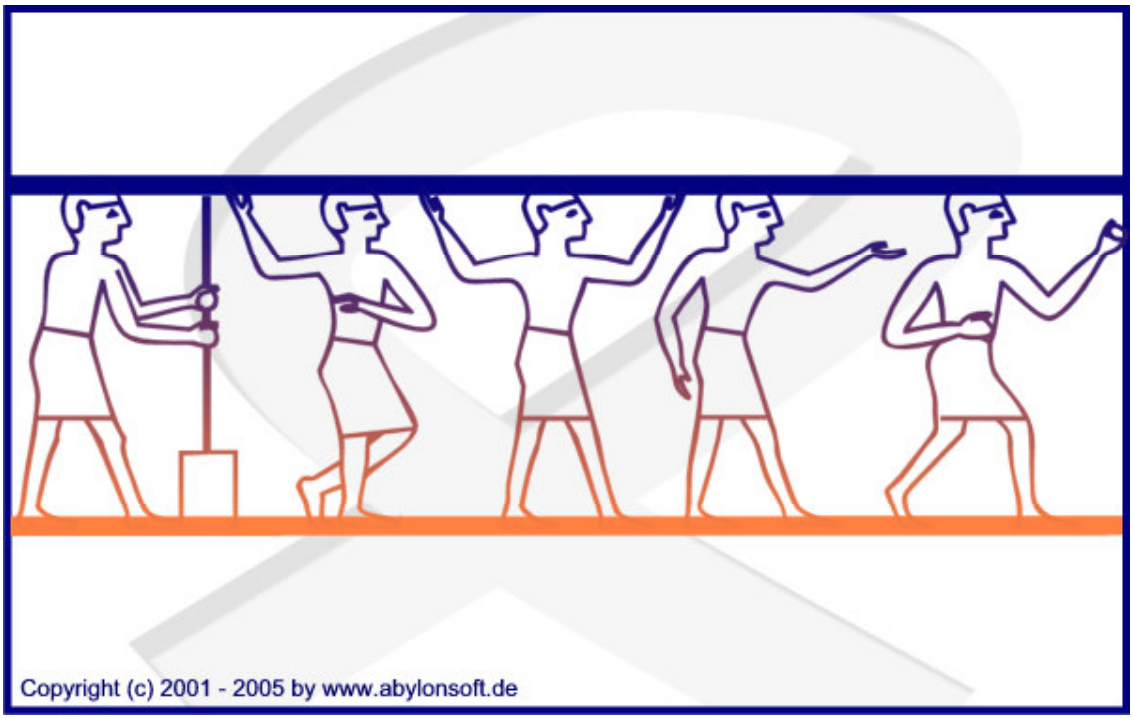
WITHEPAPER - ANLEGEN UND VERWENDEN EINES ABYLON CRYPTDRIVE

ABYLONSOFT – DR. KLABUNDE



Softwareentwicklung, Beratung und Verkauf von IT-Sicherheitssoftware

Revision 2.1

abylonsoft - Dr. Thomas Klabunde
Zum Eichwald 43
D-55444 Seibersbach
Tel.: +49-(0)-6724-602759-0
Fax.: +49-(0)-6724-602759-1
Homepage: http://www.abylonsoft.de
Kontakt: http://www.abylonsoft.de/dcontact.php

Stand: 10.07.2008

HISTORIE

Version	Datum	Kommentar
1.0	24.10.2005	Dokument neu erstellt (TK)
2.0	23.06.2008	Dokument entsprechend Version 7 angepasst (WB)
2.1	10.07.2008	Einsatz eines Wechseldatenträgers ergänzt (TK)

INHALTSVERZEICHNIS

Historie *2*

Inhaltsverzeichnis *3*

1 Content *4*

2 Funktionsweise des abylon CRYPTDRIVE *4*

3 Anlegen und Administrieren eines neuen abylon CRYPTDRIVE *5*

3.1 Anlegen eines SYMM-System CRYPTDRIVE mit Passworteingabe oder Chipkarte **5**

3.2 Anlegen eines HYBRID-System CRYPTDRIVE mit Zertifikaten **10**

3.3 Administrieren eines HYBRID-System CRYPTDRIVE mit Zertifikaten **14**

3.4 Anlegen eines abylon CRYPTDRIVE auf einem Wechseldatenträger (SYMM und HYBRID-System) **16**

4 Verwenden eines abylon CRYPTDRIVE (SYMM und HYBRID-System) *20*

4.1 Öffnen und arbeiten mit einem abylon CRYPTDRIVE **20**

4.2 Importieren eines bestehenden abylon CRYPTDRIVE **22**

4.3 Umbenennen oder Verschieben eines abylon CRYPTDRIVE **23**

4.4 Ändern des Passwortes oder des Verschlüsselungssystems **24**

5 Hinweise *26*

5.1 Automatisches Öffnen **26**

5.2 Automatisches Schließen **26**

5.3 Automatisch öffnen, Freigaben zuweisen und Programme starten **26**

5.4 Gleichzeitiger Zugriff durch Installation auf einem Server **27**

5.5 Datenverlust vermeiden **27**

5.6 Unterschied zwischen abylon CRYPTDRIVE und abylon SHAREDDRIVE **27**

5.7 Einschränken der Anwender-Rechte **28**

5.8 Weitere Dokumente und FAQs **29**

1 CONTENT

Dieses Whitepaper beschreibt das Anlegen und Verwenden eines **abylon CRYPTDRIVE** zum Schutz der Daten auf einem Rechner.

2 FUNKTIONSWEISE DES ABYLON CRYPTDRIVE

Das **abylon CRYPTDRIVE** schützt Ihre vertraulichen Daten vor unerlaubtem Zugriff. Die Daten werden in sogenannten verschlüsselten Containern auf der Festplatte abgelegt, wobei der Einsatz des Blowfish- (448 Bit) und AES-Algorithmus (256 Bit) höchste Sicherheit garantiert. Das Laufwerk wird durch die Eingabe des Passwortes oder das Einstecken der Chipkarte geöffnet und als neues Laufwerk im Datei Explorer angezeigt. Erst jetzt können hier gespeicherte Daten bearbeitet und Programme gestartet werden. Bei jeder Dateioperation erfolgt die Ver- und Entschlüsselung ohne merkliche Zeitverzögerung automatisch im Hintergrund.

Im professionellen Umfeld können für die Zugriffsberechtigung auch Zertifikate eingesetzt werden. Hierbei werden eine Vielzahl handelsüblicher Zertifikatschipkarten und Token unterstützt.

3 ANLEGEN UND ADMINISTRIEREN EINES NEUEN ABYLON CRYPTDRIVE

3.1 Anlegen eines SYMM-System CRYPTDRIVE mit Passworteingabe oder Chipkarte

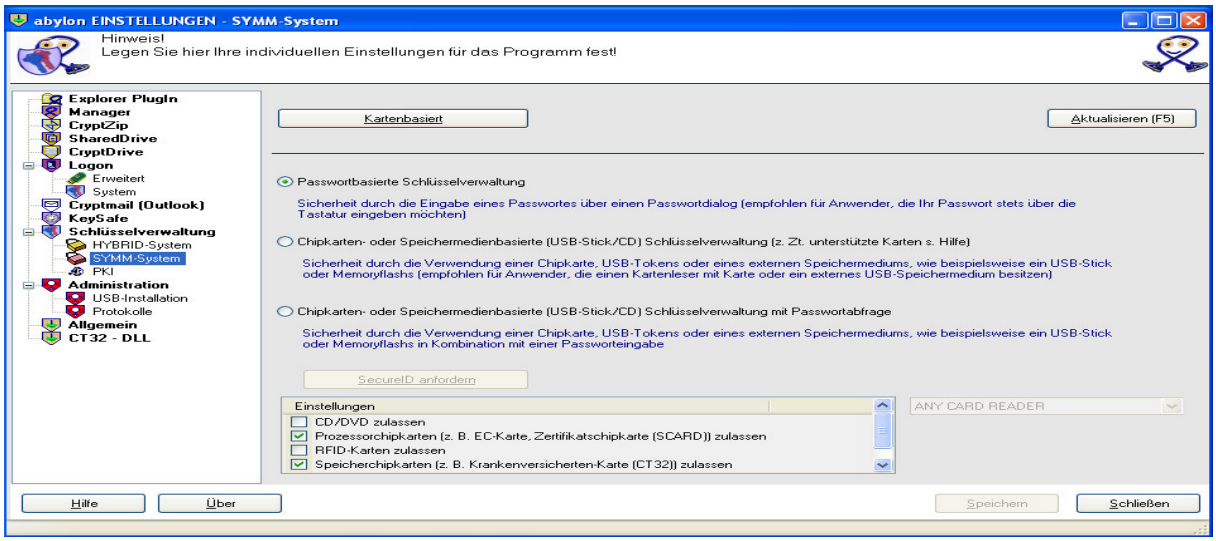
Anleitung zum Anlegen eines **abylon CRYPTDRIVE** unter Verwendung des SYMM-System. Hierbei wird die Passworteingabe oder die Verwendung von Chipkarten (z. B. EC-Karte) unterstützt und als Verschlüsselungsalgorithmus AES (Schlüssellänge 256 Bit) und Blowfish (Schlüssellänge 448 Bit) eingesetzt.

HINWEIS Für die Verwendung einer Chipkarte wird ein Kartenleser benötigt, welcher eine PC/SC-Schnittstelle (EC-Karte) oder einer CT32-API (Speicherchipkarte) anbietet.

1. Öffnen Sie den Einstellungsdialog und wechseln auf die Seite '*Schlüsselverwaltung->SYMM-System*'

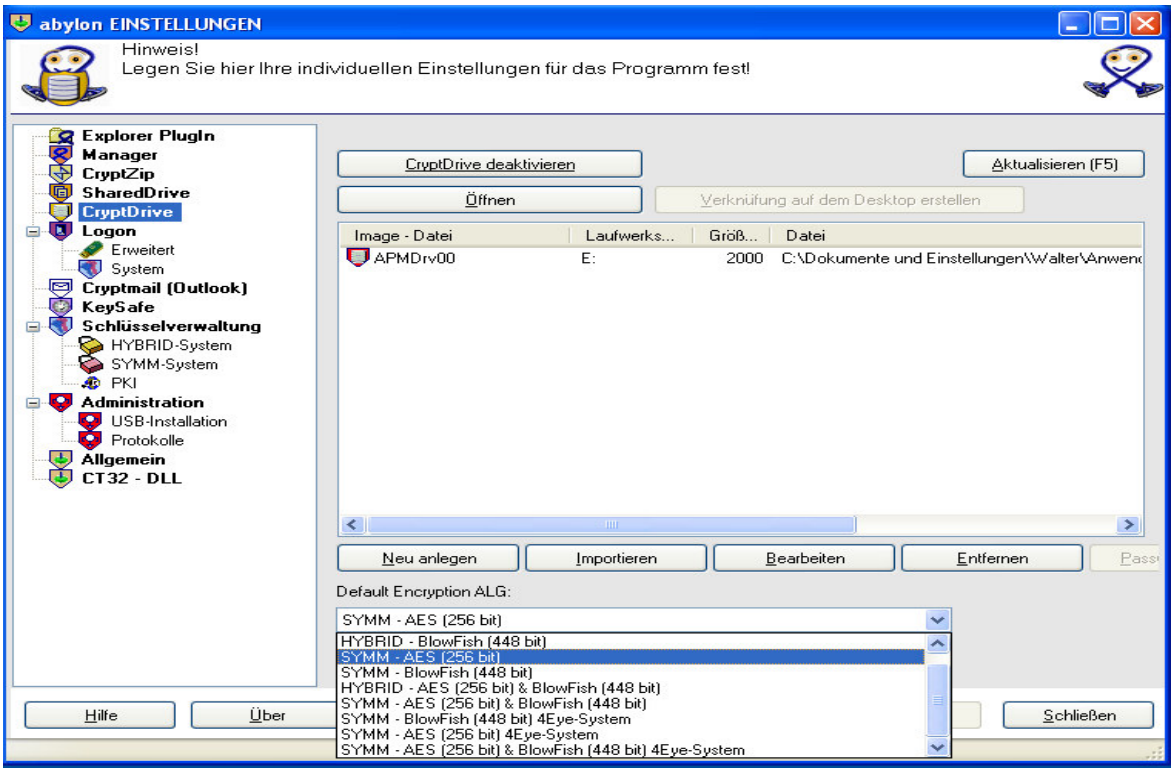
Hier können Sie folgende Optionen selektieren:

- **Passwortbasierte Schlüsselverwaltung:** Beim SYMM-System erfolgt die Sicherheit (Verschlüsselung oder Zugriffskontrolle) durch die Eingabe eines Passwortes über einen Passwortdialog (empfohlen für Anwender, die Ihr Passwort stets über die Tastatur eingeben möchten).
- **Chipkartenbasierte Schlüsselverwaltung:** Beim SYMM-System erfolgt die Sicherheit (Verschlüsselung oder Zugriffskontrolle) durch die Verwendung einer Chipkarte, USB-Token, einer CD/DVD oder eines externen Speichermediums. Ein Passwort ist nicht erforderlich!
- **Chipkarten- oder Speichermedien basierte (USB-Stick/CD) Schlüsselverwaltung mit Passwortabfrage:** Beim SYMM-System erfolgt die Sicherheit (Verschlüsselung oder Zugriffskontrolle) durch die Verwendung einer Chipkarte, USB-Token, einer CD/DVD oder eines externen Speichermediums. Für eine erweiterte Sicherheit muss zusätzlich ein Passwort eingegeben werden!



2. Wechseln Sie nun im Einstellungsdialog auf die Seite '*CryptDrive*' und wählen einen der folgenden '*Default Encryption ALG*' aus:

- **SYMM – AES (256 bit)**: Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit).
- **SYMM – Blowfish (448 bit)**: Passwortbasierte symmetrische Verschlüsselung mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).
- **SYMM-AES 4Eye-System:** Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit). Beim Vieraugensystem (4Eye-System) müssen hintereinander 2 Passwörter eingegeben werden.
- **SYMM-Blowfish 4Eye-System:** Passwortbasierte symmetrische Verschlüsselung mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit). Beim Vieraugensystem (4Eye-System) müssen hintereinander 2 Passwörter eingegeben werden.
- **SYMM-AES & Blowfish:** Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit) und anschließend mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).
- **SYMM-AES & Blowfish 4Eye-System:** Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit) und anschließend mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit). Beim Vieraugensystem (4Eye-System) müssen hintereinander 2 Passwörter eingegeben werden.

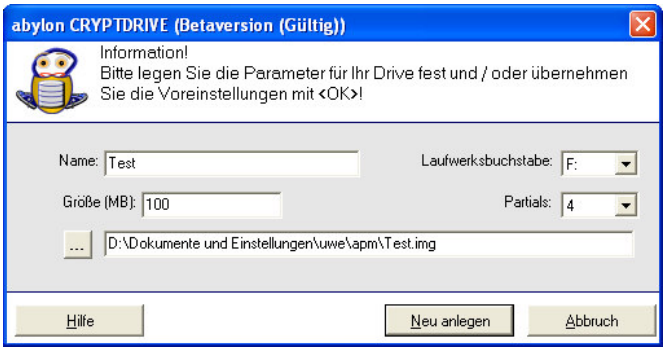


3. Drücken Sie den Schalter '*Neu anlegen*'

4. In dem angezeigten Dialog können Sie folgende Optionen festlegen:

- **Name:** Angezeigter Name des CRYPTDRIVE
- **Laufwerksbuchstabe:** Buchstabe, unter dem das CRYPTDRIVE im Datei Explorer angezeigt wird
- **Größe in MB:** Speichergröße des CRYPTDRIVE in MB (max. 200.000 MB = 200 GB)
- **Partials:** Anzahl der Teile, in der das CRYPTDRIVE auf der Festplatte aufgeteilt wird
- **Speicherort**: Verzeichnis und Dateiname, unter dem das CRYPTDRIVE auf der Festplatte gespeichert sein wird

Zum Abschließen des Vorgangs drücken Sie den Schalter '*Neu anlegen*'.



5. Sie werden nun gefragt, ob das Laufwerk direkt geöffnet werden soll. Bestätigen Sie hier mit '*Ja*'.

6. Je nach Einstellung auf der Seite '*Schlüsselverwaltung->SYMM-System*'

müssen Sie nun

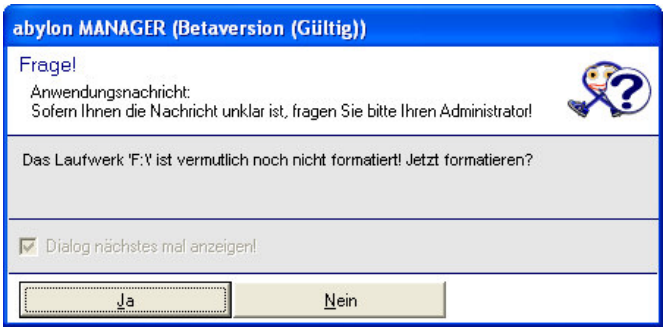
- **2 mal das gewünschte Passwort eingeben**

oder

- **die zu verwendende Chipkarte in den Kartenleser einlegen**

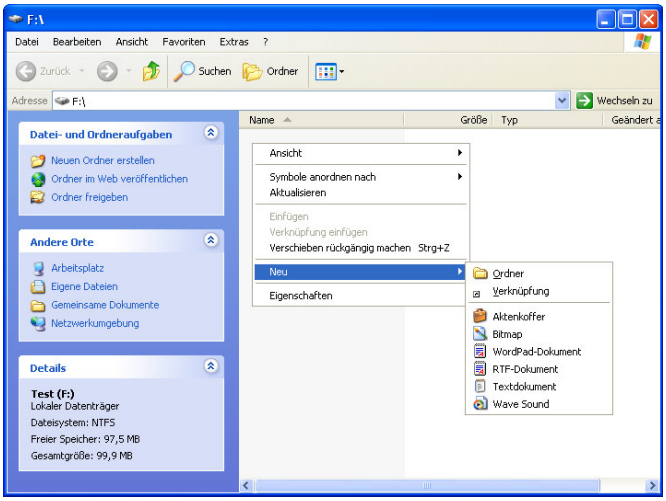
oder

7. Die Laufwerksdateien werden nun auf der Festplatte angelegt. Zum Abschluss muss das neue virtuelle Laufwerk noch formatiert werden. Bestätigen Sie hier mit '*Ja*'.

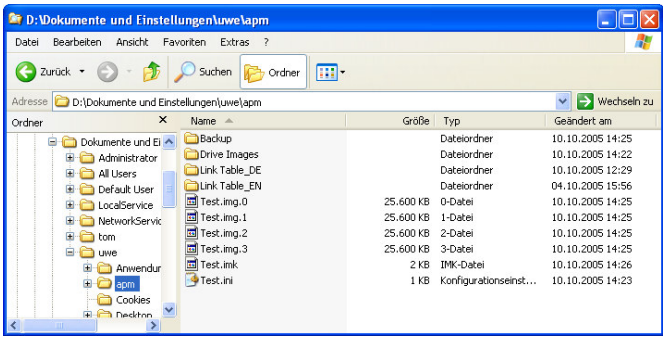


HINWEIS Der Formatierungsvorgang kann je nach Größe des Laufwerkes einige Minuten in Anspruch nehmen.

8. Das angelegte Laufwerk wird nun im Datei Explorer mit dem angegebenen Laufwerksbuchstaben angezeigt. Nun können Sie dieses Laufwerk wie gewohnt verwenden und Dateien und Verzeichnisse anlegen oder Programme installieren.

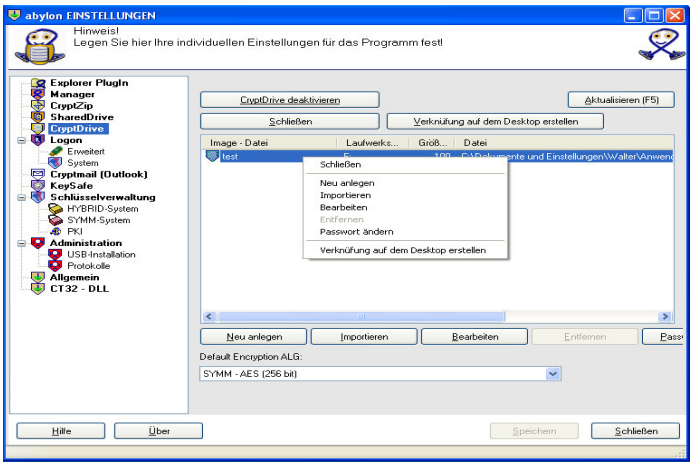


9. Die Dateien werden NICHT direkt auf Ihrer Festplatte abgelegt sondern in den sogenannten verschlüsselten Container. Dadurch sind die Dateien unsichtbar und gegen einen unbefugten Zugriff gesichert.



10. In den Einstellungen unter 'CryptDrive' werden alle eingerichteten CRYPTDRIVEs in einer Liste angezeigt. Hier können die einzelnen Laufwerke geöffnet und geschlossen werden.

Zusätzlich lassen sich über die rechte Maustaste Verknüpfungen auf dem Desktop erstellen. Über diese Icons können ebenfalls die Laufwerke geöffnet und geschlossen werden. Diese Verknüpfungen können beispielsweise auch in den Autostart des Startmenus kopiert werden.



11. Ein verschlüsseltes CRYPTDRIVE lässt sich in Zukunft nur durch die Eingabe des Passwortes oder die entsprechende Chipkarte öffnen.

oder

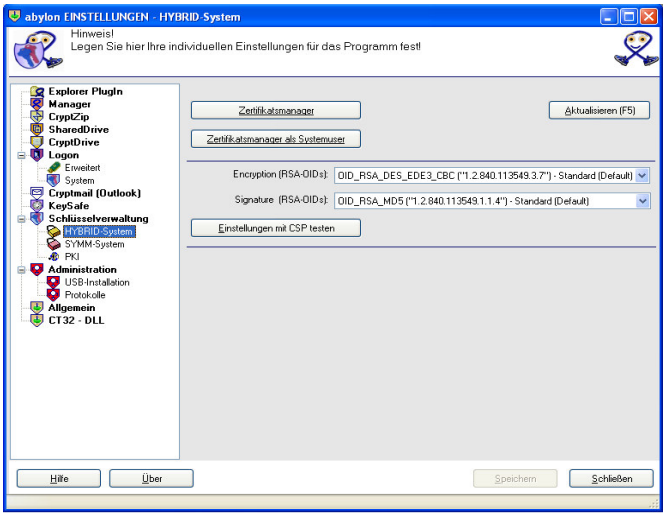
3.2 Anlegen eines HYBRID-System CRYPTDRIVE mit Zertifikaten

Anleitung zum Anlegen eines **abylon CRYPTDRIVE** unter Verwendung des HYBRID-Systems. Hierbei werden zur Authentifizierung Softwarezertifikate oder Zertifikatstoken benötigt und als Verschlüsselungsalgorithmus AES (Schlüssellänge 256 Bit) und Blowfish (Schlüssellänge 448 Bit) eingesetzt.

HINWEIS Für die Verwendung von Zertifikaten auf externen Token (z. B. Chipkarten) muss der verwendete CSP (Crypto Service Provider) einen Link der Zertifikate in der Windows-Zertifikatsdatenbank eintragen. Zusätzlich muss als Verwendungszweck der Zertifikate sowohl die Verschlüsselung als auch die Signatur angegeben sein.

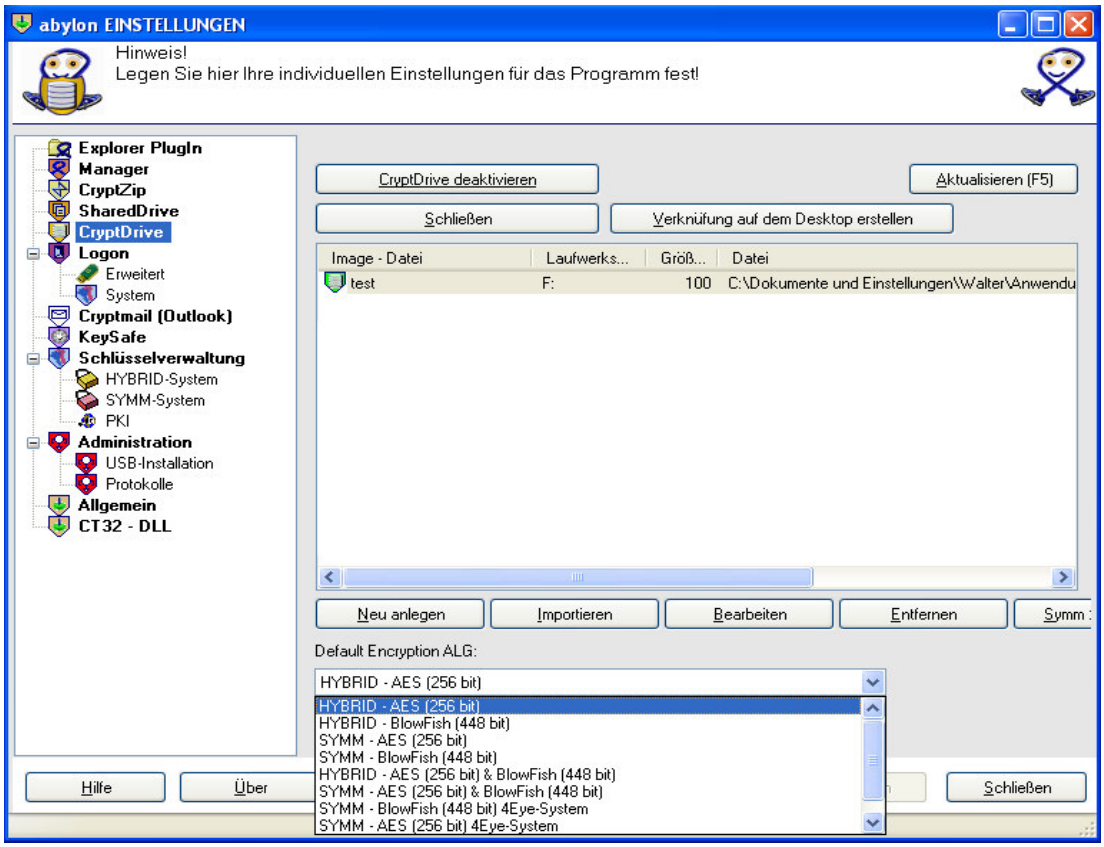
1. Falls noch nicht erfolgt, müssen Sie zuerst Ihr eigenes Signatur- und Verschlüsselungszertifikat festlegen. Öffnen Sie hierzu den Einstellungsdialog und wechseln auf die Seite '*Schlüsselverwaltung->HYBRID-System*'

Öffnen Sie den '*Zertifikatsmanager*' und legen Sie dort Ihr Signatur- und Verschlüsselungszertifikat fest.



2. Wechseln Sie nun im Einstellungsdialog auf die Seite '*CryptDrive*' und wählen einen der beiden folgenden '*Default Encryption ALG*' aus:

- **HYBRID – AES (256 bit)**: Die Authentifizierung zum Öffnen des Laufwerkes erfolgt mit Zertifikaten und das Laufwerk wird mit dem symmetrischen Verschlüsselungsverfahren AES und einer Schlüssellänge von 256 Bit verschlüsselt.
- **HYBRID – Blowfish (448 bit)**: Die Authentifizierung zum Öffnen des Laufwerkes erfolgt mit Zertifikaten und das Laufwerk wird mit dem symmetrischen Verschlüsselungsverfahren Blowfish und einer Schlüssellänge von 448 Bit verschlüsselt.
- **HYBRID – AES (256 bit) & HYBRID – Blowfish (448 bit) :** Die Authentifizierung zum Öffnen des Laufwerkes erfolgt mit Zertifikaten und das Laufwerk wird mit dem symmetrischen Verschlüsselungsverfahren AES (Schlüssellänge 256 Bit) und anschließend mit dem Blowfish -Algorithmus (Schlüssellänge 448 Bit) verschlüsselt.

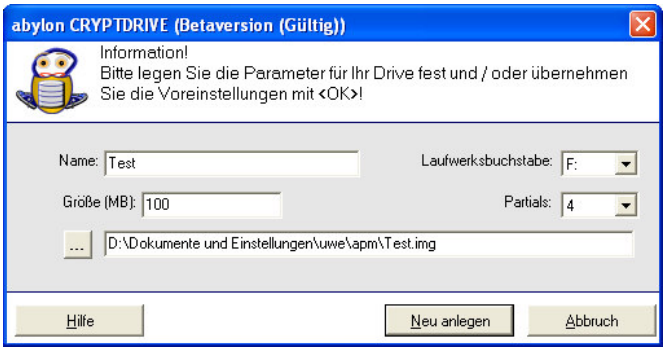


3. Drücken Sie den Schalter '*Neu anlegen*'

4. In dem angezeigten Dialog können Sie folgende Optionen festlegen:

- **Name:** Angezeigter Name des CRYPTDRIVE
- **Laufwerksbuchstabe:** Buchstabe, unter dem das CRYPTDRIVE im Datei Explorer angezeigt wird
- **Größe in MB:** Speichergröße des CRYPTDRIVE in MB (max. 200.000 MB = 200 GB)
- **Partials:** Anzahl der Teile, in der das CRYPTDRIVE auf der Festplatte aufgeteilt wird
- **Speicherort**: Verzeichnis und Dateiname, unter dem das CRYPTDRIVE auf der Festplatte gespeichert sein wird

Zum Abschließen des Vorgangs drücken Sie den Schalter '*Neu anlegen*'.

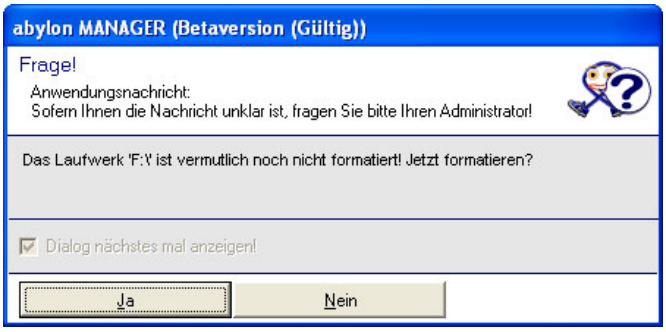


5. Sie werden nun gefragt, ob das Laufwerk direkt geöffnet werden Soll. Bestätigen Sie hier mit '*Ja*'.

6. Entsprechend der Sicherheitsstufe des Zertifikates werden Sie nach dessen Passwort (PIN) gefragt.

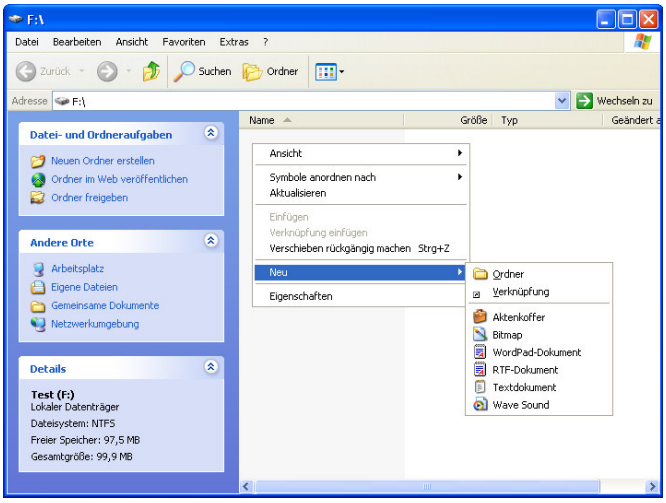
HINWEIS Je nach verwendetem CSP unterscheidet sich der Passwortdialog.

7. Die Laufwerksdateien werden nun auf der Festplatte angelegt. Zum Abschluss muss das neue virtuelle Laufwerk noch formatiert werden. Bestätigen Sie hier mit '*Ja*'.

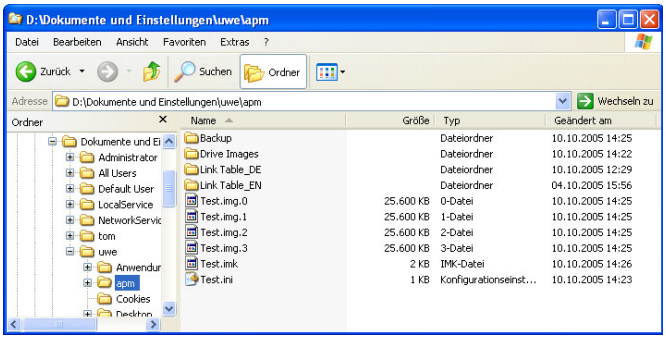


HINWEIS Der Formatierungsvorgang kann je nach Größe des Laufwerkes einige Minuten in Anspruch nehmen. Bestehende Daten auf der Festplatte werden NICHT überschreiben.

8. Das angelegt Laufwerk wird nun im Datei Explorer mit dem angegebenen Laufwerksbuchstaben angezeigt. Nun können Sie dieses Laufwerk wie gewohnt verwenden und Dateien und Verzeichnisse anlegen oder Programme installieren.

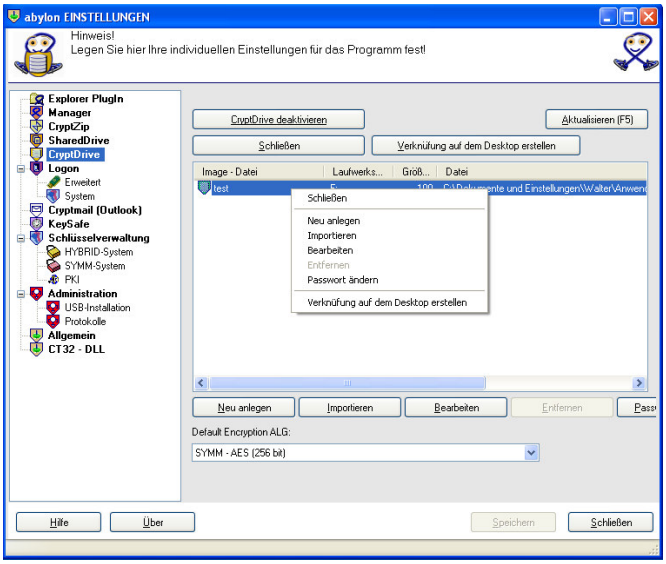


9. Die Dateien werden NICHT direkt auf Ihrer Festplatte abgelegt, sondern in den sogenannten verschlüsselten Container. Dadurch sind die Dateien unsichtbar und gegen einen unbefugten Zugriff gesichert.



10. In den Einstellungen unter 'CryptDrive' werden alle eingerichteten CRYPTDRIVEs in einer Liste angezeigt. Hier können die einzelnen Laufwerke geöffnet und geschlossen werden.

Zusätzlich lassen sich über die rechte Maustaste Verknüpfungen auf dem Desktop erstellen. Über diese Icons können ebenfalls die Laufwerke geöffnet und geschlossen werden. Diese Verknüpfungen können beispielsweise auch in den Autostart des Startmenus kopiert werden.



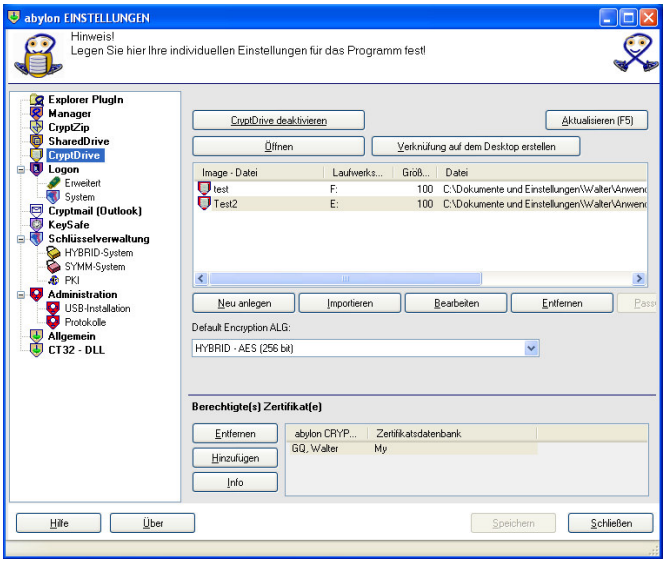
3.3 Administrieren eines HYBRID-System CRYPTDRIVE mit Zertifikaten

Die Administration der Zugriffsberechtigung eines **abylon CRYPTDRIVE** ist nur bei der Verwendung des HYBRID-Systems möglich. Hierbei können einem CRYPTDRIVE berechtigte Zertifikate hinzugefügt oder entfernt werden.

Dies ermöglicht eine einfache und zentrale Administration. Um in Zukunft beispielsweise einem Mitarbeiter den Zugriff auf das CRYPTDRIVE zu verwehren, braucht nur das entsprechende Zertifikat gelöscht werden.

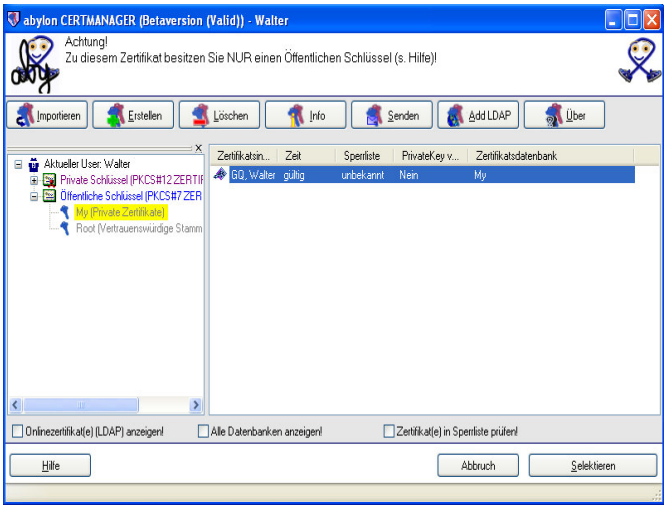
1. Eine Administration der Zugriffsberechtigungen ist nur bei Laufwerken mit dem '*Encryption Algorithm*' **HYBRID – AES** oder **HYBRID – Blowfish** möglich. Öffnen Sie dazu im Einstellungsdialog die Seite '*CryptDrive*' und wählen das zu administrierende Laufwerk aus. Im unteren Bereich des Fensters wird eine Liste der berechtigten Zertifikate angezeigt. Hier können die Zertifikate hinzugefügt oder entfernt werden.

HINWEIS Eine Administration der HYBRID-System Laufwerke ist auch direkt im **abylon CERTMANAGER** möglich!



2. Zum Entfernen oder Hinzufügen drücken Sie den entsprechenden Schalter.

2a. Beim **Hinzufügen** öffnet sich der **abylon CERTMANGER** zum Auswählen der gewünschten Zertifikate. Dabei können sowohl öffentliche (PKCS#7 Zertifikate) als auch private Schlüssel (PKCS#12 Zertifikate) ausgewählt werden. Zusätzlich ist ein Zugriff auf LDAP-Server und die Verwendung der **abylon SMALL PKI** und **abylon DATEI PKI** (Aktivierung in den Einstellungen unter Schlüsselverwaltung->PKI) möglich.



2b. Beim **Entfernen** wird das selektierte Zertifikat aus der Liste der berechtigten Zertifikate entfernt.

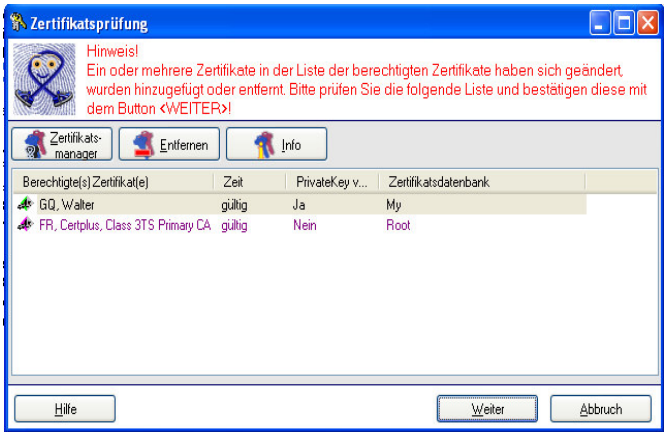
3. Die Änderungen der Zugriffs-berechtigungen müssen Sie durch Eingabe des Passwortes (PIN) bestätigen.

HINWEIS Je nach verwendetem CSP unterscheidet sich der Passwortdialog, bzw. die Passworteingabe ist aufgrund des PIN-Cashe nicht notwendig.

4. Beim nächsten Öffnen des CRYPTDRIVE werden in einem Dialog noch einmal die Änderungen der berechtigten Zertifikate angezeigt.

Sollten nicht berechtigte Zertifikate aufgeführt sein, so können diese hier entfernt werden. Dieser Dialog dient der Sicherheit, sodass nicht heimlich unberechtigte Zertifikate eingeschleust werden können.

Zum Abschluss müssen Sie nur noch die Änderungen durch drücken des Schalters '*Weiter*' übernehmen.



5. Danach werden Sie zweimal aufgefordert Ihr Passwort (PIN) einzugeben, sofern kein PIN-Cache aktiviert wurde.

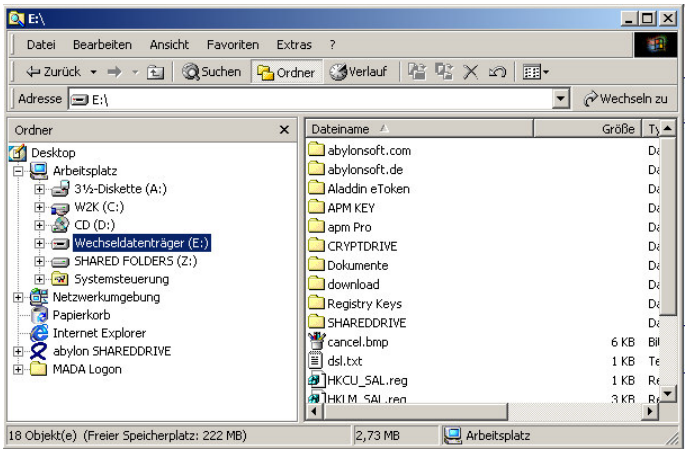
HINWEIS Je nach verwendetem CSP unterscheidet sich der Passwortdialog.

HINWEIS Zum Einschränken der Anwender-Rechte lesen Sie bitte das Whitepaper „Informationen zu Programmsteuerdateien und Registry für Administrative Zwecke“. Das aktuelle Dokument finden Sie auf der abylonsoft-Homepage unter '*Download*'!

3.4 Anlegen eines abylon CRYPTDRIVE auf einem Wechseldatenträger (SYMM und HYBRID-System)

Beim Anlegen eines neuen **CRYPTDRIVE** kann der Speicherort für die Container frei gewählt werden. Hierbei können auch Wechseldatenträger, wie z. B. USB-Sticks oder USB-Festplatten ausgewählt werden.

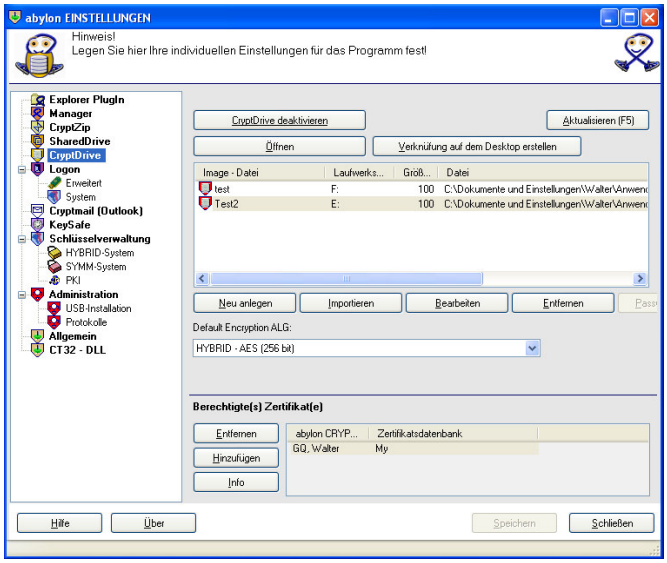
1. Zuerst müssen die Treiber des Wechseldatenträger (z. B. USB-Stick) auf dem Rechner installiert werden. Durch Plug&Play erfolgt dies in der Regel voll automatisch. Danach wird der Wechseldatenträger im Datei Explorer angezeigt.



2. Öffnen Sie den abylon Einstellungsdialog und wechseln auf die Seite '*CryptDrive*'.

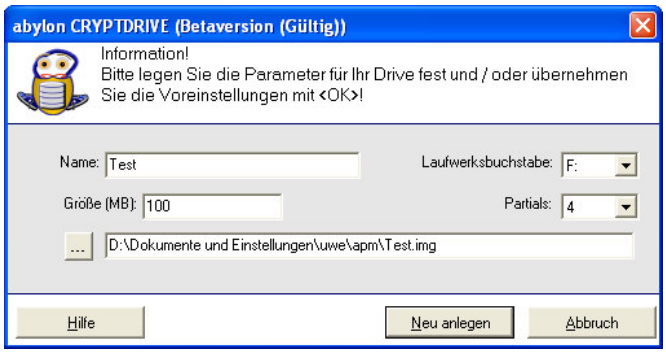
Hier wählen Sie unter Default Encryption ALG den gewünschten Verschlüsselungsalgorithmus aus (SYMM oder HYBRID).

Mit '*Neu anlegen'* ein neues CRYPTDRIVE an.



3. In dem Einstellungsdialog können Sie den Namen, die Größe und den Speicherort des neuen CRYPTDRIVEs festlegen. Als Speicherort wählen Sie den Wechseldatenträger oder ein entsprechenden Ordner auf dem Wechseldatenträger aus (Hier Verzeichnis CRYPTDRIVE auf dem Laufwerk 'E')

Zum Schluss drücken Sie noch auf den Schalter '*Neu anlegen*'.



4. Sie werden nun gefragt, ob das Laufwerk direkt geöffnet werden Soll. Bestätigen Sie hier mit '*Ja*'.

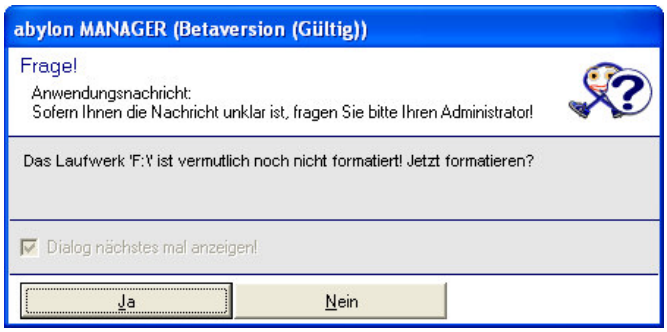
5. Je nach verwendetem Verschlüsselungs-Algorithmus (Default Encryption ALG – siehe Punkt **2**) müssen Sie nun:

- 2 mal das Passwort eingeben (SYMM-System)
- den USB-Stick oder die Chipkarte stecken (SYMM-System)
- das Zertifikatspasswort eingeben (HYBRID-System)

HINWEIS Beim HYBRID-System wird bei der Einrichtung Ihr Verschlüsselungszertifikat verwendet! Zusätzlichen Berechtigungen können im Anschluss im CERTMANAGER vergeben werden.

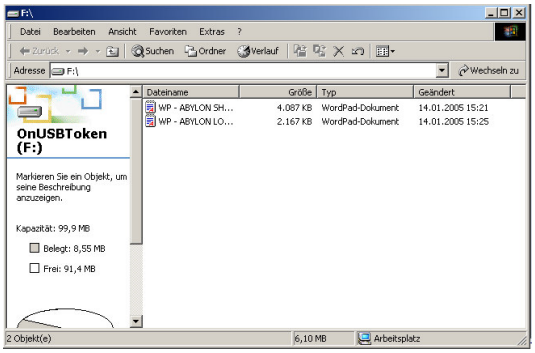
HINWEIS Je nach verwendetem CSP unterscheidet sich der Passwortdialog.

6. Die Laufwerksdateien werden nun auf der Festplatte angelegt. Zum Abschluss muss das neue virtuelle Laufwerk noch formatiert werden. Bestätigen Sie hier mit '*Ja*'.



HINWEIS Der Formatierungsvorgang kann je nach Größe des Laufwerkes einige Minuten in Anspruch nehmen. Bestehende Daten auf dem Wechseldatenträger werden NICHT überschreiben.

7. Nun kann das verschlüsselte Laufwerk wie gewohnt verwendet werden.

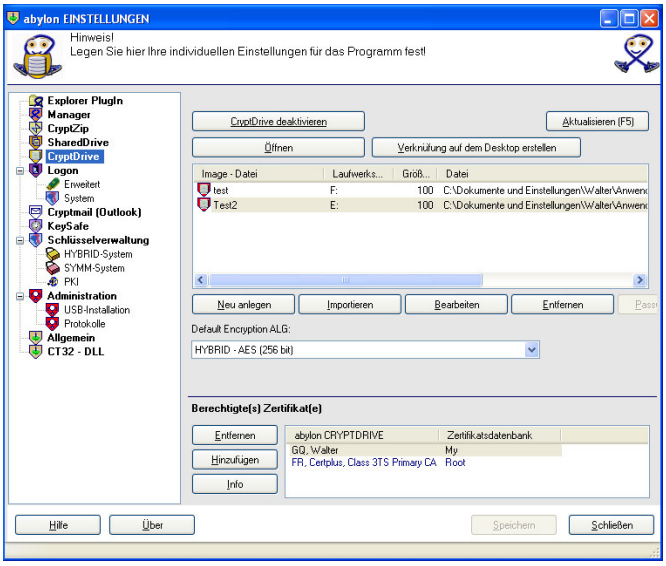


4 VERWENDEN EINES ABYLON CRYPTDRIVE (SYMM UND HYBRID-SYSTEM)

Bis auf die Passworteingabe gibt es im Einsatz des **abylon CRYPTDRIVE** zwischen dem SYMM- und HYBRID-System keinen Unterschied.

4.1 Öffnen und arbeiten mit einem abylon CRYPTDRIVE

1. Öffnen Sie im Einstellungsdialog die Seite '*CryptDrive*' und selektieren das zu öffnende Laufwerk. Zum Öffnen drücken Sie den Schalter '*Öffnen*'.

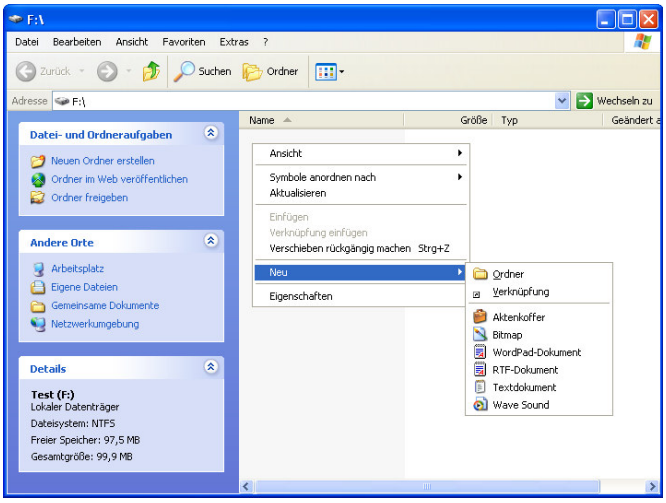


Sofern Sie Verknüpfungen für das CRYPTDRIVE angelegt haben, klicken Sie auf das Öffnen-Icon.

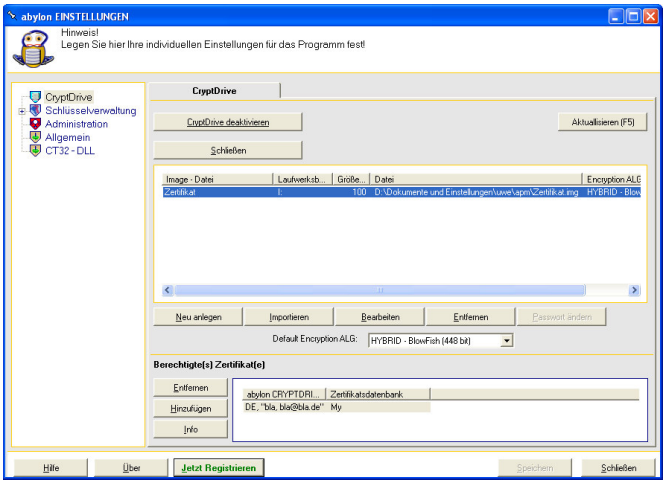
2. Sie werden nun aufgefordert, das entsprechende Passwort einzugeben oder die zugehörige Chipkarte einzulegen.

3. Danach öffnet sich ein Datei Explorer mit dem entsprechenden Laufwerk.

Wie gewohnt können Sie neue Dateien und Verzeichnisse anlegen, öffnen, kopieren und löschen oder Programme installieren.



4. Zum Abschluss sollten Sie erst alle geöffneten Dateien und dann das CRYPTDRIVE schließen. Dazu können Sie die Verknüpfung oder im Einstellungsdialog den Schalter '*Schließen*' wählen.

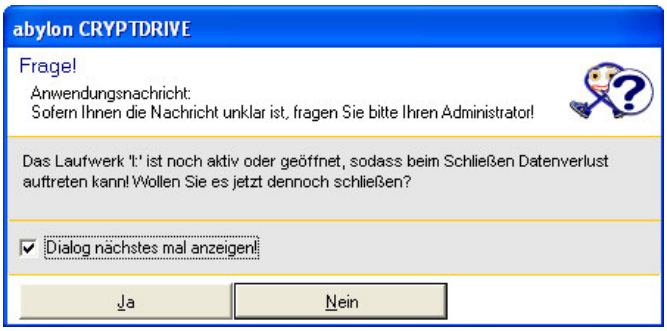


Öffnen Test

Schließen Test

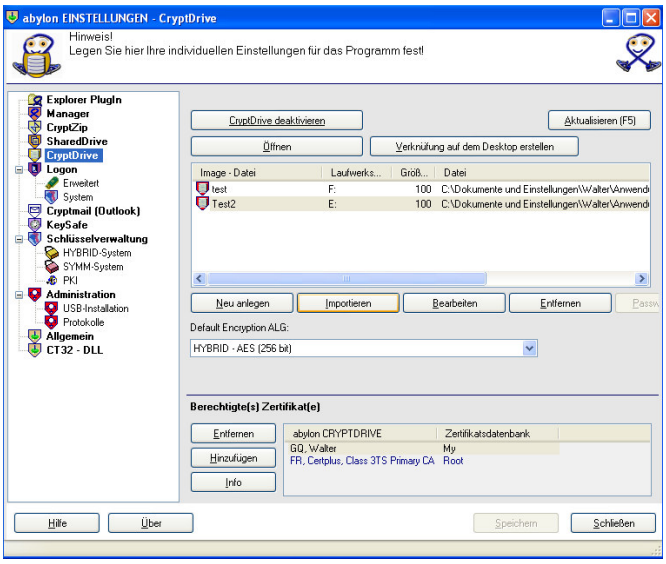
5. Sollte noch eine Datei geöffnet sein oder der Datei Explorer im Laufwerk stehen, so werden Sie mit einem Hinweisdialog darauf hingewiesen.

Sollten Sie beispielsweise eine Datei noch nicht gespeichert haben, so kann dies zum Datenverlust führen.

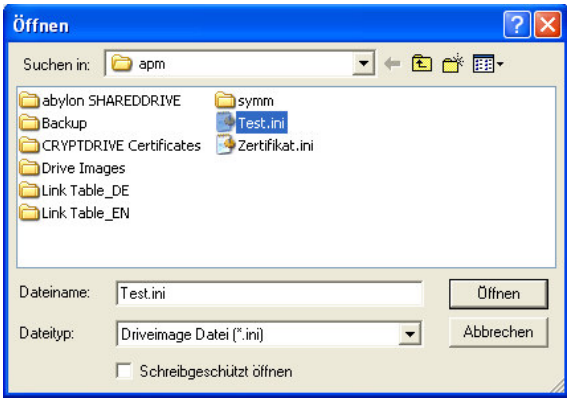


4.2 Importieren eines bestehenden abylon CRYPTDRIVE

1. Öffnen Sie im Einstellungsdialog die Seite '*CryptDrive*' und drücken Sie den Schalter '*Importieren*'.

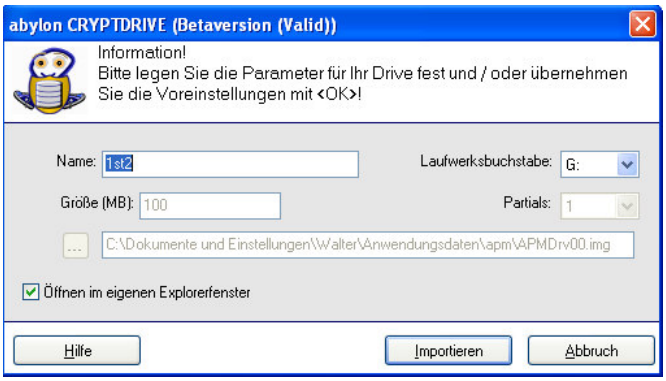


2. Wechseln Sie in das Verzeichnis, in dem CRYPTDRIVE gespeichert ist. Wählen Sie die zugehörige INI-Datei aus und bestätigen mit dem Schalter '*Öffnen*'.



3. Im Optionsdialog können Sie noch den Namen und den Laufwerksbuchstaben festlegen.

Schließen Sie die Operation mit dem Schalter '*Importieren*' ab.



4. Nun können Sie das CRYPTDRIVE direkt öffnen.

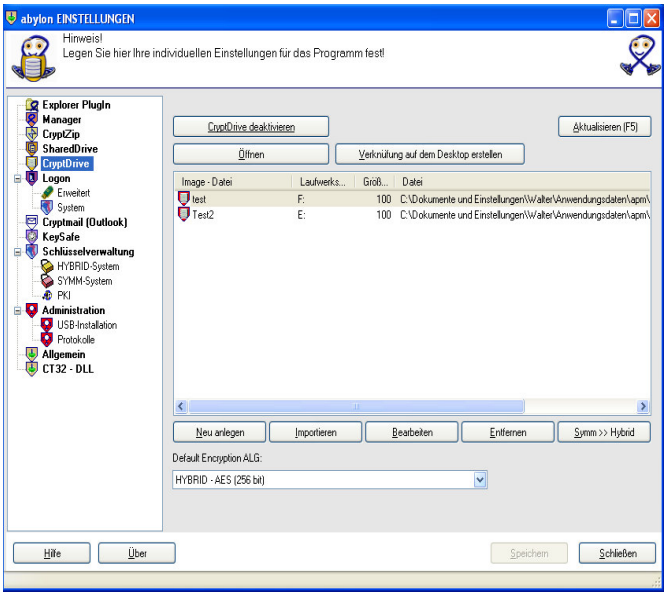
5. Sie werden nun aufgefordert, das entsprechende Passwort einzugeben oder die zugehörige Chipkarte einzulegen.

Danach können Sie das CRYPTDRIVE wie gewohnt verwenden.

In Zukunft wird das importierte CRYPTDRIVE in der Laufwerksliste aufgeführt.

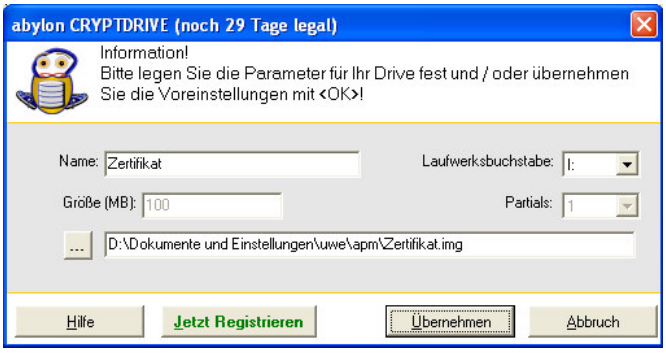
4.3 Umbenennen oder Verschieben eines abylon CRYPTDRIVE

1. Öffnen Sie im Einstellungsdialog die Seite '*CryptDrive*' und drücken Sie den Schalter '*Bearbeiten*'.



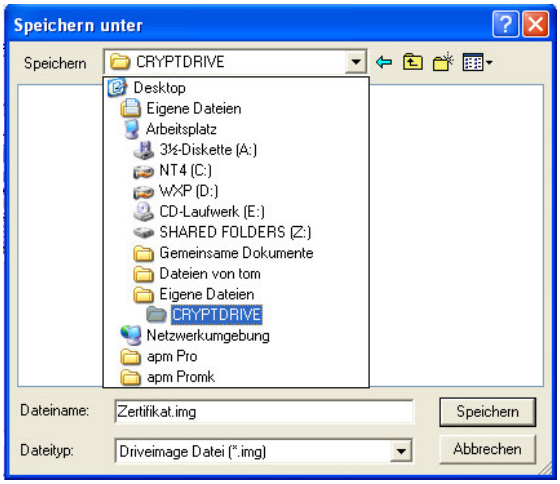
2. In dem Dialog lassen sich der '*Name*', der '*Laufwerksbuchstabe*' und der '*Speicherort*' des CRYPTDRIVE ändern.

3a. Geben Sie einfach einen neuen Namen und einen anderen Laufwerksbuchstaben ein . Zum Bestätigen drücken Sie den Schalter '*Übernehmen*'



3b. Wenn Sie das Laufwerk verschieben wollen, dann wählen mit dem Schalter '...' ein neues Verzeichnis aus und bestätigen ebenfalls mit '*Übernehmen*'.

Je nach Größe des CRYPTDRIVE kann der Verschiebevorgang mehrere Minuten in Anspruch nehmen.

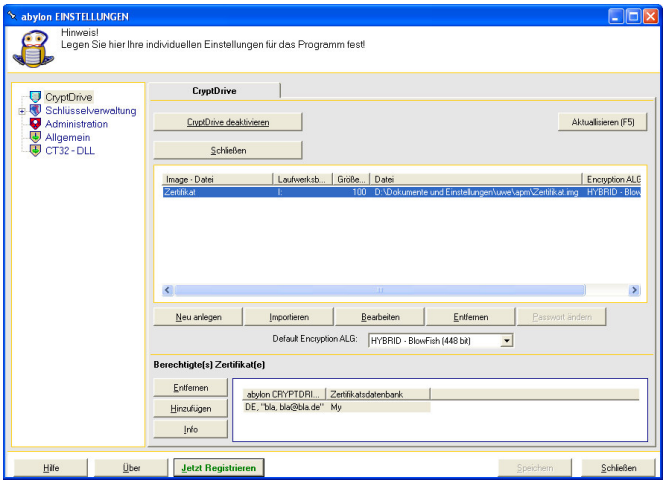


4.4 Ändern des Passwortes oder des Verschlüsselungssystems

1. Zum Ändern des Passwortes oder des Verschlüsselungssystems öffnen Sie im Einstellungsdialog die Seite '*CryptDrive*' und wählen das gewünschte CRYPTDRIVE und den neuen '*Default Encryption ALG*' aus.

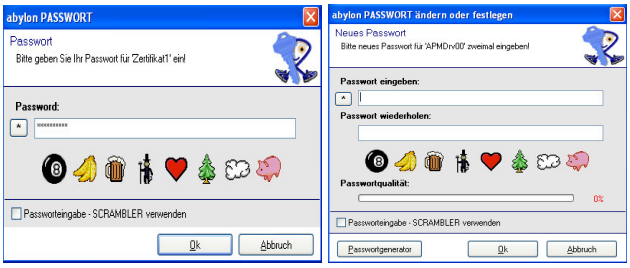
Dach drücken Sie den Schalter '*Passwort ändern*', '*Symm >> Hybrid*' oder '*Hybrid >> Symm*'.

Dabei sind folgende Änderungen möglich:



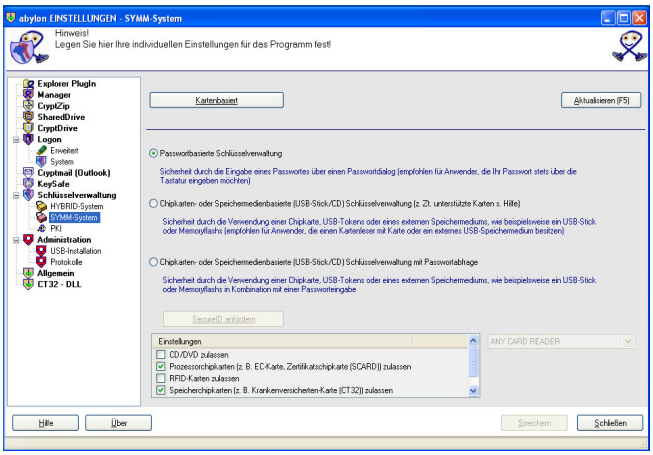
2a. Passwort ändern (Symm >> Symm):

Zum Ändern des Passwortes müssen Sie einmalig das alte Passwort und danach zweimal das neue Passwort eingeben.



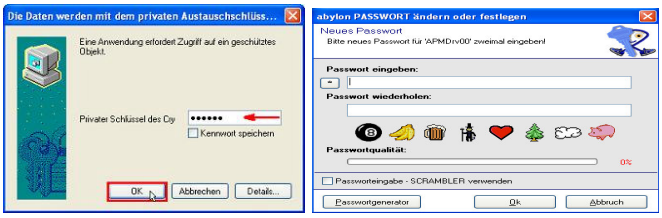
2b. Passwort ändern (Symm >> Symm):

Um die Passworteingabe zur Chipkartenverwendung oder umgekehrt zu ändern, müssen Sie vorher das neue System auf der Seite '*Schlüsselverwaltung->SYMM-System*' ändern.



2c. Verschlüsselungssystems (Symm >> Hybrid): Zum Ändern des Verschlüsselungssystems müssen Sie erst das alte Passwort und danach Ihr Zertifikatspasswort (PIN) eingeben.

2d. Verschlüsselungssystems (Hybrid >> Symm): Zum Ändern des Verschlüsselungssystems müssen Sie erst Ihr Zertifikatspasswort (PIN) und danach zweimal das neue Passwort eingeben.



HINWEIS Ein Änderung des symmetrischen Verschlüsselungssystems von AES nach Blowfish oder umgekehrt ist NICHT möglich!

5 HINWEISE

5.1 Automatisches Öffnen

Um ein **abylon CRYPTDRIVE** automatisch nach der Anmeldung zu öffnen, müssen Sie nur die Verknüpfungen auf dem Desktop erstellen und das Öffnen-Icon in den Autostartordner des Startmenu kopieren.

5.2 Automatisches Schließen

Ein automatisches Schließen geöffneter **abylon CRYPTDRIVEs** ist zur Zeit noch NICHT möglich. Verwenden Sie hierzu die erstellten Verknüpfungen (Icons) auf dem Desktop.

Geübte Administratoren können beispielsweise folgende Kommandozeile mit dem Bildschirmschoner verbinden:

"Programmpfad\APMPCaller.exe "Name CRYPTDRIVE" /UNMOUNT"

5.3 Automatisch öffnen, Freigaben zuweisen und Programme starten

Zu diesem Zweck müssen Sie eine Batch-Datei (z. B. *„startdrive.bat"*) erstellen und in den Autostart von Windows legen.

Beispiel Batch-Datei:

```
@echo off
"C:\Programme\abylonsoft\abylon\APMPCaller.EXE" "Drive1" /MOUNT
net share "Freigabeordner"="M:\Verzeichnis1"
net share m$ /delete
M:\Programme\Grafik.exe
@echo on
```

Erklärung:

2. Zeile = Automatisches Öffnen des CRYPTDRIVES mit dem Namen "Drive1"

3. Zeile = Einrichten der Freigabe von Verzeichnis 1

4. Zeile = Entfernt die administrative Freigabe auf Laufwerk "M"

5. Zeile = Automatisches Starten des Programms "Grafik.exe"

Die NTFS-Sicherheitseinstellungen können wie gewohnt einmalig im Datei Explorer über die rechte Maustaste Einstellungen->Sicherheitseinstellungen zugewiesen werden!

HINWEIS Für eine Funktionsdefinition und weitere administrative Möglichkeiten geben Sie in Start->Ausführen->CMD "net share /?", "net use /?", "net view /?" sowie "net user /?" ein oder lesen die entsprechende Windowsdokumentration!

5.4 Gleichzeitiger Zugriff durch Installation auf einem Server

Einrichtung

Zum gleichzeitigen Zugriff mehrerer Anwender auf ein verschlüsseltes **abylon CRYPTDRVE** ist eine Installation der Software auf einem Server notwendig. Dort werden die verschlüsselten Laufwerke angelegt und nach deren Öffnen einmalig die Berechtigungen (NTFS-System) vergeben. Spezielle Freigaben müssen wie in 5.3 beschrieben eingerichtet werden.

Einsatz

Nach jedem Hochfahren der Servers müssen die verschlüsselten Laufwerke geöffnet werden. Eine Automatisierung dieses Vorgangs erfolgt durch das Anlegen einer Batch-Datei im Autostart (siehe5.3). Nun kann der gleichzeitige Zugriff der einzelnen Anwender über das Netzwerk erfolgen. Die Ver- und Entschlüsselung der Daten wird auf dem Server durchgeführt, sodass die Übertragung der Dateien über das Netzwerk unverschlüsselt erfolgt.

HINWEIS Bei einer Installation des **abylon CRYPTDRVE** auf den Client und nur der Speicherung der Laufwerke auf dem Server, erfolgt die Übertragung der Dateien übers Netzwerk verschlüsselt. Jedoch ist bei diesem Einsatz KEIN gleichzeitiger Schreibzugriff mehrerer Anwender möglich.

5.5 Datenverlust vermeiden

Um Datenverlust zu vermeiden, sollten Sie alle offenen **abylon CRYPTDRIVEs** vor dem Herunterfahren des Rechners schließen!

5.6 Unterschied zwischen abylon CRYPTDRIVE und abylon SHAREDDRIVE

Virtuelles Laufwerk (abylon CRYPTDRIVE):

Beim Einrichten des virtuellen Laufwerkes wird eine Image-Datei in der Größe des Laufwerks angelegt, wobei die Image-Datei entsprechend der gewählten Anzahl der Partials aufgesplittert sein kann. In diesem Image werden alle Dateien verschlüsselt gespeichert.

Vorteile:	• Nach dem Öffnen kann das Laufwerk wie eine ganz normale Festplatte verwendet werden (Vollkommene Integration in den MS Datei Explorer) • Eine Installation von Programmen auf dem virtuellen Laufwerk ist möglich
Nachteile:	• Wird nur eine Datei leicht geändert, so muss das komplette Image gesichert werden (Großer Datentransfer und Speicherbedarf beim Backup) • Kein gleichzeitiger Schreibzugriff mehrere Anwender auf ein virtuelles Laufwerk möglich (Nur der 1. Anwender besitzt Schreib- und Leserechte)

Datenlaufwerk (abylon SHAREDDRIVE):

Beim Datenlaufwerk wird jede Datei in einer nummerierten und verschlüsselten Image-Datei gespeichert.

Vorteile:	• Jede Datei wird in einer einzelnen Image-Datei gespeichert (Bei Änderungen muss das Backup-System nur diese Datei speichern) • Gleichzeitiger Zugriff von mehreren Anwendern möglich • Speicherbedarf auf der Festplatte ist nur abhängig von der gespeicherten Datenmenge
Nachteile:	• Es können keine Programme installiert werden (reines Datenlaufwerk)

5.7 Einschränken der Anwender-Rechte

Zum Einschränken der Anwender-Rechte lesen Sie bitte das Whitepaper „Informationen zu Programmsteuerdateien und Registry für Administrative Zwecke“. Das aktuelle Dokument finden Sie auf unserer Homepage im Download-Bereich: http://www.abylonsoft.de/cryptdrive/download.htm

5.8 Weitere Dokumente und FAQs

Weitere Dokumente und FAQs (Frequently Asked Questions) finden Sie auf unserer Homepage im Support-Bereich: http://www.abylonsoft.de/cryptdrive/support.htm