten, zusätzlichen Arbeitsschritte zum sicheren der Dateien ausführen, sondern Sie speichern Ihre Excel-Tabellen oder CAD-Zeichnungen wie gewohnt auf einen Datenträger wie z.B. der Festplatte.

Wenn Sie nur einzelne Dateien verschlüsseln möchten, können Sie dies durch einfaches Drag and Drop (ziehen der Dateien auf ein Symbol auf Ihrem Windows Desktop) erledigen.

Um Passwörter, Bank-PINs und Notizen kümmert sich der Passwortlistenmanager, mit dem Sie - wie bei einem Schlüsselkasten - alle Ihre Kennwörter mit nur einem Schlüssel (in diesem Fall ein Passwort) einschließen und somit vor dem Zugriff anderer Personen schützen können.

Mit dem Steganografie-Modul können Sie Daten in einem Bild verstecken und mit den „Shredder“ löschen Sie Dateien sicher und unwiederbringlich von Ihrer Festplatte.

1.1 Verschlüsselungsverfahren

Um Texte oder andere, wie auch immer geartete Daten unleserlich zu machen, wurden in der Mathematik die verschiedensten Verfahren entwickelt, die je nach Stand der Rechnertechnik als sicher erachtet wurden. Viele dieser Verschlüsselungsverfahren galten lange Zeit als unüberwindbar, also nicht für solche Personen zu entschlüsseln, die keinen oder einen falschen Schlüssel besaßen. Die moderne Rechnertechnik hat es aber immer durch rapide Geschwindigkeitssteigerung geschafft, diese Verschlüsselungen durch reine, sogenannte Brute-Force Methoden zu knacken. Hierbei werden alle möglichen Schlüssel mit dem Computer durch einfaches „ausprobieren“ oder durch geeignete mathematische Verfahren (sog. Algorithmen) in relativ kurzer Zeit geprüft und der verschlüsselte Text somit wieder lesbar gemacht. Mit dieser Methode kann ein Rechner, für den ein Mensch im ungeeignetsten Fall mehrerer Millionen Jahre benötigen würden, ein Verschlüsselungsverfahren in wenigen Stunden oder sogar Minuten zu Fall bringen.

Auf der anderen Seite werden jedoch ungeheure Anstrengungen zur Schaffung neuer, sicherer Verfahren gemacht. Diese ermöglichen es, auch bei der z.Zt. absehbaren

Steigerung der Rechengeschwindigkeit zukünftiger Computer, die Sicherheit der Daten auf mehrere Jahrzehnte zu garantieren.

PrimalCrypt nutzt mehrere verschiedene Verfahren, die je nach Bedarf eingesetzt werden können.

Für die Verschlüsselung der Image-Dateien kann zwischen dem AES (Rijndael) und dem TwoFish-Algorithmus gewählt werden, bei der Einzeldateiverschlüsselung wird immer das Blowfish-Verfahren eingesetzt wird.

Der Advanced Encryption Standard (AES) ist das zur Zeit am meisten favorisierte Verschlüsselungsverfahren, welches von den U.S Amerikanischen Behörden zum Schutz von sensiblen und als „Top Secret“ eingestuften Informationen eingesetzt wird. Im Oktober 2000 wurde das Rijndael-Verschlüsselungsverfahren zum Advanced Encryption Standard (erweiterter Verschlüsselungsstandard) ausgewählt und gilt trotz einigen theoretisch möglichen Angriffsverfahren für die nächsten 30 bis 40 Jahre als sicher.

In PrimalCrypt können für AES Schlüssellängen von 128, 192 und 256 Bit gewählt werden, je nachdem, ob die Geschwindigkeit oder die Sicherheit der Verschlüsselung für Sie wichtig sind.

TwoFish - ein mit 128 Bit Schlüssellänge arbeitender Algorithmus - wurde von Bruce Schneier entwickelt und war einer der fünf Finalisten im Auswahlverfahren zum Advanced Encryption Standard. Auch TwoFish gilt als sehr sicher, ist aber etwas langsamer als AES/Rijndael.

Der Verschlüsselungsalgorithmus Blowfish wurde ebenfalls von Bruce Schneier entwickelt und gilt als einer der schnellsten Blockverschlüsseler auf 32-Bit Prozessoren.

Trotz seines Alters – Blowfish wurde 1993 entworfen und im April 1994 erstmals publiziert – wurden bis heute keine besonderen Schwachstellen durch verschiedene Kryptoanalysen bekannt. PrimalCrypt verwendet eine Schlüssellänge von 448 Bit, die für Blowfish als extrem sicher erachtet wird.

1.2 Passwörter und Schlüssel

Für den Zugriff auf verschlüsselte Image-Dateien können in PrimalCrypt entweder das klassische Passwort, Schlüsseldateien oder eine Kombination aus beidem genutzt werden.

Passwörter haben den Vorteil der „Unverlierbarkeit“ (sofern Sie Ihre Kennwörter nicht auf einem Blatt Papier vermerkt haben und dieses in der Kantine liegen lassen). Sie können Passwörter ohne jegliche weitere Hilfsmittel zum entschlüsseln Ihrer Image-Dateien eingeben. Jedoch ist ein zu kurzes oder ein schlecht gewähltes Passwort meist selbst von einem Laien in kürzester Zeit auffindbar. Daher sollten Sie Ihre Zugangspasswörter möglichst lang (16 Zeichen oder mehr) gemischt aus Buchstaben, Zahlen und Sonderzeichen und möglichst nicht aus der Kombination eines Namens und eines Geburtsdatums (z.B. Erwin1954) wählen. Akronyme (aus Anfangsbuchstaben mehrerer Wörter neu zusammengesetzte Wörter) können gute Passwörter ergeben.

Z.B. kann aus dem Satz :

**Fest gemauert in der Erde
Steht die Form, aus Lehm gebrannt
(Schiller +1805)**

das Passwort **FgidESdFaLg(S+1805)** geformt werden, was allen Anforderungen genügt.

Als zweite, wesentlich komfortabler nutzbare Alternative können Schlüsseldateien zum freigeben der Daten eines Images dienen.

Schlüsseldateien (oder Token) besitzen die Funktion eines Passwortes und können als einzelne Dateien gespeichert, oder aber an eine bestehende Datei angehängt werden.

Diese Dateien beinhalten einen auf Zufallsbasis generierten, langen Schlüssel und werden durch sogenannte Zertifikate auf „Echtheit“ geprüft.

Eine Schlüsseldatei kann z.B. auf einem USB-Memorystick abgelegt werden. Beim einstecken des Memorysticks an einen USB-Anschluss Ihres Computers erkennt PrimalCrypt die Schlüsseldaten, vergleicht diese mit den vorhandenen Zertifikaten, sucht die passende Image-Datei und mountet diese wie eine Festplatte auf Ihrem Rechner.

Danach kann der Schlüsselträger (der USB-Stick) wieder herausgezogen werden.

Dieses Prinzip lehnt sich also stark an die im echten Leben benutzen Schlüssel zum öffnen eines Türschlosses an.

Wie bei eben einem normalen Haustürschlüssel auch, besteht aber die Gefahr, dass dieser verloren geht. Daher kann ein PrimalCrypt-Schlüssel zusätzlich mit einem Passwort gesichert werden, das beim Stecken des Schlüssels abgefragt wird.

Eine Schlüsseldatei kann nur auf einem, von Windows automatisch erkannten Trägerlaufwerk gespeichert werden. Dazu zählen die bereits erwähnten USB-Sticks, aber auch externe per USB-Anschluss verbundene Festplatten.

Andere Datenträger wie z.B. SD Speicher Karten oder Zip-Disketten werden zumeist nicht automatisch erkannt und sind deshalb ungeeignet.

Eine Schlüsseldatei kann wie gesagt auch an eine bereits existierende Datei angehängt werden. Hierbei muss jedoch darauf geachtet werden, dass diese Dateien möglichst keine normalen, lesbaren Texte beinhalten und danach nicht mehr geändert werden dürfen. Eine Bild-Datei eignet sich sehr gut, da die Daten zum Einen von einem Menschen nicht als lesbar betrachtet werden können (sondern nur deren Ausprägung als visuelles Bild) - also ein angehängter Schlüssel nicht ohne weitere Hilfsmittel erkannt wird - zum Anderen werden Bilder nicht oder nur selten geändert, womit ein versehentliches Überschreiben der Schlüsseldaten fast ausgeschlossen werden kann.

Schlüsseldateien sind nicht übertragbar. Beim Erstellen eines Schlüssels wird dieser auf sein Trägerlaufwerk festgelegt (gebündelt). Hierdurch wird ein unbemerktes Kopieren der Schlüsseldatei verhindert, da die kopierten Schlüsseldaten auf einem anderen Trägerlaufwerk nicht mehr von einem Zertifikat als echt erkannt werden. Schlüssel können aber mit Hilfe eines Hauptschlüsselzertifikats neu erstellt oder verteilt werden werden (siehe Abschnitt 1.3).

1.3 Schlüsselzertifikate

Wenn in PrimalCrypt eine Image-Datei mit einem Schlüssel erstellt wird, so wird im Programmverzeichnis ein passendes Zertifikat abgelegt. Dieses Zertifikat ist (wie auch ein Schlüssel) auf sein Trägerlaufwerk gebündelt und somit vor Diebstahl geschützt.

Schlüssel beinhaltet eine per Zufall erzeugte Zeichenkette zum öffnen der Image-Datei. Dieses Zufallspasswort kann nicht mehr rekonstruiert werden. Der Verlust einer Schlüsseldatei oder eines Zertifikats (durch versehentliches oder absichtliches löschen) würde also dazu führen, dass das Image nicht mehr geöffnet werden kann. Ein kompletter Datenverlust wäre also die Folge.

Um dies zu verhindern, erstellt PrimalCrypt zusätzlich ein sogenanntes Hauptschlüsselzertifikat (HSZ). Dieses ist sozusagen Ihr Sicherheitsnetz. Das HSZ beinhaltet alle Informationen, um daraus ein normales Zertifikat oder einen passenden Schlüssel neu zu erstellen. Im Gegensatz zu einem Schlüsselzertifikat - welches mit einem Schlüssel verglichen und dann entschlüsselt wird – werden Hauptschlüsselzertifikate durch ein Passwort geschützt. Das HSZ sollte immer auf einem Wechsel- und weg schließbaren Datenträger wie z.B. einer Diskette oder einer CD aufbewahrt werden. Nur so kann bei einem Festplatten defekt verhindert werden, dass sowohl Zertifikat (bzw. Schlüssel) und Hauptschlüsselzertifikat verloren gehen.

Da Image-Dateien (mit einer Ausnahme, siehe Abschnitt 2.2) beliebig von einer Festplatte auf eine andere kopiert werden können, besteht für diese (bei regelmäßiger Datensicherung) soweit keine Gefahr. Durch das Fehlen des passenden Zertifikats wären aber dennoch alle Daten verloren.



Bewahren Sie Ihre Hauptschlüsselzertifikate immer an einem sicheren Ort, getrennt von Ihrem Arbeitsrechners auf.

Die Möglichkeiten mittels eines Hauptschlüsselzertifikats einen Schlüssel oder ein Zertifikat zu duplizieren, werden im Kapitel 5 näher erläutert.

2 Laufwerke und Images

Für das Speichern von Daten werden in PrimalCrypt sogenannte Image-Dateien eingesetzt. Eine Image-Datei ist hierbei zunächst im klassischen Sinne nichts anderes wie ein Textdokument, eine Bild-Datei oder ein Programm. Wie jede andere Datei wird ein Image auf der Festplatte oder einem anderen Datenträger gespeichert. Eine Image-Datei kann also auch kopiert, verschoben, umbenannt oder in den Papierkorb gelegt (und dort später gelöscht) werden.

Image-Dateien besitzen standardgemäß die Dateiergung .img um sie als Image zu kennzeichnen. Grundsätzlich kann aber auch jede andere Dateiergung (.bmp, .doc oder aber auch .xyz) gewählt werden. Des weiteren können CD-Images die im ISO Standard gespeichert wurden von PrimalCrypt genutzt werden. ISO-Images besitzen die Endung .iso, was jedoch ebenfalls nicht zwingend ist.

Der interne Aufbau einer Image-Datei spiegelt in etwa die Organisation von Datenblöcken auf einer Festplatte (bzw. den Daten-Tracks einer CD bei einem ISO-Image) wieder.

Ein virtueller Festplattentreiber (ein Programm zum steuern eines Gerätes) bindet diese Image-Dateien wie eine gewöhnliche Festplatte in das Betriebssystem ein. Dieses einbinden (mounten) geschieht für den Anwender und auch Windows völlig transparent. D.h. zwischen einer „echten“ Festplatte (oder einer CD) und einem gemounteten Image kann kein Unterschied festgestellt werden. Wie jede Diskette, Festplatte oder CD erhält auch das gemountete Image einen Laufwerksbuchstaben, unter dem es angesprochen werden kann.



Abbildung 1. Gemountete Image-Datei als Laufwerk H:

Ein Image kann wie eine extern angebundene Festplatte wieder entfernt werden, wenn sie nicht mehr benötigt wird. Dieses entfernen (unmount) schließt die Image-Datei und versteckt Ihre (verschlüsselten) Daten in sich.

Image-Dateien sind also eine Art Container, die durch ihren inneren Aufbau wie ein physikalisches (Festplatten-) Laufwerk betrachtet werden und somit andere Dateien in ihnen gespeichert werden können.

PrimalCrypt verwendet als virtuellen Festplattentreiber den von Bo Brantén entwickelten und unter der GNU General Public License (GPL) frei erhältlichen Open Source Treiber FileDisk.sys (bzw. den, unter anderem von Stefan Scherrer um die Verschlüsselungsalgorithmen erweiterten CrossCrypt Treiber). Weitere Informationen zu Filedisk und dessen Weiterentwicklung finden Sie im Internet unter <http://www.acc.umu.se/~bosse/> bzw. für CrossCrypt unter <http://www.scherrer.cc/crypt/>.

Die GNU Public License finden Sie im Installationsverzeichnis von PrimalCrypt oder unter <http://www.gnu.org/copyleft/gpl.html>.

Das ursprünglich für die Bedienung benötigte DOS-Programm FileDisk.exe wurde von uns um einige Funktionen erweitert und als Dynamic Link Library (DLL) neu programmiert.

Dieser Quellcode ist - ebenfalls unter der GPL veröffentlicht - unter <http://www.apteryx.de> frei erhältlich.

2.1 Neue Images erstellen

Um eine neue Image-Datei mit PrimalCrypt zu erstellen, wählen Sie entweder im Hauptmenü unter „**Laufwerke**“ den Menüpunkt „**Laufwerk neu erstellen...**“, oder klicken Sie direkt in der links stehenden Menüleiste unter der Kategorie „**Laufwerke**“ auf „**Neu erstellen**“.



Abbildung 2. Laufwerke : Neu erstellen

Für die Erstellung eines neuen Laufwerk-Images bietet PrimalCrypt zwei Möglichkeiten der Parametereingabe.

Der Erstellungsassistent leitet Sie Schritt für Schritt durch die gesamte Prozedur, während Sie in der Profi-Ansicht alle benötigten Eingabefelder auf einer Seite im Gesamtüberblick haben.

Im Folgenden werden Sie in die Erstellung einer Image-Datei in der Profi-Ansicht eingeführt. Die benötigten Eingabeparameter im Erstellungsassistenten sind jedoch größtenteils identisch und intuitiv nachvollziehbar, so dass hier nicht näher auf die Unterschiede eingegangen werden soll.

Sie können entweder ein Festplatten-Image erstellen, auf dem Sie wie auf einer normalen Festplatte Dateien und Programme speichern können, oder aber eine oft benötigte Daten-CD als Image sichern.

2.1.1 ISO CD-Images

PrimalCrypt kann neben den „normalen“ Image-Dateien auch Images im so genannte ISO 9660 Format verwalten und erstellen.

Diese Norm beschreibt ein hierarchisches Dateisystem mit Verzeichnissen und Unterverzeichnissen für CD-ROMs.



Es können keine Audio-CDs als Image gespeichert werden, da sich die Repräsentation der Daten hier grundsätzlich von der einer reinen Computerdaten-CD im ISO 9660 Format unterscheidet.

CD-Images bieten den Vorteil, dass sich nicht immer die Original CD im Laufwerk befinden muss und Sie auch mehrere solcher Images gleichzeitig gemountet haben können.

Verlangt z.B. ein Programm zur Routenplanung immer seine Daten-CD mit dem Kartenmaterial, so brauchen Sie diese nicht jedes mal einzulegen, sondern erstellen ein ISO-Image dieser CD und mounten Sie mit PrimalCrypt. Ihr Routenplaner erkennt den Unterschied nicht.

Wenn Sie eine nicht kopiergeschützte Daten CD-ROM als Image-Datei auf Ihre Festplatte sichern möchten, klicken Sie das Auswahlfeld „**ISO-Image erstellen**“ an. Es werden dann einige, nicht benötigte Optionen ausgeblendet.

Wählen Sie nun bitte noch das Quell-Laufwerk, von dem die Daten gelesen werden sollen, in der entsprechenden Auswahlliste aus. Die sonst noch benötigten Angaben sind mit denen der Festplatten-Images weitgehend identisch (s. Kapitel 2.1.2).

2.1.2 Image-Dateien

Für jede Art von Image-Datei müssen Sie den Speicherort und den Dateinamen angeben. Geben Sie hierzu die vollständige Pfadangabe (z.B. C:\MeinImage.img) in das Eingabefeld ein, oder klicken Sie auf den Schalter „**Auswählen...**“ um die Datei mit dem Speichern-Dialog auszuwählen.

Abbildung 3. Festlegen der Image-Datei

Wenn Sie ein Portables Automount-Image (PAI) erstellen möchten, markieren Sie zusätzlich das entsprechende Auswahlfeld. Beachten Sie bitte, dass ein PAI nur auf automatisch erkannten Laufwerken wie z.B. USB-Memorysticks abgelegt und nicht nachträglich dorthin kopiert werden kann. PAIs werden auch nur im Hauptverzeichnis des Trägerlaufwerks erkannt. Eine nähere Beschreibung zu Portablen Automount-Images finden Sie in 2.2.

2.1.3 Laufwerkseigenschaften

Im nächsten Schritt müssen Sie die Größe des Images (entfällt bei einem ISO-Image) und den Typ der Verschlüsselung wählen. Geben Sie die Image-Größe entweder in Kilobyte (KB), Megabyte (MB) oder Gigabyte (GB) ein. Die genannten Einheiten können Sie in der Auswahlliste, rechts neben dem Eingabefeld für die Größenangabe festlegen.

Für die Verschlüsselung können sie zwischen AES (Rijndael) mit verschiedenen Schlüssellängen und TwoFish wählen. Falls Sie nur eine einfache Image-Datei benötigen, um z.B. Bilder oder Textdokumente zu speichern, können Sie hier auch angeben, dass keine Verschlüsselung erfolgen soll.

Um die Arbeitsgeschwindigkeit der verschiedenen Algorithmen zu testen, klicken Sie auf den Schalter „**Geschwindigkeitstest...**“. In dem sich öffnenden Dialogfenster kann geprüft werden, wie schnell die Verschlüsselungsverfahren auf Ihrem Rechner ausgeführt werden können. Klicken Sie hierzu auf den Schalter „**Testen**“. Die Testreihe wird mit 1 Megabyte großen Datenblöcken durchgeführt. Die Ver- und Entschlüsselung findet hierbei im Hauptspeicher (RAM) des Rechners statt und kann je nach Auslastung des Prozessors (CPU) zu leicht verschiedenen Ergebnissen führen. Da die Test nicht auf der Festplatte, sondern im RAM ablaufen, sind die angegebenen Durchsatzraten für die Arbeit mit Image-Dateien nicht ganz repräsentativ. Festplatten sind im Normalfall um mehrere Zehnerpotenzen langsamer als der Hauptspeicher. Dadurch ist der Unterschied zwischen der Schreib-/Lesegeschwindigkeit ohne Verschlüsselung, im Vergleich mit einer Verschlüsselung auf der Festplatte bei weitem geringer. Bei einem langsamen Rechner spiegeln die Testergebnisse aber durchaus ein gutes Bild für die spätere Arbeitsgeschwindigkeit wieder.

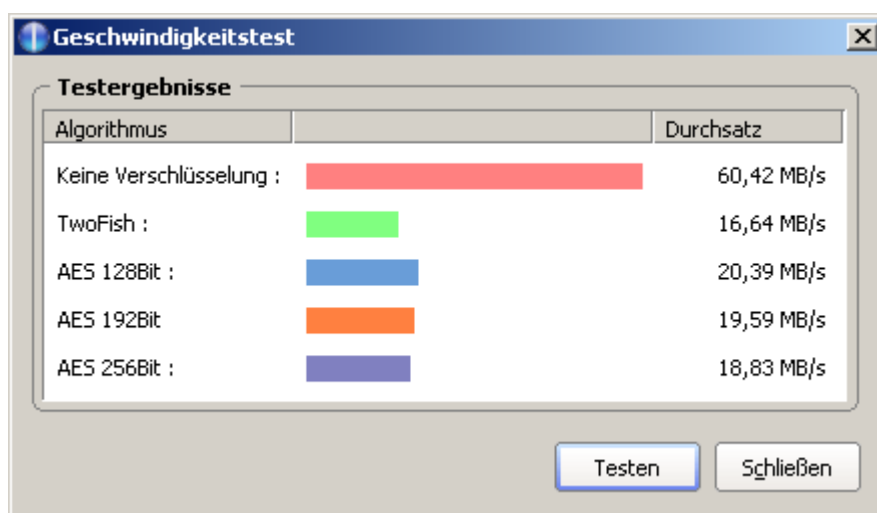


Abbildung 4. Ermittelte Durchsatzraten für die verschiedenen Algorithmen


Die von PrimalCrypt erstellten Images müssen, bevor Daten in ihnen gespeichert werden können, zunächst formatiert werden. D.h. Windows muss das Laufwerk mit einem Dateisystem versehen, um die gespeicherten Dateien verwalten zu können.

PrimalCrypt kann die Laufwerksformatierung gleich nach dem Erstellen der Image-Datei durchführen. Wählen Sie hierzu das von Ihnen gewünschte Dateisystem aus der

Auswahlliste. Sie können zwischen FAT (File Allocation Table), FAT32 und NTFS (NT Filesystem) wählen. Wenn Sie als Formatierungstyp „Keine“ ausgewählt haben, müssen Sie das Laufwerk nachträglich im Windows-Explorer formatieren.

Für die Auswahl der verschiedenen Dateisysteme sollten Sie folgendes beachten :

- FAT formatierte Laufwerke können zwischen 19KB und 2GB groß sein und werden von allen Windows Versionen unterstützt.
- FAT32 kann für Laufwerksgrößen von 32MB bis 32GB eingesetzt werden, wird allerdings nicht von Windows NT 4 unterstützt.
- NTFS kann nur unter Windows NT 4, Windows 2000 und XP eingesetzt werden. Die minimale Laufwerksgröße liegt bei 2526KB (ca. 2,5MB), die maximale bei 2TB (2048GB) .



The screenshot shows a configuration window titled 'Laufwerk'. It contains several settings:

- Verschlüsselungsverfahren :** AES 256Bit (SHA-1)
- Größe :** 100 MB
- Formatierung :** NTFS
- Bevorzugter Laufwerksbuchstabe :** X:
- Verfügbare Speicherplatz :** 594,1 GB auf Laufwerk C:
- Datenträgerbezeichnung :** Mein Laufwerk

Abbildung 5. Eingabe der Laufwerkseigenschaften

Eine Image-Datei wird normalerweise unter dem ersten von Windows bereitgestellten freien Laufwerksbuchstaben gemountet. Soll das Laufwerk immer unter einem bestimmten Laufwerksbuchstaben erreichbar sein, weil Sie z.B. ein Programm darauf installiert haben oder in Ihrer Textverarbeitung den Speicherpfad auf das verschlüsselte Laufwerk gesetzt haben, wählen Sie einfach den bevorzugten Laufwerksbuchstaben in der entsprechenden Auswahlliste. Die Einstellungen können in der Laufwerksverwaltung auch nachträglich geändert werden (siehe Kapitel 2.4).



Wählen Sie keinen Laufwerksbuchstaben, der bereits von einem CD-ROM oder einem anderen fest installierten Laufwerk belegt ist. Doppelbelegung eines Laufwerksbuchstaben kann zu Datenverlusten führen.

Im Erstellungsassistenten haben Sie noch die Möglichkeit, ein Startprogramm (z.B. den Windows Explorer) zu wählen, welches beim mounten der Image-Datei automatisch geöffnet wird. Diese Einstellung ist in der Profi-Ansicht aus Gründen der Übersichtlichkeit nicht vorhanden. Sie können aber nachträglich in der Laufwerksverwaltung ein Startprogramm auswählen.

Wenn Sie ein Verschlüsselungsverfahren gewählt haben, benötigt PrimalCrypt noch die Angabe über die Art des verwendeten Zugangsschlüssels. Sie können das Image entweder über ein Passwort, oder mit einer Schlüsseldatei vor den

Zugriffen durch andere Personen schützen.





2.1.4 Passwortschutz

Für die Verschlüsselung durch ein Passwort, klicken Sie unter „**Schutzverfahren**“ auf den Radioschalter „**Passwortschutz**“.

Abbildung 6. Passwortvergabe für eine Image-Datei

Geben Sie im ersten Eingabefeld Ihr gewähltes Passwort ein, und bestätigen Sie dieses in der zweiten Eingabezeile nochmals.

Warnsymbole links neben den Eingabefeldern geben Ihnen Auskunft über die Sicherheit des gewählten Kennwortes und die Übereinstimmung der beiden Passworteingaben.

-  Das Passwort wurde nicht korrekt bestätigt / stimmt nicht überein.
-  Das Passwort ist nicht sicher. Sie sollten ein längeres Kennwort wählen.
-  Das Passwort ist zwar sicher, aber zu kurz.
-  Das gewählte Passwort ist sicher.

Für das Passwortschutzverfahren müssen Sie nun keine weiteren Eingaben machen.

„Drücken“ Sie als letzten Schritt nur noch auf den Schalter „**Laufwerk erstellen**“, um die gewünschte Image-Datei zu erstellen.

2.1.5 Schlüsselschutz

Falls Sie sich für den Zugriff per Schlüsseldatei entschieden haben, klicken Sie unter „**Schutzverfahren**“ auf den Radioschalter „**Schlüsselschutz**“.

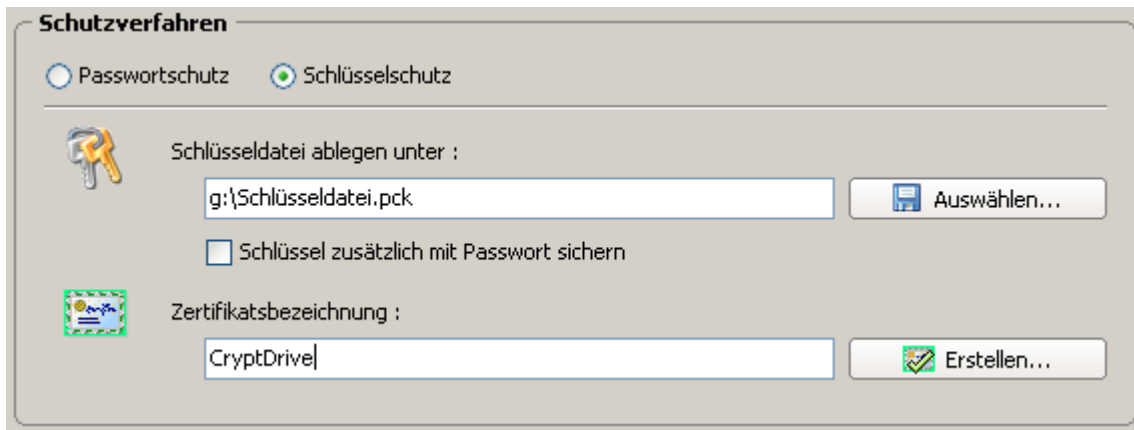


Abbildung 7. Angabe der Schlüsseldatei und der Zertifikatsbezeichnung

Legen Sie zunächst den Speicherort und den Namen für die Schlüsseldatei fest. Geben Sie hierzu entweder den vollständigen Dateipfad in das Eingabefeld ein, oder wählen Sie durch einen Mausklick auf den Schalter „**Auswählen...**“ den Speicherort und Dateinamen über ein Dialogfenster aus.

Ist die angegebene Datei bereits vorhanden, schreibt PrimalCrypt den Schlüsselcode an das Ende der bestehenden Datei. Der Schlüssel wird dadurch versteckt, die Schlüsseldatei darf aber danach nicht mehr geändert werden.

Wenn der Dateiname noch nicht existiert, wird eine einzelne Schlüsseldatei erzeugt. Die Dateiergung .pck ist hierbei nicht zwingend notwendig. Sie können jede beliebige Dateiergung (wie z.B. .jpg oder auch .datei) eingeben und so den Dateityp verschleiern.

Eine Schlüsseldatei kann nicht nachträglich verschoben werden.

Der eingegebene Dateipfad muss auf das endgültige Trägerlaufwerk verweisen. Dieses Trägerlaufwerk muss von Windows automatisch erkannt werden. Die Auswahl beschränkt sich dadurch vornehmlich auf USB-Datenträger, wie Memorysticks oder USB-Festplatten. Aber auch CD-ROMs werden automatisch erkannt falls die Autorun-Option unter Windows nicht deaktiviert wurde. Die Datenträger eines Wechselplattenlaufwerks, wie z.B. Zip-Disketten, SD-Karten oder auch Floppydisks müssen manuell durch einen Doppelklick auf das jeweilige Laufwerkssymbol gemountet werden. Deshalb kann PrimalCrypt darauf befindliche Schlüssel nicht automatisch erkennen.

Schlüsseldateien können nicht in einem Unterverzeichnis abgelegt werden.

D.h. Sie müssen als Dateipfad das sog. Root- bzw. Hauptverzeichnis des Trägerlaufwerks auswählen. Im Beispielfall (Abbildung 7.) wäre das also „g:\“.

Geben Sie für die Zertifikatsbezeichnung einen für Sie eindeutigen Namen ein.

Dieser Bezeichner wird nur für interne Zwecke in der Schlüsselverwaltung verwendet. Als Vorgabe schlägt PrimalCrypt den Dateinamen der Image-Datei vor.

Soll der **Schlüssel zusätzlich mit einem Passwort versehen** werden, klicken Sie bitte noch die entsprechende Option an.

Wenn alle Angaben vollständig sind, klicken Sie auf den Schalter „**Erstellen...**“, um das Hauptschlüsselzertifikat (HSZ) anzulegen.

Dazu müssen Sie den Dateipfad und den Dateinamen, sowie ein Zugriffspasswort für das Hauptschlüsselzertifikat eingeben. Das HSZ kann zwar prinzipiell überall abgelegt werden, jedoch sollten Sie als Speichermedium z.B. eine Diskette wählen um diese an einem sicheren Ort aufbewahren zu können. Das Hauptschlüsselzertifikat ist die einzige Möglichkeit, defekte oder gelöschte Schlüsseldateien oder Zertifikate wiederherstellen zu können.

Wurde die Option „**Schlüssel zusätzlich mit Passwort sichern**“ gewählt, benötigt PrimalCrypt von Ihnen außer dem Passwort für die Hauptschlüsseldatei auch noch das zusätzliche Passwort für den Schlüssel.

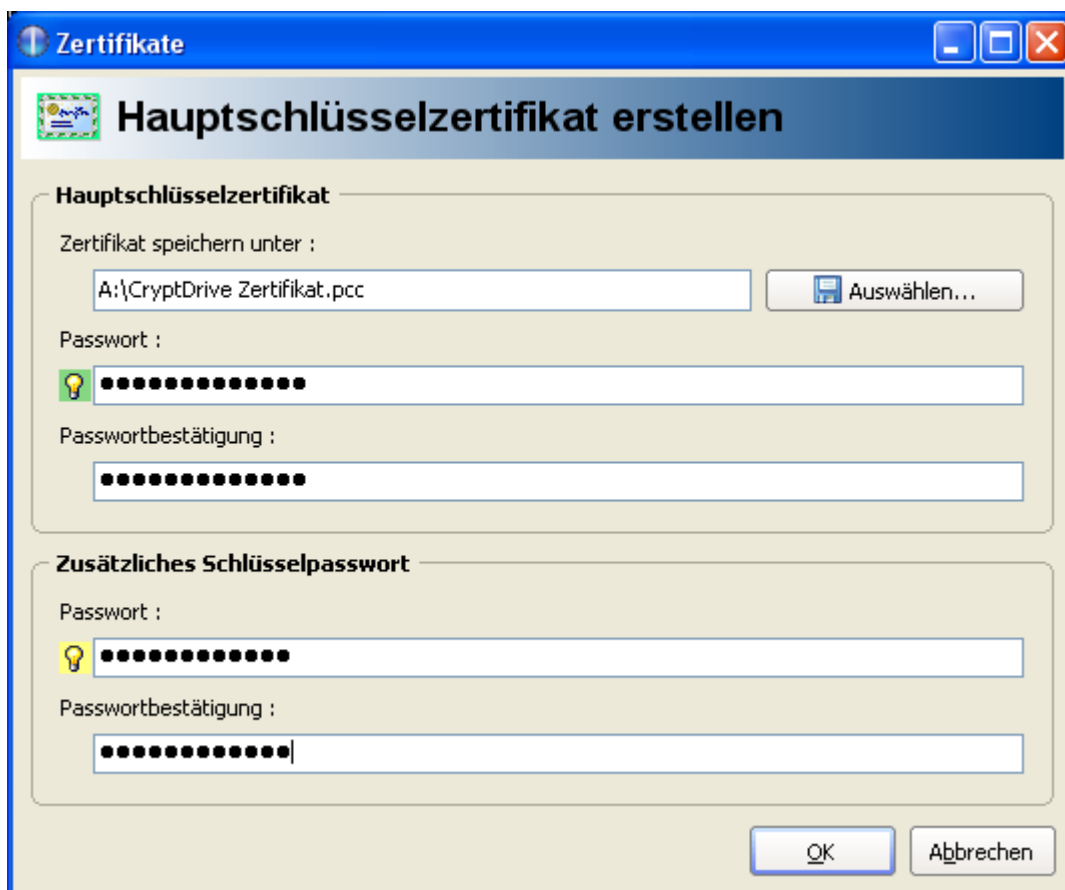


Abbildung 8. Erstellen des Hauptschlüsselzertifikats und Eingabe des Schlüsselpasswortes

Schließen Sie den Dialog durch einen Klick auf den „**OK**“ Schalter.

Im PrimalCrypt Hauptfenster müssen Sie jetzt nur noch den den Schalter „**Laufwerk erstellen**“ betätigen.

Entfernen Sie nach der vollständigen Fertigstellung den Schlüsselträger (also das Laufwerk, auf dem die Schlüsseldatei abgelegt wurde) unbedingt über das Symbol „**Hardware entfernen oder auswerfen**“ in der Windows-Taskleiste.



Abbildung 9. Hardware entfernen oder auswerfen

Klicken Sie hierzu in der Taskleiste mit der **linken** Maustaste auf das in Abbildung 9. Rot markierte Symbol. In dem zugehörigen Kontextmenü wählen Sie für unseren Beispielfall „**USB-Massenspeicher – Laufwerk(G:) anhalten**“. Erst wenn Windows meldet, dass der gewählte Massenspeicher sicherer entfernt werden kann, dürfen Sie den Memorystick oder die Festplatte aus dem USB-Anschluss Ihres Rechners ziehen. Dieses Vorgehen gilt natürlich nicht für CD-Medien.



Entfernen Sie nie einen USB-Massenspeicher ohne die vorherige Abmeldung. Dies kann vor allem bei langsamen Speichermedien, wie den bei USB-Memorysticks verwendeten Flash-Speichern zu Datenverlusten führen.

2.2 Portable Automount-Images

Manchmal benötigt man Daten auf mehreren Rechnerarbeitsplätzen, die nicht über ein Netzwerk miteinander verbunden sind. Wenn diese Datenbestände ständig zwischen den verschiedenen Rechnern aktualisiert werden müssen, werden die zu synchronisierenden Daten zunehmend auf wiederbeschreibbaren, transportablen Datenträgern abgelegt. Hier bieten sich vor allem tragbare USB-Festplatten oder USB-Memorysticks an.

Geht ein solcher Datenträger verloren, ist der finanzielle Verlust der Hardware meist zu verschmerzen. Oft sind die Daten wesentlich wertvoller und können, wenn Sie in die falschen Hände geraten, missbraucht werden.

Mit PrimalCrypt ist es nun natürlich kein Problem, eine verschlüsselte Image-Datei auf diesen Datenträger zu legen und die Daten darin zu speichern.

Der Haken an der Sache ist jedoch, dass Sie diese Image-Dateien nicht mit einer Schlüsseldatei schützen können.

Zur Erinnerung: Eine Schlüsseldatei wird von einem Zertifikat auf dessen „Echtheit“ geprüft. Stimmen Schlüssel und Zertifikat überein, kann das passende Image als Laufwerk gemountet werden. Wo sich diese Image-Datei befindet (also auf welchem Laufwerk), ist im Zertifikat vermerkt. Also z.B. g:\CryptDrive.img.

Nun kann es aber sein, dass Sie gerade Ihre Digital-Kamera via USB-Anschluss mit Ihrem Rechner verbunden haben und diese von Windows den Laufwerksbuchstaben G: zugewiesen bekommen hat. Beim Einstecken des Datenträgers, auf dem sich das Image CryptDrive.img befindet, vergibt Windows nun den Buchstaben H: und wird somit nicht durch das Zertifikat gefunden.

Als andere Alternative würden also nur Passwortverschlüsselte Images in Frage kommen. Diese besitzen kein Zertifikat und können manuell ausgewählt werden. Es bedeutet aber

einen relativ hohen Aufwand um an die gewünschten Daten heranzukommen: Einstecken des USB-Laufwerks, öffnen von PrimalCrypt, auswählen der Image-Datei und - zu guter Letzt - Eingabe des Passwortes.

Wünschenswert wäre es, wenn man nur den ersten Punkt (also einstecken des USB-Laufwerks) durchführen müsste und dann, wie gewohnt mit den Dateien arbeiten könnte.

Genau dies ermöglichen die portablen Automount-Images (PAI). Ein PAI bekommt im Gegensatz zu einem normalen Image seinen Schlüssel gleich mitgeliefert. Dadurch kann es - wie ein Schlüsselkind - für sich selber sorgen, oder besser gesagt, sich selber um das Aufschließen der Türe kümmern. Durch die PAIs erhalten Sie also Plug and Play – einstecken und loslegen – für Ihre verschlüsselten Daten. Dabei wird das PAI natürlich nur an den Rechner geöffnet, auf denen sich ein passendes Zertifikat befindet.

Um ein Portables Automount-Image zu erstellen, können Sie so vorgehen als ob Sie ein mit Schlüsselschutz versehenes Images anlegen möchten. Als Speicherort geben Sie das Hauptverzeichnis des Trägerlaufwerks an. Zusätzlich wählen Sie die Option „**Portables Automount-Image erstellen**“.

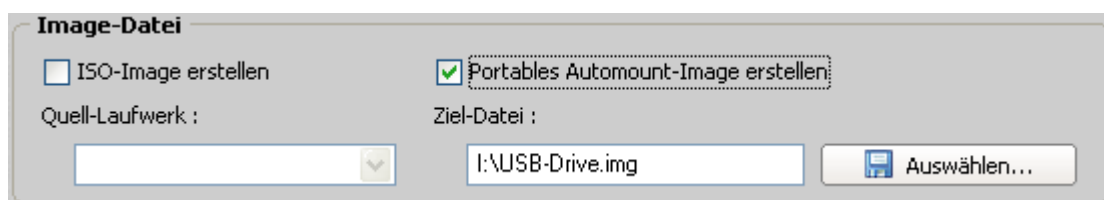


Abbildung 10. Erstellen eines portablen Automount-Images

Die Auswahl des Verschlüsselungsverfahrens, sowie der Formatierung der Image-Datei ist identisch mit der ab Kapitel 2.1.3 beschriebenen Vorgehensweise.

Da ein PAI immer mit einem Schlüsselcode versehen ist, steht für die Wahl des Schutzverfahrens nur der „**Schlüsselschutz**“ zur Verfügung. Der Speicherort für die Schlüsseldatei muss nicht mehr angegeben werden.

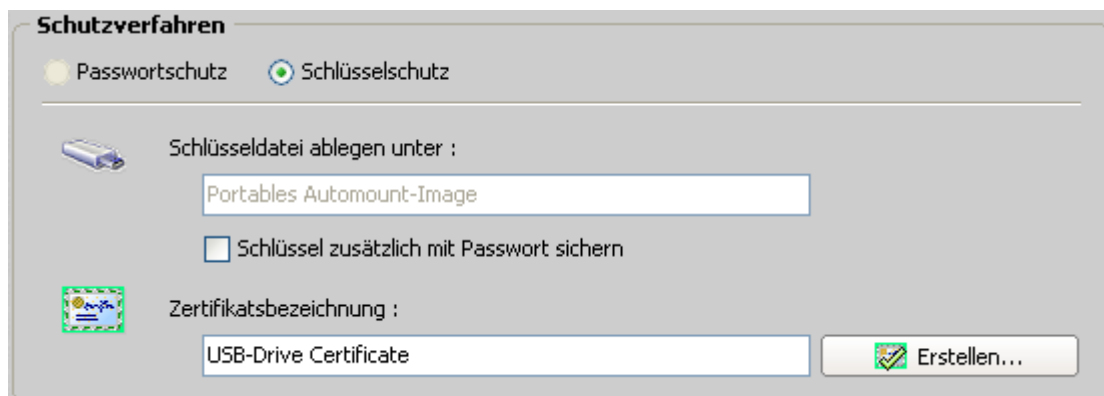


Abbildung 11. Angabe der Zertifikatsbezeichnung für ein portables Automount-Image

Klicken Sie eventuell noch die Option „**Schlüssel zusätzlich mit Passwort sichern**“ an, um das portable Automount-Image zusätzlich durch eine Passwortabfrage zu schützen.

Geben Sie noch einen, für die Schlüsselverwaltung eindeutigen Zertifikatsbezeichner ein und klicken Sie auf den Schalter „**Erstellen...**“.

Nachdem Sie die weiteren Eingaben im Dialogfenster „Zertifikate“ vervollständigt haben (siehe Kapitel 2.1.5), genügt ein letzter Mausklick auf den Schalter „**Laufwerk erstellen**“ um die Image-Datei als ein portables Automount-Image zu speichern.

2.3 Laufwerke verwalten

Eine Image-Datei ist zunächst einmal eine recht wertlose Sache. Auf der Festplatte benötigt sie eventuell mehrere Megabyte Speicherplatz und die in ihr gespeicherten Daten sind weder sichtbar, noch können sie durch irgendeine gängige Applikation bearbeitet werden.

Bisher haben wir immer von Images oder Image-Dateien geredet. Brauchbar werden diese allerdings erst, wenn sie wie ein Festplattenlaufwerk bzw. eine CD behandelt werden können.

Eine im üblichen Sinne verwendete (Hardware) Festplatte wird in einem Computer über ein so genanntes Treiberprogramm (Treiber oder Driver) angesprochen. Dieser Treiber weiß über die von der Festplatte verwendeten Steuerbefehle und deren Anwendung Bescheid. D.h. der Treiber hat Kenntnis darüber, wo die Festplatte angeschlossen ist (z.B. IDE- oder USB-Anschluss), welche Befehle zum Übertragen der Daten notwendig sind und die Art und Weise, wie die Daten an die Festplatte übergeben werden müssen. Zusätzlich zu diesem „Wissen“ bietet der Treiber eine standardisierte Schnittstelle zwischen dem verwendeten Gerät und dem Betriebssystem. Windows-Programme müssen somit nicht die verschiedenen Eigenarten eines Gerätes kennen, sondern nur noch die für das Betriebssystem üblichen Systemaufrufe zum Lesen, Schreiben, etc. beherrschen.

PrimalCrypt verwendet einen virtuellen Festplattentreiber, um Windows den Umgang mit Image-Dateien zu ermöglichen. Da ein Image keine wirkliche Festplatte ist (also sozusagen unwirklich) wird sie als virtuell bezeichnet. Die Eigenarten dieses Gerätes sind also, dass es zum einen nicht in Form einer greifbaren, elektromechanischen Einheit vorhanden ist und zum anderen, dass die Daten beim Hineinschreiben verschlüsselt und beim Herauslesen entschlüsselt werden. Dem Betriebssystem sind diese Geräteeigenschaften völlig unbekannt, es benötigt nur die vorgeschriebene Schnittstelle um mit dem (virtuellen) Gerät arbeiten zu können.

Der Treiber wurde dem Betriebssystem bereits bei der Installation von PrimalCrypt bekannt gemacht. Die Image-Dateien kennt Windows aber noch nicht. Diese Zuweisung geschieht in PrimalCrypt durch den Laufwerksbrowser.

Um eine Image-Datei als Laufwerk hinzuzufügen oder dieses wieder zu entfernen, wechseln Sie über das Hauptmenü „**Laufwerke**“ / „**Laufwerke verwalten...**“ in den Laufwerksbrowser. Durch einen Mausklick in der linken Menüleiste auf „**Bestehende verwalten**“ (Kategorie „**Laufwerke**“), erreichen Sie den Laufwerksbrowser ebenfalls.



Abbildung 12. Bestehende Laufwerke verwalten

Im Hauptfensterbereich wird eine Liste der freien Laufwerksbuchstaben angezeigt. Möchten Sie nun ein Image als Laufwerk P: mounten, klicken Sie auf die entsprechende Zeile der Auswahlliste.

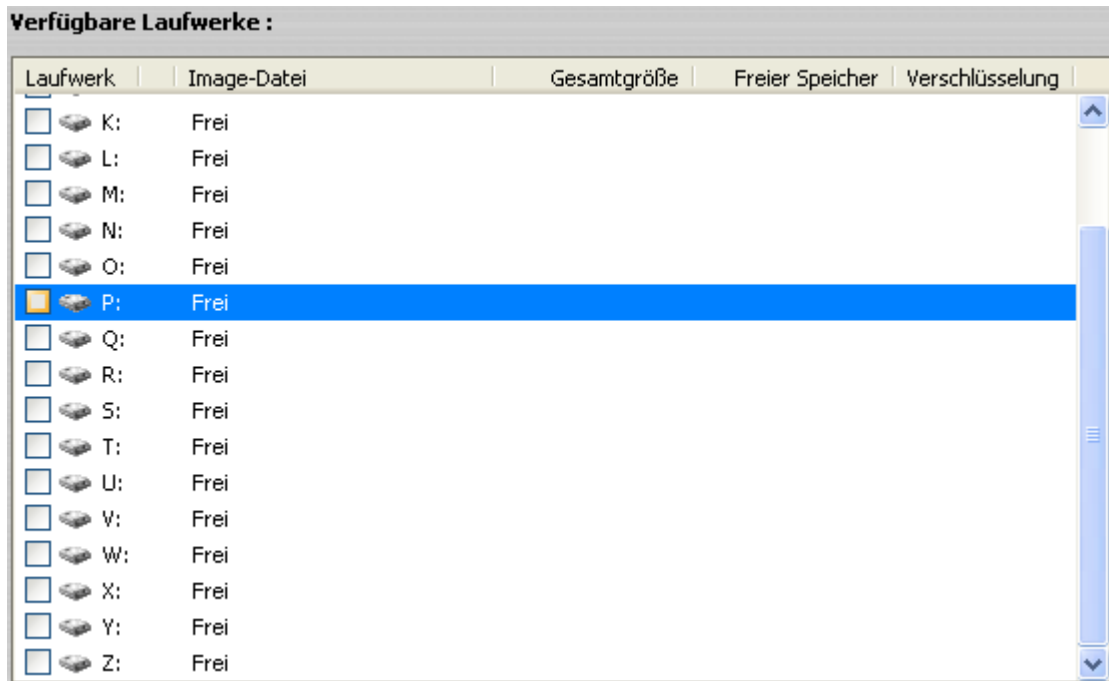


Abbildung 13. Liste der verfügbaren Laufwerke im Laufwerksbrowser

Unterhalb der Liste der verfügbaren Laufwerke, finden Sie ein Eingabefeld um den Pfad und Dateinamen für die zu öffnende Image-Datei anzugeben.

Image-Dateien dürfen auch innerhalb eines freigegebenen Verzeichnisses auf einem Netzwerkserver liegen. Falls für das Freigabeverzeichnis eine Laufwerksverknüpfung (per „Netzwerklaufwerk verbinden“) erstellt wurde, kann der Image-Pfad über den entsprechend verknüpften Laufwerksbuchstaben angesprochen werden.

Also z.B. „S:\Images\CryptDrive.img“, wobei S: das Netzwerklaufwerk bezeichnet.

Wurde keine explizite Laufwerksverknüpfung erstellt, muss der vollständige Serverpfad im sog. UNC-Format angegeben werden. Wenn der Server z.B. den Namen „NetServer“ besitzt und sich die Image-Datei „CryptDrive.img“ im Verzeichnis „\Daten\Images\“ befindet, lautet der vollständige UNC-Pfad „\\NetServer\Daten\Images\CryptDrive.img“. Beachten Sie bitte, dass vor dem Servernamen zwei nach links gerichtete Schrägstriche (Backslash) angegeben werden müssen.

Alternativ zu direkter Eingabe des Pfadnamens können Sie mit einem Mausklick auf den Schalter „**Auswählen...**“ oder den Schalter „**Laufwerk mounten**“ die Image-Datei über einen Auswahldialog angeben, oder durch klicken auf das nach unten gerichtete Dreieck neben dem Schalter „Laufwerk mounten“ eines der zuletzt gemounteten Laufwerke aus einem Menü wählen.

Handelt es sich bei der gewählten Datei um ein ISO-CD Image, müssen Sie zusätzlich die Option „**Als CD-ROM Laufwerk hinzufügen**“ angekreuzt haben. Normalerweise besitzen CD-ROM Images die Dateiendung „.iso“. PrimalCrypt wählt in diesem Fall automatisch die entsprechende Option für Sie aus. Achten Sie aber dennoch auf die korrekte Einstellung

für die jeweilige Datei.

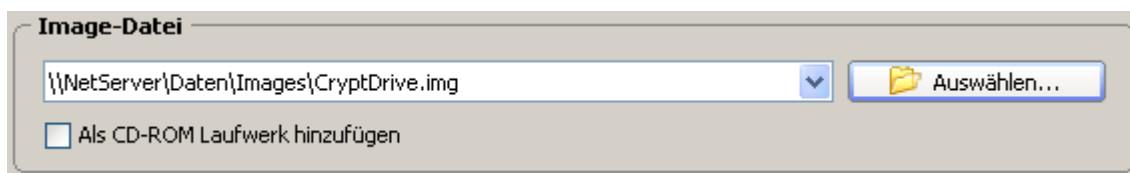


Abbildung 14. Auswahl der zu öffnenden Image-Datei

Wenn Sie eine normale Image-Datei als CD-ROM Laufwerk mounten, kann der Inhalt des Laufwerks später nicht gelesen werden. Das Gleiche gilt auch für den umgekehrten Fall (also mounten eines ISO-Images als normales Laufwerk). Dies liegt daran, dass sich das Aufzeichnungsformat einer CD-ROM grundlegend von dem eines Festplattenlaufwerks unterscheidet.

Klicken Sie nun auf den Schalter „**Laufwerk mounten**“.

PrimalCrypt versucht nun, das gewählte Image unter dem angegebenen Laufwerksbuchstaben zu mounten. Sie werden zunächst noch nach dem gültigen Passwort gefragt.



Abbildung 15. Passwortdialog

Bei einem unverschlüsselten Image lassen Sie das Eingabefeld leer. Bestätigen Sie die Eingabe durch klicken des „**OK**“ Schalters.

PrimalCrypt kann nicht prüfen, ob Ihre Passworteingabe korrekt war. Das Laufwerk wird im Falle einer ungültigen Eingabe zwar unter dem angegebenen Laufwerksbuchstaben gemountet, ein Zugriff darauf ist aber nicht möglich.

Sie erkennen diesen Fehler daran, dass das Laufwerk keine Angaben zur Gesamtgröße und den zur Verfügung stehenden freien Speicher besitzt. Außerdem wird für die Verschlüsselung „**Keine**“ angezeigt.

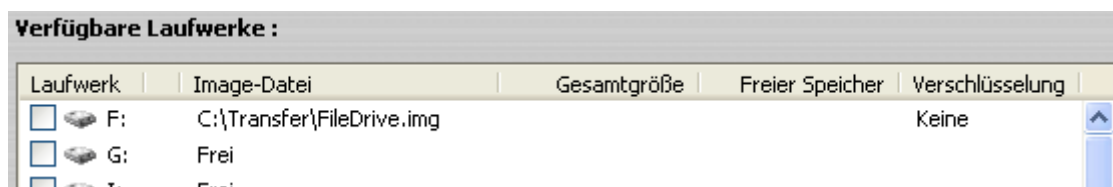


Abbildung 16. Anzeige des Laufwerks nach falscher Passworteingabe

Sie müssen in diesem Fall das Laufwerk wieder entfernen und erneut mit dem richtigen Passwort mounten.

In manchen Fällen kann PrimalCrypt beim erstellen einer Image-Datei die Formatierung nicht vollständig durchführen. Dieses Problem tritt hauptsächlich auf langsamen Rechner auf. Sie müssen in diesem Fall das Laufwerk manuell formatieren. Hierzu mounten Sie zunächst die Image-Datei. Für nicht formatierte Laufwerke wird keine Angabe über die Gesamtgröße und den verbleibenden freien Speicherplatz angezeigt. Die Angabe über den verwendeten Verschlüsselungsalgorithmus ist jedoch korrekt.

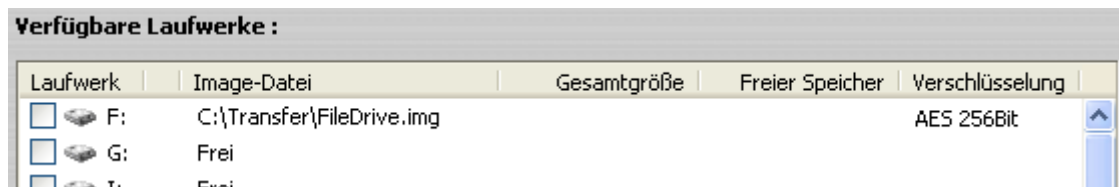


Abbildung 17. Nicht formatiertes Laufwerk im Laufwerksbrowser

Wechseln Sie in den Windows-Explorer und wählen Sie unter „Arbeitsplatz“ das gerade gemountete Laufwerk aus. Klicken Sie mit der rechten Maustaste auf das Laufwerksymbol und dann im Kontextmenü auf „Formatieren...“. Im Formatierungsdialog können Sie dann einen optionalen Datenträgerbezeichner und den Typ des Dateisystems angeben.

Als Formatierungsoption klicken Sie zusätzlich „Quickformat“ an, um das Laufwerk schneller zu formatieren. Bestätigen Sie abschließend Ihre Angaben mit einem Klick auf den Schalter „Starten“.

Nach erfolgreicher Formatierung beenden Sie den Dialog durch einen Mausklick auf den Schalter „Schließen“.

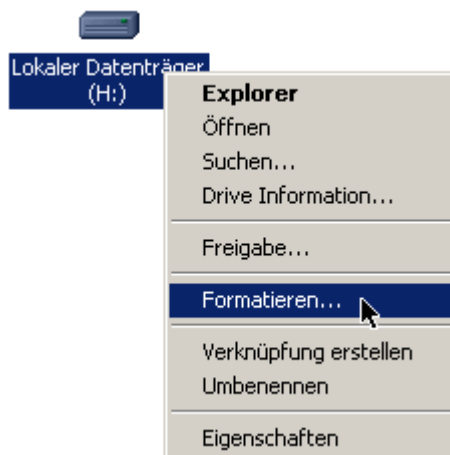


Abbildung 18. Kontextmenü für Laufwerke

Nach dem Formatieren kann das gemountete Laufwerk dann uneingeschränkt benutzt werden.

Wenn der Zugriff auf ein Laufwerk nicht mehr benötigt wird, kann es über den Laufwerksbrowser wieder entfernt werden (unmount). Wählen Sie zunächst das entsprechende Laufwerk aus.

Der Schalter „**Laufwerk mounten**“ ändert seine Beschriftung in „**Laufwerk entfernen**“. Klicken Sie auf diesen Schalter um das gewählte Laufwerk aus dem Windows-Dateisystem zu entfernen.



PrimalCrypt kann ein Laufwerk nicht entfernen, wenn eine darauf befindliche Datei oder ein Windows Explorer-Fenster für das Laufwerk oder eines seiner Unterverzeichnisse geöffnet ist.

Wurden mehrere Image-Dateien gemountet und Sie benötigen auf keines der Laufwerke mehr einen Zugriff, können Sie alle Images durch einen Mausklick auf „**Alle Laufwerke entfernen**“ schließen.

Es stehen noch andere Möglichkeiten zum mounten bzw. unmounten der Laufwerke zur Verfügung :

1. Ziehen Sie eine Image-Datei auf den Laufwerksbrowser und lassen Sie diese über dem Laufwerksbuchstaben, unter dem das Image gemountet werden soll „fallen“.
2. Wählen Sie im Hauptmenü von PrimalCrypt den Menüpunkt „**Laufwerke**“ und dann
 - „**Laufwerk mounten...**“, um eine Image-Datei direkt auszuwählen und unter dem ersten freien Laufwerksbuchstaben zu mounten.
 - „**Image auswählen...**“, um eine Image-Datei über einen Auswahldialog zu suchen. Der Dateipfad wird dann im Eingabefeld „**Image-Datei**“ angezeigt. Die Auswahl des Laufwerksbuchstabens und das eigentliche mounten muss dann noch manuell erfolgen.
 - „**Laufwerk entfernen**“, um ein einzelnes Laufwerk zu entfernen.
 - „**Alle Laufwerke entfernen**“, um alle gemounteten Laufwerke zu entfernen.
3. Klicken Sie mit der **rechten** Maustaste auf das PrimalCrypt Schlüsselsymbol in der Windows Taskleiste.



Abbildung 19. PrimalCrypt Taskleisten-Symbol

Über das Kontextmenü können Sie dann einen der Menüpunkte

- „**Laufwerk mounten**“
- „**Laufwerk entfernen**“
- „**Alle Laufwerke entfernen**“

auswählen. Diese entsprechen in der Funktion den jeweiligen Hauptmenüpunkten.

Laufwerks-Images können auch automatisch beim Starten von PrimalCrypt gemountet werden. Dazu markieren Sie das Ankreuzfeld auf der linken Seite des entsprechenden Laufwerkeintrags.

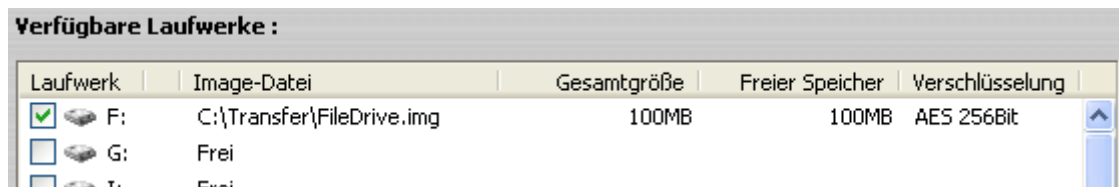


Abbildung 20. Laufwerk für automatisches mounten markieren

Soll das automatische mounten wieder aufgehoben werden, entfernen Sie die Markierung entweder im Laufwerksbrowser oder in der Laufwerksverwaltung (siehe Kapitel 2.4).

2.4 Laufwerksverwaltung

In der Laufwerksverwaltung werden alle erstellten Laufwerks-Images aufgeführt. Hier können Sie verschiedene Einstellungen bezüglich des Verhaltens einer Image-Datei beim Mounten vornehmen.

Klicken Sie im Laufwerksbrowser auf den Schalter „**Laufwerksverwaltung**“ oder wählen Sie im Hauptmenü „**Laufwerke**“ den Menüpunkt „**Laufwerksverwaltung...**“.



Abbildung 21. Laufwerksverwaltung

Es werden die Pfade zu den verwalteten Image-Dateien und die eventuell zugeordneten, bevorzugten Laufwerksbuchstaben angezeigt. Zusätzlich befindet sich vor jedem Eintrag wie im Laufwerksbrowser ein Ankreuzfeld, dass den jeweiligen Automount-Status der Image-Datei darstellt.

Soll ein Image beim starten von PrimalCrypt automatisch gemountet werden, markieren Sie das entsprechende Ankreuzfeld. Um das automatische mounten wieder abzuschalten, löschen Sie die Markierung wieder.

Im Gegensatz zum Laufwerksbrowser kann die Automount-Funktion hier ein- und ausgeschaltet werden, ohne dass das entsprechende Image als Laufwerk gemountet sein muss.

Eventuell nicht aufgelistete Image-Dateien (z.B. von einer älteren PrimalCrypt Version) können Sie durch klicken des Schalters „**Hinzufügen...**“ in die List aufnehmen.

Nicht mehr benötigte Einträge entfernen Sie durch einen Klick auf den Schalter „**Löschen**“ und mit „**Bearbeiten...**“ können Einstellungen geändert werden.

Die Dialogfenster zum Hinzufügen und Bearbeiten eines Eintrags sind hierbei identisch.

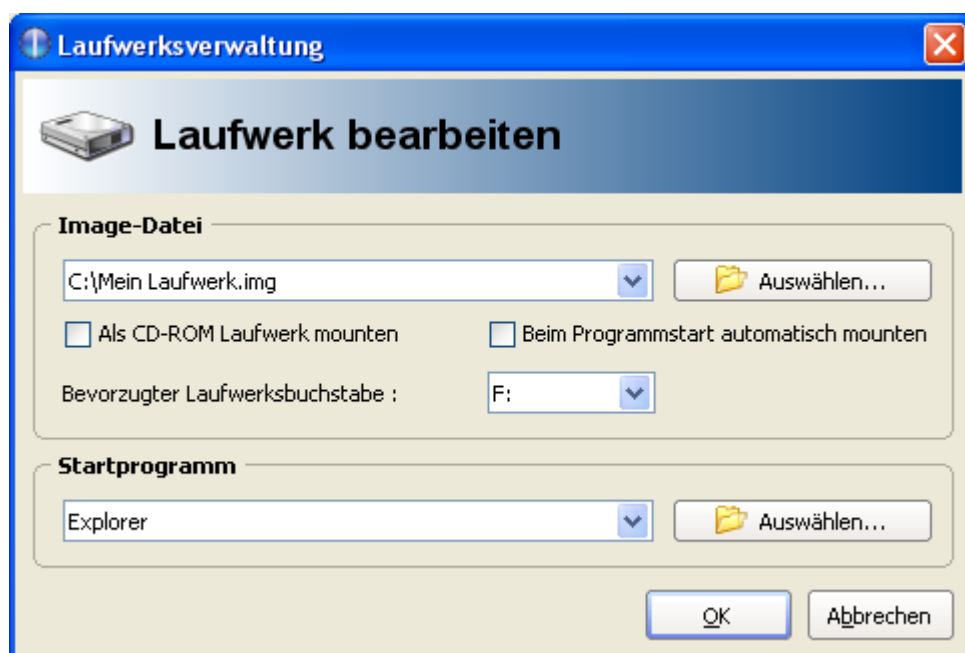


Abbildung 22. Laufwerkseintrag hinzufügen oder bearbeiten

Um eine normale, Passwortgeschützte Image-Datei hinzuzufügen, wählen Sie durch klicken des Schalters „**Auswählen...**“ mit dem Windows Öffnen-Dialog eine Image-Datei auf der Festplatte aus.

Möchten Sie eine Schlüssel geschützte Image-Dateien oder ein portables Automount-Image hinzufügen (nachdem Sie ein Schlüsselzertifikat von einem anderen Rechner übertragen haben), wählen Sie in der Combobox den Bezeichner für das zugehörige Schlüsselzertifikat aus.

Es ist nicht möglich, ein mit einem Schlüssel geschütztes Image über den Schalter „Auswählen...“ hinzuzufügen, da sich der Vorgang des Mountens grundsätzlich von dem einer Passwort geschützten Image-Datei unterscheidet.

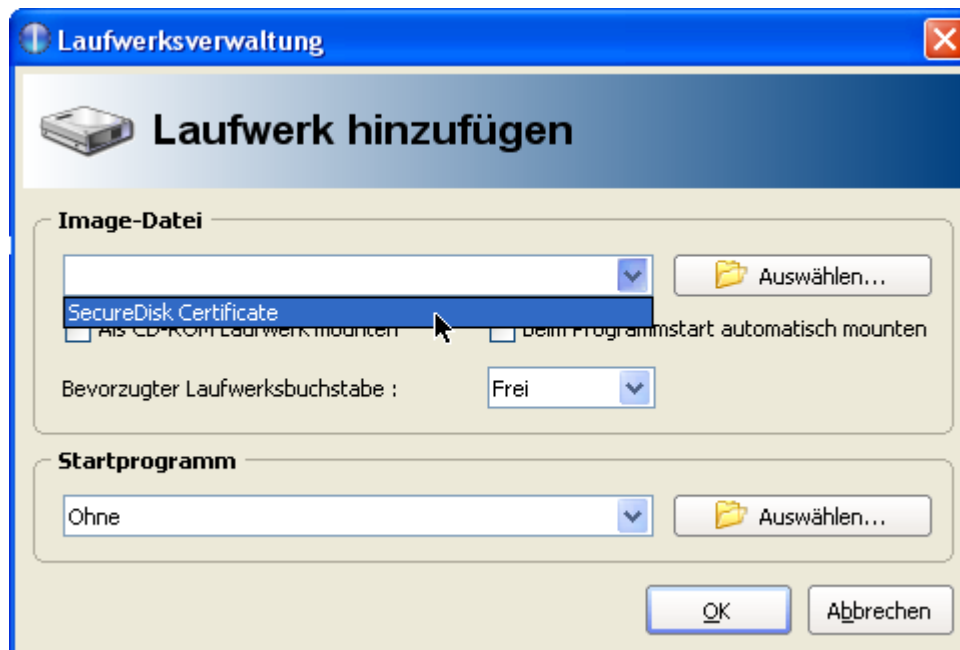


Abbildung 23. Schlüssel geschütztes Image hinzufügen

Nach der Auswahl der Image-Datei müssen Sie noch angeben, ob das Image als CD-ROM Laufwerk gemountet werden soll. Besitzt der Name der Datei die Endung „.iso“, wird die entsprechende Checkbox automatisch markiert. Schlüssel geschützte Images können nur normale Laufwerks-Images sein, deshalb ist diese Vorgabe in diesem Fall nicht anwählbar.

Optional können Sie noch auswählen, ob das Image beim Programmstart automatisch gemountet (nur bei Passwort geschützten Images möglich) und ob ein bestimmter Laufwerksbuchstabe zugeordnet werden soll.

Zusätzlich haben Sie die Möglichkeit, ein Programm auszuwählen, dass nach dem Mounten der Image-Datei automatisch ausgeführt werden soll. In der Combobox werden alle bereit ausgewählten Programme aufgelistet. Neue Programme fügen Sie über den Schalter „**Auswählen**“ hinzu. In der Liste finden Sie auch den (Windows) Explorer. Wird dieser als Autorun Programm angegeben, öffnet sich nach dem Mounten sofort ein Explorer-Fenster das den Inhalt des Laufwerks anzeigt.

3 Dateiverschlüsselung

Die meisten Verschlüsselungsprogramme beschränken sich auf eine bestimmte Funktion. Entweder können verschlüsselte Image-Dateien verwaltet werden oder einzelne Dateien ver- oder entschlüsselt werden. Für jede Funktion benötigen Sie eine eigene, spezialisierte Applikation.

PrimalCrypt bietet Ihnen alles unter einer Oberfläche.

Außer den bisher beschriebenen Image-Dateien können Sie zusätzlich Ihre alltäglich benötigten Passwörter verwalten, Daten in Bilddateien verstecken, Dateien sicher löschen oder auch einzelne Dokumente ver- und entschlüsseln und so z.B. einen sicheren Transport via E-Mail garantieren.

Für die Einzeldateiverschlüsselung wird in PrimalCrypt immer der von Bruce Schneier entwickelte, sehr schnelle und sichere Blockverschlüsselungsalgorithmus Blowfish verwendet.

Mit DropCrypt können Sie sehr komfortabel - durch einfaches „Drag and Drop“ auf ein Desktop-Symbol - Dateien verschlüsseln und natürlich wieder entschlüsseln. Alternativ benutzen Sie die in PrimalCrypt eingebauten Programmmodule.

3.1 DropCrypt

Bei DropCrypt handelt es sich um ein eigenständiges Programm, dass zu PrimalCrypt mitgeliefert wird.

DropCrypt wird über den Einstellungsdialog in PrimalCrypt ein-, bzw. ausgeschaltet und konfiguriert (siehe Kapitel 8.4). Hier vergeben Sie einmalig ein Passwort, dass dann von DropCrypt immer für die Dateiverschlüsselung verwendet wird.

Wurde DropCrypt von Ihnen eingeschaltet, erscheint auf Ihrem Windows-Desktop ein neues Symbol.



Abbildung 24. DropCrypt Symbol auf dem Desktop

Um eine oder mehrere Dateien zu ver- oder entschlüsseln, markieren Sie diese im Windows-Explorer und ziehen (Drag) diese bei weiter gedrückter linker Maustaste auf das DropCrypt-Symbol. Dort lassen Sie die Maustaste los. Die Dateien werden sozusagen auf dem Symbol fallen gelassen (Drop). Sie können natürlich auch ganze Ordner mit Dateien und Unterordnern auf das Desktop-Symbol ziehen.

DropCrypt erkennt selbständig, ob eine Datei bereits verschlüsselt wurde. In diesem Fall

werden Sie nach dem in PrimalCrypt vergebenen Passwort gefragt. Unverschlüsselte Dateien werden ohne Rückfrage mit dem DropCrypt Passwort verschlüsselt.

Werden verschlüsselte und unverschlüsselte Dateien gleichzeitig auf das DropCrypt-Symbol gezogen, werden die jeweiligen Umkehrfunktionen automatisch, passend zu jeder Datei ausgeführt. Sie können während des Ver- bzw. Entschlüsselungsvorgangs mit anderen Applikationen weiterarbeiten, da DropCrypt als eigenständiger Hintergrundprozess läuft.

Sie können DropCrypt jederzeit abbrechen, der aktuell ablaufende Vorgang für eine Datei wird aber immer vollständig abgeschlossen.

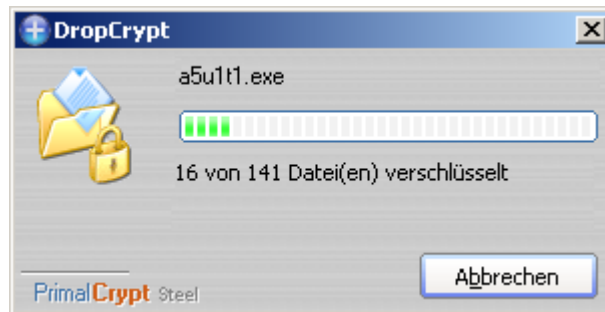


Abbildung 25. DropCrypt-Dialog

Kapitel 8.4 beschreibt die möglichen Einstellungsoptionen für DropCrypt.

3.2 Dateien verschlüsseln

Dateien können auch direkt in PrimalCrypt verschlüsselt werden.

Die Dateiverschlüsselung und die Dateientschlüsselung sind hier aber als getrennte Funktionen aufgeführt. Während DropCrypt eine bereits verschlüsselte Datei entschlüsselt, kann PrimalCrypt eine verschlüsselte Datei nochmals, z.B. mit einem anderen Passwort verschlüsseln. Dieser Vorgang kann beliebig oft wiederholt werden.

Klicken Sie in der Menüleiste unter der Kategorie „**Dateien**“ auf „**Verschlüsseln/Entschlüsseln**“ und wählen Sie dann den Tabulator „**Verschlüssel**“.

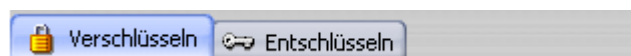


Abbildung 26. Tabulator zur Auswahl Verschlüsseln oder Entschlüsseln

Alternativ wählen Sie im Hauptmenü „**Datei**“ den Menüpunkt „**Dateien verschlüsseln...**“.

Dateien die verschlüsselt werden sollen, können direkt per „Drag and Drop“ auf den Dateibrowser gezogen werden oder über den Schalter „**Datei hinzufügen**“ einzeln per Dialog-Fenster ausgewählt werden.

Durch klicken des Schalters „**Dateien entfernen**“ werden alle markierten Einträge wieder aus der Liste gelöscht. „**Alle Dateien entfernen**“ leer die Liste vollständig.

Wurde von Ihnen DropCrypt aktiviert, so können Sie die dort verwendeten Einstellungen übernehmen. Klicken Sie dazu die Option „**DropCrypt-Einstellungen verwenden**“ an. Sowohl das Passwort als auch die sonstigen Vorgaben von DropCrypt werden nun für die

Dateiverschlüsselung vorgegeben.

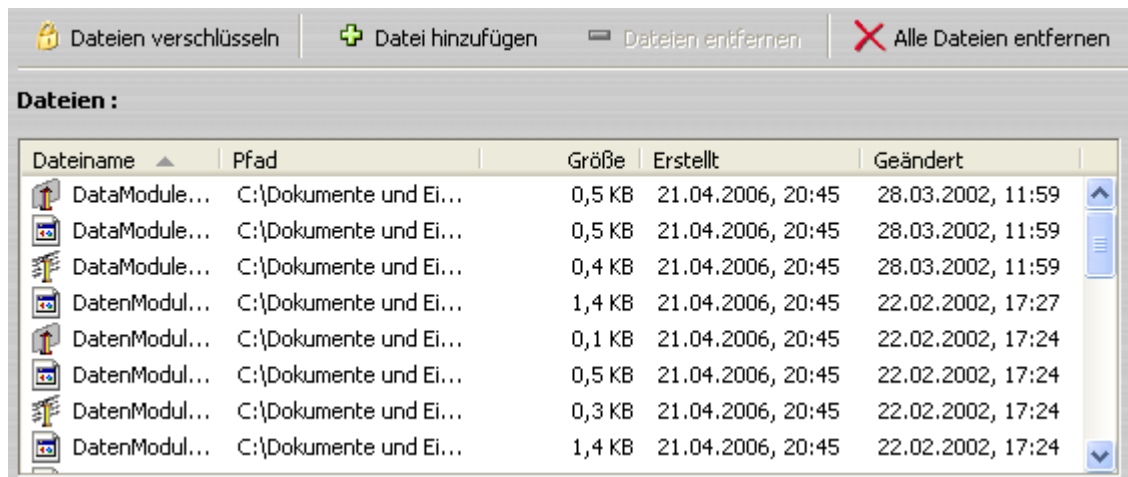


Abbildung 27. Dateibrowser für Dateiver- und entschlüsselung

Wurde die Option nicht ausgewählt, müssen Sie eventuell noch die folgenden Angaben machen :

- **Original Dateien nach dem verschlüsseln löschen.** Alle zu verschlüsselnden Dateien werden nach der Verschlüsselung nach DOD 5220.22-M Standard sicher gelöscht.
- **Alle verschlüsselten Dateien in diesem Ordner ablegen.** Die verschlüsselten Dateien werden in dem angegebenen Verzeichnis (Dateipfad) abgelegt.
- **Dateien als Verschlüsselt markieren.** Alle Dateien erhalten nach der Verschlüsselung die Dateiendung „.pxx“. Die alte Dateiendung wird mit einem Unterstrich an den Dateinamen angehängt. Aus „MeinBild.bmp“ wird also „MeinBild_bmp.pxx“.

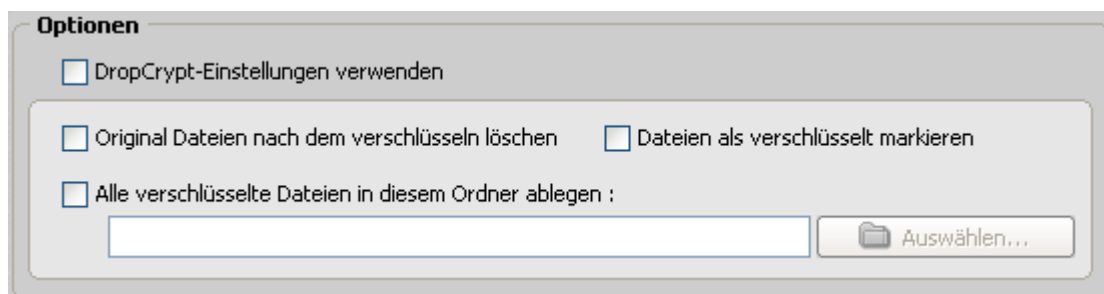


Abbildung 28. Verschlüsselungsoptionen

Wenn Sie die Option „**Alle verschlüsselten Dateien in diesem Ordner ablegen**“ nicht gewählt haben, die Original Dateien aber gelöscht werden sollen, so wird die nicht verschlüsselte Datei durch die verschlüsselte ersetzt.

Soll die Original Datei nicht gelöscht werden, so wird die verschlüsselte Datei in dem selben Verzeichnis wie das unverschlüsselte Original abgelegt. Bei nicht gesetzter Option „Dateien als verschlüsselt markieren“ wird der Dateiname durch den Zusatz „Kopie“ erweitert (also z.B. „Bild1.bmp“ zu „Bild1 Kopie.bmp“).

Werden die verschlüsselten Dateien in ein anderes Verzeichnis als das des Originals gespeichert, wird der gleiche Dateiname übernommen. Existiert bereits eine andere Datei mit dem gleichen Namen, so wird die neu hinzugefügte mit einer bei „1“ beginnenden, fortlaufenden Nummer gekennzeichnet (z.B. Bild1_1.bmp).

Klicken Sie zum Schluss auf den Schalter **„Dateien verschlüsseln“**.

Wenn Sie die DropCrypt-Einstellungen übernommen haben, müssen keine weiteren Eingaben gemacht werden. Andernfalls werden Sie noch nach einem Passwort zum Verschlüsseln der Dateien gefragt, welches Sie dann nochmals aus Sicherheitsgründen bestätigen müssen.

Die Verschlüsselung wird in einem eigenen Prozesszweig (Thread) durchgeführt, so dass Sie in PrimalCrypt weiterarbeiten können. Eine Entschlüsselung von Dateien ist aber während des Verschlüsselungsvorgangs nicht möglich.

3.3 Dateien entschlüsseln

Zum Entschlüsseln von Dateien klicken Sie in der Menüleiste unter der Kategorie **„Dateien“** auf **„Verschlüsseln/Entschlüsseln“** und wählen dann den Tabulator **„Verschlüsseln“** aus, oder Sie wechseln direkt über den Menüpunkt **„Datei“** - **„Dateien entschlüsseln...“** zu diesem Modul.

Die Bedienungsoberfläche ist die gleiche wie für die Dateiverschlüsselung.

Ziehen Sie die zu entschlüsselnden Dateien in den Dateibrowser. Oder klicken Sie auf den Schalter **„Datei hinzufügen“** um einzelne Dateien per Dialog-Fenster auszuwählen.

Entfernen Sie markierte Dateien über den Schalter **„Dateien entfernen“** oder löschen Sie alle Einträge aus der Dateiliste, indem Sie auf **„Alle Dateien entfernen“** klicken.

Durch die Option **„DropCrypt-Einstellungen übernehmen“** werden die Einstellungen für das Ausgabeverzeichnis und die Option zum löschen der Original Dateien von DropCrypt übernommen.

Klicken Sie auf den Schalter **„Dateien entschlüsseln“**. Sie werden nun nach dem Entschlüsselungspasswort gefragt. Diese Eingabe wird auf alle gewählten Dateien angewandt. Achten Sie daher darauf, dass die Dateien zuvor auch wirklich mit diesem Passwort verschlüsselt wurden. Das Entschlüsseln mit einem falschen Passwort kommt einer Verschlüsselung gleich und kann u.U. zum vollständigen Datenverlusten führen.

Um dies zu vermeiden, markieren Sie die Option **„Passwort prüfen“**. Dies schaltet die Plausibilitätsprüfung ein, die zuerst testet, ob das eingegebene Passwort richtig ist.

PrimalCrypt erkennt, ob eine Datei verschlüsselt ist. Unverschlüsselte Dateien können also nicht versehentlich durch nochmalige Entschlüsselung unleserlich gemacht werden.

Mehrfach verschlüsselte Dateien müssen mit den jeweiligen Passwörtern in umgekehrter Reihenfolge wieder entschlüsselt werden.

Wurde eine Datei z.B. mit dem Passwort „Hans“ und dann in einer zweiten Verschlüsselungsrunde mit „Müller“ verschlüsselt, so muss bei der ersten Entschlüsselung das Kennwort „Müller“ und bei der zweiten Entschlüsselung das Kennwort „Hans“ eingegeben werden.

Wird bei nicht gesetzter Option „Passwort prüfen“ versehentlich ein falsches Passwort für die Entschlüsselung angegeben, kann dies über eine **Verschlüsselung** mit dem falsch eingegebenen Passwort wieder rückgängig gemacht werden.

Beispiel :

Eine Datei „Test.txt“ wird verschlüsselt. Als Passwort haben Sie „Schlüssel“ angegeben.

Zum entschlüsseln geben Sie versehentlich „schlüssel“ ein. Die zwei Passwörter unterscheiden sich, da das erste mit einem Großbuchstaben beginnt, das Zweite aber mit einem Kleinbuchstaben. Nach der Entschlüsselung ist der Text nicht lesbar, weil die Datei durch die Falscheingabe nochmals verschlüsselt wurde.

Um die Textdatei korrekt zu dekodieren, muss die falsche Schlüsseleingabe rückgängig gemacht werden. Verschlüsseln Sie die Datei deshalb nochmals mit dem Passwort „schlüssel“. Danach können das Textdokument jetzt mit der richtigen Passworteingabe „Schlüssel“ entschlüsseln und somit wieder lesbar machen.

Für das Überschreiben und Löschen der Original-Dateien gelten die gleichen Einstellungen, wie in Kapitel 3.2 für die Dateiverschlüsselung beschrieben.

4 Passwortlisten

Heutzutage benötigen wir für unseren Alltag immer mehr Passwörter. Dies fängt bei der PIN für unserer Bankkarten an und geht über das Zugangspasswort bei eBay bis hin zur elektronischen Schließanlage an Eingangstüren.

Um die Flut an den (zum Teil kryptischen) Passwörtern bewältigen zu können, greifen viele Menschen zu Papier und Bleistift und schreiben die eigentlich geheimen Zugangsdaten einfach auf. Diese Art von Gedächtnisauflagerung ist zwar nahe liegend, aber natürlich alles Andere als sicher.

PrimalCrypt bietet in seinem Funktionsumfang eine Art Schlüsselkasten für Passwörter und (geheime) Notizen; die Passwortliste. Während ein Schlüsselkasten durch ein Schloss vor dem Zugriff durch fremde Personen geschützt wird, besitzen Passwortlisten ein Zugangskennwort. Sie müssen sich also nur noch ein Kennwort merken um an die in der Liste abgelegten Passwörter zu gelangen.

4.1 Neue Listen erstellen

Wechseln Sie in die Passwortverwaltung. Sie erreichen diese über das Hauptmenü „Datei“ und dem Menüpunkt „**Passwörter & Schlüssel verwalten...**“. Alternativ klicken Sie in der linken Menüleiste unter „**Passwörter & Schlüssel**“ auf „**Verwalten**“.

Im Hauptfensterbereich sehen Sie zwei Tabulatoren. Selektieren Sie durch einen Mausklick den Tabulator „**Passwörter**“.



Abbildung 29. Tabulatoren in der Passwort- und Schlüsselverwaltung

Klicken Sie auf den Schalter „**Neue Liste erstellen...**“ oder wählen Sie im Hauptmenü unter „Datei“ den Menüpunkt „**Neue Passwortliste...**“. Das Dialogfenster zum erstellen einer neuen Passwortliste wird angezeigt.

Geben Sie den vollständigen Dateipfad und Namen, eine für Sie eindeutige Beschreibung für die neue Passwortliste und das Kennwort, mit dem die Passwortliste verschlüsselt werden soll in die entsprechenden Eingabefelder ein.

Sie müssen **alle** geforderten Angaben ausfüllen, ansonsten ist der Schalter „**OK**“ zum Bestätigen und Erstellen der Liste nicht anwählbar.

Die Standard Dateiendung für Passwortlisten ist „.pcl“. Dies ist jedoch nicht zwingend. Sie können auch jede andere Dateiendung wählen.

Die Beschreibung für die Liste sollte auf alle Fälle eindeutig sein. Wenn der beschreibende Name mehrfach verwendet wird, ist eine Unterscheidung später nur noch schwer möglich.

Vergeben Sie für die Passwortlisten grundsätzlich ein sicheres Zugangskennwort. Zur Erinnerung: „Sicher“ heißt mindestens 16 Zeichen, gemischte Groß- und Kleinbuchstaben sowie Zahlen und/oder Sonderzeichen.



Abbildung 30. Dialogfenster „Passwortliste erstellen“




Klicken nach dem Ausfüllen der Eingabefelder auf den Schalter „OK“. Die neue Passwortliste wird erstellt und geöffnet.

4.2 Einträge hinzufügen und bearbeiten

Um einen neuen Eintrag in einer Passwortliste zu erstellen, klicken Sie auf den Schalter „**Hinzufügen...**“ oder wählen Sie im Hauptmenü „**Bearbeiten**“ den Menüpunkt „**Passwort hinzufügen...**“.

Für einen neuen Passwordeintrag wird zumindest ein eindeutiger Name benötigt. In der Auswahlliste „**Typ**“ können Sie einen von vier vordefinierten Eintragstypen auswählen. Zusätzlich können auch noch eigene, benutzerdefinierte Typen vergeben werden.

Die vergebenen Typen werden in der Passwortliste durch verschiedene Symbole gekennzeichnet.

-  Symbol für Passwörter und Image-Passwörter
-  Symbol für PINs
-  Symbol für geschützte Notizen



-  Symbol für Passwörter und Image-Passwörter
-  Symbol für benutzerdefinierte Typen

Abbildung 31. Passwörter hinzufügen und bearbeiten

Wenn Sie einen benutzerdefinierten Typ erstellen möchten, wählen Sie in der Typenliste den Eintrag „< **Neu benutzerdefiniert** >“. Die Auswahlliste (Combobox) ändert sich zu einem Eingabefeld, in das Sie einen beschreibenden Namen für den neuen Typ eingeben können.

Abbildung 32. Erstellen benutzerdefinierter Passworttypen

Beim verlassen des Eingabefeldes oder durch drücken der ENTER bzw. RETURN Taste auf Ihrer Tastatur, wird der neue Typ in die Liste übernommen. Falls Sie es sich anders überlegt haben sollten, oder versehentlich < Neu benutzerdefiniert > ausgewählt wurde, drücken Sie die ESC Taste. Die neue Typenbezeichnung wird dann nicht übernommen.

Für die Eingabe des geschützten Eintrags steht Ihnen ein einzeliges Eingabefeld zur Verfügung. Dies reicht für normale Passwörter, PINs, etc. ohne weiteres aus. Werden aber ausführlichere Informationen wie z.B. ein Benutzername und ein Passwort benötigt, ist die Darstellung in einer Zeile eher unübersichtlich.

Dieser Art von Informationen sollten Sie den Typ „Geschützte Notiz“ vergeben.

Für geschützte Notizen ändert sich das einzelne Eingabefeld in eine Combobox, die - wenn sie geöffnet wird - ein mehrzeiliges Textfeld anzeigt.

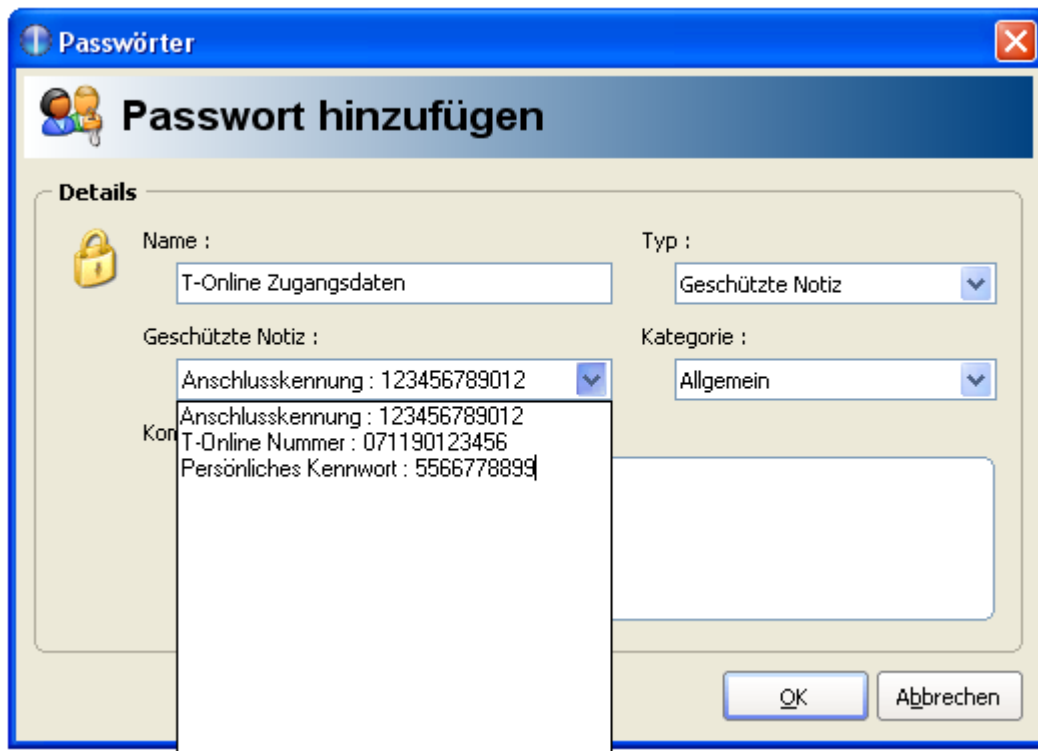


Abbildung 33. Eingabe einer mehrzeiligen, geschützten Notiz

Hier können Sie beliebig viele Textzeilen eingeben und so Ihre Angaben besser formatieren.

Optional kann von Ihnen noch ein Kommentar vergeben werden. Die Kommentarzeilen werden immer beim Auswählen eines Passworteintrages offen angezeigt und dienen einer genaueren Beschreibung oder für zusätzliche Information wie z.B. einer Telefonnummer.

Jedes Passwort kann einer Kategorie zugeordnet werden. Diese dient der besseren Übersicht. Wählen Sie entweder eine bestehende Kategorie aus der Auswahlliste, oder erstellen Sie Ihre eigenen, indem Sie in der Auswahlliste „< **Neue Kategorie** >“ auswählen und dann einen beschreibenden Namen eingeben.

Wenn Sie einen Eintrag aus Ihrer Passwortliste ändern oder löschen möchten, selektieren Sie in der Liste die entsprechende Zeile und klicken Sie auf den Schalter „**Bearbeiten...**“ bzw. „**Löschen**“. Im Hauptmenü finden Sie ebenfalls unter „**Bearbeiten**“ die jeweiligen Menüpunkte.

4.3 Passwortlisten öffnen

Zum öffnen einer Passwortliste wählen Sie im Hauptmenü „**Datei**“ den Menüpunkt „**Passwortliste öffnen...**“ oder klicken auf den Schalter „**Auswählen**“. Der Standarddialog zum öffnen von Dateien wird angezeigt, über den Sie zur gewünschten Datei navigieren können.

Nachdem Sie die Datei ausgewählt haben, klicken Sie im Dialogfenster auf „**Öffen**“. Im Eingabefeld der Combobox „**Passwortliste** :“ steht nun der vollständige Dateipfad und Name.



Abbildung 34. Auswählen einer Passwortlisten Datei

Sie können den Dateipfad natürlich auch direkt in das Eingabefeld der Combobox eintragen.

Drücken Sie anschließend den Schalter „**Liste öffnen**“. Das Eingabefeld zeigt jetzt den Beschreibungstext der Passwortliste an.

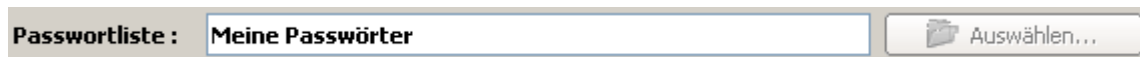


Abbildung 35. Anzeige des Beschreibungstextes einer geöffneten Passwortliste

Wenn in den PrimalCrypt-Einstellungen die Option „**Passwortlisten History speichern**“ ausgewählt ist (siehe Kapitel 8.2), wird die Dateibeschreibung in der Auswahlliste der Combobox gespeichert. Es ist deshalb wichtig, dass Sie beim Erstellen einer Passwortliste die Beschreibung eindeutig wählen, da sonst eventuell der selbe Text mehrfach in der Liste angezeigt wird.

Nach der ersten manuellen Auswahl, können Sie dann über die Combobox bequem Ihre Passwortlisten wählen.



Abbildung 36. Auswahl einer Passwortliste über die Combobox

Nach dem Öffnen der Passwortdatei haben Sie nun die Möglichkeit neue Einträge zu erstellen oder den aktuell ausgewählten Eintrag anzeigen, bearbeiten oder eventuell löschen zu können.

Die Sortierreihenfolge der Passwortliste kann geändert werden, indem Sie auf den Titelpfopf der zu sortierenden Spalte klicken. Die ausgewählte Spalte wird durch ein kleines Dreieck im Titelpfopf markiert. Ein erneuter Mausklick auf den aktuellen Titel ändert die alphanumerische Sortierung innerhalb der Spalte. Zeigt die Spitze des Dreiecks nach oben, wird in aufsteigender Reihenfolge sortiert, ein nach unten gerichtetes Dreieck zeigt eine absteigende Sortierung an.

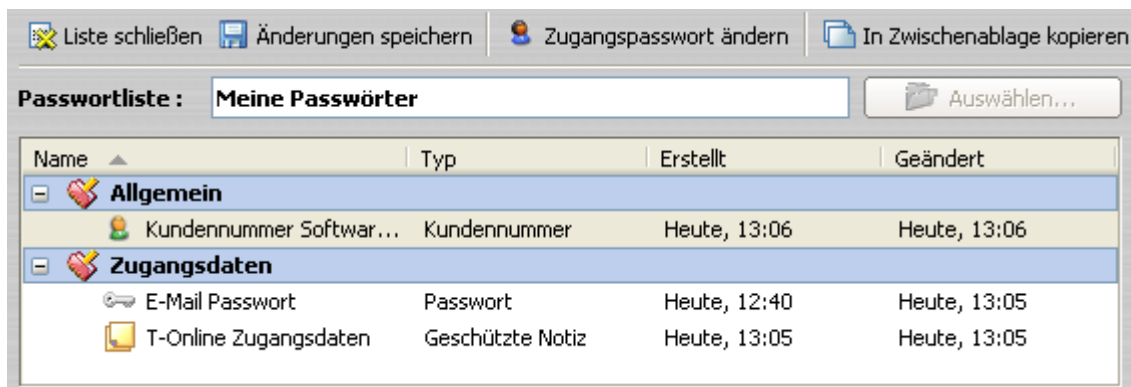


Abbildung 37. Einträge einer geöffneten Passwortliste

Die in Abbildung 37. gezeigte Liste wird also aufsteigend nach Namen sortiert.

PrimalCrypt speichert die von Ihnen eingestellte Sortierung, so dass Sie diese nicht nach jedem Programmstart erneut durchführen müssen.

Die Passworteinträge werden in den, von Ihnen vergebenen Kategorien aufgelistet. Soll aus Gründen der Übersicht eine Kategorie vollständig ausgeblendet werden, klicken Sie auf das kleine Minus Symbol im entsprechenden Eintrag. Das Symbol ändert sich in ein Plus Zeichen um anzuzeigen, dass innerhalb dieser Kategorie weitere Einträge enthalten sind. Zum einblenden dieser Einträge genügt ein weiterer Mausklick auf das Plus Symbol.

Für den aktuell ausgewählten Eintrag werden das Passwort und der Kommentar angezeigt. Das Passwort wird hierbei zunächst als eine Folge von Punkten („•“) dargestellt. Dies gilt zur Sicherheit vor den Blicken fremder Personen, die Ihnen eventuell über die Schulter schauen. Klicken Sie auf den Schalter „**Einblenden**“ um das Passwort für Sie lesbar zu machen. Ein erneuter Mausklick auf diesen Schalter blendet das Kennwort wieder aus.

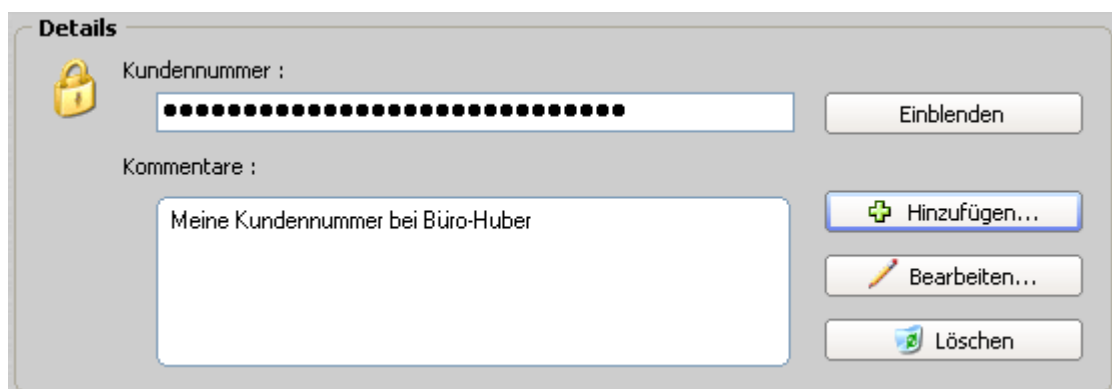


Abbildung 38. Detail anzeige für einen Passworteintrag

Wenn Sie den gewählten Passworteintrag z.B. in das Eingabefeld einer Internetseite eintragen wollen, klicken Sie einfach auf den Schalter „**In Zwischenablage kopieren**“. Das zu kopierende Passwort muss dazu nicht eingeblendet sein.

Wechseln Sie dann in Ihren Internetbrowser, fokussieren Sie das entsprechende Eingabefeld, indem Sie es anklicken und wählen dann den Menüpunkt „**Einfügen**“ über das Hauptmenü „**Bearbeiten**“. In den meisten Fällen können Sie auch die Tastenkombination **STRG** und **V** auf Ihrer Tastatur drücken.

Im PrimalCrypt Passwortdialog kann ein in die Zwischenablage kopiertes Passwort eingefügt werden, indem Sie in das Eingabefeld mit der rechten Maustaste klicken und so das Kontextmenü öffnen (auch das funktioniert bei den meisten anderen Programmen). Wählen Sie dann den Menüpunkt „**Einfügen**“. Auch hier hat die Tastenkombination **STRG-V** die gleiche Bedeutung.

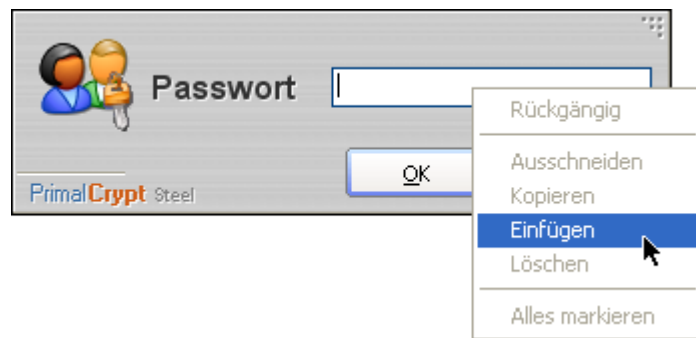


Abbildung 39. Einfügen eines kopierten Passwortes über das Kontextmenü

Sie können jederzeit das Zugangspasswort einer geöffneten Passwortliste ändern. Klicken Sie hierzu auf den Schalter „**Zugangspasswort ändern...**“ und geben Sie dann im Passwortdialog das neue Kennwort ein.

Eine geöffnete Passwortliste kann nach einer voreingestellten Zeit automatisch geschlossen werden (siehe Kapitel 8.2). Dies dient zu Ihrem Schutz, falls Sie einmal Ihren Arbeitsplatz verlassen und vergessen haben die Passwortliste wieder zu schließen. Falls Sie Änderungen in der Liste vorgenommen haben, werden diese dann (je nach Einstellung) ohne Rückfrage zuvor gespeichert.

Sie sollten aber möglichst immer durch drücken des Schalters „**Liste schließen**“ den Zugriff auf Ihre Passwörter sperren, wenn Sie diese nicht mehr benötigen.

Passwortlisten können auch über das PrimalCrypt Taskleistensymbol geöffnet oder geschlossen werden. Klicken Sie mit der rechten Maustaste auf das PrimalCrypt Schlüsselsymbol in der Taskleiste. Im Kontextmenü wählen Sie dann „**Passwortliste öffnen...**“ bzw. „**Passwortliste schließen**“. Diese zwei Menüpunkte finden Sie auch im Hauptmenü „**Datei**“ der PrimalCrypt-Applikation.

5 Schlüsselverwaltung

Die Schlüsselverwaltung ist die zentrale Stelle, um Schlüsseldateien und Zertifikate zu kopieren oder neu zu erstellen.

Wurde z.B. eine Schlüsseldatei zerstört oder versehentlich gelöscht, so können Sie in der Schlüsselverwaltung mit Hilfe des Hauptschlüsselzertifikats diesen Schlüssel neu anlegen.

Um in die Schlüsselverwaltung zu gelangen, wählen Sie im Hauptmenü „**Datei**“ den Menüpunkt „**Passwörter & Schlüssel verwalten...**“ oder klicken in der linken Menüleiste unter der Kategorie „**Passwörter & Schlüssel**“ auf „**Verwalten**“. Im Hauptfensterbereich selektieren Sie durch einen Mausklick den Tabulator „**Schlüssel**“.



Abbildung 40. Die Schlüsselverwaltung

In der Zertifikatsliste finden Sie alle bereits erstellten Schlüsselzertifikate. Direkt unter der Liste befindet sich der Verwaltungsassistent. Hier können Sie die von Ihnen gewünschte Aufgabe auswählen, indem Sie auf eine der Auswahlmöglichkeiten klicken.

5.1 Zweitschlüssel für ein Image erstellen

Nehmen wir an, Sie hätten eine Image-Datei unter dem Namen „KeyDrive.img“ erstellt. Für diese Datei haben Sie sich für den Schlüsselschutz entschieden und dem Schlüssel zusätzlich das Passwort „Urlaub1998“ vergeben.

Das Hauptschlüsselzertifikat wurde unter „a:\Keydrive Zertifikat.pcc“ abgespeichert und die Schlüsseldatei befindet sich auf einem USB-Memorystick.

Um das Image als Laufwerk zu mounten, müssen Sie jetzt nur Ihren Memorystick in eine USB-Buchse einstecken und Ihr Passwort eingeben.

Nehmen wir weiterhin an, dass Sie einer zweiten Person den Zugang zu Ihrer Image-Datei gewähren möchten. Das Kopieren der Schlüsseldatei von einem Memorystick auf einen anderen ist nicht möglich, da diese Dateien auf das Trägerlaufwerk gebündelt sind.

Die Schlüsselverwaltung bietet Ihnen nun die Möglichkeit, entweder einen Zweitschlüssel, oder ein Schlüsselduplikat zu erstellen.

Der Unterschied zwischen diesen beiden Methoden :

- Ein Schlüsselduplikat ist eine simple 1:1 Kopie einer Schlüsseldatei auf ein anderes Trägerlaufwerk. Es bezieht sich auf das gleiche Zertifikat wie das Original.
- Ein Zweitschlüssel erhält eine vollständig neue Zertifikatsdatei. Diese bezieht sich auf das gleiche Image wie das Original, kann jedoch ein unterschiedliches Zusatzpasswort erhalten.

Schauen wir nochmals auf unser Beispiel. Sie haben dort das zusätzliche Passwort „Urlaub1998“ vergeben. Dieses Passwort wird nicht im Schlüssel selbst, sondern im zugehörigen Zertifikat gespeichert. Falls Sie das Passwort auch für andere geschützte Daten einsetzen, werden Sie es sicherlich nicht einer anderen Person verraten wollen. Dies müssten Sie aber, wenn Sie nur eine Schlüsselkopie erstellen würden, denn Sie hätten zwar nun zwei Schlüssel, aber immer noch nur ein passendes Zertifikat.

Durch den Zweitschlüssel erhält jeder Benutzer seinen eigenen, persönlichen Schlüssel samt zugehörigen Zertifikat und einem eventuell vergebenen Zusatzpasswort.

Noch offensichtlicher wird der Unterschied zwischen Kopie und Zweitschlüssel für den Fall, dass sich die Image-Datei auf einem im Netzwerk stehenden Dateiserver befindet.

Beide Benutzer möchten auf ihrem jeweils eigenen Arbeitsrechner auf diese Datei zugreifen, diese also über das Netzwerk als Laufwerk mounten. Eine Schlüsselkopie wäre für diesen Fall überhaupt nicht möglich. Das für eine simple Kopie zugehörige Zertifikat befände sich nämlich auf einem anderen Rechner. Der Zweitschlüssel kann hingegen auf dem Rechner des zusätzlichen Benutzers erstellt werden und erhält dort auch seine Zertifikatsdatei.

Klicken Sie im Verwaltungsassistenten auf den Eintrag **„Einen Zweitschlüssel für ein Image erstellen“**.

Auf der zweiten Seite des Assistenten müssen Sie nun den vollständigen Pfadnamen zum Hauptschlüsselzertifikat (HSZ) der Image-Datei eingeben. Befindet sich das HSZ auf einer Diskette, legen Sie diese in das Diskettenlaufwerk ein. Geben Sie dann in das Eingabefeld den Dateipfad und Namen ein, oder klicken Sie auf den Schalter **„Auswählen...“** um die Datei mit Hilfe eines Auswahldialogs zu suchen.

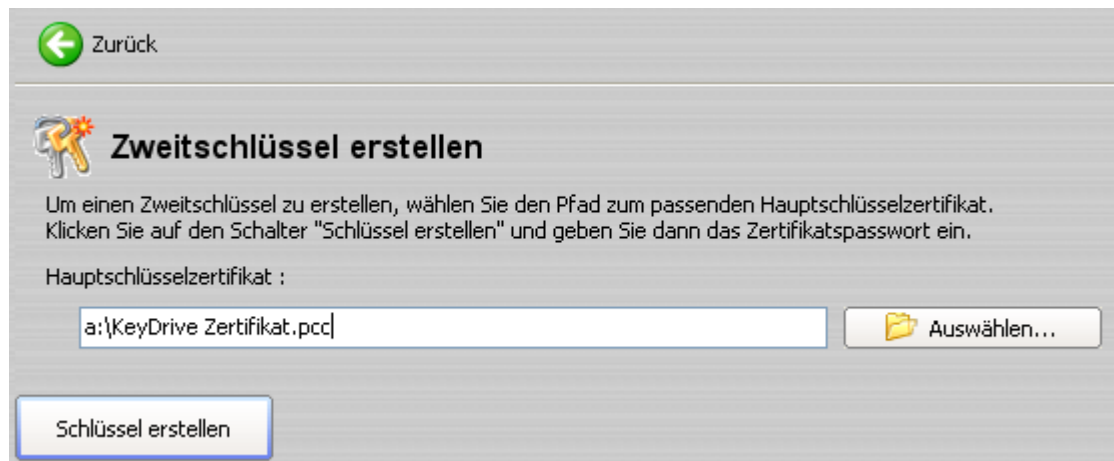


Abbildung 41. Erstellen eines Zweitschlüssels

Klicken Sie danach auf den Schalter „**Schlüssel erstellen**“. Sie werden nach dem Passwort des Hauptschlüsselzertifikats gefragt. Nach dem Bestätigen der Eingabe gelangen Sie in das Dialogfenster zum Erstellen eines neuen Hauptschlüsselzertifikats. Geben Sie hier den Speicherort und das Passwort für das **neue** HSZ ein und klicken Sie auf den Schalter „**OK**“.

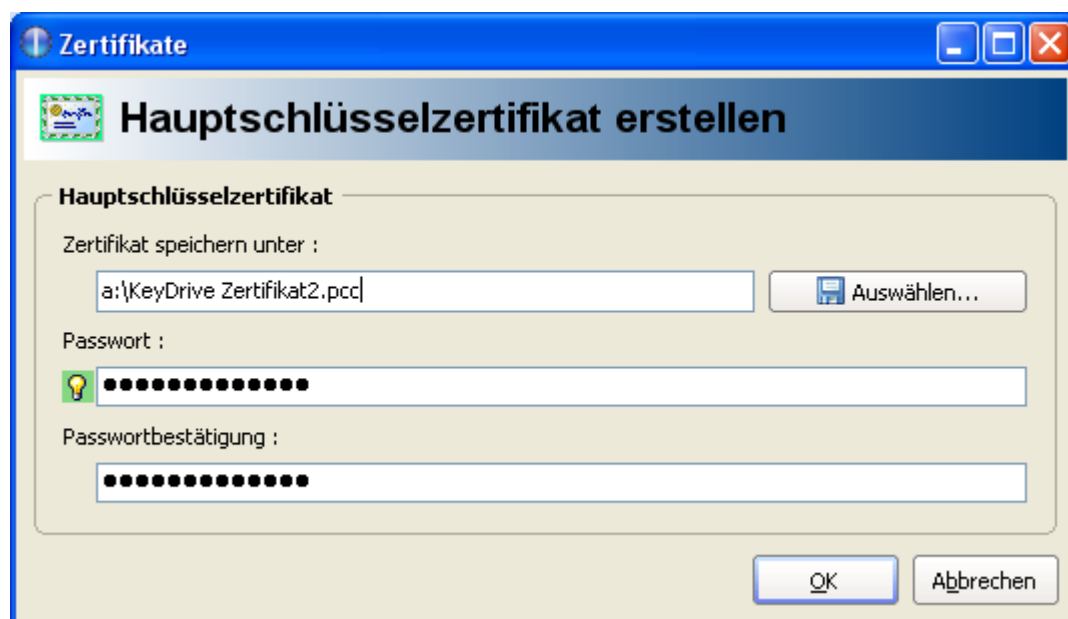


Abbildung 42. Erstellen eines neuen Hauptschlüsselzertifikats

Das neu erstellte Hauptschlüsselzertifikat dient später zur Reparatur des Zweitschlüssels oder des zugehörigen Schlüsselzertifikats.

Im letzten Schritt benötigt PrimalCrypt von Ihnen noch die Angaben, wo sich die Image-Datei befindet und auf welchem Trägerlaufwerk die neue Schlüsseldatei abgelegt werden soll.

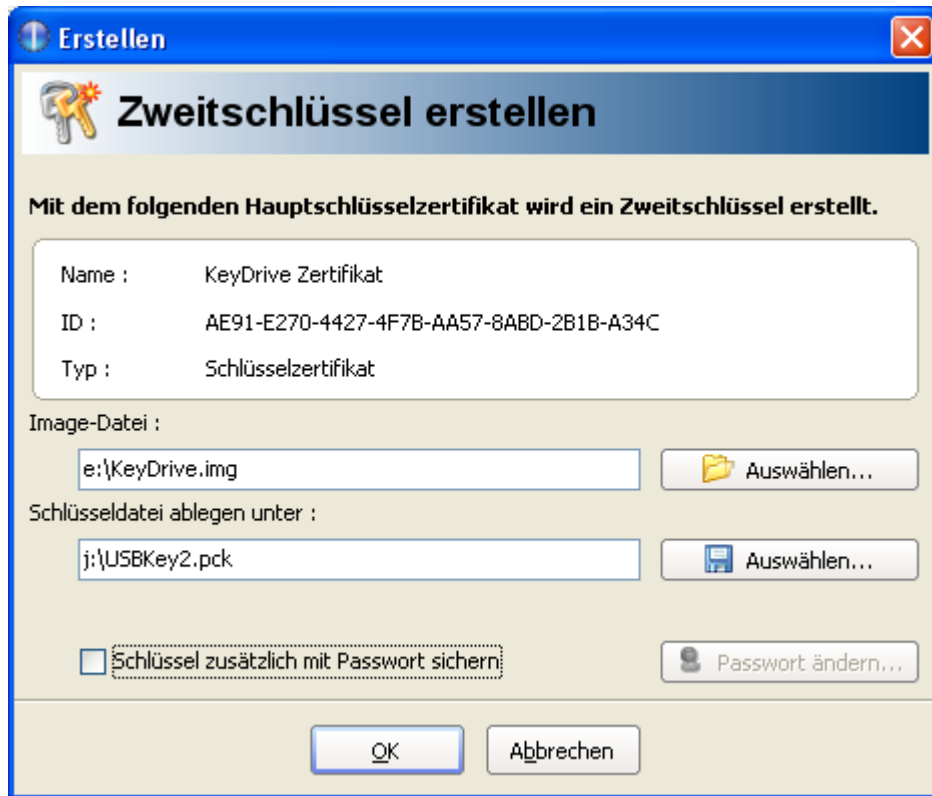


Abbildung 43. Dialogfenster zum erstellen eines Zweitschlüssels

Befindet sich die Image-Datei auf einem Dateiserver im Netzwerk, geben Sie entweder den vollständigen UNC-Dateipfad (z.B. „\\NetServer\Daten\Images\KeyDrive.img“) oder falls für das Freigabeverzeichnis eine Laufwerksverknüpfung erstellt wurde, die übliche – mit einem Laufwerksbuchstaben beginnende – Pfadangabe ein (z.B. „S:\KeyDrive.img“).

Die neue Schlüsseldatei muss sich wieder auf einem automatisch erkennbaren Datenträger (USB-Festplatte, Memorystick etc.) befinden. Soll der Schlüssel aus Sicherheitsgründen ein zusätzliches, oder neues Passwort erhalten, wählen Sie die Option **„Schlüssel zusätzlich mit Passwort sichern“**. Klicken Sie auf den Schalter **„Passwort ändern...“** und geben dann das neue Kennwort ein.

Betätigen Sie abschließend den Schalter **„OK“** um den Zweitschlüssel zu erstellen. Sie können nun weitere Zweitschlüssel erstellen oder durch einen Mausklick auf den **„Zurück“** Schalter wieder zum Hauptfenster des Verwaltungsassistenten gelangen.

5.2 Schlüssel duplizieren oder reparieren

Wenn Sie eine persönliche Sicherungskopie eines Schlüssels benötigen (z.B. auf einem anderen USB-Stick) oder eine Schlüsseldatei beschädigt oder gelöscht wurde, wählen Sie im Verwaltungsassistenten den Eintrag **„Einen Schlüssel duplizieren, oder einen beschädigten oder gelöschten Schlüssel neu erstellen“**. Sie gelangen auf die zweite Seite des Assistenten, auf der Sie gebeten werden den Pfad zu Ihrem passenden Hauptschlüsselzertifikat einzugeben.

Nach erfolgter Eingabe klicken Sie auf den Schalter **„Schlüssel erstellen“**.

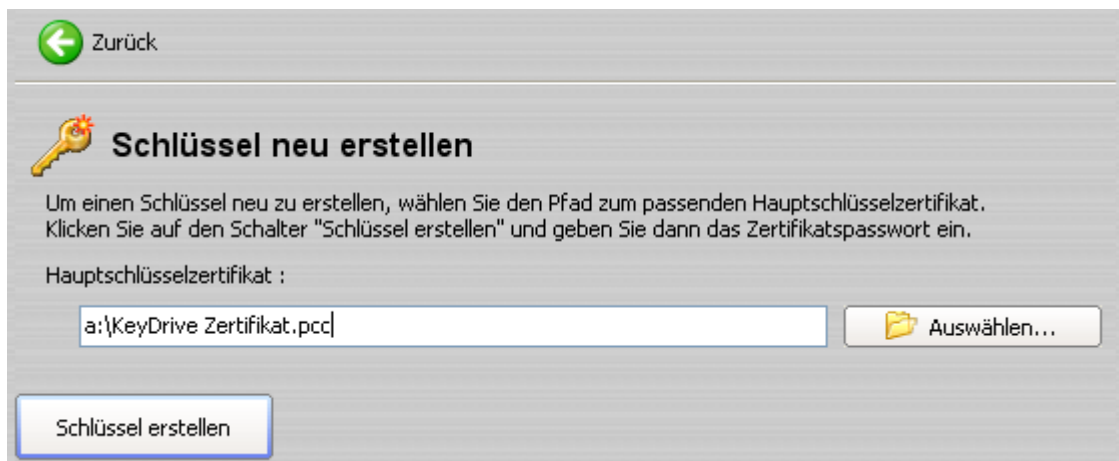


Abbildung 44. Erstellen eines Schlüssel Duplikates

Sie werden nach dem Passwort des Hauptschlüsselzertifikats gefragt, und gelangen nach dem Bestätigen der Eingabe in das Dialogfenster zum Erstellen eines neuen Schlüssels. Geben Sie den Dateipfad und Namen der neuen Schlüsseldatei ein. Das Trägerlaufwerk muss wie immer, von Windows automatisch erkennbar sein. Klicken Sie abschließend auf „OK“, um die Schlüsselkopie zu erstellen.

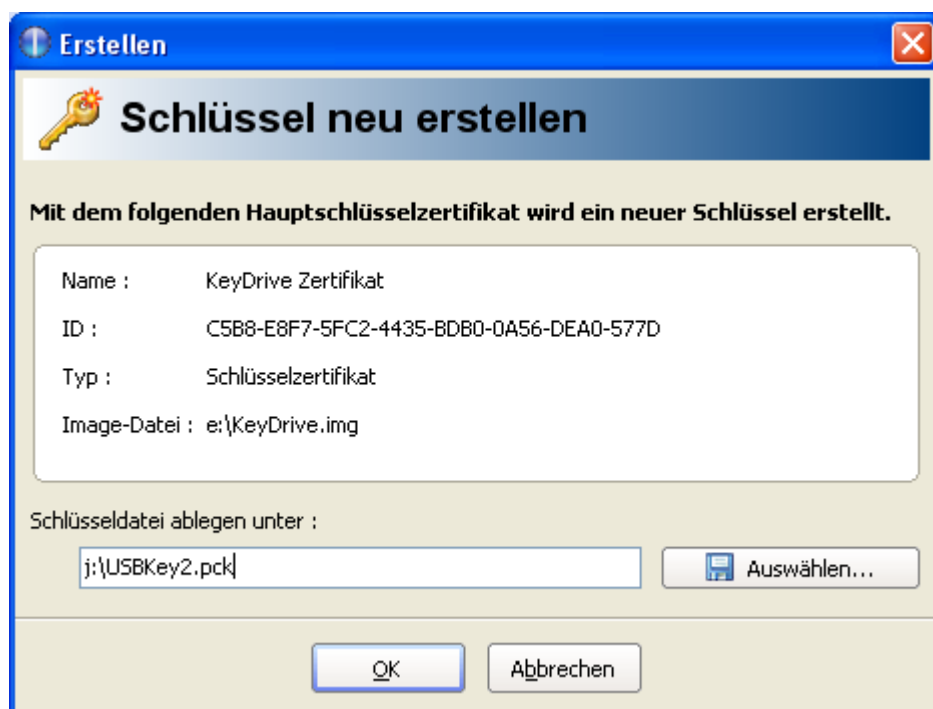


Abbildung 45. Dialogfenster zum Erstellen eines Schlüssel Duplikates

Sie können nun weitere Schlüssel Duplikate erstellen oder durch einen Mausklick auf den Schalter „Zurück“ wieder zum Hauptfenster des Verwaltungsassistenten gelangen.

5.3 Zertifikate übertragen oder reparieren

Wenn ein Schlüsselzertifikat beschädigt oder gelöscht wurde, Sie auf einen anderen Rechner umziehen müssen, oder das Zusatzpasswort einer mit einem Schlüssel geschützten Image-Datei ändern möchten, wählen Sie im Verwaltungsassistenten den Punkt **„Ein Zertifikat auf einen anderen Rechner übertragen, oder ein beschädigtes oder gelöscht Zertifikat neu erstellen“**.

Auf der zweiten Seite des Verwaltungsassistenten geben Sie dann den vollständigen Dateipfad zum passenden Hauptschlüsselzertifikat in das Eingabefeld ein.

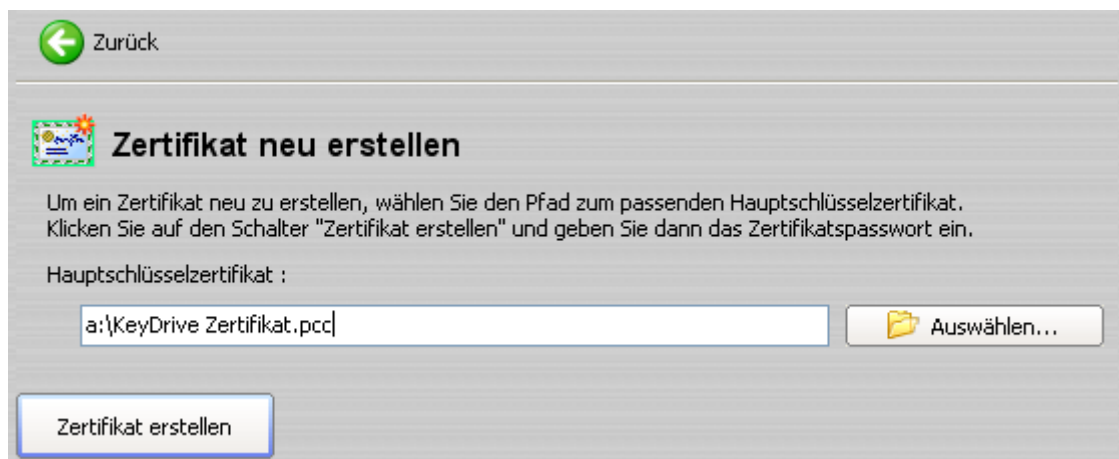


Abbildung 46. Erstellen eines neuen Zertifikats

Klicken Sie danach auf **„Zertifikat erstellen“** und bestätigen Sie die Passwortabfrage für Ihr Hauptschlüsselzertifikat.

Sie können nun noch ein zusätzliches Kennwort für das neue Zertifikat vergeben. Wählen Sie hierzu im Erstellungsdialog die Option **„Schlüssel zusätzlich mit Passwort sichern“**, klicken auf den Schalter **„Passwort ändern...“** und geben Sie dann das neue Passwort ein.

Durch klicken auf den Schalter **„OK“** wird das neue Zertifikat erstellt.

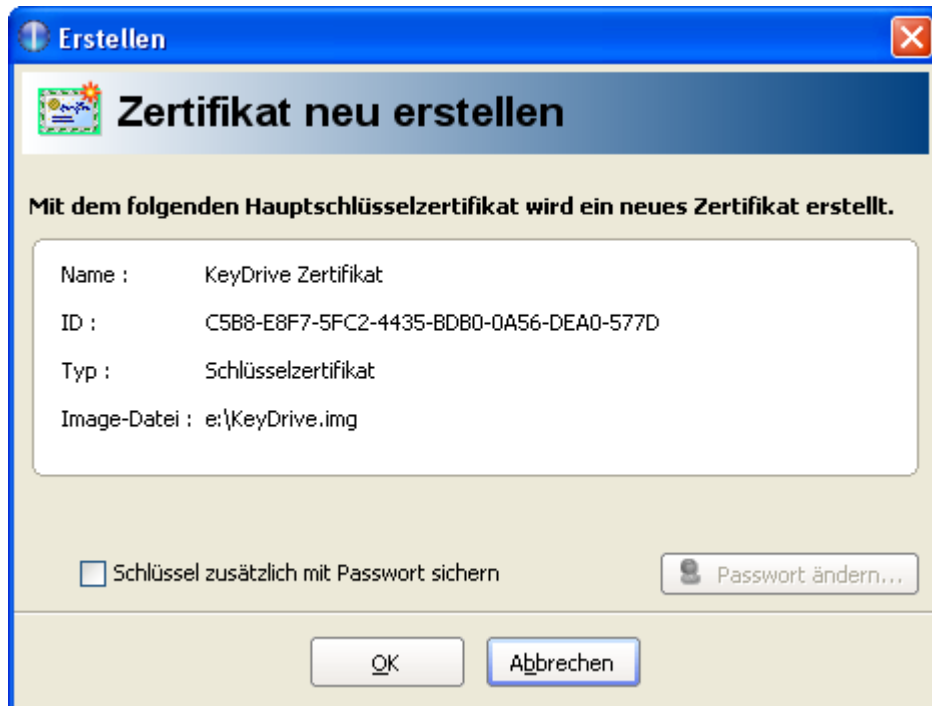


Abbildung 47. Dialogfenster zum erstellen eines Schlüsselzertifikats

Wenn Sie mit PrimalCrypt auf einen neuen Arbeitsrechner umziehen, oder die Festplatte tauschen müssen, können Sie Ihre Image-Dateien einfach dorthin kopieren. Die Zertifikate sind aber so kodiert, dass sie nur auf der Festplatte gültig sind, auf der sie erstellt wurden. Deshalb ist es notwendig, dass Sie die Zertifikate mit dem Verwaltungsassistenten neu erstellen. Sie müssen aber beachten, dass die neu erstellten Zertifikate den ursprünglichen Dateipfad zu ihren jeweiligen Image-Dateien behalten. Lag die Image-Datei auf Ihrem alten Rechner z.B. im Pfad „d:\Images“, so muss sie auch auf dem neuen Rechner auf das Laufwerk „D:“ und in das Verzeichnis „\Images“ kopiert werden. Ist dies nicht möglich, weil in Ihrem neuen Rechner keine Partition mit dem entsprechenden Laufwerksbuchstaben existiert, müssen Sie stattdessen einen Zweitschlüssel erstellen. Für einen Zweitschlüssel wird ebenfalls ein neues Zertifikat angelegt, bei dem Sie aber noch den Pfad zu Ihrer Image-Datei angeben können.

Wurde einer Schlüssel geschützten Image-Datei ein zusätzliches Passwort vergeben und dieses soll geändert oder gelöscht werden, gehen Sie bitte folgendermaßen vor:

- Löschen Sie zunächst - wie in Kapitel 5.4 beschrieben – das für Ihren Schlüssel und die Image-Datei passende Zertifikat.
- Erstellen Sie ein neues Zertifikat und geben Sie entweder das geänderte Passwort ein, oder schalten Sie - falls Sie kein Zusatzpasswort mehr möchten - die Option „**Schlüssel zusätzlich mit Passwort sichern**“ ab.

5.4 Zertifikate löschen

Wird eine Image-Datei nicht mehr benötigt, so kann ein eventuell vorhandener Schlüssel und dessen Zertifikat ebenfalls gelöscht werden. Die Image- und Schlüsseldateien können direkt über den Windows-Explorer in den Papierkorb gelegt werden. Das Zertifikat müssen Sie aber in der Schlüsselverwaltung von PrimalCrypt löschen.

Wählen Sie zunächst aus der Liste das zu löschende Zertifikat aus.

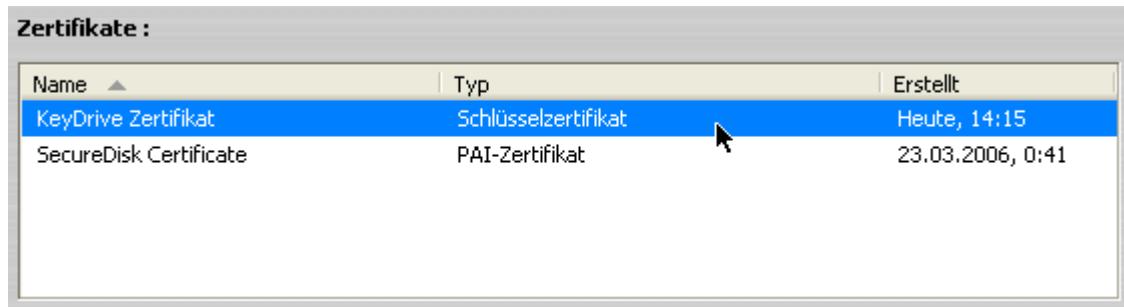


Abbildung 48. Auswählen eines Schlüsselzertifikats

Klicken Sie dann im Verwaltungsassistenten auf den Eintrag „**Zertifikat löschen**“. Auf der nächsten Seite des Assistenten müssen Sie den Löschvorgang bestätigen. Geben Sie in das Eingabefeld das Wort „**LÖSCHEN**“ (in Großbuchstaben und ohne Anführungszeichen) ein und klicken Sie danach auf den Schalter „**OK**“.

Um weitere Zertifikate zu löschen, markieren Sie diese wieder in der Liste und bestätigen den Vorgang erneut durch Eingabe der Sicherheitsabfrage.

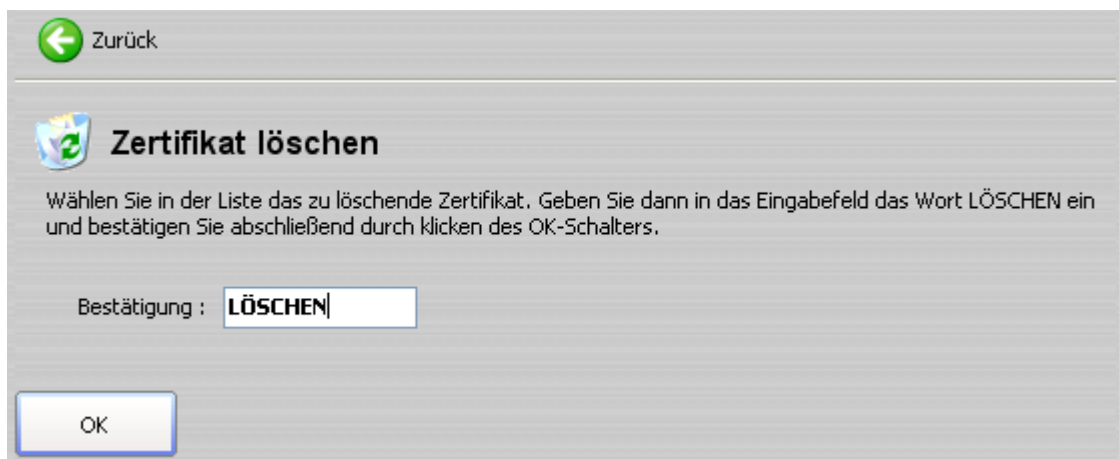


Abbildung 49. Löschen eines Zertifikats

Versehentlich gelöschte Zertifikate können Sie, wie in Kapitel 5.3 beschrieben wieder neu erstellen.

6 Sicheres Löschen

Manchmal ist es notwendig, seine Festplatte und somit eventuell persönliche Daten wie z.B. Familienbilder oder Textdokumente aus der Hand zu geben. Muss Ihr Rechner einmal repariert werden, oder Sie haben vor, Ihre alte Festplatte an eine andere Person zu verschenken, so werden Sie sicherlich diese besonderen Daten vor all zu neugierigen Blicken schützen wollen.

Löschen der Dateien unter Windows stellt kein Hindernis dar. Mit speziellen Programmen können die Daten meist ohne Verluste wieder hergestellt werden. Auch ein Formatieren der Festplatte löscht die Daten nicht vollständig.

PrimalCrypt bietet mit dem „Shredder“ ein Programmmodul, mit dem eben solche Daten sicher und unwiederbringlich gelöscht werden können. Hierzu werden die Dateien nach dem vom U.S Department of Defence aufgestellten Standard zum beseitigen von Dateien (DOD 5220.22-M) überschrieben. Dieser Standard schreibt vor, dass die Daten auf einem Festplattenmedium durch ein festgelegtes Zeichen (z.B 0), danach mit einem per Zufallsgenerator gebildeten Zeichen und zum Schluss mit dem Komplement des im ersten Durchlaufs festgelegten Zeichens überschrieben werden.

Hierdurch wird sichergestellt, dass ein Programm zum Wiederherstellen gelöschter Dateien keine Möglichkeit hat, diese wieder lesbar zu machen. Spezialisierte Firmen zur Datenrettung können aber eventuell zumindest einen Teil der gespeicherten Informationen wiederherstellen. Diese Verfahren sind jedoch sehr teuer und für Privatpersonen wenig praktikabel. Deshalb bietet DOD 5220.22-M zumindest für den mittleren Sicherheitsbedarf einen sehr guten Schutz.

Klicken Sie in der Menüleiste unter der Kategorie „**Dateien**“ auf den Punkt „**Sicher löschen**“, oder wählen Sie unter dem Hauptmenü „**Datei**“ den Menüpunkt „**Dateien sicher löschen...**“.

PrimalCrypt wechselt zum Shredder-Modul wo wie Sie die zu löschenden Dateien und Ordner entweder per „Drag&Drop“ auf den Dateibrowser ziehen können, oder durch anklicken des Schalters „**Datei hinzufügen**“ einzelne Dateien per Dialog-Fenster auswählen können.

Um versehentlich hinzugefügte Dateien wieder aus der Auswahl zu entfernen, klicken Sie den entsprechenden Eintrag an (mit gedrückter STRG-Taste können auch mehrere Einträge ausgewählt werden) und betätigen dann den Schalter „**Dateien entfernen**“. Über „**Alle Dateien entfernen**“ wird die Liste vollständig geleert.

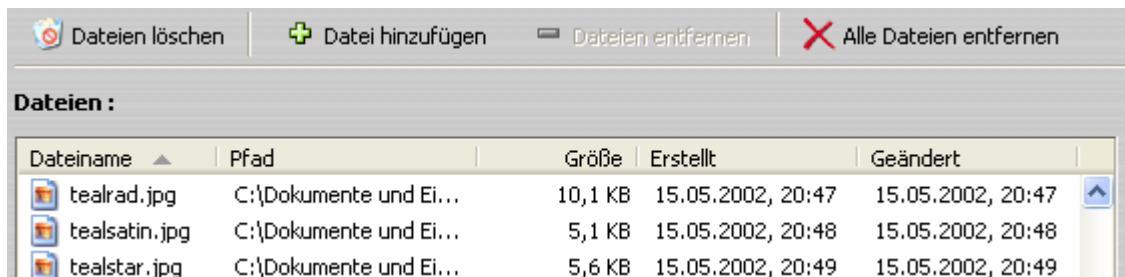


Abbildung 50. Sicheres löschen von Dateien

Um die in der Shredder-Auswahl befindlichen Dateien zu löschen, klicken Sie den Schalter „**Dateien löschen**“ und bestätigen danach die Sicherheitsabfrage.

7 Steganografie

Eine weitere Möglichkeit, persönliche Daten vor dem Zugriff durch andere Personen zu schützen ist, diese zu verstecken. Während die Dateiverschlüsselung die Daten unleserlich macht, werden bei der sog. Steganografie (griech. „verdeckt schreiben“) die eigentlichen Daten so verborgen, dass deren Existenz nicht auffällt. Dies wird z.B. erreicht, indem man die geheime Botschaft in eine unwichtige hinein mischt.

In PrimalCrypt können Sie Dateien mit dem Steganografie-Modul in Bildern verstecken. Dabei werden die Datenbits der zu versteckenden Dateien in die einzelnen Farbwerte des Trägerbildes geschrieben. Pro Bildpunkt werden in einer Bilddatei mit 24 Bit Farbtiefe drei Bytes (ein Byte = 8 Bit) benötigt, nämlich für jede der drei Grundfarben (Rot, Grün und Blau) ein Byte. An jedes Farbbyte kann ein einzelnes Bit der geheimen Botschaft angehängt werden, ohne dass die Änderung einem Betrachter auffallen würde. Bei einem Bild mit einer Größe von 1024 x 768 Bildpunkten können also $1024 \times 768 \times 3 \text{ Bit} = 2.359.296 \text{ Bit}$ oder 294.912 Byte (288 KB) der geheimen Botschaft untergebracht werden. Davon werden von PrimalCrypt noch 12 Bytes für Verwaltungsdaten abgezogen. Da in PrimalCrypt die zu versteckenden Daten noch komprimiert werden, können Sie (je nach möglichem Grad der Komprimierung) zum Teil die dreifache Menge an Daten unterbringen.

Zusätzlich besteht die Möglichkeit, die Daten zuvor zu verschlüsseln. Somit können Sie sicher sein, dass selbst wenn die Daten entdeckt werden, diese nicht ohne weiteres lesbar sind.

Um in das Steganografie-Modul zu gelangen, klicken Sie in der Menüleiste in der Kategorie „**Dateien**“ auf den Eintrag „**Verstecken**“. Alternativ gelangen Sie über das Hauptmenü „**Datei**“ und dem Menüpunkt „**Dateien verstecken...**“ hierher.

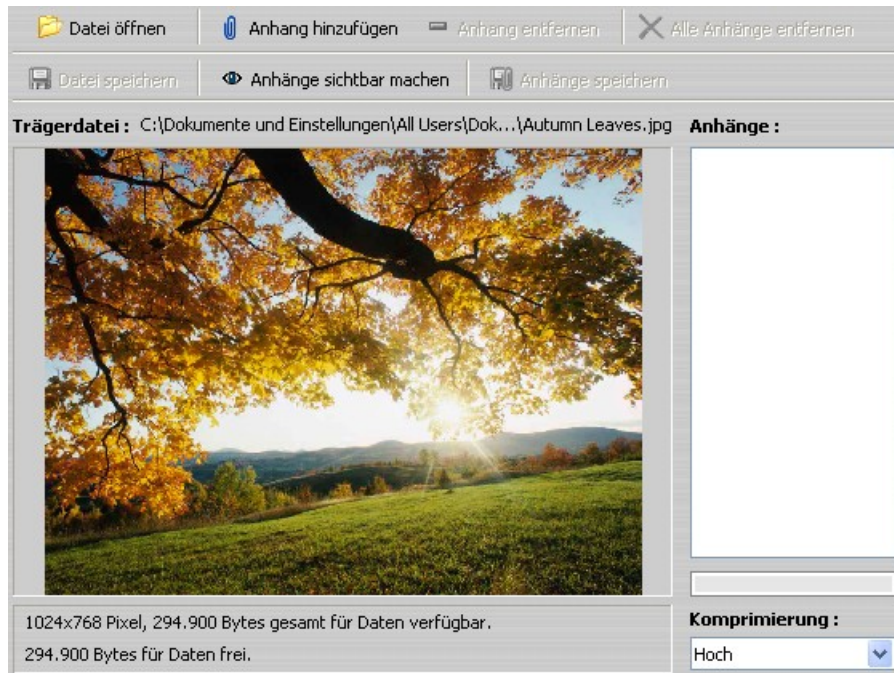


Abbildung 51. Geöffnete Trägerdatei im Steganografie-Modul

7.1 Dateien verstecken

Zuerst müssen Sie eine Trägerdatei (also das Bild in dem Ihre Daten versteckt werden sollen) öffnen. Klicken Sie dazu auf den Schalter „**Datei öffnen**“ und wählen Sie ein Bild aus.

PrimalCrypt kann die meisten, gängigen Bildformate öffnen. Gespeichert werden die Bilder aber immer im Bitmap-Format, da hier die eigentliche Bilddaten nicht in komprimierter Form vorliegen.

Im unteren Fensterbereich sehen Sie Informationen zur Größe des Bildes und der Anzahl der maximalen und der freien Datenbytes. Direkt daneben befindet sich eine Combobox, in der Sie den Grad der Komprimierung einstellen können. Im Normalfall können Sie die voreingestellte hohe Komprimierung belassen.

Ein Balken zeigt Ihnen grafisch den belegten, bzw. den noch freien Speicherplatz an. Ganz rechts befindet sich die Dateiliste für die angehängten Dateien.

Um eine Datei in dem ausgewählten Bild zu verstecken, klicken Sie auf den Schalter „**Anhang hinzufügen**“ oder ziehen Sie diese per Drag&Drop auf die Dateiliste.

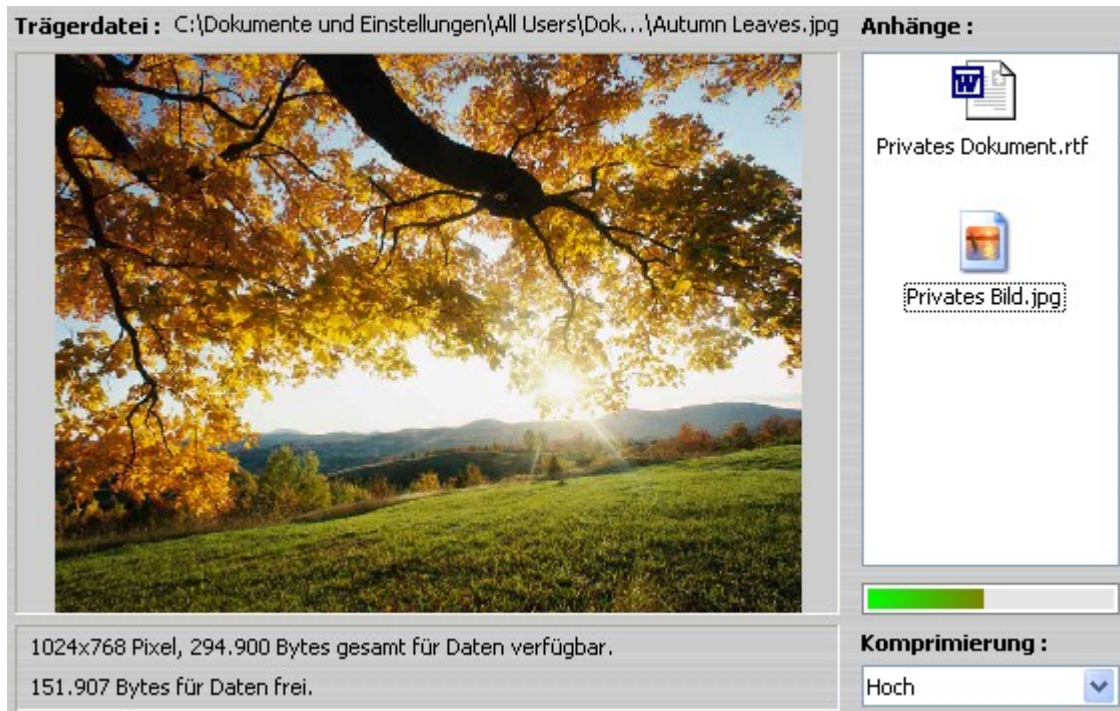


Abbildung 51. Geöffnete Trägerdatei mit zwei Anhängen in der Dateiliste

Möchten Sie einen oder mehrere Anhänge wieder entfernen, markieren Sie diese(n) und klicken auf **„Anhang entfernen“**. Mit dem Schalter **„Alle Anhänge entfernen“** wird die Dateiliste vollständig geleert.

Wenn alle Dateien angehängt wurden, müssen Sie das Trägerbild noch speichern. Klicken Sie auf **„Datei speichern“**. Sie werden zunächst nach einem Passwort gefragt, mit dem die Anhänge verschlüsselt werden sollen.

Wünschen Sie keine Verschlüsselung, so lassen Sie die Eingabefelder einfach frei. Ansonsten tragen Sie ein Passwort ein und bestätigen die Richtigkeit durch erneute Eingabe. Klicken Sie auf **„OK“**. Als letzten Schritt müssen Sie noch den Speicherort und den neuen Dateinamen für das Bild angeben.



Beachten Sie bitte, dass die Trägerdatei nicht mehr mit einem Bildeditor bearbeitet werden darf. Wird auch nur ein Bildpunkt geändert, so können dadurch alle versteckten Dateien unbrauchbar gemacht werden.

Schließen Sie das geöffnete Trägerbild, indem Sie einen Mausklick mit der rechten Taste auf den Bildbereich machen und dann im Kontextmenü **„Datei schließen“** auswählen.

Nun können Sie das Bild z.B. per E-Mail an eine eingeweihte Person versenden, die aus diesem die geheimen Daten mit PrimalCrypt wieder sichtbar machen kann.

7.2 Versteckte Dateien sichtbar machen

Um Ihre Dateien wieder sichtbar zu machen, öffnen Sie das Bild in dem Sie die Daten

versteckt haben. Klicken Sie als nächstes auf den Schalter **„Anhänge sichtbar machen“**. Wenn die angehängten Dateien verschlüsselt wurden, werden Sie nun zur Eingabe des Passwortes aufgefordert. Unverschlüsselte Anhänge werden sofort in der Dateiliste angezeigt.

Sie können nun entweder neue Anhänge hinzufügen, bereits angehängte Dateien entfernen, oder die Dateien wieder auf Ihre Festplatte speichern.

Zum speichern klicken Sie auf den Schalter **„Anhänge speichern“**. Wurde zuvor keine Datei aus der Liste markiert, werden Sie nun aufgefordert einen Ordner auf Ihrer Festplatte auszuwählen, in dem alle angehängten Dateien gespeichert werden sollen.

Bei einzeln markierten Dateien können Sie nicht nur den Speicherort, sondern auch einen eventuell neuen Dateinamen angeben.



Wenn Sie das Trägerbild behalten möchten, die versteckten Daten aber nicht mehr benötigen, entfernen Sie am besten alle Anhänge und speichern das Bild erneut unter dem gleichen Namen.

8 Einstellungen

Um in das Einstellungsfenster von PrimalCrypt zu gelangen, wählen Sie im Hauptmenü **„Bearbeiten“** den Menüpunkt **„Einstellungen“** oder klicken in der linken Menüleiste unter der Kategorie **„Einstellungen“** auf **„Allgemein“**.

Im Bereich des Hauptfensters sehen Sie die verschiedenen Konfigurationsmöglichkeiten. Wurden von Ihnen diverse Einstellungen geändert und sollen diese dauerhaft übernommen werden, klicken Sie auf den Schalter **„Einstellungen speichern“**. Beim Beenden von PrimalCrypt gehen nicht gespeicherte Einstellungen verloren, Sie werden auch nicht nochmals gefragt, ob die Änderungen übernommen werden sollen. Falsch vorgenommene Einstellungen können sofort durch einen Mausklick auf den Schalter **„Änderungen verwerfen“** rückgängig gemacht werden.

8.1 Zugangspasswort

Sie können PrimalCrypt vor unbefugten Zugriffen ganz oder teilweise schützen, indem Sie ein Zugangspasswort vergeben.

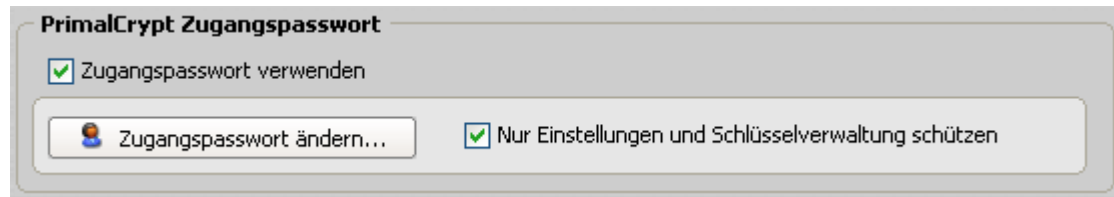


Abbildung 52. Einstellung Zugangspasswort

Klicken Sie auf „**Zugangspasswort verwenden**“. Sie werden sofort zur Eingabe eines neuen Zugangspasswortes aufgefordert. Ein einmal vergebenes Passwort können Sie durch klicken auf den Schalter „**Zugangspasswort ändern...**“ jederzeit umbenennen. Wenn Sie ein Zugangspasswort verwenden, werden Sie jedes mal wenn das PrimalCrypt-Fenster geöffnet wird, zur Eingabe dieses Kennwortes aufgefordert. Sie können aber auch nur einzelne Bereiche schützen lassen. Wählen Sie hierzu „**Nur Einstellungen und Schlüsselverwaltung schützen**“, es erfolgt dann nur eine Passwortabfrage, wenn Sie entweder in die PrimalCrypt-Einstellungen oder in die Schlüsselverwaltung wechseln. Alle anderen Bereiche bleiben frei zugänglich.

8.2 Passwortlisten

Wurde von Ihnen eine Passwortliste geöffnet, so besteht die Gefahr, dass Sie Ihren Arbeitsplatz verlassen und dabei vergessen die Liste wieder zu schließen. PrimalCrypt kann das für Sie automatisch nach einer voreingestellten Zeit erledigen.

Klicken Sie die Option „**Passwortlisten automatisch schließen**“ an. Geben Sie die gewünschte Zeit (in Minuten), nach deren Ablauf PrimalCrypt eine geöffnete Liste wieder sperren soll in das Eingabefeld ein. Über den Up-/Down Schalter, rechts neben dem Eingabefeld können Sie den Wert in Minuten Schritten erhöhen oder verringern.

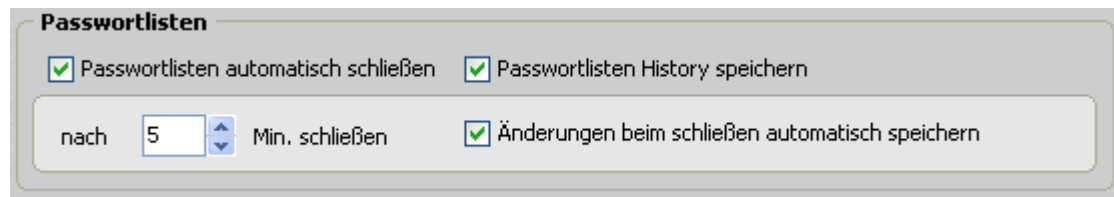


Abbildung 53. Einstellungen für Passwortlisten

Wurden in einer Passwortliste Änderungen vorgenommen, diese aber bis zum Zeitpunkt des automatischen Schließens nicht gespeichert, so fragt PrimalCrypt vor dem Schließen, ob die Änderungen übernommen werden sollen. Solange diese Abfrage nicht bestätigt wurde, bleibt die Liste geöffnet und somit für Alle zugänglich.

Wählen Sie deshalb auch die Option „**Änderungen beim schließen automatisch speichern**“. So gehen Ihre neu erstellten oder geänderten Passworteinträge nicht verloren und Sie können sicher sein, dass nach Ablauf der voreingestellten Zeit keine fremden Personen Zugriff auf Ihre Passwörter erhalten.

PrimalCrypt hält einmal geöffnete Passwortlisten in einer Combobox zur Auswahl bereit. Sie müssen dann nicht mehr den Pfad zu der zu öffnenden Datei eingeben, sondern brauchen lediglich den gewünschten Eintrag aus der gespeicherten Auswahl anklicken.

Möchten Sie dies aus Sicherheitsgründen vermeiden (um z.B. niemanden einen Hinweis auf das Vorhandensein einer Passwortliste zu geben), so schalten Sie die Option „**Passwortlisten History speichern**“ einfach ab. Die Auswahlliste bleibt dann leer und eventuell gespeicherte Einträge werden gelöscht.

8.3 Laufwerke

Genau wie bei Passwortlisten, speichert PrimalCrypt für gemountete Image-Dateien die Pfade in einer Combobox ab. Diesen „Schnellzugriff“ können Sie durch Ausschalten der Option „**Image-Datei History speichern**“ unterbinden. Dies bietet den Vorteil, dass Sie Ihre Images in einem Unterverzeichnis auf der Festplatte verstecken können und fremde Personen über die Auswahlliste keinen Hinweis auf den Speicherort dieser Dateien erhalten.

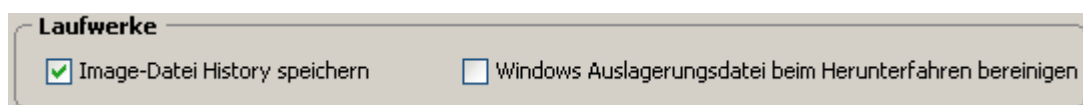


Abbildung 54. Einstellungen für Laufwerke

Grundsätzlich behält PrimalCrypt von Ihnen eingegebene Passwörter so kurz wie möglich im Hauptspeicher. Wird ein Passwort nicht mehr benötigt, füllt PrimalCrypt den Speicherbereich, in dem der Text abgelegt war mit Zufallszahlen. Schädlingsprogrammen, die den Speicher nach Kennwörter absuchen, wird das Auffinden somit erheblich erschwert, wenn nicht sogar unmöglich gemacht.

Als Schwachstelle bleibt die Auslagerungsdatei von Windows. Da Windows ein Multitask-Betriebssystem ist, wechseln sich die gerade laufenden Programme in kurzen Zeitabständen ab, um vom Prozessor oder anderen Betriebsmitteln bedient zu werden. Dabei

kann es vorkommen, dass nicht genügend physikalischer Speicher (RAM / Hauptspeicher) vorhanden ist, um den Bedarf des vom Prozessor ausgewählten Programmes zu decken. Windows wählt in diesem Fall einen gerade nicht benötigten Speicherbereich aus und kopiert die darin enthaltenen Daten in den virtuellen Speicher. Dieser befindet sich in Form der Auslagerungsdatei auf der Festplatte.

Im normalen Betrieb verhindert Windows den Zugriff durch andere Programme auf diese Datei. Wird die Festplatte aber unter einem anderen Betriebssystem wie z.B. Linux gemountet, kann der Inhalt der Auslagerungsdatei ohne besondere Vorkehrungen nach Passwörtern oder anderen wichtigen Daten durchsucht werden. Wurde PrimalCrypt also während einer Passwortabfrage von einem anderen Programm verdrängt und der Speicherbereich, in dem das Kennwort abgelegt war in die Auslagerungsdatei geschrieben, so besteht die Möglichkeit, dass fremde Personen Zugriff darauf erhalten.

Um dies zu verhindern, kann PrimalCrypt Windows anweisen, die Auslagerungsdatei beim Herunterfahren des Betriebssystems mit Null-Zeichen zu füllen.

Wenn Sie durch besonders erhöhten Sicherheitsbedarf von dieser Möglichkeit Gebrauch machen müssen, wählen Sie die Einstellungsoption „**Windows Auslagerungsdatei beim Herunterfahren bereinigen**“.

8.4 DropCrypt Einstellungen

PrimalCrypt bietet mit der Zusatzapplikation DropCrypt die Möglichkeit, Dateien durch einfaches „Drag & Drop“ auf ein Desktop-Symbol zu ver- und entschlüsseln.

Um DropCrypt nutzen zu können, müssen Sie in den PrimalCrypt-Einstellungen zuerst die Option „**DropCrypt verwenden**“ aktivieren.

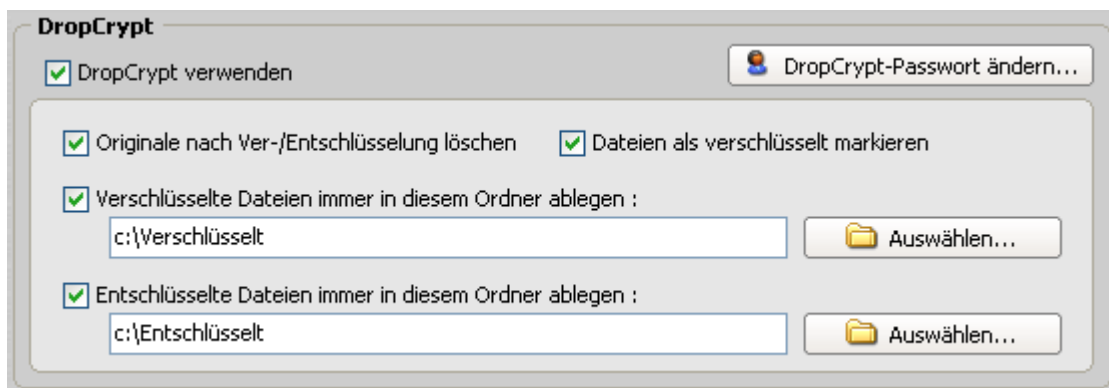


Abbildung 55. DropCrypt Einstellungen

Sie werden sofort aufgefordert ein DropCrypt-Passwort für die Dateiverschlüsselung einzugeben. Durch anklicken des Schalters „**DropCrypt-Passwort ändern...**“ können Sie das vergebenen Passwort jederzeit neu eingeben.

Schalten Sie die Option „**Verschlüsselte Dateien in diesem Ordner ablegen :**“ ein, wenn Sie möchten, dass die durch DropCrypt verschlüsselten Dateien in einem bestimmten Verzeichnis abgelegt werden sollen. Geben Sie den Pfad zu diesem Verzeichnis entweder

direkt in das Eingabefeld ein, oder drücken Sie den Schalter „**Auswählen**“ um den Ordner mit Hilfe eines Auswahldialogs zu bestimmen.

Für entschlüsselte Dateien können Sie ebenfalls ein bestimmtes Ablageverzeichnis auswählen.

Schalten Sie die Option „**Dateien als verschlüsselt markieren**“ ein, wenn Sie möchten, dass verschlüsselte Dateien mit der Endung „.pxx“ versehen werden sollen. Die alte Dateiendung wird hierbei mit einem Unterstrich an den Dateinamen angehängt (z.B. „MeinText_txt.pxx“).

Mit der Option „**Originale nach Ver-/Entschlüsselung löschen**“ bestimmen Sie, ob eine Datei, nachdem sie verschlüsselt bzw. entschlüsselt wurde, von der Festplatte gelöscht werden soll.

- Wenn Sie die Optionen zum Speichern der verschlüsselten, bzw. entschlüsselten Dateien in einen anderen Laufwerkspfad nicht gewählt haben, die Original Dateien aber gelöscht werden sollen, so wird die Originaldatei einfach ersetzt.
- Soll die Original Datei nicht gelöscht werden, so wird die verschlüsselte, bzw. entschlüsselte Datei in dem selben Verzeichnis wie das Original abgelegt. Bei nicht gesetzter Option „Dateien als verschlüsselt markieren“ wird der Dateiname durch den Zusatz „Kopie“ erweitert (also z.B. „Bild1.bmp“ zu „Bild1 Kopie.bmp“).
- Werden die ver-/entschlüsselten Dateien in ein anderes Verzeichnis als das des Originals gespeichert, wird der gleiche Dateiname übernommen. Existiert bereits eine andere Datei mit dem gleichen Namen, so wird die neu hinzugefügte mit einer bei „1“ beginnenden, fortlaufenden Nummer gekennzeichnet (z.B. Bild1_1.bmp).

Wenn DropCrypt aktiviert wurde, erscheint nach dem Speichern der Einstellungen das DropCrypt-Symbol auf Ihrem Windows-Desktop. Nach dem Deaktivieren von DropCrypt verschwindet dieses Symbol wieder.

9 Taskleistensymbol

Nach der Installation von PrimalCrypt befindet sich im Autostart Ordner (Startmenü → Programme → Autostart) ein Verweis auf das PrimalCrypt-Hauptprogramm. Bei jedem Windows Start wird PrimalCrypt also automatisch geladen. Sie finden danach in der Taskleiste ein kleines Schlüsselsymbol. Solange dieses Symbol angezeigt wird, läuft PrimalCrypt im Hintergrund und überwacht, ob eventuell ein USB-Memorystick mit einer Schlüsseldatei an Ihren Rechner angeschlossen wird.

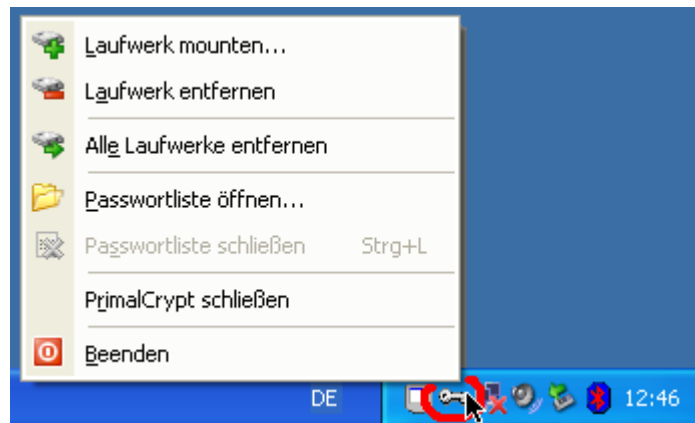


Abbildung 56. PrimalCrypt Taskleistensymbol mit geöffneten Kontextmenü

Das Hauptfenster wird nach dem Autostart zunächst nicht angezeigt.

Wenn sie nun mit der **linken** Maustaste auf das Taskleisten-Symbol klicken, öffnet sich das PrimalCrypt Hauptfenster. Sie können das Fenster dann entweder über das Schließkreuz (der kleine Schalter rechts oben im Fenstertitel) oder über das Hauptmenü „**Datei**“, Menüpunkt „**Schließen**“ wieder unsichtbar machen. Dadurch wird PrimalCrypt nicht beendet. Wenn Sie das Programm vollständig beenden möchten, klicken Sie im Hauptmenü „**Datei**“ auf den Menüpunkt „**Beenden**“.

Wird das Taskleistensymbol mit der **rechten** Maustaste angeklickt, öffnet sich ein kleines Kontextmenü über das Sie einige, auch im Hauptmenü verfügbare Aktionen auswählen können.

10 Updates

PrimalCrypt wird immer wieder weiterentwickelt. Gerne nehmen wir auch die Wünsche und Änderungsvorschläge der Benutzer in unsere Entwicklungen mit auf.

Updates oder neue Vollversionen erhalten Sie über das Internet. Hierzu benutzen Sie einfach unseren Update-Downloader „Up2Date“. Sie können das Programm entweder über das Windows-Startmenü (Start → Programme → SES → SES Up2Date) oder direkt aus PrimalCrypt heraus aufrufen (Hauptmenü „Hilfe“, Menüpunkt „Nach Updates suchen...“).

Sofort nach dem Aufruf versucht das Programm eine Internet-Verbindung zum Update-Server aufzubauen. Sollten Sie eine Firewall installiert haben, müssen Sie eventuell noch bestätigen, dass SES Up2Date ein Zugriff auf das Internet erlaubt wird.

Wenn Sie Up2Date aus PrimalCrypt heraus gestartet haben, wird nur nach Updates für Up2Date selbst und für PrimalCrypt gesucht. Wurde der Update-Downloader über das Startmenü geöffnet, so wird eine Liste der verfügbaren Updates für alle installierten Programme von ApteryX oder SES geladen.

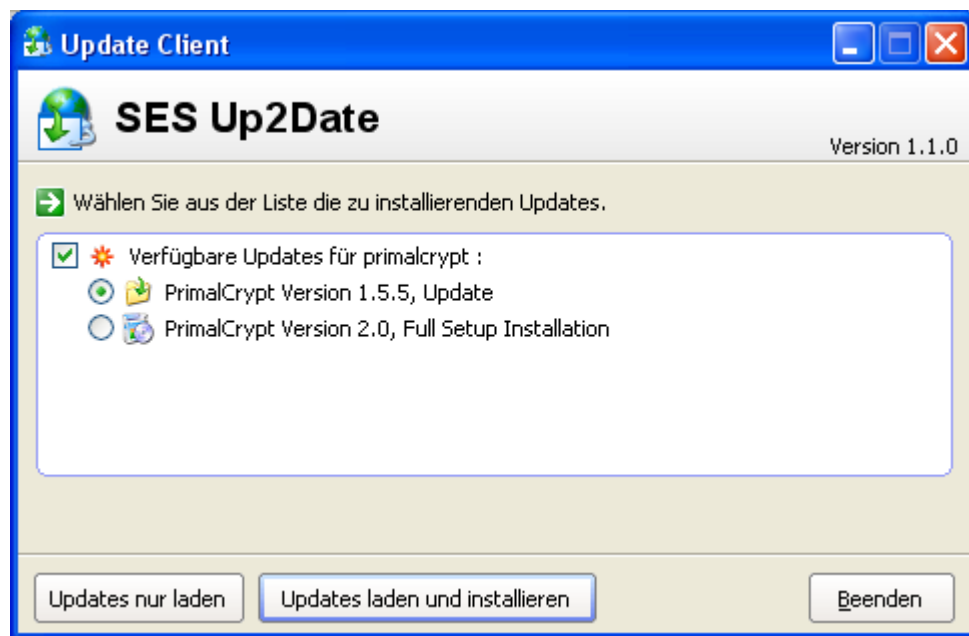


Abbildung 57. SES Up2Date

Sind für ein Produkt mehrere Update Versionen verfügbar, markieren Sie das Update, welches Sie benötigen (in Abbildung 57 z.B. PrimalCrypt Update auf Version 1.5.5).

Sie können immer kostenlos auf eine Version mit gleicher Hauptversionsnummer updaten. Programmpackete mit einer höheren Hauptversionsnummer sind dagegen immer kostenpflichtig, d.h. Sie benötigen eine neue Lizenzierung zur Freischaltung aus dem Demomodus. Ein Update von Version 1.2 auf 1.9 ist also kostenlos, auf Version 2.0 jedoch nicht.

Sollen die ausgewählten Updates zunächst nur geladen, aber nicht installiert werden,

klicken Sie auf **„Updates nur laden“**. Beim nächsten Start von Up2Date werden Sie darauf hingewiesen, dass eine Installation noch aussteht und Sie können diese dann noch nachträglich ausführen.

Wenn die Installation gleich nach dem Download der Dateien erfolgen soll, klicken Sie auf **„Updates laden und installieren“**.

Sollte der Download wegen Übertragungsproblemen mit einem Fehler beendet werden, starten Sie Up2Date gegebenenfalls ein paar Minuten später erneut.

11 Installation, Deinstallation und Registrierung

Nach der Installation von PrimalCrypt befindet sich das Programm im Demonstrations Modus. Sie können es zeitlich unbegrenzt mit einigen funktionalen Einschränkungen benutzen. Diese Einschränkungen sind im Einzelnen :

- Verschlüsselte Image-Dateien/Laufwerke können max. 25MB groß sein.
- Es werden nur Image-Dateien bis zu einer max. Größe von 25MB gemountet.
- Es ist nur ein Demoschlüssel für Image-Dateien verfügbar (siehe Kapitel 2.1.5 über Schlüssel geschützte Image-Dateien).
- In Passwortlisten können max. 4 Passwörter gespeichert werden.
- Bei den Funktionen Sicheres Löschen und Dateien verschlüsseln/entschlüsseln können immer nur max. 2 Dateien gleichzeitig bearbeitet werden.
- Im Steganografiemodul wird nur ein Anhang pro Trägerdateien akzeptiert.
- DropCrypt ist deaktiviert.

11.1 Registrierung

Um die Funktionen von PrimalCrypt vollständig nutzen zu können, müssen Sie das Programm zuerst registrieren. Öffnen Sie hierzu den Registrierungsbrowser über das Hauptmenü „**Hilfe**“ und dem Menüpunkt „**PrimalCrypt registrieren...**“.

Im Registrierungsbrowser klicken Sie zunächst auf den Schalter „**Schlüssel ermitteln**“.

Sie werden nun aufgefordert, die Ausführungsstufe auszuwählen.

PrimalCrypt ist in drei Stufen verfügbar.

1. **Vollversion.** Das Programm enthält keine Einschränkungen.
2. **Standardversion.** Die Funktionen „Sicheres Löschen“ und „Dateien verstecken“ sind nur im Demo-Modus ausführbar.
3. **Family Version.** Bis auf die Funktionen „Passwortlisten“ und „Verschlüsselte Laufwerke“ sind alle anderen Funktionen nur im Demo-Modus anwendbar.

Wählen Sie in der Combobox eine der Ausführungsstufen und klicken Sie auf „**OK**“.

Als nächstes werden die Registrierungsnummer und der bereitgestellte Registrierungsschlüssel angezeigt. Wenn Sie mit der Registrierung einverstanden sind, klicken Sie auf den Schalter „**Schlüssel bestätigen**“. PrimalCrypt wurde nun als neu Registriert eingestuft.

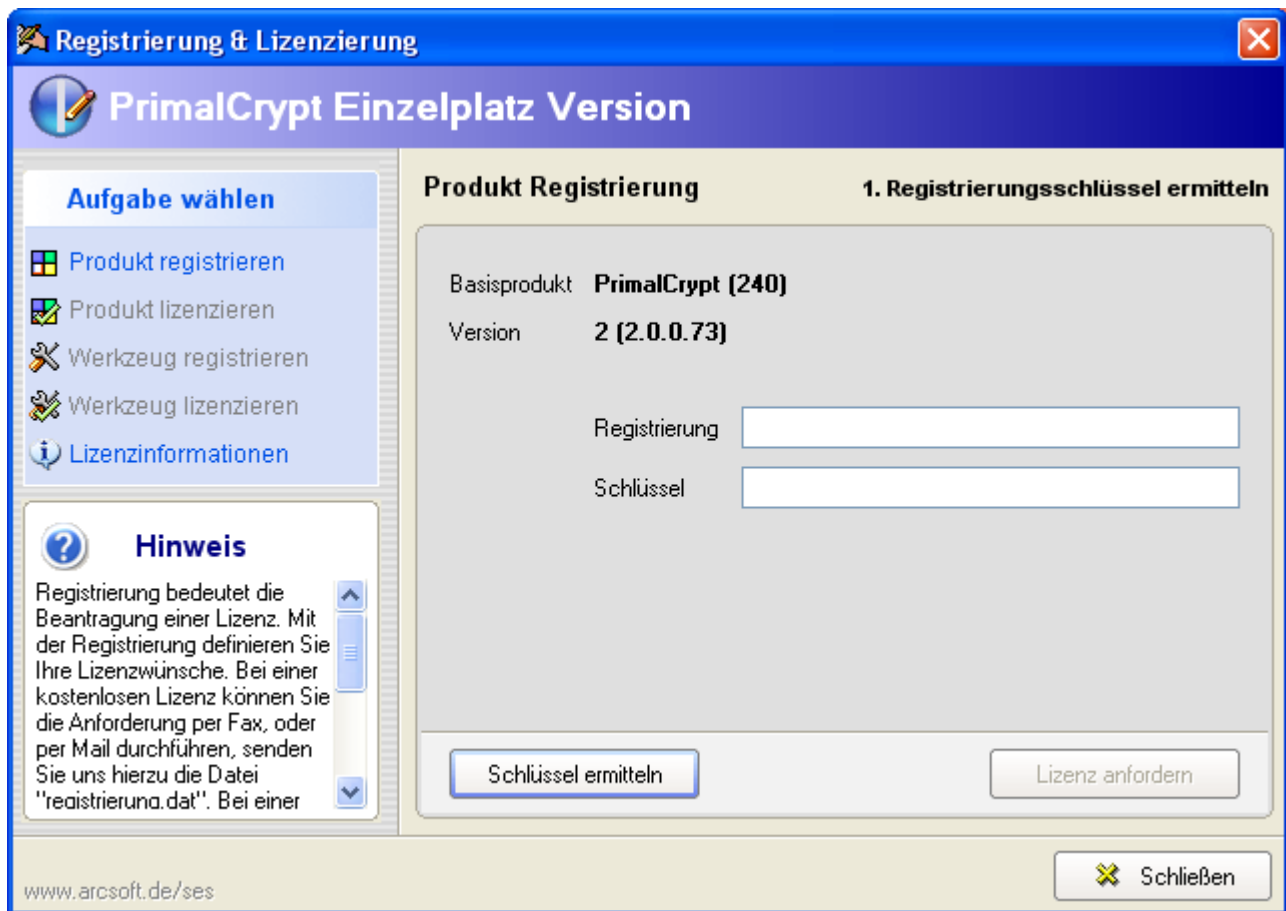


Abbildung 58. Registrierungsbrowser

Fordern Sie nun noch eine Lizenz an, indem Sie den entsprechenden Schalter anklicken. Geben Sie in der Lizenzanforderung die benötigten Daten ein und klicken Sie auf „**Weiter**“.

Sie sehen nun nochmals die ermittelten Registrierungsdaten. Möchten Sie Änderungen vornehmen klicken Sie bitte auf „**Zurück**“ ansonsten auf „**Auftrag faxen**“ um einen Lizenzierungsauftrag zu drucken. Dieses Formular senden Sie dann bitte rechtsverbindlich unterschrieben per Fax oder Post an die angegebene Fax Nummer bzw. Adresse.

Nachdem Sie das Auftragsformular gedruckt haben, werden Sie zum Speichern der Registrierungsdatei aufgefordert. Merken Sie sich bitte den Speicherort, den diese Datei sollten Sie zur schnelleren Bearbeitung Ihres Auftrages als E-Mail Anhang an die Adresse registration@arcsoft.de senden.

Sie erhalten schnellstmöglich eine Auftragsbestätigung mit allen Daten die Sie für eine Überweisung des Rechnungsbetrages benötigen. Nach Eingang der Überweisung senden wir Ihnen umgehend per E-Mail eine Lizenzierungsdatei. Mit dieser Datei wird dann PrimalCrypt für die von Ihnen lizenzierte Ausführungsstufe freigeschaltet.

11.2 Lizenzierung

Zum einlesen der Lizenzierungsdatei gehen Sie bitte folgendermaßen vor :

- Speichern Sie die erhaltene Lizenzierungsdatei auf Ihrer Festplatte. Diese Datei ist im Zip-Format komprimiert.
- Entpacken Sie die im Zip-Format vorliegende Datei mit einem entsprechenden Programm wie zum Beispiel WinZip.
- Öffnen Sie PrimalCrypt und wählen Sie im Hauptmenü „**Hilfe**“ den Menüpunkt „**PrimalCrypt lizenzieren...**“.
- Im Registrierungsbrowser klicken Sie den Schalter „**Lizenzdatei einlesen...**“.
- Wählen Sie im Windows Öffnen-Dialog die zuvor entpackte Lizenzierungsdatei.
- Klicken Sie den Schalter „**Lizenzieren**“.

Möchten Sie eventuell eine höhere Ausführungsstufe als die zuvor von Ihnen gewählte Registrieren/Lizenzieren, so können Sie dies jederzeit im Registrierungsbrowser tun.

11.3 Installation und Deinstallation

Soll PrimalCrypt wieder deinstalliert werden, machen Sie dies bitte immer über die Systemsteuerung (Start → Systemsteuerung → Software) um auch Einträge aus der Registrierungsdatenbank und Dateien im Windows Systemordner zu entfernen.

Nach einer Deinstallation befindet sich der PrimalCrypt Programmordner noch auf Ihrer Festplatte (im Normalfall C:\Programme\SES\PrimalCrypt). In diesem Ordner sind noch Dateien wie z.B. die Programmeinstellungen oder die Lizenzierungsdatei enthalten.

Wenn PrimalCrypt neu installieren, werden diese Dateien beibehalten. D.h. Sie müssen beim Vorhandensein einer Lizenzdatei keine erneute Lizenzierung vornehmen.

Möchten Sie, dass PrimalCrypt vollständig von der Platte entfernt wird, müssen Sie den genannten Ordner manuell löschen.

Sie können eine Neuinstallation von PrimalCrypt erst dann ausführen, wenn eine eventuell bereits vorhandene Version zuvor deinstalliert wurde. Führen Sie ein Update auf eine neue Vollversion mit SES Up2Date aus, wird die alte Version automatisch entfernt.

Copyright © 2006 J. Walke ApteryX Software Research und Kaiser ArcSoft GmbH
Wollerweg 18
70329 Stuttgart

Einige Programme oder Programmteile wurden in Kooperation zwischen den Firmen ApteryX Software Research und Kaiser ArcSoft erstellt. Dieser Kooperationszusammenschluss wird von den Beteiligten Firmen als Softwareentwicklung Stuttgart (kurz SES) bezeichnet.

*Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten.
Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung durch eines der Kooperationsmitglieder von SES urheberrechtswidrig und daher strafbar.*

*Alle Informationen in diesem Buch wurden mit größter Sorgfalt kontrolliert.
Weder der Autor noch die Firmen ApteryX Software Research und Kaiser ArcSoft können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.*

In diesem Handbuch werden eingetragene Warenzeichen, Handelsnamen und Gebrauchsnamen verwendet. Auch wenn diese nicht als solche gekennzeichnet sind, gelten die entsprechenden Schutzbestimmungen. So ist Windows ein eingetragenes Warenzeichen von Microsoft, Inc.