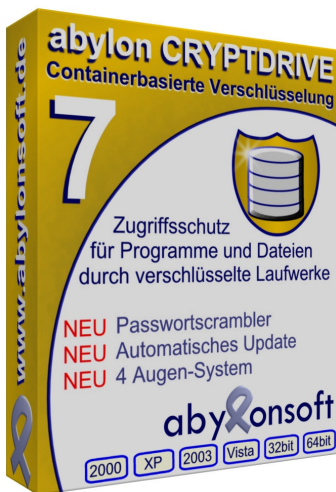




Containerbasierte, verschlüsselte Laufwerke für Programme und Daten



Speichern Sie Ihre sensiblen Dateien unverschlüsselt auf dem Rechner und bieten so ein leichtes Angriffsziel? Dabei können Ihre Daten hochsicher auf einem abylon CRYPTDRIVE gespeichert werden. Erst nach dem Öffnen mit Passwort, Chipkarte, USB-Token oder CD wird das Laufwerk im Datei Explorer angezeigt. Nun können Dateien geöffnet und Programme gestartet werden, wobei die AES- oder Blowfish-Verschlüsselung automatisch und im Hintergrund erfolgt.

- Netzwerkfähige containerbasierte, verschlüsselte Laufwerke
- Verschlüsselung mit dem Blowfish- (448 Bit) oder AES-Algorithmus (256 Bit)
- Zugriffsberechtigungen über Passwort, Chipkarte, USB-Token, CD oder Zertifikat
- Automatische Verschlüsselung im Hintergrund für Programme und Dateien
- Nur geöffnete Laufwerke sind im Datei Explorer sichtbar

Zertifizierungen / Awards



Kontakt

abylonsoft

abylonsoft – Dr. Thomas Klabunde
 Zum Eichwald 43
 D – 55444 Seibersbach

Tel. +49 (6724) 60 27 59 – 0
 Fax. +49 (6724) 60 27 59 – 1

Internet: <http://www.abylonsoft.de>
 Support: <http://www.abylonsoft.de/support.htm>

Warum brauchen Sie abylon CRYPTDRIVE

Speichern Sie auch noch Ihre Daten unverschlüsselt auf Ihrem Rechner? Dabei würden Sie doch auch keine vertraulichen Daten ans Schwarze Brett hängen oder in der Tageszeitung veröffentlichen. Der Rechner bietet zahlreiche Schwachstellen, welche potentielle Angreifer ausnutzen können. Von den Daten ist schnell eine Kopie erstellt und schon können diese Informationen missbraucht werden.

Große Gefahren bestehen auch bei der gemeinsamen Nutzung von Rechnern und Netzwerken, beim Diebstahl, der Reparatur oder der Entsorgung von Rechnern.

Wie funktioniert abylon CRYPTDRIVE

Mit abylon CRYPTDRIVE lassen sich spielend einfach virtuelle, komplett verschlüsselte Laufwerke erstellen. Somit sind alle Dateien und Programme, die sich auf diesem Laufwerk befinden, vor unberechtigtem Zugriff geschützt.

- Verschlüsselung mit dem Blowfish- (448 Bit) oder AES-Algorithmus (256 Bit)
- Netzwerkfähige containerbasierte, verschlüsselte Laufwerke
- Nur geöffnete Laufwerke sind sichtbar
- Zugriffsberechtigungen über Kennwort, externes Gerät oder Zertifikat

Auf dem Computer gespeicherte Dateien können auf vielfältige Weise in die falschen Hände gelangen. Abhilfe schafft nur eine ausreichende Verschlüsselung der Daten. Das abylon CRYPTDRIVE bietet ein einfaches Verfahren zum Erstellen von verschlüsselten Laufwerken, den sogenannten Containern. Durch die Verschlüsselung mit dem Blowfish- (448 Bit) oder AES-Algorithmus (256 Bit) sind die auf dem Laufwerk gespeicherten Dateien und Programme vor unbefugtem Zugriff gesichert. Erst wenn das Laufwerk geöffnet wird, ist ein Zugriff über den Datei Explorer möglich, wobei die Ver- und Entschlüsselung automatisch im Hintergrund erfolgt. Als Geheimnis zum Öffnen des Laufwerkes kann entweder ein Passwort über die Tastatur eingegeben, eine Chipkarte, eine CD bzw. ein USB-Stick verwendet werden. Die Kombination von Passwort und Medium ist zur Abwehr von Keyloggern ebenfalls möglich.

Im professionellen Umfeld können auch die Zugriffsberechtigungen über Zertifikate administriert werden. Dabei werden zahlreiche Zertifikatschipkarten oder USB-Token unterstützt.

Einsatzbereiche und Szenarien

1. **Schutz** von Dateien auf dem lokalen Rechner: Sie verwenden Ihren Heimcomputer zusammen mit Ihrem Partner oder Ihren Kinder und möchten nicht das spezielle Dateien auf Ihrer Festplatte (z. B. Textdokumente, Bilder oder Videos) von diesen gesehen werden. Speichern Sie einfach diese Dateien in einem verschlüsselten Laufwerk und nach dem Schließen kommt niemand ohne das entsprechende Passwort oder die passende Chipkarte an die Dateien.

2. **Installation** von Programmen auf dem abylon CRYPTDRIVE: Auf dem verschlüsselten Laufwerk ist die Installation von Software möglich. Legen Sie ein neues verschlüsseltes Laufwerk an, öffnen dieses und starten danach die Installation des Programms. Bei der Auswahl des Zielordners wählen Sie dann einen Ordner auf dem verschlüsselten Laufwerk aus. Mit dem Schließen des Laufwerks werden auch die Programmdateien der Software verschlüsselt und sind nicht mehr im Zugriff. Das Programm lässt sich erst wieder ausführen, wenn das entsprechende abylon CRYPTDRIVE

geöffnet wird.

3. **Anlegen** von Links auf dem Desktop und automatisches Öffnen nach dem Hochfahren: Zum schnellen Öffnen und Schließen von einzelnen verschlüsselten Laufwerken können Sie im Verbindungsmanager Icons (Verweise) auf dem Desktop erstellen (Menu der rechten Maustaste). Diese ermöglichen Ihnen einen schnellen Zugriff. Vor dort lassen sich die Verweise beispielsweise in den Autostart-Ordner des Startmenu kopiert. So werden nach dem Hochfahren des Rechners die entsprechenden verschlüsselten Laufwerke automatisch geöffnet.

4. **Zugriff** von mehreren unterschiedlichen Rechnern: Als Speicherort (Initialverzeichnis = UNC-Pfad) der verschlüsselten Laufwerke können Sie auch einen Netzwerkrechner auswählen. Dabei ist der Zugriff auf ein verschlüsseltes Laufwerk von verschiedenen Rechnern möglich. Die Übertragung der Daten erfolgt hierbei verschlüsselt über das Netzwerk und erst auf dem Client werden die Dateien entschlüsselt. (HINWEIS Ein gleichzeitiger Zugriff mehrerer Anwender ist nur beim Mounten und Freigeben der verschlüsselten Laufwerke auf einem Server möglich!)

5. **Speicherung** auf einem externen Device: Sie können die verschlüsselten Laufwerke auch auf einem externen Device (z. B. USB-Token) speichern. Damit können Sie die verschlüsselten Daten mitnehmen und auch bei Verlust sind diese vor illegalem Zugriff gesichert.

6. **Zugriffsberechtigungen** durch Zertifikate: Im HYBRID-Modus können einem Laufwerk mehrere Zertifikate als Berechtig zugewiesen werden, womit beispielsweise auch Ihr Kollege oder Vorgesetzter auf Ihre Daten zugreifen kann. Dies kann vor allem im Krankheitsfall oder bei Verlust der Zertifikatschipkarte das Unternehmen vor Schaden schützen.

7. **Batchverarbeitung**: Mittels einer ausführbaren Batch-Datei können die Laufwerke automatisch geöffnet, Freigaben zugewiesen und Programme gestartet werden

8. **Diverse** Schutzfunktionen gegen Keylogger: Der PasswordScrambler die Passworteingabe über die Tastatur und die Bild-Eingabe verwendet kryptische Passwortsequenzen

Sprache

- Deutsch, Englisch, Spanisch (Beta)

Download der Testversion und Withepapers

- <http://www.abylonsoft.de/cryptdrive/download.htm>

Weitere Informationen

- <http://www.abylonsoft.de/cryptdrive/index.htm>

Systemvoraussetzungen:

- Prozessor: Pentium (oder vergleichbare)
- Arbeitsspeicher: 256 MByte RAM
- Freier Festplattenspeicher ca. 25 Mbyte
- Betriebssystem Windows NT4, 2000, XP, Vista 32 und 64bit, 2003 oder WTS
- Administrationsrechte für die Installation

Pressemitteilungen und Veröffentlichungen

Übersicht: <http://www.abylonsoft.de/presse.htm>