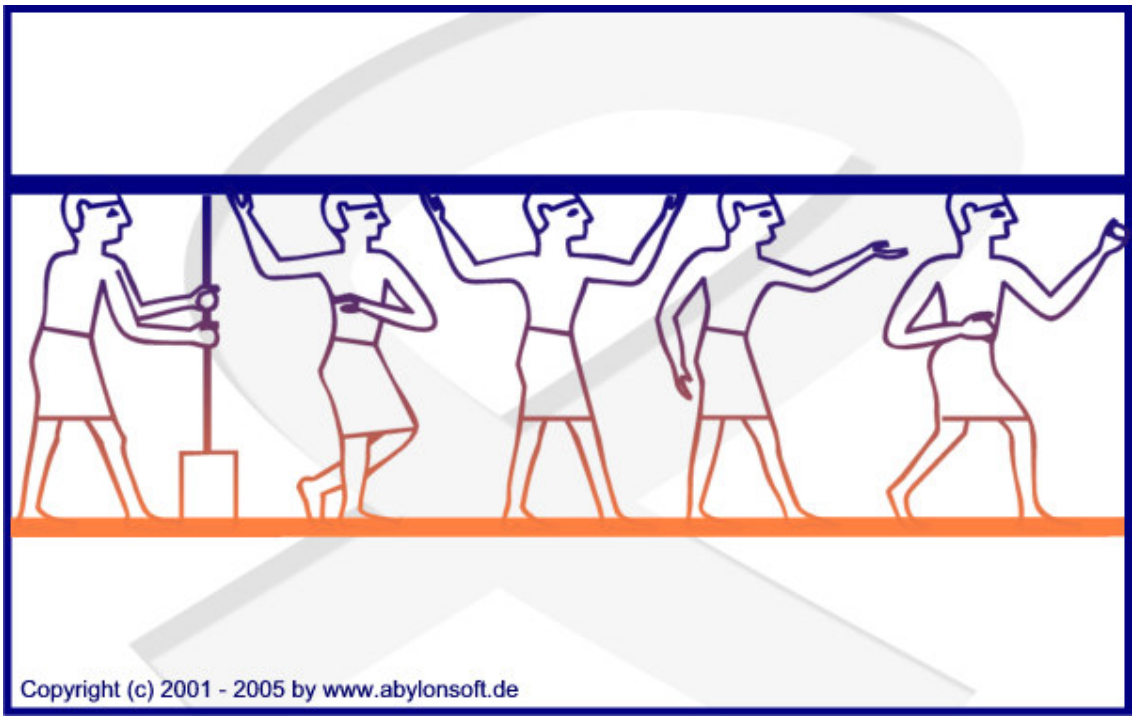
WITHEPAPER - ANLEGEN UND VERWENDEN EINES ABYLON SHAREDDRIVE

ABYLONSOFT – DR. KLABUNDE



Softwareentwicklung, Beratung und Verkauf von IT-Sicherheitssoftware

Revision 2.00

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: 24.06.2008

HISTORIE

Version	Datum	Kommentar
1.0	16.10.2005	Dokument neu erstellt
2.0	23.06.2008	Dokument entsprechend Version 7 angepasst (WB)
2.1	12.07.2008	Hinweise ergänzt (TK)

.

INHALTSVERZEICHNIS

1 CONTENT

Dieses Whitepaper beschreibt Ihnen die Funktionsweise und die Verwendung des Softwareproduktes **abylon SHAREDDRIVE**. Anhand von Anwendungsbeispielen wird der Einsatz beschrieben und die Technik hinter dem Produkt erklärt.

2 FUNKTIONSWEISE DES ABYLON SHAREDDRIVE

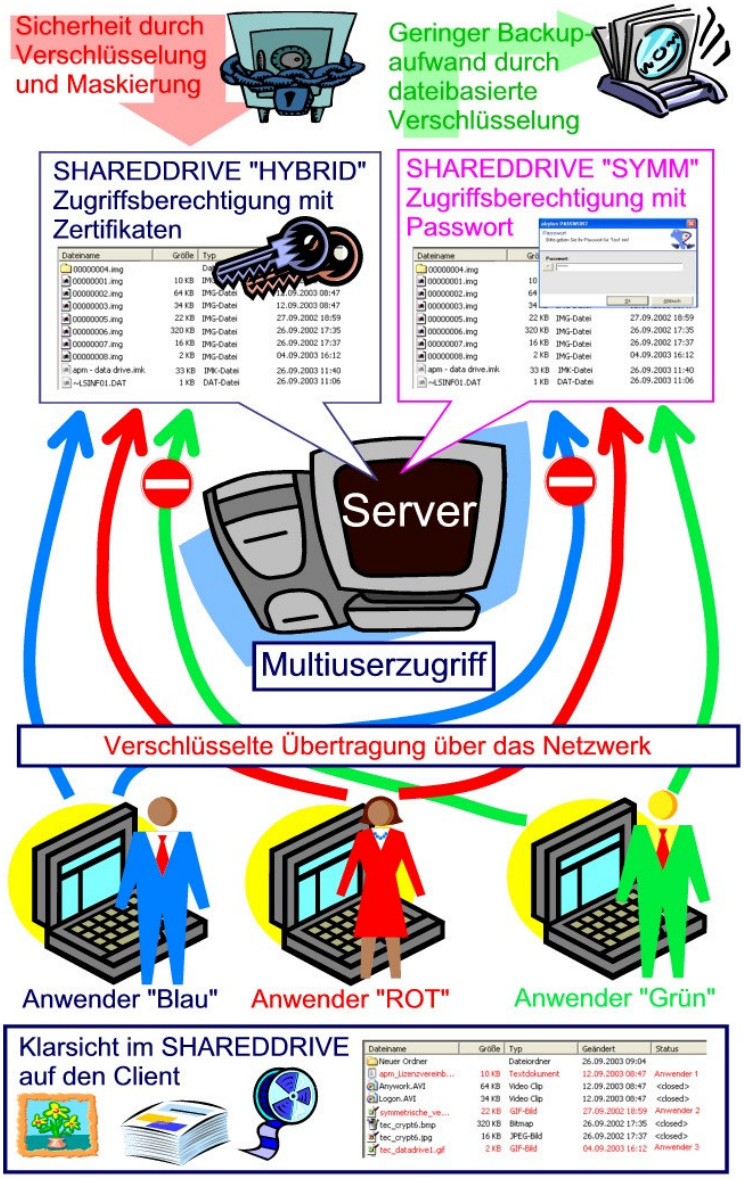
2.1 Programmbeschreibung und Funktionsumfang

Das **abylon SHAREDDRIVE** (verschlüsseltes Datenlaufwerk) integriert sich vollständig in den MS Datei Explorer und wird dort als eigenständiges Laufwerk angezeigt. Dabei werden die allgemeinen Funktionen des Datei Explorers unterstützt, wie beispielsweise Kopieren, Einfügen und Öffnen. Die Dateien werden beim Speichern auf das Datenlaufwerk immer verschlüsselt abgelegt (Blowfish - 448 Bit / AES - 256 Bit), ohne das der Anwender eine zusätzliche Operation ausführen muss. Der Speicherort der verschlüsselten Dateien im Basisverzeichnis kann auf dem lokalen Rechner oder einem Netzwerkrechner liegen. Die Übertragung der Daten vom Server über das Netzwerk erfolgt verschlüsselt und die Entschlüsselung wird erst auf dem Client durchgeführt. Die Zugriffsberechtigungen der einzelnen Datenlaufwerke wird durch die Vergabe eines Passwortes (SYMM-System) oder durch die Zuweisung von X.509 Zertifikaten (HYBRID-System, PKCS, RSA) geregelt. Der dateibasierte Aufbau ermöglicht den gleichzeitigen Zugriff von mehreren Anwendern. Eine zusätzliche Sicherheit bietet die Verschleierung der Originaldateinamen durch zufällige Nummern. Nur berechtigte Personen bekommen den Originaldateinamen im Datei Explorer angezeigt. Zudem ist das **abylon SHAREDDRIVE** besonders sicher bei Computerabstürzen. Es werden immer nur die wirklich benötigten Dateien geöffnet und alle weiteren Dateien bleiben unangetastet und verschlüsselt auf der Festplatte gespeichert. Dadurch wird der mögliche Datenverlust auf ein Minimum reduziert. Nach dem Neustart des Rechners wird zusätzlich das Temporärverzeichnis gründlich gereinigt. Durch die individuelle Verschlüsselung und Speicherung jeder einzelnen Datei besitzt das **abylon SHAREDDRIVE** besonders bei der Sicherung der Daten durch Backupsysteme große Vorteile. Im Gegensatz zu verschlüsselten Laufwerken auf Image-Basis müssen nur geänderte Daten gesichert werden, wodurch das Datentransfervolumen und der benötigten Speicherplatz stark reduziert werden.

- Automatische Verschlüsselung von Daten

- Verschlüsselung mit dem Blowfish- (448 Bit) oder AES-Algorithmus (256 Bit)
- Unterstützung der asymmetrischen (HYBRID-System) und symmetrische Verschlüsselung (SYMM-System)
- Beim SYMM-System erfolgt die Zugriffsberechtigung über ein Passwort oder eine EC-/KV-Karte
- Beim HYBRID-System erfolgt die Zugriffsberechtigung individuell durch die Zuweisung von X.509-Zertifikaten (Chipkarten- und USB-Tokenunterstützung)
- Integration in den MS Datei Explorer auf der Ebene des Desktop
- Der Speicherort des Basisverzeichnisses kann auf dem lokalen Rechner oder einem Netzwerkrechner liegen
- Pro Rechner können mehrere SHAREDDRIVEs eingerichtet werden
- Daten werden vom Server immer verschlüsselt über das Netzwerk übertragen und erst auf dem Client entschlüsselt
- KEINE spezielle Software auf dem Server notwendig
- Jede Datei wir als verschlüsselte Image Datei gespeichert
- Der Originaldateiname wird mit einer zufälligen Nummer maskiert, sodass kein Rückschluss auf Art und Inhalt der Datei geschlossen werden kann
- Mehrere Anwender können gleichzeitig auf ein SHAREDDRIVE zugreifen
- Anzeige von geöffneten Dateien
- Speicherbedarf nur Abhängig von der Größe der Dateien
- Maximale Größe nur Abhängig von des Festplattenbegrenzung
- Absturzsicherung: Entschlüsselung nur der benötigten Dateien und Säuberung des Temporärverzeichnisses nach dem Neustart
- Geringer Backupaufwand durch die individuelle Verschlüsselung und Speicherung jeder einzelnen Datei

2.2 Funktionsweise



Das **abylon SHAREDDRIVE** schütz Ihre vertraulichen Daten vor unerlaubten Zugriff durch Verschlüsselung (Blowfish- (448 Bit) oder AES-Algorithmus (256 Bit)). Jede einzelne Datei wird maskiert und individuell verschlüsselt im SHAREDDRIVE gespeichert. Der Speicherort der verschlüsselten Dateien kann sich auf dem lokalen Client oder einem Server befinden. Die Übertrag der Daten über das Netzwerk erfolgt immer verschlüsselt und erst auf dem Client werden die Daten entschlüsselt. Die maskierten Namen der gespeicherten Dateien werden erst auf dem Client im SHAREDDRIVE aufgelöst, sodass nur berechtigte Personen die Dateinamen und Inhalte angezeigt bekommen. Bei jeder Datei-Operation erfolgt die Ver- und Entschlüsselung automatisch im Hintergrund. Durch den dateibasierten Aufbau können gleichzeitig mehrere Anwender auf das selbe SHAREDDRIVE zugreifen.

Die Zugriffsberechtigung auf die einzelnen SHAREDDRIVE erfolgt durch Passworteingabe oder mittels Chipkarte (SYMM-System). Im professionellen Umfeld können für die Zugriffsberechtigung auch Zertifikate eingesetzt werden (HYBRID-System). Hierbei werden eine Vielzahl handelsüblicher Zertifikatschipkarten und Token unterstützt.

3 ANLEGEN UND ADMINISTRIEREN EINES NEUEN ABYLON SHAREDDRIVE

3.1 Anlegen eines SYMM-System SHAREDDRIVE mit Passworteingabe oder Chipkarte

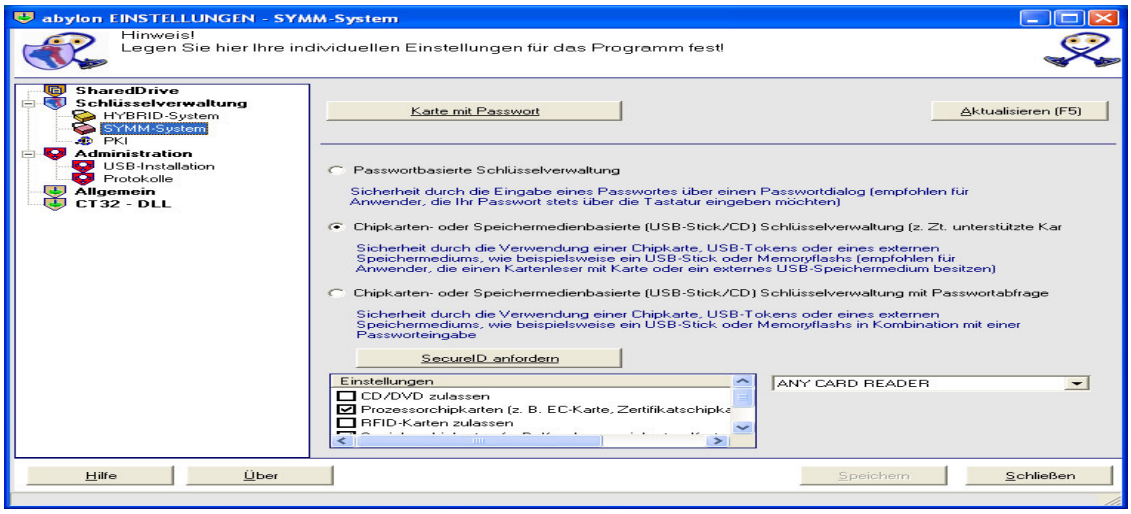
Anleitung zum Anlegen eines **abylon SHAREDDRIVE** unter Verwendung des SYMM-System. Hierbei wird die Passworteingabe oder die Verwendung von Chipkarten (z. B. EC-Karte) unterstützt und als Verschlüsselungsalgorithmus AES (Schlüssellänge 256 Bit) und Blowfish (Schlüssellänge 448 Bit) eingesetzt.

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*'

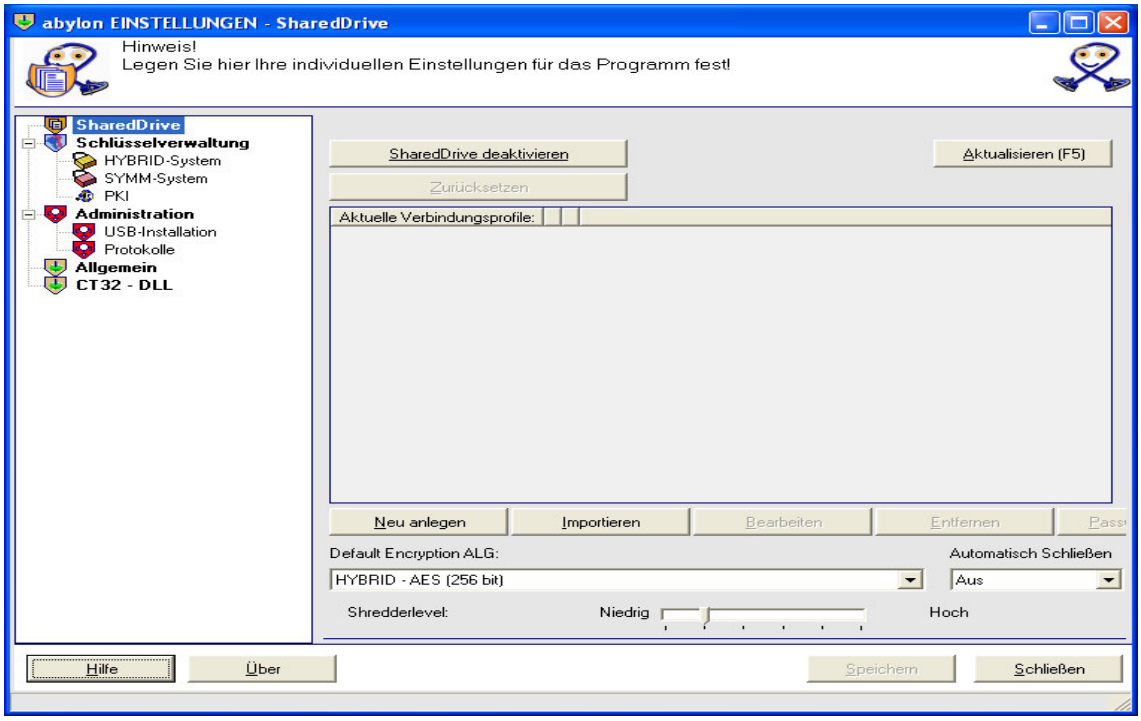
Hier können Sie folgende Optionen selektieren:

- **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).
- **Chipkarten- oder Speichermedienbasierte (USB-Stick) Schlüsselverwaltung:** Beim SYMM-System erfolgt die Sicherheit (Verschlüsselung oder Zugriffskontrolle) durch die Verwendung einer Chipkarte, USB-Tokens, 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-Tokens, 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 '*SharedDrive*' und wählen einen der folgenden '*Default Encryption ALG*' aus:

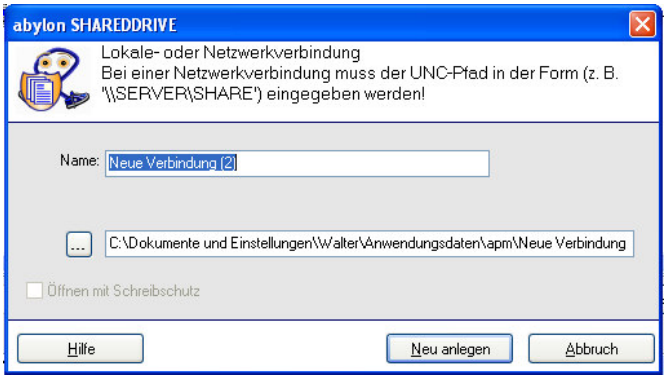
- **SYMM-AES:** Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit).
- **SYMM-AES 4Eye-System:** Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit). Beim Vieraugensystem (4Eye-System) müssen hintereinander 2 Passwörter eingegeben werden.
- **SYMM-Blowfish:** Passwortbasierte symmetrische Verschlüsselung mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).
- **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 448 Bit) und anschließend mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).
- **SYMM-AES & Blowfish 4Eye-System:** Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 448 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 SHAREDRIVE
- **Speicherort**: Verzeichnis und Dateiname, unter dem das SHAREDRIVE auf der Festplatte gespeichert sein wird



5. Beim '*Neu anlegen*' müssen je nach Einstellung auf der Seite '*Schlüsselverwaltung->SYMM-System*' nun

- **2 mal das gewünschte Passwort eingeben**

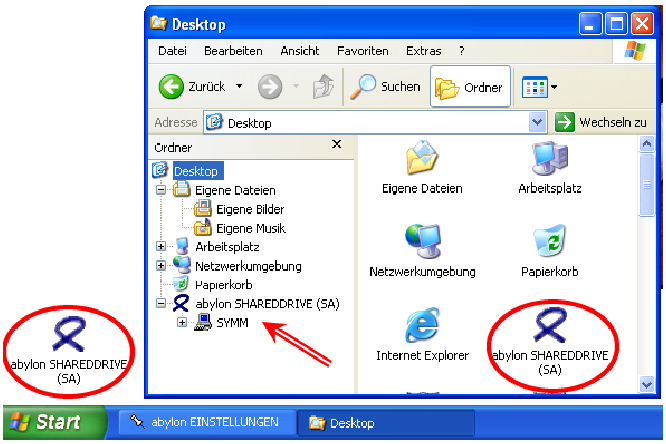
oder

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

oder

6. Das neue SHAREDDRIVE wird über den Desktop oder den Datei Explorer geöffnet. Klicken Sie dazu auf den Verweis abylon SHAREDDRIVE (Schleife) oder selektieren diesen im Datei Explorer. Hier werden alle eingerichteten SHAREDDRIVEs angezeigt.

HINWEIS Sollte das SHAREDDRIVE (Schleife) nicht angezeigt werden, wechseln Sie auf den Desktop oder in den Datei Explorer und drücken einmalig **F5** auf Ihrer Tastatur)



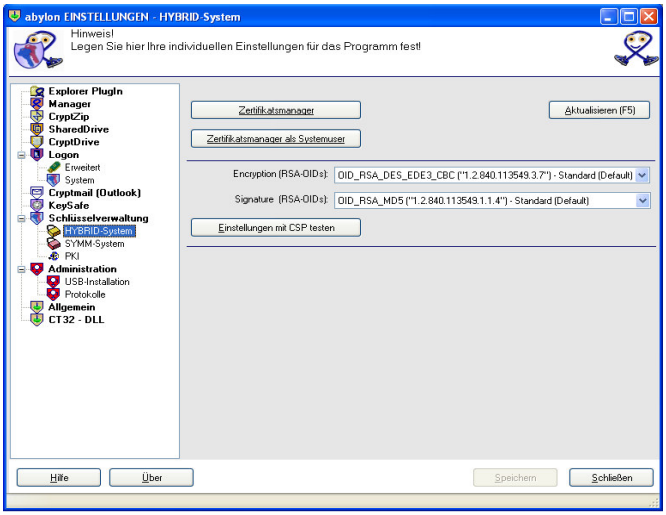
3.2 Anlegen eines HYBRID-System SHAREDDRIVE mit Zertifikaten

Anleitung zum Anlegen eines **abylon SHAREDDRIVE** 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.

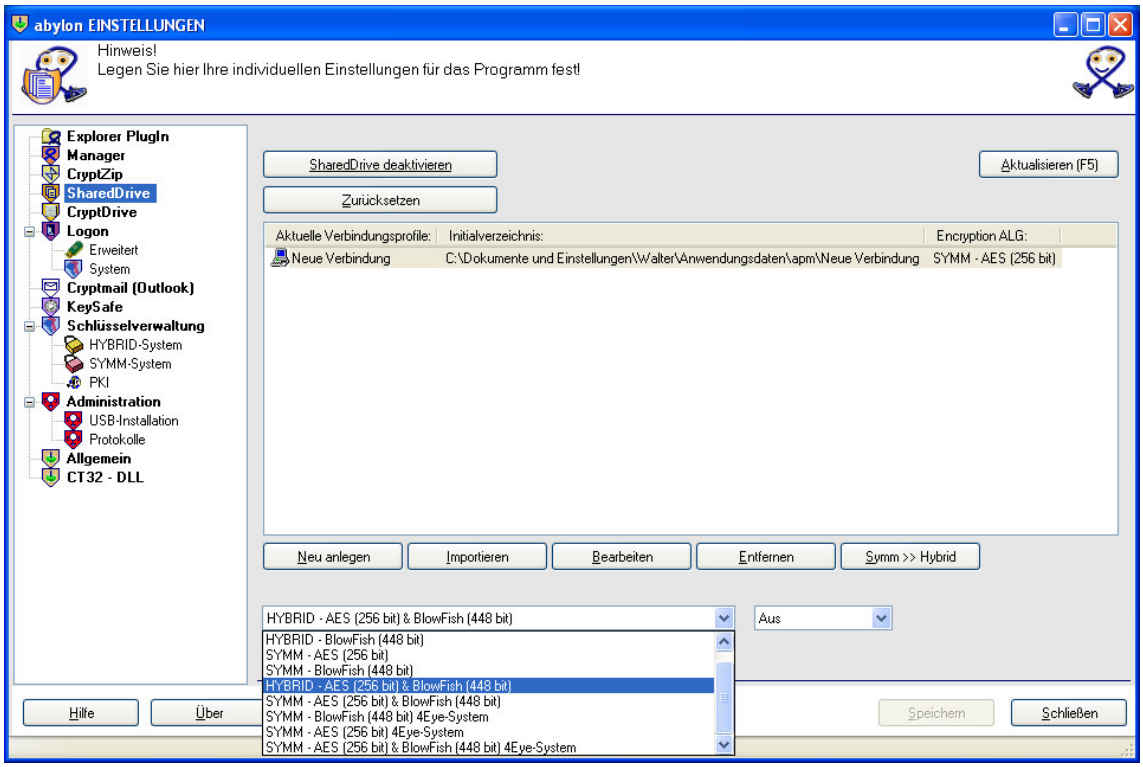
1. Falls noch nicht erfolgt, müssen Sie zuerst Ihr eigenes Signatur- und Verschlüsselungszertifikat festlegen. Öffnen Sie hierzu den Einstellungsdialog und wechseln auf die Seite '*Schlüsselverwaltung->HYBRID-System*'

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



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

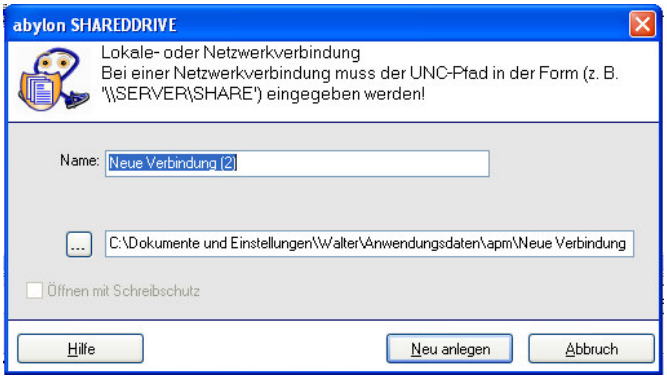
- **HYBRID – AES (256 bit)**: Die Authentifizierung zum Öffnen des Laufwerkes erfolgt mit Zertifikaten und das Laufwerk wird mit dem symmetrischen Verschlüsselungsverfahren AES und einer Schlüssellänge von 256 Bit verschlüsselt.
- **HYBRID – Blowfish (448 bit)**: Die Authentifizierung zum Öffnen des 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 SHAREDRIVE
- **Speicherort**: Verzeichnis und Dateiname, unter dem das SHAREDRIVE auf der Festplatte gespeichert sein wird



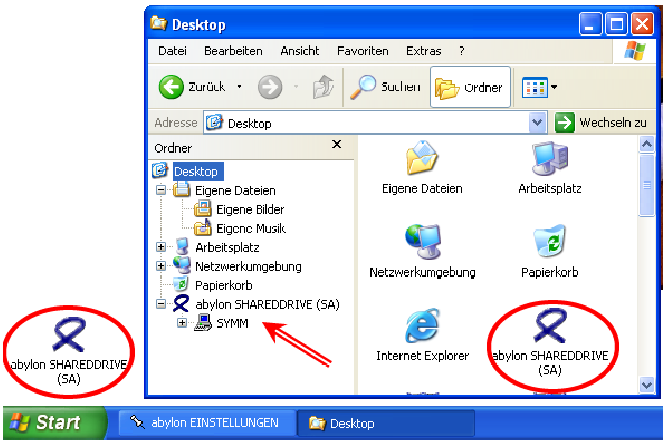
Zum Abschließen drücken Sie den Schalter '*Neu anlegen*'.

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

HINWEIS Je nach verwendetem CSP unterscheidet sich der Passwortdialog.

6. Das neue SHAREDDRIVE wird über den Desktop oder den Datei Explorer geöffnet. Klicken Sie dazu auf den Verweis abylon SHAREDDRIVE (Schleife) oder selektieren diesen im Datei Explorer. Hier werden alle eingerichteten SHAREDDRIVEs angezeigt.

HINWEIS Sollte das SHAREDDRIVE (Schleife) nicht angezeigt werden, wechseln Sie auf den Desktop oder in den Datei Explorer und drücken einmalig **F5** auf Ihrer Tastatur)

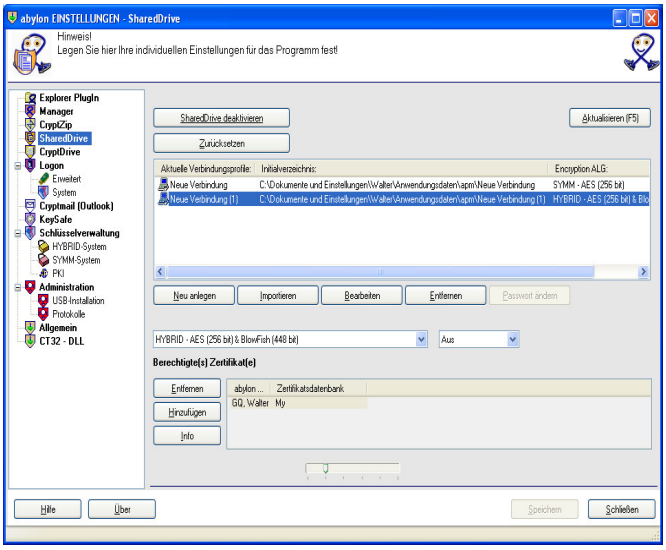


3.3 Administrieren eines HYBRID-System SHAREDDRIVE mit Zertifikaten

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

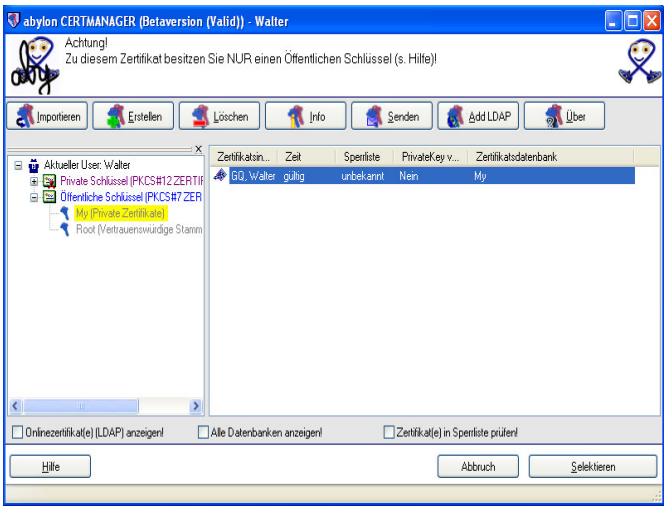
Dies ermöglicht eine einfache und zentrale Administration. Um in Zukunft beispielsweise einem Mitarbeiter den Zugriff auf das SHAREDDRIVE zu verwehren, braucht nur das entsprechende Zertifikat gelöscht werden.

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 '*SharedDrive*' 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.

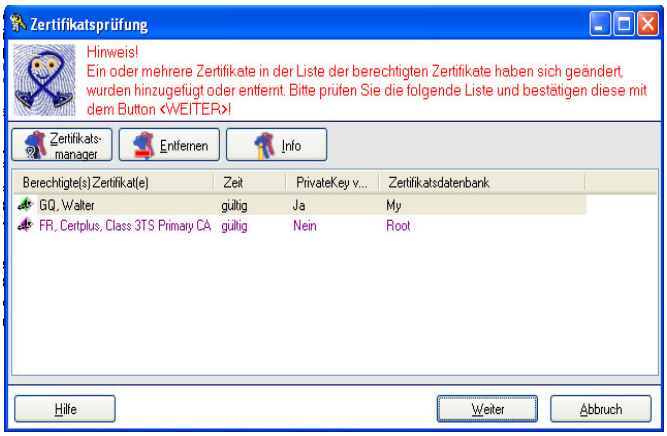
3. Die Änderungen der Zugriffs-berechtigungen müssen Sie durch Eingabe des Passwortes (PIN) bestätigen.

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

4. Beim nächsten Öffnen des SHAREDDRIVE 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*'!

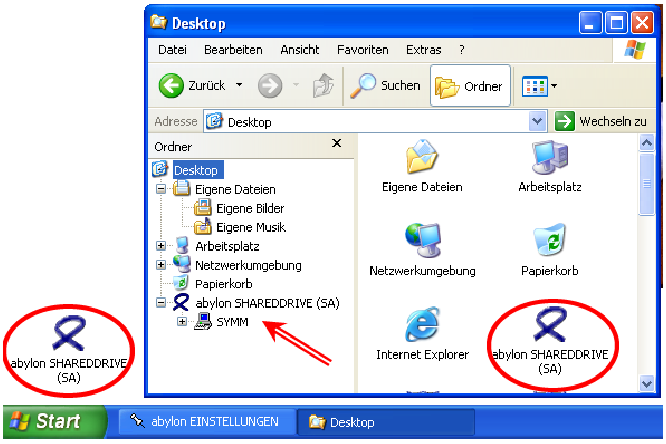
4 VERWENDEN EINES ABYLON SHAREDDRIVE (SYMM UND HYBRID-SYSTEM)

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

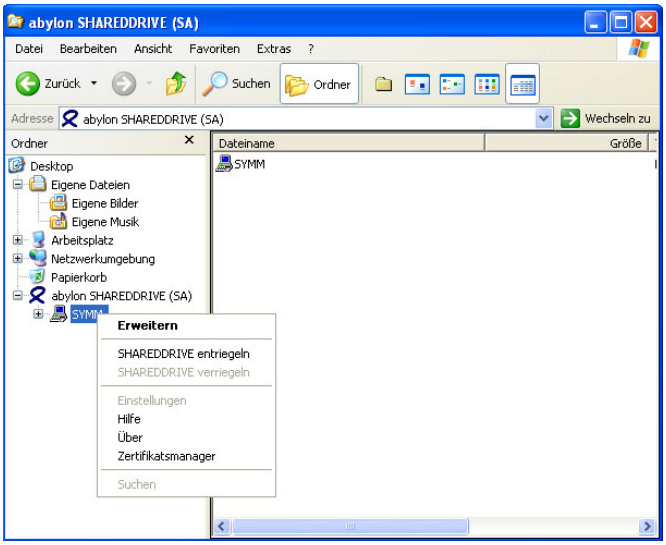
4.1 Öffnen und arbeiten mit einem abylon SHAREDDRIVE

1. Das SHAREDDRIVE wird über den Desktop oder den Datei Explorer geöffnet. Klicken Sie dazu auf den Verweis abylon SHAREDDRIVE (Schleife) oder selektieren diesen im Datei Explorer. Hier werden alle eingerichteten SHAREDDRIVEs angezeigt.

HINWEIS Sollte das SHAREDDRIVE (Schleife) nicht angezeigt werden, wechseln Sie auf den Desktop oder in den Datei Explorer und drücken einmalig **F5** auf Ihrer Tastatur)



2. Das SHAREDDRIVE wird über das Menu (Rechte Maustaste) oder durch Klicken entriegelt.

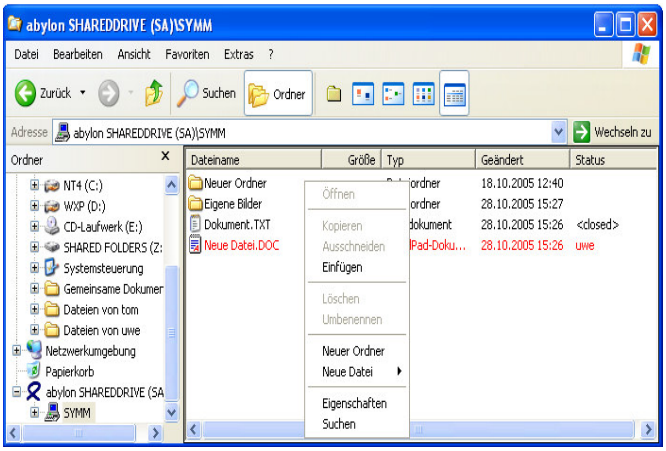


3. Je nach Verschlüsselungssystem und verwendetes Geheimnis müssen Sie nun

- **Ihr Passwort eingeben**
- **die Chipkarte in den Kartenleser einlegen**
- **den USB-Stick stecken**
- **die PIN zu Ihrem Zertifikat eingeben**

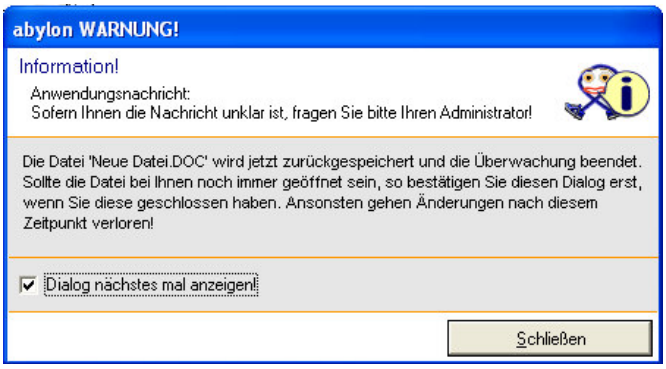
4. Nun können Sie wie gewohnt arbeiten, Dateien anlegen, kopieren, öffnen oder löschen. Dabei erfolgt die Ver- und Entschlüsselung im Hintergrund und ohne merklich Zeitverzögerung.

Geöffnete Dateien werden rot markiert, sodass weitere Nutzer dies angezeigt bekommen. Sollte dennoch eine Datei durch zwei Anwender geändert werden, so wird automatisch eine Kopie von der Datei angelegt, sodass keine Daten verloren gehen.



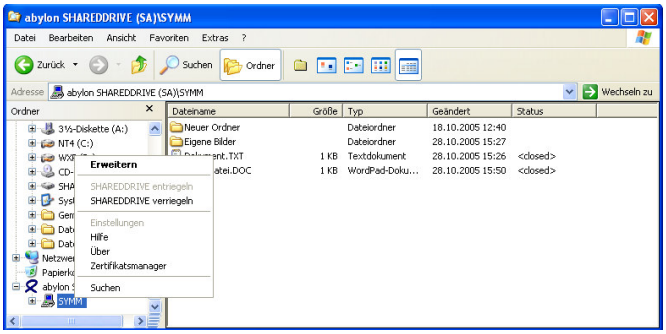
5. Beim Speichern eines Dokumentes wird diese automatisch Verschlüsselt und in SHAREDDRIVE zurück kopiert.

Beim Schließen des Dokuments zeigt Ihnen ein Dialog die Beendigung der Dateiüberwachung an.



6. Das SHAREDDRIVE wird über das Menu (Rechte Maustaste) wieder verriegelt.

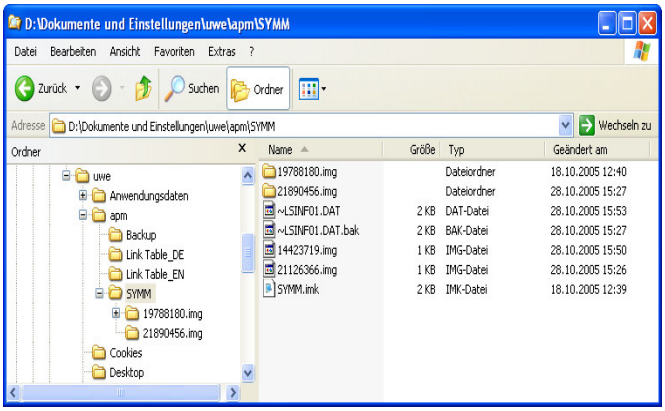
HINWEIS Das automatische Schließen der SHAREDDRIVEs nach einer gewissen Zeit der Nichtbenutzung ist über den Einstellungsdialog möglich!



7. In den Einstellungen festgelegten Initialverzeichnis werden alle Dateien und Ordner als verschlüsselte und maskierte IMG-Dateien gespeichert.

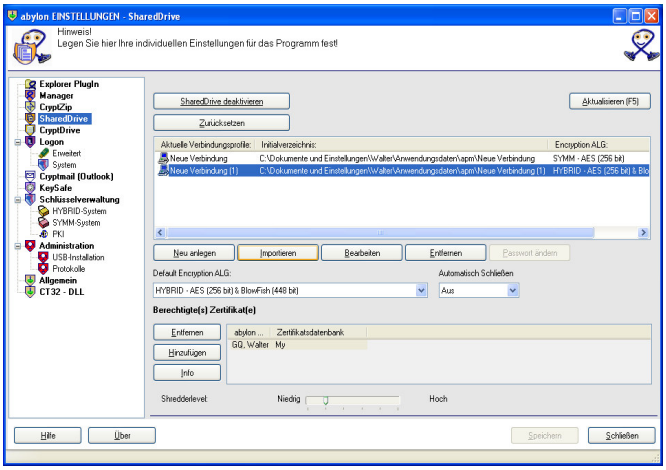
Diese Dateien können sich auf dem lokalen Client oder einem Netzwerkrechner befinden!

HINWEIS Beim Backup müssen auch die IMK-Datei (Einstellungs- und Schlüsseldatei) und die DAT-Datei (Zuordnungstabelle) gesichert werden!

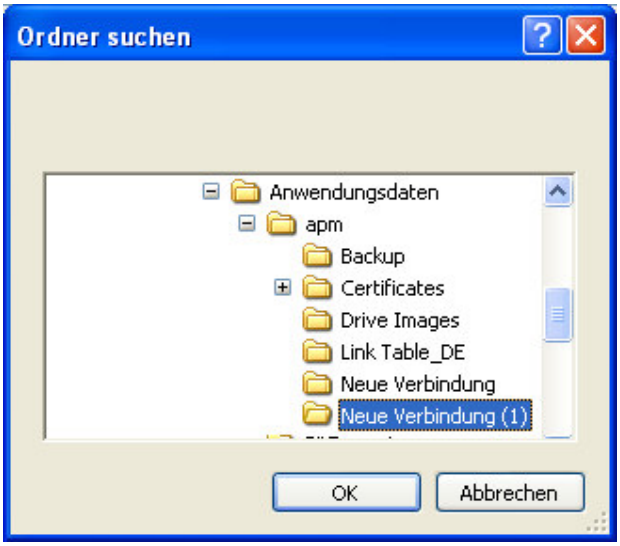


4.2 Importieren eines bestehenden abylon SHAREDDRIVE

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

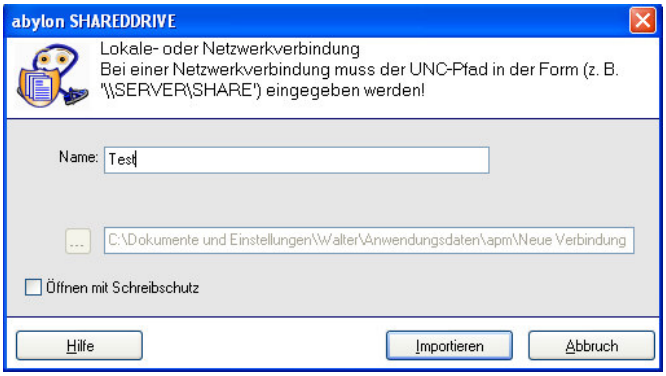


2. Wechseln Sie in das Verzeichnis, in dem SHAREDDRIVE gespeichert ist. Wählen Sie das zugehörige Verzeichnis aus und bestätigen mit dem Schalter '*OK*'.



3. Im Optionsdialog können Sie noch den Namen festlegen.

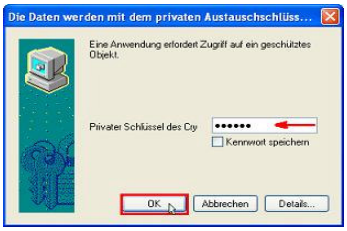
Schließen Sie die Operation mit dem Schalter '*Importieren*' ab.



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

Danach können Sie das SHAREDDRIVE wie gewohnt verwenden.

In Zukunft wird das importierte SHAREDDRIVE im Einstellungsdialog aufgeführt.

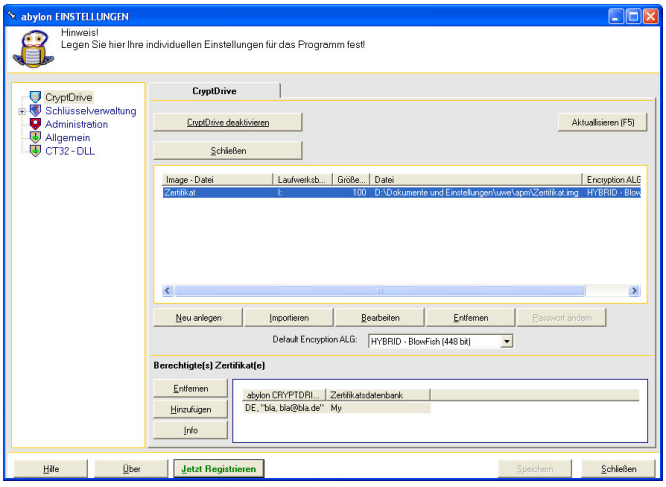


4.3 Ändern des Passwortes oder des Verschlüsselungssystems

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

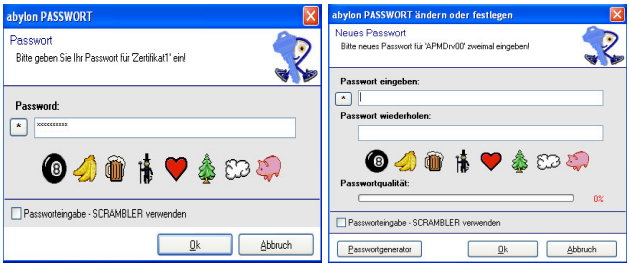
Dach drücken Sie den Schalter '*Passwort ändern*', '*Symm >> Hybrid*' oder '*Hybrid >> Symm*'.

Dabei sind folgende Änderungen möglich:



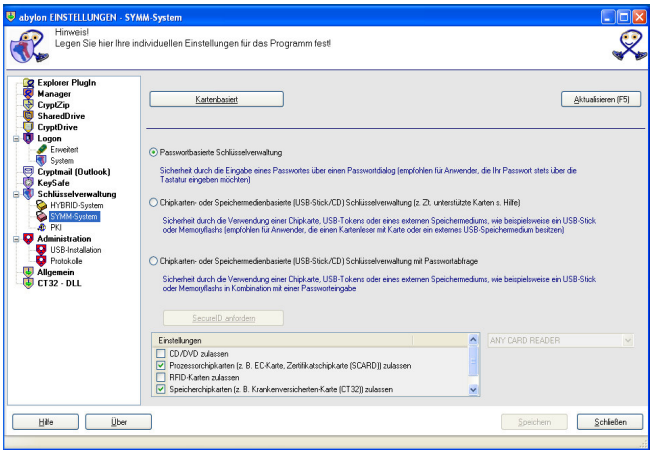
2a. Passwort ändern (Symm >> Symm):

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 Aktualisierung des Datei Explorer mit F5

Bei länger Operationen (z. B. bei großen Dateien) kann es vorkommen, dass die Anzeige des Datei Explorer nicht aktualisiert wird.

Mit der **Taste F5** erzwingen Sie die Aktualisierung der Anzeige des Datei Explorer.

5.2 Zugriff nicht möglich (Datei Explorer grau hinterlegt) Ansichtsprobleme!

Bei allen Dateioperationen im **abylon SHAREDDRIVE** wird das aktuelle Verzeichnis für jeden weiteren Zugriff gesperrt (grau hinterlegt!). Beispielsweise bei einem Absturz wird diese Sperre nicht mehr zurück gesetzt. Mit der **Taste F10** oder im Einstellungsdialog mit dem Schalter '*Zurücksetzen*' wird diese Sperre aufgehoben werden.

5.3 Automatisches Schließen

Im Einstellungsdialog kann eine Zeit festgelegt werden, nach der das SHAREDDRIVE bei Nichtbenutzung geschlossen wird.

5.4 Automatisches Öffnen

Ein automatisches Öffnen des **abylon CRYPTDRIVE** nach dem Verbinden des Wechseldatenträgers mit dem Rechner ist zur Zeit noch NICHT möglich.

5.5 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)

5.6 Verwendung des CD- oder DVD-Laufwerks als SHAREDDRIVE

Hierzu gehen sie wie folgt vor:

1. Einrichten eines SHAREDDRIVE

2. Kopieren der Daten ins Datenlaufwerk im Datei Explorer

3. Brennen der kompletten Dateien des SHAREDDRIVE auf CD oder DVD unter Verwendung eines entsprechenden Brennprogramms (inkl. der IMK-Einstellungsdatei)

4. Einrichten einer neuen Verbindung mit dem entsprechenden Initialverzeichnis auf CD oder DVD (Beachten Sie die Verzeichnisstruktur!)

Nun ist der Zugriff aus dem Datei Explorer auf die verschlüsselten Daten der CD oder DVD möglich und nur im entsprechenden SHAREDDRIVE werden die Dateien nicht maskiert angezeigt.

HINWEIS Bei der neuen Verbindung ist der Profilname unabhängig vom Namen der IMK-Datei und kann frei gewählt werden!

5.7 Weiter Optionen

Weiter Optionen/Einstellungsmöglichkeiten neben dem Einstallungsdialog:

- **Über die UserConfig.XML:**

Unsere Software bietet über eine sogenannte User-Config-Datei einige Möglichkeiten die Rechte für den Anwender zu beschränken. Eine Übersicht über die möglichen Optionen sind in der In der Datei "*Informationen zu Programmsteuerdateien und Registry für Administrative Zwecke*" zusammengestellt. (siehe Download-Seite unter Withepapers: http://www.abylonsoft.de/shareddrive/download.htm)

- **Über die Registry**

Zusätzlich sind folgende Einstellungen in der Registry unter '*HKLM/Software/abylon/SHAREDDRIVE/SHAREDDRIVE*' möglich:

- **TimeOut** = "**0**" (DEFAULT) oder "**n**" (Sekunden, nach denen das SHAREDDRIVE automatisch geschlossen wird)!
  Der Wert 180 bedeutet, dass das SHAREDDRIVE nach 3 Minuten Nichtbenutzung geschlossen wird. Die Prozessüberwachung läuft bei geöffneten Dateien weiter, sodass Änderungen auch nach dem Schließen des SHAREDDRIVE übernommen werden.
- **CallExtern** = "NO" (DEFAULT) oder "YES"
  NO = Prozessüberwachung im Thread des Datei Explorer! Sollte der Datei Explorer abstürzen, so wird auch die Prozessüberwachung geschlossen. Falls der Anwender in diesem Fall die Daten nicht manuell speichert, kann es zu Datenverlust führen. Diese Situation sollte in der Regel nicht vorkommen! DIESE OPTION WIRD VOM ENTWICKLER EMPFOHLEN!
  YES = Prozessüberwachung als eigener Thread! Sollte der Datei Explorer abstürzen, so läuft die Prozessüberwachung weiter. Allerdings ist mit dieser Option der Funktionsaufruf deutlich langsamer und es wird mehr RAM-Speicher benötigt!
- **ExecuteViaProcess** = "NO" (DEFAULT) oder "YES"
  NO = Prozessaufruf über ShellExecute! ShellExecute ist das von Microsoft propagierte Werkzeug, dass jedoch auch einige Bugs beinhaltet. Sollte es Probleme bei der Dateiüberwachung geben, so kann hiermit auf CreateProzess umgestellt werden! DIESE OPTION WIRD VOM ENTWICKLER EMPFOHLEN!
  YES = Prozessaufruf über CreateProcess! Läuft sehr zuverlässig, ist jedoch nicht bis ins letzte Detail getestet!
- **WaitForOffice** = "NO" (DEFAULT) oder "YES"
  Dieser Wert sollte immer auf "NO" stehen! Nur wenn im Datei Explorer Probleme beim Zurücksetzen des Dateistatus auftreten kann evtl. die Option "YES" Abhilfe schaffen!
- **DDRIVEOPT** sollte immer auf "4" stehen!

5.8 Dateinamen werden nicht mehr angezeigt

Wenn im SHAREDDRIVE nur noch nummern mit der IMG-Dateierweiterung angezeigt werden, dann ist die Zuordnung zwischen Datei und Dateiname verloren gegangen. Dies kann beispielsweise bei einem Systemabsturz passieren oder wenn beim Zurückkopieren eines Backups nicht die DAT-Datei gesichert wurde. Durch dieses Anzeigeproblem ist jedoch NICHT der Dateiinhalt verloren. Zur Wiederherstellung gehen Sie wie folgt vor:

1. Kopieren der unbekannten Datei aus dem SHAREDDRIVE in eine unverschlüsseltes Verzeichnis (HINWEIS Hierbei erfolgt die korrekte Entschlüsselung)
2. Umbenennen der entschlüsselten Datei und öffnen mit dem entsprechenden Programm (HINWEIS Sollten die Originaldateinamen und Dateityp nicht mehr bekannt sein oder sich nicht mehr zuordnen lassen, so kann das Öffnen der Datei mit einem normalen Editor hilfreiche Informationen liefern)

5.9 Weitere Dokumente und FAQs

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