DriveCrypt 4.2

SECURE HARD DISK ENCRYPTION

© 2003 SecurStar

Table of Contents

© 2003 SecurStar

© 2003 SecurStar

© 2003 SecurStar

© 2003 SecurStar

1 Willkommen

1.1 Einleitung

DriveCrypt

Mit dem Programm DriveCrypt kann man auf allen Microsoft Betriebssystemen virtuell verschlüsselte Laufwerke erstellen. DriveCrypt erstellt hierbei einen Container auf der Festplatte und meldet diesen im System an. Hierbei wird ein neuer logischer Laufwerksbuchstabe vergeben, über den auf den erstellten Container wie auf eine Festplatte zugegriffen werden kann. Die wichtigste Funktion hierbei stellt die Verschlüsselung aller Daten mit einem Algorithmus Ihrer Wahl dar. Alle Daten, die in das neue logische Laufwerk geschrieben werden, werden hierbei verschlüsselt.

DriveCrypt ist das schnellste und in seinen Funktionalitäten das flexibelste "Echtzeit" Festplattenverschlüsselungsprogramm, das derzeit auf dem Markt erhältlich ist. Besondere Sorgfalt wurde darauf gelegt, die Vorgänge der Verschlüsselung selbst so gut wie möglich versteckt und im Hintergrund zu halten.

Wie die Echtzeit Verschlüsselung von DriveCrypt funktioniert:

Wenn die Daten von der Platte gelesen werden, entschlüsselt diese DRIVECRYPT vollautomatisch, befor sie in den Speicher geladen werden. Wenn die Daten zurückgeschrieben werden, so findet wiederum eine vollautomatische Verschlüsselung statt. Diese Prozesse sind völlig unsichtbar für den Benutzer oder andere Applikationen.

In Folge dessen braucht der Benutzer nicht an die Entschlüsselung und Verschlüsselung zu denken. Auch braucht er keinerlei Veränderungen an der Funktionsweise seines PC´s vorzunehmen. Es werden immer nur die benötigten Daten entschlüsselt (nie die komplette Platte).

© 2003 SecurStar

1.2 Hauptfunktionen

Einige der Hauptfunktionen von DriveCrypt:

1) DriveCrypt bietet Militär-Kryptographie durch seine 1344-Bit Datenverschlüsselung.
Es werden die besten und bewährtesten Verschlüsselungsalgorithmen benutzt wie: AES, Blowfish, TEA 16, Tea 32, DES, Triple DES und Misty 1.

2) Sehr schnelle "Echtzeit" Verschlüsselung. Die Daten bleiben zu jeder Zeit auf der Festplatte verschlüsselt und werden nur bei Benutzung in Echtzeit vom Prozessor entschlüsselt.

3) DriveCrypt kann sowohl virtuelle Container als auch ganze Festplattenpartitionen (DriveCrypt Standardversion) erstellen und verschlüsseln.

4) Die DRIVECRYPT Standard Edition kann unsichtbare Laufwerke in einem verschlüsselten Container erstellen. Hier werden zwei Passwörter für einen Container vergeben. Das Passwort des versteckten Laufwerks gibt Ihnen den Zugang auf Ihre Arbeitsplatte, welche in den ungenutzen Bereichen Ihres Containers versteckt ist. Ein anderes Passwort gibt Ihnen nur Zugang zu Ihrem "Grundcontainer", in dem Sie nur Daten speichern, welche Sie beruhigt an dritte weitergeben können. Jeder wird denken, dass dies die einzigen verschlüsselten Daten sind. Das ist sehr nützlich, wenn Sie jemand zwingen sollte, Ihr Passwort für den Container rauszugeben. Indem Sie dem Gegner nur das eine Passwort geben, wo er nur die Daten findet, die Sie ihn sehen lassen wollen: z. B. Daten, die Sie dort hineingespeichert haben, befor Sie das versteckte Laufwerk im Container erstellt haben. Er wird nicht zweifeln, dass es keine weiteren Daten mehr gibt.

5) Verschlüsselte Dateien können in einer Musikdatei (WAV-Datei) versteckt werden. Dies wird als Steganographie bezeichnet.

6) Spezielle Funktionen verhindern das Ausspionieren von Passwörtern durch trojanische Pferde und sogenannte Keyboard-Sniffer. Einige dieser trojanischen Pferde / Sniffer sind z.B. Skin98 oder Back Orifice.

7) Es ist nicht möglich zu beweisen, dass eine große, auf der Festplatte abgelegte Datei, ein virtueller Laufwerkscontainer von DriveCrypt ist,

© 2003 SecurStar

wenn nicht das hierfür richtige Passwort eingegeben wird. Die DriveCrypt Containerdateien haben keine Standard-Dateiendungen und Dateiheader, welche darauf hinweisen, dass die Dateien nicht nur aus Zufallsdaten bestehen und zu DriveCrypt gehört.

8) Verglichen mit allen Konkurrenzprodukten, wurde in DriveCrypt das Hacken mittels „brute force Attacke" sehr erschwert und zeitaufwendiger gestaltet.

9) Alle Laufwerke können bequem und schnell mittels Hotkeys im System an- und abgemeldet werden.

10) Mittels eines zweiten Passwortes ist möglich, einem weiteren Benutzer den Zugriff auf verschlüsselte Dateien zu ermöglichen. Dies kann jederzeit wieder rückgängig gemacht werden.

11) DriveCrypt erlaubt es, den freien Speicherplatz einer Festplatte unwiederbringlich zu löschen. Dies stellt sicher, das gelöschte Dateien niemals durch spezielle Festplattentools wieder hergestellt werden können.

12) Der Windows-Arbeitsbildschirm kann - mittels Hotkeys oder Screensaver - durch einen Passwortbildschirm abgesperrt werden. Dies ist besonders dann wichtig, wenn man den Arbeitsplatz verlässt und sicher gehen möchte, dass in der Zwischenzeit niemand unbefugten Zugriff auf die Daten nehmen kann. Nach der Eingabe des korrekten Passwortes wird der Ursprungszustand des Rechners blitzschnell wiederhergestellt und es kann wieder normal weitergearbeitet werden.

13) Die Größe eines verschlüsselten Laufwerkes kann jederzeit geändert werden.
(DriveCrypt Standardversion)

14) Es werden spezielle externe Hardwaregeräte wie Fingerabdruck- und SmartCard-Leser, sowie USB Token unterstützt.

15) Alte Container, die mit anderen führenden Verschlüsselungsprogrammen erstellt wurden, können ebenso geöffnet werden.

16) Jegliche Arten von Festplatten und austauschbare Medien wie Floppy-, Zip-, Jazz-, Sygate-, CD-Rom-, DVD-Geräte etc….. werden unterstützt.

17) Die DriveCrypt Standardversion kann bis zu 16 Terabyte an

© 2003 SecurStar

verschlüsselten Daten gleichzeitig verarbeiten. (Die Home-Edition 4 GB)

18) Leichte, schnelle und sichere Installation: Wärend der Installation wählt der Admin einfach die Laufwerke aus, die verschlüsselt werden sollen. Dann selektiert er die Verschlüsselungsmethode und das Master Passwort. DRIVECRYPT wird dann den Rest machen und die ausgewählten Laufwerke verschlüsseln.

19) Verschlüsselte Daten können leicht wiederhergestellt werden: Wenn ein Benutzer die Firma verlässt, können die verschlüsselten Daten seines PC´s ganz einfach wiederhergestellt werden. Dies wird von Admin gemacht, welcher einfach das Masterpasswort oder das lokale Adminpasswort verwendet.

20) Es gibt keine Hintertürchen (Backdoors): DRIVECRYPT hat KEINE HINTERTÜRCHEN. Verschlüsselte Daten sind nur von authorisierten Benutzern einsehbar. Auch der Hersteller selbst oder irgendjemand sonst kann die DRIVECRYPT Verschlüsselung durchbrechen. Lesen Sie die FAQ um mehr Infos zu bekommen.

21) DriveCrypt arbeitet auf folgenden Windowsplattformen : Windows 95/98/ME/NT/2000/XP

1.3 Daten in einer Musikdateien verbergen

DRIVECRYPT benutzt fortgeschrittene Steganographie, um sensiblen Daten in einer Musikdatei zu verbergen.

Steganographie ist die Kunst und die Wissenschaft in einer Art zu kommunizieren, welche die Existenz der Kommunikation verbirgt. Im Kontrast zu Kryptographie, bei welcher der "Feind" die Erlaubnis hat, Botschaften zu entdecken, abzufangen und zu verändern, ohne dabei gewisse Sicherheitsaspekte zu brechen, welche von einem Verschlüsselungssystem vorausgesetzt werden, ist das Ziel der Steganographie, Botschaften in anderen "harmlosen" Botschaften so zu verstecken, sodass "Feinde" gar nicht erkennen können, dass eine zweite geheime Botschaft in der "harmlosen" Botschaft vorhanden ist. Steganographie wird in der (besonders militärischen) Literatur auch als Übertragungssicherheit bezeichnet (kurz TRANSEC).

Ein gutes Steganographie-System sollte die gleichen Voraussetzungen

© 2003 SecurStar

erfüllen, wie bei der Kryptographie durch die "Kerckhoff Prinzipien" vorgegeben wird. Diese besagen, dass die Sicherheit eines Systems darauf beruhen muss, dass der "Feind" das komplette Design und die Einrichtung des steganographischen Systems kennt. Die einzig fehlende Information ist eine einfach zu ändernde Nummernsequenz, der geheime Schlüssel. Ohne diesen Schlüssel sollte der "Feind" nicht die kleinste Chance haben, bei einem überwachten Kommunikationskanal herauszufinden, dass es dort verschlüsselte Kommunikation gibt.

DRIVECRYPT kann mit der fortgeschrittenen Steganographietechnik ganze Laufwerke in Musikdateien verstecken. Es gibt viele einfache Softwaretools, mit denen man Dateien in bestimmten Bits von digitalem Bildmaterial oder PGP Nachrichten in Dateien durch Wiederherstellung von binären Zufallssequenzen verstecken kann. Aber die meisten benutzten staganographischen Programme fallen bei der genauen Analyse von den übertragenen Daten auf, und verraten um was es sich hierbei handelt.

Falls Sie DRIVECRYPT fortgeschrittene Steganographie testen wollen, erstellen Sie bitte eine 16 Bit Stereo Audiodatei. (dies geht ganz einfach mit einer Software wie "WinDAC". Mit ihr kann man Audiodateien aus Liedern einer Musik-CD erstellen. Mit DRIVECRYPT kann man daraufhin ein verschlüsseltes Laufwerk in der Musikdatei erstellen (Im Laufwerkerstellungs-Wizard muss die Funktion "Benutze Cryptographische Funktionen" aktiviert sein.)

Der durch DRIVECRYPT entstandene Musikfile stellt einen virtuellen Container dar, in welchen Dateien wie auf einer normalen Festplatte gespeichert werden können. Für unautorisierte Benutzer sieht diese Datei aus wie eine ganz normale Musikdatei.

DRIVECRYPT ist das stärkste, flexibelste und schnellste auf dem heutigen Markt erhältliche Verschlüsselungsprogramm. Es bietet militärstarke Verschlüsselung und schützt Ihre Daten auf schnelle und zuverlässige Art und Weise.

1.4 SecurStar kontaktieren

Um die neuesten Versionen und Infos´s zu unseren Programmen zu bekommen besuchen uns bitte unter:
http://www.securstar.com

Fragen können Sie uns unter support@securstar.com zukommen lassen.

© 2003 SecurStar

Wir versuchen Ihre Fragen so schnell und kompetent wie möglich zu beantworten.

Sie können uns auch über das Kontaktformular unserer Homepage erreichen:
http://www.securstar.com/contact.php

Telefonsupport wird nur gegen Anfrage gewährleistet.

Wenn Sie Ideen, Vorschläge, Kommentare, Kritik oder Fragen zu unseren Programmen haben, würden wir uns sehr freuen, von Ihnen zu hören!

1.5 Lizenzvertrag

ENDVERBRAUCHER NUTZUNGSVERTRAG

Endverbraucher Nutzungsvertrag für die SECURSTAR DRIVECRYPT Software

ACHTUNG: DIESER LIZENZVERTRAG IST EINE ÜBERSETZUNG DER UNTEN AUFGEFÜHRTEN ENGLISCHEN "EULA" (Endbenutzerlizenzvereinbarung).
DER LIZENZGEBER ÜBERNIMMT KEINERLEI HAFTUNG FÜR FALSCHE ÜBERSETZUNGEN UND WEISST AUSDRÜCKLICH DARAUF HIN, DASS SICH DER RECHTSKRÄFTIGE VERTRAG AUS DER ENGLISCHSPRACHIGEN "EULA" ERGIBT.

WICHTIG: Bevor Sie diese Software starten, installieren, benutzen, darauf zugreifen oder Funktionen einstellen, bitte diesen Vertrag unbedingt lesen:

Dieser Endverbraucher Nutzungsvertrag ("EVNV") stellt eine rechtliche Vereinbarung zwischen Ihnen (als Lizenznehmer) und der SecurStar GmbH ("Lizenzgeber") für das oben bezeichnete Softwareprodukt dar. Diese Vereinbarung gilt neben der oben genannten Computersoftware (auch als " Softwareprodukt " oder "Software" bezeichnet), auch für die zum Produkt gehörigen Medien, gedrucktes Material, sowie "Online-" oder digitale Dokumentation.

Mit der Installation, dem Kopieren oder der Nutzung dieses Softwareprodukt erklären Sie sich mit den Bedingungen dieser EVNV einverstanden. Falls Sie nicht mit diesen Nutzungsbedingungen

© 2003 SecurStar

einverstanden sind, dürfen Sie dieses Softwarteprodukt nicht verwenden.

SOFTWAREPRODUKT-LIZENZ
Dieses Softwareprodukt ist durch deutsches Urheberrecht und durch internationale Urheberrechtsvereinbarungen, sowie durch anderweitige geistige Eigentümergesetze und Vereinbarungen geschützt. Dieses Softwareprodukt wird somit nur lizenziert und nicht "verkauft".

1 . ERTEILUNG DER LIZENZ: Sie sind berechtigt, diese Software in maschinenlesbarer Form und lediglich für die als Matrize vorgeschriebene Nutzung der maßgeblichen Lizenzbedingungen, auf einem Computer als Einzelarbeitsplatz zu installieren und zu nutzen. Jede Komponente dieser Software, welche speziell auf einem Server abgelegt werden soll, darf auf einem in Ihrem Arbeitsbereich befindlichen einzelnen Server installiert werden. Jede Einzelbenutzerkomponente darf auf so vielen Arbeitsplätzen installiert werden, wie Sie Einzelplatzlizenzen lizenziert haben.

2 . BESCHREIBUNG VON ANDEREN RECHTEN UND EINSCHRÄNKUNGEN: Es ist nicht erlaubt, den Programmiercode des Softwareprodukt weder durch Nachbau, Dekompilierung, Umsetzung, Disassemblieren, noch mit anderen Möglichkeiten herzustellen oder durch Dritte herstellen zu lassen. Alleinige Ausnahme hierzu stellt geltendes Recht in Form eines Gesetzes dar, welches durch die vorher aufgezählten Einschränkungen aufgehoben werden würde.

Das Softwareprodukt ist als Einzelprodukt lizenziert.
Die in diesem Produkt eingebauten Komponenten dürfen nicht separat auf mehr als einem einzelnen Computer eingesetzt werden. Dieses Softwareprodukt sowie dessen Komponenten dürfen nicht vermietet, verpachtet, verliehen oder verteilt werden.

SOFTWAREÜBERTRAGUNG: Diese Software darf nicht an Dritte weitergegeben werden.

Kündigung: Falls die Bedingungen und Konditionen der EVNV nicht eingehalten werden, kann der Lizenzgeber diese EVNV aufkündigen. In einem solchen Fall müssen alle Kopien dieses Softwareprodukt sowie aller einzelnen Komponenten deinstalliert und gelöscht werden.

3. URHEBERRECHTSSCHTUZ: Alle Titel und Urheberrechte in und an dem Softwareprodukt (eingenommen Bilder, Fotos, Animationen, Videos, Audio, Musik, Text, "Applets" (usw), welche in dem Softwareprodukt enthalten sind), sowie das beigefügte gedruckte Material und jede Kopie dieses Softwareprodukt gehören dem

© 2003 SecurStar

Lizenzgeber oder dessen Zulieferer. Dieses Softwareprodukt ist durch Urheberrechtsgesetze und internationalen Vereinbarungen und Regelungen geschützt. Deshalb sind Sie verpflichtet dieses Softwareprodukt wie jedes andere Urheberrechtsmaterial zu behandeln. Ebenso darf das beigefügte gedruckte Material des Softwareprodukt nicht vervielfältigt werden.

Der Lizenznehmer muss akzeptieren, dass einige der in diesem Softwareprodukt benutzten Verschlüsselungsalgorithmen das maßgebliche Eigentum von anderen Personen oder Firmen ist, und hierfür eine zusätzliche Lizenz für jede kommerzielle Nutzung benötigt wird (z.B. wenn das Softwareprodukt auf einem Geschäftscomputer eingesetzt wird.) Eine weitere Lizenzpflicht ist bei dem Idee Algorithmus der Fall und muss somit von dem Lizenznehmer berücksichtigt werden.

4 . GARANTIE-AUSSCHLUSSKLAUSEL: Jede Nutzung dieser Software geschieht auf eigenes Risiko. Diese Software wird geliefert wie sie ist. "," Mit allen eventuellen Fehlern", und ohne jegliche Garantie. Der Lizenzgeber, dessen Zulieferer und Distributoren lehnen jede Garantie ab. Der Lizenzgeber übernimmt keine Garantie für die allgemeine Markttauglichkeit oder Funktionsweise, sowie für die Funktionalität des Produktes für eine besondere Zweckbestimmung. Dies umfasst auch die im Rahmen des Lizenzrechtes angefertigten Matrizen.
In einigen Ländern ist eine solche Garantiebeschränkung nicht zulässig. In diesem Fall ist der Garantiezeitraum auf 60 Tage beschränkt. Der Garantiezeitraum tritt in diesem Fall mit der ersten Installation des Softwareprodukt auf dem Computer des Lizenznehmers in Kraft. Die Anfertigung von Matrizen ist zu unterlassen, vorausgesetzt sie dienen dem Lizenznehmer einzig und allein als Hilfe zur Reparatur des Softwareprodukt oder als Ersatz des beschädigten Originals. Falls die Benutzerlizenz gekündigt wird, werden bereits bezahlte Lizenzgelder rückerstattet.
Einige Staaten, Provinzen oder andere Rechtsstaatlichkeiten erlauben keine Garantieeinschränkungen. Es kann deshalb vorkommen, dass die oben erwähnten Einschränkungen nicht für alle Lizenznehmer gelten. Der Lizenznehmer kann andere Rechte haben, da die Matrize von Staat zu Staat, Provinz zu Provinz oder bei anderen Rechtsstaatlichkeiten verschieden sein kann.

Der Lizenzgeber kann nicht garantieren, dass Matrizen den in der Software enthaltenen Funktionen mit Ihren Erwartungen übereinstimmen oder das die Funktionalität der Software ohne Unterbrechungen oder auftretende Fehler gewährleistet werden. Zu anderen Erklärungen, als den in dieser Vereinbarung aufgeführten Garantien, ist der Lizenzgeber nicht verpflichtet. Der Lizenznehmer ist für die Auswahl seiner Software, um ein gewünschtes Resultat zu

© 2003 SecurStar

erhalten, sowie für dessen Einkauf, das Herunterladen, die Benutzung und das Ergebnis das er durch Matrizesoftware erhält, voll verantwortlich.

5 . HAFTUNGSBESCHRÄNKUNG: Für eventuell auftretenden Schäden, seihen diese auf fehlerhafte Software oder der unfachgemäßen Nutzung der Software zurückzuführen, übernimmt der Lizenzgeber keinerlei Haftung. Dies gilt insbesondere für Datenverluste, Hardwareschäden, Gewinnausfälle und andere Kosten, die auf den Lizenznehmer zukommen können. Zu keinem Zeitpunkt werden der Lizenzgeber, dessen Zulieferer oder dessen Distributoren mehr Verantwortung für den Lizenznehmer übernehmen. Diese Vereinbarung umfasst die Benutzbarkeit (oder Nichtbenutzbarkeit) der Software, wird in berechtigten Fällen lediglich der Kaufpreis zurückerstattet den der Lizenznehmer an den Lizenzgeber und dessen Distributoren gezahlt wurde. Einige Staaten, Provinzen oder andere Rechtsstaatlichkeiten erlauben keine Garantieeinschränkungen. Es kann deshalb vorkommen, dass die oben erwähnten Einschränkungen nicht für alle Lizenznehmer gelten. Der Lizenznehmer kann andere Rechte haben, da die Matrize von Staat zu Staat, Provinz zu Provinz oder bei anderen Rechtsstaatlichkeiten verschieden sein kann. Lizenzgeber, dessen Zulieferer und dessen Distributoren können im Falle von Matrizensoftware nicht durch Klagen von Dritten verantwortlich gemacht werden. Lizenzgeber, dessen Zulieferer und dessen Distributoren werden diese Software einem Lizenznehmer nicht anbieten, wenn letzterer nicht mit der "GARANTIE-AUSSCHLUSSKLAUSEL" und den "HAFTUNGSBESCHRÄNKUNGEN" in dieser Vereinbarung einverstanden ist.

6 . DER LIZENZNEHMER IST DAMIT EINVERSTANDEN, DASS BEIM VERSGESSEN DER PASSWÖRTER EIN EVENTUELLER DATENVERLUST ENTSTEHT UND DASS DER LIZENZGEBER HIERFÜR KEINERLEI TECHNISCHE HILFE FÜR DIE WIEDERHERSTELLUNG VON SOLCHEN PASSWÖRTERN ANBIETEN KANN, SOWIE DASS DAS VERGESSEN EINES PASSWORTES AUTOMATISCH DEN EVENTUELLEN VERLUST IHRER DATEN NACH SICH ZIEHT, WENN SICH DIESE DATEN IN FESTPLATTENPARTITIONEN, VIRTUELLEN CONTAINERN, ODER IN MATRIZEN DIE DURCH NUTZUNG VON DIESEM SOFTWAREPRODUKT ERSTELLT WURDEN, BEFINDEN. DER LIZENZNEHMER AKZEPTIERT, DASS KEINERLEI HINTERTÜREN EXISTIEREN, MIT DENEN AUF VERSCHLÜSSELTE DATEN ZUGRIFF GENOMMEN WERDEN KANN.

7 . EXPORTGESETZE: Diese Software und die dazugehörigen Technologien können der Kontrolle von Import- und Exportgesetzen

© 2003 SecurStar

Ihres Landes unterliegen. Dies kann ebenso für Import- und Exportregulierungen in anderen Ländern gelten. Sie stimmen überein, dass Sie sich an diese Gesetze und Regulierungen halten und dass Sie dafür verantwortlich sind, benötigte Export-, Wiederexport oder Importlizenzen zu besorgen. Der Lizenzgeber kann nicht dafür verantwortlich gemacht werden, wenn die Nutzung im Land des Lizenznehmers nicht gestattet ist. Ebenso erklärt sich der Lizenznehmer damit einverstanden, dass die Lizenz nicht für eine Verletzung von Gesetzen einzelner Länder gedacht und lizenzierbar ist.

8 . ALLGEMEIN: Diese Vereinbarung ist für Sie bindend, sowie für Ihre Angestellten, Arbeitgeber, Vertragspartner und Agenten, sowie für Ihre Nachfolger und Vertreter. Weder diese Software noch andere Informationen, sowie Matrizen die Sie dadurch erhalten, dürfen exportiert werden, außer es steht im Einklang mit in Deutschland vorherrschenden Gesetzen oder anderen zutreffenden Bestimmungen. Diese Vereinbarung unterliegt der Gerichtsbarkeit von deutschen Gesetzen und München ist als Gerichtsstand bestimmt.
Diese Vereinbarung ist als komplette Bedingung zwischen Ihnen und SecurStar Ltd. zu verstehen. Sie erklären sich damit einverstanden, dass SecurStar Ltd. nicht für Unwahrheiten oder Angaben Ihrerseits (Ihrer Agenten oder anderer), welche bei der Vereinbarungserklärung (weder bekannt oder bewusst verschwiegen) bestehen, verantwortlich gemacht werden kann, außer diese unwahren Behauptungen oder Erklärungen wurden in betrügerischer Absicht gemacht. Diese Vereinbarung ersetzt jede andere Kunst von Vereinbarung oder Übereinkunft, eingeschlossen (aber nicht ausschließlich) der Werbung, mit Respekt gegenüber der Software.
Falls eine der Punkte dieser Vereinbarung nicht eingehalten werden können, kann dieser Punkt nach Absprache entfernt werden und übriggebliebenen Punkte gelten weiterhin uneingeschränkt. Diese Vereinbarung ist die komplette und einzigartige Übereinkunft zwischen Ihnen und SecurStar, welche jede anderweitige oder vorher bestandene Vereinbarung, mündlich oder schriftlich, und jede andere Kommunikation zwischen Ihnen und SecurStar, welche in Verbindung zum Thema dieser Vereinbarung steht, nichtig macht.

(C) Copyright 2001 Lizenzgeber. Alle Rechte vorbehalten.
Nutzung, Kopieren, Verteilung und Dekompilierung ist durch das Urheberrecht und durch stirbt Lizenz vorbehalten. DriveCrypt und Securstar sind eingetragene Warenzeichen der SecurStar GmbH in Deutschland und anderen Ländern.

Wenn Sie weitere Fragen zu Höhle Nutzungsbedingungen haben, setzen Sie sich bitte mit SecurStar GmbH unter info@securstar.de in Verbindung

SOFTWAREENTWICKLERVERTRAG
VER. 23/07/2001

- - - - ENGLISH LICENSE AGREEMENT - - - -

END-USER LICENSE AGREEMENT

END-USER LICENSE AGREEMENT FOR SECURSTAR DRIVECRYPT SOFTWARE

IMPORTANT-READ CAREFULLY BEFORE OPENING, INSTALLING, USING, ACCESSING, OR MANIPULATING THE SOFTWARE: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity)("you", "your", or "Licensee") and SecurStar GmbH. ("Licensor") for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, you may not use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by German copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. You are permitted to install and use the SOFTWARE in machine-readable form only and solely on a single desktop computer provided by you, solely for the purposes described in the applicable Licensor documentation. Any components of the SOFTWARE explicitly designed to reside and operate from a server, may be installed on a single server solely on your premises, and any client component is to be installed on as many clients as user licenses purchased and described in the applicable Licensor documentation.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS. You may not reverse engineer, decompile, translate, disassemble, or otherwise attempt to derive source code from the SOFTWARE PRODUCT, or authorize any third party to do any of the foregoing except and only to the extent that such activity is expressly permitted by applicable law

© 2003 SecurStar

notwithstanding this limitation. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer. You may not rent, lease, loan, or distribute the SOFTWARE PRODUCT or any part thereof.

Software Transfer. You may not transfer your license of the Software to a third party.

Termination. Without prejudice to any other rights, Licensor may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

3. COPYRIGHT. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by Licensor or its suppliers. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material. You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

Licensee agrees that some of the ciphers used in the SOFTWARE PRODUCT are the intellectual property of others, and may need a licence for ANY commercial use, such as use on a business system. Licensee acknowledge this is especially true in the case of the IDEA algorithm.

4. DISCLAIMER OF WARRANTIES. ANY USE OF THE SOFTWARE IS AT YOUR OWN RISK.THE SOFTWARE IS PROVIDED "AS IS," "WITH ALL FAULTS," WITHOUT WARRANTY OF ANY KIND. LICENSOR, ITS SUPPLIERS AND DISTRIBUTOR DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. SOME JURISDICTIONS DO NOT ALLOW THE DISCLAIMER OF IMPLIED WARRANTIES, SO THE DISCLAIMER OF IMPLIED WARRANTIES ABOVE MAY NOT APPLY TO LICENSEE, IN WHICH CASE THE DURATION OF ANY SUCH IMPLIED WARRANTIES IS LIMITED TO sixty (60) DAYS FROM THE DATE LICENSEE FIRST INSTALLED THE SOFTWARE ON LICENSEE'S COMPUTER; PROVIDED, HOWEVER, THAT LICENSEE'S SOLE AND EXCLUSIVE

© 2003 SecurStar

REMEDY, AND LICENSOR'S SOLE OBLIGATION SHALL IN ANY CASE BE THAT LICENSOR WILL, AT ITS OPTION, REPAIR OR REPLACE LICENSEE'S COPY OF THE SOFTWARE, OR TERMINATE THIS LICENSE AGREEMENT AND REFUND AMOUNTS ALREADY PAID THEREFOR BY LICENSEE. Some States, Provinces, or other jurisdictions do not allow for exclusions of implied warranties or limitations on how long an implied warranty lasts, so the above exclusion or limitation may not apply to Licensee. Licensee may have other rights which vary from state to state, Province to Province, or in other jurisdictions.

Licensor does not warrant that the functions contained in the Software will meet your requirements or that the operation of the Software will be uninterrupted or error-free. Any representation, other than the warranties set forth in this Agreement, will not bind the Licensor. You assume full responsibility for the selection of the Software to achieve your intended results, and for the buying or downloading, use and results obtained from the Software. Licensee also assume the entire risk as it applies to the quality and performance of the Software

5. LIMITATION OF LIABILITY. REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, TO THE EXTENT PERMITTED BY THE LAW OF THE JURISDICTION IN WHICH LICENSEE OBTAINED THIS LICENSE, LICENSOR, ITS SUPPLIERS AND DISTRIBUTORS WILL NOT BE LIABLE FOR ANY INDIRECT, EXEMPLARY, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES OF ANY CHARACTER, INCLUDING BUT NOT LIMITED TO DAMAGES FOR COMPUTER MALFUNCTION, LOSS OF INFORMATION, LOST PROFITS AND BUSINESS INTERRUPTION, AND THE COST TO OBTAIN SUBSTITUTE SOFTWARE, ARISING IN ANY WAY OUT OF THIS AGREEMENT OR THE USE OF (OR INABILITY TO USE) THE SOFTWARE HOWEVER CAUSED AND WHETHER ARISING UNDER A THEORY OF CONTRACT, TORT OR ANY OTHER LEGAL THEORY, EVEN IF LICENSOR, ITS SUPPLIERS DISTRIBUTOR WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LICENSOR'S, ITS SUPPLIERS' OR DISTRIBUTOR'S TOTAL LIABILITY TO LICENSEE RELATING TO THIS AGREEMENT OR THE USE (OR INABILITY TO USE) THE SOFTWARE EXCEED THE AMOUNT PAID BY LICENSEE TO LICEN
SOR OR LICENSOR'S DISTRIBUTOR FOR THIS LICENSE. SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO LICENSEE. LICENSOR, ITS SUPPLIERS AND DISTRIBUTORS SHALL NOT BE LIABLE FOR ANY CLAIMS OF THIRD PARTIES

© 2003 SecurStar

RELATING TO THE SOFTWARE. LICENSOR, ITS SUPPLIERS AND DISTRIBUTORS WOULD NOT PROVIDE THE SOFTWARE TO LICENSEE IF LICENSEE DID NOT AGREE TO THE "DISCLAIMER OF WARRANTIES" AND "LIMITATION OF LIABILITY" PROVISIONS IN THIS AGREEMENT.

6. LICENSEE AGREE THAT IN THE EVENT OF LOSS OR FORMATTING OF PASSWORDS USED BY THIS SOFTWARE PRODUCT, NO TECHNICAL SUPPORT CAN BE GIVEN TO ASSIST IN RECOVERY SUCH PASSWORD, AND THAT YOUR FORGETTING OF ANY PASSWORDS EQATES TO LOSS OF YOUR DATA WHEN THAT DATA IS STORED ON ANY DISK PARTITION, OR DISK DRIVE IMAGES CREATED, AND/OR OPERATED BY THE EXECUTION OF THIS SOFTWARE PRODUCT. LICENSEE ACCEPT THAT NO BACK DOORS EXIST, TO GAIN ACCESS TO SCRAMDLED (CRYPTED) DATA.

7. EXPORT LAW. The SOFTWARE and related technology may be subject to import/export control laws in your country and may be subject to export or import regulations in other countries. You agree to strictly comply with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export or import as may be required. Licensor cannot be held responsible for uses which may be illegal in the Licensee country, and Licensee also agrees, that the software is not intended or licensed for such purposes.
8. GENERAL. This Agreement is binding on you as well as your employees, employers, contractors and agents, and on any successors and assignees. Neither the Software nor any information derived there from may be exported except in accordance with the laws of Germany or other applicable provisions. This Agreement is governed by the laws of Germany and the court of Munich (Germany) shall have sole jurisdiction over any dispute arising hereunder.
This Agreement is the entire agreement between you and SecurStar Ltd. and you agree that SecurStar Ltd will not have any liability for any untrue statement or representation made by its, its agents or anyone else (whether innocently or negligently) upon which you relied upon entering this Agreement, unless such untrue statement or representation was made fraudulently. This Agreement supersedes any other understandings or agreements, including, but not limited to, advertising, with respect to the Software.
If any provision of this Agreement is held to be unenforceable, that provision will be removed and the remaining provisions will remain in full force. This Agreement is the complete and exclusive statement of the agreement between us which supersedes any proposal or prior agreement, oral or written, and any other communications between us in relation to the subject matter of this Agreement.

© 2003 SecurStar

(c)Copyright 2001 Licensor. All rights reserved.
Protected by copyright and licenses restricting use, copying, distribution and decompilation. Licensor and Licensor are trademarks of Licensor in Germany and other countries.

For questions concerning this Agreement, please contact SecurStar GmbH at info@securstar.de

SOFTWARE DEVELOPMENT AGREEMENT
Ver. 23/07/2001

1.6 Kauf und Aktuallisierung von DriveCrypt

Die DRIVECRYPT Software kann auf der SecurStar Homepage gekauft werden.
http://www.securstar.com

Wenn Sie ein Neukunde sind, klicken Sie bitte auf den "Kaufen-Link" und wählen das Produkt welches Sie kaufen wollen.

Bestehende Kunden müssen sich in der private area der SecurStar Homepage einloggen, befor sie eine Bestellung abgeben können. Die Login Details wurden Ihnen beim Kauf der Vorgängerversion zugesendet und können durch einen Klick auf den "*forgot password*" Link auf der Hauptseite unserer Homepage.

Um Ihre alte DRIVECRYPT Version aktuallisieren zu können, loggen Sie Sich einfach in Ihre private area ein um die neueste Version Ihrer Software zu bekommen oder Ihren neuen Registrierungsschlüssel zu generieren.

Hinweis: Wenn Sie nicht mehr updateberechtigt sind (weil Sie z. B. schon vor mehr als 6 Monaten gekauft haben oder Ihr 12 monatiger Upgrade Service ist ausgelaufen), sollten Sie einen neuen 12 monatlichen Upgradeservice bestellen.

1.7 Standard und Home Edition (Vergleich)

DRIVECRYPT gibt es in der Standard und der Home Edition.
Die Standard Edition hat alle Features der Home Edition. Zuzüglich hat sie noch weitere, welche im Chart angezeigt werden. Hier sind die Unterschiede gegenübergestellt worden.

© 2003 SecurStar

FEATURES	HOME EDITION	STANDARD EDITION
Container Verschlüsselung	JA	JA
Max. Containergröße	4 GB	UNBEGRENZT
Container Größenveränderung	NEIN	JA
Gleichzeitig anmeldbare Container	1	8
Partitionen Verschlüsselung	NEIN	JA
Max Partitionsgröße	N/A	2000 GB
Gleichzeitig benutzbare verschlüsselte Datenmenge	4 GB	UNBEGRENZT
FAT 16 und FAT 32 Unterstützung	JA	JA
NTFS Unterstützung	NEIN	JA
Unsichtbare Container Erstellung	NEIN	JA
Versteckt Daten in Musikdateien (Steganographie)	JA	JA
1344 Bit Verschlüsselung	JA	JA
Anzahl der Verschlüsselungsalgorithmen	11	11
Nichtbeweisbare Verschlüsselung	JA	JA
Verstärkte Passwortsicherheit	JA	JA
Schutz gegen Passwörterspionage (antisniffing)	JA	JA
Schutz gegen Brute-force und Wörterbuchattacken	JA	JA
Administratoren Passwortkontrolle (Schlüsseldateien)	JA	JA
Zweitbenutzer Zugriff	JA	JA
Sichere Datenlöschung (Wiping)	JA	JA

© 2003 SecurStar

Sie können noch mehr über die einzelnen Funktionen erfahren, wenn Sie den Paragraph Hauptfunktionen besuchen.

© 2003 SecurStar

2 Installation von DriveCrypt

2.1 Systemvoraussetzungen

DriveCrypt benötigt sehr geringe Systemvoraussetzungen:

- Ein PC-kompatibler Computer mit Windows 95 / 98 / ME / NT / 2000 / XP
- Mindestens 2 MB freien Festplattenspeicher für die DriveCrypt-Installation.
- weiterer Festplattenplatz, um die DriveCrypt-Laufwerksdateien erstellen zu können.
  (Diese können entweder auf FAT16/32 oder NTFS Laufwerken, einer leeren Festplattenpartition, einer Diskette, oder, falls Steganography-Verschlüsselung gewünscht wird, aus einer großen WAV-Datei bestehen.)

2.2 Installation von DriveCrypt

Um DriveCrypt zu installieren, startet man die Installationsdatei DC-Install.exe und folgt den Anweisungen auf dem Bildschirm.

Hinweis: Um die Software erfolgreich zu installieren, müssen die Nutzungsbedingungen akzeptiert, und eine gültige Seriennummer eingeben werden.

Falls eine Personalisierung der Installation gewünscht wird, kann man, nachdem die Nutzungsbedingungen akzeptiert wurden, das Verzeichnis für die DriveCrypt- Installation ändern. Ebenso besteht die Möglichkeit, einen anderen Namen für die DriveCrypt Programmdatei anzugeben.

Wenn die Installation abgeschlossen und der Computer neu gestartet wurde, können mit DriveCrypt verschlüsselte Laufwerke erstellt und genutzt werden.

Es ist auch möglich, verschlüsselte Container mit Computern einzulesen, die selbst kein DriveCrypt installiert haben. Hierzu wird das Programm im Traveller-Modus betrieben. Dies wird bei der Installation durch das entsprechende Häkchen festgelegt.

Falls man sicher gehen möchte, dass NUR ADMINISTRATOREN verschlüsselte Laufwerke erstellen können und diese nur durch einen Benutzer mit dem dazugehörigen Schlüssel geöffnet werden

© 2003 SecurStar

können, müssen dazu die nötigen Installationsdialoge während dem Installationsprozesses ausgewählt werden.

2.3 Traveller Modus (Reisemodus)

Falls Sie Containerdateien auf einem Rechner öffnen möchten in dem DriveCrypt nicht installiert/registriert wurde, können Sie dies mit dem Reisemodus (Traveller Modus) tun.

Reisemodus wird wie folgt installiert:

1) Starten Sie bitte die DriveCrypt Installationsdatei vom Computer, wo DriveCrypt ursprünglich REGISTRIERT wurde, und wählen Sie während der Installationsroutinen, die Option, „Reisemodus installieren"

2) Sie können dann das Verzeichnis auswählen, indem die Software im Reisemodus installiert werden soll.

3) Geben Sie bitte das Betriebssystem an, mit dem Sie DriveCrypt im Reisemodus benutzen möchten (Diese Option ermöglicht es Ihnen, die Softwaregröße so anzupassen, dass sie auf einer einzigen Diskette platz hat).

4) Kopieren Sie die generierten Dateien auf dem Rechner, wo Sie die verschlüsselten Container öffnen möchten und starten Sie dann die DriveCrypt.exe Datei.

5) Benutzen Sie DriveCrypt wie gewohnt.

Einschränkungen des Reisemodus:

Bei der Benutzung von DriveCrypt im Reisemodus, gibt es einige Einschränkungen:

a) Reisemodus kann nur vom Computer installiert werden, wo DriveCrypt bereits REGISTRIERT wurde.

b) Reisemodus kann zwar verschlüsselte DriveCrypt Container öffnen, nicht jedoch verschlüsselte Partitionen

c) Befinden sich die verschlüsselten DriveCrypt Container auf einer

© 2003 SecurStar

WECHSELPLATTE (USB-Stick, USB-Drive, Zip-Drive, Floppy Disk usw.) können diese, im Lese-/Schreibmodus geöffnet werden.
Befinden sich die Container allerdings auf einer fixen Festplatte, so können diese nur im Lesemodus geöffnet werden.

2.4 DriveCrypt registrieren

Um DriveCrypt zu registrieren und die Demoversion in einer Vollversion zu verwandeln benötigen Sie einen Registrierschlüssel und müssen diesen in der Software registrieren

Es gibt zwei Möglichkeiten die Software zu registrieren:

1) Automatische Onlineregistrierung
(Empfehlenswert, wenn der Rechner mit dem Internet verbunden ist)

2) Manuelle Registrierung
(Registrierungsschlüssel vom SecurStar Server herunterladen und die Software registrieren)
Genauere Informationen hierzu, entnehmen Sie bitte Ihrer Email-Bestellbestätigungen

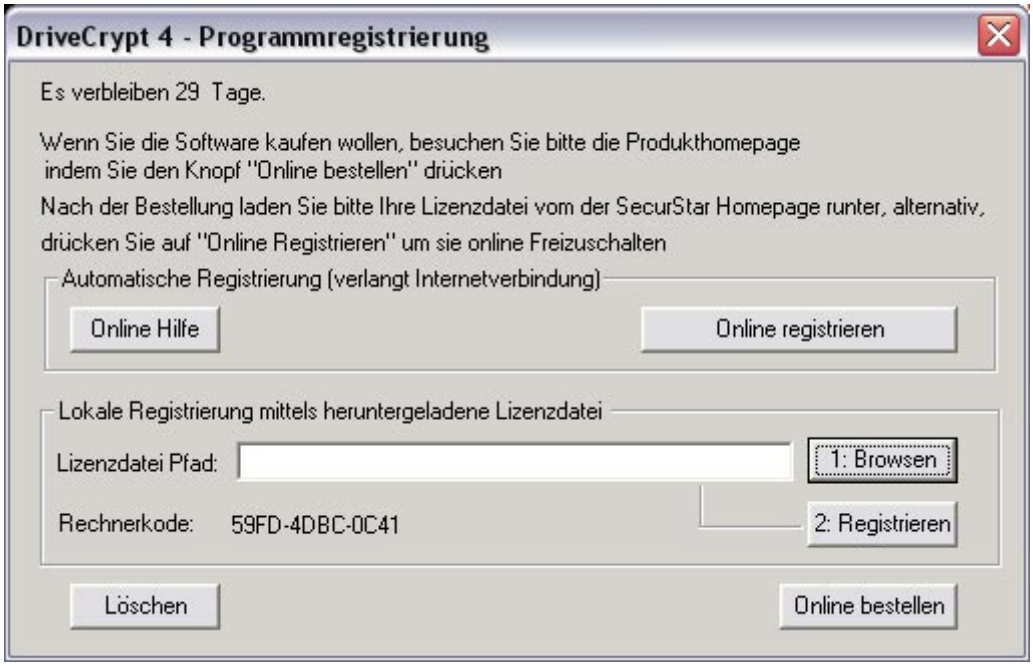
2.4.1 Automatische Registrierung

Folgen Sie bitte diesen Schritten, um DriveCrypt automatisch über das Internet zu registrieren:

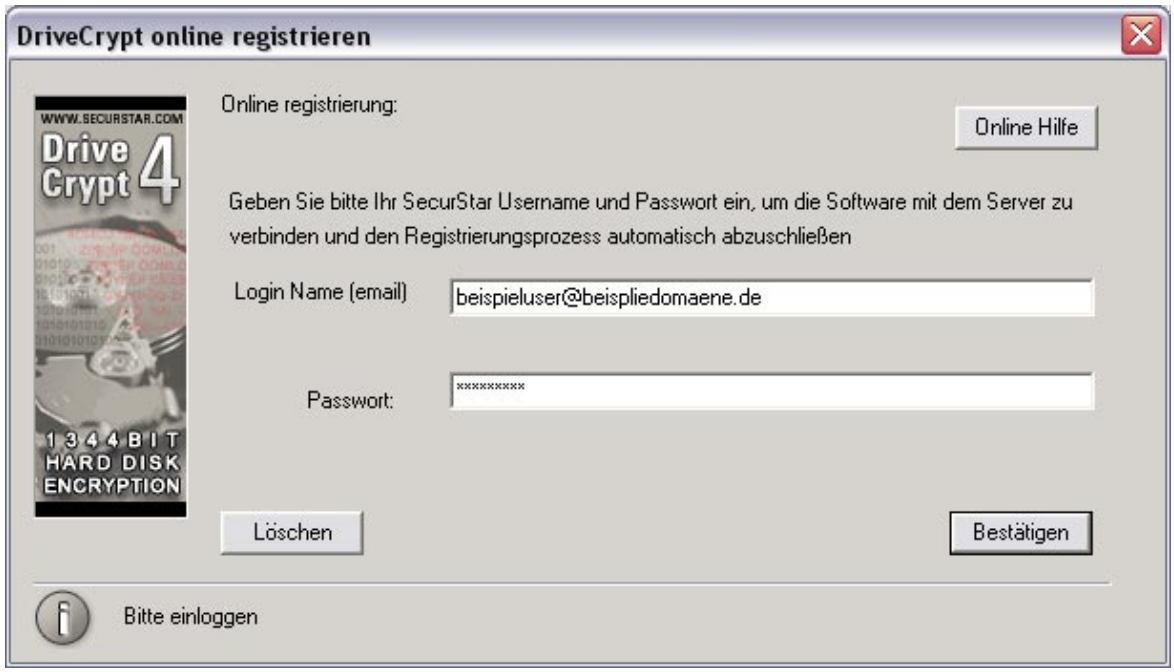
Starten Sie die DriveCrypt software und drücken Sie auf "REGISTRIERUNG -> DRIVECRYPT REGISTRIEREN".

Das folgende Dialog wird erscheinen:

© 2003 SecurStar



Drücken Sie bitte auf "**Online Registrieren**" (Get LicenseKey Online) um das folgende Fenster zu öffnen:

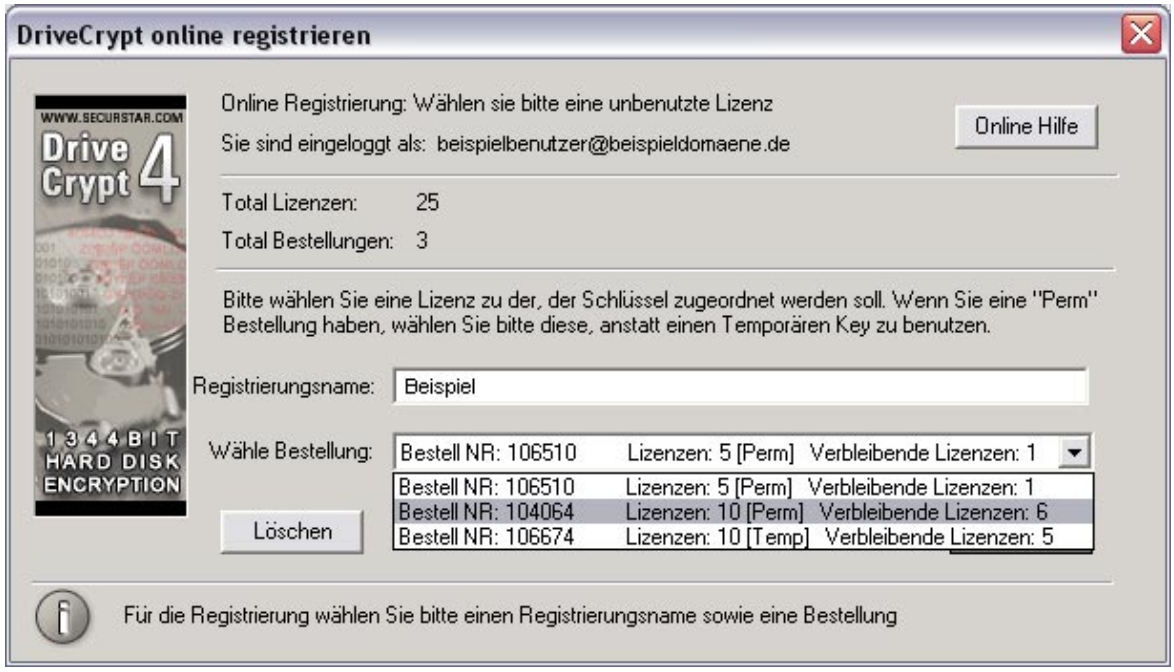


Geben Sie hier bitte Ihre persönlichen Logindaten zur SecurStar Homepage ein und bestätigen Sie die Eingabe mit "Bestätigen" (Sie sollten die Logindaten per Email, bei der Softwarebestellung, erhalten haben)

© 2003 SecurStar

Die Software wird sich nun über das Internet mit dem SecurStar Server verbinden.

Falls Sie mehrere Onlinebestehllungen gemacht haben, werden Sie eine Zusammenfassung Ihrer Bestellungen sehen und Sie können wählen, zu welcher Bestellung Sie die Lizenz benutzen möchten und bestätigen Sie.



Geben Sie bitte Ihren Namen (oder den Namen auf wem Sie die Software registriren möchten) im dafür vorgesehenen Feld ein und drücken Sie auf **"Bestätigen"**.

Unser Server wird automatisch eine Lizenz vom Server herunterladen und diese dann registrieren.

© 2003 SecurStar

Gratulation, die DriveCrypt Software wurde erfolgreich registriert!
Sie können jetzt Ihre Daten wirkungsvoll absichern.

Sollten Sie zu den oben erwähnten Punkten irgendwelche Fragen haben, steht Ihnen das SecurStar Team jederzeit gerne zur Verfügung.

2.5 Entfernen von DriveCrypt

Aus dem Hauptmenü von DriveCrypt wählt man folgende Funktion:

Generell -> DriveCrypt deinstallieren.

Bei der Deinstallation von DriveCrypt wird ein Fenster geöffnet, in dem man die Deinstallation bestätigen muss.

2.5.1 Lizenz transferieren

Wenn Sie die DriveCrypt Softwarelizenz auf einem anderen Computer

© 2003 SecurStar

verschieben möchten, folgen Sie bitte die folgenden Schritte:

Option 1 (Automatisch) –Empfohlen -

a) Deinstallieren Sie DriveCrypt : **Generell->DriveCrypt deinstallieren->Online Deinstallation**
(DriveCrypt wird Ihre Lizenz auf dem SecurStar Server wiederherstellen um Ihnen die Möglichkeit zu geben, die Software auf einer anderen Maschine zu installieren)

b) Installieren und registrieren Sie DriveCrypt auf der neuen Maschine.

Option 2 (Manuell)

a) Deinstallieren Sie DriveCrypt :
Generell->DriveCrypt deinstallieren
Und erstellen Sie einen DEINSTALLATIONSCODE indem Sie im dafür vorgesehenen Feld die Seriennummer duplizieren und dann bestätigen.

b) Dies wird Ihnen einen Deinstallationscode im Dialogfenster anzeigen. Eine Kopie des Deinstallationscode wird auch in der Datei c:\DCUninstall.txt kopiert.

c) Der Deinstallationscode ermöglicht es Ihnen, Ihren alten generierten Schlüssel auf unseren Onlineserver zu löschen. Loggen Sie sich hierfür im privaten Bereich unserer Homepage ein, zerstören Sie Ihre alte Lizenz durch eingabe des Deinstallationscode und generieren Sie anschliessend eine neue Lizenz für die neue Maschine.

Sollten Sie zu den oben erwähnten Punkten irgendwelche Fragen haben,
steht Ihnen das SecurStar Team jederzeit gerne zur Verfügung.

© 2003 SecurStar

3 Bildschirm und Menübeschreibungen

3.1 Bildschirm und Menübeschreibungen

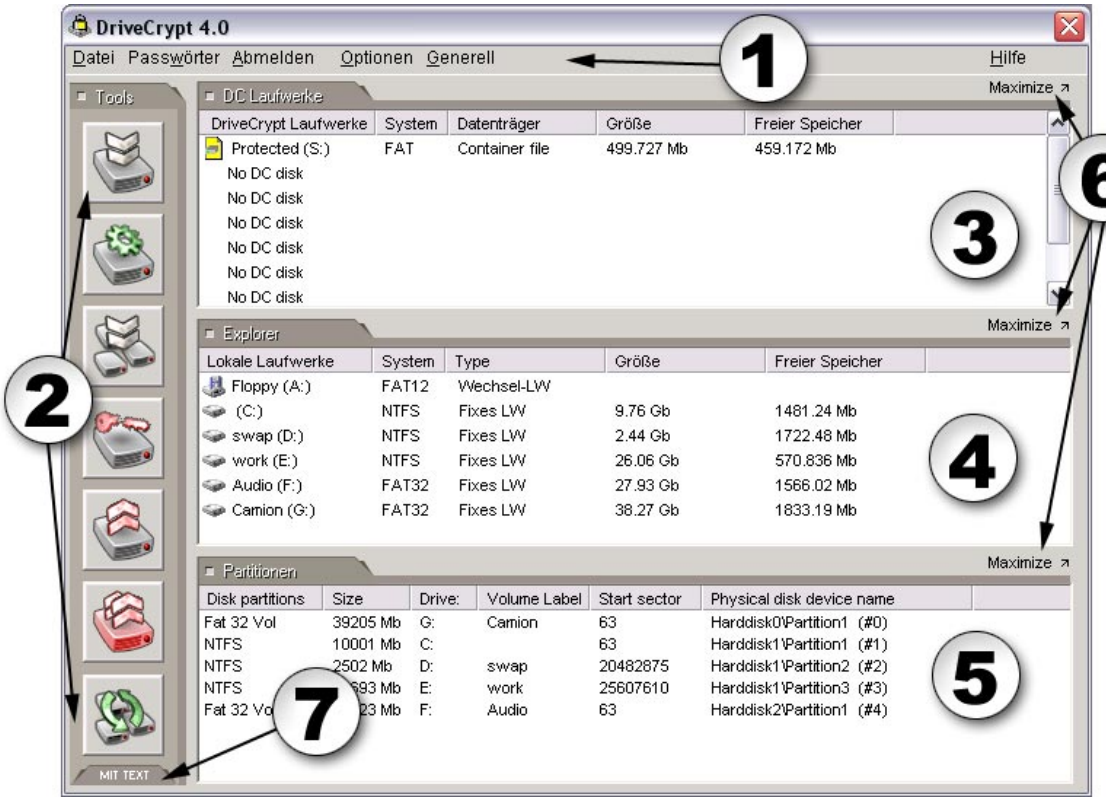
Dieser Teil der Dokumentation bietet Beschreibungen für die am meisten genutzten Fenster und aller vom Hauptbildschirm erreichbaren Menüs.

Die am meisten benutzten Screenshots werden grafisch mit einem Erklärungstext dargestellt, welche die einzelnen Elemente des Inhaltes erklären.

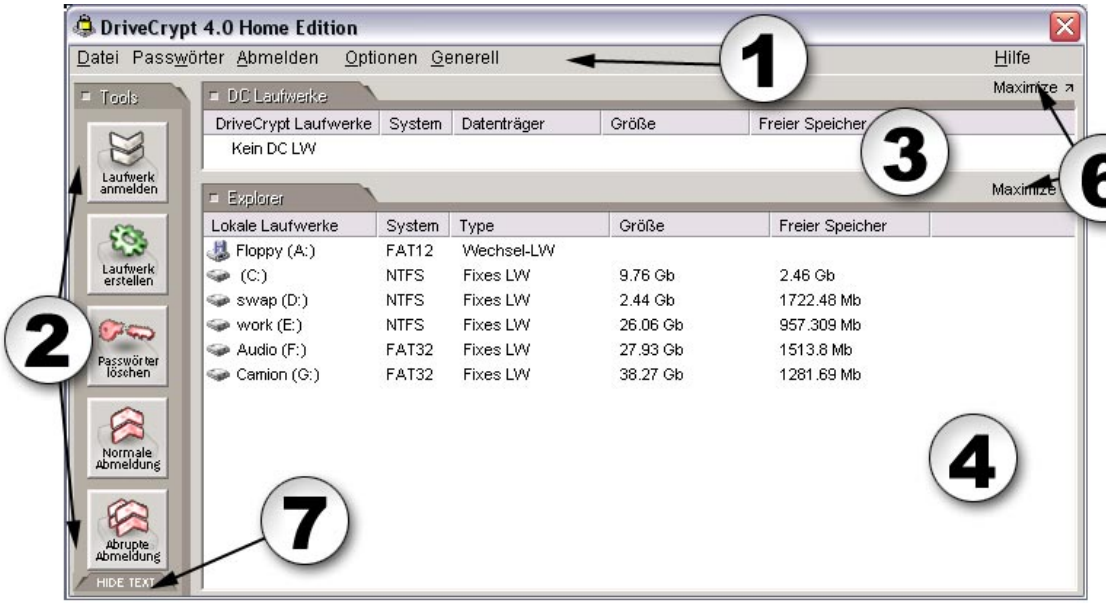
Alle Menüpunkte des Hauptbildschirms werden ebenso mit Screenshots mit Beschreibungen über die einzelnen Funktionen erklärt.

3.2 Der Hauptbildschirm

Das ist der Hauptbildschirm der DriveCrypt Standard Edition



Das ist der Hauptbildschirm der DriveCrypt Home Edition



Beschreibung:

1 Menüs. Auf den folgenden Seiten sind die unterschiedlichen Menüs beschrieben.

2 Die Werkzeugleiste beinhaltet die am häufigst benutzten Funktionen wie Erstellung und Abmeldung von verschlüsselten Laufwerken, Passwörter löschen etc.

3 This area shows mounted volumes and available slots.

4 Dieser Bereich zeigt alle normalen Festplatten an, die es im System gibt.
Mit der linken Maustaste auf ein Festplattensymbol wird dieses geöffnet.
Mit der rechten Maustaste auf ein Festplattensymbol öffnet dies ein vertikales Menü, in dem man Funktionen wie freien Speicherplatz löschen, Laufwerksnamen vergeben, defragmentieren etc findet.

5 Dieser Bereich zeigt die Geräte, welche im System vorhanden sind. Um eine Partition zu formatieren, muss man einfach mit der rechten Maustaste auf dieses klicken. Warnung: Dies zerstört alle auf der Partition existierenden Daten! **Hinweis: Dieser Bereich ist in der Grundeinstellung als versteckt angegeben.** Man kann den Partitionenzugriff im **Optionen**dialogfeld einschalten.

6 Hilft dem Benutzer die Panelgrösse zu maximieren, wenn der sichtbare Bereich zu klein ist.

7 Schaltet zwischen diesen Ansichten: Icons mit und ohne Text.

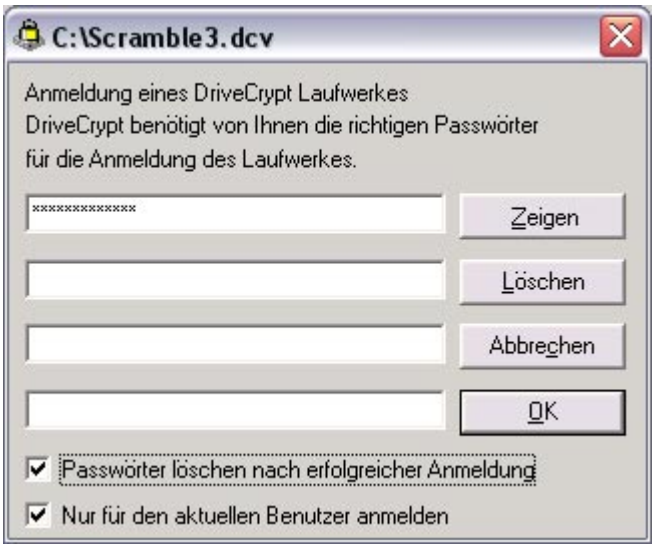
© 2003 SecurStar

3.3 Passwort- und Passwortbestätigungsbildschirm

Festplattenlaufwerk-Passwörter:

Dieser Teil enthält 4 Eingabefelder, in welche die Passwörter eingegeben werden. Es können hierzu alle 4 Zeilen benutzt werden falls dies nötig ist.

Um zwischen den 4 Zeilen zu springen, benutzt man die **Tab** und die **Shift-Tab** Tasten.



Zeigen: Man kann die Passwortanzeige zwischen Normaltext und „durch Sternchen verdeckt" auswählen.

Löschen: Entleert alle Textfelder.

Abbrechen: Schließt die Dialogfelder, die keine Aktionen ausführen.

Ok: Speichert die eingegebenen Passwörter und schließt das Dialogfenster.

Hinweis: Wenn man die Beschreibung in der Titelleiste außer Acht lässt, gleichen sich der Passwortbestätigungsbildschirm und Schlüsseldatei-Passwortbildschirm mit dem oben gezeigten Passwortfenster.

© 2003 SecurStar

3.4 Der rote Low Level Benachrichtigungsbildschirm (nur unter Win 95/98/Me)

Diese Funktion wurde entworfen, um zu verhindern, dass durch ein anderes Programm Eingaben über die Tastatur zwischen dem Benutzer und dem Betriebssystem Windows/DriveCrypt abgefangen und gespeichert werden.

Wenn diese Funktion in den "**Einstellungen**" aktiviert ist, übernimmt diese Funktion die Aufgabe des normalen Windowseingabefensters.

Anstelle dessen wird ein roter Bildschirm geöffnet, der wie ein CGA Bildschirm aussieht.

Der Bildschirm erfüllt exakt die gleichen Funktionen wie der Windows-Passwortbildschirm. Folgende Tasten übernehmen die Funktionen folgender Knöpfe**:**

Taste	**Knopf**
Enter	Übernehmen
BildUnten	Anzeigen
BildHoch	Verstecken
Escape	Abbruch
Pos1/Home	Reset

Zusätzlich zu den oben angegebenen Tasten kann man mit der Taste F1 ein | (Rohr) Symbol und mit der Taste F2 eine # (Raute) eingegeben werden.

Diese Funktionen sollten nicht benutzt werden, wenn die Tastatur nicht dem Standart QWERTY Typ entspricht (z.B. eine französische Tastatur).

Hinweis: Der rote Bildschirmmodus wird momentan NICHT durch Windows NT oder Windows 2000 unterstützt.

© 2003 SecurStar

4 Beschreibung der Menüfunktionen

4.1 Menüfunktionen: Datei

Datei

Anmeldung einer Container Datei:
Wird benutzt, um ein bereits vorhandenes verschlüsseltes Laufwerk anzumelden.
Siehe hierzu 'Wie man.. Anmeldung von verschlüsselten Laufwerken'.

Erstellung einer Container Datei:
Wird benutzt, um ein neues verschlüsseltes Laufwerk anzumelden.
Siehe hierzu 'Wie man.. Erstellung eines verschlüsselten Laufwerkes'.

Erstellung einer DKF Zugriffsdatei, damit andere Benutzer Zugriff auf das DriveCrypt Laufwerk erhalten:
Siehe hierzu die Kapitel "Wie man… **Zweitschlüssel Benutzerzugriff**".

Tempdatein-Pfad anzeigen:
Zeigt den Pfad des Verzeichnisses an, in welchem temporäre Dateien der Anwendungen abgespeichert werden (den Wert der TEMP Umgebungsvariable), und erlaubt es dieses Verzeichnis anzuzeigen. Daten, welche hier abgelegt werden, sind nicht verschlüsselt und stellen deshalb eine Möglichkeit für Datendiebe dar.

Swapdatei-Information:
Windows 'hinterlegt' Daten aus dem Arbeitsspeicher, welcher nicht sofort benötigt wird, auf der Festplatte, welcher auch als "Virtueller Speicher" bekannt ist. Daten, die in diesen 'virtuellen Speicher' Swapdatei abgelegt werden, wird nicht verschlüsselt und stellt deshalb ein Risiko des Datendiebstahls dar. *Siehe hierzu auch das Kapitel über*

© 2003 SecurStar

***Freien Speicherplatz löschen**, um mehr über das Löschen der Swapdatei-Auslagerung zu erfahren.*

Header Backup Daten benutzen:
Wenn der DriveCrypt Container erstellt wird, werden 2 KB entscheidende Daten erstellt, welche benötigt werden, um den Container öffnen zu können. Diese Daten werden benötigt, um einen einzigartigen Initialenwert ("IVs") für jeden Sektor und den Verschlüsselungssektor zu erstellen. Ohne diese Daten kann der Container nicht angemeldet werden. Im Falle eines Fehlers in dem 2 KB Bereich durch einen Sektorfehler oder ähnliches, ein zweiter 2 KB Block existiert im Header und dieser wird anstelle dessen benutzt. Dieser wird doppelt verschlüsselt als einfach nur kopiert um sicherzustellen, dass DriveCrypt Container deswegen nicht einfach als diese erkannt werden können. Falls einmal ein Laufwerk nicht mehr angemeldet werden kann, liegt das daran, dass entscheidende Daten kaputt gegangen sind. Man kann somit über das Dateimenü die Funktion „Gebrauch der Header-Backup-Daten" aktivieren und danach versuchen, dass Laufwerk erfolgreich anzumelden.
Normalerweise wird natürlich das Laufwerk angemeldet, aber es wird die Sicherheitskopie dazu benutzt. Man kann die Sicherheitskopie vorher prüfen, ob diese OK ist, indem man das Laufwerk damit anmeldet!
Die Auswahl gilt nur für die jetzige DriveCrypt Sitzung.
Ein anderer Weg um Container gegen Headerprobleme zu sichern, ist die Möglichkeit, DKF Dateien zu benutzen, welche ihren eigene, einzeln verschlüsselte Kopie der Headerdatei haben. Die Containerdatei muss an der gleichen Stelle der Festplatte bleiben wie die DKF-Datei, weil dieser bestimmte verschlüsselte Informationen über den Pfad des Containers enthält.

Fenster schließen:
Schließt das DriveCrypt Fenster. Das Programm wird trotzdem noch minimiert weiterfunktionieren.

Beenden:
Beendet DriveCrypt und bietet die Option, die Passwörter resistent zu merken oder zu löschen. Diese müssen bei einem späteren Neustart von DriveCrypt dann neu eingegeben werden.

Hinweis : Die angemeldeten entschlüsselten Laufwerke sind immer noch aktiv, bis diese abgemeldet werden, oder MS Windows beendet wird.

© 2003 SecurStar

4.2 Menüfunktionen: Passwörter

Passwörter

Eingabe eines Laufwerkspasswortes:
Öffnet ein Dialogfenster, in welches das Passwort eingegeben wird, um ein verschlüsseltes Laufwerk anzumelden.

Zwischengespeicherte Passwörter löschen:
Löscht alle Passwörter, welche im Speicher durch die VxD Komponente und das DriveCrypt Interface gespeichert werden.

HINWEIS: Wenn die Funktion "**Eingabe aller Passwörter im roten Low Level Bildschirm Modus**" aktiviert ist, dann wird diese benutzt, um den "Eingabe des Festplattenpasswortes" Dialog zu nutzen anstelle des Windows Passwortbildschirm. (Noch nicht unterstützt unter Windows NT oder Windows 2000)

4.3 Menüfunktionen: Abmeldung

Abmeldung :

Alles Abmelden:
Meldet alle angemeldeten Laufwerke ab.

Alles Abrupt Abmelden:
Meldet alle angemeldeten Laufwerke abrupt ab.
Siehe hierzu das Kapitel "Wie man…
Abmeldung von verschlüsselten Laufwerken".

© 2003 SecurStar

4.4 Menüfunktionen: Partitionen

Partitionen

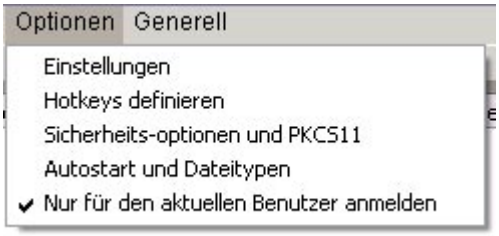
Partitionen anmelden:
Zeigt das Dialogfenster, welches die Eingabe des Passwortes zur verschlüsselten Partition ermöglicht.

Partitionen aktualisieren:
Aktualisiert das Laufwerke- / Partitionenfenster und veranlasst DriveCrypt dazu, jede Partition mit den gemerkten Passwörter anzumelden, sofern dies möglich ist.

4.5 Menüfunktionen: Optionen

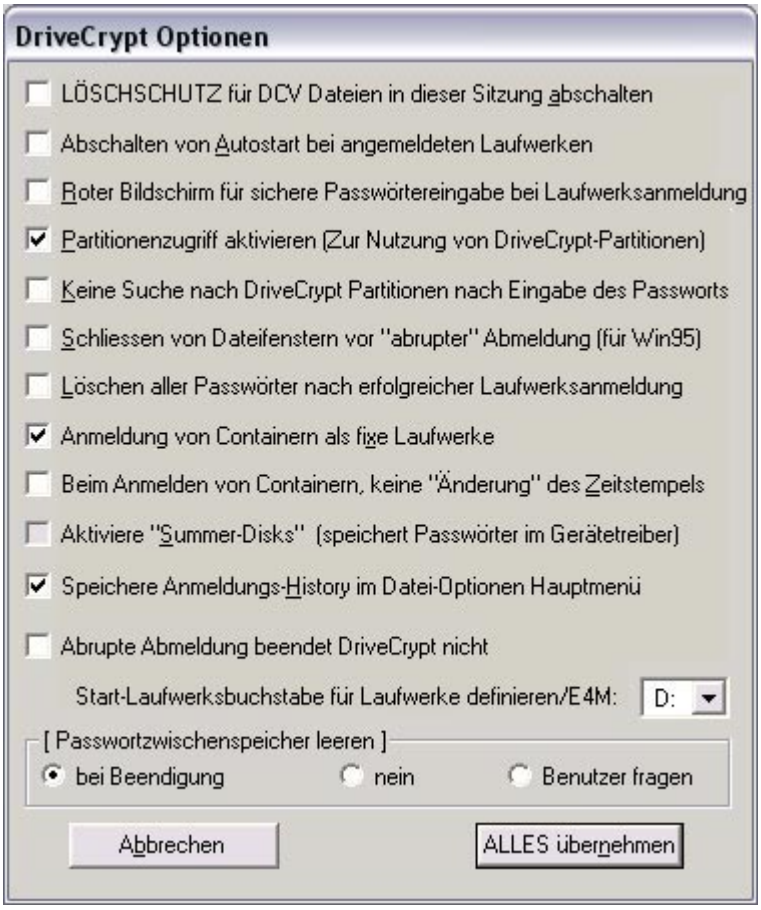
Optionen:

Um DriveCrypt zu konfigurieren bitte folgende Optionen aufrufen



EINSTELLUNGEN:

© 2003 SecurStar



Löschschutz für DCV Dateien in dieser Sitzung abschalten:
DriveCrypt beinhaltet eine Funktion, welche es verhindert, dass aus Versehen die SVL Datei gelöscht wird. Falls man wirklich einen Container löschen möchte, stellt man die Funktion um, löscht die Datei, und stellt danach die Funktion wieder zurück.

Abschalten von Autostart bei angemeldeten Laufwerken:
Stellt die Autostart-Funktion von DriveCrypt ab.

Roter Bildschirm für sichere Passwörtereingabe bei Laufwerksanmeldung: Aktiviert/Deaktiviert den roten Low Level Bildschirm, welcher dazu benutzt wird, um die Passwörter sicher einzugeben. Siehe hierzu das Kapitel "**Bildschirmbeschreibungen und Menüs**".

Partitionenzugriff aktivieren (Zur Nutzung von DriveCrypt-Partitionen):
Diese Einstellung wird aktiviert, um die physikalischen Partitionen anzuzeigen, welche an den Computer angeschlossen sind.

© 2003 SecurStar

(Grundeinstellung ist auf AUS)

Keine Suche nach DriveCrypt Partitionen nach Eingabe des Passworts:
Nachdem ein Passwort eingegeben wird, führt DriveCrypt keine Suche der verschlüsselten Festplattenpartitionen durch.

Schliessen von Dateifenstern vor "abrupter" Abmeldung (für Win95):
Schließt automatisch alle Explorerfenster, welche noch Dateien aus verschlüsselten Laufwerken anzeigen, wenn abrupte Abmeldung aktiv ist. Bei Windows 98/ME/NT/2000 wird diese Option nicht gebraucht, da offene Fenster für das Betriebssystem nicht gleichzeitig bedeuten, dass Dateien geöffnet sind.

Löschen aller Passwörter nach erfolgreicher Laufwerksanmeldung :
Löscht alle passwörter aus dem Computerspeicher sobald ein verschlüsseltes Laufwerk angemeldet wurde.

Anmeldung von Containern als fixe Laufwerke:
Mit dieser Funktion kann festgelegt werden, ob ein verschlüsseltes Laufwerk als ein fest definiertes oder als ein Wechsellaufwerk erkannt und angemeldet werden soll.

Beim Anmelden von Containern, keine "Änderung" des Zeitstempels
Hier kann definiert werden, ob ein "zuletzt veränderter" Zeitstempel eines Containers auf das Erstellungsdatum zurückgesetzt werden soll, wenn dieser Container wieder abgemeldet wird. Als Grundeinstellung ist vorgegeben, dass die „zuletzt veränderte" Zeit zu dem Zeitpunkt der Containererstellung zurückgesetzt werden soll, wenn ein Container abgemeldet wird. Dies beugt vor, dass der Container für Schnüffler im System so aussieht, als sei dieser nie verändert worden, da er die gleiche Zeit trägt, als wie dieser erstellt wurde. Dies ist besonders für Wav-Files wichtig, welche nach deren Erstellung kaum verändert werden.

Aktiviere "Summer-Disks" (speichert Passwörter im Gerätetreiber)
Dies erlaubt es, sehr alte überholte Scramdisk formatierte Laufwerke nur unter Windows 95/98/ME zu öffnen. (Hinweis: Diese Funktion speichert Passwörter in den Gerätetreibern.)

Speichere Anmeldungs-History im Datei-Optionen Hauptmenü:
Dies speichert Protokollinformationen über die letzten acht Containerdateien, welche als letztes angemeldet wurden. Wenn diese Option aktiviert ist. Wenn diese Option aktiv ist, kann man im Dateimenü den Dateipfad von den letzten acht angemeldeten Containern sehen. Man kann nun diese direkt aus dem Dateimenü auswählen, um diese erneut anzumelden, ohne diese erst heraussuchen zu müssen oder die Datei auf

© 2003 SecurStar

der Festplatte anzuklicken ect.

Abrupte Abmeldung beendet DriveCrypt nicht
Mit dieser Funktion verhindert man dass nach einer abrupten Laufwerksabmeldung das DriveCrypt Programm beendet wird.

Start-Laufwerksbuchstabe für Laufwerke definieren/E4M:
Wenn der Laufwerksbuchstabe für einen anzumeldenden Container nicht definiert ist, wird der Laufwerksbuchstabe, der hier festgelegt wird, für den nächsten anzumeldenden Container benutzt. Der nächste Container, bei dem der Laufwerks-buchstabe nicht eingestellt ist, wird den darauf folgenden Laufwerksbuchstaben bekommen usw. Voraussetzung dafür ist, dass noch Laufwerksbuchstaben verfügbar sind.

[Passwortmerker löschen, wenn das Anwendungsfenster verlassen wird]:
Hier wird festgelegt, ob DriveCrypt die Passwörter aus dem Puffer löschen soll, wenn das Programm geschlossen wird.

Abbrechen
Verwirft alle Änderungen, welche im Konfigurationsfenster vorgenommen wurden und kehrt zum DriveCrypt Hauptbildschirm zurück.

Alles übernehmen
Akzeptiert alle Änderungen und kehrt zum DriveCrypt Hauptbildschirm zurück.

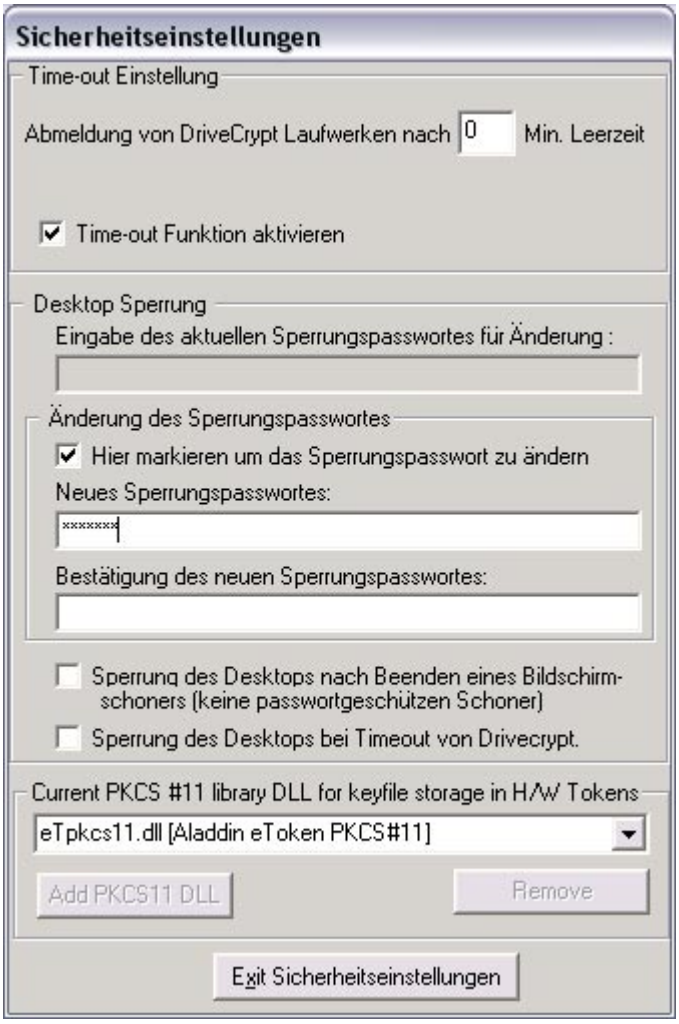
Einstellung der Hotkeys

© 2003 SecurStar

Öffnet den Einstellungsbildschirm zur Konfiguration der Hotkeys, mit deren Hilfe es möglich ist, schnell Laufwerke anzumelden/abzumelden und die Sperrung der lokalen Konsole zu erwirken.

Sicherheitseinstellungen

© 2003 SecurStar



Öffnet den Einstellungsbildschirm und ermöglicht die Einstellung von: Zeitabschaltungs-Sicherheitseinstellungen und das **Passwort für die Sperrung der lokalen Konsole**.

Hier können auch neue PKCS#11 Treiber für externe USB-Token definiert werden.

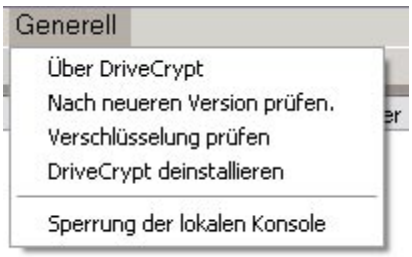
Dateibezeichnung / Autostart

© 2003 SecurStar

Öffnet den Einstellungsbildschirm für die Autostart-Funktion sowie die Dateibezeichnungszuweisungen. Für mehr Details sehen Sie die Kapitel "**AutoStart Drivecrypt**" und "**Einstellung der Laufwerksassoziierung**".

4.6 Menüfunktionen: Generell

Generell:



Über DriveCrypt:
Programmier- und Versionsinformationen.

© 2003 SecurStar

Nach neueren Version prüfen:
Wird auf dem online server geprüft ob eine neuere Version existiert. Eine Mitteilung mit der Versionsinformation (und eventuell eine andere Mitteilung) wird erscheinen.

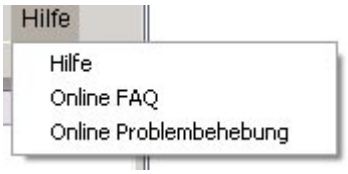
Verschlüsselung prüfen:
Startet ein Dienstprogramm, welches die von DriveCrypt genutzten Algorithmen dahingehend überprüft, ob diese den gleichen Chiffretext erstellt, der auch im Internet publiziert ist und als 'sicher überprüft' gilt.

DriveCrypt deinstallieren:
Entfernt das DriveCrypt Programm und deren Treiber komplett aus dem System.

Sperrung der lokalen Konsole:
Startet den lokalen Konsole-Aussperrmodus.
(Mehr Informationen finden Sie hierzu im Kapitel
Sperrung der lokalen Konsole)

4.7 Menüfunktionen: Hilfe

Hilfe:



Hilfe:
Startet die Hilfsfunktion.

Online Frequent Asked Questions:
Springt zum FAQ Bereich von Drivecrypt.

Online Knowledge Database:
Springt zur online Knowlegebase, welche man durchsuchen kann.

© 2003 SecurStar

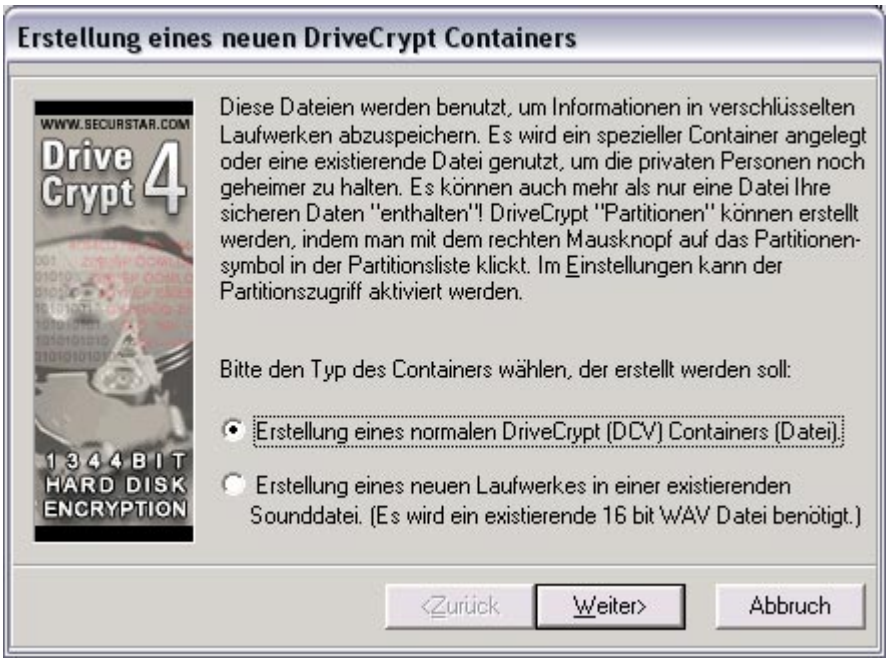
5 Benutzung von DriveCrypt

5.1 Erstellung eines verschlüsselten Laufwerkes

Um ein verschlüsseltes Laufwerk zu erstellen, muss man im Hauptfenster von DriveCrypt auf das Symbol „*Laufwerk erstellen*" klicken.

Ebenso kann aus dem **Datei-**Menü "***Laufwerk erstellen***" ausgewählt werden. Alternativ gibt es die Möglichkeit, mit der rechten Maustaste auf das DriveCrypt Symbol in der Taskleiste zu klicken und „***Laufwerk erstellen***" auszuwählen

Im neuen Dialog wählt man: ***Erstellun eines normalen DriveCrypt (DCV) Containers (Datei)***,
und mit ***WEITER*** bestätigen.



Hinweis: Falls das neue Laufwerk in einer Musikdatei erstellt werden soll (16 Bit .WAV), schlagen Sie bitte das Kapitel „***Verstecken eines Laufwerkes in einer Musikdatei***" auf.

© 2003 SecurStar

Im nächsten Dialog kann der Dateiname sowie die Position des neuen Containers angegeben werden. Ebenso ist es hier möglich, die Größe des Laufwerkes und das Formatierungsverfahren zu definieren.

Hinweis: Die Größe des Containers hängt von der Auswahl des Formatierungsverfahren ab. Wählen Sie das Ihnen am meisten zusagende Dateiformat nach der folgenden Tabelle aus.

Dateiformat	Betriebssystem	Laufwerksgröße
FAT 16	Windows 95/98/ME / NT/2000/XP	256 kb up to 2GB
FAT 32*	Windows 98/ME/2000/XP	512 MB bis zu 4GB (Unbegrenzt, falls d Container auf einer NTFS partition, im NTFS Format ist)
NTFS*	Windows NT /2000 /XP	5 MB bis zu 4GB (Unbegrenzt, falls d Container auf einer NTFS partition, im NTFS Format ist)

** Die DriveCrypt Home Edition erstellt nur FAT und Fat 32 Container. Die maximale Grösse für FAT 32 Container ist 4 GB*

Schnellerstellung: Bei diese Funktion wird DriveCrypt nicht vor der Erstellung eines neuen Containers den nötigen Speicherplatz löschen. Dies beschleunigt den Formatierungsprozess, stellt aber keine hohe

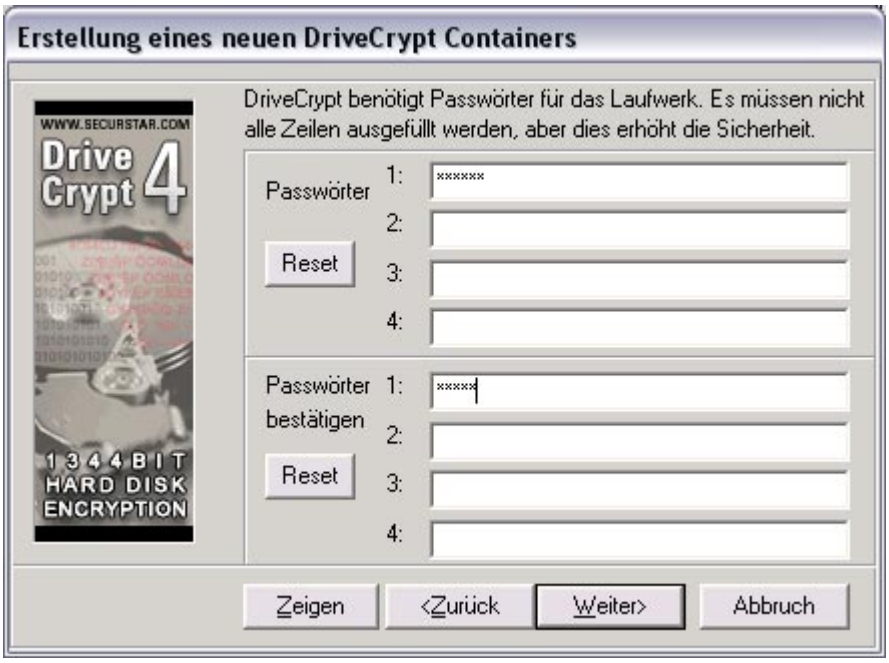
© 2003 SecurStar

Sicherheit dar, da gelöschte Dateien auf der Festplatte wieder hergestellt werden können. Auch ist es für Experten möglich, festzustellen, wie viele Sektoren der Festplatte für das neue DriveCrypt Laufwerk benutzt wurden (aber nicht was in ihnen abgespeichert ist).

Wurde ein Container mit NTFS angelegt, kann die „Schnell-Erstellung"-Funktion ohne Risiko benutzt werden, da das NTFS Format trotzdem auch auf die ausgelassenen Sektoren schreibt, solange diese noch nicht vom Container genutzt werden.

Wählen Sie bitte ***WEITER***, um fortzufahren.

Auswahl eines Passwortes: Im Passwortdialog geben Sie bitte Ihr gewünschtes Passwort ein, mit dem Sie das zu erstellende Laufwerk öffnen möchten. Bitte beachten Sie, dass ein Passwort nicht kürzer als acht, und nicht länger als 39 Zeichen sein darf.



Um ein sicheres Passwort zu wählen wird empfohlen, Wörter in Kombination von Groß- und Kleinbuchstaben, sowie Satzzeichen und Zahlen zu verwenden. Man kann auch Sätze als Passwort definieren. Beispiel: ***"Mit DriveCrypt sind meine Daten sicher !"***

Hinweis: Um die Sicherheit zu erhöhen, kann man bis zu vier Passwörter in den unterschiedlichen Zeilen angeben (Damit werden Benutzer der Software dazu angehalten, umfangreichere Passwortketten anzugeben. Jedes Passwort muss auch bei der

© 2003 SecurStar

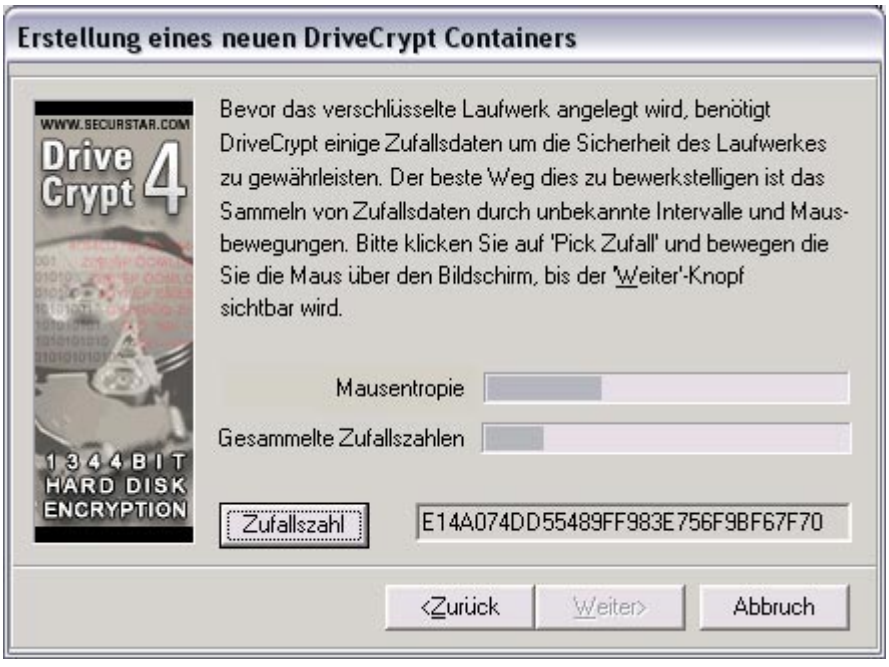
Entschlüsselung in der richtigen Reihenfolge und Zeile eingegeben werden, da diese alle zusammen als ein einziges Passwort von DriveCrypt für die Verschlüsselung/Entschlüsselung genutzt werden).

WICHTIG: Diese Passwortkette wird in Zukunft benötigt, um auf ein verschlüsseltes Laufwerk wieder zugreifen zu können. Deswegen sollte man sicherstellen, das man die Passwörter und deren Reihenfolge nicht vergisst. Anderenfalls ist es unmöglich, Ihre verschlüsselten Daten wieder herzustellen.

Sobald ein Passwort ausgewählt und zweimal zur Überprüfung eingegeben wurde, kann mit "***WEITER***" fortgefahren werden.

Datensammlung per Zufallsprinzip: Um ein hohes Maß an Sicherheit zu gewährleisten, erstellt DriveCrypt jedes Laufwerk auf unterschiedliche Arten (selbst wenn das gleiche Passwort und die selbe Laufwerksgröße bei der Laufwerkserstellung definiert wurden. Hierfür sammelt DriveCrypt einige Daten per Zufallsprinzip.

Bewegen Sie bitte die Maus über den Bildschirm und klicken hierbei mehrere Male auf den "Pick/Zufall" Knopf bis beide, die ***Mausentropie*** und die **Gesammelte Zufallszahlen,** voll aufgefüllt sind. Wenn dies geschehen ist, drücken Sie auf ***Weiter***.



Auswahl der Verschlüsselung:

© 2003 SecurStar

Hier wird der Verschlüsselungsalgorithmus definiert, mit dem das zu erstellende Laufwerk verschlüsselt werden soll.

Die Voreinstellung ist **AES 256.** Alternativ kann gewählt werden zwischen:
Triple AES, Blowfish, Triple Blowfish, Tea 16, Tea 32, DES, Triple DES, Square und **Misty 1.**

Nachdem ein Verschlüsselungsalgorithmus ausgewählt wurde, wird der Knopf "**Weiter**" sichtbar und man kann zum Abschlussdialog überwechseln.

Nach einen Klick auf "***Erstellung"*** wird das verschlüsselte Laufwerk angelegt und im System angemeldet.

5.2 Erstellung einer verschlüsselten Festplattenpartition

Die DriveCrypt Standardversion erlaubt es, eine physische (RAW) Festplattenpartition in eine geschützte, verschlüsselte Partition zu verwandeln.

WARNUNG: Das Arbeiten mit Festplattenpartitionen kann gefährlich sein und zu Datenverlust führen. Falls Sie nicht mit der Konfiguration von Festplattenpartitionen vertraut sind, wird empfohlen, keine Partitionen zu verschlüsseln. SecurStar GmbH kann für eventuell entstandene Datenverluste nicht zur Verantwortung gezogen werden.

Hinweis: Um Benutzer davor zu schützen, Versehentlich ihre Partitionen zu löschen, muss das DriveCrypt Partitionsmanagement manuell durch das Optionsmenü von DriveCrypt aktiviert werden. Hierzu wählt man ***Optionen*** und markiert die Auswahl "***Partitionszugriff aktivieren***", gefolgt von: "***Alles übernehmen***". Nun erscheinen alle verfügbaren Partitionen auf dem DriveCrypt Hauptbildschirm und können ausgewählt werden.

Um die vorhandenen Partitionen zu verschlüsseln, klickt man auf diese mit der rechten Maustaste und selektiert "***Partition als DriveCrypt formatieren***" innerhalb des auftauchenden Dialogfensters.

Nun kann man zwischen Fat16, Fat32 und NTFS das bevorzugte Dateiformat auswählen. Ist dies geschehen, *drückt man auf* ***"Weiter"***

© 2003 SecurStar

um fortzufahren…..

Um den Erstellungsprozess zu vervollständigen, folgt man den einzelnen Schritten von **Erstellung eines verschlüsselten Laufwerkes**.

5.3 Ein Laufwerk innerhalb einer Musikdatei verstecken

DriveCrypt erlaubt es Informationen in Sounddateien (.wav-Dateien) zu verstecken.
Diese Technik wird Steganographie genannt und gebraucht den ungenutzten Platz in Musikdateien.

Um ein verschlüsseltes Laufwerk in einer 16 Bit WAV Musikdatei zu erzeugen, klicken Sie auf das „Laufwerk Wizard" Symbol.

Alternativ kann aus dem Dateimenü des DriveCyrpt Hauptbildschirm "***Erstellen einer Container Datei***" ausgewählt werden, bzw. mit einem Klick der rechten Maustaste auf das DriveCrypt Symbol in der Taskleiste.

Bei diesem Punkt muss nun ausgewählt werden "***Erstellung eines neuen Laufwerkes in einer existierenden Sounddatei***", danach auf "weiter".

Auf dem nächsten Dialogfenster gibt man an, wie viele Bits der Audiodatei benutzt werden dürfen, um ein Laufwerk zu erstellen. Der Unterschied zwischen 4 und 8 Bits liegt darin, dass bei 4 Bit die Qualität der Sounddatei besser erhalten bleibt, während bei 8 Bit der Generator eine höhere Laufwerksgröße ermöglicht.

Auch muss der Name der Datei angegeben werden, in der die Daten versteckt werden sollen, sowie das Diskettenformat für die Formatierung.
Ist dies abgeschlossen, bitte mit ***"Weiter"*** fortfahren.

Um den Erstellungsprozess zu vervollständigen, folge man den Schritten von Kapitel "**Erstellung eines verschlüsselten Laufwerkes**"**.**

© 2003 SecurStar

Hinweis: DriveCrypt arbeitet mit 16 Bit Stereo .wav Dateien. Passende Dateien können mit Programmen wie **'WinDac'** oder **'Cool Edit'** hergestellt werden (man kann diese Programme direkt von der Downloadseite auf http://www.securstar.com herunterladen. Um eine bessere Performance zu erhalten, sollten keine Wav Dateien benutzt werden, welche totale Stille am Anfang des Musikstücks aufweisen.

5.4 Anmelden von verschlüsselten Laufwerken

Man kann Laufwerke auf verschiedene Arten hinzufügen :

Im **Hauptbildschirm** wählt man das Symbol "Laufwerk hinzufügen" aus:

Alternativ kann über das Dateimenü des DriveCrypt Hauptbildschirm "***Container hinzufügen***" oder durch Klick mit dem rechten Mausknopf auf das DriveCrypt Symbol in der Taskleiste ausgewählt werden.

Im Ergebnisdialogfenster :
Man definiert den Pfad und den Namen für das verschlüsselte Laufwerk und drückt auf ***Hinzufügen***

-ODER-
Man durchsucht die Festplatte und doppelklickt die Datei.

Es kann auch ein Laufwerk auf diese Weise hinzugefügt werden :

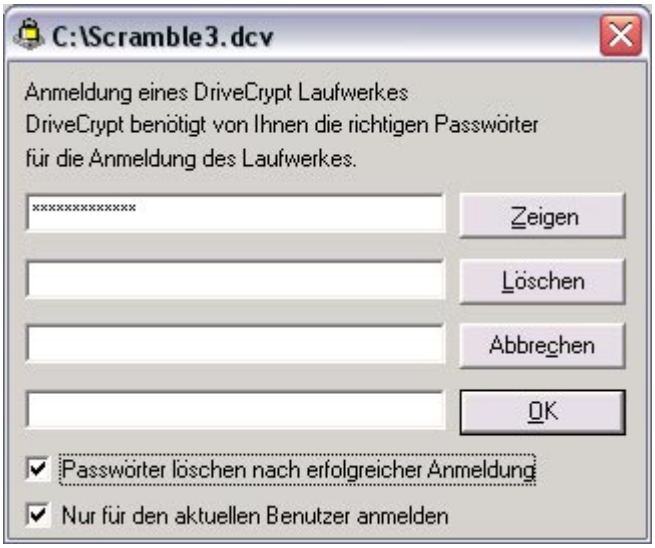
Man zieht die verschlüsselte Laufwerksdatei von einem Explorer Fenster in den DriveCrypt Hauptbildschirm.

-ODER-
Falls die .DCV Endung auf DriveCrypt registriert wurde (siehe Kapitel Erstellung von Dateiendungen), startet/öffnet man diese Datei im Windows-Explorer.

-ODER-
Wenn das "Laufwerksprotokoll" eingeschaltet ist, kann man das zuletzt erfolgreich hinzugefügte Laufwerk im DriveCrypt Hauptbildschirm auswählen, indem man über das "**Datei**" Menü eine Liste der letzten 8 erfolgreich geladenen Laufwerken erhält. (Für mehr Details über wie man das "Laufwerksprotokoll" aktiviert, ist im Kapitel "**Aktivierung der Protokollierung von hinzugefügten Laufwerken**" zu finden).

-ODER-
Man drückt den Knopf ***Hotkey hinzufügen***. Dies fügt das zuletzt erfolgreich geladene Laufwerk hinzu. (Für mehr Details über die Einstellung von Hotkeys sehen Sie bitte im Kapitel: **Hotkey Einstellungen**).

Eingabe eines Laufwerkpasswortes…



Geben Sie die Passwortkette ein, für die Sie sich entschieden haben, als das verschlüsselte Laufwerk erstellt wurde. Das Passwort muss in den selben Zeilen eingegeben werden, wie es auch angelegt wurde. Bestätigen Sie die Eingabe mit ***OK*** oder der ***Eingabe-Taste***

© 2003 SecurStar

Das angemeldete Laufwerk wird jetzt in der ersten freien Zeile im Hauptbildschirm von DriveCrypt angezeigt. Wenn im Explorer auf "Arbeitsplatz" geklickt wird, wird das Laufwerk mit den bereits vorhandenen Festplatten und Laufwerken angezeigt.

HINWEIS : Es sollten auch die Anweisung für die Einstellung der Laufwerke beachtet werden, in denen man definieren kann, wie die Laufwerke erscheinen sollen.

5.5 Anmeldung einer verschlüsselten Festplattenpartition

Es gibt verschiedene Möglichkeiten eine Partition in DriveCrypt anzumelden:

Klicken Sie auf das Passwortsymbol im DriveCrypt Hauptbildschirm.

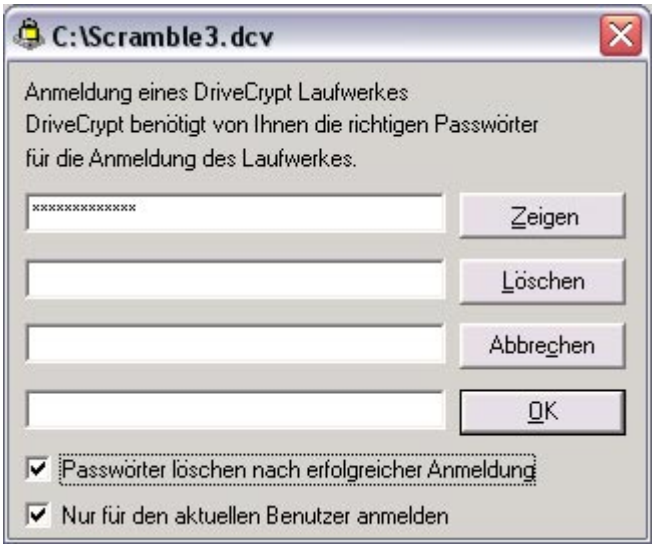
-ODER-
Klicken Sie auf "***Eingabe des Festplattenpasswortes***" in den *Passwortoptionen* im Hauptbildschirm.

-ODER-
Klicken Sie mit der rechten Maustaste auf das DriveCrypt-Symbol in der Taskleiste und wählen : "***Passworteingabe***"

-ODER-
Klicken Sie mit der rechten Maustaste auf die Partition im Partitionsfeld im Hauptbildschirm. Danach wählen Sie "***Diese Partition hinzufügen***"

Im erscheinenden Passwortfenster gibt man die Passphrase für die gewählte Partition ein und bestätigt mit ***OK***.

© 2003 SecurStar



DriveCrypt wird nun alle Partitionen des Computersystems durchsuchen und danach diese mit Hilfe des eingegeben Passwortes hinzufügen.

Hinweis: Falls gewünscht wird, dass DriveCrypt nicht alle Partitionen mit der angegebenen Passwortkette öffnet und anmeldet, markieren Sie bitte das Kästchen „**Keine Suche nach DriveCrypt-Partitionen nach Eingabe des Passwortes**" im **Optionen-** Fenster.

Das angemeldete Laufwerk wird jetzt in der ersten freien Zeile im Hauptbildschirm von DriveCrypt angezeigt. Im Explorer wird das Laufwerk neben den bereits vorhandenen Festplatten und Laufwerken unter dem „Arbeitsplatz" angezeigt.

HINWEIS: Es sollten auch die Anweisung für die Einstellung der Laufwerke beachtet werden, in denen man definieren kann, wie die Laufwerke erscheinen sollen (Laufwerksbuchstabe usw).

5.6 Zugriff auf ein verschlüsseltes Laufwerk

Starten Sie DriveCrypt und folgen Sie den hier aufgeführten Anweisungen, um auf ein Laufwerk zuzugreifen.

Es gibt unterschiedliche Möglichkeiten auf ein verschlüsseltes Laufwerk zuzugreifen:

Vom Hauptbildschirm aus klicken Sie auf das „Laufwerk anmelden"-Symbol (genauere Erläuterungen hierzu sind im Kapitel **Erklärung des Hauptbildschirms** zu finden).

© 2003 SecurStar

-ODER-
Vom Explorer / Dateimanager aus den selben Weg, wie man auf ein Laufwerk zugreift.

-ODER-
Von jedem Dateidialogfenster aus z.B. über das **Start-**Menü „Ausführen..." aufrufen oder das „**Datei öffnen"-**Dialogfenster in jeder Microsoft Office Anwendung etc.

-ODER-
Von einer MS-DOS Shell den zutreffenden Laufswerksbuchstaben eingeben, als würde man auf eine Festplatte zugreifen.

Die Masse der Operationen des verschlüsselten Laufwerks hängt vom dem jeweiligen Benutzer oder der laufenden Anwendung ab.

Verschlüsselte Laufwerke bleiben aktiviert, bis Windows beendet oder das Laufwerk abgemeldet wird. Da die auf Systembasis laufende Laufwerktreiberkomponente durchwegs immer geladen und im System vorhanden ist, muss DriveCrypt nicht gestartet sein, damit ein angemeldetes verschlüsseltes Laufwerk geöffnet werden kann.

5.7 Abmeldung von verschlüsselten Laufwerken

Um den Zugriff auf ein angemeldetes Laufwerk/Partition wieder für andere zu sperren, muss das Laufwerk abgemeldet werden.

Es gibt zwei Möglichkeiten, um ein Laufwerk / eine Partition abzumelden :

1) Die normale Abmeldung
Erlaubt es ein Laufwerk / eine Partition abzumelden, solange keine Datei dieses Laufwerks in Gebrauch ist. (Dies verhindert, dass geöffnete, ungesicherte Daten verloren gehen, falls das Laufwerk geschlossen wird).

2) Die abrupte Abmeldung:
Dies bewirkt, dass alle Laufwerke geschlossen werden, unabhängig davon, ob Dateien geöffnet sind oder Programme auf das Laufwerk zugreifen. (Dies wird normal in Panikmomenten benutzt, wenn es notwendig ist, das geöffnete Laufwerk schnell zu schließen.).

Hinweis: *Bei Windows NT/2000/XP Systemen, auf denen Festplattenhilfsprogramme wie Antivirus-Checker oder andere Tools auf*

© 2003 SecurStar

Pfade des DriveCrypt-Laufwerks zugreifen, ist es normal, das Laufwerk durch abrupte Abmeldung zu beenden.

Man kann die Abmeldung auf verschiedene Arten durchführen :
Aus dem **Abmeldungs**menü,

-ODER-
Man wählt **Abrupte Abmeldung** um alle angemeldeten Laufwerke abrupt abzumelden. DriveCrypt wartet nach dem letzten Lese/Schreib-Zugriff auf das Laufwerk ca. 2 Sekunden, damit Datenschreibvorgänge abgeschlossen werden usw.

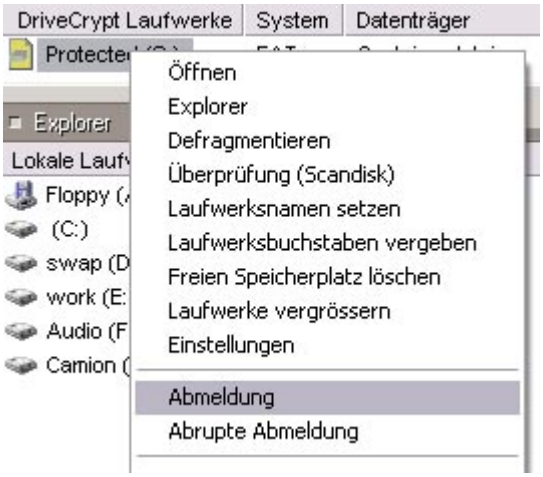
-ODER-
Auf dem DriveCrypt Hauptbildschirm drückt man auf folgendes Symbol, welches auf normalem Wege angemeldete Laufwerke abmeldet.

-ODER-
Auf dem DriveCrypt Hauptbildschirm drückt man auf dieses Symbol, um eine abrupten Abmeldung von angemeldeten Laufwerken durchzuführen.

-ODER-
Abmeldung der angemeldeten Laufwerke durch Hotkeys. Bitte sehen Sie hierzu im Kapitel **Konfiguration** nach.

-ODER-

© 2003 SecurStar



Falls es gewünscht wird, nur ein bestimmtes Laufwerk abzumelden und die anderen aktiv zu lassen, klickt man mit rechten Maustaste auf das Symbol des angemeldeten Laufwerks im DriveCrypt Hauptbildschirm, und wähle aus dem auftauchenden Dialogfeld aus:
Abmeldung / Abrupte Abmeldung

© 2003 SecurStar

6 Unsichtbare Container

6.1 Was ist ein Unsichtaber Container

DRIVECRYPT hat die Möglichkeit, ein unsichtbares Laufwerk in einem Container zu erstellen.
Unter WinXP/2000 und NT funktioniert dies auch in Partitionen.

Sie können zwei Passwörter definieren, eines für den "sichtbaren" und eines für den "unsichtbaren" Container.

Das Passwort des "sichtbaren" Laufwerks gibt Ihnen den Zugriff auf Ihre Arbeitsplatte, welche im ungenutzen Bereich des "sichtbaren" Bereichs versteckt ist. Dort speichern Sie nur von Ihnen "präparierte" Daten ab, die im Notfall jeder sehen darf.

Diese Funktion ist sehr hilfreich, wenn Sie gezwungen werden, Ihr Passwort zu nennen.

Sie geben dann einfach Ihr Passwort für den "sichtbaren" Bereich heraus und Ihr Gegner wird nur Daten sehen, die Sie vorher präpariert haben.

6.2 Erstellen von unsichtbaren Containern

Step 1: Einen normalen Container erstellen.

Um ein unsichtbares Laufwerk erstellen zu können, müssen Sie zuerst ein Verschlüsseltes Laufwerk einrichten. Das kann ein Container oder eine Partition sein. Sehen Sie dazu auch:
Erstellung eines verschlüsselten Containers oder
Erstellung einer verschlüsselten Partition

***Hinweis*:** Sie können versteckte Laufwerke in jedem CONTAINER unabhängig vom Windows Betriebssystem erstellen. Versteckte Laufwerke in Partitionen funktionieren unter Windows NT /2000 and XP. *Windows 98 PARTITIONEN unterstützen KEINE versteckten Laufwerke!!*

Step 2: Präparieren Sie Ihren Container mit künstlichen Daten

© 2003 SecurStar

Wenn Ihr Container erst einmal erstellt wurde (z. B. mit einer Grösse von 300 MB) kann es losgehen.
Ist er noch nicht angemeldet, so nehmen Sie die Anmeldung manuell vor. Füllen Sie ihn mit ein paar belanglosen Daten, welche für Sie nicht besonders wichtig sind. Es wird Ihnen so nichts ausmachen, wenn Sie Ihr Passwort einmal rausgeben müssen.

Bitte beachten sie, dass der Speicherplatz, den Sie für Ihre Fakedaten verwenden die maximale Grösse Ihres unsichtbaren Laufwerkes verkleinern wird.

In unserem Beispiel bedeutet das, dass Sie noch 250MB freien Speicher für Ihr unsichtbares Laufwerk haben, wenn Sie 50MB Fakedaten vorab einspielen.

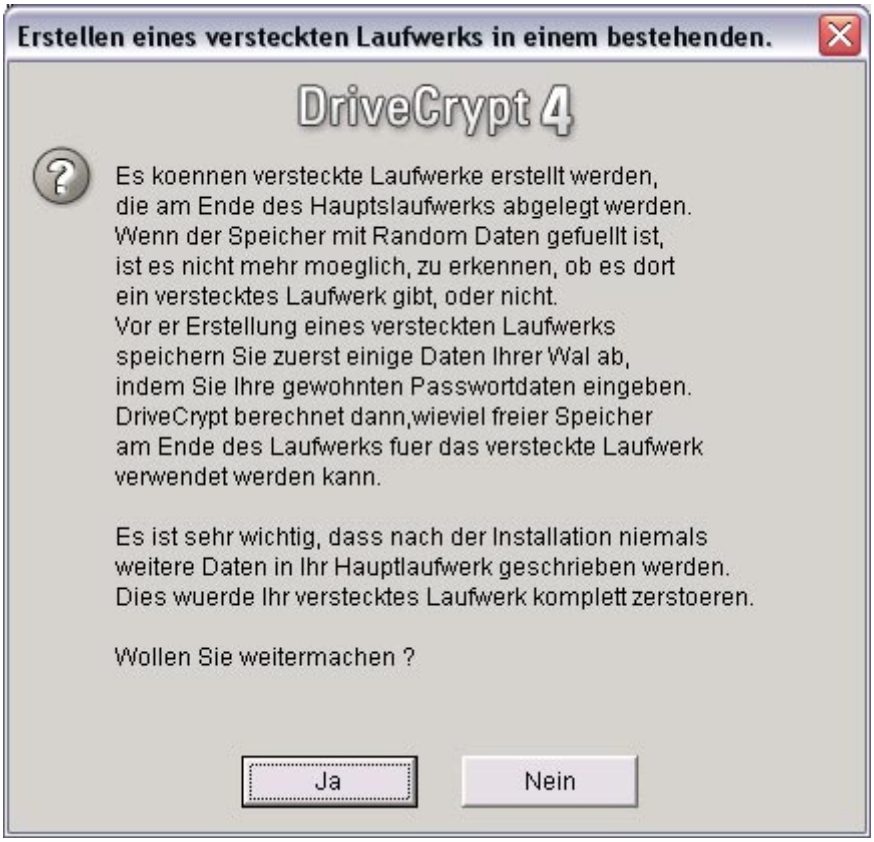
Hinweis: Wenn Sie einen neuen Container oder eine neue Partition verwenden, sollten Sie wissen, dass die Blockaufteilung (grösster Block) die reale Grösse Ihre unsichtbaren Laufwerks verringern kann. Sie sollten deshalb vorsorglich vor der Erstellung des unsichtbaren Laufwerks den Container **defragmentieren**, um den freien Speicher zu optimieren.

Step 3: Das unsichtbare Laufwerk einrichten

Auf dem DRIVECRYPT Hauptbildschirm klicken Sie einfach mit der rechten Taste auf den angemeldeten Container. Wählen Sie anschliessend in Dialogfeld die Funktion "Unsichtbare Container Erstellung".

© 2003 SecurStar

Dies startet den Hilfsagenten zur Erstellung des unsichtbaren Laufwerks:



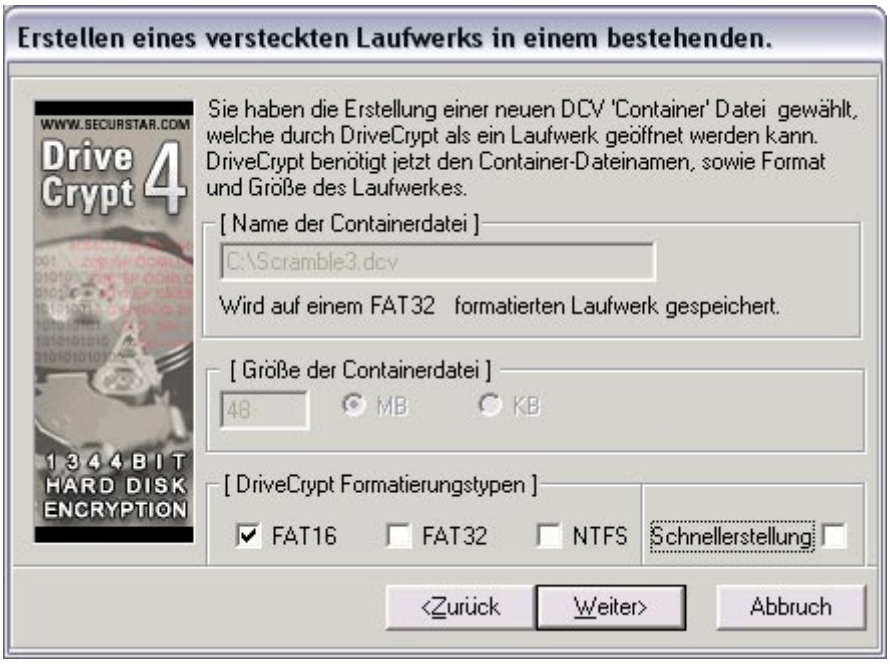
Wenn Sie sich sicher sind, klicken Sie auf "*JA*". DRIVECRYPT frägt nun nach Ihrem ersten Passwort (Aus Step1). Das stellt sicher, dass Sie auch der Eigentümer, bzw. die legitimierte Person für die Erstellung sind.

Im nexten Bildschirm berechnet DRIVECRYPT den verfügbaren Speicherplatz für das unsichtbare Laufwerk. Weiterhin haben Sie hier die Möglichkeit, den sichtbaren "unwichtigen" Bereich mit den "Nur lesen" - Rechten zu belegen. Wenn Sie vorab eine Defragmentierung des sichtbaren Bereichs vorgenommen haben, erreichen Sie die maximale Grösse Ihres versteckten Laufwerks.

© 2003 SecurStar

Warnung : Wenn Sie einmal einen versteckten Bereich eingerichtet haben, sollten Sie nie mehr Daten in den präparierten sichtbaren Bereich schreiben. Ihre Daten im versteckten Bereich könnten so verloren gehen. Genau deswegen setzen wir per Standardeinstellung die Rechte des sichtbaren Bereichs auf "Nur lesen".

Auf JA klicken schaltet zum folgenden Bildschirm:



© 2003 SecurStar

Sie können jetzt das Formatsystem für das versteckte Laufwerk einrichten und mit der Erstellung so fortfahren, wie Sie dass von normalen Containern gewöhnt sind.

WARNUNG : Benützen Sie nie ein Passwort für Ihr unsichtbares Laufwerk, dass mit dem des sichtbaren Bereichs übereinstimmt oder diesem ähnlich ist.
Beide Container (sichtbar und unsichtbar) MÜSSEN UNTERSCHIEDLICHE Passwörter haben. Sie haben sonst keine Möglichkeit mehr, den unsichtbaren Container anzumelden.

6.3 Anmelden eines Invisiben Containers

Sie können ein verstecktes Laufwerk genauso anmelden wie ein gewöhnliches. Der einzige Unterschied: Sie können Ihr Passwort für den unsichtbaren Bereich eingeben und gleich die sensiblen Daten nutzen.

Hier ist eine Schritt für Schritt Anleitung:

Sie können das versteckte Laufwerk auf drei Wegen zur Anmeldung bringen:

Auf dem Hauptbildschirm das "***Laufwerk anmelden***" Icon klicken.

Oder Sie klicken auf die "***Container Anmelden***" Funktion im **D**atei Menü des DriveCrypt Hauptbildschirms.
Auch ein Klick mit der rechten Taste auf das Icon in der Taskleiste gibt Ihenn die Möglichkeit zur Anmeldung.

Im folgenden Dialogbildschirm:
Geben Sie den Pfad des verschlüsselten Laufwerks an und drücken dann ***A***nmelden

-ODER-
Browsen Sie zum Laufwerk und starten Sie mit einem Doppelklick.

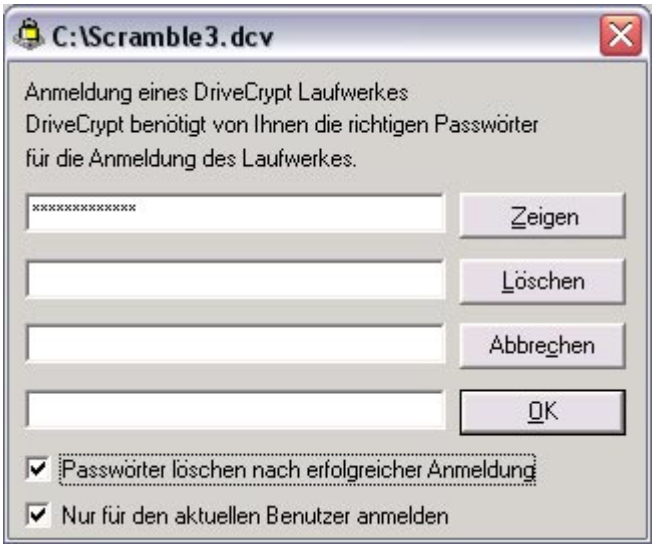
© 2003 SecurStar

Sie können auch wie folgt ein Laufwerk anmelden:

Mit Drag and Drop vom Explorer aus das Container Icon auf das DriveCrypt Icon ziehen.

-ODER-
Wenn Sie .DCV Dateitypen mit DriveCrypt assoziiert haben (siehe Hilffefunktion… Extensionen assoziieren), können Sie diese im Explorer durch einen Doppelklick starten.

Geben Sie hier das Passwort für das unsichtbare Laufwerk ein…



Geben Sie Ihre Daten, welche Sie bei der Erstellung gewählt haben ein. Die

© 2003 SecurStar

Reihenfolge der einzelnen Reihen muss der eingestellten entsprechen (entfällt, wenn Sie nur eine Reihe belegt haben).
Mit ***OK*** oder ***Enter*** bestätigen.

Der unsichtbare Container wird angemeldet und erscheint im ersten freien Slot des Hauptbildschirms von DriveCrypt. Auch im Arbeitsplatz erscheint jetzt das Laufwerk. Es sieht wie ein normales Festplattenlaufwerk aus.

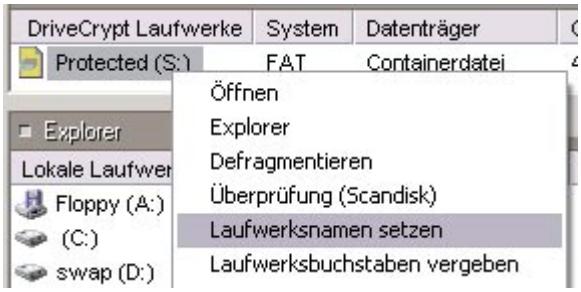
© 2003 SecurStar

7 Festplatteneinstellungen / Werkzeuge

7.1 Vergabe eines Laufwerksnamen

DriveCrypt erlaubt es einen Laufwerksnamen für alle direkt auf dem Hauptbildschirm befindlichen Laufwerken zu definieren und zu ändern.

Dazu klickt man mit der rechten Maustaste auf das Laufwerk, welches man benennen möchte. Dies öffnet ein neues Dialogfeld:



In diesem Dialogfeld wählt man: ***Laufwerksnamen setzen***

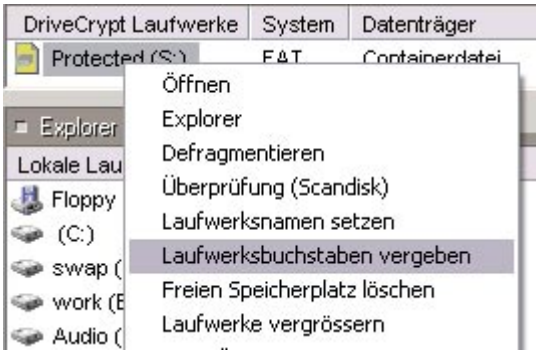
Nun gibt man den gewünschten Laufwerksnamen an und drückt auf ***Setzen***.

7.2 Definierung eines festen Laufwerksbuchstaben für ein verschlüsseltes Laufwerk

DriveCrypt erlaubt es, feste Laufwerksbuchstaben für ein verschlüsseltes Laufwerk zu vergeben. Dieser Buchstabe wird bei der nächsten Anmeldung für das Laufwerk benutzt (falls es noch aktiv ist, muss dieses abgemeldet und sodann neu angemeldet werden).

Im DriveCrypt Hauptbildschirm klickt man mit der rechten Maustaste auf das Symbol eines angemeldeten Laufwerkes, welches man mit einem festen Laufwerksbuchstaben belegen will. Dies öffnet ein neues Dialogfeld.

© 2003 SecurStar



In dem neuem Dialogfeld wählt man:***Laufwerksbuchstaben vergeben***

Nun wählt man den gewünschten Laufwerksbuchstaben aus, welcher für das verschlüsselten Laufwerk vorgesehen ist, und drückt danach auf ***Setzen***.

7.3 Passwortänderung eines verschlüsselten Laufwerks

DriveCrypt erlaubt es, das Laufwerkspasswort zu jeder Zeit zu ändern. Im DriveCrypt Hauptbildschirm klickt man mit der rechten Maustaste auf das angemeldete Laufwerk, bei welchem das Passwort geändert werden soll. Dies öffnet ein neues Dialogfeld.

In dem neuen Dialogfeld wählt man: ***Eigenschaften -> Neues Passwort***

DriveCrypt öffnet sodann ein Passwortdialogfeld.

© 2003 SecurStar

Hier gibt man das ***ALTE*** Passwort an und bestätigt mit ***OK***.
Dann gibt man das ***NEUE*** Passwort ein und bestätigt mit ***OK.***
Zur Sicherheit ***wiederholt man die Eingabe des NEUEN Passworts*** und beendet die Eingabe mit ***OK.***

7.4 Defragmentieren einer Festplatte / eines Laufwerks

Mit DriveCrypt ist es möglich, beides, also Festplatte und verschlüsseltes Laufwerk direkt vom Hauptbildschirm aus zu defragmentieren.

Im DriveCrypt-Hauptbildschirm klickt man mit der rechten Maustaste auf das zu defragmentierende Festplatten-/Laufwerkssymbol. Dies öffnet ein neues Dialogfeld.

Im neuen Dialogfeld wählt man: ***Defragmentieren***

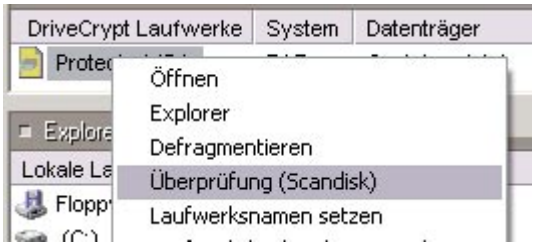
Hinweis: Bei Windows NT und 2000 Systemen kann es passieren, dass die Funktion ***Defragmentieren*** nicht sofort funktioniert, da diese noch nicht installiert wurde. Für Windows 2000 benötigt man die kommerzielle Version des "Diskeeper" (http://www.execsoft.co.uk) oder ähnliche Software, damit man DriveCrypt Laufwerke defragmentieren kann. Dies liegt daran, dass Windows 2000 nur eine Version enthält, mit der es möglich ist, Laufwerke zu defragmentieren, welche während des Bootvorgangs vorhanden sind.

7.5 Überprüfen einer Festplatte / eines Laufwerks (Scandisk)

Mit DriveCrypt kann man direkt über den Hauptbildschirm Festplatten oder verschlüsselte Laufwerke auf Fehler überprüfen lassen.

Im DriveCrypt Hauptbildschirm klickt man mit der rechten Maustaste auf das zu überprüfende Festplatten-/Laufwerkssymbol. Dies öffnet ein neues Dialogfeld.

© 2003 SecurStar



Im neuen Dialogfeld wählt man: ***Überprüfung (Scandisk)*** → ***Start.***

7.6 Festplatteneigenschaften

Mit DriveCrypt kann man die Festplatteneigenschaften von angemeldeten, verschlüsselten Laufwerken ansehen und ändern.

Im DriveCrypt Hauptbildschirm klickt man mit der rechten Maustaste auf das Symbol der Festplatte / des Laufwerks, zu welchen man die Eigenschaften wählen möchte. Dies öffnet ein neues Dialogfeld.

Im neuen Dialogfeld wählt man: ***Eigenschaften***

Im neuen Eigenschaftendialogfeld werden die aktuellen

© 2003 SecurStar

Festplatteneinstellungen angezeigt. Im Eigenschaftendialog kann man auch folgendes einstellen:

- **Setze verschlüsselte Laufwerke in den "Nur Lesen" Zustand**

Hierzu klickt man an **"Bei nächsten Anmeldung in DriveCrypt im -Nur Lesemodus-"**

- **Änderung des Laufwerk-Passworts:**

Hierzu wählt man **Neues Passwort**

DriveCrypt öffnet sodann ein Passwortdialogfeld.

Hier gibt man das ***ALTE*** Passwort an und bestätigt mit ***OK***.
Dann gibt man das ***NEUE*** Passwort ein und bestätigt mit ***OK.***
Zur Sicherheit ***wiederholt man die Eingabe des NEUEN Passworts*** und beendet die Eingabe mit ***OK.***

- **DKF wiederrufen**

Hierzu wählt man den Knopf ***"DKF wiederrufen"*** und bestätigt mit ***JA.***

7.7 Freien Speicherplatz löschen

DriveCrypt erlaubt es freien Festplatten-/Laufwerksspeicherplatz zu löschen.

Leerer Speicherplatz beinhaltet oftmals noch Daten von gelöschten Dateien, welche durch das Betriebssystem entfernt wurden.

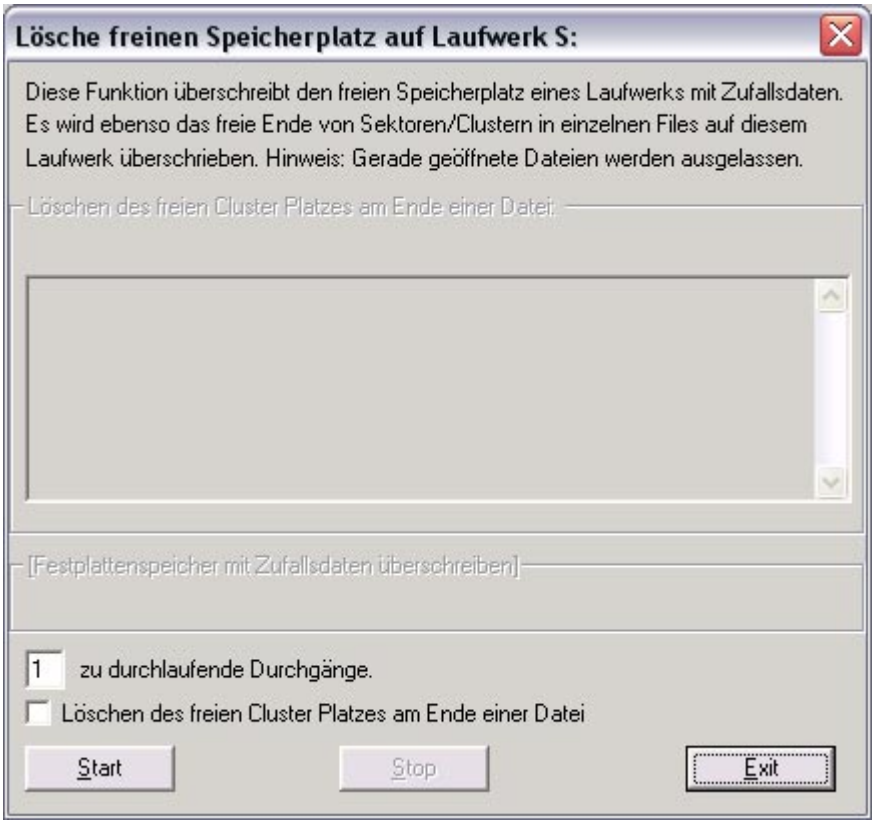
Das Überschreiben von freien Speicherplatz stellt sicher, dass zuvor gelöschte Daten auch wirklich entfernt werden und diese nicht durch Programme wie Undelete oder einem Festplattensektoren-Editor wiederhergestellt werden können. Dies wird mit Überschreiben des freien Speicherplatzes durch Zufallsdaten gewährleistet.

Es ist möglich, leeren Speicherplatz auf lokalen Festplatten sowie angemeldeten verschlüsselten Laufwerken zu löschen.

Im DriveCrypt Hauptbildschirm klickt man mit der rechten Maustaste auf das Symbol der Festplatte / des Laufwerkes, auf welcher der leere Speicherplatz gelöscht werden soll.

Dies öffnet ein neues Dialogfeld.

© 2003 SecurStar



Im neuen Löschdialogfenster kann man einstellen, wie oft man den freien Speicherplatz mit Zufallsdaten überschreiben möchte. Hierzu gibt man eine Zahl von **1 bis 99** in das ***Durchgänge*** Eingabefeld ein. Falls man auch belegten, aber gerade unbenutzten Speicherplatz des Ende einer jeden Datei löschen möchte, dann bitte auch das Feld „**Speicherleerbereich am Ende einer Datei löschen".**
Man startet den Überschreibvorgang mit einem Klick auf ***Start.***

7.8 Größe eines verschlüsselten Laufwerks ändern

DriveCrypt erlaubt es die Größe eines verschlüsselten Laufwerks zu ändern.

Im DriveCrypt Hauptbildschirm klickt man auf das angemeldete Laufwerk, welches in der Größe geändert werden soll. Dies öffnet ein neues Dialogfeld.

In dem neuen Dialogfeld wählt man: ***Laufwerkgröße ändern***

© 2003 SecurStar

DriveCrypt öffnet daraufhin ein Passwortfenster. Dies soll sicherstellen, dass derjenige, der die Größe des Laufwerks ändern möchte, auch der Besitzer bzw. die autorisierte Person ist. Hier gibt man ***das momentane Laufwerkspasswort ein***, und bestätigt mit ***OK***.

Falls das Laufwerk, welches man in der Größe ändern möchte, gerade durch ein Programm in Benutzung ist, kann man das Laufwerk abrupt abmelden falls nötig: Hierzu markiert man das Feld "***Abrupte Abmeldung des Containers***", dann drückt man auf "WEITER" zu fortzufahren.

Im neuen Dialogfeld gibt man die ***Neue Größe des Laufwerks*** ein, und bestätigt mit **WEITER** um den Änderungsvorgang zu starten.

Nachdem die Größe des Laufwerkes geändert wurde, kann man zum Hauptbildschirm zurückkehren, indem man auf ***Ende*** drückt.

7.9 Unsichtbare Contaiener

DriveCrypt ermöglicht es, Laufwerke in bestehenden Containern/Partitionen zu verstecken

Auf dem DriveCrypt Hauptbildschirm können Sie mit der rechten Maustaste auf das Laufwerk klicken, dass Sie in der Grösse verändern möchten. Dieser Vorgang öffnet ein neues Dialogfenster.
Dort wählen Sie: ***Unsichtbare Container Erstellung.***

© 2003 SecurStar

Hinweis:
Die Erstellung unsichtbarer Container in Partitionen funktioniert nicht unter Win98!
Deswegen ist diese Funktion unter Win98 einfach gesperrt..

© 2003 SecurStar

8 Einstellung von DriveCrypt Optionen

8.1 Assoziieren / Entassoziieren von .DCV .SVL .VOL .DKF Container / Schlüsseldatei mit DriveCrypt

DriveCrypt ermöglicht es, Betriebssystemendungen für DriveCrypt, ScramDisk und E4M erstellte Laufwerke, sowie .dkf Schlüsseldateien zu setzen oder aufzuheben. Die Dateiassozationen erlauben es DriveCrypt, sich automatisch zu starten, sobald ein verschlüsseltes Laufwerk mit einer der Endungen .dcv, .svl, .vol und .dkf durch Doppelklick auf die Maus ausgewählt wird.

Auf dem Hauptbildschirm wählt man ***Optionen*.**

Im **Optionen**menü wählt man den Knopf **Dateitypen/Startup**.

In dem daraus resultierenden Dialogfeld wählt man die Dateitypen, welche man automatisch assoziieren / entassoziieren möchte.

Im die neuen Einstellungen zu bestätigen, drückt man auf **OK**, um zum Optionen-Dialogfeld zurückzukehren. Dort bestätigt man die Änderungen mit **Änderungen übernehmen.**

Wenn man nächstes Mal auf einen Container- / Schlüsseldatei klickt, öffnet sich DriveCrypt und öffnet ein Passwortdialogfeld (falls das Passwort nicht bereits vorgemerkt wurde).

8.2 Aktivieren der Protokollierung von angemeldeten Laufwerken

Um eine Protokolldatei der zuletzt erfolgreich angemeldeten Laufwerke zu erhalten, muss man die Protokollierung der angemeldeten Laufwerke aktivieren. Dies kann nützlich sein, wenn Laufwerke per Hotkey angemeldet werden oder Laufwerke, ohne danach suchen zu müssen, auf dem System gefunden werden sollen.

Man kann diese Funktion aktivieren / deaktivieren, indem man das **Einstellungen**-Menü aus dem DriveCrypt Hauptbildschirm auswählt.

Im erscheinenden Einstellungendialog markiert man das Feld "Speichere Dateiprotokoll für Dateieinstellungen……". Darauf bestätigt man die Änderungen mit dem Knopf ***Änderungen übernehmen***.

© 2003 SecurStar

Hinweis: Falls die Protokolldateifunktion abgeschaltet wird, wird auch das bestehende Protokoll gelöscht.

8.3 Einstellung der Hotkeys für Anmelden / Abmelden / Aussperren

Mit DriveCrypt ist es möglich, Hotkeys für die sofortigen Zugriff auf folgende Kommandos zu definieren:

- Normale Abmeldung von angemeldeten Laufwerken
- Abrupte Abmeldung von angemeldeten Laufwerken
- Starten der Aussperrungskonsole
- Anmeldung der zuletzt erfolgreich angemeldeten Partition oder Laufwerk

Wie man die Hotkeys einstellt:

Auf dem DriveCrypt Hauptbildschirm wählt man die **Optionen -> Einstellung Hotkeys -> Sichere Hotkeys**.

Danach **wählt man das Feld** des Hotkeys, welchen man aktivieren möchte, und **gibt die gewünschte Hotkey**kombination ein.

Danach bestätigt man die Änderungen mit dem Knopf **Hotkey-Einstellungen verlassen**, und beim Einstellungsdialog drückt man den Knopf **OK**.

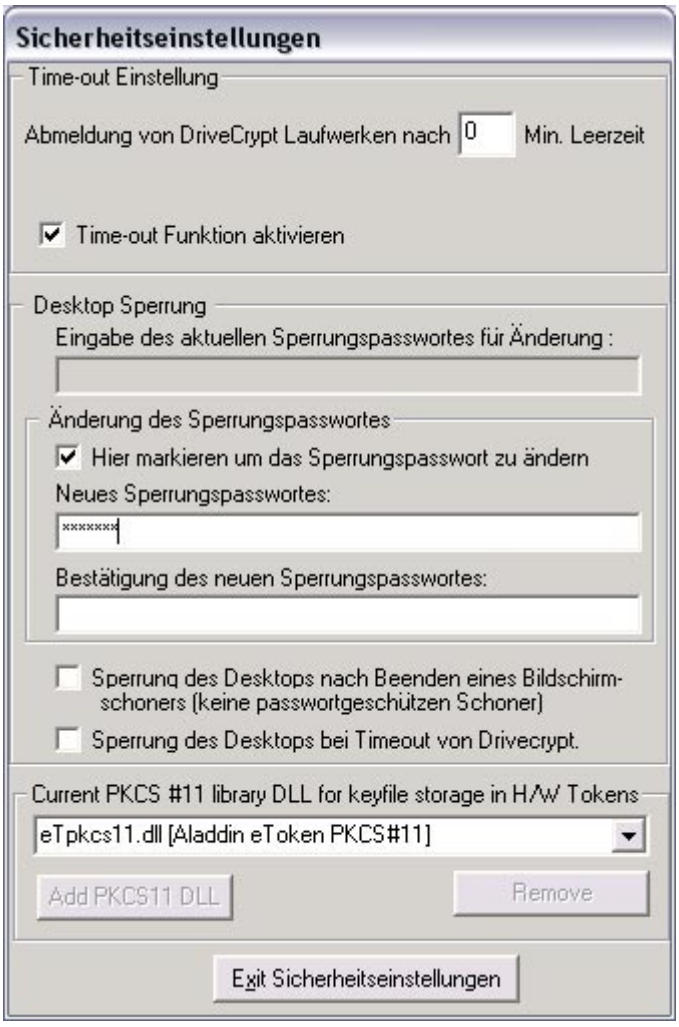
© 2003 SecurStar

8.4 Gebrauch der Timeout Funktion

DriveCrypt erlaubt es eine Timeout-Funktion für angemeldete Laufwerke zu setzen.
Dieser Timeout ermöglicht die automatische (normale oder abrupte) Abmeldung eines Laufwerks nach einer gewissen Laufwerksleerlaufzeit.

Auf dem Hauptbildschirm wählt man **Optionen.**

Vom **Optionen**menü wählt man **Sicherheitseinstellungen.**



Im erscheinenden Dialogfeld markiert man das Feld **Aktiviere Timeout Einrichtung** um diese Funktion zu aktivieren.

Hier gibt man die Leerlaufzeit in Minuten an, die DriveCrypt warten soll, bevor es versucht, eine normale Abmeldung aller Laufwerke

© 2003 SecurStar

durchzuführen. Dies kann fehlschlagen, wenn Dateien durch das Betriebssystem auf den verschlüsselten Laufwerken geöffnet sind.

Wenn man wünscht, dass DriveCrypt eine Abmeldung auf jeden Fall durchführen soll, markiert man das Feld "**Abrupte Abmeldung nach 15 Sekunden Leerlaufzeit, wenn ein Abmeldevorgang zuvor fehlgeschlagen ist**", damit DriveCrypt eine Abmelden der Laufwerke erzwingt. Diese wird 15 Sekunden nach dem ersten misslungenen Versuch geschehen.

Um die Änderungen zu bestätigen, muss das Dialogfeld mit **Exit** beendet werden. Im Optionenmenü zurückzugelangt wählt man dort **Änderungen übernehmen**.

8.5 DriveCrypt Autostart- und Laufwerksstartoptionen

Damit DriveCrypt während des Bootvorgangs automatisch mit Windows gestartet wird, wählt man auf dem Hauptbildschirm:

© 2003 SecurStar

Hier definiert man ob und wie Windows DriveCrypt beim Bootvorgang starten soll, indem man die jeweiligen Felder markiert.

Auch kann man definieren, ob DriveCrypt minimiert starten soll (nur auf der Windows Taskleiste als Symbol sichtbar)

Man kann auch auswählen, ob das DriveCrypt Symbol in der Taskleiste sichtbar sein soll.

Danach bestätigt man die Änderungen mit **OK,** danach auf dem Optionen-Dialogfenster mit **Änderungen übernehmen**.

8.6 Anmelden von verschlüsselten Laufwerken und Partitionen beim Starten des Computers

Es gibt zwei unterschiedliche Vorgänge um Laufwerke beim Systemstart anzumelden. Die Wahl des Vorgangs hängt von der Menge und des Typs der anzumeldenen Laufwerke ab.

Damit jede der Methoden funktioniert, müssen zuerst die Dateiendungen mit dem DriveCrypt-Hauptprogramm assoziiert worden sein. Um herauszufinden, wie dies funktioniert, sollte man das Kapitel "Wie man... Assoziieren von Container- und Schlüsseldateien mit Drivecrypt" beachten.

Nutzen Sie die hier abgedruckte Tabelle um auszuwählen, welcher Vorgang der richtige für Sie ist.

Verschlüsselte Laufwerke	**Methode**
Einzelner DateiContainer (.dcv) Laufwerk	1 - Verknüpfung zu Dateiname
Mehrfache DateiContainer (.dcv) Laufwerke	2 - Verknüpfung zu DKF-Datei
Steganographische (.wav) Laufwerke	2 - Verknüpfung zu DKF-Datei
Verschlüsselte Partitionen	2 - Verknüpfung zu DKF-Datei

Methode 1 - Verknüpfung zu Dateiname:

Man öffnet das **Start-Menü** mit einem Klick der linken Maustaste auf den

© 2003 SecurStar

Start-Knopf.

Anschließend das **Autostart**-Verzeichnis auswählen (dieses befindet sich innerhalb von **Programme**).

Nun klickt man mit der rechten Maustaste auf einen freien Platz in diesem Verzeichnis.

Man wählt **Neu** und **Verknüpfung erstellen** aus dem erscheinenden Menü.

Danach gibt man den Pfad der Containerdateien (.svl) in der **Kommandozeile** an und bestätigt mit **OK**.

Nun gibt man der Verknüpfung einen Namen und bestätigt abermals mit **OK**.

Wenn Windows nächstes Mal gestartet wird, öffnet sich DriveCrypt und verlangt nach einer Passworteingabe für die Containerdatei.

Nach der richtigen Eingabe wird das verschlüsselte Laufwerk zur Verfügung stehen.

Methode 2 - Verknüpfung zu DKF-Datei:

Zuerst müssen alle Containerdateien und Partitionen angemeldet werden, welche durch den Autostart angemeldet werden sollen.

Nun speichert man eine SKF Datei wie es im Kapitel "Wie erstellt man einen Zweitschlüssel Benutzerzugriff Schlüsseldatei" beschrieben ist.

Man folgt **Methode 1**, aber gibt als Pfad die Schlüsseldatei anstatt einer Containerdatei an.

Wenn Windows nächstes Mal gestartet wird, öffnet sich DriveCrypt und verlangt nach einer Passworteingabe für den Containerdatei.

Nach der richtigen Eingabe wird das verschlüsselte Laufwerk zur Verfügung stehen.

© 2003 SecurStar

8.7 Autostart Funktion für verschlüsselte Laufwerke

DriveCrypt bietet eine Funktion, welche es einem Programm oder einem assoziiertem Dokument erlaubt, diese auszuführen, wenn der bestimmte Container angemeldet wird.

Man erstellt eine Verknüpfung innerhalb des DriveCrypt Laufwerkshauptverzeichnisses ('f:\' als Beispiel), mit der etwas gestartet werden kann (wie ein Doppelklick auf die Verknüpfung), wann immer der bestimmte Container angemeldet wird.

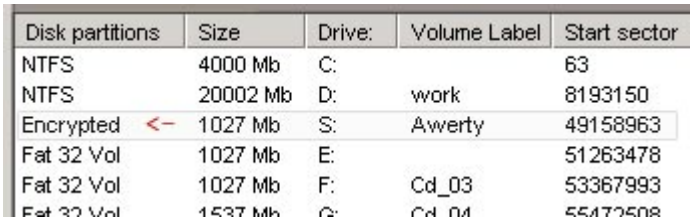
Umbenennung der Verknüpfung zu 'DriveCrypt'. Das ist alles! Jedes Mal, wenn der DriveCrypt Container angemeldet wird, werden die Anwendungen oder die Datendateien, welche in der Verknüpfung angegeben sind, gestartet.

Diese Funktion wurde eingebunden, da diese von mehreren Personen gewünscht wurde, da diese eine Möglichkeit gesucht haben, das Programme gestartet werden können, wenn diese im Autostart Menü definiert sind und sich auf einem DriveCrypt Laufwerk befinden. Nun ist es möglich, das ein Container angemeldet wird, wenn DriveCrypt aus dem Autostart "Startup" Menü geöffnet wird. DriveCrypt startet sodann die Anwendung wie dies voreingestellt ist.

Hinweis: Es besteht die Möglichkeit diese Funktion im **Optionen** dialog abzustellen.

8.8 Ändern einer verschlüsselten Partitions ID

Standardmässig markiert Drivecrypt die verschlüsselten Partitionen mit der Partionen ID 0x74. Diese teilt DriveCrypt mit, dass die Partition verschlüsselt ist und erlaubt Ihnen, durch einfach eingabe des Passwortes jede verschlüsselte Partition automatisch anzumelden. DriveCrypt zeigt diese standardmässig verschlüsselten Laufwerke als "verschlüsselt" an.



Disk partitions		Size	Drive:	Volume Label	Start sector
NTFS		4000 Mb	C:		63
NTFS		20002 Mb	D:	work	8193150
Encrypted	<-	1027 Mb	S:	Awerty	49158963
Fat 32 Vol		1027 Mb	E:		51263478
Fat 32 Vol		1027 Mb	F:	Cd_03	53367993
Fat 32 Vol		1537 Mb	G:	Cd_04	55472508

© 2003 SecurStar

Sie können diese ID unter Windows NT/2000 und XP später ändern, wenn Sie diese Identifikation nicht haben wollen.

Hinweis: *Mit dem Wechsel der ID hindert DriveCrypt am automatischen Anmelden dieser Partition. Sie wird als "unbekannt" angezeigt.*

Melden Sie das verschlüsselte Laufwerk wie gewohnt an.
(Sehen Sie auch **Erstellung einer verschlüsselten Partitioni**)

Ist die verschlüsselte Partition angemeldet, klicken Sie bitte mit der rechten Taste auf die Partition, deren Einstellungen Sie verändern möchten.

Wenn Sie "***Partition ID ändern***" wählen, dann erscheint folgender Bildschirm:

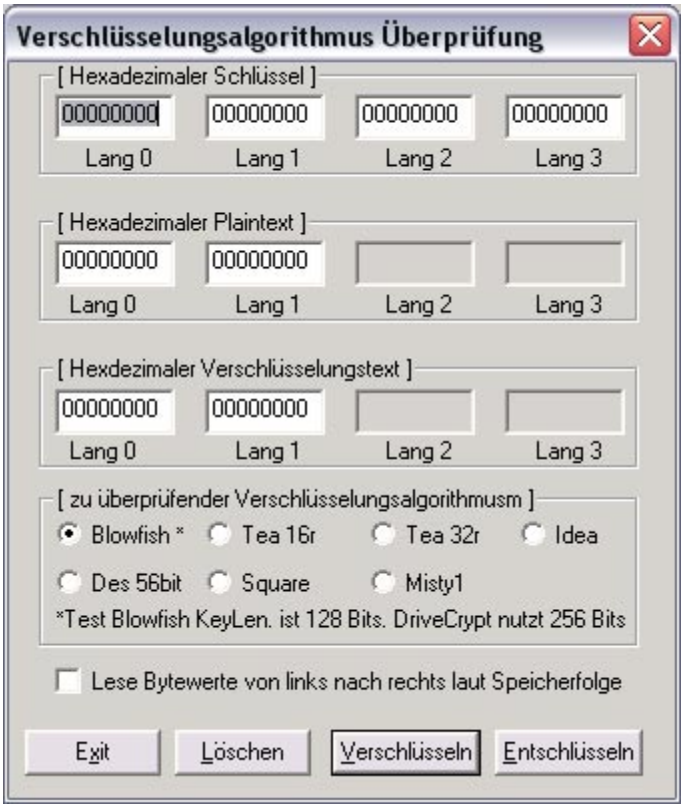
Hier können Sie die Partionen ID wählen, welche Sie verwenden wollen. Bestätigen Sie einfach mit "***ID Veändern".***

© 2003 SecurStar

8.9 Überprüfen der benutzten Algorithmen

Man braucht ein verlässliches Set bestehend aus einem Klartext, einem Schlüssel und einem Chiffretext für den Algorithmus, den man überprüfen möchte.

Im Hauptbildschirm:
Über das **General** Menü wählt man ***Verschlüsselung überprüfen***. Dies öffnet ein Überprüfungsdienstprogramm.



Im [Hexadezimaler Schlüssel] Teil:

Eingabe des 'als bestätigt anerkannten' Schlüssels.

Im [Hexadezimal Klartext] Teil:

Eingabe des 'als bestätigt anerkannten' Klartext.

Im [Chiffre Algorithmus zu prüfen] Teil:

Auswahl des Algorithmus, welcher getestet werden soll durch Anklicken des jeweiligen Knopfes.

© 2003 SecurStar

Drücken des **Verschlüsselung** Knopfes.

Überprüfung der Werte im [Hexadezimal Chiffretext] Teil gegen den 'als bestätigt anerkannten' Chiffretext.

Der Test kann auch in umgekehrter Weise durchgeführt werden. Hierzu gibt man den „als bestätigt anerkannten" Chiffretext ein und drückt den **Entschlüsseln** Knopf, um den Klartext zum Vergleich zu erhalten.

© 2003 SecurStar

9 Arbeiten mit Schlüsseldateien (Zweitschlüssel Benutzerzugriff)

9.1 Zweitschlüssel Benutzerzugriff - Erstellen einer Schlüsseldatei

Der Nutzen einer Schlüsseldatei liegt darin, anderen Benutzern den Zugriff auf verschlüsselte Laufwerke zu gewähren, ohne dass diese dabei das eigentliche Passwort von dem Laufwerk selbst kennen müssen.

Man meldet alle verschlüsselten Laufwerke an, die später Zugriff von einen weiteren Benutzer erhalten sollen. Wie man hierbei vorgeht, ist im Kapitel „Wie man... **Anmeldung von verschlüsselten Laufwerke**" zu finden.

Im Hauptbildschirm: Man klickt auf das **Datei**menü und wählt: ***DKF Zugriffsdatei erstellen***

Nun gibt man den ***Schlüsseldateinamen*** und den ***Ort*** an, unter der diese gespeichert werden sollen. Danach drückt man auf ***WEITER.***

Man kann auch weitere Einschränkungen dem Schlüsseldatei hinzufügen, wie ein Verfallsdatum (Schlüssel ist X Tage gültig) und/oder die Zeit, in welcher der Schlüssel eine Nutzung zulässt. (Beispiel: Schlüssel darf nur zu Büroöffnungszeiten genutzt werden, von 09:00 bis 18:00 Uhr).

Damit die Schlüsseldatei nach einer gewissen Anzahl von Tagen ablaufen kann, wählen Sie bitte das Kästchen ***Ablaufen nach*** und geben dort die Anzahl der Tage an, zu welcher der Schlüssel funktionieren darf.

Um die Nutzung der Schlüsseldatei auf gewissen Stunden des Tages zu begrenzen, klickt man folgendes Kästchen an "***Erlaube das Anmelden von Laufwerken zu bestimmten Zeiten."***.

Man gibt die Stunden und Minuten ein, wann die Schlüsseldatei anfangen darf zu funktionieren. ***Ebenso wird der Zeitrahmen angegeben*** (in Stunden und Minuten), in dem die Schlüsseldatei benutzbar sein darf.

Nun drückt man auf ***Weiter*** um fortzufahren.

Hinweis: Wenn der erlaubte Zeitrahmen vorüber ist, wird DriveCrypt automatisch die Laufwerke abmelden.

Nun ***gibt man*** das ***Schlüsseldatei-Passwort*** an und bestätigt mit

© 2003 SecurStar

Weiter,
um die Schlüsseldatei zu erstellen.

Hinweis : Das eingegebene Passwort ist das, welches der weitere Benutzer kennen/benutzen muss, um auf das Laufwerk zuzugreifen.

Nach dem Drücken auf ***Finish*** gelangt man zurück zum Hauptbildschirm von DriveCrypt.

Die Schlüsseldatei ist kopierbar, funktioniert aber nur auf dem System, auf dem diese erstellt und abgespeichert wurde, und arbeitet nur mit den Laufwerken zusammen, welche bei der Erstellung angemeldet waren.

Schlüsseldatei-Zugriff zu einem Laufwerk kann später wieder entfernt werden. Dies geschieht über das Laufwerk Einstellungsdialogfeld: ***Rechtsklick mit der Maus auf ein verschlüsseltes Laufwerk -> Einstellungen -> DKF entfernen.***

Zugriff auf die Schlüsseldatei bedeutet **nicht**, das der Benutzer Erlaubnis besitzt, den Laufwerks Einstellungsdialog zu sehen oder zu ändern. Die Laufwerke müssen hierzu mit den eigentlichen Passwörtern angemeldet werden, um diese abändern zu können.

9.2 Zweitschlüssel Benutzerzugriff - Anmeldung von verschlüsselten Laufwerken

Schlüsseldateien werden auf die gleich Weise angemeldet wie auch normale Laufwerke:

Um die Schlüsseldateien anzumelden, geht man im DriveCrypt Punkt für Punkt vor, wie man ein normales verschlüsseltes Laufwerk anmelden würde (Mehr Informationen im Kapitel **Anmeldung von verschlüsselten Laufwerken**).

Nun gibt man das Passwort ein, welches man während der Schlüsseldateierstellung definiert hat. Auch muss dieses in die selben Zeilen eingegeben werden, wie man Sie vorher definiert hat. Danach bestätigt man mit ***OK*** oder ***Enter.***

Hinweis: Schlüsseldateien, die mit einer früheren Version von DriveCrypt erstellt wurden, können mit der aktuellen Version nicht geöffnet werden. Diese müssen zuerst für ungültig erklärt werden (Siehe Kapitel: Wie man... Einstellungen für ein verschlüsseltes Laufwerk) und diese danach neu durch DriveCrypt erstellt werden.

© 2003 SecurStar

9.3 Zweitschlüssel Benutzerzugriff - Aufheben eines Schlüssels

Um einen Schlüssel aufheben zu können, klickt man im Hauptbildschirm mit der rechten Maustaste auf das Symbol des Laufwerkes, welches man aufheben möchte.
Im nächsten erscheinenden Dialogfeld wählt man ***Einstellungen.***

In dem neuen Einstellungendialogfeld bekommt man die aktuellen Laufwerksinformationen.

Nun drückt man auf den **DKF entfernen** Knopf und bestätigt mit ***JA.***

© 2003 SecurStar

10 Sperrung der lokalen Konsole

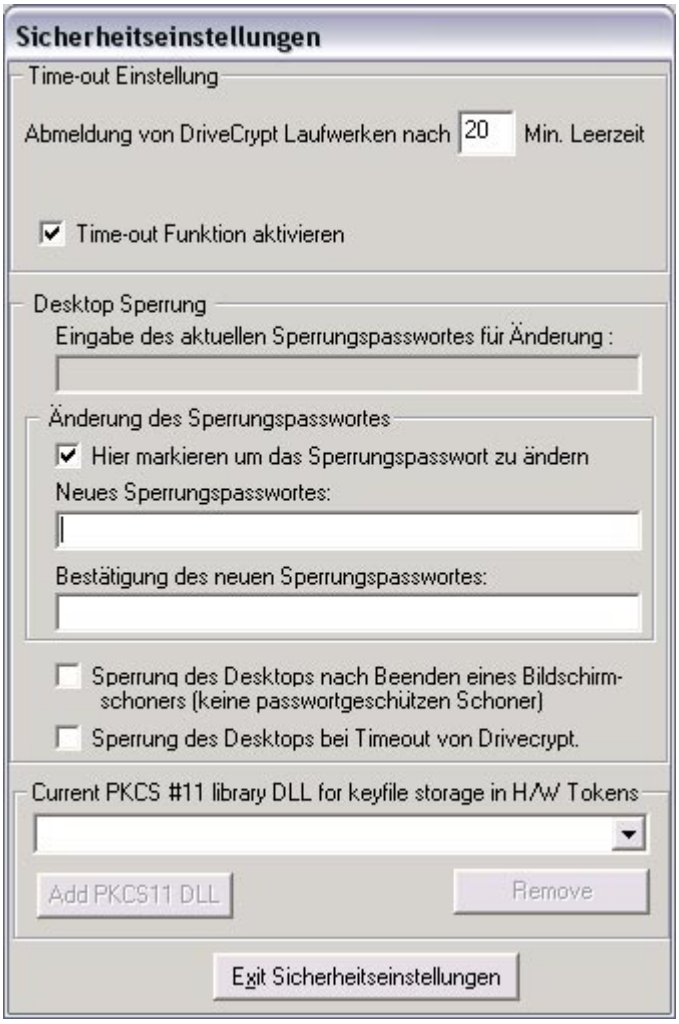
10.1 Sperrung der lokalen Konsole

Die Funktion „Sperrung der lokalen Konsole" erlaubt die Sperrung des Zugriffs auf den Computer, falls dieser für eine Weile verlassen wird. Die lokale Konsole verbirgt die Bildschirmanzeige und erlaubt nur Personen mit dem Computer weiter- zuarbeiten, wenn diese das richtige Passwort eingeben, um die Sperrung der lokalen Konsole aufzuheben.

10.2 Einstellung der Sperrung der lokalen Konsole

Um die Sperrungsfunktion zu aktivieren und ein Passwort zu setzen, muss man im DriveCrypt Hauptbildschirm auf ***Optionen*** gehen und ***dann auf den Knopf für Sicherheitseinstellungen drücken***.

© 2003 SecurStar



Man löscht den Eintrag aus dem Passwortfeld, indem man das gewünschte Passwort für die Sperrung eingibt. Bei der ersten Passwort-änderung, bitte alle Felder löschen; dies aktiviert die Änderungsfelder.

Um das Passwort ändern zu können, muss dieses Feld (Check here to change Passwort) markiert werden.

Hier gibt man das neue Passwort für den Sperrungsbildschirm ein. Mit erneuter Eingabe bestätigt man das Passwort.

Falls man einen MS Bildschirmschoner benutzt, bietet DriveCrypt die Möglichkeit, diesen nach der Abschaltung zu übernehmen und dem Benutzer des Computers nach dem Sperrungspasswort zu fragen. Um diese Funktion zu aktivieren, markiert man das dafür vorgesehene Feld.

Der Sperrungsbildschirm erkennt auch den Laufwerks-Timeout. Falls die Console gesperrt werden soll, wenn ein Laufwerk-Timeout erfolgt, markiert man dieses Feld.

© 2003 SecurStar

Nachdem dies abgeschlossen ist, klickt man auf ***Sicherheitseinstellungen beenden*** und bestätigt die Änderungen des Optionen Bildschirms, in dem auf den Knopf ***Änderungen übernehmen*** drückt.

10.3 Benutzung der Sperrung der lokalen Konsole

Es gibt verschiedene Wege die Sperrungsfunktion zu benutzen.

- Manueller Start (durch Hotkey oder Startknopf)
- Mit dem MS Windows Bildschirmschoner verbinden
- Mit dem Laufwerks-Timeout verknüpfen

Manueller Start (durch Hotkey oder Startknopf)

Im DriveCrypt Hauptbildschirm drückt man auf
General -> Sperrung der lokalen Konsole

-ODER-
In der Windows Taskleiste klickt man mit der ***rechten Maustaste auf das DriveCrypt Symbol*** und ***wählt die Sperrung der lokalen Konsole.***

-ODER-
Man drückt den vorher definierten Sperrungs-Hotkey.

Hinweis: Um einen Sperrungs-Hotkey zu setzen, wählt man vom DriveCrypt Hauptbildschirm folgendes aus: ***Optionen -> Hotkeys Einstellungen -> Sicherheits-Hotkeys.)***

Nun aktiviert man das Feld der Sicherheits-Hotkeys und ***gibt sodann die gewünschte Hotkey*** Kombination an.

© 2003 SecurStar

Man bestätigt die Änderungen, indem man auf **Hotkey Einstellungen verlassen** drückt und danach beim Optionendialog auf den Knopf **Änderungen übernehmen**.

-ODER-

Diese Funktion mit dem MS Windows Bildschirmschoner verbinden

Wenn ein MS Bildschirmschoner benutzt wird, kann DriveCrypt dessen Funktionen übernehmen. Dies bedeutet, sobald der MS Bildschirmschoner beendet wird (weil eine Benutzeraktivität erkannt wurde), startet DriveCrypt den Sperrungsbildschirm und zwingt den Benutzer dazu, dass Sperrungspasswort einzugeben, um wieder mit dem Computer arbeiten zu können.

Um die Funktion zu aktivieren ist im Kapitel **Einstellung der Sperrung der lokalen Konsole** beschrieben.

-ODER-

Diese Funktion mit dem Laufwerks-Timeout verbinden

Es kann eingestellt werden, dass der Sperrungsbildschirm in Kraft tritt, wann immer ein angemeldetes Laufwerk einen Timeout erfährt.

Wie diese Funktion aktiviert wird, findet man im Kapitel **Einstellung der Sperrung der lokalen Konsole** und **Benutzung der Timeout Funktion.**

© 2003 SecurStar

11 Kommandozeilenzugriff

11.1 Kommandozeilenzugriff

DriveCrypt unterstützt die Eingabe von Parametern mittels der Kommandozeile. Folgende Funktionen sind einstellbar:

Anmeldung einer Containerdatei:
```
DriveCrypt.exe  C:\crypted\mycontainer.dcv
```

Anmeldung aller von DriveCrypt formatierten Partitionen:
```
DriveCrypt.exe /MP
```

NORMALE Abmeldung ALLER Laufwerke
```
DriveCrypt.exe /DN
```

ABRUPTE Abmeldung ALLER Laufwerke
```
DriceCrypt.exe /DB
```

NORMALE Abmeldung einer Containerdatei durch Angabe des Namens:
```
DriveCrypt.exe /DNF C:\crypted\mycontainer.dcv
```

ABRUPTE Abmeldung eines Containers durch Angabe des Dateinamens:
```
DriveCrypt.exe /DBF C:\crypted\mycontainer.dcv
```

Abmeldung einer DriveCrypt Festplatte durch den logischen Laufwerksbuchstaben:

Normal: {Abmeldung auf normalem Wege}
```
DriveCrypt.exe /DNF X:
```

Abrupt:
```
DriveCrypt.exe /DBF X:
```

Diese zwei letzten Funktionen ermöglichen auch die Abmeldung individueller Partitionen, wenn deren logischer Laufwerksbuchstabe bekannt ist.

Hinweis: Die Parameter können dazu benutzt werden, eine Verknüpfung zum DriveCrypt Hauptprogramm anzulegen (DriveCrypt.EXE), aber es muss hierfür der Pfad zu dem Laufwerk in doppelten Anführungsstrichen angegeben werden, wenn der Name dessen Leerzeichen enthält.

© 2003 SecurStar

12 Hardwareunterstützung

12.1 Hardwareunterstützung

DriveCrypt unterstützt verschiedene Hardware- wie Fingerabdrucksensoren und SmartCard-Leser sowie USB Tokens. Diese Hardwaregeräte bieten doppelte Sicherheitsaspekte, die zum einen die Interaktion des Anwenders (Fingerabdruck) oder eines Gerätes benötigten (Smart Card oder Token) sowie die DriveCrypt-Passphrase Authentifikation, bevor Daten entschlüsselt werden können.

Um DriveCrypt zusammen mit den Hardwaregeräten zu benutzen, müssen die dafür notwendigen Hardwaretreiber installiert werden. Diese Treiber sind im Downloadbereich auf der Webseite von DriveCrypt erhältlich. http://www.securstar.com

12.2 USB Token Support

DriveCrypt ist kompatibel mit den USB Token von Aladdin, Rainbow, Eutron und andere PKCS#11 unterstützenden Token. USB Token können an jeder mit Universal Serial Bus (USB) ausgestatte-ten Arbeitsstation benutzt werden. Sie garantieren die Zuverlässigkeit, Einfachheit und Sicherheit von Smart Cards und Verschlüsselungs-Token, ohne dass ein extra Lesegerät angeschafft werden muss.

Abhängig vom eingesetzten Token, lesen Sie bitte das entsprechende Kapitel.

Aladdin R2 and PRO token

Eutron WebIdentiy token
Eutron CryptoIdentiy token

Rainbow 1000/1032 token

© 2003 SecurStar

Rainbow 2000/3000 token

Andere PKCS #11 compliant token

12.3 Benutzung eines Rainbow iKey 1000/1032 oder Eutron Weidentity Token

IUm den Token benutzen zu können, vergewissern Sie sicher, dass dieser richtig in den USB Port eingesteckt wurde und die Kontrolllampe des Tokens leuchtet. Vergewissern Sie sich bitte auch dass die Tokentreiber ordnungsgemäß installiert wurden.

Hinweis: Bei der Programmierung des Tokens, muss dieser der EINZIGE am Computer angeschlossener Token sein, bzw. er muss als erster Token vom Betriebssystem gefunden werden. Falls Zweifel bestehen, bitte entfernen Sie die anderen Token.

Melden Sie alle Laufwerke an, welche später durch den Token genutzt werden sollen. (mehr Informationen finden Sie im Kapitel "Anmeldung von verschlüsselten Laufwerken")

Hinweis: Der Rainbow I-Key 1000 hat eine Speicherkapazität von 8 KB, und erlaubt dadurch nur die Speicherung von Schlüsseldateien die maximal bis zu 3 Laufwerke verwalten.

Auf dem DriveCrypt Hauptbildschirm auf
Dateien->Erstellung der DKF Zugriff-Dateien klicken.

Danach das Kästchen "***DKF Datei in Rainbow I-Key speichern***" bzw. "**Eutron WebIdentity Token**" markieren und auf ***Weiter*** drücken.

Man kann auch weitere Einschränkungen der Schlüsseldatei hinzufügen, wie z.B. ein Verfallsdatum (Schlüssel ist X Tage gültig) und/oder die Zeit, in der der Schlüssel eine Nutzung zulässt. (Beispiel: Schlüssel darf nur zu Büroöffnungszeiten genutzt werden, von 09:00 bis 18:00 Uhr).

Damit die Schlüsseldatei nach einer gewissen Anzahl von Tagen ablaufen kann, wählen Sie bitte das Kästchen ***Ablaufen nach*** und geben dort die Anzahl der Tage an, welche gewünscht ist, zu welcher der Schlüssel funktionieren soll.

Um die Nutzung der Schlüsseldatei auf gewissen Stunden des Tages zu begrenzen, klicken Sie folgendes Kästchen an. ***Erlaube das***

© 2003 SecurStar

Anmelden von Laufwerken zu bestimmten Zeiten..

Man gibt die Stunden und Minuten ein, zu der die Schlüsseldatei anfangen darf zu funktionieren.
Ebenso wird der Zeitrahmen angegeben (in Stunden und Minuten), in dem die Schlüsseldatei benutzbar sein darf.

Drücken Sie auf ***Weiter*** um fortzufahren.

Geben Sie nun *das* ***Token Passwort*** ein und ***bestätigen Sie die Eingabe.***
Drücken Sie auf ***Weiter*** um fortzufahren…..

Die Schlüsseldatei wird nun auf den USB Token abgelegt.
Wenn dies abgeschlossen ist, drücken Sie bitte auf ***Beenden*** um zum Hauptbildschirm von DriveCrypt zurückzukehren.

12.4 So werden PKCS #11 kompatible Token programmiert

Vergewissern Sie sich, dass Ihre PKCS#11 kompatible Hardware in DriveCrypt konfiguriert wurde.

Bitte ***Optionen->Sicherheits Setup*** anklicken.

Im neuen Dialogfenster können Sie zwischen den voreingestellten USB-Token auswählen (Aladdin, Eutron oder Rainbow) und mit ***Beenden*** bestätigen.

Falls Sie andere, nicht in der Liste aufgeführte Hardwaregeräte benutzen wollen, können Sie Ihre PKCS#11 kompatiblen Geräte in DriveCrypt registrieren:

In der PKCS#11 Hardwaregeräte-Box, positionieren Sie sich auf einer leeren Zeile und drücken Sie auf: **PKCS#11 DLL hinzufügen**

Jetzt müssen Sie DriveCrypt unterrichten, wo der für Ihre Hardware geeignete PKCS#11 Treiber gespeichert ist. Bitte surfen Sie zum relevanten PKCS#11 Treiber und **bestätigen** Sie.

Der Treiber wird in DriveCrypt geladen und erscheint in der Hardware Liste.

Bestätigen Sie bitte alle Änderungen mit ***BEENDEN.***

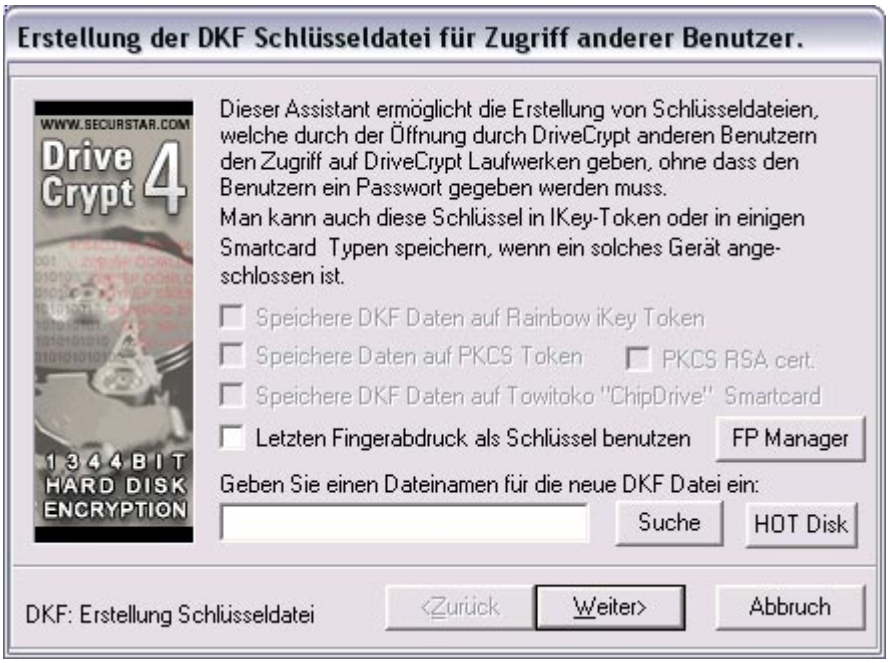
© 2003 SecurStar

Auch im OPTIONEN Dialog, bitte bestätigen mit ***Alles Bestätigen***

Ihre PKCS#11 Hardware kann jetzt programmiert werden:
Um das Gerät zu programmieren, melden Sie bitte alle Laufwerke an, welche später durch den Token genutzt werden sollen. (mehr Informationen finden Sie im Kapitel "Anmeldung von verschlüsselten Laufwerken")

Auf dem DriveCrypt Hauptbildschirm auf
Dateien->Erstellung der DKF Zugriff-Dateien klicken.

Danach das Kästchen "***Daten auf PKCS# 11 Token speichern***" markieren
und auf ***Weiter*** drücken.



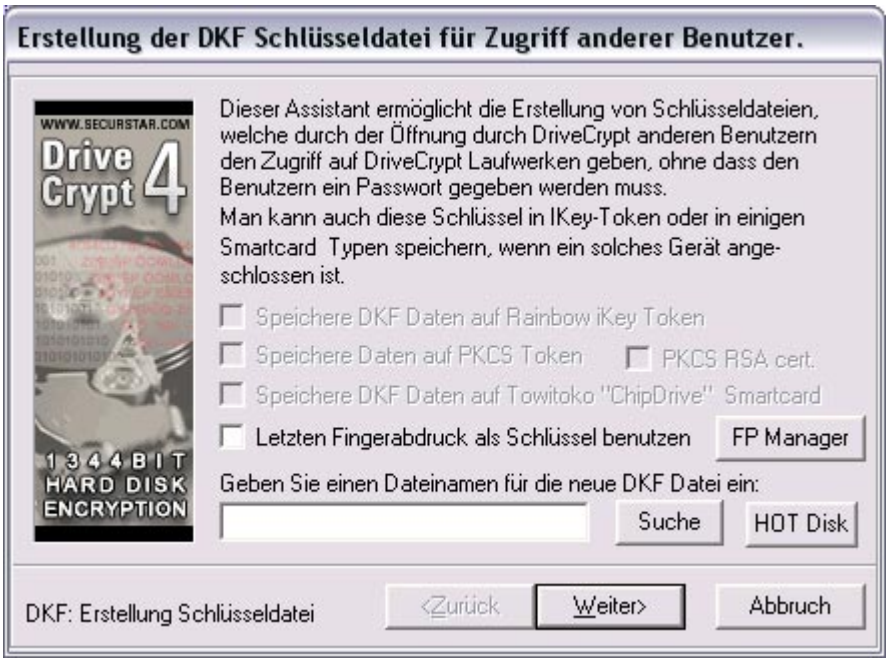
Hinweis: Diese Checkbox ist nur aktiv wenn ein PKCS#11 kompatibler Token im Rechner eingesteckt und ordnungsgemäß installiert wurde.
An dieser Stelle können Sie wählen, ob die Schlüsseldatei durch ein vom User vorgegebenes Passwort, oder, falls im Token bereits ein X-509 Zertifikat existiert, die Schlüsseldatei mittels PKI verschlüsselt wird.

Hinweis: Falls Sie nicht mit Zertifikaten arbeiten, können Sie die Handbuchabschnitte welche sich mit Zertifikaten befassen ignorieren. Der Token wird dann, wie im Kapitel 11.1.c beschrieben, benutzt.

© 2003 SecurStar

Wenn Sie mit Zertifikaten arbeiten, vergewissern Sie sich vorerst, dass sich auf dem Token ein gültiges X-509 Zertifikat befindet. Dies bedeutet, dass auf dem Token ein Zertifikat sowie ein öffentlicher und privater Schlüssel gespeichert sein muss.
Wenn von DriveCrypt kein gültiges Zertifikat im Token gefunden wird, bleibt die PKI Checkbox grau.

Falls ein gültiges Zertifikat auf dem Token vorhanden ist, Klicken Sie bitte das Kästchen für die PKI Verschlüsselung an.



Section 2
Nachdem Sie auf ***WEITER*** gedrückt haben, können weitere Einschränkungen für die Schlüsseldatei eingestellt werden. Es kann definiert werden, dass eine Schlüsseldatei nach einer gewissen Anzahl von X-Tagen ablauft....

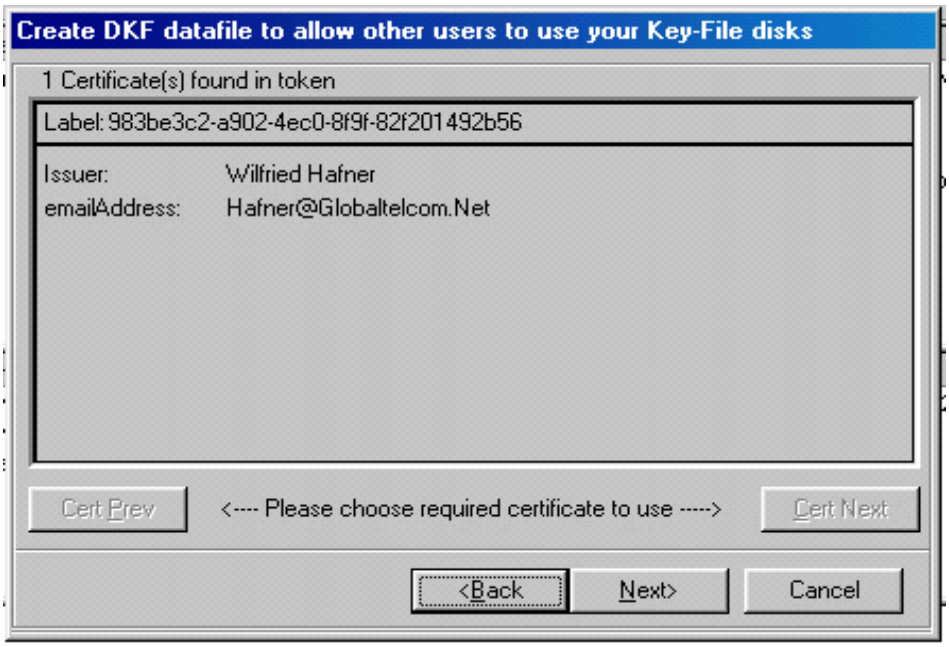
Um die Zeitbeschränkung einer Schlüsseldatei zu definieren, markieren Sie bitte die „**Verfällt nach**" Checkbox und geben Sie die Anzahl der Tage ein, nachdem die Schlüsseldatei verfallen soll.

Um die Zeitbeschränkung einer Schlüsseldatei zu definieren, markieren Sie bitte die entsprechende Checkbox und geben Sie die Uhrzeiten ein (stunden und Minuten) währen deren die Schlüsseldatei funktionieren soll.

Hinweis: Wenn das Zeitfenster überschritten wird, versucht DriveCrypt die angemeldeten Laufwerke abzumelden.

© 2003 SecurStar

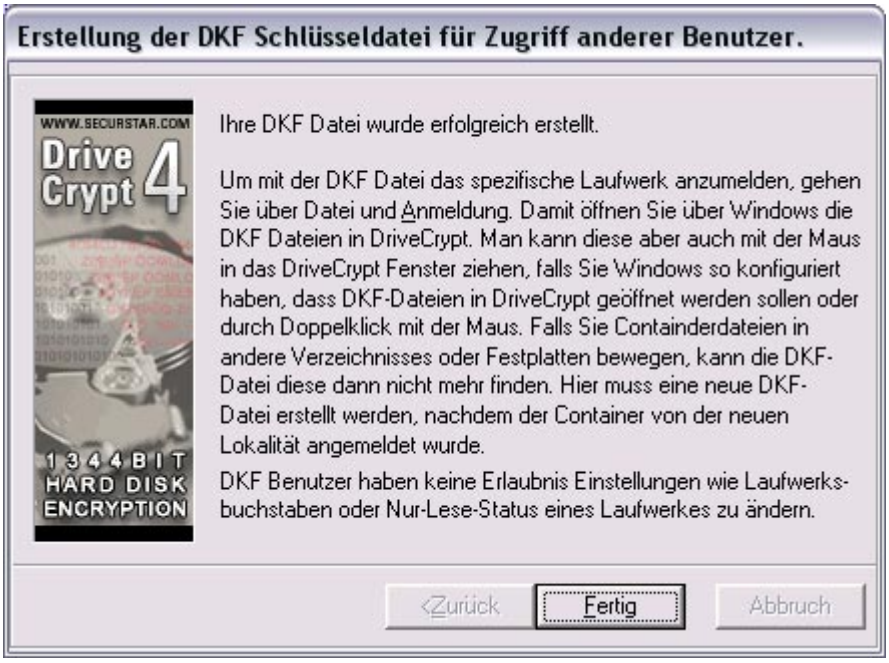
Drücken Sie auf ***Weiter*** um fortzufahren.
An dieser Stelle wird DriveCrypt die Zertifikate vom Token auslesen und jedes gültige Zertifikat im folgendem Fenster anzeigen. Drücken Sie bitte auf „Vorh. Zert" oder „Nächst. Zert" um zwischen den vorhanden Zertifikaten umzuschalten.



Nachdem Sie das gewünschte Zertifikat ausgesucht haben, drücken Sie bitte auf ***WEITER***. Der Token wird dann mit der konfigurierten Schlüsseldatei beschrieben.

Hinweis: Bei der Benutzung von Aladdin Token, wird von den Aladdin Treibern zusätzlich noch die Token PIN abgefragt bevor die Daten auf dem Token gespeichert werden können.

© 2003 SecurStar



Nachdem alle Daten auf dem Token gespeichert wurden, erhalten Sie ein Bestätigungsfenster. Bitte den Token solange im USB-Port eingesteckt lassen, bis Sie von DriveCrypt diese Bestätigung bekommen.

12.5 So werden Laufwerke mit einem USB-Token angemeldet/abgemeldet

Um ein Laufwerk mit Hilfe eines USB-Token anzumelden, steckt man den Token einfach in den USB-Port des Computers. Dies öffnet automatisch ein Token Passwortdialog auf dem Bildschirm. Geben Sie das Schlüsseldateipasswort ein und bestätigen Sie die Eingabe mit „Enter".

Die Schlüsseldatei wird jetzt aktiviert.

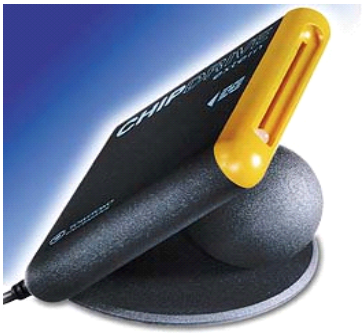
Hinweis: Während der normalen Nutzung wird der ERSTE Schlüssel, der in den USB Port eingesteckt wird, als der Schlüssel gewertet, mit dem DriveCrypt versuchen wird, verschlüsselte Laufwerke zu öffnen.

© 2003 SecurStar

Um das Laufwerk abzumelden, nimmt man einfach den USB-Token aus dem USB Port.

Hinweis : Wenn der Token aus dem USB-Port entfernt wird, findet ein normaler Abmeldungsprozess statt. Falls die Abmeldung fehl schlägt, liegt das daran, das einige Applikationen gerade auf das angemeldete Laufwerk zugreifen und der Benutzer 15 Sekunden Zeit hat, diese Applikation zu schließen.
Nach 15 Sekunden findet eine Zwangsbeendung statt.

12.6 SMART CARD Unterstützung (Towitoko Lesegeräte)



Towitoko ChipDrive-Lesegeräte bieten neben Zuverlässigkeit, Einfachheit und Sicherheit von SmartCards ebenso eine kostengünstige Alternative. Zusätzlich unterstützen Towitoko Lesegeräte mehr als 40 unterschiedliche ChipKarten.

Wie man eine SmartCard programmiert:

Um eine SmartCard nutzen zu können, stellen Sie sicher, dass der SmartCard-Leser richtig an den Computer angeschlossen ist und die SmartCard richtig in den Kartenleser eingesteckt wurde.

Zuerst meldet man alle Laufwerke an, welche man später durch die Chipkarte ansprechen möchte. (mehr Informationen finden Sie im Kapitel "Anmeldung von verschlüsselten Laufwerken")

Danach auf dem DriveCrypt Hauptbildschirm auf **Datei->Erstellung der DKF Zugriffsdatei** klicken.

Markieren Sie das Kästchen " ***DKF Datei auf SmartCard speichern***" und klicken danach auf ***Weiter***

Hinweis: DriveCrypt unterstützt Schlüsseldateien, die es ermöglichen, bis zu 8 Laufwerke gleichzeitig zu betreiben. Trotzdem benötigt **die Schlüsseldatei hierfür 2KB pro angemeldetes Laufwerk**. Dies bedeutet, falls man ein Laufwerk anmelden möchte, wird eine SmartCard mit 2 KB Speicher benötigt. Falls man 4 Laufwerke gleichzeitig per SmartCard nutzen möchte, wird hierfür eine Karte mit mindestens 8 KB Speicherplatz benötigt. Somit werden für die Anmeldung aller 8 Laufwerke eine SmartCard mit mindestens 16 KB Speicher benötigt.

Man kann auch Restriktionen sowie ein Ablaufdatum in der Schlüsseldatei definieren (Karte ist nur für X Tage gültig), und/oder eine Zeit, zu der die Möglichkeit besteht, diesen zu nutzen. (Beispiel: Der Schlüssel darf nur während der Büroöffnungszeiten benutzt werden, von 09.00 bis 18.00 Uhr).

Damit die Schlüsseldatei nach einigen Tagen ablaufen kann, muss das Kästchen ***Ablaufen nach*** aktiviert werden, damit die Eingabe der Anzahl der

© 2003 SecurStar

Tage auch durch die Software beachtet wird.

Um die Nutzung der Schlüsseldatei auf bestimmte Stunden des Tages einzuschränken, klicken Sie auf die Box: ***Anmeldung eines Laufwerks zu bestimmten Zeiten***.

Geben Sie die Stunden und Minuten an, zu der Zeit die Schlüsseldatei anfangen darf zu arbeiten. Daraufhin ***geben Sie den Zeitrahmen an***, (in Stunden und Minuten), in der die Schlüsseldatei funktionieren darf.

Drücken Sie auf ***Weiter*** um fortzufahren…..

Jetzt ***geben Sie bitte das SmartCard-Passwort*** ein und ***bestätigen Sie dies mit OK***.

Danach auf ***Weiter*** drücken um fortzufahren…..

Die Schlüsseldatei wird nun auf die SmartCard geschrieben.
Wenn dies abgeschlossen ist, drückt man ***Beenden*** um zum Hauptbildschirm zurückzukehren.
Wie man Laufwerke mit SmartCards anmeldet/abmeldet:
Um ein Laufwerk mit Hilfe einer SmartCards anzumelden, steckt man einfach die Karte in den am Computer angeschlossenen Kartenleser. Dies öffnet automatisch ein SmartCard-Passwortdialogfenster auf dem Bildschirm. Geben Sie hier das SmartCard Passwort ein und bestätigen mit „Enter".

Die Schlüsseldatei wird nun angemeldet.

Abmelden eines durch SmartCard angemeldeten Laufwerkes
Um ein Laufwerk abzumelden, nimmt man einfach die SmartCard aus dem Kartenleser.

Hinweis : *Wenn die SmartCard aus dem Kartenleser genommen wird, findet ein normaler Abmeldungsprozess statt. Falls die Abmeldung fehl schlägt, liegt das daran, das einige Applikationen gerade auf das angemeldete Laufwerk zugreifen und der Benutzer 15 Sekunden Zeit hat, um diese Applikation zu schließen. Nach 15 Sekunden findet eine Zwangsbeendung statt.*

12.7 Fingerprint Reader Support (SecuGen Reader)

DriveCrypt unterstützt den Fingerabdruck Leser von SecuGen.

© 2003 SecurStar



SecuGen bietet günstige jedoch präzise und zeitbeständige Fingerabdruck-Leser mit denen Sie Ihren Fingerabdruck als digitales Passwort benutzen können, ohne befürchten zu müssen, dass Ihre Passwörter verloren oder vergessen werden.

Wie man den Fingerabdruck Reader benutzt:

Um den Fingerabdruck Leser von SecuGen benutzen zu können, müssen Sie sicherstellen, dass das Gerät ordnungsgemäß angeschlossen ist, und dass die dazugehörigen Treiber korrekt installiert wurden.

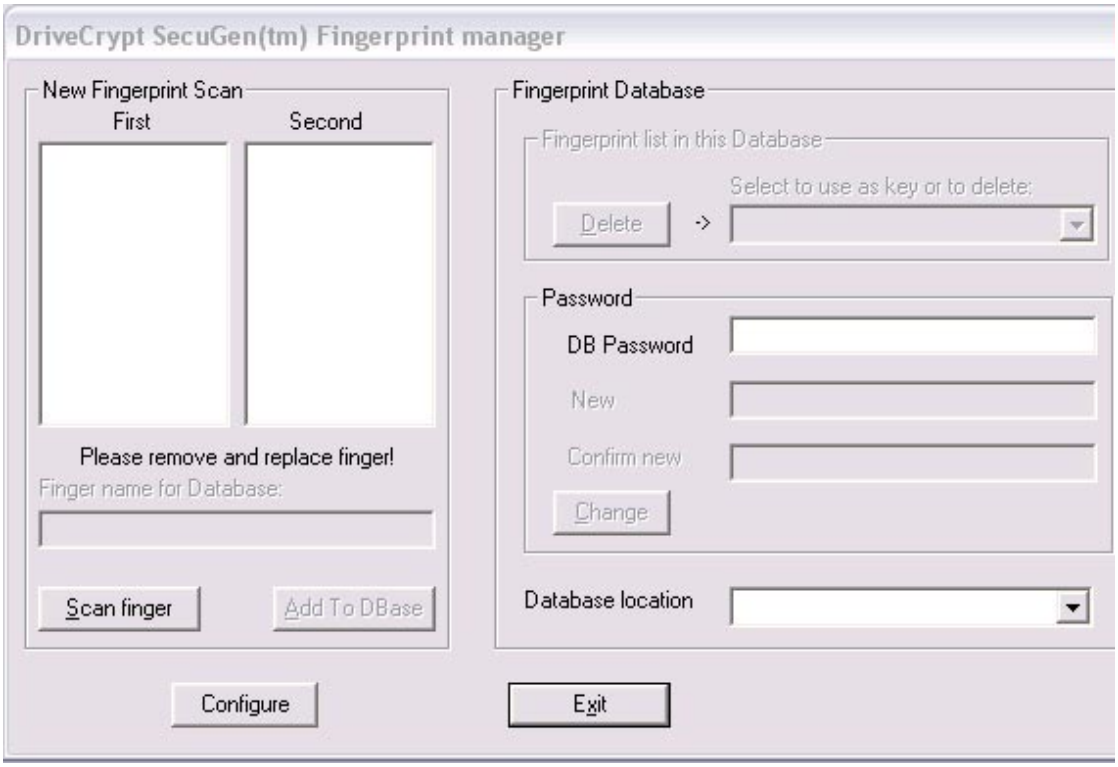
Achtung: Bitte starten Sie DriveCrypt NACHDEM der Fingerabdruck Leser angeschlossen und installiert wurde, andernfalls kann DriveCrypt die Hardware nicht erkennen. Sollten Sie DriveCrypt beenden wollen, um die Hardware anzuschließen, wählen Sie bitte im DriveCrypt Hauptbildschirm:
Datei->DriveCrypt Beenden

Registrieren Sie Ihre Finger :

Nachdem der Fingerabdruck Leser installiert ist und DriveCrypt läuft, haben Sie die Möglichkeit Ihre Fingerabdrücke in der Fingerabdruckdatenbank zu hinterlegen.

Bitte starten Sie die Fingerabdruckdatenbank wie folgt:
Datei -> Fingerabdruck Manager das wird folgendes Dialogfenster öffnen:

© 2003 SecurStar



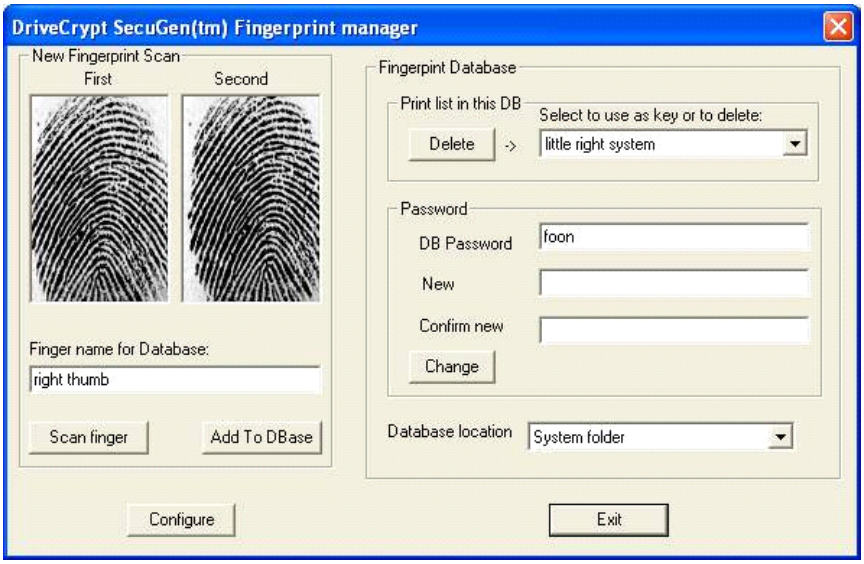
Um Ihren Fingerabdruck zu registrieren, Drücken Sie bitte auf: ***Finger Scannen***

An dieser Stelle wird die Linse des Fingerabdruck Scanners aufleuchten und das Gerät ist für den Scanvorgang bereit. Bitte legen Sie Ihren Finger auf die Linse des Lesegerätes und beobachten Sie wie Ihr Fingerabdruck auf dem Bildschirm, im Fenster „Erster" erscheint.

Bitte entfernen Sie nun Ihren Finger von dem Fingerabdruck Leser und platzieren Sie ihn einige Sekunden später erneut auf das Gerät. Das bewirkt dass Ihr Finger erneut eingescannt wird und der Abdruck auf dem Bildschirm, im Fenster „zweiter" erscheint.

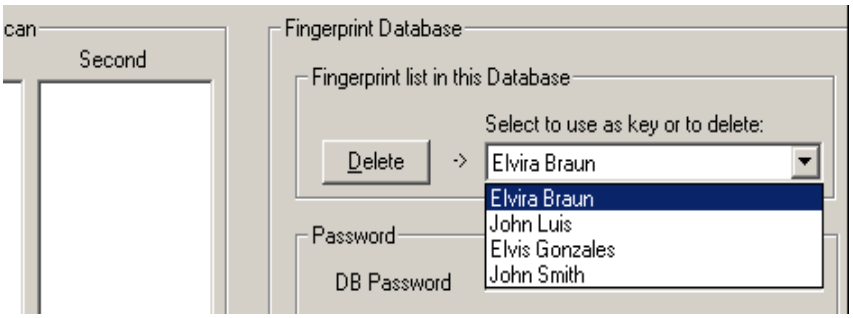
Nachdem Ihr Finger zweimal eingescannt wurde und DriveCrypt festgestellt hat, dass die beiden Fingerabdrücke in einer ausreichend guter Qualität vorliegen und auch untereinander übereinstimmen, haben Sie nun die Möglichkeit, den Fingerabdruck zu benennen, und ihn dann in der Datenbank zu hinterlegen.
Bitte drücken Sie hierfür auf dem Knopf : ***„Add to Dbase"***

© 2003 SecurStar



Löschen eines Fingerabdruckes aus er Datenbank:

Um einen Fingerabdruck aus der Datenbank zu löschen, markieren Sie bitte den zu löschenden Fingerabdruck und drücken sie dann den Knopf: **"*Löschen*".**



Schützen einer Fingerabdruck Datenbank:

DriveCrypt ermöglicht es Ihnen, die Fingerabdruck Datenbank zu schützen. Dies verhindert, dass unbefugte fremde Fingerabdrücke löschen, oder mit Ihnen neue Container verschlüsseln.

Standardmäßig wird die Datenbank von DriveCrypt NICHT geschützt, Sie können jedoch ein Passwort definieren, indem Sie es in der Textzeile: ***Neu*** eingeben, und es in der Textzeile: ***Bestätigen*** wiederholen. Anschließend drücken Sie bitte auf dem Knopf: ***Ändern***

Wenn die Datenbank passwortgeschützt ist, müssen Sie zur Erstellung

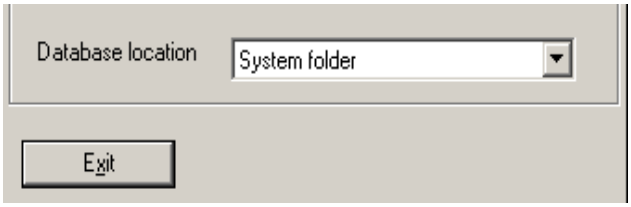
© 2003 SecurStar

neuer mit Fingerabdruck geschützter DKF Schlüsseldateien, vorher immer das Datenbank Entschlüsselungspasswort eingeben. Geben Sie hierzu, im Fingerabdruckmanager, in der Textzeile ***DB Passwort*** das Entschlüsselungspasswort ein.

Datenbank Speichern

Wichtig : Es ist ratsam, die Fingerabdruckdatenbank an einem sicheren Ort zu speichern. Standardmäßig speichert DriveCrypt die Datenbank im Verzeichnis Windows\system, Sie sollten jedoch mit DriveCrypt einen Verschlüsselten Container erstellen und die DriveCrypt Möglichkeit benutzen, die Fingerabdruckdatenbank auf dem verschlüsselten Container zu speichern. Dies verhindert dass unbefugte Zugriff auf die Datenbank bekommen.

SecurStar übernimmt KEINERLEI Verantwortung für eventuelle Sicherheits-gefahren die aus der unsachgemäßen Lagerung der Fingerabdruckdatenbank herrühren könnten. Es ist die Aufgabe der Benutzer sicherzustellen, dass die Fingerabdruckdatenbank so gut wie möglich geschützt ist (Idealerweise in einer DriveCrypt Containerdatei).



T Bitte wählen Sie in diesem Fenster wo die Fingerabdruck Datenbank gespeichert werden soll. Beachten Sie bitte, dass verschlüsselte Alternativverzeichnisse nur dann zur Verfügung stehen, wenn die jeweiligen Containerdateien angemeldet wurden.

Achtung: Wenn Sie die Fingerabdruckdatenbank in einer verschlüsselten Containerdatei speichern, müssen Sie immer darauf achten, dass diese Containerdatei angemeldet wurde, bevor DriveCrypt auf die Datenbank zugreifen soll.

Bitte beachten Sie ebenso, dass jede Fingerabdruckdatenbank 100 Fingerabdrücke speichern kann. Wenn Sie allerdings mehrere Containerdateien gleichzeitig angemeldet haben, und jede davon enthält eine Datenbank, so multipliziert sich die Anzahl der zur Verfügung stehender Fingerabdrücke (100) mit der Anzahl der angemeldeten Containerdateien. Es können Ihnen somit, Gleichzeitig bis zu 800 Fingerabdrücke zur Verfügung stehen.

© 2003 SecurStar

Fingerabdruck mit einem verschlüsselten Container verknüpfen.

Um ein Fingerabdruck mit einem verschlüsselten Container zu verknüpfen, melden Sie erst den verschlüsselten Container, wie gewohnt, mittels ihres Passwortes an.
An dieser stelle erstellen Sie dann eine DKF Schlüsseldatei:
File ->Create DKF Access File

Im neuen Dialogfenster drücken sie bitte auf dem Knopf: ***FP Manager***
Und wählen Sie aus der Fingerabdrucktabelle den Namen des Fingerabdruckes aus, den Sie für die Verschlüsselung benutzen möchten. Nachdem der gewünschte Fingerabdruck markiert wurde, bestätigen Sie bitte die Eingabe mit ***EXIT***.

ACHTUNG: Wenn die Datenbank passwortgeschützt ist, müssen Sie erst das Entschlüsselungspasswort in der Textzeile: ***DB Password*** eingeben, um den Zugang auf die Liste der registrierten Fingerabdrücke zu bekommen.

Nachdem Sie wieder zum DKF Dialogfenster gelangt sind, drücken Sie bitte auf ***Weiter*** und beenden Sie die Erstellung der DKF Schlüsseldatei wie gewohnt. (Mehrere Informationen zur Erstellung von DKF Schlüsseldateien finden Sie im Kapitel 6 dieses Handbuches)

Anmeldung einer mit Fingerabdruck gesicherten DKF Schlüsseldatei:

Um eine mit Fingerabdruck gesicherten Schlüsseldatei anzumelden, laden Sie diese, wie jede andere von DriveCrypt erstellte Containerdatei durch Doppelklick oder durch „Drag & Drop" im DriveCrypt Hauptprogramm. An dieser stelle wird sofort ein Fingerabdruck Eingabefenster auf dem Bildschirm angezeigt.... Legen Sie jetzt Ihren Finger auf dem Fingerabdruck Lesegerät, das wird die Schlüsseldatei öffnen.

Entsperrung der Lokalen Konsole mittels Fingerabdruck

DriveCrypt ermöglicht allen Benutzer mit registrierten Fingerabdrücken, das einfache entsperren der lokalen Konsole mittels Fingerabdruck.
Um den Fingerabdruck Leser aus dem Passwortgeschützten DriveCrypt Bildschirmschoner zu aktivieren, drücken Sie bitte auf die Taste ***ENTER*** oder klicken sie mit Ihrer Maus auf dem Knopf: ***FingerPrint***

© 2003 SecurStar

ACHTUNG:
Ist eine DKF Schlüsseldatei angemeldet, so ist aus Sicherheitsgründen nur der Besitzer des Fingers, welcher die Schlüsseldatei angemeldet hat berechtigt, die Lokale Konsole zu entsperren. Es ist allerdings immer möglich, die Lokale Konsole durch das vorher definierte Passwort zu entsperren.

© 2003 SecurStar

13 FAQ (Haufig gestellte Fragen)

Das sind die meistgestellten Fragen zu DriveCrypt.
Diese Liste wird immer dann aktualliesiert, wenn neue Fragen der User beantwortet wurden.

Generelle Fragen:

© 2003 SecurStar

© 2003 SecurStar

13.1 Ist DriveCrypt Windows XP kompatibel ?

Ja, ab Version 3.02b ist DriveCrypt Windows XP kompatibel.

13.2 Kann man verhindern, dass Angestellte einer Firma Daten verschlüsseln, ohne dem zuständigen Systemadministrator oder Management zuvor Zugriff auf die Daten zu geben.

Ja, während der Installation von DriveCrypt auf Windows NT 4/ 2000 Computern gibt es die Möglichkeit, dass alle neuen Container nur vom Systemadministrator angelegt werden können.
Um sicherzugehen, dass Container von anderen Computern nicht installiert werden, sollten die Benutzer dazu gehalten werden, ihre verschlüsselten Container nur mit Schlüsseldateien öffnen zu können, damit die Kontrolle über die Dateien gewährleistet bleibt.

13.3 Wie löscht man eine unerwünschte '.DRC' Container Datei?

Gehen Sie im Menü auf Optionen und klicken Sie auf [x] Deaktivieren des DRC DATEILÖSCH-Schutzes. Nun löschen Sie die Containerdatei und leeren Ihren Papierkorb, falls Sie diesen benutzen.

Man kann auch die Dateiendung von '.DRC' auf '.DEL' ändern und dann diese löschen.

13.4 Wie kann man unterschiedliche DriveCrypt Container abmelden?

Klicken Sie mit dem rechten Mausknopf auf ein Symbol eines im DriveCrypt angemeldeten Laufwerks und wählen Sie "Abmeldung" aus dem Context-Menü. Beachten Sie, dass in dieses Menü noch weitere nützliche Informationen vorhanden sind.

© 2003 SecurStar

13.5 Wird FAT32 von Windows 95, 98, 98 SE und Windows 2000 unterstützt?

Ja. DriveCrypt Container mit einer Größe von 500 MB oder mehr unterstützen FAT32.

ACHTUNG:
Benutzen Sie kein FAT32 auf Windows NT 4 oder der ersten Version von Windows 95, da diese Betriebssysteme kein FAT 32 unterstützen.

13.6 Wird NTFS bei Windows NT4 / Windows 2000 und Windows Xp unterstützt?

Ja.

13.7 Können DriveCrypt Containers mit weniger als 1 Mbyte Größe erstellt werden?

Ja. Man kann ab jetzt Containergrößen in Kbytes ab 250KB aufwärts angeben.

13.8 Kann man DriveCrypt Container mit "Defrag" oder "Scandisk" bearbeiten?

Auf Windows 95/98 Betriebssystemen ja. Hier funktioniert es in gewohnter Weise. Es gibt sogar im Context-Menü Funktionen, die Ihnen dabei helfen. Sie könenn aber keine Container defragmentieren, auf denen sich gerade geöffnete Containerdateien befinden. Melden Sie die verschlüsselten Container ab, bevor Sie diese Laufwerke defragmentieren. Bei Windows 2000 muss zuerst die kommerzielle Version von Diskkeeper (Executive Software www.execsorf.co.uk) installiert werden, damit DriveCrypt Laufwerke defragmentiert werden können. Das Standard Defragmentierungsprogramm erkennt keine neu angemeldeten Laufwerke an. Um kaputte DriveCrypt Containers zu reparieren, starten Sie ChkDsk von einer Commandshell aus, z.B.: 'ChkDsk Y:' /F

© 2003 SecurStar

13.9 Kann man DriveCrypt Container ohne den Wizard erstellen ?

Nein, in dieser Version muss der Wizard benutzt werden, um neue DriveCrypt Container zu erstellen.

13.10 Wieso muss bei der DriveCrypt Containererstellung so viel die Maus bewegt werden?

DriveCrypt benötigt Zufallszahlen, und dies ist die beste Methode diese zu erhalten.

13.11 Wie hoch ist die maximale Größe eines DriveCrypt Containers, der erstellt werden kann?

Dateien auf Windows 95/98 können nicht größer als 4 Gigabytes betragen,
somit ist hier die Größe für DriveCrypt Container begrenzt.

Partitionen können bis zu 2047 Gigabytes groß sein.

Bei Windows NT4, 2000 und XP kann die Größe einer Containerdatei genauso groß sein wie die Partitionen (2047 Gigabytes).

In zukündtigen Versionen von DriveCrypt wird es möglich sein, mehrere Container Dateien zu verbinden.

13.12 Wieso muss ich meine alten mit "Summer" formatierten Laufwerke wieder aktivieren.

Der Summer Treiber benötigt direkt den Passworttext. Es ist besser, dass die Software keinen Passworttext sendet, außer man benötigt die Kompatibilität von Summer für alte DriveCrypt Container. Summer wird nicht für neue Container empfohlen. Beachten Sie, dass mit aktiviertem Summer der Passworttext in dem für den Treiber reserviertem Speicher abgelegt wird. 'Summer' wird nicht unter Windows NT4 und Windows 2000 unterstützt.

© 2003 SecurStar

13.13 Funktioniert DriveCrypt auf Windows NT 4 oder Windows 2000?

Ja.

13.14 Wie kann man Container anmelden, nachdem man diese erstellt hat ?

Es gibt drei Wege dies zu tun:

1) Benutzen Sie unter dem Menü "Datei" die Funktion "Container anmelden"
2) Ziehen Sie die Containerdatei in das DriveCrypt Fenster
3) Erstellen Sie eine Dateiendung (DRC) für DriveCrypt (damit kann man durch Doppelklick den Container über DriveCrypt öffnen lassen.)

13.15 Wieso funktioniert meine .WAV Audiodatei nicht mit der DriveCrypt Steganographie-funktion zusammen ?

DriveCrypt benötigt 16 Bit Stereo .WAV Dateien. Funktionierende Dateien können mit Programmen wie "WinDac" oder "Cool Edit" erstellt werden. Bitte benutzen Sie keine wav-Dateien mit absoluter Stille am Anfang der Musikdatei.

13.16 Kann man DriveCrypt Laufwerke auf beschreibbaren CDs und wiederbeschreibbaren CD-RWs abspeichern?

Ja, dies ist möglich. Hierzu erstellt man eine Containerdatei auf der Festplatte und brennt diese auf die CD.

Bitte beachten Sie, dass bei beiden Fällen (auch bei CD-RWs) das DriveCrypt Laufwerk nur gelesen werden kann.

13.17 Kann man Container auf DVD RAM CDs erstellen?

Ja, man kann. Bitte beachten Sie, dass DVD RAM CDs als UDF-Format anstelle von FAT16 formattiert werden müssen. Dieses Laufwerksformat wird bei Ihrem DVD RAM-Laufwerk mitgeliefert. Auf optischen Medien gespeicherte DriveCrypt Container werden wie normale les-/schreibbare

© 2003 SecurStar

Disketten behandelt.

13.18 Was ist mit Zip und Jaz Laufwerken?

Man kann Container Dateien auf diesen Laufwerken abspeichern. Man kann auch auf diesen Partitionen erstellen.

13.19 Was bedeutet 'Abrupte Abmeldung' ?

Abrupte Abmeldung erlaubt die Abmeldung von DriveCrypt Containern, auch wenn noch Programme Dateien aus diesem Container geöffnet haben. Diese Option ist nur für Notfallsituationen gedacht, da Windows bei der Benutzung der Funktion mit einem Blue-Screen abstürzen kann.

13.20 Hat diese Version von DriveCrypt immer noch die "Sicherheitskopie" Schlüsseldaten-Informationen?]

Ja, aber diese sind häufiger als einmal verschlüsselt um eine automatische Identifikation von DriveCrypt Containerdateien auszuschließen. Es sind jetzt Zusatzfunktionen enthalten, die diese Sicherheitskopiedaten nutzen. Eine Änderung des Passworts wandelt das Format Ihres alten Containers automatisch in die neue Spezifikation um.

13.21 Für was ist der "Traveller Modus", der installiert werden kann?

Traveller modus stellt eine besondere Art dar, DriveCrypt zu installieren. Mit ihr kann man Container öffnen, ohne DriveCrypt dauerhaft auf dem relevanten Windows-System installieren zu müssen.

Bestimmte Festplattenpartitionen brauchen eine Vollinstallation von DriveCrypt, damit auf diese zugegriffen werden kann (z.B. unter Windows 95/98). DriveCrypt im Traveller Modus kann nur auf austauschbaren Medien wie Floppydisketten usw. installiert werden.

© 2003 SecurStar

13.22 Kann man ein DriveCrypt Laufwerk über ein Netzwerk anmelden?

Ja, dies ist möglich.

13.23 Ich möchte S/MIME oder PGP benutzen, wieso sollte ich dieses Produkt benutzen?

S/MIME und PGP sind gute Produkte, aber sie funktionieren nur auf Datei- oder E-Mail-Basis. DriveCrypt erlaubt komplette Laufwerksverschlüsselung.

13.24 Kann man nicht einfach Microsoft's neues EFS Dateisystem von Windows 2000 benutzen?

Ja, aber die Verschlüsselung ist durch die U.S. Exportregulierungen nur mit abgeschwächter Verschlüsselung zulässig; und es können damit keine vollständigen Laufwerke verschlüsselt werden. Dies ist eine transparente Verzeichnis- oder Dateiverschlüsselung, welche aber nicht unter anderen Betriebssystemen nutzbar ist.

13.25 Microsoft benutzt "Public-Key Verschlüsselung" im EFS, um meine Schlüssel zu schützen. Ist diese Verschlüsselung nicht stärker als die in DriveCrypt benutzte?

Nein, in diesem Falle liegt ein unterschiedlicher Weg des Schutzes von Verzeichnis- und Dateiverschlüsselung durch Verschlüsselungsschlüssel vor.

13.26 Ist Verschlüsselung/Steganographie nicht verboten ?

Eventuell ja, dies hängt davon ab, in welchem Land Sie sich befinden. Bitte überprüfen Sie die in diesem Land vorherrschenden Gesetzte und Regulierungen, bevor Sie DriveCrypt benutzen.

© 2003 SecurStar

13.27 Wurde die DriveCrypt Verschlüsselung jemals geknackt?

Nein!
In der Vergangenheit veranstalteten wir einige Wettbewerbe mit Preisgeldern von bis zu 100,000 US$ den Ersten, der einen DriveCrypt Container knackt.

Keiner hat es geschafft. Und Sie dürfen sicher sein, dass alles, was Rang und Namen hat an diesem Wettbewerb teilgenommen hat!

(Siehe auch den Pressebereich auf unserer Homepage)

13.28 Gibt es Hintertüren in Ihrer Software?

NEIN, es gibt kein "Hintertürchen". Dies würde die perfekte Reputation des Produktes zerstören. Nebenbei gibt es kein Gesetz in Deutschland, dass uns zum Einbau eines Hintertürchens zwingen könnte.

13.29 Wurden Sie jemals von einer Regierung zum Einbau einer Hintertür aufgefordert?

Bisher hat uns niemand dannach gefragt, eine einzubauen.

Bitte beachten Sie auch, dass wir die SecurStar GmbH in Deutschland angesiedelt haben, weil Deutschland eines der wenigen Länder ist, welches solche starken Verschlüsselungen freigegeben und für gut befunden hat.

Sollten sich die Gesetze in Deutschland ändern, sind wir bereit, die Firma in einem anderen Land der Welt zu verlegen. Wir haben also nicht vor, ein Hintertürchen einzubauen.

13.30 Wir sind von der "Polizei". Können Sie uns helfen, Zugang zu den verschlüsselten Daten zu bekommen?

Leider ist das nicht möglich.

Unser Produkt ist für höchste Sicherheit in der Indutrie- und Bankenwelt konzipiert.

© 2003 SecurStar

Nicht einmal unserer eigenen Programmierer können einen DriveCrypt Container knacken.

Der einzige Weg an die Daten zu kommen führt über die Eingabe des korrekten Passwortes, welches in der Regel nur der Eigentümer des Containers oder ein Admin kennt.

13.31 Ist der Sourcecode Ihrer Software verfügbar?

Mit unseren Vorgängerversionen Scramdisk und E4M hatten wir eine lange Tradition mit "open source" software gepflegt. Mit diesen Produkten konnten millionen von Usern die Sicherheit und Funktionalität der Software überprüfen.

Leider hatten unsere Mitbewerber nichts besseres zu tun als unseren Sourcecode zu klauen, ein paar Routinen zu programmieren und ein "closed sourcecode" Produkt auf den Markt zu werfen. Sie haben also unsere Software geklont und nur das Userinterface verändert.

Wir hatten also kein Interesse mehr daran, unmengen von Geld und Zeit in die Entwicklulng zu stecken, damit Wettberwerber uns das Know How wegnehmen können. Wir geben den Source Code also nur nach vorheriger vertraglicher Vereinbarung raus (NDA in Verbindung mit einem angemessenen Auftrag).

Wir sind offen für andere Wege, den Sourcecode der Öffentlichkeit zugänglich zu machen. Alles was wir bräuchten ist eine Lösung, die unsere Interessen schützt. Eine Idee könnte eine Basisversion sein (in Verbindung mit deren Sourcecode). Auf diesem Wege können Paranoide User die Software zum Verschlüsseln und Entschlüsseln verwenden.

Bitte lassen Sie es uns wissen, wenn dies eine Lösung für Sie wäre oder ob Sie eine andere interessante Idee hätten.

Mailen Sie uns an unter: opensource@securstar.de

13.32 Was sind die Vorteile von DrivCrypt gegenüber Scramdisk und E4M? ?

Es gibt eine grosse Zahl von neuen Funktionen. Wir glauben dass wir das Funktionsreichste Tool haben, das im Moment verfügbar ist. Hier sind einige der neuen aufregenten Funktionen:

© 2003 SecurStar

- Höhere Sicherheit durch bis zu 1344 Bit starken Schlüssel und SHA 256
- Unterstützt bis zu 16 Terabytes verschlüsselter Daten
- Erstellung von versteckten Containern
- Hotkey Support (schnelle An- & Abmeldung Ihrer Laufwerke)
- Lockout Konsole um Ihren PC zu schützen, wenn Sie sich mal entfernen.
- Resizable verschlüsselte Laufwerke
- Red Screen Password Modus funktioniert nun auch unter Windows NT / 2000 & XP
- Fortgeschrittene Steganographie (Dateien können in Musik Files versteckt werden)
- Optionale Register-änderungen um die Dateiassoziierungen vornehmen zu können
- Hardware Support (USB Token und SmartCards)
- Einheitlicher "InstallShield" Style Installationsprozedur.
- Fragmentationsproblem unter Win9x gelöst.
- Netzwerksupport
- Arbeitet unter Windows 95/98/ME/NT/2000 und Windows XP
- Und vieles mehr....

13.33 Wie lautet das Default Passwort der Lokout Konsole?

Bei älteren Versionen (vor Version 3.01a) lautet das Default Password: **securstar**.

Neuere Versionen haben kein Default Passwort mehr.
Definieren Sie einfach eines (so schnell wie möglich).

© 2003 SecurStar

14 Versionsgeschichte

Neue Funktionen in Version 4.20

1. Die Limitierung der Containergröße wurde aufgehoben
   (Container die sich auf einer NTFS Partition befinden, können jetzt unbegrenzte Größe haben)
2. Die Benutzeroberfläche kann jetzt sowohl aus der Taskleiste, als auch vom Desktopshortcut aufgerufen werden.
3. Die Software Registrierungsroutine wurde automatisiert

Bugfixes:

1) Die Bildschirmdarstellung bei höheren Auflösungen wurde verbessert

- - - - - - - - - -

Version 4.10

1. Traveller Modus ermöglicht Lese-/Schreibzugriff für verschlüsselte Container (Schreibzugriff nur für Wechsellaufwerke)

Bugfixes:

1) Problem bei der Erstellung unsichtbarer Laufwerke, größer als 4GB, behoben.
2) Beim anmelden/abmelden des Laufwerkes kam es sporadisch zu Systemabstürze, behoben.
3) Problem beim ändern des Passwortes von unsichtbaren Container, behoben.
4) Darstellungsproblem der Taskleiste behoben
5) Traveller Modus startet DriveCrypt in Demo Modus, behoben.
6) Die Sicherheit der Passworteingabe im Roten Bildschirmmodus wurde erhöht
7) Kleinere Fehler wurden behoben ...

- - - - - - - - - -

Version 4.0

1. Moderneres und intuitivea Userinterface (GUI)
2. Grössenverstellbare Leisten um die Möglichkeit zu haben, alle Laufwerke und Partitionen auf einmal zu sehen.
3. Möglichkeit versteckte Laufwerke in bestehenden

© 2003 SecurStar

Containern/Partitionen zu errichten
4. Neue Möglichkeit die Partition ID zu verändern
5. Verschlüsselungsalgorithmen sind schneller und optimierter
6. Das "system service module" und die "container delete protection" wurden verbessert
7. Die Möglichkeit zu wählen, ob die abrupte Abmeldung das Programm beenden soll oder nicht
8. Detailiertere Informationen über jedes Laufwerk im Hauptbildschirm
9. Integrierte Onlinehilfe in der GUI
10. Erweiterte Program Line Parameter

Bugfixes:

- Kleinere Bugs wurden entfernt…

- - - - - - - - - -

Version 3.03c

Neue Funktionen:

·Erweiterung der command line parameters
·USB-stick/disk kann ab sofort verwendet werden.
·Die Encryption engine wurde verbessert
·Eine neuarte Registrierungsmethode wurde eingeführt.
·Antivirussoftware blockiert nicht mehr.
·kleinere Implementierungen vorgenommen…

Bugfixes:

·Rainbow Ikey 1000 meldete eine Container bislang nicht automatisch an. (gelöst)
·Problem mit der sicheren Zerstörung unbenutzten Speicherbereichs gelöst.
·Kompatibilitätsprobleme mit den SecuGen Fingerprint Sytemen gelöst.
·Gemischte Sprachfiles korrigiert.
·GUI Visualisierungsproblem gelöst.
·Taskbar Icon Visualisierungsproblem gelöst.
·Lösung kleinerer bugs …

- - - - - - - - - -

© 2003 SecurStar

Version 3.03B

·Schlüssel bis zu 1344 Bit (gefragtes Feature)
·3 neue Verschlüsselungsmodi (Blowfish 448, 3Blowfish and 3AES)
·PKCS#11 Protokoll für externe USB-Token
·Möglichkeit die Software auf jeder Maschine zu installieren, ohne den Key immer neu eingeben zu müssen.
(Feature wurde gefordert von: PriceWaterhouse Coopers)
·Kein voreingestelltes Passwort mehr (Konsolen Lockout)
·Kleinere Implementierungen vorgenommen…

Bugfixes:

·"DriveCrypt" and "Authention" sind ab sofort kompatibel. "Authention" frägt permanet den USB-Token ab, was DriveCrypt vom korrekten Zugriff abhielt. (Unser Dank an Herrn Graf von Benzel (Becketall), der uns von diesem Problem berichtete)
·kleinere bugs behoben …

- - - - - - - - - -

Version 3.03a

·Der Red-Screen Support für Windows NT/2000/XP ist ab sofort verfügbar
·Weiterer Schutz gegen Containerangriffe eingebaut.
·"Lockoutkonsole" gegen ungewollte Zugriffe wärend der Abwesenheit.
·Möglichkeit, die Containe automatisch abzumelden, wenn DC beendet wird
·kleinere Veränderungen…

Bugfixes

·Einige Bugs und Kompatibilitätsprobleme unter Windows XP gelöst
·Änderung der Containerfileextensionen wegen der XP Kompatibilitätsprobleme.

- - - - - - - - - -

Version 3.02a

Neue Features:

© 2003 SecurStar

·Windows XP kompatibel
·Fingerprint Reader werden unterstützt.
·Mehr Starup Optionen und Dateiassoziierungsmöglichkeiten.
·kleinere Veränderungen…

Bugfixes

·kleinere Bugs in der grafischen Darstellung der GUI behoben

- - - - - - - - - -

Version 3.01a

Neue Features:

·Scramdisk und E4M wurden zusammengeführt und zu DriveCrypt migriert
·Windows NT und 2000 Kompatibilität für Scramdisk
·Möglichkeit zur Grössenveränderung von verschlüsselten Containern
·SmartCard Reader Support (towitoko)
·Hardwaresupport für den Rainbow ikey 1000 (USB-Token)
·Abwärtskompatibel zu E4M und Scramdisk
·Steganographie wurde verbessert
·AES 256 bit und SHA 256
·Hotkey Support
·Sichere Löschung von nicht genutztem Speicherplatz

Bugfixes:

·Kleiner Probleme bei der Kompatibilität von E4M und Scramdisk

- - - - - - - - - -

1994-2001

E4M und Scramdisk: Die Programme Scramdisk und E4M waren als Open Source Software im Internet frei verfügbar. Unser Dank gilt den hunderten von Computer und Security Spezialisten, welche unser Produkt so stark und berühmt gemacht haben.

© 2003 SecurStar

15 Fehler und Einschränkungen

Diese Version von DriveCrypt hat keine bekannten Bugs.

Wenn Sie glauben, dennoch einen gefunden zu haben, dann versichern Sie sich bitte vorher (in der knowledge base page unserer Homepage), und kontaktieren uns danach mit der kompletten Information. Dies können Sie durch ausfüllen des "**Bug-Report**" Formulares auf unserer Homepage. Dann können wir das Problem (hoffentlich) lösen.

Wir belohnen Sie dafür mit einer kostenlosen Version von DriveCrypt oder einem 12 Monatigen Update Service.

© 2003 SecurStar